FPGA Benchmarking of Round 2 Candidates in the NIST Lightweight Cryptography Standardization Process: Methodology, Metrics, Tools, and Results

Kamyar Mohajerani, Richard Haeussler, Rishub Nagpal,
Farnoud Farahmand, Abubakr Abdulgadir, Jens-Peter Kaps and Kris Gaj

Cryptographic Engineering Research Group,
George Mason University
Fairfax, VA, U.S.A.

Abstract. Twenty seven Round 2 candidates in the NIST Lightweight Cryptography (LWC) process have been implemented in hardware by groups from all over the world. All implementations compliant with the LWC Hardware API, proposed in 2019, have been submitted for hardware benchmarking to George Mason University's LWC benchmarking team. The received submissions were first verified for correct functionality and compliance with the hardware API's specification. Then, the execution times in clock cycles, as a function of input sizes, have been determined using behavioral simulation. An overhead of modifying vs. reusing a key between two consecutive inputs was quantified. The compatibility of all implementations with FPGA toolsets from three major vendors, Xilinx, Intel, and Lattice Semiconductor was verified. Optimized values of the maximum clock frequency and resource utilization metrics, such as the number of look-up tables (LUTs) and flip-flops (FFs), were obtained by running optimization tools, such as Minerva, ATHENa, and Xeda. The raw post-place and route results were then converted into values of the corresponding throughputs for long, medium-size, and short inputs. The overhead of modifying vs. reusing a key between two consecutive inputs was quantified. Power consumption and energy per bit were estimated. The results were presented in the form of easy to interpret graphs and tables, demonstrating the relative performance of all investigated algorithms. For a few submissions, the results of the initial design-space exploration were illustrated as well. An effort was made to make the entire process as transparent as possible and results easily reproducible by other groups.

Keywords: Lightweight Cryptography · authenticated ciphers · hash functions · hardware · FPGA · benchmarking

Contents

1 Introduction

A comprehensive framework for fair and efficient benchmarking of hardware implementations of lightweight cryptography was proposed in [1]. This framework was based on the idea of the Lightweight Cryptography Hardware API [2], which was published in October 2019, and has remained stable since then.

The corresponding LWC Development Package has been built as a major revision of the CAESAR Development Package [3], [4] by an extended team including representatives of the Technical University of Munich (TUM), Virginia Tech, and George Mason University. The first version of this package was published on October 14, 2019. Since then, this package was updated several times, including the most recent revision in October 2020. The advantages of the LWC Development Package over the CAESAR Development Package in terms of the smaller area overhead was demonstrated in [5]. The new package also supports additional combinations of external-internal databus widths, namely {external: 32 - internal: 16} and {external: 32 - internal: 8}. The first implementations of candidates in the Lightweight Cryptography Standardization process, compliant with the LWC Hardware API and using the new development package, were reported by members of the Virginia Tech Signatures Analysis Lab in [6].

Before the start of Round 2 of the NIST Lightweight Cryptography Standardization Process in September 2019, multiple submission teams developed hardware implementations non-compliant with the proposed LWC API [7]. These implementations used very divergent assumptions, interfaces, and optimization goals. Only 7 out 32 teams (ACE, DryGASCON, ForkAE, Romulus, SKINNY, Subterranean 2.0, and WAGE) made their HDL code public, either as a part of the corresponding Round 2 submission package or the candidate website. Preliminary results reported in the algorithm specifications were based on the use of about a dozen different FPGA families (Artix-7, Cyclone IV, Cyclone V, iCE40, Spartan-3, Spartan-6, Stratix IV, Stratix V, Virtex-6, Virtex-7, and Zynq-7000) and about the same number of standard-cell ASIC libraries (28 nm FDSOI, 45 nm NanGate FreePDK, 130 nm IBM, 10 nm Intel FinFET, 65 nm and 90 nm STMicroelectronics, 65 nm TSMC, 90 nm, 130 nm, and 180 nm UMC). Only results obtained using the same FPGA family or the same ASIC library can be fairly compared with one another. As a result, before the start of this benchmarking effort, at most 6 FPGA implementations and 4 ASIC implementations could be possibly compared with one another. However, even such a limited comparison would be highly unfair because of the use of different interfaces, assumptions, and optimization targets.

2 Previous Work

The first major cryptographic competition that included a coordinated hardware benchmarking effort based on a well-defined API was CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness), conducted in the period 2013-2019 [8].

The first version of the proposed hardware API for CAESAR was reported in [9]. This version was later substantially revised, endorsed by the CAESAR Committee in May 2016, and published as a Cryptology ePrint Archive in June 2016 [10]. A relatively minor addendum was proposed in the same month, and endorsed by the CAESAR Committee in November 2016 [11].

The commonly accepted CAESAR Hardware API provided the foundation for the GMU Development Package, released in May and June 2016 [3], [12]. This package included in particular: a) VHDL code of a generic PreProcessor, PostProcessor, and CMD FIFO, common for all Round 2 and Round 3 CAESAR Candidates (except Keyak), as well as AES-GCM, b) Universal testbench common for all API-compliant designs (aead_tb), c) Python app used to automatically generate test vectors (aeadtvgen), and d) Reference

implementations of several dummy authenticated ciphers.

This package was accompanied by the Implementer's Guide to Hardware Implementations Compliant with the CAESAR Hardware API, v1.0, published at the same time [13]. A few relatively minor weaknesses of this version of the package, discovered when performing experimental testing using general-purpose prototyping boards, were reported in [14], [15].

In December 2017, a substantially revised version of the Development Package (v.2.0) and the corresponding Implementer's Guide were published by the GMU Benchmarking Team [3], [4]. The main revisions included a) Support for the development of lightweight implementations of authenticated ciphers, b) Improved support for the development of high-speed implementations of authenticated ciphers, and c) Improved support for experimental testing using FPGA boards, in applications with intermittent availability of input sources and output destinations.

It should be stressed that at no point was the use of the Development Package required for compliance with the CAESAR Hardware API. To the contrary, [13] clearly stated that the implementations of authenticated ciphers compliant with the CAESAR Hardware API could also be developed without using any resources belonging to the package [3], [12] by just following the specification [10] directly.

Despite being non-mandatory and the lack of official endorsement by the CAESAR Committee, the CAESAR Development Package played a significant role in increasing the number of implementations developed during Round 2 of the CAESAR contest. Out of 43 implementations reported before the end of Round 2, 32 were fully compliant, and one partially compliant with the CAESAR Hardware API. All fully compliant code used the GMU Development Package. The fully and partially compliant implementations covered 28 out of 29 Round 2 candidates (all except Tiaoxin) [3]. In Round 3, the submission of the hardware description language code (VHDL or Verilog) was made obligatory by the CAESAR Committee. As a result, the total number of designs reached 27 for 15 Round 3 candidates. Out of these 27 designs, 23 were fully compliant and 1 partially compliant with the CAESAR Hardware API [3]. Overall, publishing the CAESAR Hardware API, as well as its endorsement by the organizers of the contest, had a major influence on the fairness and the comprehensive nature of the hardware benchmarking during the CAESAR competition.

Several optimized lightweight implementations compliant with the CAESAR API, and based on v.2.0 of the Development Package, were reported in [16]. In [17]–[20], several other implementations were enhanced with countermeasures against Differential Power Analysis. To facilitate this enhancement, an additional Random Data Input (RDI) port was added to the CAESAR Hardware API.

Major differences between the proposed Lightweight Cryptography Hardware API and the CAESAR Hardware API, defined in [10], [11], are as follows: In terms of the Minimum Compliance Criteria: a) One additional configuration, encryption/decryption/hashing, has been added on top of the previously supported configuration: encryption/decryption. b) On top of the maximum sizes of AD/plaintext/ciphertext already supported in the CAESAR Hardware API, two additional maximum sizes, $2^{16} - 1$ and $2^{50} - 1$, have been added.

Energy and power efficiency is a major concern for lightweight applications. The NIST LWC competition places a stronger emphasis on energy and power usage as compared to previous competitions, such as eSTREAM, SHA-3, and CAESAR. Nevertheless, some previous work related to energy and power measurements exists for these competitions. During the eSTREAM competition, [21] proposed power-time, power-area-time, and energy-per-bit metrics for hardware implementations of eSTREAM Phase 3 candidates. These metrics were calculated twice for two different use cases – a fixed frequency and a fixed throughput. For high frequencies, power consumption scales linearly, and energy-per-bit is largely frequency independent, as energy is a metric of total switching activity in a

circuit [22]. [23], [24], [25], [26], and [27] utilized a similar methodology for power and energy measurements of FPGA and ASIC devices during the SHA-3, CAESAR and the current LWC competitions. [26] stated that "vector-less" simulated power measurements were comparable to experimentally obtained measurements, with an average difference of 0.7%, although a generalized magnitude of these differences is not predictable. Other techniques for power and energy measurements have been explored, such as optimizing for maximum achievable throughput, as seen in [28].

3 Methodology

3.1 LWC Hardware API

Hardware designers participating in the hardware benchmarking of Round 2 LWC candidates are expected to follow Hardware API for Lightweight Cryptography defined in detail in [2]. The major parts of this API include the minimum compliance criteria, interface, and communication protocol supported by the LWC core. The proposed API is intended to meet the requirements of all candidates submitted to the NIST Lightweight Cryptography standardization process, as well as all CAESAR candidates and the current authenticated-cipher and hash-function standards. The main reasons for defining a common API for all hardware implementations of candidates submitted to the NIST Lightweight Cryptography standardization project [7] are: a) Fairness of benchmarking, b) Compatibility among implementations of the same algorithm by different designers, and c) Ease of creating the supporting development package, aimed at simplifying and speeding up the design process.

3.2 LWC Hardware Development Package

To make the benchmarking framework more efficient in terms of the hardware development time, the designers are provided with the following resources, compliant with the use of the proposed LWC Hardware API:
a) VHDL code supporting the API protocol, common to all Lightweight Cryptography standardization process candidates, as well as all CAESAR candidates and AES-GCM (LWC_rtl)
b) Universal testbench, common for all API-compliant designs (LWC_TB)
c) Python app used to automatically generate test vectors (cryptotvgen)
d) Reference implementations of a dummy authenticated cipher and a dummy hash function (dummy_lwc)
e) Implementer's Guide, describing all steps of the development and benchmarking process, including verification, experimental testing, and generation of results [29].

It should be stressed that the *implementations of authenticated ciphers (with an optional hash functionality), compliant with the LWC Hardware API, can also be developed without using any of the aforementioned resources, by just following the specification of the LWC Hardware API directly.*

In case the Development Package is used, the major phases of the API-compliant code development process are summarized in Fig. 1. The manual design process is based on the specification and the reference C code of a given algorithm. The HDL code specific for a given algorithm is combined with the code shared among all algorithms, provided in the folder LWC_rtl of the Development Package. Comprehensive test vectors are generated automatically by cryptotvgen based on the reference C code. These vectors are used together with the universal testbench, LWC_TB, to verify the HDL code using simulation. The same testbench can also be used for timing measurements in clock cycles. These measurements can be utilized to confirm or revise formulas for the Execution Time and Throughput derived during the timing analysis phase of the Manual Design. The complete

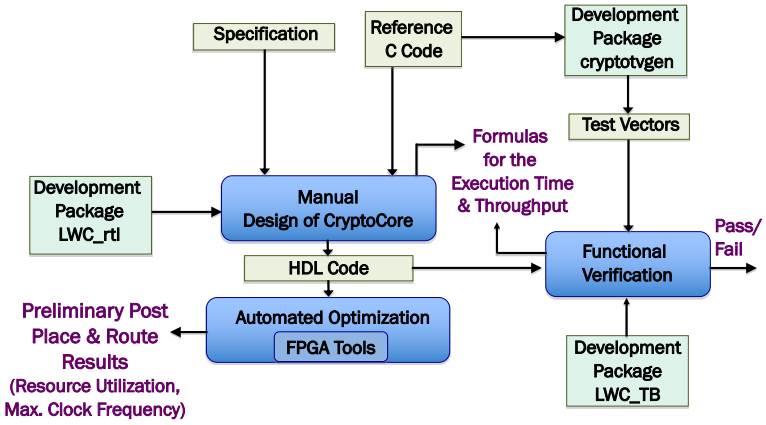

Figure 1: The API-Compliant Code Development using the Development Package

HDL code can be used by design teams to obtain the preliminary post-place & route results, such as resource utilization and maximum clock frequency.

3.3 FPGA Platforms and Tools

For the purpose of this benchmarking study, the GMU group selected three benchmarking platforms representing FPGA families of three major vendors: Xilinx, Intel, and Lattice Semiconductor. The primary criteria for the selection of FPGA devices were as follows:

1. representing widely used low-cost, low-power FPGA families
2. capable of holding SCA-protected designs (possibly using up to four times more resources than unprotected designs)
3. supported by free versions of state-of-the-art industry tools.

These criteria led to the selection of the following FPGA devices:

1. From Xilinx
   Artix-7 : xc7a12tcsg325-3, including 8,000 LUTs, 16,000 FFs, 40 18Kbit BRAMs, 40 DSPs, and 150 I/Os.
2. From Intel
   Cyclone 10 LP : 10CL016-YF484C6, including 15,408 LEs, 15,408 FFs, 56 M9K blocks, 56 multipliers (MULs), and 162 I/Os, and
3. From Lattice Semiconductor
   ECP5 : LFE5U-25F-6BG381C, including 24,000 LUTs, 24,000 FFs, 56 18Kbit blocks, 28 MULs, and 197 I/Os.

The corresponding FPGA tools capable of processing HDL code targeting these (and many other FPGA devices) were:

1. From Xilinx: Xilinx Vivado 2020.1 (lin64)
2. From Intel: Intel Quartus Prime Lite Edition Design Software, ver. 20.1
3. From Lattice Semiconductor: Lattice Diamond Software v3.11 SP2.

3.4 Optimization Target

FPGA implementations of lightweight authenticated ciphers can be developed using various optimization targets. Examples include:

1. maximum throughput assuming a certain limit on resource utilization,
2. minimum resource utilization assuming a certain minimum throughput, and
3. minimum power consumption assuming a certain minimum throughput.

Generally, the more resources the implementation is allowed to use and more power to consume, the faster it can run. An additional constraint may be the need for a circuit to operate at a specific fixed clock frequency, unrelated to the critical path of the circuit (e.g., 100 kHz).

The problem with approaches 2. and 3. is that the minimum required throughput depends strongly on an application. Multiple minimum throughputs may have to be supported by implementations of a future lightweight cryptography standard. Approach 1. is more manageable, especially after the choice of a specific FPGA platform. Our underlying assumption is that the implementation of an LWC algorithm *protected against side-channel attacks* should take no more than all look-up tables (LUTs) of the selected Xilinx FPGA device, Artix-7 : xc7a12tcsg325-3. Taking into account that protected implementations take typically up to 3-4 times more LUTs than unprotected implementations, our unprotected design should take no more than one-fourth of the total number of LUTs, i.e., 2000 LUTs. At the same time, we assume that the benchmarked implementations are not permitted to use any family-specific embedded resources, such as Block RAMs, DSP units, or embedded multipliers. Any storage should be implemented using either flip-flops or distributed memory, which, in the case of Xilinx FPGAs, is built out of LUTs. The number of Artix-7 flip-flops is limited to 4000, as in this FPGA family each LUT is accompanied by two flip-flops. The designs are also prohibited from using any family-specific primitives or megafunctions.

This proposed optimization target has been clearly communicated to all LWC submission teams, through the document titled Suggested FPGA Design Goals, posted on the LWC hardware benchmarking project website [29], as well as announcements on the lwc-forum, and private communication.

At the same time, it was never our intention to strictly enforce it. Instead, the designers have been encouraged to develop several alternative architectures, such as:

1. Basic-iterative architecture
   (a) Executing one round per clock cycle in block-cipher-based submissions
   (b) Generating one output bit per clock cycle in stream-cipher-based submissions.
2. Architectures most natural for a given authenticated cipher, such as those based on
   (a) Folding in block-cipher-based submissions
   (b) Generating 2^d bits per clock cycle in stream-cipher-based submissions.
3. Maximum throughput, assuming
   - 1000 or less LUTs
   - 2000 or less FFs
   - No BRAMs and no DSP units

   of Xilinx Artix-7 FPGAs.
   Other limits, such as 1500 LUTs, 500 LUTs, etc. are welcome too.

3.5 Deliverables

The format of deliverables was described in detail in the document titled LWC HDL Code: Suggested List of Deliverables, posted on the LWC hardware benchmarking project website [29]. Two very important parts of each submission were files: `assumptions.txt` and `variants.txt`.

The former document can be used to describe any non-standard assumptions (including any deviations from the LWC Hardware API), usage and the modifications in the LWC Development Package, the expected order of segments (such as Npub, AD, plaintext) at the input to the LWC unit, etc.

The latter file, `variants.txt`, is used to define various variants of the hardware design. Different variants may correspond to

- different algorithms of the same family described in a single submission to the NIST LWC standardization process
- different parameter sets, such as sizes of keys, nonces, tags, etc.
- support for AEAD vs. AEAD+Hash
- different hardware architectures, e.g., basic iterative, folded, unrolled, pipelined, etc.
- different parameters of the external interface, such as widths of the input and output buses.

Each variant is expected to be fully characterized in terms of its design goals, corresponding reference software implementation, non-default values of generics and constants, block sizes (for AD, plaintext, ciphertext, and hash message), and detailed formulas for the execution times of all major operations (authenticated encryption, authenticated decryption, and hashing), expressed in clock cycles.

3.6 Functional Verification

All submitted implementations were first investigated in terms of compliance with the LWC Hardware API and the completeness of their deliverables, requested for benchmarking. In particular, the compliance with the two-pass interface ([2], Fig. 2) and the use of an external FIFO was expected from two-pass implementations.

Then, a comprehensive set of new test vectors, unknown in advance to hardware designers, was generated separately for each variant of each algorithm. These tests included multiple special cases, such as empty AD, empty plaintext, various widths of an incomplete last block, etc. If these test vectors passed, the implementation was judged functionally correct and compliant with the LWC Hardware API. If these test vectors failed, the source of failure was investigated in close collaboration with hardware designers. Our original testbench was extended with additional features and a post-processing program to clearly document all test-vector failures. Log files generated by this program were passed back to hardware designers.

The designers were allowed to submit revised versions of their code. In some cases, an error was on the side of the benchmarking team. For example, an incorrect version of the reference implementation was used, or incorrect order of segments (such as Npub, AD, plaintext, ciphertext, tag) at the PDI input to the LWC core was assumed. In other cases, the previously-submitted HDL code had to be modified by the designers.

3.7 Timing Measurements

The testbench LWC_TB, being a part of the LWC Development package, has been extended to include support for measurements of the execution times for authenticated

encryption, authenticated decryption, and hashing. In the current version of this testbench, these measurements rely on the proper implementation of an optional output of the LWC core called do_last. In the cases when the hardware teams did not implement this output, requests were made to support this relatively straightforward extension.

Then, the testbench was used to measure the execution times for:

1. Input sizes used in the definitions of benchmarking metrics, such as 16 bytes, 64 bytes, 1536 bytes, N input blocks, $N + d$ input blocks, with $N = 4$ and $d = 1$ or 2, and three major input types: AD only, Plaintext (PT)/Ciphertext (CT) only, equal-size AD and Plaintext/Ciphertext (AD+PT/AD+CT).

2. All possible AD and plaintext lengths (in bytes) between 0 and 2 full input blocks, in increments of one byte.

The measurement results were compared with expected execution times, based on formulas provided by the design teams. The ideal match was very rare. However, in most cases, the difference between the execution times for $N + d$ and N blocks, required for the calculation of throughput for large inputs, was correct. Simultaneously, the actual execution times differed from expected execution times by a constant for all investigated input sizes. This kind of differences were considered minor.

In other cases, the differences between the actual and expected execution times were dependent on the input type (e.g., AD only, PT only, or AD+PT). Still, in others, they were dependent on the input lengths. In most cases, such mismatches were reported back to hardware designers.

In no case, values of the final benchmarking metrics, such as throughputs for particular input sizes were calculated based on estimated values. In all cases, only the execution times obtained experimentally, using the timing measurements, were used to calculate values of the corresponding throughputs.

In most cases, the task of deriving the detailed execution-time formulas was left as the future work for design teams.

3.8 Synthesis, Implementation, and Optimization of Tool Options

As a next step, each variant of each code was prepared in a separate folder for synthesis and implementation. This preparation was based primarily on the file `source_list.txt`, containing the list of all synthesizable files in the bottom-up order, i.e., packages and low-level units first, and the top-level unit last. Additionally, the description of each variant in the file `variants.txt` was crucial as well.

In a limited number of cases, the synthesis did not work with any of the three FPGA toolsets we used. As a result, the resubmission of the code was required. In some other cases, the problems concerned a single FPGA toolset. If any of such problems occurred, the designers were provided with the corresponding synthesis reports and requested to investigate the source of synthesis errors and warnings.

The determination of the maximum clock frequency and the corresponding resource utilization was performed using tools specific for each FPGA vendor. For Artix-7 FPGAs, Minerva: An Automated Hardware Optimization Tool described in [30], was used. The average time required to find the optimum requested clock frequency and the best optimization strategy was about 3.5 hours per algorithm variant. Still, in some cases, hardware design teams were able to generate better results by themselves. The source of such discrepancies is still under investigation, but possible reasons include different versions of Vivado, use vs. no use of the out-of-context mode, limited time that could be devoted to each Minerva run (affecting tool options), etc.

For Intel FPGAs, ATHENa – Automated Tool for Hardware EvaluatioN [31], was used. This tool supports all recent Intel FPGA families as well as older Xilinx FPGA

families before Series 7. Within this tool, we used the following settings: APPLICATION=GMU_optimization_1, and the OPTIMIZATION_TARGET=Balanced.

A new tool, Xeda[32], which stands for cross (X) electronic design automation, was developed. Xeda provides a layer of abstraction over simulation and synthesis tools and removes the difficulty associated with testing a design across multiple FPGA vendors. Additionally, Xeda allows user-made plugins that can extend functionality to new tools or allow for post-processing of synthesis and simulation results.

For Lattice Semiconductor FPGAs, Xeda and a plugin developed to find the maximum clock frequency were used. Only a single optimization strategy (i.e., the collection of flow settings), targeting optimal timing, was considered. The synthesis was performed using both the Lattice Synthesis Engine (LSE) and Synplify Pro. Only the better of the two results were reported.

3.9 Performance Metrics

The following performance metrics have been evaluated as a part of the Round 2 LWC Benchmarking Project:
Metrics obtained from tool reports after placing and routing:

1. Resource utilization
   Number of LUTs for Artix-7 and ECP5 FPGAs, LEs for Cyclone 10 LP FPGAs, and flip-flops for all FPGAs, assuming no use of embedded memories (such as BRAMs), DSP units, and embedded multipliers.

2. Maximum clock frequency in MHz.
   This metric by itself is not used for ranking of algorithms, but it affects other metrics defined below.

Metrics calculated based on universal formulas, with variables replaced by values obtained from tool reports and timing measurements:

1. Throughput in Mbits/s
   for the following sizes of inputs

   (a) Long [with Throughput = d·Block_size/(Time(N+d blocks)−Time(N blocks))]
   (b) 1536 bytes
   (c) 64 bytes
   (d) 16 bytes.

   All throughputs are calculated separately for

   - AD, plaintext (PT), AD+PT (sender's side)
   - AD, ciphertext (CT), AD+CT (receiver's side), and
   - hash message.

   We assume no difference in the execution time depending on the result of verification on the receiver's side.

2. Energy per bit in nJ/s
   as described in detail in Section 6.

Both Throughput and Energy per bit may be evaluated under different assumptions. The three commonly used assumptions are

1. each design operates at the maximum clock frequency determined by its critical path in the given FPGA device

2. each design operates at the fixed clock frequency determined by an application or the LWC core's integration with other parts of the entire system on chip

3. each design operates at the frequency corresponding to the fixed throughput, common for all designs, determined by an application or the LWC core's communication with other parts of the system.

In Section 5, we present our analysis of Throughput and Resource utilization under assumption 1., most consistent with the design goal communicated to the hardware developers at the beginning of this study. In Section 6, we discuss our results in terms of Energy per bit, Throughput, and Resource utilization under assumption 2., most commonly used in the evaluations of Energy per bit for competing implementations of the same functionality.

4 Hardware Designs

An overview of hardware design packages submitted for benchmarking is given in Table 1. A total of 40 design packages were received. These designs covered 27 out of 32 Round 2 candidates. For Ascon four and for Gimli and Xoodyak three independent design packages were received. Candidates implemented independently by two different primary designers included ACE, COMET, GIFT-COFB, SpoC, Subterranean 2.0, and TinyJAMBU.

Several hardware design groups contributed more than one hardware design package. In particular,

- George Mason University Cryptographic Engineering Research Group (CERG), USA, implemented 14 candidates: ACE, Ascon, Elephant, GIFT-COFB, Gimli, mixFeed, PHOTON-Beetle, Pyjamask, Saturnin, SKINNY-AEAD, SPIX, Subterranean 2.0, TinyJAMBU, and Xoodyak;
- Virginia Tech Signatures Analysis Lab, USA, contributed implementations of 5 candidates: Ascon, COMET, GIFT-COFB, SCHWAEMM & ESCH, and Spoc;
- CINVESTAV-IPN, Mexico, contributed implementations of 4 candidates: COMET, ESTATE, LOCUS-AEAD/LOTUS-AEAD, and Oribatida;
- Institute of Applied Information Processing and Communications, TU Graz, Austria, implemented 2 candidates: Ascon and ISAP.

The following submissions were provided by co-authors of algorithms submitted to the NIST LWC standardization process: ACE, ESTATE, ForkAE, Gimli, ISAP, KNOT, LOCUS-AEAD/LOTUS-AEAD, Oribatida, Romulus, Spook, Subterranean 2.0, TinyJAMBU, WAGE, and Xoodyak.

The implementation of DryGASCON was developed by an independent researcher, Ekawat Homsirikamol, in close collaboration with the author of the algorithm. An additional implementation of Gimli was contributed by members of the Chair of Security in Information Technology at the Technical University of Munich, Germany.

Most groups used VHDL. Four design teams used exclusively Verilog for the implementation of the entire LWC unit. As a result, these implementations did not take advantage of the LWC Development Package, available only in VHDL. Hardware design packages developed this way included those for Gimli (by the Gimli Team), Romulus, Spook-v2, and Subterranean 2.0 (by the Subterranean 2.0 Team). Four implementations modeled only the part unique to a given algorithm, its CryptoCore, in Verilog. These designs included DryGASCON, KNOT, and two submissions for SpoC. The following submissions from GMU have been implemented purely in Bluespec SystemVerilog, depending on its own Bluespec LWC development package [33]: Ascon (Ascon_GMU and Ascon_GMU2), GIFT-COFB, Gimli, Subterranean 2.0, and Xoodyak (Xoodyak_GMU2).

Table 1: Overview of hardware design packages submitted for FPGA benchmarking

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designers	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
1a	ACE	ComSec Lab University of Waterloo Canada	Mark Aagaard https://ece.uwaterloo.ca/ ∼maagaard maagaard@uwaterloo.ca Nusa Zidaric nzidaric@uwaterloo.ca	Mark Aagaard https://ece.uwaterloo.ca/ ∼maagaard maagaard@uwaterloo.ca Guang Gong https://ece.uwaterloo.ca/ ∼ggong ggong@uwaterloo.ca	Yes, Modified	VHDL	1
1b	ACE	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Omar Zabala-Ferrera ozabalaf@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	1
2a	Ascon	Institute of Applied Information Processing and Communications, TU Graz, Austria	Robert Primas https://rprimas.github.io rprimas@gmail.com	Stefan Mangard https://www.iaik.tugraz.at/ person/stefan-mangard stefan.mangard@ iaik.tugraz.at	Yes, Unmodified	VHDL	6
2b	Ascon	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
2c	Ascon	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/ team/rishub.php rnagpal2@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	No	Bluespec SystemVerilog	2
2d	Ascon	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Kamyar Mohajerani https://crytpography.gmu.edu/ team/mmohajer.php mmohajer@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	No	Bluespec SystemVerilog	3
3a	COMET	CINVESTAV, Mexico	Jose A. Bernal jose.bernal@cinvestav.mx, Cuauhtemoc Mancillas-Lopez cuauhtemoc.mancillas@ cinvestav.mx	Francisco Rodriguez-Henriquez franccisco.cinvestav.mx Cuauhtemoc Macillas_Lopez cuauhtemoc.mancillas@ cinvestav.mx	Yes, Unmodified	VHDL	3

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
3b	COMET	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@ vt.edu	Yes, Modified	VHDL	2
4	DryGASCON	Independent (previously CERG GMU)	Ekawat Homsirikamol ekawat@gmail.com		Yes, Unmodified	Verilog (CryptoCore)	1
5	Elephant	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Richard Haeussler https://crytpography.gmu.edu/ team/rhaeuss.php rhaeussl@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	5
6	ESTATE	CINVESTAV-IPN, Mexico	Cuauhtemoc Mancillas Lopez cuauhtemoc.mancillas@ cinvestav.mx http://www.cs.cinvestav.mx/ Investigadores/Cmancillas		Yes, Modified	VHDL	4
7	ForkAE	ForkAE Team	Antoon Purnal antoon.purnal@kuleuven.be Jowan Pittevils r0626755@student.kuleuven.be		Yes, Unmodified	Verilog (CryptoCore)	2
8a	GIFT-COFB	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	1
8b	GIFT-COFB	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Kamyar Mohajerani https://crytpography.gmu.edu/ team/mmohajer.php mmohajer@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	No	Bluespec SystemVerilog	6
9a	Gimli	Gimli Team	Pedro Maat Costa Massolino https://www.pmassolino.xyz pmaat@protonmail.com		No	Verilog (LWC)	7
9b	Gimli	Chair of Security in Information Technology, Technical University of Munich, Germany	Patrick Karl patrick.karl@tum.de	Michael Tempelmeier michael.tempelmeier@ tum.de	Yes, Unmodified	VHDL	3
9c	Gimli	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Kamyar Mohajerani https://crytpography.gmu.edu/ team/mmohajer.php mmohajer@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	No	Bluespec SystemVerilog	4

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
10	ISAP	Institute of Applied Information Processing and Communications, TU Graz, Austria	Robert Primas https://rprimas.github.io rprimas@gmail.com	Stefan Mangard https://www.iaik.tugraz.at/person/stefan-mangard stefan.mangard@iaik.tugraz.at	Yes, Modified	VHDL	4
11	KNOT	KNOT Team, Tsinghua University, China	Bohan Yang bohanyang@tsinghua.edu.cn, Zhengdong Li lizd@tsinghua.edu.cn	Wentao Zhang zhangwentao@iie.ac.cn, Leibo Liu liulb@tsinghua.edu.cn	Yes, Unmodified	Verilog (CryptoCore)	16
12	LOCUS-AEAD & LOTUS-AEAD	CINVESTAV-IPN, Mexico	Brisbane Ovilla Martinez brisbane@cinvestav.mx		Yes, Unmodified	VHDL	4
13	mixFeed	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Eduardo R. Ferrufino https://cryptography.gmu.edu/team/eferruf.php eferruf@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	1
14	Oribatida	CINVESTAV-IPN, Mexico	Cuauhtemoc Mancillas López cuauhtemoc.mancillas@cinvestav.mx, Alberto F. Martínez Herrera alberto.herrera.tec@gmail.com		Yes, Unmodified	VHDL	2
15	PHOTON-Beetle	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Vivian Ledynh vledynh@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	1
16	Pyjamask	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/team/rishub.php rnagpal2@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
17	Romulus	Romulus-Team, Symmetric Key and Lightweight Cryptography Lab (SyLLab), Nanyang Technological University, Singapore	Mustafa Khairallah http://www.mustafa-khairallah.com mustafam001@e.ntu.edu.sg	Thomas Peyrin https://thomaspeyrin.github.io/web/ thomas.peyrin@ntu.edu.sg	No	Verilog (LWC)	5

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
18	Saturnin	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/team/rishub.php rnagpal2@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
19	SCHWAEMM & ESCH	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Flora Coleman googly2@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
20	SKINNY-AEAD	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Scott Carlson scarlso9@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
21	SPIX	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Ayman Abbas aabbas8@gmu.edu Luke Beckwith lbeckwit@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	4
22a	SpoC_VT	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	William Diehl wdiehl@vt.edu		Yes, Modified	Verilog (CryptoCore)	1
22b	SpoC_IIT	VLSI Group, IIT Tirupati, India	A. Sathvik ee17b002@iittp.ac.in, T. Rahul ee17b030@iittp.ac.in	Vikramkumar Pudi vikram@iittp.ac.in, Anubhab Baksi anubhab001@e.ntu.edu.sg	Yes, Unmodified	Verilog (CryptoCore)	1
23	Spook-v2	Spook Team	Davide Bellizia davide.bellizia@uclouvain.be, Gaetan Cassiers gaetan.cassiers@uclouvain.be, Charles Momin charles.momin@uclouvain.be	François-Xavier Standaert fstandae@uclouvain.be	No	Verilog (LWC)	1
24a	Subterranean 2.0	Subterranean 2.0 Team	Pedro Maat Costa Massolino https://www.pmassolino.xyz pmaat@protonmail.com		No	Verilog (LWC)	1
24b	Subterranean 2.0	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Kamyar Mohajerani https://crytpography.gmu.edu/team/mmohajer.php mmohajer@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	No	Bluespec SystemVerilog	1

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
25a	TinyJAMBU	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Sammy Lin https://cryptography.gmu.edu/team/slin5.php slin5@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	3
25b	TinyJAMBU	TinyJAMBU Team	Tao Huang huangtaochn@gmail.com	Hongjun Wu https://www3.ntu.edu.sg/home/wuhj wuhongjun@gmail.com	Yes, Unmodified	VHDL	3
26	WAGE	ComSec Lab University of Waterloo Canada	Mark Aagaard https://ece.uwaterloo.ca/∼maagaard maagaard@uwaterloo.ca Nusa Zidaric nzidaric@uwaterloo.ca	Mark Aagaard https://ece.uwaterloo.ca/∼maagaard maagaard@uwaterloo.ca Guang Gong https://ece.uwaterloo.ca/∼ggong ggong@uwaterloo.ca	Yes, Modified	VHDL	1
27a	Xoodyak	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Richard Haeussler https://crytpography.gmu.edu/team/rhaeuss.php rhaeussl@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
27b	Xoodyak	Xoodyak Team + Silvia	Silvia Mella silvia.mella@st.com		Yes, Unmodified	VHDL	12
27c	Xoodyak	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Kamyar Mohajerani https://crytpography.gmu.edu/team/mmohajer.php mmohajer@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	No	Bluespec SystemVerilog	2
						Total	**124**

Twelve submissions contained a single variant. In the remaining, the number of variants varied between 2 and 16, with an average of 3.3 per hardware design submission. Most of the variants of the same algorithm share a significant portion of the HDL source code and differ only in values of generics or constants. In some cases, a separate source code was provided for each variant.

The total number of implemented variants reached 124. In Table 2, we summarize the basic features of each variant and assign each variant a unique name used in the rest of the paper. For algorithms implemented by a single group, this name consists of the name of the algorithm followed by "-<variant_number>". For algorithms implemented by two groups, we add "_<Group_Name_Abbreviation>" after the algorithm name. The abbreviations used are: CI for CINVESTAV-IPN, GMU for George Mason University, Graz for TU Graz, Austria, GT for Gimli Team, VT for Virginia Tech, IIT for IIT Tirupati, TJT for TinyJAMBU Team, UW for the University of Waterloo, and XT for Xoodyak Team + Silvia. For Spook, exceptionally, the name of the variant is Spook-v2-v2. In this name, the first v2 indicates version 2 of Spook proposed in [34]. This version is known to have higher security margins at the cost of relatively small performance overheads [34]. The second v2 indicates that it is the second, improved submission, received in November 2020.

For each variant, we also list the name of the corresponding reference software implementation. Most of these implementations can be found in the most recent version of SUPERCOP [35]. Some were submitted as a part of the hardware package (KNOT and WAGE) or were provided through the candidate's website (Subterranean 2.0).

The maximum length of inputs that can be processed by the implementations is often unlimited by the hardware design itself. In such cases, the designers either stated the maximum length required by the NIST Submission Requirements and Evaluation Criteria [7], $2^{50} - 1$, declared the maximum length as "unlimited", or left the respective field of `variants.txt` blank. The following designs have the maximum length specified explicitly as $2^{16} - 1$: two-pass implementations (ESTATE, ISAP, and Saturnin) and implementations performing precomputations dependent on the maximum input size (COMET_CI, ForkAE, and Pyjamask).

The following designs do not support key reuse between consecutive inputs: Gimli_GT (v1-v7), Gimli_GMU (v1-v5), SPIX (v1, v2, v2x2, v2x4), Subterranean_ST (v2), Subterranean_GMU (v1), TinyJAMBU_GMU (v1-v3), Xoodyak_XT (v1-v12), and Xoodyak_GMU2 (v1-v2). For algorithms that support key reuse, we list in a separate column the number of additional clock cycles required to load a new key. This number has been determined experimentally through our own measurements and often differed from the value provided as a part of the submission package. The highest overhead for loading a new key was observed in the case of Pyjamask-v1 (433 cycles), Xoodyak_GMU-v2 (266 cycles), and Pyjamask-v2 (245 cycles). The smallest overhead of 3 clock cycles was measured for Ascon_Graz (v1 and v2), Gimli_TUM (v1-v3), ISAP-v4, and SKINNY-AEAD (v1-v2). The second smallest overhead of 4 clock cycles was obtained for DryGASCON-v1, ISAP-v2, ISAP-v3, LOCUS (v1-v2), LOTUS (v1-v2), TinyJAMBU_TJT-v2, and TinyJAMBU_TJT-v3.

In Table 3, we summarize basic properties of each design variant. The following properties are specific to an algorithm and its parameter set: AD block size, Plaintext (PT)-Ciphertext (CT) block size, Hash block size. All these block sizes are expressed in bits. The numbers of clock cycles per block are influenced by the combination of the algorithm, parameter set, and hardware architecture. In authenticated ciphers based on block ciphers or permutations, basic iterative architecture is defined as an architecture executing one round of the underlying block cipher/permutation per clock cycle. In authenticated ciphers based on stream ciphers, basic iterative architecture is defined as an architecture calculating one basic block (typically one bit) of the output per clock cycle. The number of clock cycles decreases in unrolled architectures and increases in folded

514 architecture. The resource utilization in LUTs changes in the opposite direction.

Table 2: Unique names and features of the hardware design variants, including the maximum input length and support for key reuse.

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
1a	ACE_UW-v1	ACE-AE-128 & ACE-H-256	aceae128v1 acehash256v	Y	7	N/A
1b	ACE_GMU-v1	ACE-AE-128 & ACE-H-256	aceae128v1 acehash256v1	Y	8	N/A
2a	Ascon_Graz-v1	Ascon-128 & Ascon-Hash, Basic iterative	ascon128v12 asconhashv12	Y	3	unlimited
	Ascon_Graz-v2	Ascon-128a & Ascon-Hash, Basic iterative	ascon128av12 asconhashv12	Y	3	unlimited
	Ascon_Graz-v3	Ascon-128a & Ascon-Hash, 2× Unrolled	ascon128av12 asconhashv12	Y	3	unlimited
	Ascon_Graz-v4	Ascon-128a & Ascon-Hash, 2× Unrolled	ascon128av12 asconhashv12	Y	3	unlimited
	Ascon_Graz-v5	Ascon-128a & Ascon-Hash, 3× Unrolled	ascon128av12 asconhashv12	Y	3	unlimited
	Ascon_Graz-v6	Ascon-128a & Ascon-Hash, 4× Unrolled	ascon128av12 asconhashv12	Y	3	unlimited
2b	Ascon_VT-v1	Ascon-128, Basic iterative	ascon128v12	Y	8	N/A
	Ascon_VT-v2	Ascon-128 & Ascon-Hash, Basic iterative	ascon128v12, asconhashv12	Y	8	N/A
2c	Ascon_GMU-v1	Ascon-128a, 2× Unrolled	ascon128av12	Y	7	unlimited
	Ascon_GMU-v2	Ascon-128a Basic iterative	ascon128av12	Y	7	unlimited
2d	Ascon_GMU2-v1h	Ascon-128 & Ascon-Hash Basic iterative	ascon128v12, asconhashv12	Y	8	unlimited
	Ascon_GMU2-v2h	Ascon-128 & Ascon-Hash 2× Unrolled	ascon128v12, asconhashv12	Y	8	unlimited
	Ascon_GMU2-v3h	Ascon-128 & Ascon-Hash 3× Unrolled	ascon128v12, asconhashv12	Y	8	unlimited
3a	COMET_CI-v1	Folded architecture	comet128aesv1	Y	8	$2^{16}-1$
	COMET_CI-v2	Folded architecture	comet128aesv1	Y	23	$2^{16}-1$
	COMET_CI-v3	Folded architecture	comet128aesv1	Y	5	$2^{16}-1$
3b	COMET_VT-v1	Basic iterative architecture	comet128aesv1	Y	7	N/A
	COMET_VT-v2	Basic iterative architecture	comet128chamv1	Y	8	N/A

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
4	DryGASCON-v1	Basic iterative architecture, support for hashing	drygascon128k32 (aead) drygascon128 (hash)	Y	4	N/A
5	Elephant-v1	Basic iterative	elephant160v1	Y	84	unlimited
	Elephant-v2	5× Unrolled	elephant160v1	Y	20	unlimited
	Elephant-v3	4× Unrolled	elephant160v1	Y	84	unlimited
	Elephant-v4	2× Unrolled	elephant160v1	Y	39	unlimited
	Elephant-v5	4× Unrolled	elephant160v1	Y	19	unlimited
6	ESTATE-v1	Two-pass AES-based, 32-bit datapath	estatetweaes128v1	Y	8	$2^{16}-1$
	ESTATE-v2	Two-pass AES-based, 8-bit datapath	estatetweaes128v1	Y	23	$2^{16}-1$
	ESTATE-v3	Two-pass Gift-based, 32-bit datapath	estatetwegift128v1	Y	8	$2^{16}-1$
	ESTATE-v4	Two-pass, Gift-based, 8-bit datapath	estatetwegift128v1	Y	16	$2^{16}-1$
7	ForkAE-v1	Area-focused	paefforkskinnyb-128t288n104v1	Y	23	$2^{16}-1$
	ForkAE-v2	Basic iterative	paefforkskinnyb-128t288n104v1	Y	23	$2^{16}-1$
8a	GIFT-COFB_VT-v1	Basic iterative	giftcofb128v1	Y	8	N/A
8b	GIFT-COFB_GMU-v1	Basic iterative	giftcofb128v1	Y	7	unlimited
	GIFT-COFB_GMU-v2	2× Unrolled	giftcofb128v1	Y	7	unlimited
	GIFT-COFB_GMU-v3	4× Unrolled	giftcofb128v1	Y	7	unlimited
	GIFT-COFB_GMU-v4	5× Unrolled	giftcofb128v1	Y	7	unlimited
	GIFT-COFB_GMU-v5	8× Unrolled	giftcofb128v1	Y	7	unlimited
	GIFT-COFB_GMU-v6	10× Unrolled	giftcofb128v1	Y	7	unlimited
9a	Gimli_GT-v1	Basic iterative	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v2	2× Unrolled	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v3	3× Unrolled	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v4	4× Unrolled	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v5	6× Unrolled	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v6	8× Unrolled	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v7	12× Unrolled	gimli24v1	N		$2^{50}-1$
9b	Gimli_TUM-v1	Customized FSM based on 3×32-bit register, RAM-based state-memory, 32-bit datapath	gimli24v1	Y	3	N/A
	Gimli_TUM-v2	Customized FSM based on 3×32-bit register, RAM-based state-memory, 16-bit datapath	gimli24v1	Y	3	N/A
	Gimli_TUM-v3	Customized FSM based on 3×32-bit register, RAM-based state-memory, 8-bit datapath	gimli24v1	Y	3	N/A

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
9c	Gimli_GMU-v1	Basic iterative	gimli24v1	N		$2^{50}-1$
	Gimli_GMU-v2	2× Unrolled	gimli24v1	N		$2^{50}-1$
	Gimli_GMU-v4	4× Unrolled	gimli24v1	N		$2^{50}-1$
	Gimli_GMU-v5	6× Unrolled	gimli24v1	N		$2^{50}-1$
10	ISAP-v1	Two-pass, Folded	isapk128av20	Y	9	$2^{16}-1$
	ISAP-v2	Two-pass, Folded	isapa128av20	Y	4	$2^{16}-1$
	ISAP-v3	Two-pass, Folded	isapk128av20	Y	4	$2^{16}-1$
	ISAP-v4	Two-pass, Folded	isapa128av20	Y	3	$2^{16}-1$
11	KNOT-v1x1	KNOT-AEAD (128, 256, 64), Basic iterative	submitted with HW package	Y	7	unlimited
	KNOT-v1x1h	KNOT-AEAD (128, 256, 64), Basic iterative support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v1x2	KNOT-AEAD (128, 256, 64), 2× Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v1x2h	KNOT-AEAD (128, 256, 64), 2× Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v1x4	KNOT-AEAD (128, 256, 64), 4× Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v1x4h	KNOT-AEAD (128, 256, 64), 4× Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v2x1	KNOT-AEAD (128, 384, 192), Basic iterative	submitted with HW package	Y	7	unlimited
	KNOT-v2x1h	KNOT-AEAD (128, 384, 192), Basic iterative support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v2x2	KNOT-AEAD (128, 384, 192), 2× Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v2x2h	KNOT-AEAD (128, 384, 192), 2× Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v2x4	KNOT-AEAD (128, 384, 192), 4× Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v2x4h	KNOT-AEAD (128, 384, 192), 4× Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v3	KNOT-AEAD (192, 384, 96), Basic iterative	submitted with HW package	Y	9	unlimited
	KNOT-v3h	KNOT-AEAD (192, 384, 96), Basic iterative support for hashing	submitted with HW package	Y	9	unlimited

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	KNOT-v4	KNOT-AEAD (256, 512, 128), Basic iterative	submitted with HW package	Y	11	unlimited
	KNOT-v4h	KNOT-AEAD (256, 512, 128), Basic iterative support for hashing	submitted with HW package	Y	11	unlimited
12	LOCUS-v1	LOCUS, 32-bit datapath	twegift-64locusaeadv1	Y	4	unlimited
	LOCUS-v2	LOCUS, 64-bit datapath	twegift-64locusaeadv1	Y	4	unlimited
	LOTUS-v1	LOTUS, 32-bit datapath	twegift-64lotusaeadv1	Y	4	unlimited
	LOTUS-v2	LOTUS, 64-bit datapath	twegift-64lotusaeadv1	Y	4	unlimited
13	mixFeed-v1	Folded architecture	mixfeed	Y	8	$2^{50}-1$
14	Oribatida-v1	Oribatida256 256-bit datapath	oribatida256v12	Y	8	unlimited
	Oribatida-v2	Oribatida192 192-bit datapath	oribatida192v12	Y	8	unlimited
15	PHOTON-Beetle-v1	AEAD+Hash	photonbeetle-aead128rate128v1, photonbeetle-hash256rate32v1	Y	6	$2^{50}-1$
16	Pyjamask-v1	Pyjamask128d16, folded architecture	pyjamask 128aeadv1	Y	433	$2^{16}-1$
	Pyjamask-v2	Pipeline implementation of MixRows	pyjamask 128aeadv1	Y	245	$2^{16}-1$
17	Romulus-v1	Round based architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v2	Two-Round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v3	Four-round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v4	Eight-round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v5	Low-area architecture	romulusn1v12	Y	22	$2^{50}-1$
18	Saturnin-v1	Folded architecture	saturninctrcascadev2 saturninhashv2	Y	20	$2^{16}-1$
	Saturnin-v2	Unrolled SuperRound	saturninctrcascadev2 saturninhashv2	Y	20	$2^{16}-1$
19	SCHWAEMM-v1	Schwaemm-256128, AEAD only, Basic iterative architecture	schwaemm-256128v1	Y	8	N/A
	SCHWAEMM-v2	Schwaemm-256128 and Esch256 AEAD+HASH	schwaemm-256128v1, esch256v1	Y	8	N/A
20	SKINNY-AEAD-v1	Member M1, Basic iterative	skinnyaeadtk3128128v1	Y	3	unlimited

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	SKINNY-AEAD-v2	Member M2, Basic iterative	skinnyaeadtk396128v1	Y	3	unlimited
21	SPIX-v1	SB-64 8× Unrolled	spix128v1	N		unlimited
	SPIX-v2	SB-64 iterative	spix128v1	N		unlimited
	SPIX-v2x2	SB-64 2× Unrolled	spix128v1	N		unlimited
	SPIX-v2x4	SB-64 4× Unrolled	spix128v1	N		unlimited
22a	SpoC_VT-v1	spoc64, Basic iterative architecture	spoc64 sliscplight 192v1	Y	7	N/A
22b	SpoC_IIT-v1	spoc128, Basic iterative architecture	spoc128 sliscplight 256v1	Y	7	N/A
23	Spook-v2-v2	Folded architecture resource sharing Clyde128 Shadow512	spook 128su512v2	Y	7	unlimited
24a	Subterranean_ST-v2	32-bit bus	subterraneanv1	N		$2^{50}-1$
24b	Subterranean_GMU-v1	32-bit bus	subterraneanv1	N		$2^{50}-1$
25a	TinyJAMBU_GMU-v1	32-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$
	TinyJAMBU_GMU-v2	16-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$
	TinyJAMBU_GMU-v3	Bit-serial NLFSR	tinyjambu128	N		$2^{50}-1$
25b	TinyJAMBU_TJT-v1	8-step state update	tinyjambu128	Y	15	$2^{50}-1$
	TinyJAMBU_TJT-v2	32-step state update	tinyjambu128	Y	4	$2^{50}-1$
	TinyJAMBU_TJT-v3	128-step state update	tinyjambu128	Y	4	$2^{50}-1$
26	WAGE-v1	Baseline	submitted with HW package	Y	7	N/A
27a	Xoodyak_GMU-v1	384-bit datapath AEAD+Hash	xoodyakv1	Y	18	unlimited
	Xoodyak_GMU-v2	128-bit datapath AEAD+Hash	xoodyakv1	Y	266	unlimited
27b	Xoodyak_XT-v1	Basic iterative architecture, AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v2	2× Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v3	3× Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v4	4× Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v5	6× Unrolled AEAD	xoodyakv1	N		unlimited

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	Xoodyak_XT-v6	12× Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v7	Basic iterative architecture, AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v8	2× Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v9	3× Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v10	4× Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v11	6× Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v12	12× Unrolled AEAD+Hash	xoodyakv1	N		unlimited
27c	Xoodyak_GMU2-v1	Basic iterative 384-bit datapath AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_GMU2-v2	2× Unrolled 384-bit datapath AEAD+Hash	xoodyakv1	N		unlimited
S1	AESGCM-v1	Basic iterative architecture	aes128gcmv1	Y	N/A	unlimited
	AESGCM-v2	GF Multiplier folded by a factor of 32	aes128gcmv1	Y	N/A	unlimited
S2	SHA2-v1	SHA-256 Basic iterative	sha256	N/A	N/A	unlimited
S3	SHA3-v1	SHA3-256 Folded by a factor of 8	sha3256	N/A	N/A	unlimited

Three interesting properties of each variant include the ratios of

- processing AD vs. plaintext
- decrypting ciphertext vs. encrypting plaintext
- processing equal-size AD+plaintext vs. pure plaintext.

Additionally, for candidates that support hashing, we are interested in the ratio of hashing vs. processing plaintext.

For almost all candidates, decryption can be performed with exactly the same speed as encryption. As a result, in the Results section, we focus only on the timing metrics related to encryption. The following candidates process AD significantly faster than plaintext: TinyJAMBU, ForkAE (only for v1), ESTATE, LOCUS & LOTUS, Saturnin, Oribatida, Romulus, ISAP, and Xoodyak.

The ratio of the hashing throughput to the plaintext processing throughput is the highest for Saturnin and the smallest for KNOT and Subterranean 2.0.

4.1 Implementations of current standards

For comparison with the current standards, we are including in our report results for the current NIST standard in the area of authenticated encryption with associated data,

AES-GCM, and implementations of two current hash function standards, SHA-256 (representing the SHA-2 family) and SHA3-256 (representing the SHA-3 family). All of these implementations were developed by Ekawat Homsirikamol in the period 2011-2016, when he was a Ph.D. student at George Mason University. Their features are summarized at the end of Tables 2 and Tables 3.

None of these implementations is fully compliant with the LWC Hardware API. However, both variants of AES-GCM are compliant with the very similar CAESAR Hardware API [36]. Additionally, implementations of hash functions follow a similar interface and communication protocol, limited to the PDI and DO ports and to the hashing functionality.

Table 3: Summary of basic properties of all benchmarked design variants. All throughput data are for long inputs.

No.	Variant Name	AD Block Size [bits]	Cycles per AD Block	PT-CT Block Size [bits]	Cycles per PT-CT Block	Hash Msg. Block Size [bits]	Cycles per Hash Msg Block	$\frac{\text{AD Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{PT Dec Thr}}{\text{PT Enc Thr}}$	$\frac{\text{AD+PT Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{Hash Thr}}{\text{PT Enc Thr}}$
1a	ACE_UW-v1	64	130	64	130	64	130	1.00	1.00	1.00	1.00
1b	ACE_GMU-v1	64	18	64	18	64	18	1.00	1.00	1.00	1.00
2a	Ascon_Graz-v1	64	8	64	8	64	14	1.00	1.00	1.00	0.57
	Ascon_Graz-v2	128	12	128	12	64	14	1.00	1.00	1.00	0.43
	Ascon_Graz-v3	64	5	64	5	64	8	1.00	1.00	1.00	0.63
	Ascon_Graz-v4	128	8	128	8	64	8	1.00	1.00	1.00	0.50
	Ascon_Graz-v5	64	4	64	4	64	6	1.00	1.00	1.00	0.67
	Ascon_Graz-v6	128	6	128	6	64	5	1.00	1.00	1.00	0.60
2b	Ascon_VT-v1	64	10	64	10			1.00	1.00	1.00	
	Ascon_VT-v2	64	10	64	9	64	15	0.90	1.00	0.95	0.60
2c	Ascon_GMU-v1	128	5	128	5			1.00	1.00	1.00	
	Ascon_GMU-v2	128	9	128	9			1.00	1.00	1.00	
2d	Ascon_GMU2-v1h	64	7	64	7	64	13	1.00	1.00	1.00	0.54
	Ascon_GMU2-v2h	64	4	64	4	64	7	1.00	1.00	1.00	0.57
	Ascon_GMU2-v3h	64	3	64	3	64	5	1.00	1.00	1.00	0.60
3a	COMET_CI-v1	128	60	128	70			1.17	1.00	1.08	
	COMET_CI-v2	128	264	128	297			1.13	1.00	1.06	
	COMET_CI-v3	128	56	128	66			1.18	1.00	1.08	
3b	COMET_VT-v1	128	16	128	20			1.25	1.00	1.11	
	COMET_VT-v2	128	85	128	89			1.05	1.00	1.02	
4	DryGASCON-v1	128	21	128	21	128	21	1.00	1.00	1.00	1.00
5	Elephant-v1	160	88	160	171			1.94	1.00	1.32	
	Elephant-v2	160	24	160	43			1.79	1.00	1.28	
	Elephant-v3	160	28	160	51			1.82	1.00	1.00	
	Elephant-v4	160	43	160	42			0.98	0.98	0.99	
	Elephant-v5	160	23	160	22			0.96	0.96	0.98	
6	ESTATE-v1	128	44	128	88			2.00	1.00	1.33	
	ESTATE-v2	128	226	128	452			2.00	1.00	1.33	
	ESTATE-v3	128	204	128	408			2.00	1.00	1.33	
	ESTATE-v4	128	696	128	1,392			2.00	1.00	1.33	
7	ForkAE-v1	128	1209	128	3194			2.64	1.00	1.45	
	ForkAE-v2	128	106	128	123			1.16	1.00	1.07	
8a	GIFT-COFB_VT-v1	128	49	128	47			0.96	1.00	0.98	
8b	GIFT-COFB_GMU-v1	128	41	128	41			1.00	1.00	1.00	
	GIFT-COFB_GMU-v2	128	21	128	21			1.00	1.00	1.00	
	GIFT-COFB_GMU-v3	128	11	128	11			1.00	1.00	1.00	

Table 3 continued from previous page

No.	Variant Name	AD Block Size [bits]	Cycles per AD Block	PT-CT Block Size [bits]	Cycles per PT-CT Block	Hash Msg. Block Size [bits]	Cycles per Hash Msg Block	AD Enc Thr / PT Enc Thr	PT Dec Thr / PT Enc Thr	AD+PT Enc Thr / PT Enc Thr	Hash Thr / PT Enc Thr
	GIFT-COFB_GMU-v4	128	9	128	9			1.00	1.00	1.00	
	GIFT-COFB_GMU-v5	128	6	128	6			1.00	1.00	1.00	
	GIFT-COFB_GMU-v6	128	5	128	5			1.00	1.00	1.00	
9a	Gimli_GT-v1	128	24	128	24	128	24	1.00	1.00	1.00	1.00
	Gimli_GT-v2	128	12	128	12	128	12	1.00	1.00	1.00	1.00
	Gimli_GT-v3	128	8	128	8	128	8	1.00	1.00	1.00	1.00
	Gimli_GT-v4	128	6	128	6	128	6	1.00	1.00	1.00	1.00
	Gimli_GT-v5	128	4	128	4	128	4	1.00	1.00	1.00	1.00
	Gimli_GT-v6	128	4	128	4	128	4	1.00	1.00	1.00	1.00
	Gimli_GT-v7	128	4	128	4	128	4	1.00	1.00	1.00	1.00
9b	Gimli_TUM-v1	128	786	128	789	128	786	1.00	1.00	1.00	1.00
	Gimli_TUM-v2	128	1,474	128	1,481	128	1,474	1.00	1.00	1.00	1.00
	Gimli_TUM-v3	128	2,850	128	2,865	128	2,850	1.01	1.00	1.00	1.01
9c	Gimli_GMU-v1	128	25	128	25	128	25	1.00	1.00	1.00	1.00
	Gimli_GMU-v2	128	13	128	13	128	13	1.00	1.00	1.00	1.00
	Gimli_GMU-v4	128	7	128	7	128	7	1.00	1.00	1.00	1.00
	Gimli_GMU-v5	128	5	128	5	128	5	1.00	1.00	1.00	1.00
10	ISAP-v1	144	25	144	42			1.68	1.00	1.25	
	ISAP-v2	64	16	64	26			1.63	1.00	1.24	
	ISAP-v3	144	25	144	42			1.68	1.00	1.25	
	ISAP-v4	64	14	64	22			1.57	1.00	1.22	
11	KNOT-v1×1	64	28	64	28			1.00	1.00	1.00	
	KNOT-v1×1h	64	28	64	28	32	68	1.00	1.00	1.00	0.21
	KNOT-v1×2	64	14	64	14			1.00	1.00	1.00	
	KNOT-v1×2h	64	14	64	14	32	34	1.00	1.00	1.00	0.21
	KNOT-v1×4	64	7	64	7			1.00	1.00	1.00	
	KNOT-v1×4h	64	7	64	7	32	17	1.00	1.00	1.00	0.21
	KNOT-v2×1	192	28	192	28			1.00	1.00	1.00	
	KNOT-v2×1h	192	28	192	28	128	80	1.00	1.00	1.00	0.12
	KNOT-v2×2	192	14	192	14			1.00	1.00	1.00	
	KNOT-v2×2h	192	14	192	14	128	40	1.00	1.00	1.00	0.12
	KNOT-v2×4	192	7	192	13			1.00	1.00	1.00	
	KNOT-v2×4h	192	7	192	13	128	20	1.00	1.00	1.00	0.12
	KNOT-v3	96	40	96	40			1.00	1.00	1.00	
	KNOT-v3h	96	40	96	40	48	N/A	1.00	1.00	1.00	N/A
	KNOT-v4	128	52	128	52			1.00	1.00	1.00	
	KNOT-v4h	128	52	128	52	64	140	1.00	1.00	1.00	0.19
12	LOCUS-v1	64	57	64	114			2.00	0.95	1.33	
	LOCUS-v2	64	30	64	60			2.00	0.95	1.33	
	LOTUS-v1	64	57	64	114			2.00	1.00	1.33	
	LOTUS-v2	64	30	64	60			2.00	1.00	1.33	
13	mixFeed-v1	128	53	128	57			1.08	1.00	1.04	
14	Oribatida-v1	128	69	128	137			1.99	1.00	1.33	
	Oribatida-v2	96	53	96	105			1.98	1.00	1.33	
15	PHOTON-Beetle-v1	128	28	128	33	32	25	1.18	1.00	1.08	0.33
16	Pyjamask-v1	128	258	128	262			1.02	0.96	1.01	
	Pyjamask-v2	128	98	128	102			1.04	1.00	1.02	
17	Romulus-v1	128	32	128	60			1.88	1.00	1.30	
	Romulus-v2	128	18	128	32			1.78	1.00	1.28	
	Romulus-v3	128	11	128	18			1.64	1.00	1.24	
	Romulus-v4	128	7.5	128	11			1.47	1.00	1.19	

Table 3 continued from previous page

No.	Variant Name	AD Block Size [bits]	Cycles per AD Block	PT-CT Block Size [bits]	Cycles per PT-CT Block	Hash Msg. Block Size [bits]	Cycles per Hash Msg Block	$\frac{\text{AD Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{PT Dec Thr}}{\text{PT Enc Thr}}$	$\frac{\text{AD+PT Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{Hash Thr}}{\text{PT Enc Thr}}$
	Romulus-v5	128	660	128	1304			1.98	1.00	1.33	
18	Saturnin-v1	256	197	256	394	256	305	2.00	1.00	1.33	1.29
	Saturnin-v2	256	27	256	54	256	33	2.00	1.00	1.33	1.67
19	SCHWAEMM-v2	256	38	256	47	128	34	1.24	1.00	1.11	0.69
	SCHWAEMM-v1	256	38	256	47			1.24	1.00	1.11	
20	SKINNY-AEAD-v1	128	63	128	67			1.06	1.00	1.03	
	SKINNY-AEAD-v2	128	63	128	67			1.06	1.00	1.03	
21	SPIX-v1	64	13	64	15			1.15	1.00	1.07	
	SPIX-v2	64	94	64	94			1.00	1.00	1.00	
	SPIX-v2x2	64	58	64	58			1.00	1.00	1.00	
	SPIX-v2x4	64	40	64	40			1.00	1.00	1.00	
22a	SpoC_VT-v1	64	109	64	111			1.02	1.00	1.01	
22b	SpoC_IIT-v1	128	145	128	149			1.03	1.00	1.01	
23	Spook-v2-v2	256	48	256	48			1.00	1.00	1.00	
24a	Subterranean_ST-v2	32	1	32	1	8	2	1.00	1.00	1.00	0.13
24b	Subterranean_GMU-v1	32	1	32	1			1.00	1.00	1.00	
25a	TinyJAMBU_GMU-v1	32	14	32	34			2.43	1.00	1.42	
	TinyJAMBU_GMU-v2	32	26	32	66			2.54	1.00	1.43	
	TinyJAMBU_GMU-v3	32	386	32	1,026			2.66	1.00	1.45	
25b	TinyJAMBU_TJT-v1	32	49	32	129			2.63	1.00	1.42	
	TinyJAMBU_TJT-v2	32	13	32	33			2.54	1.00	1.43	
	TinyJAMBU_TJT-v3	32	3	32	8			2.67	1.00	1.45	
26	WAGE-v1	64	114	64	114			1.00	1.00	1.00	
27a	Xoodyak_GMU-v1	352	24	192	19	128	17	1.45	1.00	1.25	0.75
	Xoodyak_GMU-v2	352	266	192	261	128	259	1.80	1.00	1.40	0.67
27b	Xoodyak_XT-v1	352	24	192	19			1.48	1.00	1.25	
	Xoodyak_XT-v2	352	18	192	13			1.32	1.00	1.19	
	Xoodyak_XT-v3	352	16	192	11			1.26	1.00	1.15	
	Xoodyak_XT-v4	352	15	192	10			1.22	1.00	1.13	
	Xoodyak_XT-v5	352	14	192	9			1.18	1.00	1.11	
	Xoodyak_XT-v6	352	13	192	8			1.13	1.00	1.08	
	Xoodyak_XT-v7	352	24	192	19	128	17	1.45	1.00	1.25	0.75
	Xoodyak_XT-v8	352	18	192	13	128	11	1.32	1.00	1.19	0.79
	Xoodyak_XT-v9	352	16	192	11	128	9	1.26	1.00	1.15	0.81
	Xoodyak_XT-v10	352	15	192	10	128	8	1.22	1.00	1.13	0.83
	Xoodyak_XT-v11	352	14	192	9	128	7	1.18	1.00	1.11	0.86
	Xoodyak_XT-v12	352	13	192	8	128	6	1.13	1.00	1.08	0.89
27c	Xoodyak_GMU2-v1	352	13	192	13	128	13	1.83	1.00	1.42	0.67
	Xoodyak_GMU2-v2	352	12	192	7	128	7	1.07	1.00	1.04	0.67
S1	AESGCM-v1	128	9	128	11			1.22	1.00	1.10	
	AESGCM-v2	128	33	128	33			1.00	1.00	1.00	
S2	SHA2-v1					512	65				
S3	SHA3-v1					1088	233				

The basic iterative architecture of AES-GCM, AESGCM-v1, does not meet the area threshold selected for LWC candidates. The second variant, AESGCM-v2, contains the Galois Field multiplier folded by a factor of 32. As a result, for Artix-7 FPGAs, the area

of this implementation is 2520 LUTs, which is similar to the area of multiple hardware submissions to the LWC FPGA benchmarking study and only 26% higher than the original threshold of 2000 LUTs. As a result, this implementation was judged sufficient for the preliminary comparison.

The basic iterative architecture of SHA-256 (from the SHA-2 family) uses only about 1050 LUTs. The basic iterative architecture of SHA3-256 (from the SHA-3 family) is by far larger. Therefore, in our study, SHA-3 is represented by an architecture folded by a factor of 8. Its area is only about 1250 LUTs. In its current form, this architecture does not support padding. However, adding padding is not likely to affect significantly either throughput or area of this design.

Multiple LWC candidates support resource sharing between authenticated encryption and hashing. For the current standards, this sharing is limited to preprocessing and postprocessing only. As a result, a fair comparison is somewhat challenging, especially for hashing. All implementations of LWC candidates supporting hashing, combine both functionalities in a single unit. Thus, in terms of area, it might be fairer to compare them to the joint implementation of AES-GCM and a hash function standard (SHA-2 or SHA-3). Additionally, in terms of speed, preserving the same maximum clock frequency after combining two units may be challenging to achieve. Either two different clock domains would have to be used, or the circuit would have the maximum clock frequency equal to the minimum of the frequencies of component units (AEAD and Hash).

Additionally, better compact implementations of AES-GCM, SHA-2, and SHA-3 may already exist or be developed in the future. As a result, all comparisons with the current standards presented in Section 5 should be treated as preliminary.

4.2 Unique Features

Most of the designs assume the following standard order of segments provided at the Public Data Input (PDI) ports during encryption: Public Message Number (Npub), Associated Data (AD), Plaintext (PT). For decryption, the corresponding order is: Public Message Number (Npub), Associated Data (AD), Ciphertext (PT), and Tag. For ESTATE, the order for decryption is changed to Npub, AD, Tag, Ciphertext. For ISAP, the order for encryption is: Npub, Plaintext, AD; the order for decryption is: Npub, AD, Ciphertext, Tag. For Romulus, the order for encryption is: AD, Npub, Plaintext; the order for decryption is: AD, Npub, Ciphertext, Tag.

Gimli_GT and Subterranean_ST are the only designs that use an unconventional maximum segment size of 2^{15}, instead of the recommended $2^{16} - 1$. This feature does not considerably affect the compatibility with other API-compliant implementations, as segments of the size between $2^{15} + 1$ and $2^{16} - 1$ can be easily divided into two segments supported by the submitted design using a simple preprocessor.

5 Throughput and Area Analysis

All variants of all hardware design packages passed all GMU known-answer tests (KATs) and produced reliable timing measurements.

5.1 Results of Synthesis and Implementation

Initial versions of several designs were shown to be not fully synthesizable by at least one of the three FPGA toolsets used in this study. However, the underlying problems were located and addressed by the hardware designers within the benchmarking period.

The details of resource utilization and maximum clock frequency after placing and routing are provided for all evaluated designs in the Appendix, in Tables 22, 23, and 24.

In Table 23, the ratios between the numbers of Cyclone 10 LP LEs vs. Artix-7 LUTs are provided. The average ratio is 1.88. However, the actual ratios vary in a relatively wide range, between 1.19 for Gimli_GT-v7 and 4.76 for Xoodyak_GMU-v2. Additionally, the following designs have significantly larger area in LEs for Cyclone 10 LP FPGAs as compared to the area in LUTs for Artix-7: Xoodyak_GMU-v2, Pyjamask-v1, SHA3-v1, AESGCM-v2, COMET_VT-v1, mixFeed-v1, Pyjamask-v2, and COMET_VT-v2. The average ratios of the numbers of FFs and clock frequencies, in Cyclone 10 LP vs. Artix-7, are 1.69 and 1.72, respectively.

In Table 24, the ratios between the numbers of LUTs, flip-flops (FFs), and maximum clock frequencies in ECP5 vs. Artix-7 are summarized. The average ratio is 1.77 for LUTs, 1.06 for FFs, and 2.59 for frequencies. However, the actual ratios vary in a relatively wide range. For example, the ratio of LUTs varies between 1.15 for Oribatida-v1 and 2.65 for ISAP-v2. In particular, the following designs have significantly larger areas in LUTs for ECP5 as compared to Artix-7: ISAP-v2, ISAP-v3, mixFeed, TinyJAMBU_GMU-v3, and Romulus-v5.

5.2 Throughputs for Long Inputs

5.2.1 Results for Xilinx Artix-7

The two-dimensional graphs Throughput vs. Number of Used LUTs are shown in Figs. 2, 3, and 4. The throughputs concern the cases of Plaintext (PT) only, Associated Data (AD) only, and equal-size AD+PT, respectively. All three mentioned above graphs concern results for the Xilinx Artix-7 FPGA xc7a12tcsg325-3. The results apply to long inputs. We use the logarithmic scale on both axes. Dashed lines represent the same throughput over area ratio. In the legends of these figures, the algorithms are listed in the order of decreasing throughput. While the order of the symbols remains the same, the mapping of the symbol to the algorithm changes.

In these graphs, each candidate is represented by only one variant, selected according to the following rules. If a candidate has one or more variants with the area below 2520 LUTs (the area of the smallest implementation of AES-GCM available to us), the fastest variant meeting this criterion is selected. If a candidate does not have a variant with the area below 2520 LUTs, a variant with the smallest area is selected.

The threshold of 2520 LUTs (26% more than the intended target of 2000 LUTs) was selected because many designers tried to aggressively use close to 2000 LUTs to achieve the highest possible speed. As a result, many of them ended up with designs taking between 2000 and 2520 LUTs. Additionally, the exact number of LUTs may depend on the exact options of tools, providing different trade-offs between the area and speed. Thus, relaxing the upper limit of 2000 LUTs seems to be fully warranted, at least at this stage of the analysis, when the full space exploration remains still incomplete for the majority of candidates.

The winner for the PT only is Subterranean 2.0. Its implementation reaches the throughput of about 8.6 Gbit/s and is the second smallest in terms of the number of LUTs. The next five in terms of throughput include Ascon (6.3 Gbit/s), Xoodyak (5.5 Gbit/s), Gimli (4.4 Gbit/s), KNOT (3.2 Gbit/s), and GIFT-COFB (3.0 Gbit/s). Areas of these implementations vary between 1730 LUTs for GIFT-COFB to 2410 LUTs for Ascon. Thus, they are between 2 and 3 times larger than the area of Subterranean 2.0. The next group includes four algorithms with throughputs between 1 and 2 Gbits/s: DryGASCON, COMET, Spook-v2, and Elephant. Their areas are in the range between 1901 for Elephant to 2449 LUTs for COMET. The next algorithm in the ranking is TinyJAMBU, which reaches a speed very close to 1 Gbit/s and at the same time has by far the smallest area, around 600 LUTs. The last candidate faster and smaller than AES-GCM is Romulus, with the throughput around 875 Mbits/s. Saturnin approaches the speed of AES-GCM and, at

the same time, uses about 200 less LUTs. The design of SCHWAEMM is by far the largest, above 3000 LUTs, yet still only average (rank 15) in terms of throughput. More effort is required to demonstrate the competitiveness of this algorithm with the first 13 candidates mentioned above. All remaining algorithms have throughputs below 700 Mbits/s. Out of them, ForkAE, SKINNY-AEAD, Pyjamask, ISAP, and PHOTON-Beetle have areas exceeding 2000 LUTs.

The designs for Spoc and WAGE are in the vicinity of 1000 LUTs and clearly were not optimized for the maximum throughput assuming the resource utilization of 2000 LUTs or less. To a lower extent, the designs for mixFeed, ESTATE and Oribatida, all slightly below 1500 LUTs, are also too small to be fairly compared with others. As a result, it might be too premature to assign any negative evaluation to these candidates.

For AD only, the following changes are the most significant. Subterranean 2.0 and Xoodyak both reach the speeds beyond 8 Gbit/s. These two algorithms are followed by Ascon (6.3 Gbit/s), Gimli (4.4 Gbit/s), KNOT (3.8 Gbit/s), and GIFT-COFB (3.0 Gbit/s). TinyJAMBU moves from position 11 for processing plaintext only to position 7 for AD only. The algorithms with throughputs in the range between 1 and 1.7 Gbit/s include COMET, Saturnin, Romulus, DryGASCON, Elephant, Spook-v2, and ISAP. Among the first dozen algorithms in the ranking, there is only one change, Spook-v2 is replaced by Saturnin. Fourteen algorithms have throughputs for AD greater than 1 Gbit/s.

Only 10 out of 27 investigated candidates support hashing. The two-dimensional graph, Throughput vs. Area for hashing long messages on Artix-7 FPGA is shown in Fig. 5.

The two fastest designs are Gimli and Xoodyak, with throughputs approximately equal to 4.4 and 3.6 Gbits/s, respectively. These are also the only only algorithms with the throughputs greater than SHA-2. Very close behind SHA-2 are DryGASCON and Saturnin, with the throughputs between 1.4 and 1.6 Gbits/s. They are followed by Ascon at about 1 Gbit/s and Subterranean at around 760 Mbits/s. The remaining algorithms, ACE, SCHWAEMM (ESCH), KNOT, and PHOTON-Beetle have throughputs below 510 Mbits/s and areas between 1600 and 2500 LUTs. Subterranean and all candidates from the last group listed above have throughputs lower than the folded implementation of SHA-3.

The corresponding detailed numerical results can be found in Tables 25, 26, 27, 28.

Only one variant per each LWC candidate is ranked. If a given LWC candidate has designs with the area below the threshold of 2520 LUTs, the best of these designs is used to represent a given candidate in rankings. If, for a given LWC candidate, all its variants exceed the area threshold, the smallest of these designs is included in the ranking.

5.2.2 Results for Intel Cyclone 10 LP and Lattice Semiconductor ECP5

The equivalent graphs for Intel Cyclone 10 LP are shown in Figs. 6, 7, 8, and 9. The corresponding tables are listed as Tables 29, 30, 31, and 32.

The area threshold used for the selection of the best designs has been set to 5000 LEs. This value was selected based on the fact that the average ratio of the number of Cyclone 10 LP LEs to the number of Artix-7 LUTs, calculated over all available designs, was close to 2.0.

The conclusions from these tables and graphs are very close to the conclusions based on the results for the Artix-7 FPGA. Pyjamask and mixFeed are the only candidates with no variant fitting within 5000 LEs. In the case of Artix-7 FPGAs, the only candidate exceeding the corresponding area threshold was SCHWAEMM.

For PT only, Subterranean is almost two times faster than the second candidate in the ranking, Ascon. Ascon, Gimli, and Xoodyak are the only algorithms with speeds between 2.5 and 3 Gbit/s. Out of them, Ascon has by far the largest area, approaching 5000 LEs. For AD only, the speed of Xoodyak is only about 20% lower than the speed of Subterranean 2.0. These two algorithms are followed by Ascon, Gimli, and KNOT, with throughputs between 2.8 and 3.0 Gbit/s. The next two are TinyJAMBU and GIFT-COFB,

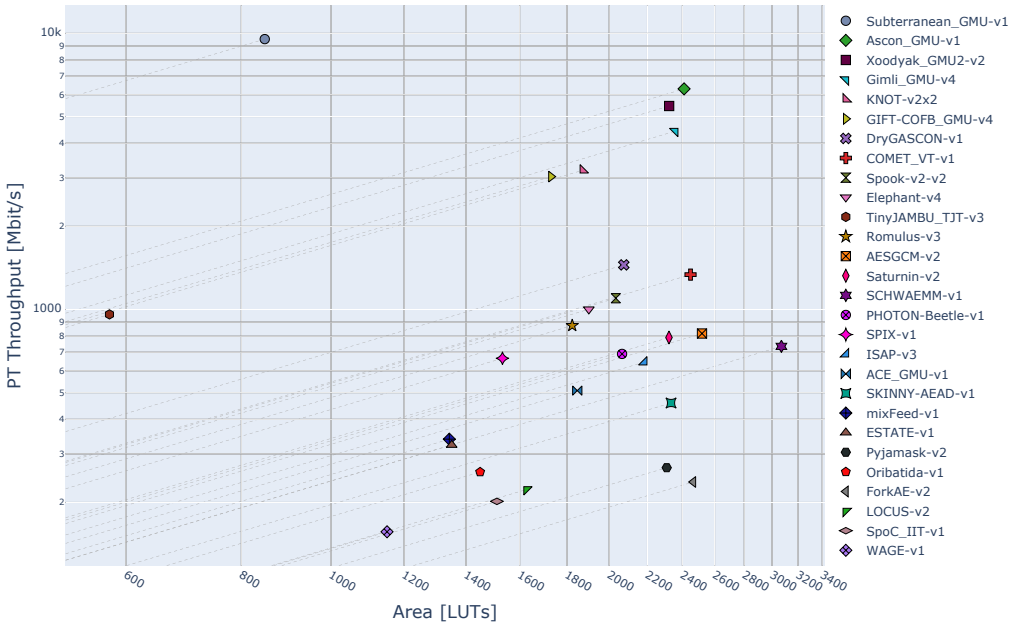

Figure 2: Artix-7 Encryption PT Throughput for Long Messages vs LUTs

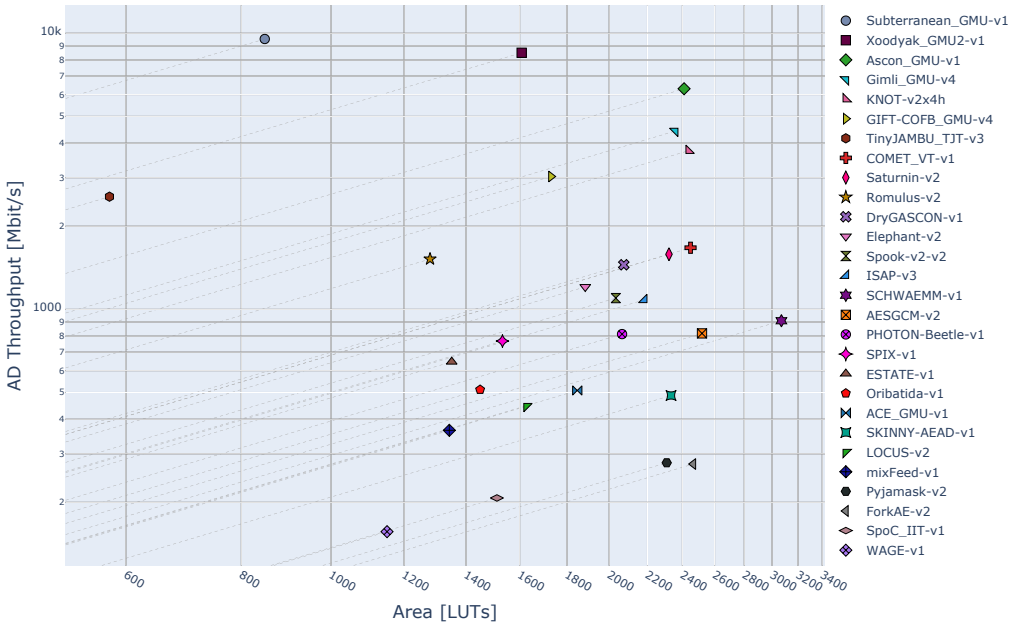

Figure 3: Artix-7 Encryption AD Throughput for Long Messages vs LUTs

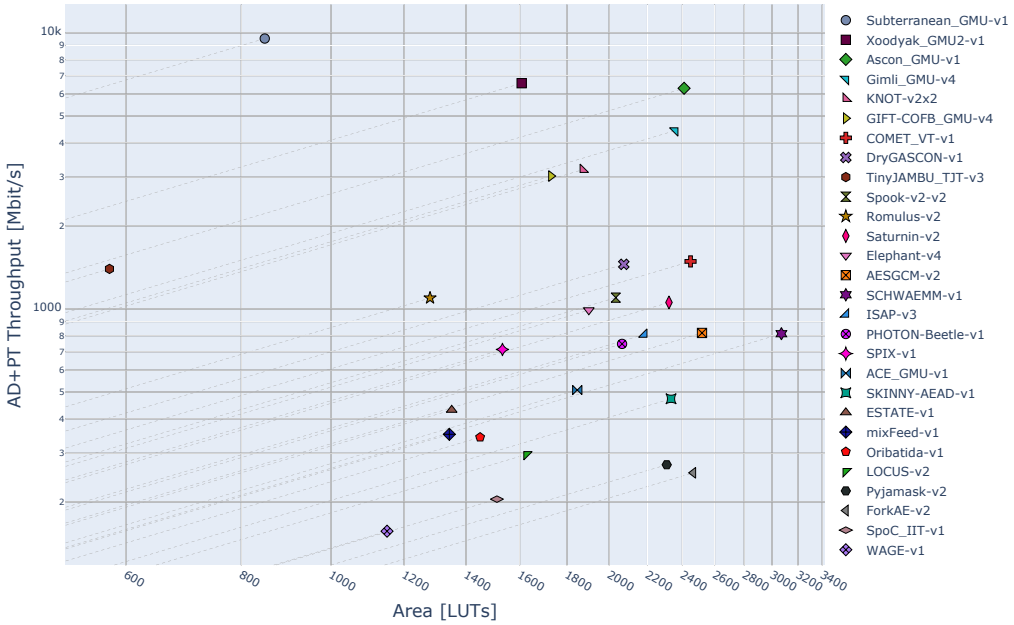

Figure 4: Artix-7 Encryption AD+PT Throughput for Long Messages vs LUTs

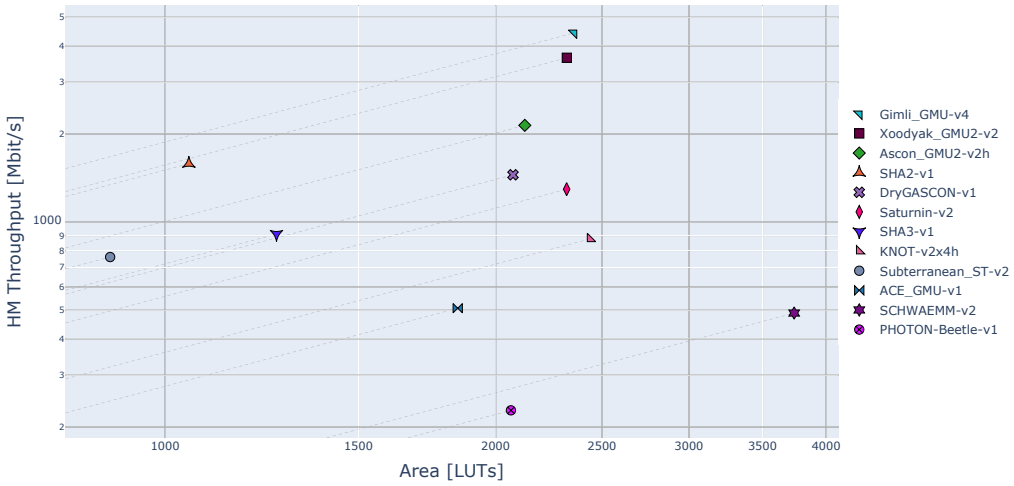

Figure 5: Artix-7 Hashing Throughput for Long Messages vs LUTs

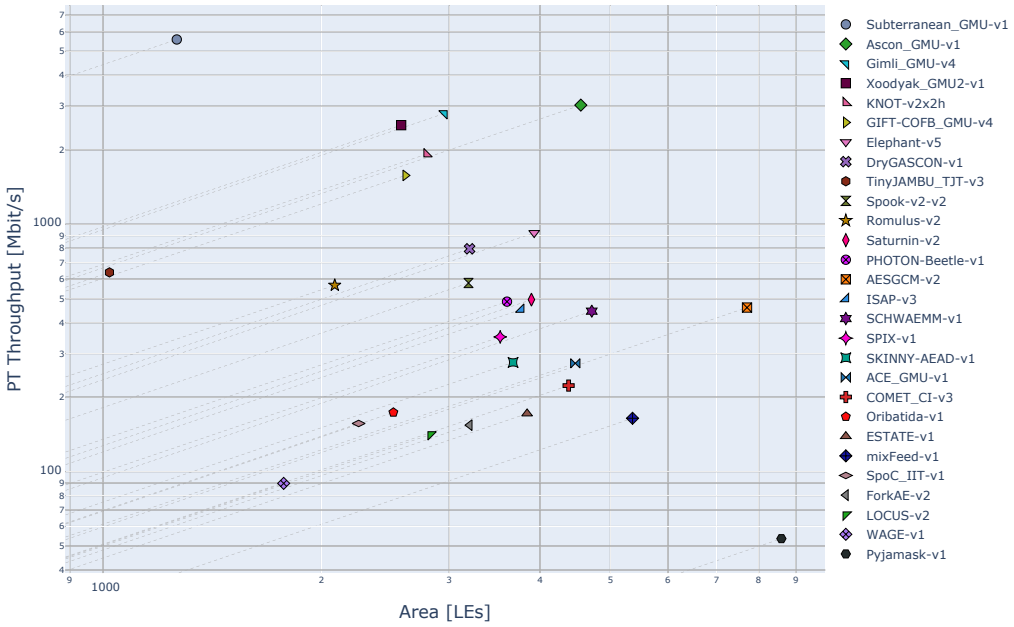

Figure 6: Cyclone 10 LP Encryption PT Throughput for Long Messages vs LEs

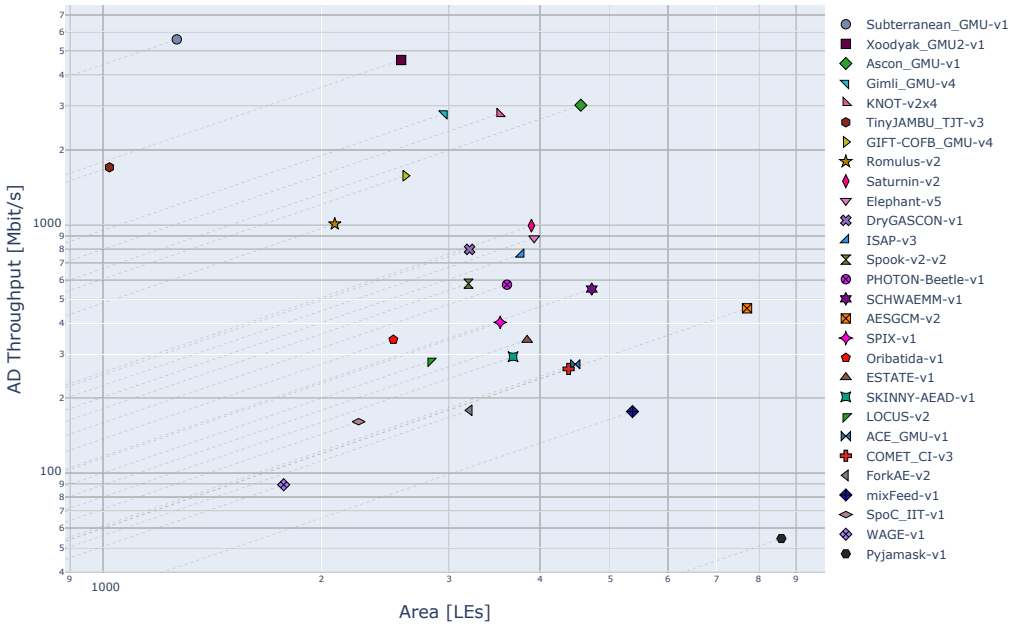

Figure 7: Cyclone 10 LP Encryption AD Throughput for Long Messages vs LEs

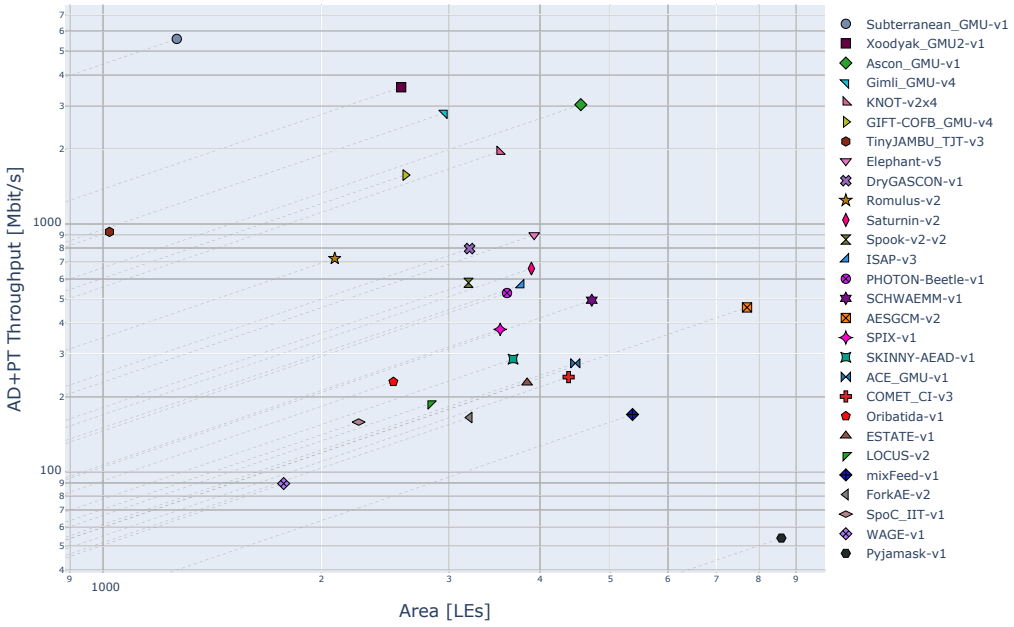

Figure 8: Cyclone 10 LP Encryption AD+PT Throughput for Long Messages vs LEs

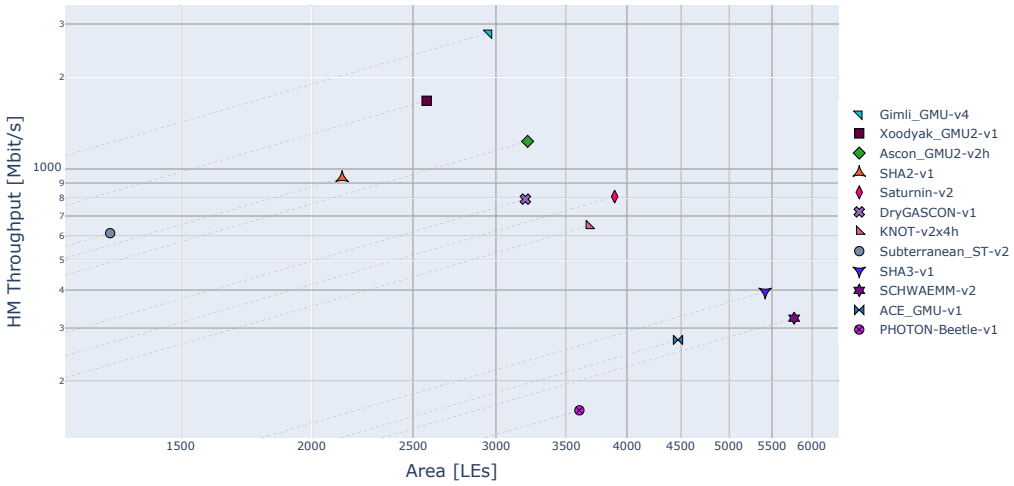

Figure 9: Cyclone 10 LP Hashing Throughput for Long Messages vs LEs

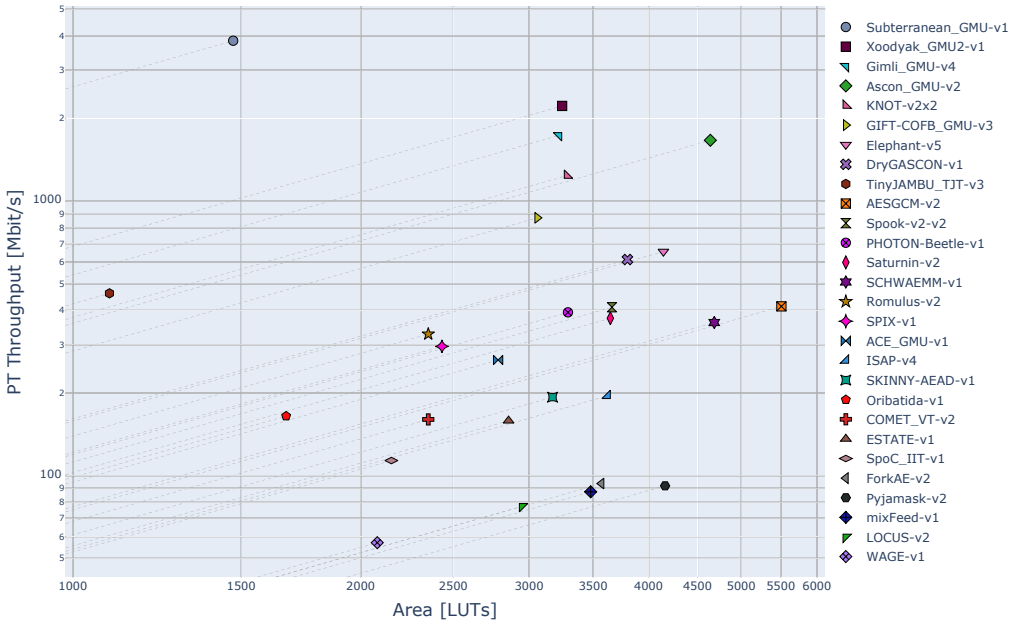

Figure 10: ECP5 Encryption PT Throughput for Long Messages vs LUTs

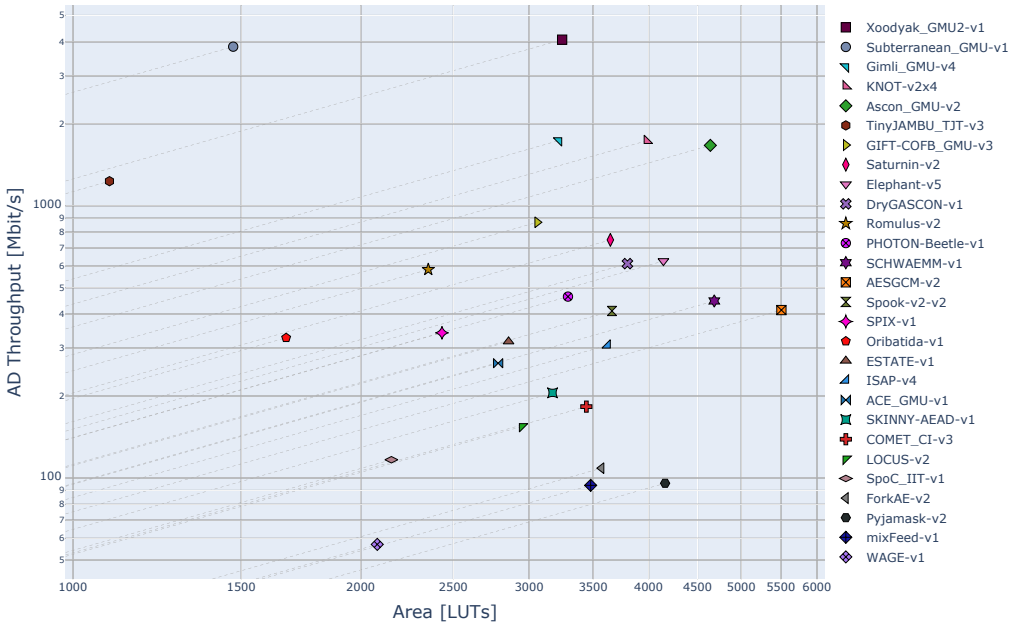

Figure 11: ECP5 Encryption AD Throughput for Long Messages vs LUTs

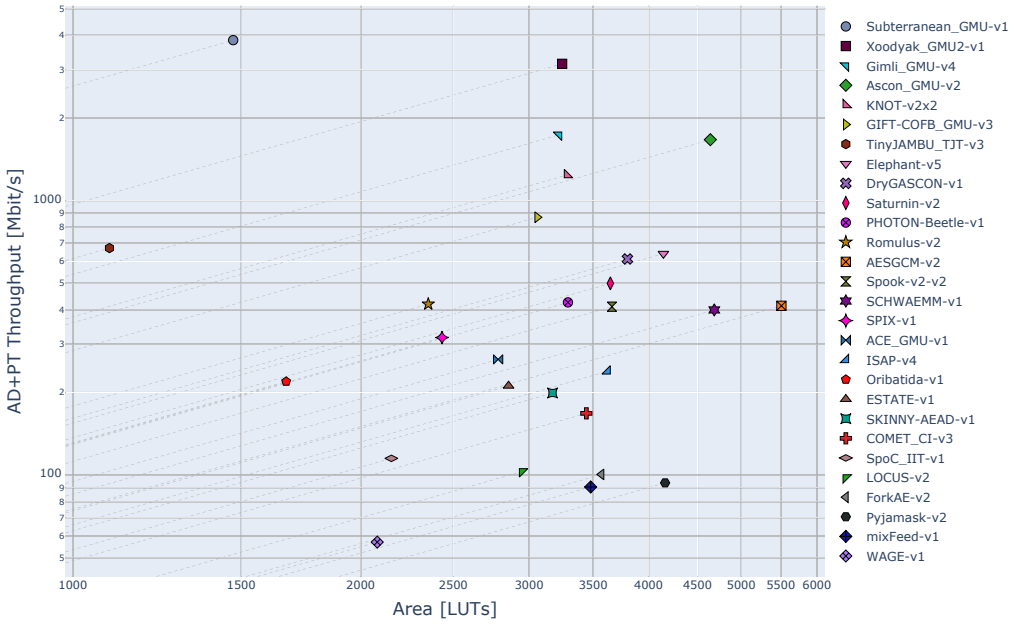

Figure 12: ECP5 Encryption AD+PT Throughput for Long Messages vs LUTs

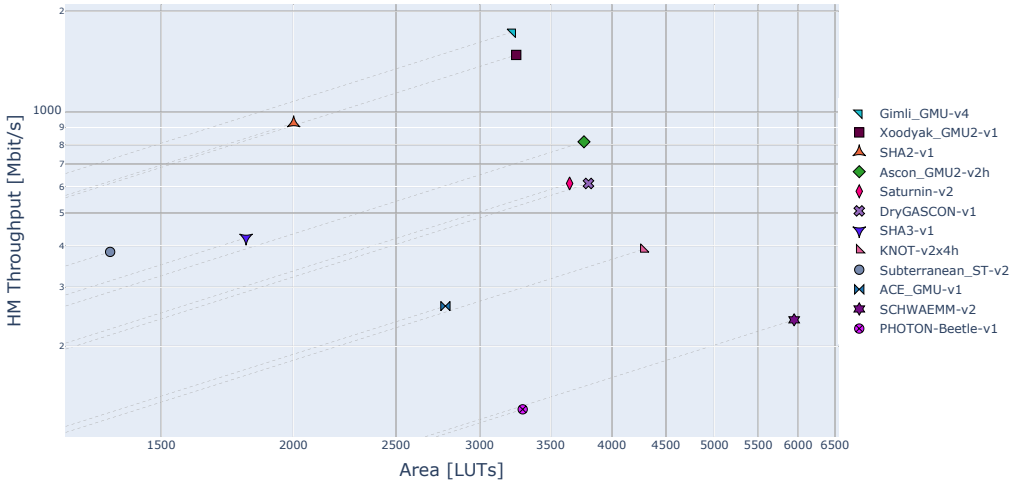

Figure 13: ECP5 Hashing Throughput for Long Messages vs LUTs

with throughputs in the range of 1.6-1.7 Gbit/s. Out of the mentioned above 7 algorithms, TinyJAMBU and Subterranean 2.0 have the smallest and Ascon the largest area. Romulus and Saturnin are next in the ranking, with throughputs around 1 Gbit/s. For hashing, compared to Artix-7, Ascon becomes inferior to SHA-2. Additionally, DryGASCON and Saturnin swap places at positions 5 and 6.

The two-dimensional graphs for Lattice Semiconductor ECP5 are shown in Figs. 10, 11, 12, and 13. The corresponding tables are listed as Tables 33, 34, 35, and 36.

The area threshold used for the selection of the best designs has been set to 5000 LUTs. This value was selected based on the fact that the average ratio of the number of ECP5 LUTs to the number of Artix-7 LUTs, calculated over all available designs, was close to 2.0. All investigated algorithms, except AES-GCM, have a variant with area falling below this threshold. The conclusions from these tables and graphs are relatively close to the conclusions based on the results for the Artix-7 FPGA.

Table 4: FPGA Rankings based on Encryption PT Throughput for Long Messages

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Ascon_GMU-v1	Ascon_GMU-v1	Xoodyak_GMU2-v1
3	Xoodyak_GMU2-v2	Gimli_GMU-v4	Gimli_GMU-v4
4	Gimli_GMU-v4	Xoodyak_GMU2-v1	Ascon_GMU-v2
5	KNOT-v2x2	KNOT-v2x2h	KNOT-v2x2
6	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v3
7	DryGASCON-v1	Elephant-v5	Elephant-v5
8	COMET_VT-v1	DryGASCON-v1	DryGASCON-v1
9	Spook-v2-v2	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
10	Elephant-v4	Spook-v2-v2	AESGCM-v2
11	TinyJAMBU_TJT-v3	Romulus-v2	Spook-v2-v2
12	Romulus-v3	Saturnin-v2	PHOTON-Beetle-v1
13	AESGCM-v2	PHOTON-Beetle-v1	Saturnin-v2
14	Saturnin-v2	AESGCM-v2	SCHWAEMM-v1
15	SCHWAEMM-v1	ISAP-v3	Romulus-v2
16	PHOTON-Beetle-v1	SCHWAEMM-v1	SPIX-v1
17	SPIX-v1	SPIX-v1	ACE_GMU-v1
18	ISAP-v3	SKINNY-AEAD-v1	ISAP-v4
19	ACE_GMU-v1	ACE_GMU-v1	SKINNY-AEAD-v1
20	SKINNY-AEAD-v1	COMET_CI-v3	Oribatida-v1
21	mixFeed-v1	Oribatida-v1	COMET_VT-v2
22	ESTATE-v1	ESTATE-v1	ESTATE-v1
23	Pyjamask-v2	mixFeed-v1	SpoC_IIT-v1
24	Oribatida-v1	SpoC_IIT-v1	ForkAE-v2
25	ForkAE-v2	ForkAE-v2	Pyjamask-v2
26	LOCUS-v2	LOCUS-v2	mixFeed-v1
27	SpoC_IIT-v1	WAGE-v1	LOCUS-v2
28	WAGE-v1	Pyjamask-v1	WAGE-v1

The ranking of candidates depending on the FPGA family used is summarized in Tables 4, 5, 6, and 7, for PT only, AD only, AD+PT, and Hash message respectively. For the processing of PT, the top candidate, Subterranean 2.0 is the same for all families. The ranking at positions 2–4 depends on an FPGA family, but always includes Ascon, Gimli, and Xoodyak. The positions of Ascon and Xoodyak (2nd and 4th for Cyclone 10 LP) are swapped when moving from Cyclone 10 LP to ECP5. KNOT and GIFT-COFB are consistently at positions 5 and 6 for all candidates. The list of algorithms at positions from 7 to 12 vary but includes consistently DryGASCON, Elephant, Spook-v2, and TinyJAMBU. Romulus is outside of the first 12 only for ECP5, where its position drops to 15th. The difference in Throughputs between variants v2 and v3 of this algorithm are minimal for all three families. The mentioned above 11 candidates have performance better than AES-GCM for all three FPGA families. The position of COMET drops down significantly for Cyclone 10 LP and ECP5, because the fastest variant of this algorithm,

Table 5: FPGA Rankings based on Encryption AD Throughput for Long Messages

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Xoodyak_GMU2-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Subterranean_GMU-v1
3	Ascon_GMU-v1	Ascon_GMU-v1	Gimli_GMU-v4
4	Gimli_GMU-v4	Gimli_GMU-v4	KNOT-v2x4
5	KNOT-v2x4h	KNOT-v2x4	Ascon_GMU-v2
6	GIFT-COFB_GMU-v4	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
7	TinyJAMBU_TJT-v3	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v3
8	COMET_VT-v1	Romulus-v2	Saturnin-v2
9	Saturnin-v2	Saturnin-v2	Elephant-v5
10	Romulus-v2	Elephant-v5	DryGASCON-v1
11	DryGASCON-v1	DryGASCON-v1	Romulus-v2
12	Elephant-v2	ISAP-v3	PHOTON-Beetle-v1
13	Spook-v2-v2	Spook-v2-v2	SCHWAEMM-v1
14	ISAP-v3	PHOTON-Beetle-v1	AESGCM-v2
15	SCHWAEMM-v1	SCHWAEMM-v1	Spook-v2-v2
16	AESGCM-v2	AESGCM-v2	SPIX-v1
17	PHOTON-Beetle-v1	SPIX-v1	Oribatida-v1
18	SPIX-v1	Oribatida-v1	ESTATE-v1
19	ESTATE-v1	ESTATE-v1	ISAP-v4
20	Oribatida-v1	SKINNY-AEAD-v1	ACE_GMU-v1
21	ACE_GMU-v1	LOCUS-v2	SKINNY-AEAD-v1
22	SKINNY-AEAD-v1	ACE_GMU-v1	COMET_CI-v3
23	LOCUS-v2	COMET_CI-v3	LOCUS-v2
24	mixFeed-v1	ForkAE-v2	SpoC_IIT-v1
25	Pyjamask-v2	mixFeed-v1	ForkAE-v2
26	ForkAE-v2	SpoC_IIT-v1	Pyjamask-v2
27	SpoC_IIT-v1	WAGE-v1	mixFeed-v1
28	WAGE-v1	Pyjamask-v1	WAGE-v1

Table 6: FPGA Rankings based on Encryption AD+PT Throughput for Long Messages

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
3	Ascon_GMU-v1	Ascon_GMU-v1	Gimli_GMU-v4
4	Gimli_GMU-v4	Gimli_GMU-v4	Ascon_GMU-v2
5	KNOT-v2x2	KNOT-v2x4	KNOT-v2x2
6	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v3
7	COMET_VT-v1	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
8	DryGASCON-v1	Elephant-v5	Elephant-v5
9	TinyJAMBU_TJT-v3	DryGASCON-v1	DryGASCON-v1
10	Spook-v2-v2	Romulus-v2	Saturnin-v2
11	Romulus-v2	Saturnin-v2	PHOTON-Beetle-v1
12	Saturnin-v2	Spook-v2-v2	Romulus-v2
13	Elephant-v4	ISAP-v3	AESGCM-v2
14	AESGCM-v2	PHOTON-Beetle-v1	Spook-v2-v2
15	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1
16	ISAP-v3	AESGCM-v2	SPIX-v1
17	PHOTON-Beetle-v1	SPIX-v1	ACE_GMU-v1
18	SPIX-v1	SKINNY-AEAD-v1	ISAP-v4
19	ACE_GMU-v1	ACE_GMU-v1	Oribatida-v1
20	SKINNY-AEAD-v1	COMET_CI-v3	ESTATE-v1
21	ESTATE-v1	Oribatida-v1	SKINNY-AEAD-v1
22	mixFeed-v1	ESTATE-v1	COMET_CI-v3
23	Oribatida-v1	LOCUS-v2	SpoC_IIT-v1
24	LOCUS-v2	mixFeed-v1	LOCUS-v2
25	Pyjamask-v2	ForkAE-v2	ForkAE-v2
26	ForkAE-v2	SpoC_IIT-v1	Pyjamask-v2
27	SpoC_IIT-v1	WAGE-v1	mixFeed-v1
28	WAGE-v1	Pyjamask-v1	WAGE-v1

Table 7: FPGA Rankings based on Hash Throughput for Long Messages

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4
2	Xoodyak_GMU2-v2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
3	Ascon_GMU2-v2h	Ascon_GMU2-v2h	SHA2-v1
4	SHA2-v1	SHA2-v1	Ascon_GMU2-v2h
5	DryGASCON-v1	Saturnin-v2	Saturnin-v2
6	Saturnin-v2	DryGASCON-v1	DryGASCON-v1
7	SHA3-v1	KNOT-v2x4h	SHA3-v1
8	KNOT-v2x4h	Subterranean_ST-v2	KNOT-v2x4h
9	Subterranean_ST-v2	SHA3-v1	Subterranean_ST-v2
10	ACE_GMU-v1	SCHWAEMM-v2	ACE_GMU-v1
11	SCHWAEMM-v2	ACE_GMU-v1	SCHWAEMM-v2
12	PHOTON-Beetle-v1	PHOTON-Beetle-v1	PHOTON-Beetle-v1

COMET_VT-v1, exceeds the limit of area for both of these families. For Cyclone 10 LP, this limit is also exceeded by COMET_VT-v2.

For the processing of AD, Xoodyak outperforms Subterranean 2.0 for ECP5. The opposite is true for the remaining two families. Algorithms at positions 3–5 now include Ascon, Gimli, and KNOT, with Ascon earning the 3rd position for Artix-7 and Cyclone 10 LP, while Gimli claiming the same spot for ECP5. At positions 6 and 7, GIFT-COFB swaps places with TinyJAMBU, depending on the FPGA family. The list of algorithms at positions from 8 to 12 vary but includes consistently DryGASCON, Elephant, Romulus, and Saturnin. SCHWAEMM is the only other algorithm with Throughput higher than AES-GCM for all FPGA families, but it exceeds the area of AES-GCM in case of Artix-7. COMET falls beyond the first 12 for the same reasons as in the case of processing PT.

For the processing of Hash messages, the ranking of candidates does not change for the majority of algorithms. The only swaps appear between DryGASCON and Saturnin, at positions 4 and 5 (not counting SHA-2), and between ACE and KNOT, at positions 7 and 9 (not counting either SHA-2 or SHA-3). Three candidates - Gimli, Xoodyak, and Ascon - have their throughput higher than SHA-2 for Artix-7 and Cyclone 10 LP, but only the first two for ECP5. Similarly, Subterranean 2.0 outperforms a folded implementation of SHA-3 for Cyclone 10 LP, but not for Artix-7 or ECP5.

5.2.3 Initial Design Space Explorations

Initial design space explorations, involving at least four variants, were conducted for the following six candidates: Ascon, COMET, ESTATE, Gimli, KNOT, Romulus, TinyJAMBU, and Xoodyak. In the following two-dimensional graphs, apart from points representing variants of an investigated algorithm, we include also points corresponding to the implementations with the highest Throughput (Subterranean v2.0), smallest area (TinyJAMBU), and largest area (SCHWAEMM).

In Figs. 14 and 15, the Artix-7 results are presented for multiple designs of Ascon. Two variants of Ascon_GMU outperform other variants in terms of throughput. Ascon_GMU-v1 is a 2× unrolled variant of Ascon-128a, Ascon_GMU-v2 is the basic iterative architecture of the same algorithm. The comparison between Ascon_VT-v1 and Ascon_VT-v2, demonstrates that, in Ascon, adding hashing functionality comes with no penalty in terms of area or throughput. The best designs from GMU outperform those from TU Graz, and those in turn outperform designs from Virginia Tech.

In Figs. 16 and 17, the Artix-7 results are presented for five designs of COMET. COMET_VT-v1, COMET_CI-v1, COMET_CI-v2, and COMET_CI-v3 are realizations of the primary parameter set: COMET-128_AES-128/128. COMET_VT-v2 is the realization of the parameter set COMET-128_CHAM-128/128. The difference in performance between the first four mentioned above variants comes from using differ-

ent hardware architectures. COMET_VT-v1 uses the basic iterative architecture, while COMET_CI-v1, COMET_CI-v2, and COMET_CI-v3 use folded architectures with different folding factors. For the same basic iterative architecture, the implementation of COMET-128_AES-128/128 (COMET_VT-v1) is both faster and bigger than the implementation of COMET-128_CHAM-128/128 (COMET_VT-v2). As shown in Table 3, the number of clock cycles per block is significantly higher for COMET-128_CHAM-128/128. At the same time, implementing one round of CHAM-128/128 takes significantly less area than implementing one round of AES-128/128. COMET_CI-v3 is a minor improvement over COMET_CI-v1. COMET_CI-v2 is over 4 times slower and about 42% smaller.

In Figs. 18 and 19, the Artix-7 results are presented for four designs of ESTATE. ESTATE-v1 and ESTATE-v2 are implementations of the parameter set ESTATE_TweAES-128, obtained by instantiating the ESTATE mode of operation with the TweAES-128 block cipher. ESTATE-v3 and ESTATE-v4 are implementations of the parameter set ESTATE_TweGIFT-128, obtained by instantiating the ESTATE mode of operation with the TweGIFT-128 block cipher. Within each pair, the former implementation uses a 32-bit datapath and the latter an 8-bit datapath. For the implementations using the same datapath width, the realizations of ESTATE_TweAES-128 (ESTATE-v1 and ESTATE-v2) are significantly faster. At the same time, both 8-bit architectures (ESTATE-v2 and ESTATE-v4) have areas smaller than 1000 LUTs.

In Figs. 22, 23, and 24, the Artix-7 results are presented for ten designs of Gimli. Seven designs from the Gimli Team and four designs from GMU are optimized for maximum throughput. Three designs from the Technical University of Munich (TUM) are optimized for the minimum area. Gimli_GT-v1 and Gimli_GMU-v1 are basic iterative architectures of Gimli, with one round executed per one clock cycle. The designs from Gimli_GT-v2 to Gimli_GT-v7 are unrolled architectures, with a different number of rounds executed per clock cycle. The unrolling factor is 2 for Gimli_GT-v2, 3 for Gimli_GT-v3, 4 for Gimli_GT-v4, 6 for Gimli_GT-v5, and 8 for Gimli_GT-v6, and 12 for Gimli_GT-v7. Only Gimli_GT-v1, Gimli_GT-v2, and Gimli_GT-v4 have areas smaller than the area of AES-GCM (2520 LUTs). Out of these three, Gimli_GT-v4 is by far the fastest. The number of clock cycles per block in Gimli_GT-v6 and Gimli_GT-v7 is limited by the LWC interface, capable of reading one 128-bit block in no less than 4 clock cycles. As a result, the speed of designs with 6 and 8 rounds unrolled is approximately the same. The throughput of Gimli_GT-v7, with 12 rounds unrolled, is lower because of the decrease in the maximum clock frequency. Somewhat surprisingly, Gimli_GT-v4, with 4 rounds unrolled, is both smaller and faster than Gimli_GT-v3, with 3 rounds unrolled. Similarly, the designs Gimli_GMU-v2 and Gimli_GMU-v4 are unrolled architectures, with unrolling factors of 2 and 4, respectively. These designs clearly outperform the corresponding designs from the Gimli Team for the same types of architectures in terms of both throughput and area. The designs from the Technical University of Munich (TUM) have a substantially higher number of clock cycles per round (786, 1474, and 2850 vs. 24 for Gimli_GT-v1). At the same time, they all reach the area below 1000 LUTs, which may be important in some applications. For hashing, Gimli_GMU-v4 is the fastest design with an area smaller than the area of AES-GCM, at about 4.4 Gbit/s, followed by Gimli_GT-v4 at about 3.0 Gbit/s.

In Figs. 25 and 26, the Artix-7 results are presented for six variants of KNOT, representing 6 different architectures, implementing the parameter set KNOT-AEAD(128, 384, 192). The parameter sets of KNOT are denoted as KNOT-AEAD(k, b, r), where k is the key length, b is the state size, and r is the bitrate. The bitrate determines the block size of plaintext and AD. The parameter set KNOT-AEAD(128, 384, 192) has a substantial advantage in terms of throughput over the parameter sets KNOT-AEAD(128, 256, 64), KNOT-AEAD(192, 384, 96), and KNOT-AEAD(256, 512, 128), with 10 variants summarized in Table 2. For processing PT, KNOT-v2x2 is the fastest, and its area does

not exceed 2000 LUTs. Adding hashing to this architecture increases its area by about 13%. For processing AD, KNOT-v2x4h is the fastest among architectures not exceeding 2500 LUTs. The FPGA options have been selected to optimize throughput/area, rather than throughput itself. Only this way, this architecture could be implemented using less than 2500 LUTs. The choice of tool options for KNOT-v2x4 has led to a larger design despite not supporting hashing functionality. The smaller area could be accomplished only at the cost of a significant decrease in the circuit throughput and some decrease in the throughput/area ratio. Basic iterative architectures KNOT-v2x1 and KNOT-v2x1h are the smallest but also the slowest.

In Figs. 27 and 28, the Artix-7 results are presented for five designs of Romulus. All variants are implementations of the same primary parameter set Romulus-N1, with the plaintext and AD block sizes of 128-bits. The implemented variants differ only in hardware architecture. These hardware architectures are called by authors: the round-based architecture (Romulus-v1), two-round architecture (Romulus-v2), four-round architecture (Romulus-v3), eight-round architecture (Romulus-v4), and low-area architecture (Romulus-v4). With the increase in the number of rounds unrolled, the number of clock cycles per block decreases, but at the same time, the clock frequency decreases. For Artix-7, Romulus-v2 with the two-round architecture is optimal from the point of view of throughput. Romulus-v3 and Romulus-v4 are both bigger and slower. Romulus-v1 has a somewhat comparable speed and area smaller than 1000 LUTs. As a result, its throughput/area ratio is the second largest. Romulus-v5 is only about 70 LUTs smaller than Romulus-v1 and over 20 times slower. As shown in Tables 29, 30, 31, and 32, 33, 34, 35 for Cyclone 10 LP FPGAs, Romulus-v2 is the also fastest, but for ECP5 FPGAs, it is outperformed by Romulus-v3.

In Figs. 29 and 30, the Artix-7 results are presented for six designs of TinyJAMBU. These designs differ in the number of steps executed per clock cycle. These numbers of steps are: 128 for TinyJAMBU_TJT-v3, 32 for TinyJAMBU_TJT-v2 and TinyJAMBU_GMU-v1, 16 for TinyJAMBU_GMU-v2, 8 for TinyJAMBU_TJT-v1, and 1 for TinyJAMBU_GMU-v1. The larger number of steps per clock cycle, the higher the throughput. At the same time, the area of the circuit increases only moderately. For the same number of steps per clock cycle, 32, TinyJAMBU_TJT-v2 is both slightly faster and significantly smaller than TinyJAMBU_GMU-v1.

In Figs. 31, 32, and 33 the Artix-7 results are presented for eight variants of Xoodyak. Four of these designs were submitted by the Xoodyak Team + Silvia, with Silvia Mella as the primary designer. Two sets, with two different variants in each, were submitted by two different GMU primary designers. Variants Xoodyak_XT-v7, Xoodyak_XT-v8, and all variants from GMU support hashing. By comparing the throughput and area of Xoodyak_XT-v7 vs. Xoodyak_XT-v1, and Xoodyak_XT-v8 vs. Xoodyak_XT-v2, it can be seen that the support for hashing does not introduce any performance penalty in terms of either area or speed. Xoodyak_XT-v8 (a 2× unrolled architecture) is slightly faster than the basic iterative architecture, but it also takes over 600 more LUTs. For the processing of PT, Xoodyak_GMU2-v2 outperforms Xoodyak_XT-v8 by over 3 Gbit/s and a factor of 2.2. For the processing of AD, Xoodyak_GMU2-v1 outperforms Xoodyak_XT-v8 by over 5 Gbit/s and a factor of 2.5. Xoodyak_GMU2-v1 is smaller than Xoodyak_GMU2-v2 by about 700 LUTs. However, even the larger of the two designs has only 2322 LUTs. Xoodyak_GMU2-v1 is a preferred choice for applications with a large size of AD. Xoodyak_GMU2-v2 should be used when the input consists mostly of plaintext. Xoodyak_GMU-v1, with the 384-bit datapath, is slightly slower than the four investigated designs from Xoodyak Team. Its area falls between areas of Xoodyak_XT-v7 and Xoodyak_XT-v8, with the same AEAD+Hash functionality. The second design from GMU is very significantly slower, and only about 170 LUTs smaller than Xoodyak_XT-v1. Thus, this design is not really competitive. For hashing, Xoodyak_GMU2-v2 offers

throughput about 3.6 Gbits/s and Xoodyak_GMU2-v1 about 3 Gbit/s. The throughput of Xoodyak_XT-v8 exceeds 1.8 Gbit/s, Xoodyak_XT-v7 1.5 Gbit/s, and Xoodyak_GMU-v1 640 Mbit/s.

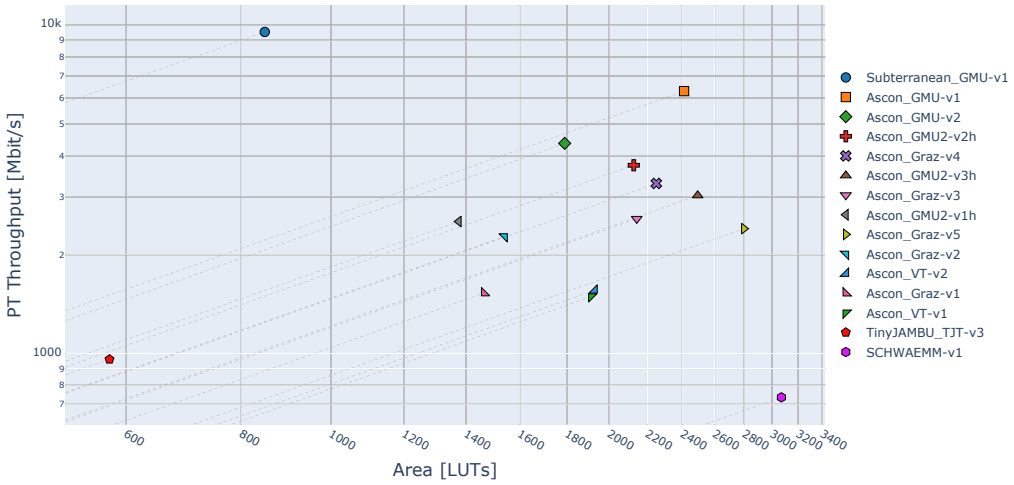

Figure 14: Artix-7 Ascon PT Throughput for Long Messages vs LUTs

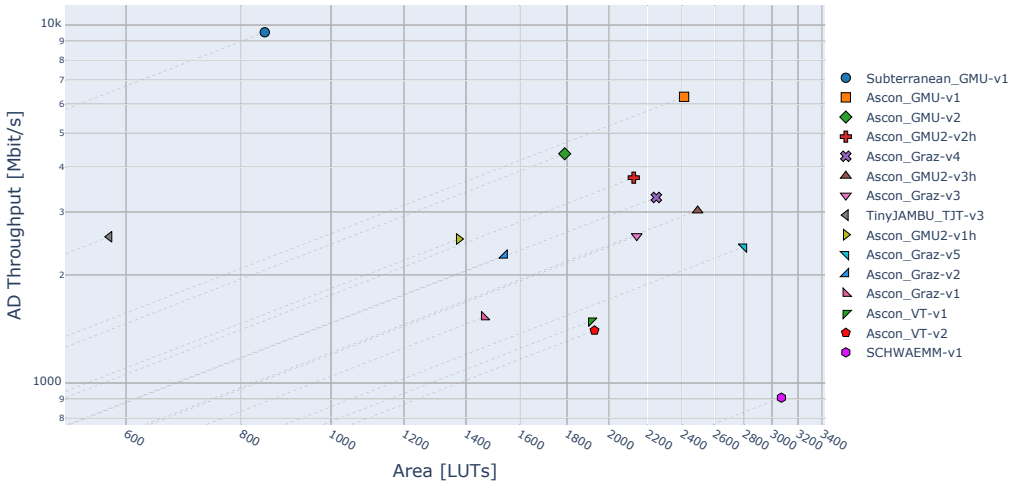

Figure 15: Artix-7 Ascon AD Throughput for Long Messages vs LUTs

5.3 Throughputs for Short Inputs

In the Appendix, in Tables 37–69, we provide values of throughputs for medium and short input sizes, such as 1536 bytes, 64 bytes, and 16 bytes, respectively.

For 1536-byte plaintexts, the throughputs are very close to throughputs for long inputs. The average percentage is 96%, the minimum 89% (Subterranean_ST-v2). Multiple algorithms reach 99%. For 64-byte plaintexts, this ratio varies from 25% for Subterranean_ST-v2 to 99% for ForkAE-v1, with an average of 57%. For 16-byte plaintexts, the ratio varies from 8% for Subterranean_ST-v2 to 98% for ForkAE-v1, with an average of 29%. For 1536-byte ADs, the average percentage is 95%, the minimum 88% (Xoodyak_GMU2-v2). Multiple algorithms reach 99%. For 64-byte ADs, this ratio varies from 22% for Xoodyak_GMU2-v2 to 99% for ForkAE-v1, with an average of 52%. For 16-byte ADs,

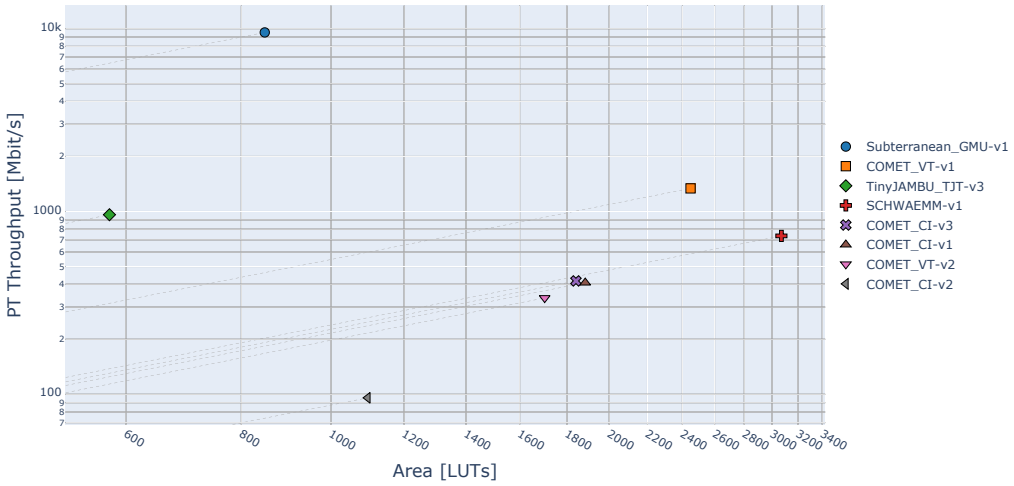

Figure 16: Artix-7 COMET PT Throughput for Long Messages vs LUTs

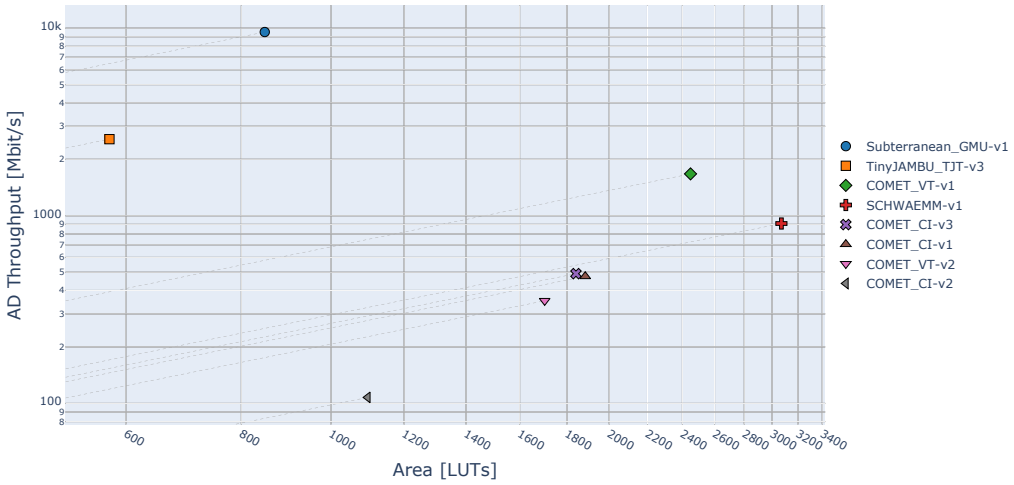

Figure 17: Artix-7 COMET AD Throughput for Long Messages vs LUTs

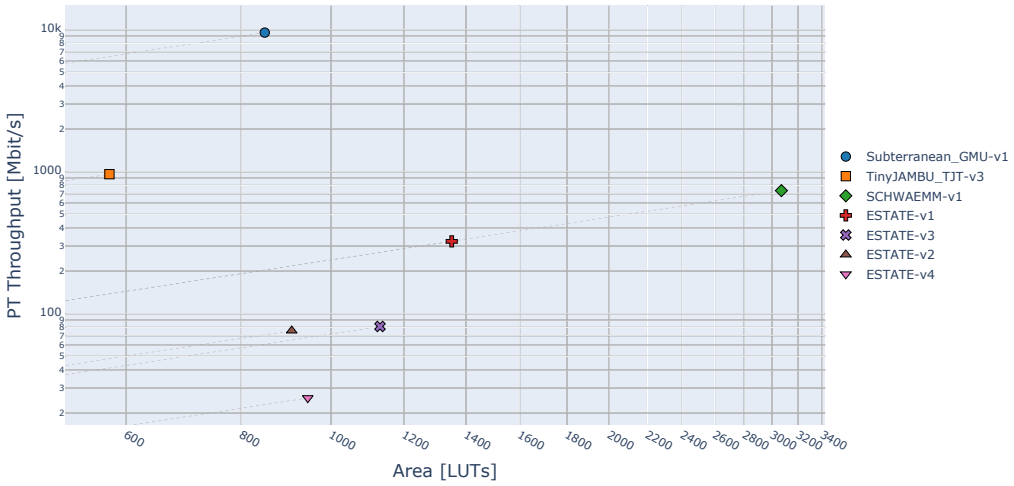

Figure 18: Artix-7 ESTATE PT Throughput for Long Messages vs LUTs

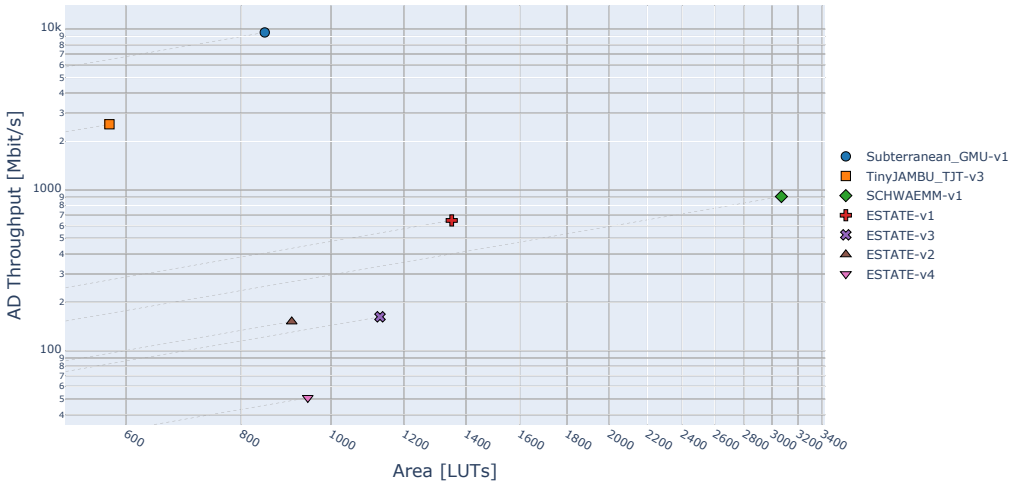

Figure 19: Artix-7 ESTATE AD Throughput for Long Messages vs LUTs

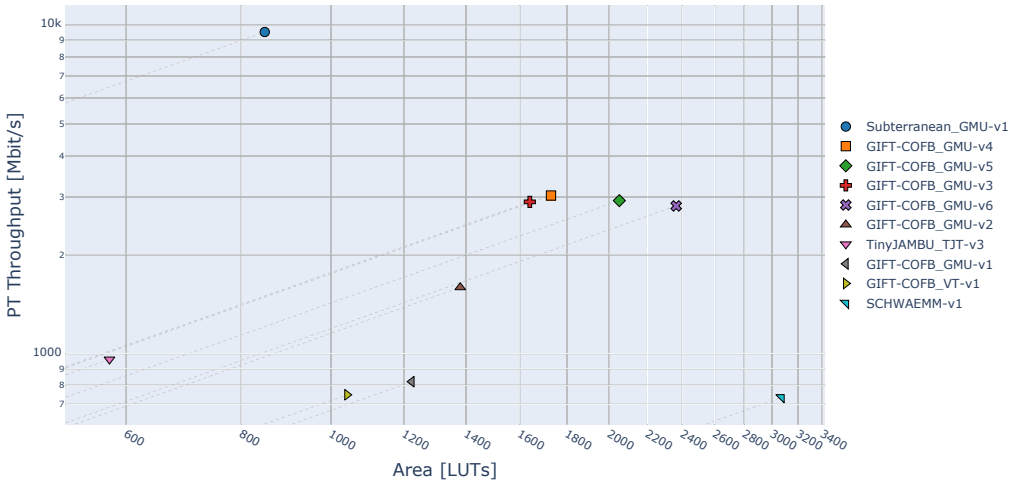

Figure 20: Artix-7 GIFT-COFB PT Throughput for Long Messages vs LUTs

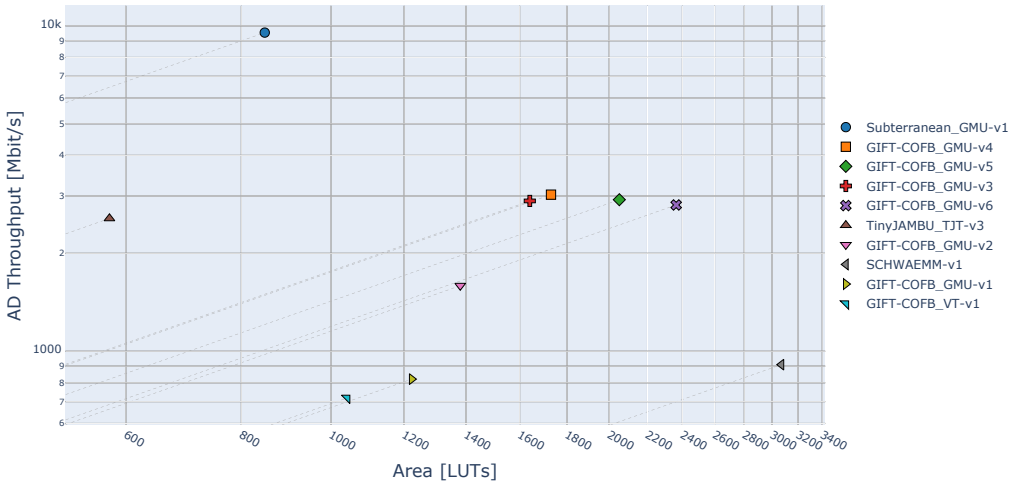

Figure 21: Artix-7 GIFT-COFB AD Throughput for Long Messages vs LUTs

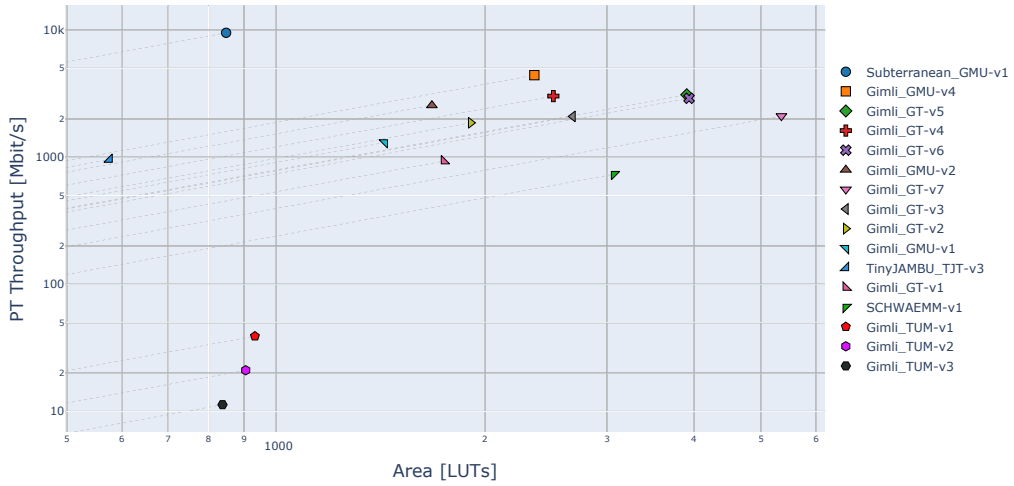

Figure 22: Artix-7 Gimli PT Throughput for Long Messages vs LUTs

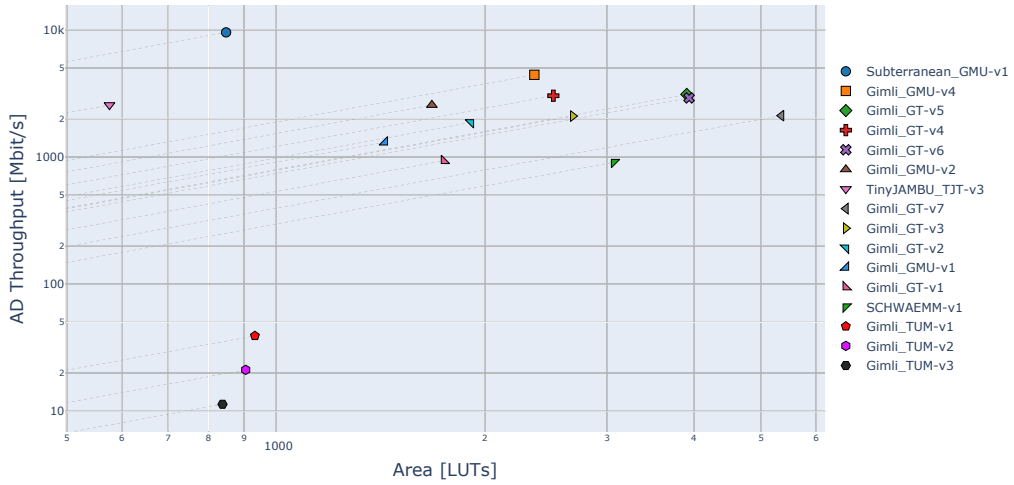

Figure 23: Artix-7 Gimli AD Throughput for Long Messages vs LUTs

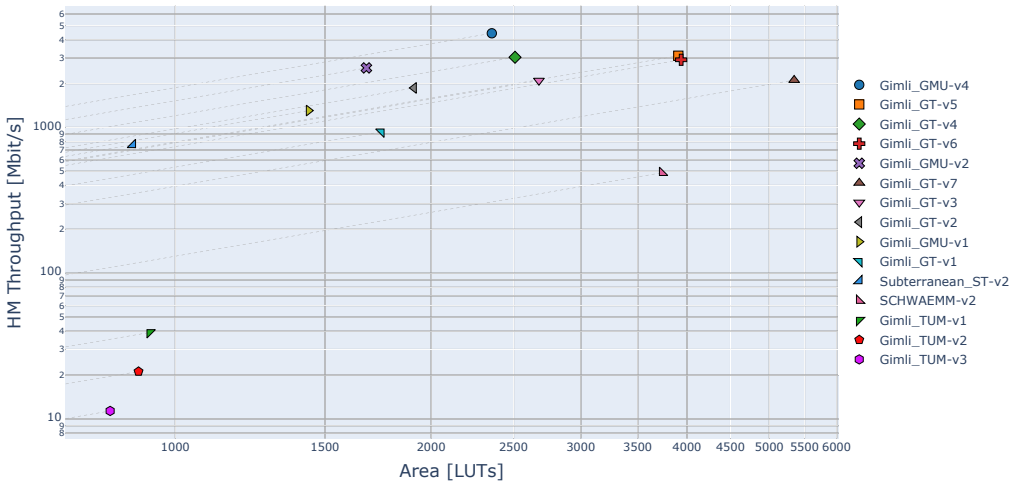

Figure 24: Artix-7 Gimli Hash Throughput for Long Messages vs LUTs

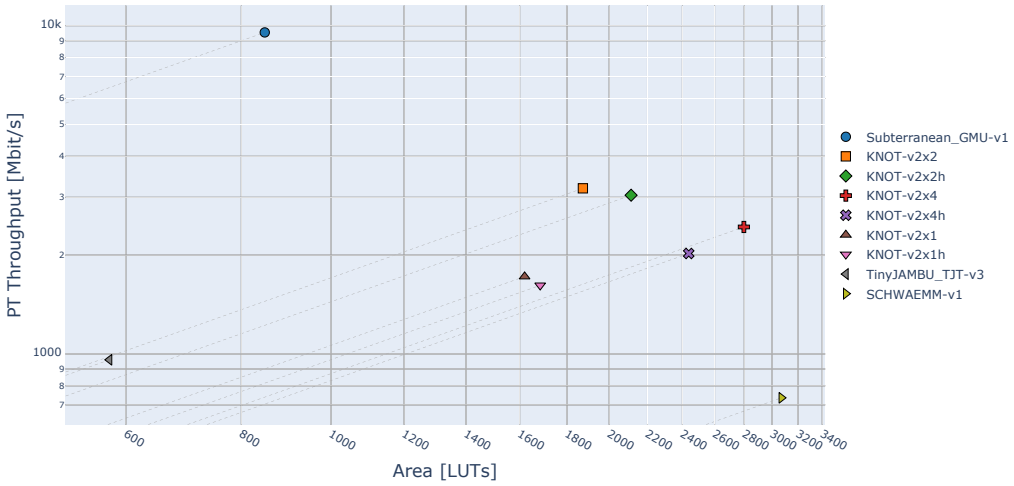

Figure 25: Artix-7 KNOT PT Throughput for Long Messages vs LUTs

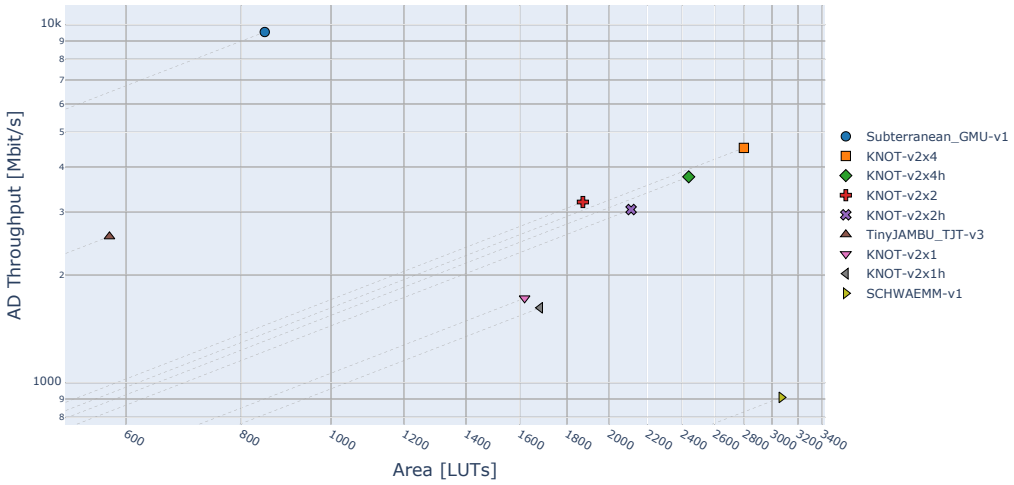

Figure 26: Artix-7 KNOT AD Throughput for Long Messages vs LUTs

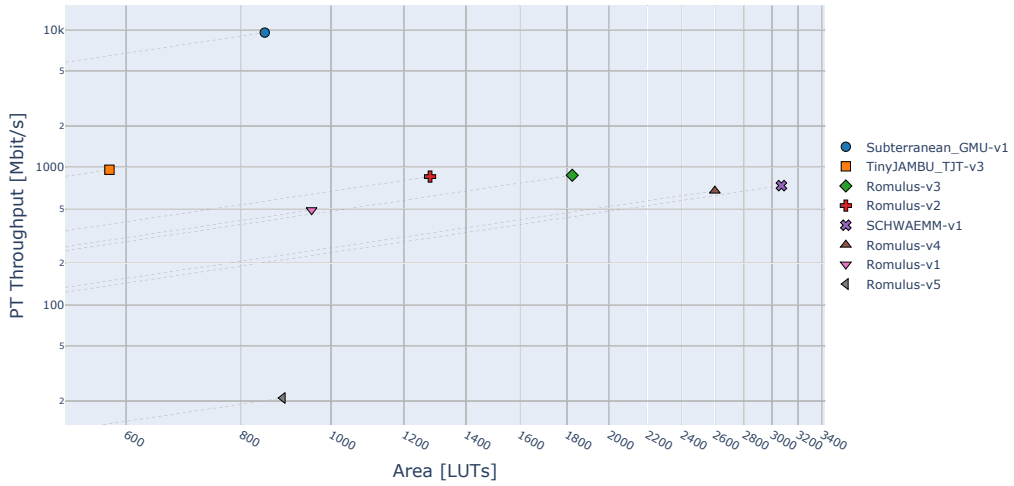

Figure 27: Artix-7 Romulus PT Throughput for Long Messages vs LUTs

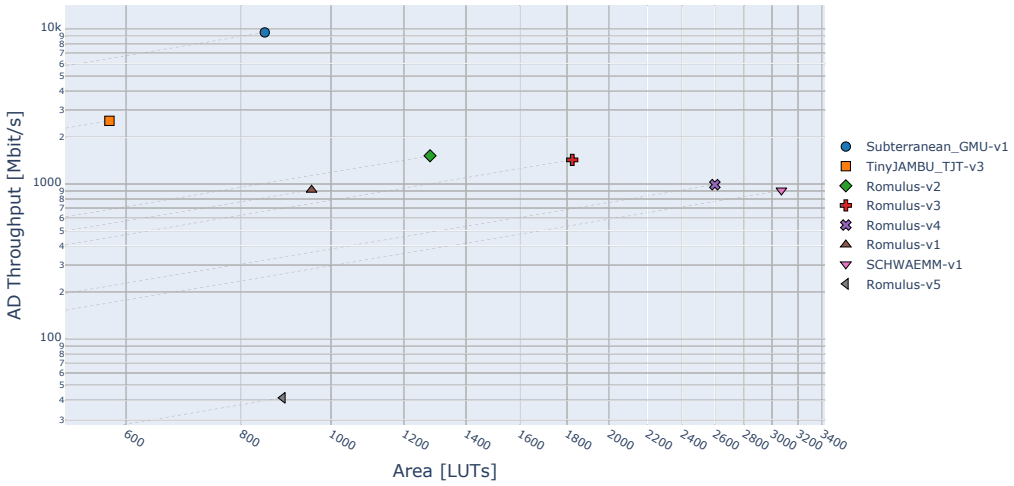

Figure 28: Artix-7 Romulus AD Throughput for Long Messages vs LUTs

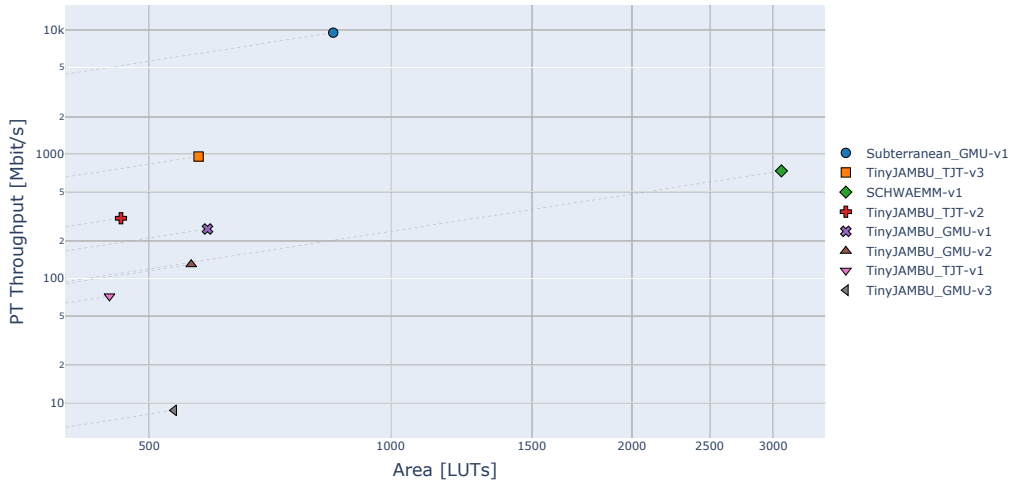

Figure 29: Artix-7 TinyJAMBU PT Throughput for Long Messages vs LUTs

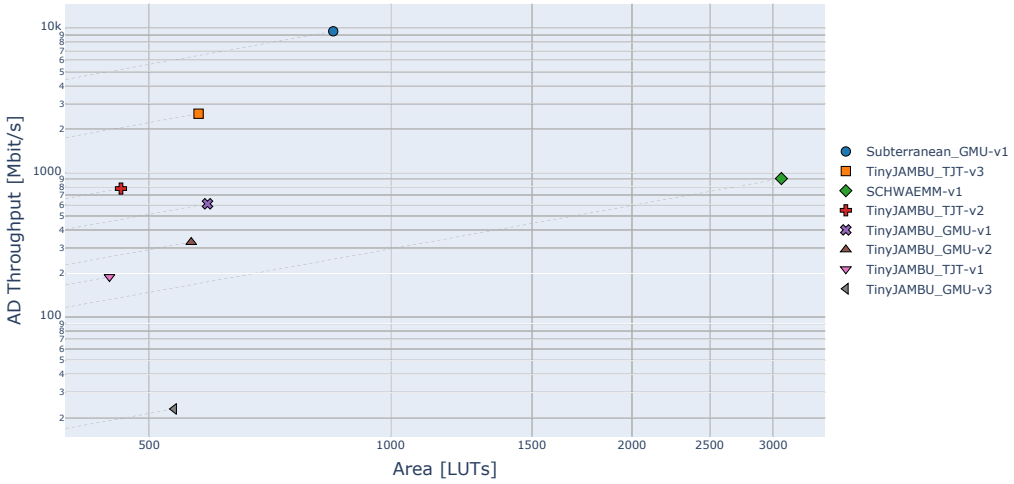

Figure 30: Artix-7 TinyJAMBU AD Throughput for Long Messages vs LUTs

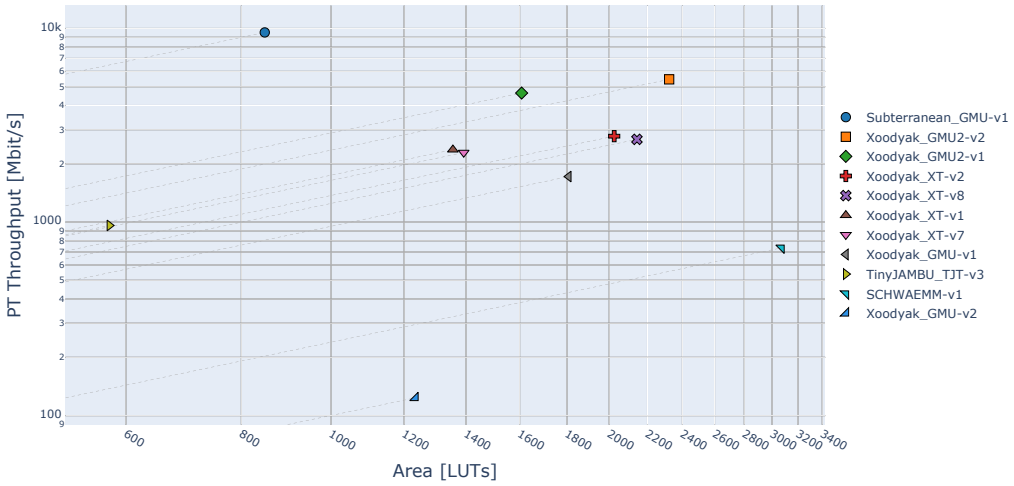

Figure 31: Artix-7 Xoodyak PT Throughput for Long Messages vs LUTs

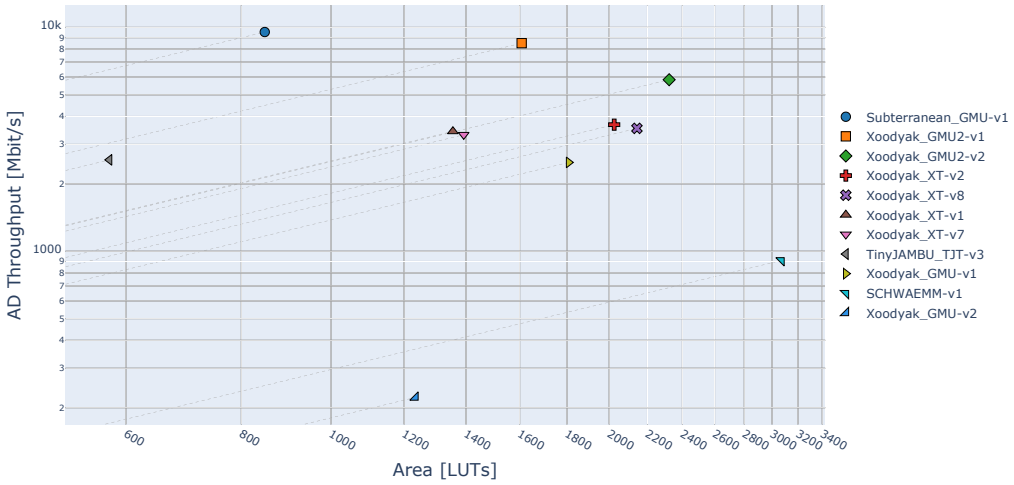

Figure 32: Artix-7 Xoodyak AD Throughput for Long Messages vs LUTs

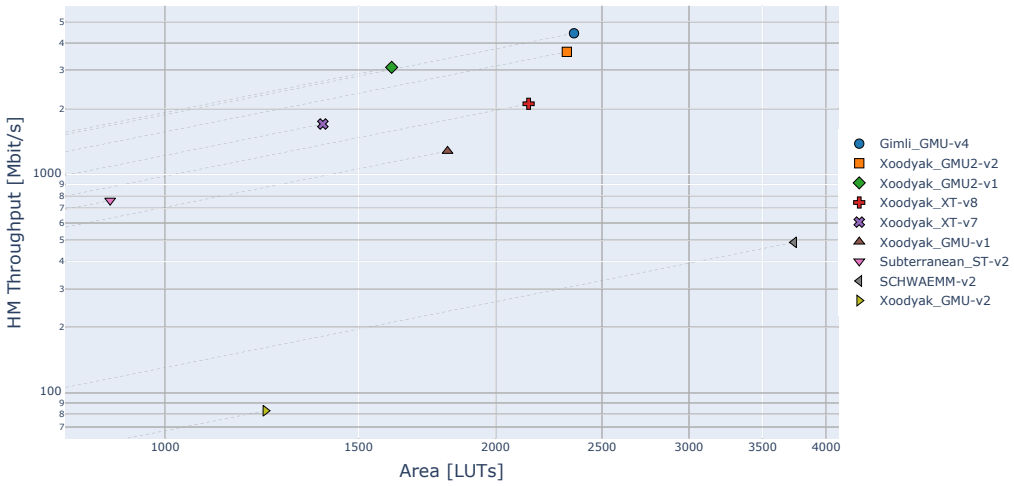

Figure 33: Artix-7 Xoodyak Hash Throughput for Long Messages vs LUTs

Table 8: Xilinx Artix-7 Encryption PT Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Ascon_GMU-v1	Ascon_GMU-v1	Ascon_GMU-v1	Ascon_GMU-v1
3	Xoodyak_GMU2-v2	Xoodyak_GMU2-v2	Gimli_GMU-v4	GIFT-COFB_GMU-v3
4	Gimli_GMU-v4	Gimli_GMU-v4	Xoodyak_GMU2-v1	Gimli_GMU-v4
5	KNOT-v2x2	KNOT-v2x2	GIFT-COFB_GMU-v3	Xoodyak_GMU2-v1
6	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	KNOT-v2x2	COMET_VT-v1
7	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1
8	COMET_VT-v1	COMET_VT-v1	COMET_VT-v1	KNOT-v2x2
9	Spook-v2-v2	Spook-v2-v2	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
10	Elephant-v4	Elephant-v4	Romulus-v2	Romulus-v2
11	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Spook-v2-v2	PHOTON-Beetle-v1
12	Romulus-v3	Romulus-v3	PHOTON-Beetle-v1	Elephant-v2
13	Saturnin-v2	Saturnin-v2	Elephant-v4	SKINNY-AEAD-v2
14	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1	ESTATE-v1
15	PHOTON-Beetle-v1	PHOTON-Beetle-v1	SKINNY-AEAD-v2	Spook-v2-v2
16	SPIX-v1	SPIX-v1	SPIX-v1	ForkAE-v2
17	ISAP-v3	ISAP-v3	Saturnin-v2	SCHWAEMM-v1
18	ACE_GMU-v1	ACE_GMU-v1	ACE_GMU-v1	SPIX-v1
19	SKINNY-AEAD-v1	SKINNY-AEAD-v2	ESTATE-v1	Oribatida-v1
20	mixFeed-v1	mixFeed-v1	ForkAE-v2	LOCUS-v2
21	ESTATE-v1	ESTATE-v1	Oribatida-v1	ACE_GMU-v1
22	Pyjamask-v2	Pyjamask-v2	mixFeed-v1	Saturnin-v2
23	Oribatida-v1	Oribatida-v1	LOCUS-v2	SpoC_IIT-v1
24	ForkAE-v2	ForkAE-v2	ISAP-v3	mixFeed-v1
25	LOCUS-v2	LOCUS-v2	SpoC_IIT-v1	ISAP-v3
26	SpoC_IIT-v1	SpoC_IIT-v1	Pyjamask-v2	Pyjamask-v2
27	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 9: Xilinx Artix-7 Encryption AD Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Ascon_GMU-v1	GIFT-COFB_GMU-v3
3	Ascon_GMU-v1	Ascon_GMU-v1	Xoodyak_GMU2-v1	Ascon_GMU-v1
4	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4
5	KNOT-v2x4h	KNOT-v2x4h	GIFT-COFB_GMU-v3	TinyJAMBU_TJT-v3
6	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	TinyJAMBU_TJT-v3	Xoodyak_GMU2-v1
7	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	KNOT-v2x4h	COMET_VT-v1
8	COMET_VT-v1	COMET_VT-v1	COMET_VT-v1	DryGASCON-v1
9	Saturnin-v2	Romulus-v2	DryGASCON-v1	KNOT-v2x2
10	Romulus-v2	DryGASCON-v1	Romulus-v2	Romulus-v2
11	DryGASCON-v1	Saturnin-v2	PHOTON-Beetle-v1	PHOTON-Beetle-v1
12	Elephant-v2	Elephant-v2	Spook-v2-v2	ESTATE-v1
13	Spook-v2-v2	Spook-v2-v2	Elephant-v2	SKINNY-AEAD-v2
14	ISAP-v3	ISAP-v3	ESTATE-v1	Elephant-v2
15	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1	Spook-v2-v2
16	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Saturnin-v2	ForkAE-v2
17	SPIX-v1	SPIX-v1	SKINNY-AEAD-v2	LOCUS-v2
18	ESTATE-v1	ESTATE-v1	SPIX-v1	SCHWAEMM-v1
19	Oribatida-v1	Oribatida-v1	LOCUS-v2	Saturnin-v2
20	ACE_GMU-v1	ACE_GMU-v1	ISAP-v3	Oribatida-v2
21	SKINNY-AEAD-v1	SKINNY-AEAD-v2	Oribatida-v1	SPIX-v1
22	LOCUS-v2	LOCUS-v2	ACE_GMU-v1	ACE_GMU-v1
23	mixFeed-v1	mixFeed-v1	ForkAE-v2	SpoC_IIT-v1
24	Pyjamask-v2	ForkAE-v2	mixFeed-v1	ISAP-v2
25	ForkAE-v2	Pyjamask-v2	SpoC_IIT-v1	mixFeed-v1
26	SpoC_IIT-v1	SpoC_IIT-v1	Pyjamask-v2	Pyjamask-v2
27	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 10: Xilinx Artix-7 Encryption AD+PT Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Xoodyak_GMU2-v1	Ascon_GMU-v1	Ascon_GMU-v1	Ascon_GMU-v1
3	Ascon_GMU-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	GIFT-COFB_GMU-v3
4	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4	Xoodyak_GMU2-v1
5	KNOT-v2x2	KNOT-v2x2	GIFT-COFB_GMU-v4	Gimli_GMU-v4
6	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	KNOT-v2x2	TinyJAMBU_TJT-v3
7	COMET_VT-v1	COMET_VT-v1	COMET_VT-v1	COMET_VT-v1
8	DryGASCON-v1	DryGASCON-v1	TinyJAMBU_TJT-v3	KNOT-v2x2
9	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	DryGASCON-v1	DryGASCON-v1
10	Spook-v2-v2	Romulus-v2	Romulus-v2	Romulus-v2
11	Romulus-v2	Spook-v2-v2	Spook-v2-v2	PHOTON-Beetle-v1
12	Saturnin-v2	Saturnin-v2	Elephant-v2	Elephant-v2
13	Elephant-v4	Elephant-v4	PHOTON-Beetle-v1	SKINNY-AEAD-v2
14	SCHWAEMM-v1	SCHWAEMM-v1	Saturnin-v2	ESTATE-v1
15	ISAP-v3	ISAP-v3	SCHWAEMM-v1	Spook-v2-v2
16	PHOTON-Beetle-v1	PHOTON-Beetle-v1	SPIX-v1	Saturnin-v2
17	SPIX-v1	SPIX-v1	SKINNY-AEAD-v2	SPIX-v1
18	ACE_GMU-v1	ACE_GMU-v1	ESTATE-v1	ForkAE-v2
19	SKINNY-AEAD-v1	SKINNY-AEAD-v2	ACE_GMU-v1	LOCUS-v2
20	ESTATE-v1	ESTATE-v1	ISAP-v3	SCHWAEMM-v1
21	mixFeed-v1	mixFeed-v1	Oribatida-v1	ACE_GMU-v1
22	Oribatida-v1	Oribatida-v1	LOCUS-v2	Oribatida-v1
23	LOCUS-v2	LOCUS-v2	ForkAE-v2	SpoC_IIT-v1
24	Pyjamask-v2	Pyjamask-v2	mixFeed-v1	mixFeed-v1
25	ForkAE-v2	ForkAE-v2	SpoC_IIT-v1	ISAP-v3
26	SpoC_IIT-v1	SpoC_IIT-v1	Pyjamask-v2	Pyjamask-v2
27	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 11: Xilinx Artix-7 Hash Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4
2	Xoodyak_GMU2-v2	Xoodyak_GMU2-v2	Xoodyak_GMU2-v2	Xoodyak_GMU2-v2
3	Ascon_GMU2-v2h	Ascon_GMU2-v2h	Ascon_GMU2-v2h	DryGASCON-v1
4	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1	Ascon_GMU2-v2h
5	Saturnin-v2	Saturnin-v2	Saturnin-v2	Subterranean_ST-v2
6	KNOT-v2x4h	KNOT-v2x4h	Subterranean_ST-v2	PHOTON-Beetle-v1
7	Subterranean_ST-v2	Subterranean_ST-v2	KNOT-v2x4h	Saturnin-v2
8	ACE_GMU-v1	ACE_GMU-v1	SCHWAEMM-v2	KNOT-v2x4h
9	SCHWAEMM-v2	SCHWAEMM-v2	ACE_GMU-v1	SCHWAEMM-v2
10	PHOTON-Beetle-v1	PHOTON-Beetle-v1	PHOTON-Beetle-v1	ACE_GMU-v1

Table 12: Intel Cyclone 10 LP Encryption PT Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Ascon_GMU-v1	Ascon_GMU-v1	Gimli_GMU-v4	Gimli_GMU-v4
3	Gimli_GMU-v4	Gimli_GMU-v4	Ascon_GMU-v1	Ascon_GMU2-v2h
4	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	GIFT-COFB_GMU-v3
5	KNOT-v2x2h	KNOT-v2x2h	GIFT-COFB_GMU-v3	Xoodyak_GMU2-v1
6	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	KNOT-v2x4	KNOT-v2x4
7	Elephant-v5	Elephant-v5	DryGASCON-v1	TinyJAMBU_TJT-v3
8	DryGASCON-v1	DryGASCON-v1	TinyJAMBU_TJT-v3	DryGASCON-v1
9	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Romulus-v2	Romulus-v2
10	Spook-v2-v2	Romulus-v2	Elephant-v5	PHOTON-Beetle-v1
11	Romulus-v2	Spook-v2-v2	PHOTON-Beetle-v1	Elephant-v5
12	Saturnin-v2	PHOTON-Beetle-v1	Spook-v2-v2	SKINNY-AEAD-v1
13	PHOTON-Beetle-v1	Saturnin-v2	SCHWAEMM-v1	ESTATE-v1
14	ISAP-v3	SCHWAEMM-v1	SKINNY-AEAD-v1	ForkAE-v2
15	SCHWAEMM-v1	ISAP-v4	Saturnin-v2	Spook-v2-v2
16	SPIX-v1	SPIX-v1	SPIX-v1	COMET_CI-v3
17	SKINNY-AEAD-v1	SKINNY-AEAD-v1	COMET_CI-v3	Oribatida-v1
18	ACE_GMU-v1	ACE_GMU-v1	ACE_GMU-v1	SCHWAEMM-v1
19	COMET_CI-v3	COMET_CI-v3	ESTATE-v1	LOCUS-v2
20	Oribatida-v1	Oribatida-v1	ISAP-v4	SpoC_IIT-v1
21	ESTATE-v1	ESTATE-v1	Oribatida-v1	Saturnin-v2
22	mixFeed-v1	mixFeed-v1	ForkAE-v2	SPIX-v1
23	SpoC_IIT-v1	SpoC_IIT-v1	SpoC_IIT-v1	ACE_GMU-v1
24	ForkAE-v2	ForkAE-v2	LOCUS-v2	ISAP-v4
25	LOCUS-v2	LOCUS-v2	mixFeed-v1	mixFeed-v1
26	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
27	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1

Table 13: Intel Cyclone 10 LP Encryption AD Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Gimli_GMU-v4	GIFT-COFB_GMU-v3
3	Ascon_GMU-v1	Ascon_GMU-v1	Xoodyak_GMU2-v1	Gimli_GMU-v4
4	Gimli_GMU-v4	Gimli_GMU-v4	Ascon_GMU-v1	TinyJAMBU_TJT-v3
5	KNOT-v2x4	KNOT-v2x4	TinyJAMBU_TJT-v3	Ascon_GMU2-v2h
6	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	GIFT-COFB_GMU-v3	Xoodyak_GMU2-v1
7	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	KNOT-v2x4	KNOT-v2x4
8	Romulus-v2	Romulus-v2	DryGASCON-v1	DryGASCON-v1
9	Saturnin-v2	Saturnin-v2	Romulus-v2	Romulus-v2
10	Elephant-v5	Elephant-v5	PHOTON-Beetle-v1	PHOTON-Beetle-v1
11	DryGASCON-v1	DryGASCON-v1	Elephant-v5	ESTATE-v1
12	ISAP-v3	ISAP-v3	Spook-v2-v2	SKINNY-AEAD-v1
13	Spook-v2-v2	PHOTON-Beetle-v1	SCHWAEMM-v1	Elephant-v5
14	PHOTON-Beetle-v1	Spook-v2-v2	ESTATE-v1	ForkAE-v2
15	SCHWAEMM-v1	SCHWAEMM-v1	Saturnin-v2	LOCUS-v2
16	SPIX-v1	SPIX-v1	ISAP-v4	Spook-v2-v2
17	Oribatida-v1	ESTATE-v1	SKINNY-AEAD-v1	COMET_CI-v3
18	ESTATE-v1	Oribatida-v1	LOCUS-v2	Saturnin-v2
19	SKINNY-AEAD-v1	SKINNY-AEAD-v1	Oribatida-v1	SCHWAEMM-v1
20	LOCUS-v2	LOCUS-v2	COMET_CI-v3	Oribatida-v1
21	ACE_GMU-v1	ACE_GMU-v1	SPIX-v1	ISAP-v4
22	COMET_CI-v3	COMET_CI-v3	ForkAE-v2	SpoC_IIT-v1
23	ForkAE-v2	ForkAE-v2	ACE_GMU-v1	SPIX-v1
24	mixFeed-v1	mixFeed-v1	SpoC_IIT-v1	ACE_GMU-v1
25	SpoC_IIT-v1	SpoC_IIT-v1	mixFeed-v1	mixFeed-v1
26	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
27	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1

Table 14: Intel Cyclone 10 LP Encryption AD+PT Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Gimli_GMU-v4
3	Ascon_GMU-v1	Ascon_GMU-v1	Gimli_GMU-v4	GIFT-COFB_GMU-v3
4	Gimli_GMU-v4	Gimli_GMU-v4	Ascon_GMU-v1	Ascon_GMU2-v2h
5	KNOT-v2x4	KNOT-v2x4	GIFT-COFB_GMU-v3	Xoodyak_GMU2-v1
6	GIFT-COFB_GMU-v4	GIFT-COFB_GMU-v4	KNOT-v2x4	KNOT-v2x4
7	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
8	Elephant-v5	Elephant-v5	DryGASCON-v1	Romulus-v2
9	DryGASCON-v1	DryGASCON-v1	Romulus-v2	DryGASCON-v1
10	Romulus-v2	Romulus-v2	Elephant-v5	PHOTON-Beetle-v1
11	Saturnin-v2	Saturnin-v2	PHOTON-Beetle-v1	Elephant-v5
12	Spook-v2-v2	Spook-v2-v2	Spook-v2-v2	SKINNY-AEAD-v1
13	ISAP-v3	ISAP-v3	Saturnin-v2	ESTATE-v1
14	PHOTON-Beetle-v1	PHOTON-Beetle-v1	SCHWAEMM-v1	Saturnin-v2
15	SCHWAEMM-v1	SCHWAEMM-v1	SKINNY-AEAD-v1	Spook-v2-v2
16	SPIX-v1	SPIX-v1	ISAP-v4	ForkAE-v2
17	SKINNY-AEAD-v1	SKINNY-AEAD-v1	SPIX-v1	COMET_CI-v3
18	ACE_GMU-v1	ACE_GMU-v1	ESTATE-v1	LOCUS-v2
19	COMET_CI-v3	COMET_CI-v3	COMET_CI-v3	SCHWAEMM-v1
20	Oribatida-v1	Oribatida-v1	ACE_GMU-v1	Oribatida-v1
21	ESTATE-v1	ESTATE-v1	Oribatida-v1	SPIX-v1
22	LOCUS-v2	LOCUS-v2	LOCUS-v2	SpoC_IIT-v1
23	mixFeed-v1	mixFeed-v1	ForkAE-v2	ACE_GMU-v1
24	ForkAE-v2	ForkAE-v2	SpoC_IIT-v1	ISAP-v4
25	SpoC_IIT-v1	SpoC_IIT-v1	mixFeed-v1	mixFeed-v1
26	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
27	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1

Table 15: Intel Cyclone 10 LP Hash Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
3	Ascon_GMU2-v2h	Ascon_GMU2-v2h	Ascon_GMU2-v2h	DryGASCON-v1
4	Saturnin-v2	DryGASCON-v1	DryGASCON-v1	Subterranean_ST-v2
5	DryGASCON-v1	Saturnin-v2	Subterranean_ST-v2	Ascon_GMU2-v2h
6	KNOT-v2x4h	KNOT-v2x4h	Saturnin-v2	PHOTON-Beetle-v1
7	Subterranean_ST-v2	Subterranean_ST-v2	KNOT-v2x4h	Saturnin-v2
8	SCHWAEMM-v2	SCHWAEMM-v2	SCHWAEMM-v2	KNOT-v2x4h
9	ACE_GMU-v1	ACE_GMU-v1	PHOTON-Beetle-v1	SCHWAEMM-v2
10	PHOTON-Beetle-v1	PHOTON-Beetle-v1	ACE_GMU-v1	ACE_GMU-v1

Table 16: Lattice ECP5 Encryption PT Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
3	Gimli_GMU-v4	Gimli_GMU-v4	Ascon_GMU-v2	Ascon_GMU-v2
4	Ascon_GMU-v2	Ascon_GMU-v2	Gimli_GMU-v4	Gimli_GMU-v4
5	KNOT-v2x2	KNOT-v2x2	KNOT-v2x2	TinyJAMBU_TJT-v3
6	GIFT-COFB_GMU-v3	GIFT-COFB_GMU-v3	GIFT-COFB_GMU-v3	GIFT-COFB_GMU-v3
7	Elephant-v5	Elephant-v5	DryGASCON-v1	DryGASCON-v1
8	DryGASCON-v1	DryGASCON-v1	TinyJAMBU_TJT-v3	KNOT-v2x4
9	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	PHOTON-Beetle-v1	PHOTON-Beetle-v1
10	Spook-v2-v2	Spook-v2-v2	Elephant-v5	Romulus-v2
11	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Romulus-v2	Elephant-v2
12	Saturnin-v2	Saturnin-v2	Spook-v2-v2	ESTATE-v1
13	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1	SKINNY-AEAD-v1
14	Romulus-v2	Romulus-v2	SKINNY-AEAD-v1	Oribatida-v1
15	SPIX-v1	SPIX-v1	ACE_GMU-v1	Spook-v2-v2
16	ACE_GMU-v1	ACE_GMU-v1	SPIX-v1	SCHWAEMM-v1
17	ISAP-v4	SKINNY-AEAD-v1	Saturnin-v2	ACE_GMU-v1
18	SKINNY-AEAD-v1	ISAP-v4	ESTATE-v1	ForkAE-v2
19	Oribatida-v1	Oribatida-v1	Oribatida-v1	COMET_CI-v3
20	COMET_VT-v2	ESTATE-v1	COMET_CI-v3	SPIX-v1
21	ESTATE-v1	COMET_VT-v2	SpoC_IIT-v1	Saturnin-v2
22	SpoC_IIT-v1	SpoC_IIT-v1	ForkAE-v2	SpoC_IIT-v1
23	ForkAE-v2	ForkAE-v2	LOCUS-v2	LOCUS-v2
24	Pyjamask-v2	Pyjamask-v2	ISAP-v4	mixFeed-v1
25	mixFeed-v1	mixFeed-v1	mixFeed-v1	ISAP-v4
26	LOCUS-v2	LOCUS-v2	Pyjamask-v2	Pyjamask-v2
27	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 17: Lattice ECP5 Encryption AD Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Subterranean_GMU-v1	Subterranean_GMU-v1	Xoodyak_GMU2-v1	TinyJAMBU_TJT-v3
3	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4	Xoodyak_GMU2-v1
4	KNOT-v2x4	Ascon_GMU-v2	Ascon_GMU-v2	Ascon_GMU2-v2h
5	Ascon_GMU-v2	KNOT-v2x4	TinyJAMBU_TJT-v3	Gimli_GMU-v4
6	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	GIFT-COFB_GMU-v3	GIFT-COFB_GMU-v3
7	GIFT-COFB_GMU-v3	GIFT-COFB_GMU-v3	KNOT-v2x4	DryGASCON-v1
8	Saturnin-v2	Saturnin-v2	DryGASCON-v1	PHOTON-Beetle-v1
9	Elephant-v5	DryGASCON-v1	PHOTON-Beetle-v1	KNOT-v2x4
10	DryGASCON-v1	Elephant-v5	Elephant-v5	ESTATE-v1
11	Romulus-v2	Romulus-v2	Romulus-v2	Romulus-v2
12	PHOTON-Beetle-v1	PHOTON-Beetle-v1	ESTATE-v1	Elephant-v5
13	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1	SKINNY-AEAD-v1
14	Spook-v2-v2	Spook-v2-v2	Spook-v2-v2	Oribatida-v1
15	SPIX-v1	SPIX-v1	Saturnin-v2	Spook-v2-v2
16	Oribatida-v1	Oribatida-v1	Oribatida-v1	SCHWAEMM-v1
17	ESTATE-v1	ESTATE-v1	SKINNY-AEAD-v1	ForkAE-v2
18	ISAP-v4	ISAP-v4	SPIX-v1	Saturnin-v2
19	ACE_GMU-v1	ACE_GMU-v1	ACE_GMU-v1	COMET_CI-v3
20	SKINNY-AEAD-v1	SKINNY-AEAD-v1	COMET_CI-v3	LOCUS-v2
21	COMET_CI-v3	COMET_CI-v3	LOCUS-v2	ACE_GMU-v1
22	LOCUS-v2	LOCUS-v2	ISAP-v4	SPIX-v1
23	SpoC_IIT-v1	SpoC_IIT-v1	ForkAE-v2	SpoC_IIT-v1
24	ForkAE-v2	ForkAE-v2	SpoC_IIT-v1	ISAP-v4
25	Pyjamask-v2	Pyjamask-v2	mixFeed-v1	mixFeed-v1
26	mixFeed-v1	mixFeed-v1	Pyjamask-v2	Pyjamask-v2
27	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 18: Lattice ECP5 Encryption AD+PT Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1	Subterranean_GMU-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
3	Gimli_GMU-v4	Gimli_GMU-v4	Gimli_GMU-v4	Ascon_GMU2-v2h
4	Ascon_GMU-v2	Ascon_GMU-v2	Ascon_GMU-v2	Gimli_GMU-v4
5	KNOT-v2x2	KNOT-v2x2	KNOT-v2x4	GIFT-COFB_GMU-v3
6	GIFT-COFB_GMU-v3	GIFT-COFB_GMU-v3	GIFT-COFB_GMU-v3	TinyJAMBU_TJT-v3
7	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	KNOT-v2x4
8	Elephant-v5	Elephant-v5	DryGASCON-v1	DryGASCON-v1
9	DryGASCON-v1	DryGASCON-v1	Elephant-v5	Romulus-v2
10	Saturnin-v2	Saturnin-v2	PHOTON-Beetle-v1	PHOTON-Beetle-v1
11	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Romulus-v2	Elephant-v5
12	Romulus-v2	Romulus-v2	Spook-v2-v2	ESTATE-v1
13	Spook-v2-v2	Spook-v2-v2	SCHWAEMM-v1	SKINNY-AEAD-v1
14	SCHWAEMM-v1	SCHWAEMM-v1	Saturnin-v2	Saturnin-v2
15	SPIX-v1	SPIX-v1	SPIX-v1	Oribatida-v1
16	ACE_GMU-v1	ACE_GMU-v1	ESTATE-v1	Spook-v2-v2
17	ISAP-v4	ISAP-v4	ACE_GMU-v1	SCHWAEMM-v1
18	Oribatida-v1	Oribatida-v1	Oribatida-v1	ACE_GMU-v1
19	ESTATE-v1	ESTATE-v1	SKINNY-AEAD-v1	SPIX-v1
20	SKINNY-AEAD-v1	SKINNY-AEAD-v1	COMET_CI-v3	COMET_CI-v3
21	COMET_CI-v3	COMET_CI-v3	ISAP-v4	ForkAE-v2
22	SpoC_IIT-v1	SpoC_IIT-v1	SpoC_IIT-v1	SpoC_IIT-v1
23	LOCUS-v2	LOCUS-v2	ForkAE-v2	LOCUS-v2
24	ForkAE-v2	ForkAE-v2	LOCUS-v2	ISAP-v4
25	Pyjamask-v2	Pyjamask-v2	mixFeed-v1	mixFeed-v1
26	mixFeed-v1	mixFeed-v1	Pyjamask-v2	Pyjamask-v2
27	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 19: Lattice ECP5 Hash Throughput Rankings for Different Input Sizes

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Gimli_GMU-v4	Gimli_GMU-v4	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Gimli_GMU-v4	Gimli_GMU-v4
3	Ascon_GMU2-v2h	Ascon_GMU2-v2h	DryGASCON-v1	DryGASCON-v1
4	Saturnin-v2	DryGASCON-v1	Ascon_GMU2-v2h	Ascon_GMU2-v2h
5	DryGASCON-v1	Saturnin-v2	Subterranean_ST-v2	Subterranean_ST-v2
6	KNOT-v2x4h	Subterranean_ST-v2	Saturnin-v2	PHOTON-Beetle-v1
7	Subterranean_ST-v2	KNOT-v2x4h	KNOT-v2x4h	Saturnin-v2
8	ACE_GMU-v1	ACE_GMU-v1	SCHWAEMM-v2	KNOT-v2x4h
9	SCHWAEMM-v2	SCHWAEMM-v2	ACE_GMU-v1	SCHWAEMM-v2
10	PHOTON-Beetle-v1	PHOTON-Beetle-v1	PHOTON-Beetle-v1	ACE_GMU-v1

the ratio varies from 6% for Xoodyak_GMU2-v1 to 95% for ForkAE-v1, with an average of 24%. All mentioned above percentages are dependent only on the algorithm and its hardware architecture. They do not depend on a particular FPGA device.

In Tables 8, 9, 10, and 11, we summarize the relative changes in rankings for Artix-7. For processing of PT only, the following algorithms rank higher for short messages than for long messages: GIFT-COFB, COMET, TinyJAMBU, Romulus, PHOTON-Beetle, SKINNY-AEAD, ESTATE, ForkAE, Oribatida, LOCUS, and SpoC. The opposite is true for the following candidates: Xoodyak, KNOT, Elephant, Spook, SCHWAEMM, SPIX, Saturnin, mixFeed, ISAP, Pyjamask, and WAGE. The following 10 algorithms remain among the best 12, independently of the size of inputs: Subterranean 2.0, Ascon, Xoodyak, Gimli, KNOT, GIFT-COFB, DryGASCON, COMET, TinyJAMBU, and Romulus. For the plaintext of the size of 64 bytes, Elephant drops to position 13. For the plaintext of the size of 16 bytes, Spook-v2 drops to position 15. Out of the mentioned above 10 algorithms, the following 6 also support hashing: Gimli, Xoodyak, Ascon, DryGASCON, Subterranean 2.0, and KNOT (with the first four substantially faster than the remaining two). A candidate particularly fast in hashing but not so good for processing small plaintexts is Saturnin.

For processing of AD only, the following algorithms rank consistently higher for short messages than for long messages: GIFT-COFB, TinyJAMBU, COMET, DryGASCON, PHOTON-Beetle, ESTATE, SKINNY-AEAD, ForkAE, LOCUS, and SpoC. The opposite is true for the following candidates: Xoodyak, KNOT, Elephant, SCHWAEMM, Saturnin, Oribatida, SPIX, ISAP, mixFeed, Pyjamask, and WAGE. The following 8 algorithms remain among the best 10, independently of the size of inputs: Subterranean 2.0, Xoodyak, Ascon, Gimli, KNOT, GIFT-COFB, TinyJAMBU, COMET, Romulus, and DryGASCON. For 16-byte ADs, Elephant drops to position 14 and Saturnin to position 19.

For Hashing, DryGASCON moves ahead of Ascon and Subterranean 2.0 ahead of Saturnin for 16-byte messages. The position of ACE drops for smaller messages. The ranking of Saturnin gets significantly worse, and the ranking of PHOTON-Beetle improves for 16-byte inputs.

In Tables 12–18, we summarize the relative changes in rankings for Cyclone 10 LP and ECP5.

6 Power and Energy Evaluation

6.1 Power Estimation Flow

The total power consumed by an FPGA device executing an authenticated encryption or hashing algorithm can be divided into:

- **Device Static Power**, which is the power from CMOS transistor leakage currents. This power is consumed even if the device is programmed with a blank bitstream. Its value is influenced mostly by device technology, voltage, and operating temperature.
- **Dynamic Power**, which is the power consumed for charging and discharging driven capacitances (CMOS transistor gates, interconnects, etc).

  The following formula can be used for simple estimation of dynamic power:

$$P_{dynamic} = \alpha C V^2 f$$

  where α denotes activity rate, which is 1 if the driving signal toggles at every clock cycles, f denotes the operating frequency, and V is the supply voltage.

In our experiments, we relied on Xilinx's Vivado v2020.1 power analysis feature (Report Power) [37] to obtain vector-based power estimations for the submitted designs on the target Artix-7 device (xc7a12tcsg325-3, 28nm process technology), assuming a typical process corner and operating conditions.

A power estimation tool tries to predict dynamic device power based on signal activity and by utilizing capacitance models for the mapped FPGA resources, including LUTs, FFs, and interconnects. Xilinx claims an accuracy of +/-10% of maximum process power values [38] and total accuracy of +/-15% [37] for Vivado power estimations obtained using post-implementation timing simulation. Our flow ensures that 100% of the netlists signals are matched during power estimation and that a "Production" device model and a "High" confidence level is reported by Vivado. We also expect that the absence of BRAMs, DSPs, encrypted IP blocks, and latches in the implemented LWC designs should improve Vivado's power estimations' accuracy.

Switching activity of all internal nodes and ports of the design is collected through post-implementation timing simulation using Vivado Simulator (`xsim`) using LWC VHDL testbench (LWC_TB) and `N` distinct test vectors of fixed size and operation. The test vectors are generated using cryptotvgen [29] [39] with key, nonce, plaintext, AD, and hash message chosen from a uniform random distribution.

`N` is chosen in such a way to keep the variance of power results for the same design, simulated with different sets of random test vectors of the same size, within 10%, while making the time required for post-implementation simulations manageable. For inputs of the size 16 bytes, `N` is set to 20, and for inputs of the size 1536 bytes, `N` is set to 5.

Power and energy estimations of two-pass submissions (Saturnin, ISAP) do not include the power required for writing to and reading from the two-pass FIFO. The two-pass FIFO is not synthesized. It is also not included in the resource utilization of the design. Cycle measurements, on the other hand, cover the entire operation of the core, including the read/write operations from/to the two-pass FIFO.

The recording of node switching activities and cycles count begin after the reset of the design under test (DUT) is complete and the first input words are provided by the testbench. The generated SAIF (Switching Activity Interchange Format) file contains toggle counts of each node, as well as timing attributes about the length of an interval each signal stayed at a particular value (0, 1, X, etc.). Using post-implementation timing simulation ensures accounting for all node activities, including glitch transitions.

After simulation is complete, the implemented design is reloaded to Vivado from its last checkpoint, and power estimation is performed using the SAIF file. The output of the tool is a power report estimating the average dynamic and static power.

The described above power estimation flow is graphically illustrated in Fig. 34.

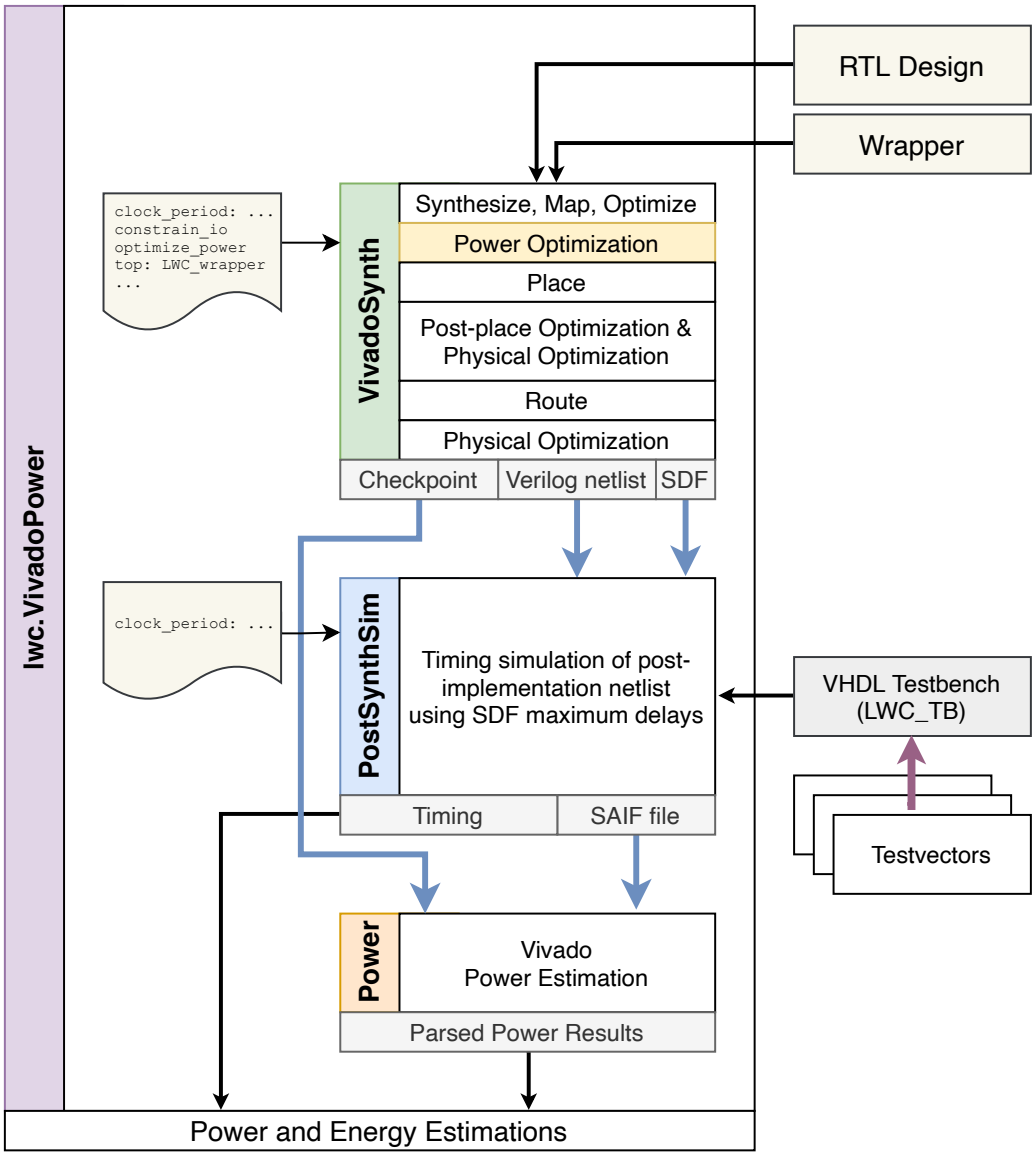

Figure 34: Vivado power estimation flow, automated using Xeda [32]

In addition to power optimizations performed during general optimization stages, an extra `power_opt_design` stage is performed during the power flow. During power optimization, Vivado uses ASIC-style clock-gating techniques based on sequential analysis of the design [40]. The power optimization stage can execute either before or after design placement. We use pre-place power optimization, which is believed to be most effective for most designs.

All estimations are performed for a fixed clock frequency, supported by all evaluated designs, equal to 75 MHz. However, with the dynamic power dominating total power for the majority of designs, the rankings of algorithms in terms of the selected primary metric,

energy per bit, remains almost independent of the specific frequency choice.

6.2 Results and Analyses

Estimated static power is almost the same for all submissions and equal to around 60 mW. Estimated dynamic power spans a wide range, with a maximum reported power of 20,533 mW (20.5 Watts) for hashing of short messages in Ascon_Graz-v6, and a minimum reported dynamic power of 4 mW for all operations of TinyJAMBU_TJT-v1.

In bar graphs with multiple metrics, shown in Figs. 35–40 and Fig. 45 a variant of a candidate with the best value of each data is selected. As a result, some candidates are represented by two variants. The exact values of all estimated metrics are summarized in Tables 20 and 21.

The notation used in all figures and tables belonging to this section is as follows:

- *Enc 1536,0*: authenticated encryption with the plaintext size = 1536 bytes and AD size = 0 bytes
- *Enc 0,1536*: authenticated encryption with the plaintext size = 0 bytes and AD size = 1536 bytes
- *Dec 1536,0*: authenticated decryption with the ciphertext size = 1536 bytes and AD size = 0 bytes
- *AEAD 1536*: arithmetic mean of authenticated encryption/decryption operations with either plaintext/ciphertext size or AD equal to 1536 bytes, i.e., the average of "*Enc 1536,0*", "*Enc 0,1536*", and "*Dec 1536,0*"
- *Enc 16,0*: authenticated encryption with the plaintext size = 16 bytes and AD size = 0 bytes
- *Enc 0,16*: authenticated encryption with the plaintext size = 0 bytes and AD size = 16 bytes
- *Dec 16,0*: authenticated decryption with the ciphertext size = 16 bytes and AD size = 0 bytes
- *AEAD 16*: arithmetic mean of authenticated encryption/decryption operations with either plaintext/ciphertext size or AD equal to 16 bytes, i.e., average of "*Enc 16,0*", "*Enc 0,16*", and "*Dec 16,0*".
- *Hash 1536*: hashing with the message size = 1536 bytes
- *Hash 16*: hashing with the message size = 16 bytes.

The results are missing for ESTATE and Oribatida. For ESTATE, the interface of a two-pass FIFO used in the submitted code is different than that defined in the LWC Hardware API. Supporting this FIFO would require a non-trivial change in the testbench LWC_TB. For Oribatida, timing simulations take excessively long time, possibly because of the limited syntesizability of the code (as indicated by a large number of synthesis warnings for v1 and a failing post-synthesis simulation for v2). The remaining 25 candidates covered by this study are represented in all graphs and tables.

In unrolled architectures of multiple submissions, we see superlinear increase of power with respect to the unrolling factor. This effect comes from the sharp increase in glitches happening in more complex combinational paths during each clock cycle and has previously been observed in [27]. Incorporating glitch filtering techniques, such as those presented in [41], may be helpful in reducing energy consumption of unrolled implementations. However, these techniques were not applied to any of the received submissions.

The primary metric according to which we suggest evaluating all submissions is energy per bit. The smaller the value of this metric, the better. Values of this metric are depicted, for various types of inputs, in Fig. 35 for AEAD inputs of the size of 1536 bytes, in Fig. 37 for AEAD inputs of the size of 16 bytes, and in Fig. 39 for hashing.

In Fig. 41, three bars per candidate, depicted in Fig. 35, are averaged, leading to the simplified comparison. Similarly, in Fig. 42, three bars per candidate, depicted in Fig. 37 are averaged, resulting in one bar per each candidate.

Finally, in Fig. 45, the results from Figs. 41 and 42 are combined together.

The corresponding graphs, illustrating throughput-over-area for the mentioned above cases, are shown in Figs. 36, 38, 40, 43, 44.

In Figs. 46–57, we present two dimensional graphs showing the relation (or the lack of it) between energy per bit and power on one side, and average throughput, average throughput-over-area, and area on the other side. Thus, six possible two-dimensional charts are presented.

The general conclusions from these graphs are:

- Candidates that were previously shown to excel in throughput, assuming a certain limit on the circuit area, perform equally well in terms of energy per bit for a fixed frequency. One clear exception is a worse ranking of Saturnin.
- On average, the higher the throughput (for a fixed clock frequency), the smaller energy per bit.
- For the received submissions (aiming at particular maximum area), the higher the throughput over area (for a fixed clock frequency), the smaller energy per bit.
- There is no clear relationship between Energy per bit and Area.
- There is no clear correlation between Average Power and metrics such as Area, Throughput, or Throughput-over-Area.

Additional space exploration graphs, concerning performance of multiple variants of each candidate in terms of energy per bit and power are included in Appendix B.

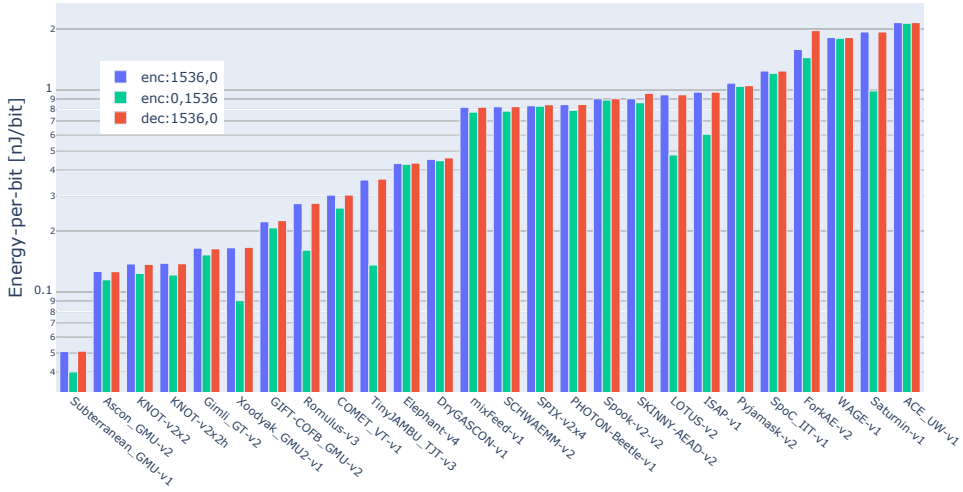

Figure 35: Energy-per-bit for Authenticated Encryption and Decryption of 1536-Byte messages at 75MHz

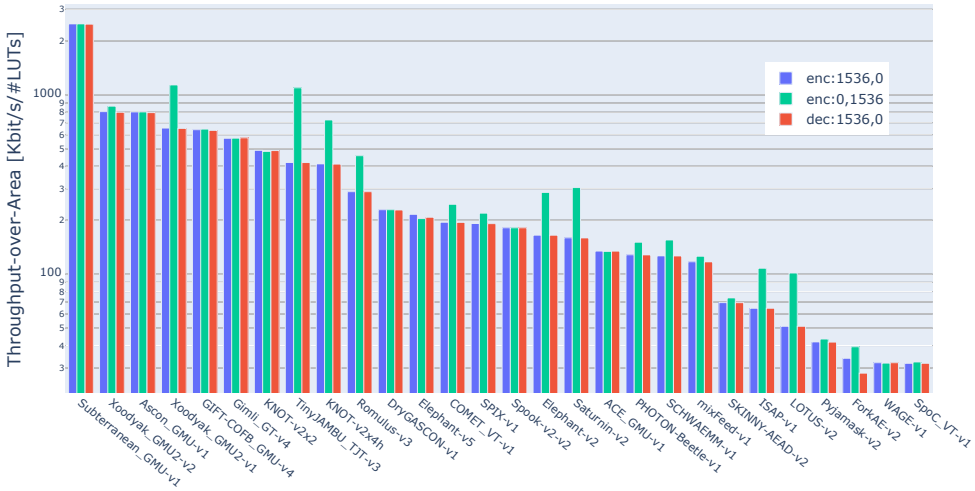

Figure 36: Throughput-over-Area for Authenticated Encryption and Decryption of 1536-Byte messages at 75MHz

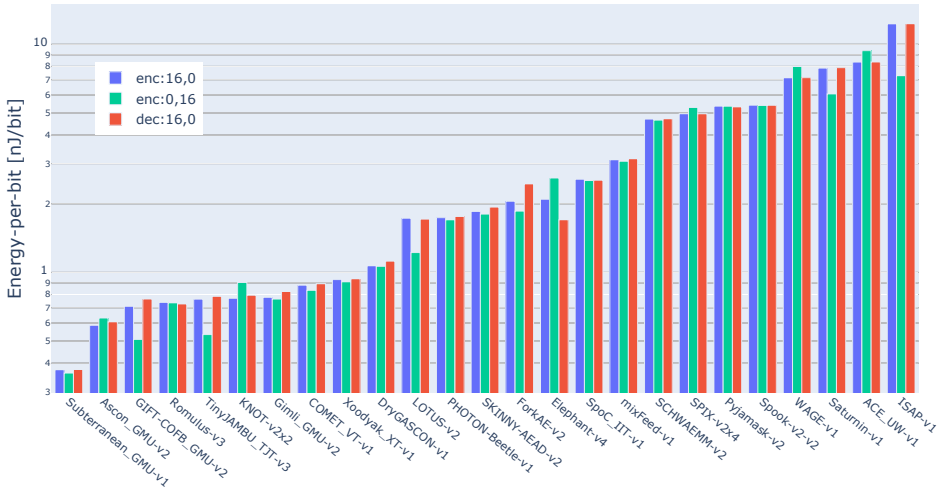

Figure 37: Energy-per-bit for Authenticated Encryption and Decryption of 16-Byte messages at 75MHz

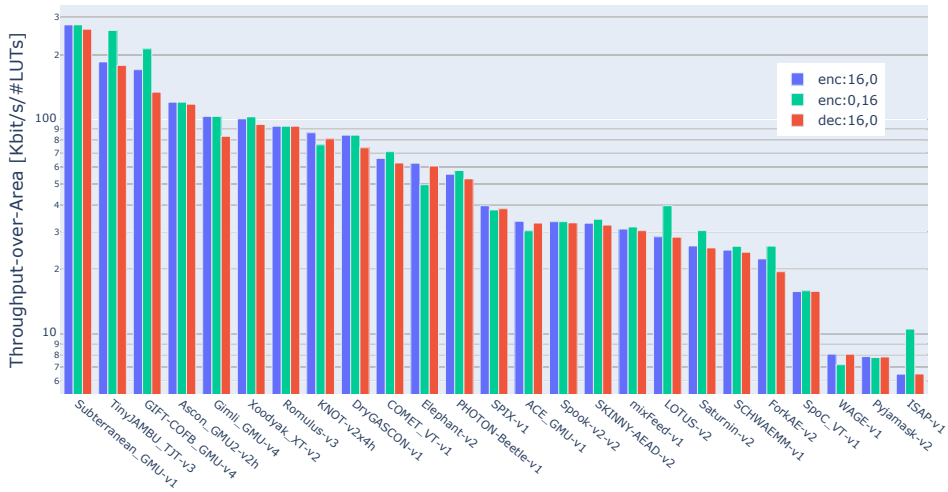

Figure 38: Throughput-over-Area for Authenticated Encryption and Decryption of 16-Byte messages at 75MHz

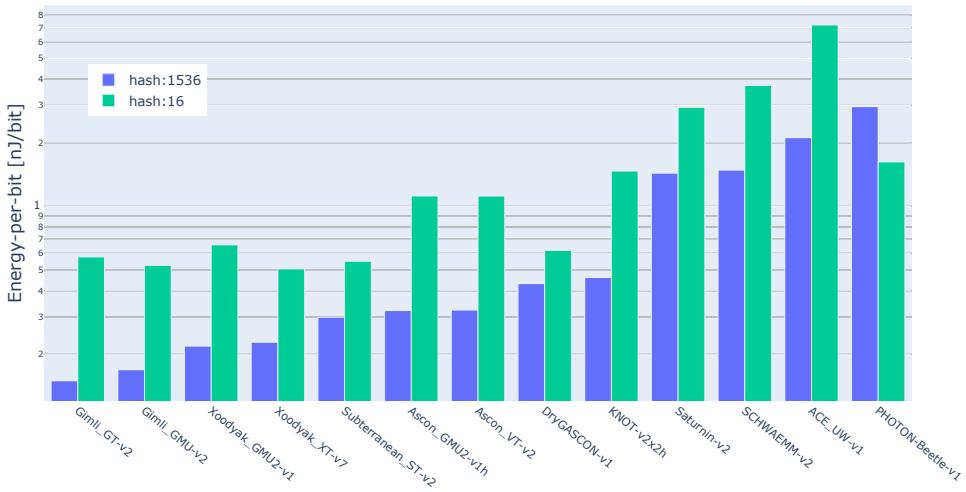

Figure 39: Energy-per-bit for Hashing at 75MHz

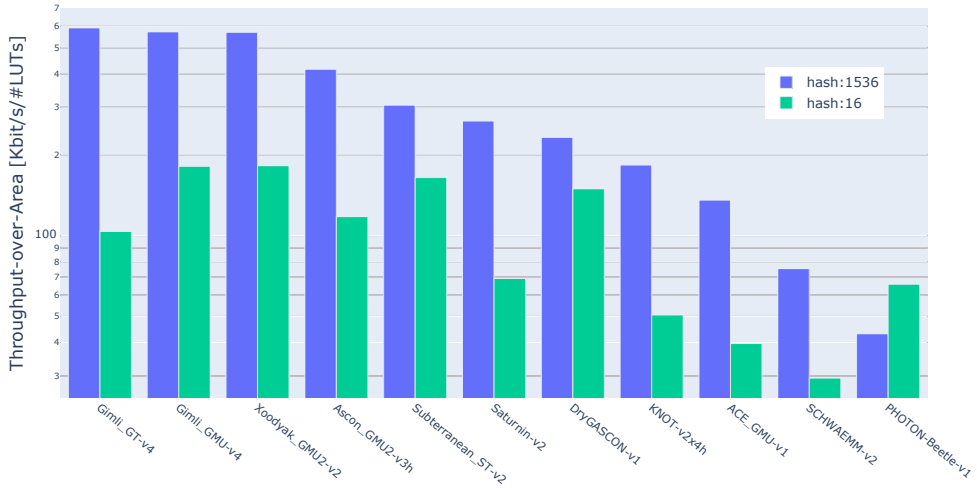

Figure 40: Hashing Throughput-over-Area at 75MHz

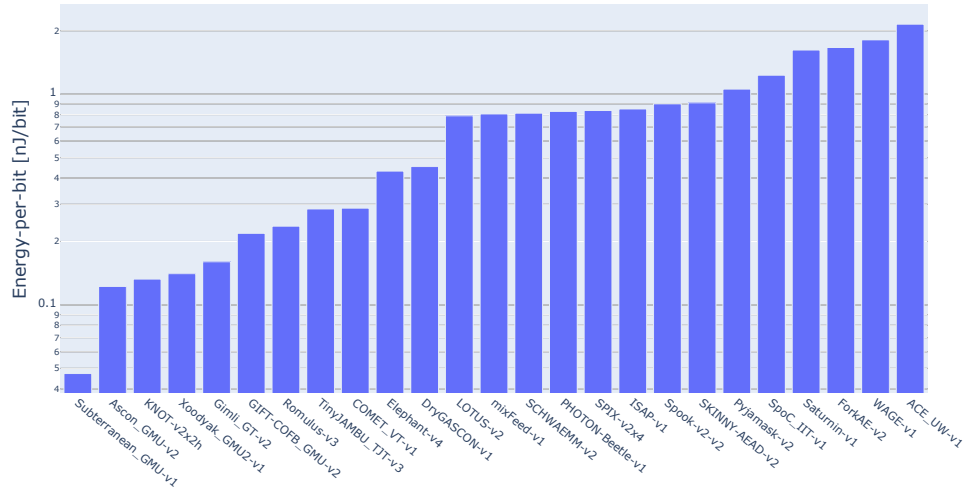

Figure 41: AEAD Long Average Energy-per-bit at 75MHz

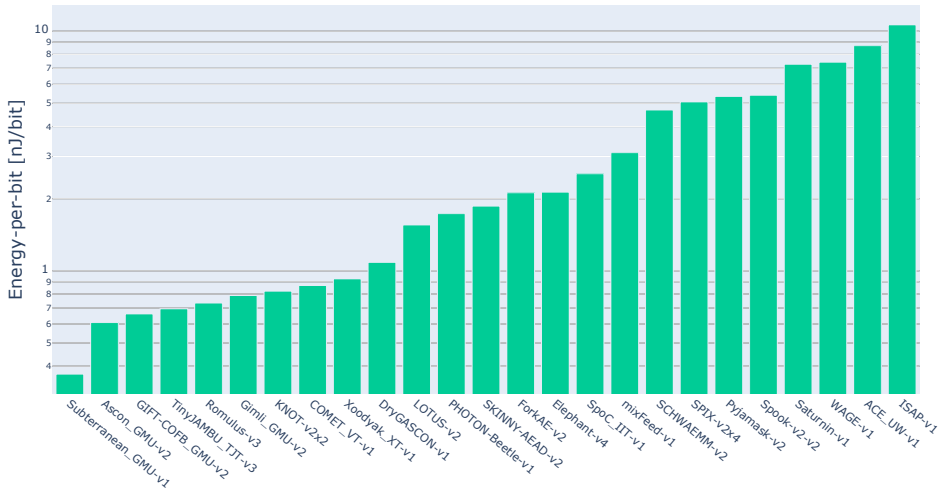

Figure 42: AEAD Short Average Energy-per-bit at 75MHz

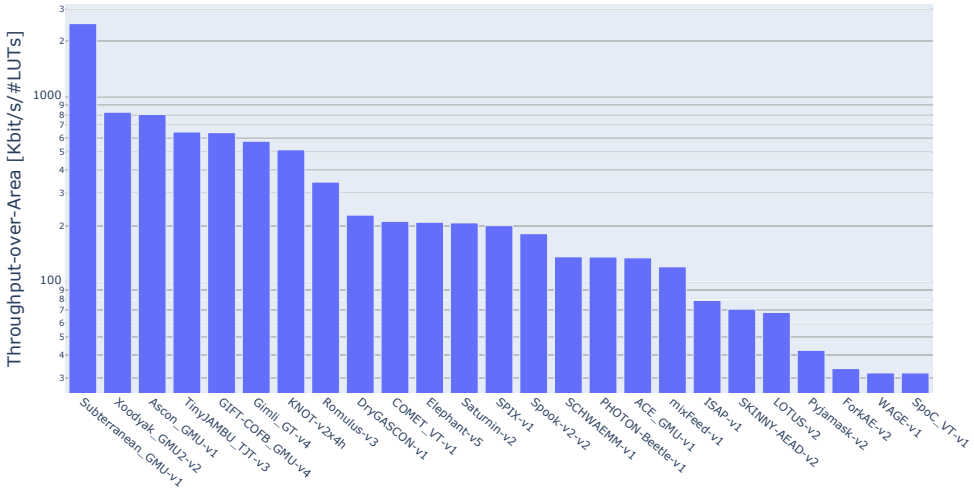

Figure 43: AEAD Long Average Throughput-over-Area at 75MHz

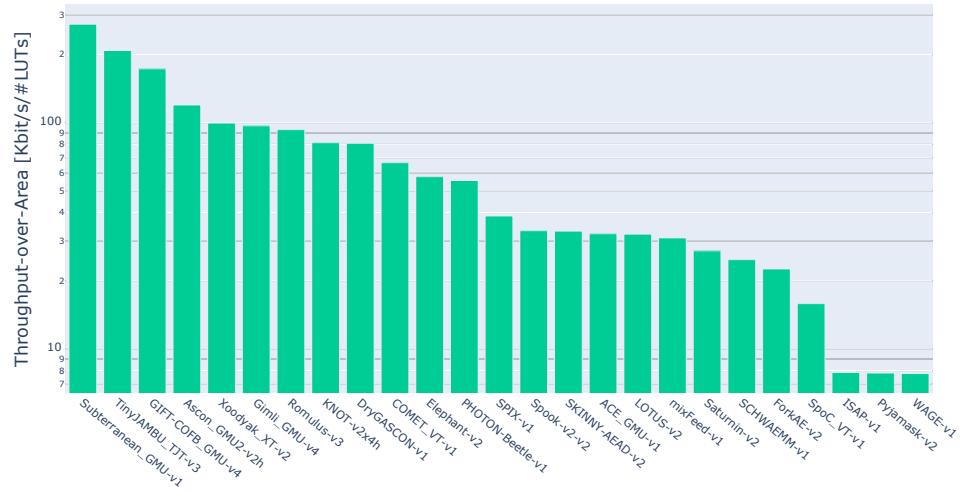

Figure 44: AEAD Short Average Throughput-over-Area at 75MHz

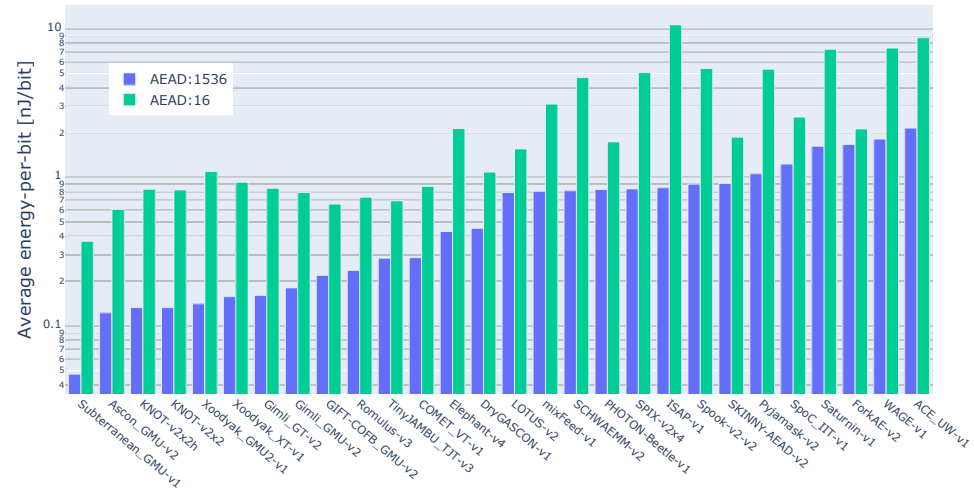

Figure 45: Energy-per-bits for AEAD of long and short messages at 75MHz

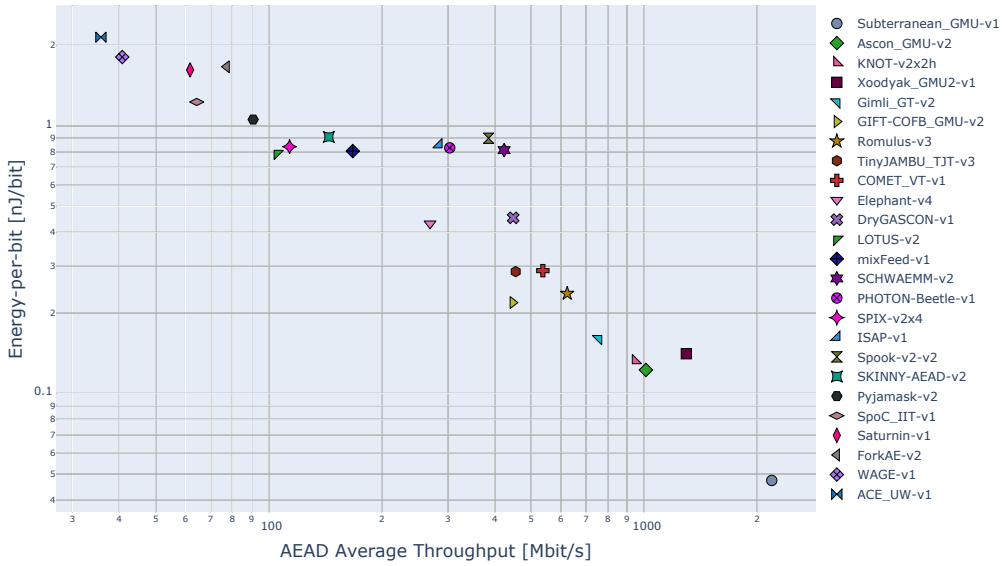

Figure 46: Average Energy-per-bit vs. Average Throughput for AEAD of 1536-Byte messages at 75MHz

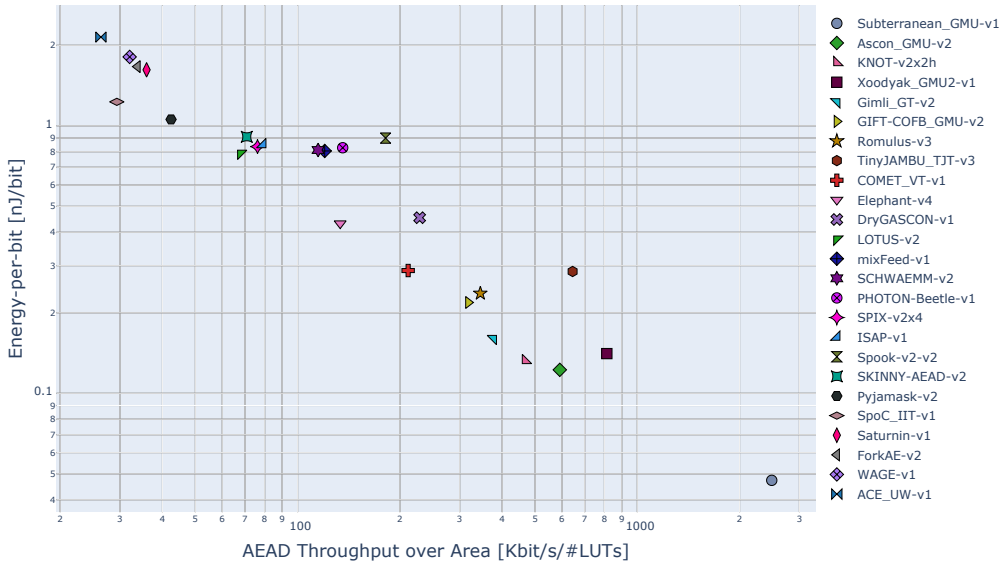

Figure 47: Average Energy-per-bit vs. Average Throughput-over-Area for AEAD of 1536-Byte messages at 75MHz

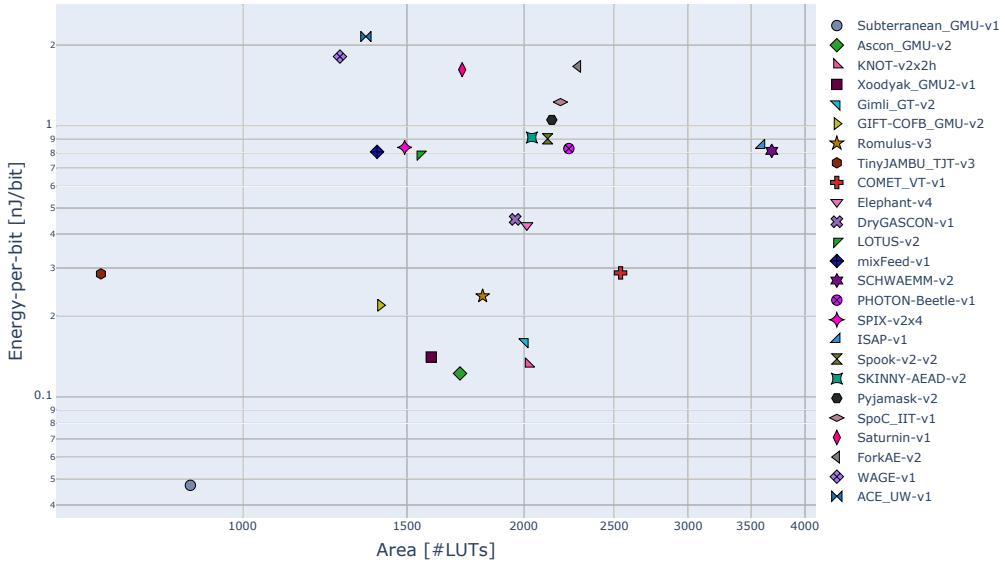

Figure 48: Average Energy-per-bits for AEAD of 1536-Byte messages at 75MHz vs. Area (LUTs)

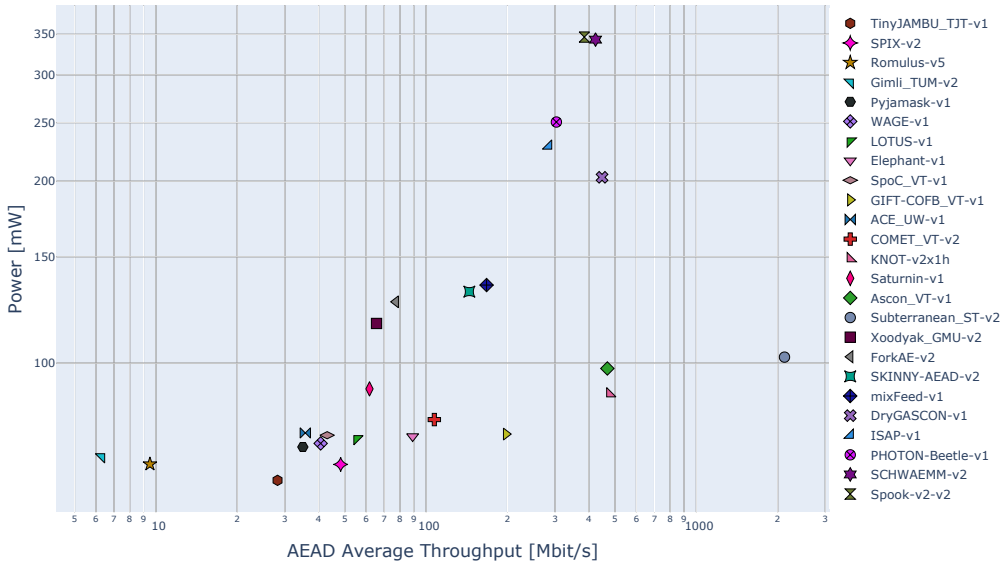

Figure 49: Average Power vs. Average Throughput for AEAD of 1536-Byte messages at 75MHz

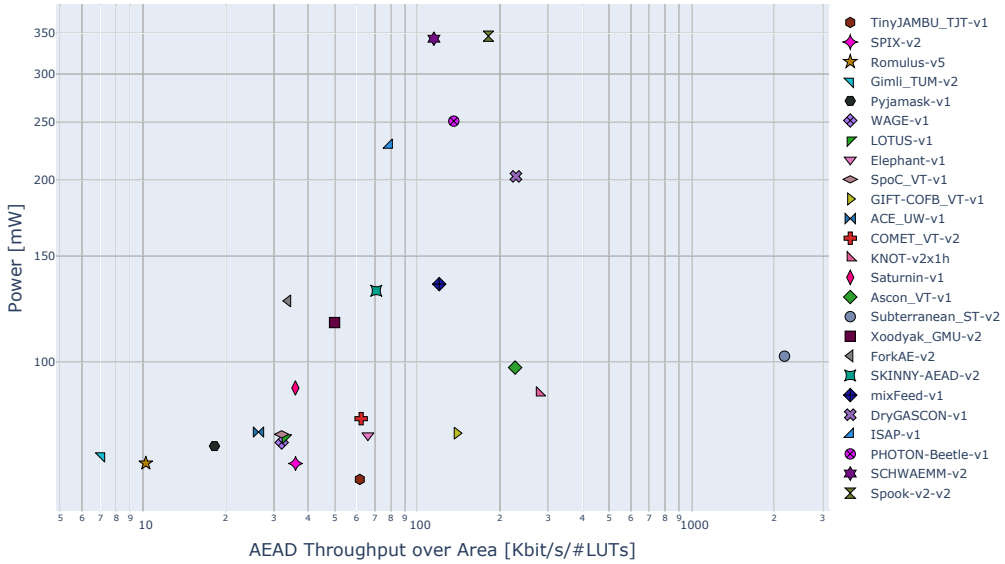

Figure 50: Average Power vs. Average Throughput-over-Area for AEAD of 1536-Byte messages at 75MHz

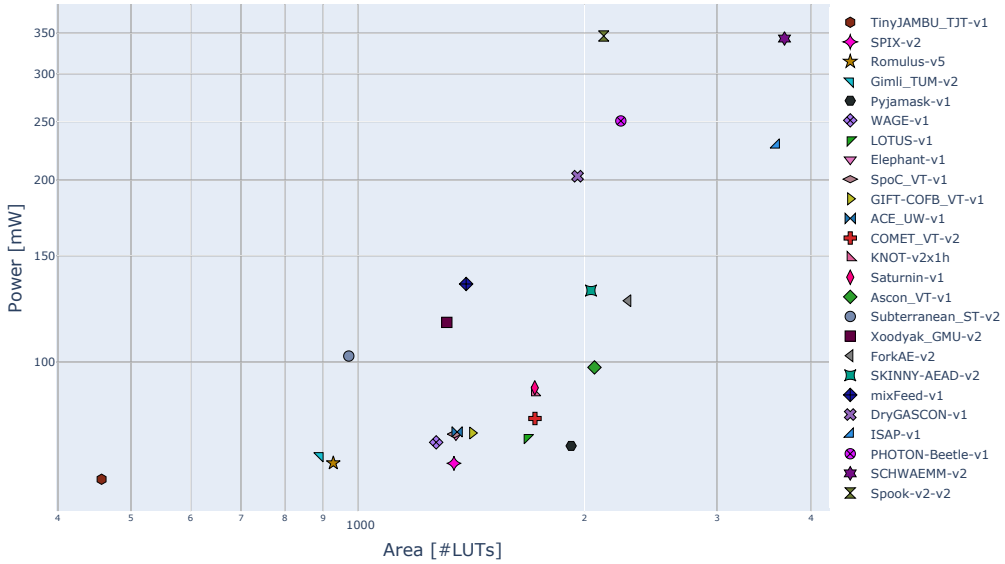

Figure 51: Average Power for AEAD of 1536-Byte messages at 75MHz vs. Area (LUTs)

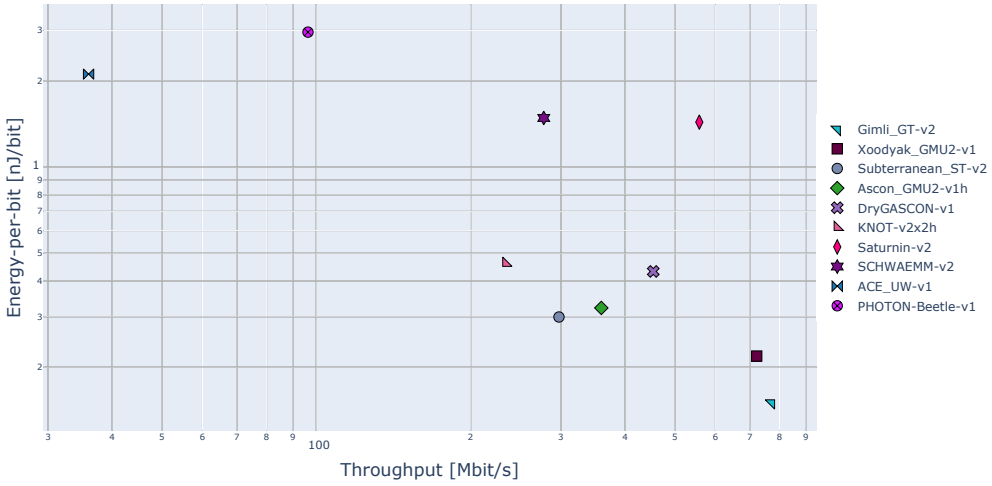

Figure 52: Energy-per-bit vs. Throughput for Hashing of 1536-Byte messages at 75MHz

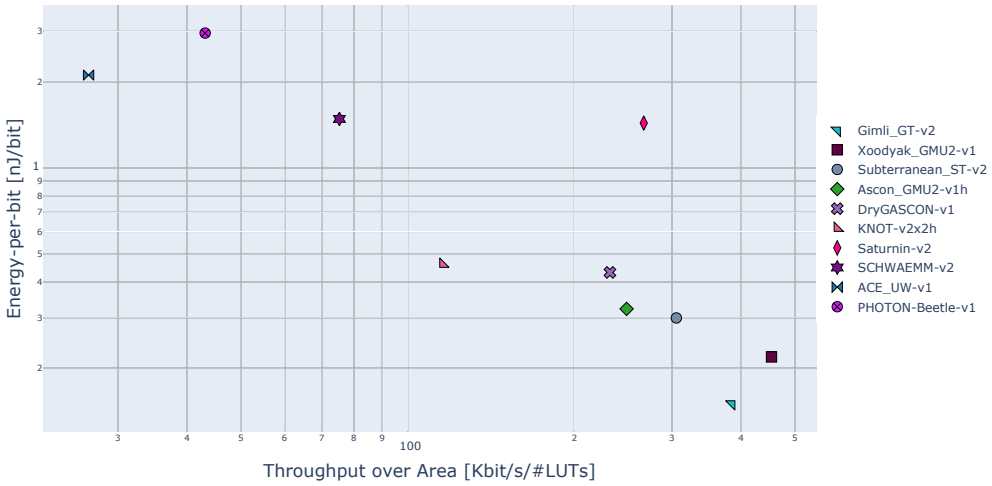

Figure 53: Energy-per-bit vs. Throughput-over-area for Hashing of 1536-Byte messages at 75MHz

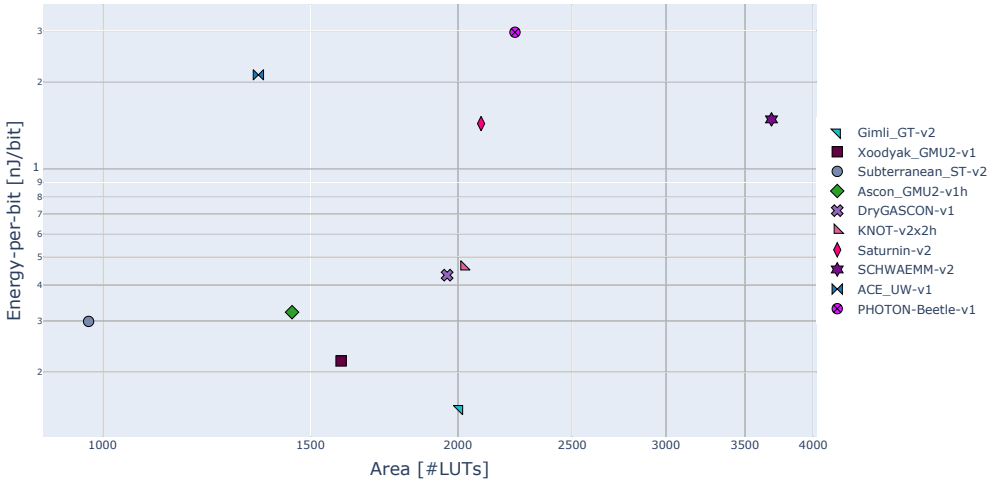

Figure 54: Energy-per-bit of hashing 1536-Byte messages at 75MHz vs. Area (LUTs)

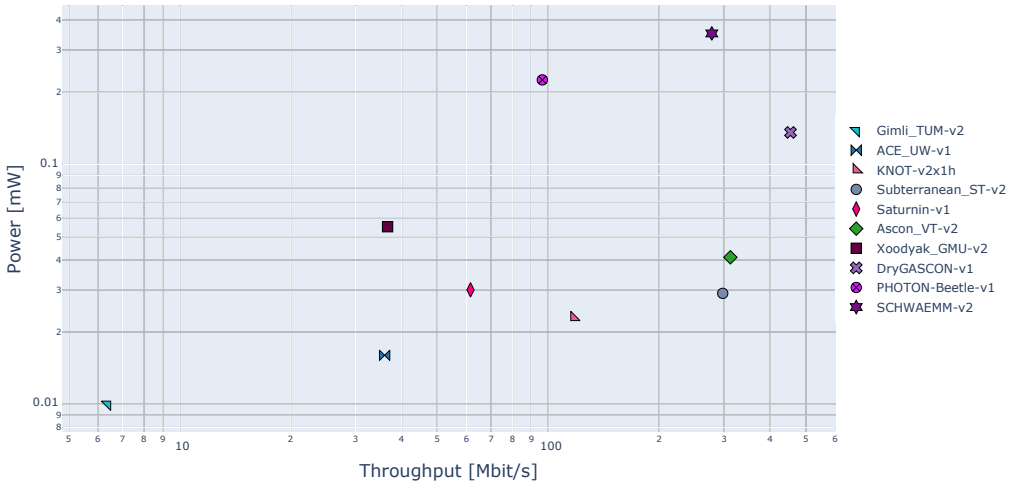

Figure 55: Power vs. Throughput for Hashing of 1536-Byte messages at 75MHz

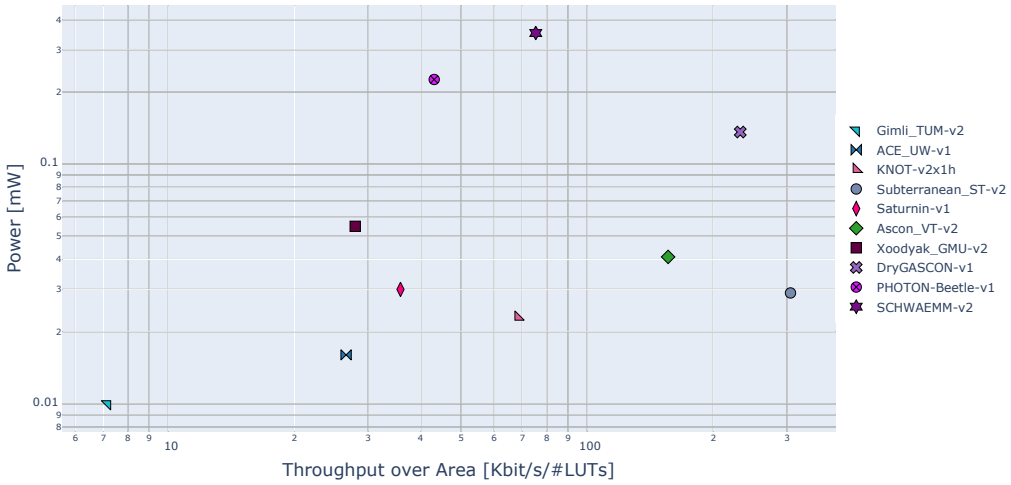

Figure 56: Power vs. Throughput-over-Area for Hashing of 1536-Byte messages at 75MHz

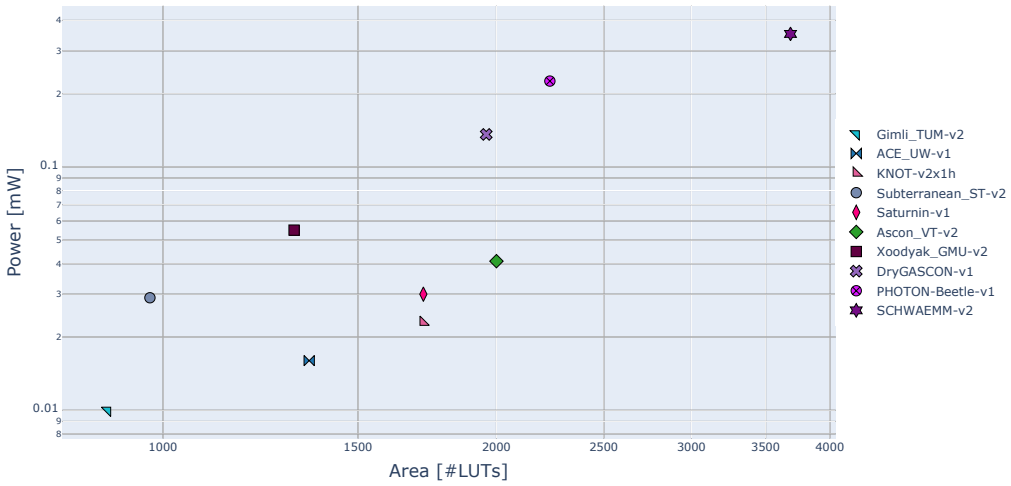

Figure 57: Power for Hashing of 1536-Byte messages at 75MHz vs. Area (LUTs)

Table 20: Estimated total power (mW) at 75MHz for encryption, decryption, and hashing on Xilinx Artix-7

Submission	Enc 1536,0	Enc 0,1536	Dec 1536,0	Enc 16,0	Enc 0,16	Dec 16,0	Hash 1536	Hash 16
ACE_UW-v1	77	76	77	76	76	76	76	76
ACE_GMU-v1	4,048	4,048	4,046	3,845	3,898	3,769	4,048	3,985
Ascon_GMU-v1	427	404	423	265	303	236		
Ascon_GMU-v2	128	116	127	107	109	100		
Ascon_GMU2-v1h	123	115	123	104	105	102	116	116
Ascon_GMU2-v2h	447	435	448	285	316	279	488	475
Ascon_GMU2-v3h	2,605	2,598	2,596	1,470	1,714	1,428	3,280	3,148
Ascon_Graz-v1	113	106	113	104	103	101		
Ascon_Graz-v2	121	114	121	112	113	109		
Ascon_Graz-v3	390	380	388	305	319	288	452	450
Ascon_Graz-v4	484	473	481	393	426	371	618	611
Ascon_Graz-v5	2,526	2,524	2,521	1,808	1,929	1,676	3,278	3,205
Ascon_Graz-v6	14,582	14,654	14,468	10,395	11,560	9,600	20,634	19,064
Ascon_VT-v1	100	94	100	101	98	98		
Ascon_VT-v2	104	95	104	102	99	98	101	103
COMET_VT-v1	149	162	149	147	150	142		
COMET_VT-v2	81	80	81	81	81	81		
DryGASCON-v1	203	200	206	177	176	162	196	181
Elephant-v1	76	75	76	76	75	76		
Elephant-v2	461	421	461	427	423	416		
Elephant-v3	257	236	257	242	237	237		
Elephant-v4	118	113	117	112	112	108		
Elephant-v5	392	379	388	349	352	302		
ForkAE-v2	123	130	126	105	109	109		
GIFT-COFB_GMU-v1	78	75	79	78	78	77		
GIFT-COFB_GMU-v2	99	93	100	96	94	91		
GIFT-COFB_GMU-v3	208	195	205	179	164	155		
GIFT-COFB_GMU-v4	340	324	337	280	250	232		
GIFT-COFB_VT-v1	77	75	77	76	76	76		
Gimli_GMU-v1	95	91	95	91	90	88	91	93
Gimli_GMU-v2	130	122	130	117	115	108	122	124
Gimli_GMU-v4	389	373	385	293	289	247	378	355
Gimli_GT-v1	97	92	97	89	88	92	92	89
Gimli_GT-v2	124	115	124	101	99	109	116	103
Gimli_GT-v3	289	275	285	181	179	215	279	190
Gimli_GT-v4	495	478	486	254	256	311	487	275
Gimli_TUM-v1	71	71	71	71	71	71	71	71
Gimli_TUM-v2	70	70	70	70	70	70	70	70
ISAP-v1	226	234	226	287	276	288		
KNOT-v2x1	93	86	93	85	83	84		
KNOT-v2x1h	91	85	91	84	83	83	83	83
KNOT-v2x2	131	116	130	105	104	104		
KNOT-v2x2h	132	114	131	106	105	105	108	105
KNOT-v2x4	428	629	423	444	467	419		
KNOT-v2x4h	419	674	409	453	475	430	637	533
LOCUS-v2	83	81	85	82	82	82		
LOTUS-v1	75	75	75	75	75	75		

Table 20 continued from previous page

Submission	Enc 1536,0	Enc 0,1536	Dec 1536,0	Enc 16,0	Enc 0,16	Dec 16,0	Hash 1536	Hash 16
LOTUS-v2	75	75	75	76	75	75		
mixFeed-v1	134	136	134	134	135	133		
PHOTON-Beetle-v1	242	267	242	216	220	208	285	239
Pyjamask-v1	73	72	73	72	72	72		
Pyjamask-v2	97	97	94	90	89	89		
Romulus-v1	99	96	99	95	94	94		
Romulus-v2	149	139	149	131	131	129		
Romulus-v3	143	133	143	124	124	122		
Romulus-v5	68	68	68	68	68	68		
Saturnin-v1	91	90	91	88	88	88	90	87
Saturnin-v2	784	764	787	551	476	590	801	425
SCHWAEMM-v1	338	394	338	377	387	368		
SCHWAEMM-v2	325	379	325	360	371	353	412	405
SKINNY-AEAD-v1	128	131	138	124	126	127		
SKINNY-AEAD-v2	128	130	136	124	126	127		
SPIX-v1	1,454	1,654	1,451	1,754	1,801	1,701		
SPIX-v2	68	68	68	68	68	68		
SPIX-v2x2	73	72	73	72	72	72		
SPIX-v2x4	95	94	96	96	95	95		
SpoC_IIT-v1	79	79	79	79	79	79		
SpoC_VT-v1	76	76	76	76	76	76		
Spook-v2-v2	348	343	348	383	382	378		
Subterranean_GMU-v1	111	88	111	91	88	87		
Subterranean_ST-v2	109	88	110	86	84	85	89	88
TinyJAMBU_GMU-v1	68	68	68	68	68	68		
TinyJAMBU_GMU-v2	66	66	66	66	66	66		
TinyJAMBU_GMU-v3	65	65	65	65	65	65		
TinyJAMBU_TJT-v1	64	64	64	64	64	64		
TinyJAMBU_TJT-v2	68	68	68	68	68	68		
TinyJAMBU_TJT-v3	106	105	107	100	98	99		
WAGE-v1	74	73	74	73	73	73		
Xoodyak_GMU-v1	169	148	168	170	168	165	169	162
Xoodyak_GMU-v2	117	115	117	116	116	116	115	114
Xoodyak_GMU2-v1	172	164	172	160	158	152	158	160
Xoodyak_GMU2-v2	1,011	669	1,001	795	792	722	990	919
Xoodyak_XT-v1	130	115	131	127	126	123		
Xoodyak_XT-v2	572	455	569	615	625	580		
Xoodyak_XT-v7	130	116	128	128	127	124	127	124
Xoodyak_XT-v8	583	464	584	625	635	592	641	549
Xoodyak_XT-v9	4,784	3,732	4,797	5,341	5,468	4,966	5,534	4,463

Table 21: Estimated energy-per-bit (pJ/bit) at 75MHz for encryption, decryption, and hashing on Xilinx Artix-7

Variant	Enc 1536,0	Enc 0,1536	Dec 1536,0	Enc 16,0	Enc 0,16	Dec 16,0	Hash 1536	Hash 16
ACE_UW-v1	2,152	2,135	2,152	8,361	9,382	8,369	2,112	7,197
ACE_GMU-v1	15,681	15,752	15,687	59,792	67,124	59,759	15,580	52,403
Ascon_GMU-v1	238	225	238	1,010	1,155	1,040		
Ascon_GMU-v2	126	115	126	586	631	607		
Ascon_GMU2-v1h	186	174	186	664	704	660	322	1,120
Ascon_GMU2-v2h	390	379	391	1,287	1,425	1,289	731	2,493
Ascon_GMU2-v3h	1,720	1,712	1,716	5,718	6,492	5,697	3,514	11,920
Ascon_Graz-v1	194	183	194	676	734	687		
Ascon_Graz-v2	157	149	158	681	782	696		
Ascon_Graz-v3	421	412	420	1,407	1,572	1,416	774	2,684
Ascon_Graz-v4	422	414	421	1,732	2,055	1,747	1,058	3,644
Ascon_Graz-v5	2,191	2,194	2,193	7,213	8,098	7,193	4,211	14,439
Ascon_Graz-v6	9,576	9,655	9,542	37,140	43,711	37,200	22,098	71,986
Ascon_VT-v1	213	201	213	657	719	677		
Ascon_VT-v2	200	203	200	652	726	667	324	1,120
COMET_VT-v1	301	260	302	879	834	892		
COMET_VT-v2	767	724	767	2,256	2,222	2,281		
DryGASCON-v1	453	446	461	1,069	1,063	1,120	432	619
Elephant-v1	1,101	580	1,101	2,758	3,409	2,781		
Elephant-v2	1,682	887	1,683	4,110	5,129	4,127		
Elephant-v3	1,111	580	1,112	2,733	3,367	2,746		
Elephant-v4	432	428	434	2,093	2,595	1,702		
Elephant-v5	754	770	775	3,614	4,488	2,871		
ForkAE-v2	1,585	1,444	1,965	2,051	1,857	2,445		
GIFT-COFB_GMU-v1	340	325	344	1,062	743	1,122		
GIFT-COFB_GMU-v2	223	208	225	710	508	765		
GIFT-COFB_GMU-v3	245	229	244	762	543	815		
GIFT-COFB_GMU-v4	329	312	330	1,014	724	1,073		
GIFT-COFB_VT-v1	386	388	386	1,183	842	1,206		
Gimli_GMU-v1	257	246	257	1,060	1,048	1,112	242	744
Gimli_GMU-v2	184	172	185	778	764	825	169	526
Gimli_GMU-v4	299	286	299	1,215	1,198	1,268	283	841
Gimli_GT-v1	254	240	254	1,188	1,175	1,290	237	836
Gimli_GT-v2	165	153	164	840	826	863	150	577
Gimli_GT-v3	259	246	254	1,209	1,196	1,347	243	834
Gimli_GT-v4	337	325	329	1,512	1,497	1,722	321	1,036
Gimli_TUM-v1	6,018	5,996	6,018	23,366	23,344	23,380	5,936	17,560
Gimli_TUM-v2	11,136	11,085	11,136	43,170	43,119	43,191	10,974	32,451
ISAP-v1	974	603	974	12,301	7,287	12,314		
KNOT-v2x1	194	181	194	1,101	1,309	1,114		
KNOT-v2x1h	189	179	190	1,088	1,309	1,101	707	2,199
KNOT-v2x2	138	123	137	770	904	794		
KNOT-v2x2h	139	121	138	777	912	802	461	1,469
KNOT-v2x4	407	340	404	2,007	2,403	2,021		
KNOT-v2x4h	399	365	390	2,048	2,444	2,074	1,365	4,128
LOCUS-v2	1,047	515	1,072	1,873	1,336	1,873		
LOTUS-v1	1,796	905	1,796	3,182	2,277	3,189		

Table 21 continued from previous page

Variant	Enc 1536,0	Enc 0,1536	Dec 1536,0	Enc 16,0	Enc 0,16	Dec 16,0	Hash 1536	Hash 16
LOTUS-v2	946	477	946	1,728	1,222	1,713		
mixFeed-v1	820	775	821	3,118	3,071	3,150		
PHOTON-Beetle-v1	845	792	846	1,738	1,701	1,759	2,960	1,622
Pyjamask-v1	2,070	2,012	2,154	9,294	9,321	9,388		
Pyjamask-v2	1,080	1,040	1,049	5,358	5,354	5,319		
Romulus-v1	627	334	628	1,393	1,384	1,386		
Romulus-v2	506	273	507	1,161	1,162	1,146		
Romulus-v3	274	161	274	739	736	728		
Romulus-v5	9,348	4,876	9,357	19,108	19,100	19,091		
Saturnin-v1	1,934	988	1,935	7,868	6,062	7,903	1,463	3,066
Saturnin-v2	2,348	1,201	2,360	10,237	7,504	11,195	1,435	2,935
SCHWAEMM-v1	858	816	859	4,925	4,854	4,918		
SCHWAEMM-v2	825	784	826	4,702	4,653	4,718	1,484	3,727
SKINNY-AEAD-v1	904	871	975	1,864	1,815	1,947		
SKINNY-AEAD-v2	904	864	961	1,851	1,802	1,934		
SPIX-v1	4,737	4,719	4,735	27,644	29,698	27,694		
SPIX-v2	1,406	1,413	1,406	8,460	9,111	8,495		
SPIX-v2x2	931	923	931	5,492	5,912	5,530		
SPIX-v2x4	835	830	844	4,963	5,287	4,961		
SpoC_IIT-v1	1,240	1,207	1,240	2,561	2,528	2,537		
SpoC_VT-v1	1,777	1,745	1,777	3,589	3,557	3,581		
Spook-v2-v2	904	891	904	5,410	5,396	5,404		
Subterranean_GMU-v1	51	40	51	374	362	375		
Subterranean_ST-v2	51	41	52	493	473	487	299	550
TinyJAMBU_GMU-v1	973	406	973	1,887	1,313	1,907		
TinyJAMBU_GMU-v2	1,832	732	1,833	3,481	2,375	3,501		
TinyJAMBU_GMU-v3	28,042	10,708	28,042	52,179	34,839	52,198		
TinyJAMBU_TJT-v1	3,474	1,341	3,474	6,734	4,574	6,734		
TinyJAMBU_TJT-v2	945	378	945	1,844	1,270	1,864		
TinyJAMBU_TJT-v3	358	136	362	764	534	785		
WAGE-v1	1,815	1,799	1,815	7,135	7,995	7,143		
Xoodyak_GMU-v1	233	144	232	1,247	1,232	3,840	304	664
Xoodyak_GMU-v2	2,221	1,260	2,221	12,656	12,656	12,691	3,137	6,357
Xoodyak_GMU2-v1	165	91	166	1,092	1,079	1,113	219	658
Xoodyak_GMU2-v2	534	330	534	3,689	3,675	3,708	740	2,154
Xoodyak_XT-v1	179	111	181	930	910	938		
Xoodyak_XT-v2	539	328	538	2,966	2,949	2,972		
Xoodyak_XT-v7	179	112	177	937	917	946	228	507
Xoodyak_XT-v8	549	334	552	3,014	2,996	3,034	746	1,558
Xoodyak_XT-v9	3,813	2,384	3,837	21,364	21,302	21,364	5,281	10,855

7 Conclusions and Future Work

For the processing of long plaintexts on Xilinx Artix-7 FPGAs, with a budget of 2520 LUTs or less, 12 candidates outperform the current standard AES-GCM. These candidates, in the order of Throughput, include Subterranean 2.0, Ascon, Xoodyak, Gimli, KNOT, GIFT-COFB, DryGASCON, COMET, Spook-v2, Elephant, TinyJAMBU, and Romulus. All these algorithms, as well as Saturnin, Elephant, and ISAP, outperform AES-GCM for the processing of long ADs while meeting the area limit. Out of them, only Gimli, Xoodyak, and Ascon support hashing faster than SHA-2. Two additional ones, DryGASCON and Saturnin, perform hashing faster than the folded implementation of SHA-3. For authenticated encryption, almost the same algorithms lead the ranking in terms of Energy per bit. Exceptions include Spook-v2 and Saturnin, which rank at positions higher than 12. For hashing, the order of algorithms remains almost the same, except of Subterranean 2.0 moving to position 3, ahead of Ascon, and KNOT moving ahead of Saturnin.

When the same designs are implemented using Intel Cyclone 10 LP, 13 candidates outperform AES-GCM for processing of plaintexts. These candidates are Subterranean v2.0, Ascon, Gimli, Xoodyak, KNOT, GIFT-COFB, Elephant, DryGASCON, TinyJAMBU, Spook-v2, Romulus, Saturnin, and PHOTON-Beetle. All of them also outperform AES-GCM for processing of AD. However, it should be noted that the implementation of AES-GCM uses 7711 LEs, about 54% more than the limit of 5000 LEs imposed on LWC candidates. Out of the mentioned above candidates, only Gimli and Xoodyak support hashing faster than SHA-2. Additionally, Ascon, Saturnin, DryGASCON, and Subterranean v2.0 perform hashing faster than the implementation of SHA-3 adhering to similar resource utilization constraints (taking 5417 LEs).

When all candidates are implemented using Lattice Semiconductor ECP5, 9 candidates perform faster than AES-GCM for processing of PT only. These candidates are Subterranean v2.0, Xoodyak, Gimli, Ascon, KNOT, GIFT-COFB, Elephant, DryGASCON, and TinyJAMBU. All of them perform faster also for the processing of AD. However, it should be noted that the implementation of AES-GCM uses 5507 LUTs, about 10% more than the limit of 5000 LUTs imposed on LWC candidates. For hashing, only Gimli and Xoodyak perform faster than SHA-2. Additionally, Ascon, Saturnin and DryGASCON perform faster than the folded implementation of SHA-3.

The reader should take into account that the number of algorithms outperforming AES-GCM depends on a particular implementation of the current NIST standard used in our study. Thus, this numbers may decrease in the future, if the better implementation of AES-GCM, compliant with the LWC Hardware API and meeting the resource utilization limit, is developed. However, concurrently, better implementations of LWC candidates may be developed as well.

In Round 3, the evaluation should focus on the ranking of implementations protected against side-channel attacks.

References

[1] J.-P. Kaps, W. Diehl, M. Tempelmeier, F. Farahmand, E. Homsirikamol, and K. Gaj, "A Comprehensive Framework for Fair and Efficient Benchmarking of Hardware Implementations of Lightweight Cryptography," Tech. Rep. 1273, 2019.

[2] J.-P. Kaps, W. Diehl, M. Tempelmeier, E. Homsirikamol, and K. Gaj, "Hardware API for Lightweight Cryptography," Oct. 2019.

[3] Cryptographic Engineering Research Group (CERG) at George Mason University, *Hardware Benchmarking of CAESAR Candidates*, https://cryptography.gmu.edu/athena/index.php?id=CAESAR, 2019.

[4] P. Yalla and J.-P. Kaps, "Evaluation of the CAESAR hardware API for lightweight implementations," in *2017 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Cancun: IEEE, Dec. 2017.

[5] P. Karl and M. Tempelmeier, "A Detailed Report on the Overhead of Hardware APIs for Lightweight Cryptography," Cryptology ePrint Archive 2020/112, Feb. 2020.

[6] B. Rezvani, F. Coleman, S. Sachin, and W. Diehl, "Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look," Cryptology ePrint Archive 2019/824, Feb. 2020.

[7] NIST, *Lightweight Cryptography: Project Overview*, https://csrc.nist.gov/projects/lightweight-cryptography, 2019.

[8] *CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness - web page*, 2019. [Online]. Available: https://competitions.cr.yp.to/caesar.html.

[9] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, M. U. Sharif, and K. Gaj, "A universal hardware API for authenticated ciphers," in *2015 International Conference on ReConFigurable Computing and FPGAs, ReConFig 2015*, Riviera Maya, Mexico, Dec. 2015.

[10] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, P. Yalla, J.-P. Kaps, and K. Gaj, "CAESAR Hardware API," Cryptology ePrint Archive 2016/626, 2016.

[11] ——, "Addendum to the CAESAR Hardware API v1.0," George Mason University, Fairfax, VA, GMU Report, Jun. 2016.

[12] E. Homsirikamol, P. Yalla, and F. Farahmand, *Development Package for Hardware Implementations Compliant with the CAESAR Hardware API*, 2016. [Online]. Available: https://cryptography.gmu.edu/athena/index.php?id=CAESAR.

[13] E. Homsirikamol, P. Yalla, F. Farahmand, W. Diehl, A. Ferozpuri, J.-P. Kaps, and K. Gaj, "Implementer's Guide to Hardware Implementations Compliant with the CAESAR Hardware API," GMU, Fairfax, VA, GMU Report, 2016.

[14] M. Tempelmeier, G. Sigl, and J.-P. Kaps, "Experimental Power and Performance Evaluation of CAESAR Hardware Finalists," in *2018 International Conference on ReConFigurable Computing and FPGAs, ReConFig 2018*, Cancun, Mexico, Dec. 2018, pp. 1–6.

[15] M. Tempelmeier, F. De Santis, G. Sigl, and J.-P. Kaps, "The CAESAR-API in the Real World — Towards a Fair Evaluation of Hardware CAESAR Candidates," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018*, Washington, DC, Apr. 2018, pp. 73–80.

[16] F. Farahmand, W. Diehl, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Improved Lightweight Implementations of CAESAR Authenticated Ciphers," Cryptology ePrint Archive 2018/573, Jun. 2018.

[17] W. Diehl, A. Abdulgadir, F. Farahmand, J.-P. Kaps, and K. Gaj, "Comparison of Cost of Protection Against Differential Power Analysis of Selected Authenticated Ciphers," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, DC, USA: IEEE, May 2018.

[18] W. Diehl, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Comparing the Cost of Protecting Selected Lightweight Block Ciphers against Differential Power Analysis in Low-Cost FPGAs," en, *Computers*, vol. 7, no. 2, p. 28, Apr. 2018.

[19] W. Diehl, A. Abdulgadir, F. Farahmand, J.-P. Kaps, and K. Gaj, "Comparison of Cost of Protection against Differential Power Analysis of Selected Authenticated Ciphers," *Cryptography*, vol. 2, no. 3, p. 26, Sep. 2018.

[20] W. Diehl, F. Farahmand, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Face-off Between the CAESAR Lightweight Finalists: ACORN vs. Ascon," Cryptology ePrint Archive 2019/184, Mar. 2019.

[21] T. Good and M. Benaissa, "Hardware performance of eStream phase-III stream cipher candidates," p. 11, 2008.

[22] S. Kerckhof, F. Durvaux, C. Hocquet, D. Bol, and F.-X. Standaert, "Towards Green Cryptography: A Comparison of Lightweight Ciphers from the Energy Viewpoint," in *Cryptographic Hardware and Embedded Systems – CHES 2012*, ser. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, 2012, pp. 390–407.

[23] B. Baldwin and W. P. Marnane, "Yet Another SHA-3 Round 3 FPGA Results Paper," p. 12,

[24] M. Knezevic, K. Kobayashi, J. Ikegami, S. Matsuo, A. Satoh, Ü. Kocabas, J. Fan, T. Katashita, T. Sugawara, K. Sakiyama, I. Verbauwhede, K. Ohta, N. Homma, and T. Aoki, "Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 5, pp. 827–840, May 2012.

[25] M. Tempelmeier, G. Sigl, and J. Kaps, "Experimental Power and Performance Evaluation of CAESAR Hardware Finalists," in *2018 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Dec. 2018, pp. 1–6.

[26] F. Farahmand, W. Diehl, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Improved Lightweight Implementations of CAESAR Authenticated Ciphers," in *2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines, FCCM 2018*, Boulder, CO, Apr. 2018, pp. 29–36.

[27] A. Caforio, F. Balli, and S. Banik, "Energy Analysis of Lightweight AEAD Circuits," Cryptology ePrint Archive 2020/607, Oct. 2020. [Online]. Available: https://eprint.iacr.org/2020/607.

[28] L. Henzen, P. Gendotti, P. Guillet, E. Pargaetzi, M. Zoller, and F. K. Gürkaynak, "Developing a Hardware Evaluation Method for SHA-3 Candidates," in *Cryptographic Hardware and Embedded Systems, CHES 2010*, ser. Lecture Notes in Computer Science, vol. 6225, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 248–263. DOI: 10.1007/978-3-642-15031-9_17.

[29] Cryptographic Engineering Research Group (CERG) at George Mason University, *Hardware Benchmarking of Lightweight Cryptography*, https://cryptography.gmu.edu/athena/index.php?id=LWC, 2019.

[30] F. Farahmand, W. Diehl, and K. Gaj, "Minerva: Automated hardware optimization tool," in *International Conference on ReConfigureable Computing and FPGAs (ReConfig)*, Cancun, Mexico, 2017, pp. 1–8.

[31] K. Gaj, J.-P. Kaps, V. Amirineni, M. Rogawski, E. Homsirikamol, and B. Y. Brewster, "ATHENa - Automated Tool for Hardware EvaluatioN: Toward Fair and Comprehensive Benchmarking of Cryptographic Hardware Using FPGAs," in *2010 International Conference on Field Programmable Logic and Applications, FPL 2010*, Milan, Italy: IEEE, Aug. 2010, pp. 414–421.

[32] K. Mohajerani and R. Nagpal, *Xeda: Cross-EDA Abstraction and Automation*, Dec. 9, 2020. [Online]. Available: https://github.com/XedaHQ/xeda.

[33] K. Mohajerani, *BlueLight: Bluespec implementations of Lightweight Cryptography Candidates*, Dec. 9, 2020. [Online]. Available: https://github.com/kammoh/bluelight.

[34] D. Bellizia, F. Berti, O. Bronchain, G. Cassiers, S. Duval, C. Guo, G. Leander, G. Leurent, C. Momin, O. Pereira, T. Peters, F.-X. Standaert, B. Udvarhelyi, and F. Wiemer, "Spook: Sponge-Based Leakage-Resistant Authenticated Encryption with a Masked Tweakable Block Cipher," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. S1, pp. 295–349, 2020.

[35] D. J. Bernstein and T. Lange, *eBACS: ECRYPT Benchmarking of Cryptographic Systems*, 2020. [Online]. Available: https://bench.cr.yp.to.

[36] Cryptographic Engineering Research Group (CERG) at George Mason University. (2019). "Hardware Benchmarking of CAESAR Candidates," [Online]. Available: https://cryptography.gmu.edu/athena/index.php?id=CAESAR.

[37] Xilinx, *[UG907] Vivado Design Suite User Guide: Power Analysis and Optimization*, 2020. [Online]. Available: https://www.xilinx.com/support/documentation/sw_manuals/xilinx2020_1/ug907-vivado-power-analysis-optimization.pdf.

[38] ——, (Aug. 5, 2013). "AR #55595: 2013.x Vivado Power Analysis - How do I generate SAIF for accurate Power Analysis?" Xilinx, [Online]. Available: https://www.xilinx.com/support/answers/55595.html (visited on 01/25/2021).

[39] CERG, *LWC Hardware API Development Package*, CERG, Dec. 16, 2020. [Online]. Available: https://github.com/GMUCERG/LWC (visited on 02/15/2021).

[40] A. K. Sultania, C. Zhang, D. K. Gandhi, and F. Zhang, "Power Analysis and Optimization," in *Designing with Xilinx® FPGAs: Using Vivado*, Cham: Springer International Publishing, 2017, pp. 177–187. DOI: 10.1007/978-3-319-42438-5_15.

[41] N. K. Dumpala, S. B. Patil, D. Holcomb, and R. Tessier, "Energy Efficient Loop Unrolling for Low-Cost FPGAs," in *2017 IEEE 25th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, Apr. 2017, pp. 117–120.

A Throughput and Area – Detailed Results

Table 22: Xilinx Artix-7 Resource Usage and Maximum Frequency

Variant	LUTs	FFs	Slices	Freq. [MHz]
ACE_UW-v1	1,229	894	400	200
ACE_GMU-v1	1,847	968	583	143
AESGCM-v1	3,270	1,498	1,008	211
AESGCM-v2	2,520	1,611	810	211
Ascon_GMU-v1	2,410	974	670	246
Ascon_GMU-v2	1,790	974	513	307
Ascon_GMU2-v1h	1,375	862	436	276
Ascon_GMU2-v2h	2,126	861	632	234
Ascon_GMU2-v3h	2,493	860	689	142
Ascon_Graz-v1	1,465	666	396	191
Ascon_Graz-v2	1,541	668	431	213
Ascon_Graz-v3	2,142	665	582	201
Ascon_Graz-v4	2,249	669	620	206
Ascon_Graz-v5	2,797	666	785	150
Ascon_VT-v1	1,913	539	518	233
Ascon_VT-v2	1,928	544	515	219

Table 22 continued from previous page

Variant	LUTs	FFs	Slices	Freq. [MHz]
COMET_CI-v1	1,884	1,543	639	223
COMET_CI-v2	1,096	1,034	372	222
COMET_CI-v3	1,841	1,453	553	215
COMET_VT-v1	2,449	947	695	209
COMET_VT-v2	1,703	736	504	234
DryGASCON-v1	2,074	1,220	596	238
Elephant-v1	1,291	910	379	229
Elephant-v2	1,884	900	541	181
Elephant-v3	1,717	982	501	200
Elephant-v4	1,901	1,501	567	263
Elephant-v5	2,645	1,502	759	217
ESTATE-v1	1,351	733	428	222
ESTATE-v2	907	416	269	268
ESTATE-v3	1,130	846	347	259
ESTATE-v4	944	557	292	277
ForkAE-v1	1,191	808	361	208
ForkAE-v2	2,466	1,343	720	228
GIFT-COFB_GMU-v1	1,223	887	379	263
GIFT-COFB_GMU-v2	1,380	880	417	261
GIFT-COFB_GMU-v3	1,641	882	499	249
GIFT-COFB_GMU-v4	1,730	873	539	213
GIFT-COFB_GMU-v5	2,051	873	655	137
GIFT-COFB_GMU-v6	2,363	872	696	110
GIFT-COFB_VT-v1	1,041	604	321	275
Gimli_GMU-v1	1,435	934	437	255
Gimli_GMU-v2	1,678	935	504	260
Gimli_GMU-v4	2,357	932	752	242
Gimli_GT-v1	1,747	1,169	502	175
Gimli_GT-v2	1,909	1,164	528	175
Gimli_GT-v3	2,678	1,163	752	131
Gimli_GT-v4	2,510	1,161	717	142
Gimli_GT-v5	3,907	1,162	1,057	97
Gimli_GT-v6	3,937	1,160	1,075	91
Gimli_GT-v7	5,347	1,161	1,418	66
Gimli_TUM-v1	933	261	269	241
Gimli_TUM-v2	905	245	266	244
Gimli_TUM-v3	838	249	252	253
ISAP-v1	3,491	1,177	937	193
ISAP-v2	2,157	1,005	618	200
ISAP-v3	2,182	1,172	655	188
KNOT-v2x1	1,620	853	474	251
KNOT-v2x1h	1,684	857	504	236
KNOT-v2x2	1,873	855	525	233
KNOT-v2x2h	2,112	858	584	222
KNOT-v2x4	2,797	856	740	165
KNOT-v2x4h	2,438	859	675	137
LOCUS-v1	1,824	1,037	613	216
LOCUS-v2	1,628	789	492	209
LOTUS-v1	1,652	916	469	145

Table 22 continued from previous page

Variant	LUTs	FFs	Slices	Freq. [MHz]
LOTUS-v2	1,487	788	462	141
mixFeed-v1	1,343	230	406	151
Oribatida-v1	1,450	1,319	466	276
Oribatida-v2	1,450	1,319	466	276
PHOTON-Beetle-v1	2,065	729	620	178
Pyjamask-v1	1,979	1,306	592	229
Pyjamask-v2	2,308	1,415	780	213
Romulus-v1	953	501	271	229
Romulus-v2	1,280	501	344	214
Romulus-v3	1,824	504	507	123
Romulus-v4	2,602	503	702	58
Romulus-v5	887	422	246	214
Saturnin-v1	1,725	1,329	518	215
Saturnin-v2	2,321	768	622	167
SCHWAEMM-v1	3,071	1,396	872	135
SCHWAEMM-v2	3,740	1,541	1,004	130
SHA2-v1	1,051	937	345	201
SHA3-v1	1,263	277	351	195
SKINNY-AEAD-v1	2,333	1,659	776	240
SKINNY-AEAD-v2	2,337	1,627	711	240
SPIX-v1	1,533	756	440	156
SPIX-v2	1,181	894	397	182
SPIX-v2x2	1,267	1,004	416	187
SPIX-v2x4	1,332	890	411	176
SpoC_IIT-v1	1,512	919	448	235
SpoC_VT-v1	1,079	805	348	230
Spook-v2-v2	2,033	1,517	597	206
Subterranean_ST-v2	891	610	253	190
Subterranean_GMU-v1	848	578	266	298
TinyJAMBU_GMU-v1	591	428	212	266
TinyJAMBU_GMU-v2	564	430	197	268
TinyJAMBU_GMU-v3	537	433	191	278
TinyJAMBU_TJT-v1	446	209	136	290
TinyJAMBU_TJT-v2	461	325	142	315
TinyJAMBU_TJT-v3	576	432	215	240
WAGE-v1	1,150	760	332	279
Xoodyak_GMU-v1	1,808	851	495	170
Xoodyak_GMU-v2	1,234	98	323	168
Xoodyak_GMU2-v1	1,608	1,249	513	314
Xoodyak_GMU2-v2	2,322	1,228	692	199
Xoodyak_XT-v1	1,355	555	407	234
Xoodyak_XT-v2	2,025	557	579	188
Xoodyak_XT-v7	1,392	559	402	226
Xoodyak_XT-v8	2,143	559	618	181
Minimum	**446**	**98**	**136**	**58.0**
Average	**1,798**	**880**	**528**	**209.7**
Maximum	**5,347**	**1,659**	**1,418**	**315.0**

Table 23: Intel Cyclone 10 LP Resource Usage and Maximum Frequency

Variant	LEs	$\frac{\text{LEs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
ACE_UW-v1	1,903	1.55	918	1.03	106.5	1.88
ACE_GMU-v1	4,473	2.42	1,025	1.06	77.0	1.86
AESGCM-v1	8,754	2.68	1,585	1.06	121.0	1.74
AESGCM-v2	7,711	3.06	1,699	1.05	118.7	1.78
Ascon_GMU-v1	4,552	1.89	981	1.01	118.4	2.08
Ascon_GMU-v2	3,113	1.74	982	1.01	160.6	1.91
Ascon_GMU2-v1h	2,415	1.76	867	1.01	175.6	1.57
Ascon_GMU2-v2h	3,215	1.51	865	1.00	134.8	1.74
Ascon_GMU2-v3h	4,161	1.67	867	1.01	91.7	1.55
Ascon_Graz-v1	2,517	1.72	775	1.16	141.4	1.35
Ascon_Graz-v2	2,634	1.71	775	1.16	143.3	1.49
Ascon_Graz-v3	3,716	1.74	774	1.16	109.7	1.83
Ascon_Graz-v4	3,730	1.66	774	1.16	108.7	1.90
Ascon_Graz-v5	4,905	1.75	775	1.16	80.1	1.87
Ascon_VT-v1	2,432	1.27	634	1.18	176.6	1.32
Ascon_VT-v2	2,695	1.40	640	1.18	172.0	1.27
COMET_CI-v1	4,663	2.48	1,885	1.22	115.8	1.93
COMET_CI-v2	2,629	2.40	1,632	1.58	132.9	1.67
COMET_CI-v3	4,379	2.38	1,768	1.22	114.8	1.87
COMET_VT-v1	10,200	4.17	955	1.01	88.9	2.35
COMET_VT-v2	5,204	3.06	826	1.12	110.6	2.12
DryGASCON-v1	3,199	1.54	1,310	1.07	130.5	1.82
Elephant-v1	2,056	1.59	1,005	1.10	163.1	1.40
Elephant-v2	2,729	1.45	998	1.11	113.2	1.60
Elephant-v3	2,504	1.46	996	1.01	123.2	1.62
Elephant-v4	3,050	1.60	1,485	0.99	157.6	1.67
Elephant-v5	3,926	1.48	1,507	1.00	126.9	1.71
ESTATE-v1	3,839	2.84	1,401	1.91	118.0	1.88
ESTATE-v2	1,946	2.15	1,026	2.47	174.3	1.54
ESTATE-v3	2,279	2.02	1,442	1.70	180.2	1.44
ESTATE-v4	1,572	1.67	1,098	1.97	200.1	1.38
ForkAE-v1	2,129	1.79	1,194	1.48	135.7	1.53
ForkAE-v2	3,200	1.30	1,415	1.05	148.1	1.54
GIFT-COFB_GMU-v1	1,903	1.56	884	1.00	159.8	1.65
GIFT-COFB_GMU-v2	2,111	1.53	883	1.00	156.5	1.67
GIFT-COFB_GMU-v3	2,523	1.54	882	1.00	131.8	1.89
GIFT-COFB_GMU-v4	2,609	1.51	879	1.01	110.8	1.92
GIFT-COFB_GMU-v5	4,828	2.35	881	1.01	51.5	2.66
GIFT-COFB_GMU-v6	6,630	2.81	880	1.01	37.2	2.96
GIFT-COFB_VT-v1	1,877	1.80	774	1.28	184.4	1.49
Gimli_GMU-v1	1,908	1.33	945	1.01	154.5	1.65
Gimli_GMU-v2	2,158	1.29	942	1.01	153.9	1.69
Gimli_GMU-v4	2,953	1.25	943	1.01	153.4	1.58
Gimli_GMU-v5	5,576		944		82.4	

Table 23 continued from previous page

Variant	LEs	$\frac{\text{LEs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
Gimli_GT-v1	2,378	1.36	1,156	0.99	142.8	1.23
Gimli_GT-v2	3,145	1.65	1,155	0.99	114.8	1.52
Gimli_GT-v3	3,651	1.36	1,156	0.99	85.8	1.53
Gimli_GT-v4	5,010	2.00	1,154	0.99	88.2	1.61
Gimli_GT-v5	5,948	1.52	1,155	0.99	58.6	1.66
Gimli_GT-v6	4,820	1.22	1,153	0.99	45.2	2.01
Gimli_GT-v7	6,379	1.19	1,154	0.99	32.3	2.05
Gimli_TUM-v1	2,044	2.19	1,130	4.33	101.3	2.38
Gimli_TUM-v2	2,074	2.29	1,136	4.64	97.3	2.51
Gimli_TUM-v3	2,115	2.52	1,143	4.59	100.5	2.52
ISAP-v1	4,589	1.31	1,268	1.08	126.6	1.52
ISAP-v2	3,852	1.79	1,108	1.10	136.4	1.47
ISAP-v3	3,767	1.73	1,268	1.08	131.9	1.43
ISAP-v4	3,026		1,119		155.0	
KNOT-v2x1	2,059	1.27	957	1.12	161.7	1.55
KNOT-v2x1h	2,532	1.50	963	1.12	159.4	1.48
KNOT-v2x2	2,472	1.32	958	1.12	138.7	1.68
KNOT-v2x2h	2,792	1.32	964	1.12	140.1	1.58
KNOT-v2x4	3,519	1.26	960	1.12	102.0	1.62
KNOT-v2x4h	3,678	1.51	966	1.12	101.5	1.35
LOCUS-v1	2,978	1.63	1,045	1.01	125.8	1.72
LOCUS-v2	2,828	1.74	804	1.02	132.4	1.58
LOTUS-v1	2,642	1.60	1,010	1.10	103.5	1.40
LOTUS-v2	2,445	1.64	895	1.14	99.6	1.42
mixFeed-v1	5,363	3.99	1,659	7.21	73.2	2.06
Oribatida-v1	2,512	1.73	1,331	1.01	185.7	1.49
Oribatida-v2	2,221	1.53	1,202	0.91	174.5	1.58
PHOTON-Beetle-v1	3,602	1.74	836	1.15	125.4	1.42
Pyjamask-v1	8,599	4.34	6,236	4.78	109.7	2.09
Pyjamask-v2	8,692	3.77	6,092	4.30	90.6	2.35
Romulus-v1	1,735	1.82	500	1.00	143.2	1.60
Romulus-v2	2,086	1.63	500	1.00	141.7	1.51
Romulus-v3	2,407	1.32	500	0.99	79.3	1.55
Romulus-v4	3,409	1.31	500	0.99	40.4	1.44
Romulus-v5	1,960	2.21	507	1.20	130.2	1.64
Saturnin-v1	3,802	2.20	2,155	1.62	145.0	1.48
Saturnin-v2	3,892	1.68	1,641	2.14	104.6	1.60
SCHWAEMM-v1	4,713	1.53	1,489	1.07	81.8	1.65
SCHWAEMM-v2	5,773	1.54	1,624	1.05	85.7	1.52
SHA2-v1	2,139	2.04	1,191	1.27	118.6	1.69
SHA3-v1	5,417	4.29	3,444	12.43	84.5	2.31
SKINNY-AEAD-v1	3,672	1.57	1,677	1.01	144.6	1.66
SKINNY-AEAD-v2	3,532	1.51	1,645	1.01	139.5	1.72
SPIX-v1	3,525	2.30	867	1.15	82.1	1.90
SPIX-v2	1,864	1.58	1,001	1.12	130.6	1.39

Table 23 continued from previous page

Variant	LEs	$\frac{\text{LEs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
SPIX-v2x2	1,993	1.57	1,000	1.00	134.7	1.39
SPIX-v2x4	2,310	1.73	999	1.12	132.6	1.33
SpoC_IIT-v1	2,250	1.49	996	1.08	182.2	1.29
SpoC_VT-v1	1,696	1.57	820	1.02	167.7	1.37
Spook-v2-v2	3,188	1.57	1,485	0.98	108.5	1.90
Subterranean_ST-v2	1,285	1.44	601	0.98	153.7	1.24
Subterranean_GMU-v1	1,264	1.49	586	1.01	174.5	1.71
TinyJAMBU_GMU-v1	856	1.45	447	1.04	196.8	1.35
TinyJAMBU_GMU-v2	841	1.49	448	1.04	196.2	1.37
TinyJAMBU_GMU-v3	817	1.52	452	1.04	191.1	1.46
TinyJAMBU_TJT-v1	686	1.54	429	2.05	200.8	1.44
TinyJAMBU_TJT-v2	777	1.69	435	1.34	196.2	1.60
TinyJAMBU_TJT-v3	1,021	1.77	432	1.00	159.7	1.50
WAGE-v1	1,774	1.54	846	1.11	159.6	1.75
Xoodyak_GMU-v1	3,135	1.73	947	1.11	106.8	1.59
Xoodyak_GMU-v2	5,871	4.76	2,237	22.83	77.0	2.18
Xoodyak_GMU2-v1	2,575	1.60	1,256	1.01	170.3	1.84
Xoodyak_GMU2-v2	5,058	2.18	1,237	1.01	97.2	2.05
Xoodyak_XT-v1	2,231	1.65	573	1.03	136.3	1.72
Xoodyak_XT-v2	3,541	1.75	573	1.03	88.8	2.12
Xoodyak_XT-v7	2,272	1.63	583	1.04	128.5	1.76
Xoodyak_XT-v8	3,630	1.69	583	1.04	90.0	2.01
Minimum	**686**	**1.19**	**429**	**0.91**	**32.3**	**1.23**
Average	**3,317**	**1.86**	**1,145**	**1.65**	**126.9**	**1.70**
Maximum	**10,200**	**4.76**	**6,236**	**22.83**	**200.8**	**2.96**

Table 24: Lattice ECP5 Resource Usage and Maximum Frequency

Variant	LUTs	$\frac{\text{LUTs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Slices	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
ACE_UW-v1	2,156	1.75	923	1.03	1,379	73.8	2.71
ACE_GMU-v1	2,784	1.51	944	0.97	1,605	74.2	1.93
AESGCM-v1	6,740	2.06	1,403	0.94	3,903	108.2	1.95
AESGCM-v2	5,507	2.19	1,512	0.94	3,226	106.7	1.98
Ascon_GMU-v1	5,909	2.45	1,173	1.20	3,303	84.3	2.92
Ascon_GMU-v2	4,641	2.59	974	1.00	2,605	117.2	2.62
Ascon_GMU2-v1h	2,928	2.13	864	1.00	1,700	110.1	2.51
Ascon_GMU2-v2h	3,764	1.77	862	1.00	2,130	89.2	2.62
Ascon_GMU2-v3h	4,925	1.98	862	1.00	2,811	61.2	2.32
Ascon_Graz-v1	2,544	1.74	676	1.01	1,538	59.3	3.22
Ascon_Graz-v2	2,603	1.69	674	1.01	1,600	64.0	3.33
Ascon_Graz-v3	3,305	1.54	674	1.01	1,897	63.7	3.16
Ascon_Graz-v4	3,379	1.50	675	1.01	1,981	61.9	3.33
Ascon_Graz-v5	4,646	1.66	876	1.31	2,694	55.6	2.70
Ascon_Graz-v6	5,346		675		2,937	38.8	
Ascon_VT-v1	3,130	1.64	550	1.02	1,673	84.9	2.74
Ascon_VT-v2	3,041	1.58	557	1.02	1,757	75.4	2.90
COMET_CI-v1	3,255	1.73	1,798	1.17	2,175	80.9	2.76
COMET_CI-v2	1,974	1.80	1,607	1.55	1,662	94.3	2.35
COMET_CI-v3	3,443	1.87	1,677	1.15	2,198	80.0	2.69
COMET_VT-v1	5,266	2.15	877	0.93	3,001	98.4	2.12
COMET_VT-v2	2,353	1.38	748	1.02	1,449	111.5	2.10
DryGASCON-v1	3,801	1.83	1,223	1.00	2,223	100.5	2.37
Elephant-v1	2,368	1.83	923	1.01	1,464	97.5	2.35
Elephant-v2	3,073	1.63	916	1.02	1,823	85.5	2.12
Elephant-v3	2,901	1.69	915	0.93	1,874	88.3	2.26
Elephant-v4	3,157	1.66	1,421	0.95	1,855	97.6	2.69
Elephant-v5	4,145	1.57	1,422	0.95	2,389	90.1	2.41
ESTATE-v1	2,855	2.11	1,017	1.39	1,895	109.0	2.04
ESTATE-v2	1,689	1.86	762	1.83	1,135	115.4	2.32
ESTATE-v3	1,820	1.61	1,137	1.34	1,349	107.1	2.42
ESTATE-v4	1,329	1.41	832	1.49	911	118.1	2.35
ForkAE-v1	2,022	1.70	1,024	1.27	1,357	67.9	3.06
ForkAE-v2	3,571	1.45	1,371	1.02	2,184	90.0	2.53
GIFT-COFB_GMU-v1	2,727	2.23	884	1.00	1,560	106.5	2.47
GIFT-COFB_GMU-v2	2,628	1.90	877	1.00	1,579	105.0	2.49
GIFT-COFB_GMU-v3	3,059	1.86	876	0.99	1,781	74.7	3.33
GIFT-COFB_GMU-v4	3,311	1.91	873	1.00	1,915	57.1	3.73
GIFT-COFB_GMU-v5	3,821	1.86	873	1.00	2,124	36.5	3.76
GIFT-COFB_VT-v1	2,214	2.13	689	1.14	1,248	114.3	2.41
Gimli_GMU-v1	2,328	1.62	934	1.00	1,436	102.0	2.50
Gimli_GMU-v2	2,617	1.56	933	1.00	1,649	103.0	2.52
Gimli_GMU-v4	3,223	1.37	932	1.00	1,816	94.9	2.55
Gimli_GMU-v5	4,586		934		2,507	52.5	

Table 24 continued from previous page

Variant	LUTs	$\frac{\text{LUTs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Slices	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
Gimli_GT-v1	2,537	1.45	1,165	1.00	1,570	78.2	2.24
Gimli_GT-v2	2,852	1.49	1,166	1.00	1,631	76.2	2.30
Gimli_GT-v3	4,451	1.66	1,170	1.01	2,479	55.6	2.35
Gimli_GT-v4	4,027	1.60	1,168	1.01	2,231	60.7	2.34
Gimli_GT-v5	5,738	1.47	1,127	0.97	3,214	23.3	4.16
Gimli_GT-v6	6,341	1.61	1,126	0.97	3,466	31.5	2.89
Gimli_GT-v7	8,238	1.54	1,126	0.97	4,418	16.4	4.01
Gimli_TUM-v1	1,767	1.89	260	1.00	1,072	78.0	3.09
Gimli_TUM-v2	1,767	1.95	263	1.07	1,040	73.5	3.32
Gimli_TUM-v3	1,772	2.12	272	1.09	1,064	78.5	3.22
ISAP-v1	6,701	1.92	1,185	1.01	4,164	61.1	3.16
ISAP-v2	5,708	2.65	1,028	1.02	3,475	68.0	2.94
ISAP-v3	5,703	2.61	1,377	1.18	3,636	65.6	2.86
ISAP-v4	3,623		1,350		2,314	67.2	
KNOT-v2x1	2,275	1.40	864	1.01	1,329	85.5	2.94
KNOT-v2x1h	2,446	1.45	872	1.02	1,445	78.9	2.99
KNOT-v2x2	3,287	1.75	870	1.02	1,809	90.4	2.58
KNOT-v2x2h	3,373	1.60	877	1.02	1,866	75.3	2.95
KNOT-v2x4	3,984	1.42	872	1.02	2,144	63.2	2.61
KNOT-v2x4h	4,283	1.76	879	1.02	2,342	60.9	2.25
LOCUS-v1	2,857	1.57	882	0.85	1,691	73.0	2.96
LOCUS-v2	2,950	1.81	759	0.96	1,757	72.5	2.88
LOTUS-v1	2,413	1.46	935	1.02	1,400	54.6	2.66
LOTUS-v2	2,208	1.49	807	1.02	1,324	52.7	2.68
mixFeed-v1	3,479	2.59	517	2.25	1,833	38.9	3.88
Oribatida-v1	1,671	1.15	987	0.75	1,128	176.5	1.56
Oribatida-v2	2,497	1.72	1,117	0.85	1,563	114.2	2.42
PHOTON-Beetle-v1	3,294	1.59	753	1.03	1,938	101.4	1.75
Pyjamask-v1	3,897	1.97	1,937	1.48	2,593	92.7	2.47
Pyjamask-v2	4,162	1.80	1,791	1.27	2,794	73.2	2.91
Romulus-v1	1,998	2.10	508	1.01	1,198	80.5	2.84
Romulus-v2	2,353	1.84	508	1.01	1,353	82.0	2.61
Romulus-v3	3,847	2.11	569	1.13	2,092	45.0	2.73
Romulus-v4	5,086	1.96	571	1.14	2,710	21.6	2.69
Romulus-v5	1,961	2.21	395	0.94	1,131	76.5	2.80
Saturnin-v1	3,070	1.78	1,589	1.20	1,929	92.6	2.32
Saturnin-v2	3,648	1.57	1,074	1.40	2,241	79.0	2.11
SCHWAEMM-v1	4,685	1.53	1,408	1.01	2,933	66.3	2.04
SCHWAEMM-v2	5,947	1.59	1,546	1.00	3,839	63.8	2.04
SHA2-v1	2,001	1.90	844	0.90	1,142	117.7	1.71
SHA3-v1	1,804	1.43	249	0.90	1,008	90.3	2.16
SKINNY-AEAD-v1	3,174	1.36	1,601	0.96	1,967	101.1	2.37
SKINNY-AEAD-v2	3,182	1.36	1,569	0.96	1,956	98.4	2.44
SPIX-v1	2,432	1.59	684	0.91	1,366	69.3	2.25
SPIX-v2	2,078	1.76	822	0.92	1,325	89.2	2.04

Table 24 continued from previous page

Variant	LUTs	$\frac{\text{LUTs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Slices	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
SPIX-v2x2	2,107	1.66	820	0.82	1,317	80.2	2.33
SPIX-v2x4	2,265	1.70	818	0.92	1,360	86.7	2.03
SpoC_IIT-v1	2,153	1.42	1,048	1.14	1,399	132.2	1.78
SpoC_VT-v1	2,049	1.90	740	0.92	1,314	98.2	2.34
Spook-v2-v2	3,662	1.80	1,494	0.98	2,258	77.0	2.67
Subterranean_ST-v2	1,342	1.51	613	1.00	828	95.7	1.99
Subterranean_GMU-v1	1,471	1.74	577	1.00	874	120.0	2.48
TinyJAMBU_GMU-v1	720	1.22	397	0.93	456	124.8	2.13
TinyJAMBU_GMU-v2	908	1.61	355	0.83	550	128.3	2.09
TinyJAMBU_GMU-v3	1,277	2.38	352	0.81	807	108.1	2.57
TinyJAMBU_TJT-v1	580	1.30	397	1.90	451	111.3	2.61
TinyJAMBU_TJT-v2	689	1.50	351	1.08	488	125.4	2.51
TinyJAMBU_TJT-v3	1,092	1.90	348	0.81	661	115.4	2.08
WAGE-v1	2,081	1.81	825	1.09	1,287	101.6	2.75
Xoodyak_GMU-v1	3,172	1.75	878	1.03	1,990	74.0	2.30
Xoodyak_GMU-v2	2,316	1.88	114	1.16	1,286	74.8	2.25
Xoodyak_GMU2-v1	3,248	2.02	1,261	1.01	1,834	150.5	2.09
Xoodyak_GMU2-v2	4,058	1.75	1,233	1.00	2,351	69.7	2.86
Xoodyak_XT-v1	2,402	1.77	489	0.88	1,521	95.7	2.44
Xoodyak_XT-v2	4,077	2.01	489	0.88	2,095	70.3	2.67
Xoodyak_XT-v7	2,489	1.79	499	0.89	1,536	88.4	2.56
Xoodyak_XT-v8	4,121	1.92	499	0.89	2,125	71.3	2.54
MINIMUM	**580**	**1.15**	**114**	**0.75**	**451**	**16.4**	**1.56**
AVERAGE	**3,178**	**1.76**	**913**	**1.05**	**1,883**	**83.9**	**2.58**
MAXIMUM	**8,238**	**2.65**	**1,937**	**2.25**	**4,418**	**176.5**	**4.16**

Table 25: Xilinx Artix-7 Encryption PT Throughput for Long Messages

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	9,536.0	1	848	298	1
Ascon_GMU-v1	6,297.6	2	2,410	246	5
Subterranean_ST-v2	6,080.0		891	190	0.25
Xoodyak_GMU2-v2	5,458.3	3	2,322	199	7
Xoodyak_GMU2-v1	4,637.5		1,608	314	13
Gimli_GMU-v4	4,425.1	4	2,357	242	7
Ascon_GMU-v2	4,366.2		1,790	307	9
Ascon_GMU2-v2h	3,744.0		2,126	234	4
Ascon_Graz-v4	3,296.0		2,249	206	8
KNOT-v2x2	3,195.4	5	1,873	233	14
Gimli_GT-v5	3,104.0		**3,907**	97	4
KNOT-v2x2h	3,044.6		2,112	222	14
Ascon_GMU2-v3h	3,029.3		2,493	142	3
Gimli_GT-v4	3,029.3		2,510	142	6
GIFT-COFB_GMU-v4	3,029.3	6	1,730	213	9
GIFT-COFB_GMU-v5	2,922.7		2,051	137	6
Gimli_GT-v6	2,912.0		**3,937**	91	4
GIFT-COFB_GMU-v3	2,897.5		1,641	249	11
GIFT-COFB_GMU-v6	2,816.0		2,363	110	5
Xoodyak_XT-v2	2,776.6		2,025	188	13
Xoodyak_XT-v8	2,673.2		2,143	181	13
Ascon_Graz-v3	2,572.8		2,142	201	5
Gimli_GMU-v2	2,560.0		1,678	260	13
Ascon_GMU2-v1h	2,523.4		1,375	276	7
AESGCM-v1	2,455.3		**3,270**	211	11
KNOT-v2x4	2,436.9		**2,797**	165	13
Ascon_Graz-v5	2,400.0		**2,797**	150	4
Xoodyak_XT-v1	2,364.6		1,355	234	19
Xoodyak_XT-v7	2,283.8		1,392	226	19
Ascon_Graz-v2	2,272.0		1,541	213	12
Gimli_GT-v7	2,112.0		**5,347**	66	4
Gimli_GT-v3	2,096.0		**2,678**	131	8
KNOT-v2x4h	2,023.4		2,438	137	13
Gimli_GT-v2	1,866.7		1,909	175	12
KNOT-v2x1	1,721.1		1,620	251	28
Xoodyak_GMU-v1	1,717.9		1,808	170	19
KNOT-v2x1h	1,618.3		1,684	236	28
GIFT-COFB_GMU-v2	1,590.9		1,380	261	21
Elephant-v5	1,578.2		**2,645**	217	22
Ascon_VT-v2	1,557.3		1,928	219	9
Ascon_Graz-v1	1,528.0		1,465	191	8
Ascon_VT-v1	1,491.2		1,913	233	10
DryGASCON-v1	1,450.7	7	2,074	238	21
COMET_VT-v1	1,337.6	8	2,449	209	20
Gimli_GMU-v1	1,305.6		1,435	255	25
Spook-v2-v2	1,098.7	9	2,033	206	48
Elephant-v4	1,001.9	10	1,901	263	42

Table 25 continued from previous page

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
TinyJAMBU_TJT-v3	960.0	11	576	240	8
Gimli_GT-v1	933.3		1,747	175	24
Romulus-v3	874.7	12	1,824	123	18
Romulus-v2	856.0		1,280	214	32
GIFT-COFB_GMU-v1	821.1		1,223	263	41
AESGCM-v2	818.4	13	2,520	211	33
Saturnin-v2	791.7	14	2,321	167	54
GIFT-COFB_VT-v1	748.9		1,041	275	47
SCHWAEMM-v1	735.3	15*	**3,071**	135	47
SCHWAEMM-v2	708.1		**3,740**	130	47
PHOTON-Beetle-v1	690.4	16	2,065	178	33
Romulus-v4	674.9		**2,602**	58	11
Elephant-v2	673.5		1,884	181	43
SPIX-v1	665.6	17	1,533	156	15
ISAP-v1	661.7		**3,491**	193	42
ISAP-v3	644.6	18	2,182	188	42
Elephant-v3	627.5		1,717	200	51
ACE_GMU-v1	508.4	19	1,847	143	18
ISAP-v2	492.3		2,157	200	26
Romulus-v1	488.5		953	229	60
SKINNY-AEAD-v2	458.5		2,337	240	67
SKINNY-AEAD-v1	458.5	20	2,333	240	67
COMET_CI-v3	417.0		1,841	215	66
COMET_CI-v1	407.8		1,884	223	70
mixFeed-v1	339.1	21	1,343	151	57
COMET_VT-v2	336.5		1,703	234	89
ESTATE-v1	322.9	22	1,351	222	88
TinyJAMBU_TJT-v2	305.5		461	315	33
SPIX-v2x4	281.6		1,332	176	40
Pyjamask-v2	267.3	23	2,308	213	102
Oribatida-v1	257.9	24	1,450	276	137
Oribatida-v2	252.3		1,450	276	105
TinyJAMBU_GMU-v1	250.4		591	266	34
ForkAE-v2	237.3	25	2,466	228	123
LOCUS-v2	222.9	26	1,628	209	60
Elephant-v1	214.3		1,291	229	171
SPIX-v2x2	206.3		1,267	187	58
SpoC_IIT-v1	201.9	27	1,512	235	149
WAGE-v1	156.6	28	1,150	279	114
LOTUS-v2	150.4		1,487	141	60
Saturnin-v1	139.7		1,725	215	394
SpoC_VT-v1	132.6		1,079	230	111
TinyJAMBU_GMU-v2	129.9		564	268	66
SPIX-v2	123.9		1,181	182	94
Xoodyak_GMU-v2	123.6		1,234	168	261
LOCUS-v1	121.3		1,824	216	114
Pyjamask-v1	111.9		1,979	229	262
ACE_UW-v1	98.5		1,229	200	130

Table 25 continued from previous page

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
COMET_CI-v2	95.7		1,096	222	297
LOTUS-v1	81.4		1,652	145	114
ESTATE-v3	81.3		1,130	259	408
ESTATE-v2	75.9		907	268	452
TinyJAMBU_TJT-v1	71.9		446	290	129
Gimli_TUM-v1	39.1		933	241	789
ESTATE-v4	25.5		944	277	1,392
Gimli_TUM-v2	21.1		905	244	1,481
Romulus-v5	21.0		887	214	1,304
Gimli_TUM-v3	11.3		838	253	2,865
TinyJAMBU_GMU-v3	8.7		537	278	1,026
ForkAE-v1	8.3		1,191	208	3,194

Table 26: Xilinx Artix-7 Encryption AD Throughput for Long Messages

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	9,536.0	1	848	298	1
Xoodyak_GMU2-v1	8,502.2	2	1,608	314	13
Ascon_GMU-v1	6,297.6	3	2,410	246	5
Subterranean_ST-v2	6,080.0		891	190	0.25
Xoodyak_GMU2-v2	5,837.3		2,322	199	12
KNOT-v2x4	4,525.7		**2,797**	165	7
Gimli_GMU-v4	4,425.1	4	2,357	242	7
Ascon_GMU-v2	4,366.2		1,790	307	9
KNOT-v2x4h	3,757.7	5	2,438	137	7
Ascon_GMU2-v2h	3,744.0		2,126	234	4
Xoodyak_XT-v2	3,676.4		2,025	188	18
Xoodyak_XT-v8	3,539.6		2,143	181	18
Xoodyak_XT-v1	3,432.0		1,355	234	24
Xoodyak_XT-v7	3,314.7		1,392	226	24
Ascon_Graz-v4	3,296.0		2,249	206	8
KNOT-v2x2	3,195.4		1,873	233	14
Gimli_GT-v5	3,104.0		**3,907**	97	4
KNOT-v2x2h	3,044.6		2,112	222	14
Ascon_GMU2-v3h	3,029.3		2,493	142	3
Gimli_GT-v4	3,029.3		2,510	142	6
GIFT-COFB_GMU-v4	3,029.3	6	1,730	213	9
AESGCM-v1	3,000.9		**3,270**	211	9
GIFT-COFB_GMU-v5	2,922.7		2,051	137	6
Gimli_GT-v6	2,912.0		**3,937**	91	4
GIFT-COFB_GMU-v3	2,897.5		1,641	249	11
GIFT-COFB_GMU-v6	2,816.0		2,363	110	5
Ascon_Graz-v3	2,572.8		2,142	201	5
Gimli_GMU-v2	2,560.0		1,678	260	13
TinyJAMBU_TJT-v3	2,560.0	7	576	240	3
Ascon_GMU2-v1h	2,523.4		1,375	276	7
Xoodyak_GMU-v1	2,493.3		1,808	170	24
Ascon_Graz-v5	2,400.0		**2,797**	150	4
Ascon_Graz-v2	2,272.0		1,541	213	12
Gimli_GT-v7	2,112.0		**5,347**	66	4
Gimli_GT-v3	2,096.0		**2,678**	131	8
Gimli_GT-v2	1,866.7		1,909	175	12
KNOT-v2x1	1,721.1		1,620	251	28
COMET_VT-v1	1,672.0	8	2,449	209	16
KNOT-v2x1h	1,618.3		1,684	236	28
GIFT-COFB_GMU-v2	1,590.9		1,380	261	21
Saturnin-v2	1,583.4	9	2,321	167	27
Ascon_Graz-v1	1,528.0		1,465	191	8
Romulus-v2	1,521.8	10	1,280	214	18
Elephant-v5	1,509.6		**2,645**	217	23
Ascon_VT-v1	1,491.2		1,913	233	10
DryGASCON-v1	1,450.7	11	2,074	238	21
Romulus-v3	1,431.3		1,824	123	11

Table 26 continued from previous page

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Ascon_VT-v2	1,401.6		1,928	219	10
Gimli_GMU-v1	1,305.6		1,435	255	25
Elephant-v2	1,206.7	12	1,884	181	24
Elephant-v3	1,142.9		1,717	200	28
ISAP-v1	1,111.7		**3,491**	193	25
Spook-v2-v2	1,098.7	13	2,033	206	48
ISAP-v3	1,082.9	14	2,182	188	25
Romulus-v4	989.9		**2,602**	58	7.5
Elephant-v4	978.6		1,901	263	43
Gimli_GT-v1	933.3		1,747	175	24
Romulus-v1	916.0		953	229	32
SCHWAEMM-v1	909.5	15*	**3,071**	135	38
SCHWAEMM-v2	875.8		**3,740**	130	38
GIFT-COFB_GMU-v1	821.1		1,223	263	41
AESGCM-v2	818.4	16	2,520	211	33
PHOTON-Beetle-v1	813.7	17	2,065	178	28
ISAP-v2	800.0		2,157	200	16
TinyJAMBU_TJT-v2	775.4		461	315	13
SPIX-v1	768.0	18	1,533	156	13
GIFT-COFB_VT-v1	718.4		1,041	275	49
ESTATE-v1	645.8	19	1,351	222	44
TinyJAMBU_GMU-v1	608.0		591	266	14
Oribatida-v1	512.0	20	1,450	276	69
ACE_GMU-v1	508.4	21	1,847	143	18
Oribatida-v2	499.9		1,450	276	53
COMET_CI-v3	491.4		1,841	215	56
SKINNY-AEAD-v1	487.6	22	2,333	240	63
SKINNY-AEAD-v2	487.6		2,337	240	63
COMET_CI-v1	475.7		1,884	223	60
LOCUS-v2	445.9	23	1,628	209	30
Elephant-v1	416.4		1,291	229	88
mixFeed-v1	364.7	24	1,343	151	53
COMET_VT-v2	352.4		1,703	234	85
TinyJAMBU_GMU-v2	329.8		564	268	26
LOTUS-v2	300.8		1,487	141	30
SPIX-v2x4	281.6		1,332	176	40
Saturnin-v1	279.4		1,725	215	197
Pyjamask-v2	278.2	25	2,308	213	98
ForkAE-v2	275.3	26	2,466	228	106
LOCUS-v1	242.5		1,824	216	57
Xoodyak_GMU-v2	222.3		1,234	168	266
SpoC_IIT-v1	207.4	27	1,512	235	145
SPIX-v2x2	206.3		1,267	187	58
TinyJAMBU_TJT-v1	189.4		446	290	49
LOTUS-v1	162.8		1,652	145	57
ESTATE-v3	162.5		1,130	259	204
WAGE-v1	156.6	28	1,150	279	114
ESTATE-v2	151.8		907	268	226

Table 26 continued from previous page

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
SpoC_VT-v1	135.0		1,079	230	109
SPIX-v2	123.9		1,181	182	94
Pyjamask-v1	113.6		1,979	229	258
COMET_CI-v2	107.6		1,096	222	264
ACE_UW-v1	98.5		1,229	200	130
ESTATE-v4	50.9		944	277	696
Romulus-v5	41.5		887	214	660
Gimli_TUM-v1	39.2		933	241	786
TinyJAMBU_GMU-v3	23.0		537	278	386
ForkAE-v1	22.0		1,191	208	1,209
Gimli_TUM-v2	21.2		905	244	1,474
Gimli_TUM-v3	11.4		838	253	2,850

Table 27: Xilinx Artix-7 Encryption AD+PT Throughput for Long Messages

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	9,536.0	1	848	298	2
Xoodyak_GMU2-v1	6,569.8	2	1,608	314	26
Ascon_GMU-v1	6,297.6	3	2,410	246	10
Subterranean_ST-v2	6,080.0		891	190	0.5
Xoodyak_GMU2-v2	5,697.7		2,322	199	19
Gimli_GMU-v4	4,425.1	4	2,357	242	14
Ascon_GMU-v2	4,366.2		1,790	307	18
Ascon_GMU2-v2h	3,744.0		2,126	234	8
Xoodyak_XT-v2	3,299.1		2,025	188	31
Ascon_Graz-v4	3,296.0		2,249	206	16
KNOT-v2x2	3,195.4	5	1,873	233	28
Xoodyak_XT-v8	3,176.3		2,143	181	31
KNOT-v2x4	3,168.0		**2,797**	165	20
Gimli_GT-v5	3,104.0		**3,907**	97	8
KNOT-v2x2h	3,044.6		2,112	222	28
GIFT-COFB_GMU-v4	3,029.3	6	1,730	213	18
Ascon_GMU2-v3h	3,029.3		2,493	142	6
Gimli_GT-v4	3,029.3		2,510	142	12
Xoodyak_XT-v1	2,960.4		1,355	234	43
GIFT-COFB_GMU-v5	2,922.7		2,051	137	12
Gimli_GT-v6	2,912.0		**3,937**	91	8
GIFT-COFB_GMU-v3	2,897.5		1,641	249	22
Xoodyak_XT-v7	2,859.2		1,392	226	43
GIFT-COFB_GMU-v6	2,816.0		2,363	110	10
AESGCM-v1	2,700.8		**3,270**	211	20
KNOT-v2x4h	2,630.4		2,438	137	20
Ascon_Graz-v3	2,572.8		2,142	201	10
Gimli_GMU-v2	2,560.0		1,678	260	26
Ascon_GMU2-v1h	2,523.4		1,375	276	14
Ascon_Graz-v5	2,400.0		**2,797**	150	8
Ascon_Graz-v2	2,272.0		1,541	213	24
Xoodyak_GMU-v1	2,150.7		1,808	170	43
Gimli_GT-v7	2,112.0		**5,347**	66	8
Gimli_GT-v3	2,096.0		**2,678**	131	16
Gimli_GT-v2	1,866.7		1,909	175	24
KNOT-v2x1	1,721.1		1,620	251	56
KNOT-v2x1h	1,618.3		1,684	236	56
GIFT-COFB_GMU-v2	1,590.9		1,380	261	42
Elephant-v5	1,543.1		**2,645**	217	45
Ascon_Graz-v1	1,528.0		1,465	191	16
Ascon_VT-v1	1,491.2		1,913	233	20
COMET_VT-v1	1,486.2	7	2,449	209	36
Ascon_VT-v2	1,475.4		1,928	219	19
DryGASCON-v1	1,450.7	8	2,074	238	42
TinyJAMBU_TJT-v3	1,396.4	9	576	240	11
Gimli_GMU-v1	1,305.6		1,435	255	50
Spook-v2-v2	1,098.7	10	2,033	206	96

Table 27 continued from previous page

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Romulus-v2	1,095.7	11	1,280	214	50
Romulus-v3	1,085.8		1,824	123	29
Saturnin-v2	1,055.6	12	2,321	167	81
Elephant-v4	990.1	13	1,901	263	85
Gimli_GT-v1	933.3		1,747	175	48
Elephant-v2	864.5		1,884	181	67
ISAP-v1	829.6		**3,491**	193	67
GIFT-COFB_GMU-v1	821.1		1,223	263	82
AESGCM-v2	818.4	14	2,520	211	66
SCHWAEMM-v1	813.2	15*	**3,071**	135	85
Elephant-v3	810.1		1,717	200	79
ISAP-v3	808.1	16	2,182	188	67
Romulus-v4	802.6		**2,602**	58	18.5
SCHWAEMM-v2	783.1		**3,740**	130	85
PHOTON-Beetle-v1	747.0	17	2,065	178	61
GIFT-COFB_VT-v1	733.3		1,041	275	96
SPIX-v1	713.1	18	1,533	156	28
Romulus-v1	637.2		953	229	92
ISAP-v2	609.5		2,157	200	42
ACE_GMU-v1	508.4	19	1,847	143	36
SKINNY-AEAD-v1	472.6	20	2,333	240	130
SKINNY-AEAD-v2	472.6		2,337	240	130
COMET_CI-v3	451.1		1,841	215	122
COMET_CI-v1	439.1		1,884	223	130
TinyJAMBU_TJT-v2	438.3		461	315	46
ESTATE-v1	430.5	21	1,351	222	132
TinyJAMBU_GMU-v1	354.7		591	266	48
mixFeed-v1	351.4	22	1,343	151	110
COMET_VT-v2	344.3		1,703	234	174
Oribatida-v1	343.0	23	1,450	276	206
Oribatida-v2	335.4		1,450	276	158
LOCUS-v2	297.2	24	1,628	209	90
Elephant-v1	282.9		1,291	229	259
SPIX-v2x4	281.6		1,332	176	80
Pyjamask-v2	272.6	25	2,308	213	200
ForkAE-v2	254.9	26	2,466	228	229
SPIX-v2x2	206.3		1,267	187	116
SpoC_IIT-v1	204.6	27	1,512	235	294
LOTUS-v2	200.5		1,487	141	90
TinyJAMBU_GMU-v2	186.4		564	268	92
Saturnin-v1	186.3		1,725	215	591
Xoodyak_GMU-v2	173.4		1,234	168	527
LOCUS-v1	161.7		1,824	216	171
WAGE-v1	156.6	28	1,150	279	228
SpoC_VT-v1	133.8		1,079	230	220
SPIX-v2	123.9		1,181	182	188
Pyjamask-v1	112.7		1,979	229	520
LOTUS-v1	108.5		1,652	145	171

Table 27 continued from previous page

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
ESTATE-v3	108.3		1,130	259	612
TinyJAMBU_TJT-v1	104.3		446	290	178
COMET_CI-v2	101.3		1,096	222	561
ESTATE-v2	101.2		907	268	678
ACE_UW-v1	98.5		1,229	200	260
Gimli_TUM-v1	39.2		933	241	1,575
ESTATE-v4	34.0		944	277	2,088
Romulus-v5	27.9		887	214	1,964
Gimli_TUM-v2	21.1		905	244	2,955
TinyJAMBU_GMU-v3	12.6		537	278	1,412
ForkAE-v1	12.1		1,191	208	4,403
Gimli_TUM-v3	11.3		838	253	5,715

Table 28: Xilinx Artix-7 Hash Throughput for Long Messages

Variant	**Throughput HM [Mbit/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per Block**
Gimli_GMU-v4	4,425.1	1	2,357	242	7
Xoodyak_GMU2-v2	3,638.9	2	2,322	199	7
Gimli_GT-v5	3,104.0		**3,907**	97	4
Xoodyak_GMU2-v1	3,091.7		1,608	314	13
Gimli_GT-v4	3,029.3		2,510	142	6
Gimli_GT-v6	2,912.0		**3,937**	91	4
Gimli_GMU-v2	2,560.0		1,678	260	13
Ascon_GMU2-v2h	2,139.4	3	2,126	234	7
Gimli_GT-v7	2,112.0		**5,347**	66	4
Xoodyak_XT-v8	2,106.2		2,143	181	11
Gimli_GT-v3	2,096.0		**2,678**	131	8
Gimli_GT-v2	1,866.7		1,909	175	12
Ascon_GMU2-v3h	1,817.6		2,493	142	5
Xoodyak_XT-v7	1,701.6		1,392	226	17
Ascon_Graz-v4	1,648.0		2,249	206	8
Ascon_Graz-v3	1,608.0		2,142	201	8
Ascon_Graz-v5	1,600.0		**2,797**	150	6
SHA2-v1	1,583.3	4	1,051	201	65
DryGASCON-v1	1,450.7	5	2,074	238	21
Ascon_GMU2-v1h	1,358.8		1,375	276	13
Gimli_GMU-v1	1,305.6		1,435	255	25
Saturnin-v2	1,295.5	6	2,321	167	33
Xoodyak_GMU-v1	1,280.0		1,808	170	17
Ascon_Graz-v2	973.7		1,541	213	14
Ascon_VT-v2	934.4		1,928	219	15
Gimli_GT-v1	933.3		1,747	175	24
SHA3-v1	910.6	7	1,263	195	233
KNOT-v2x4h	876.8	8	2,438	137	20
Ascon_Graz-v1	873.1		1,465	191	14
Subterranean_ST-v2	760.0	9	891	190	2
KNOT-v2x2h	710.4		2,112	222	40
ACE_GMU-v1	508.4	10	1,847	143	18
SCHWAEMM-v2	489.4	11*	**3,740**	130	34
KNOT-v2x1h	377.6		1,684	236	80
PHOTON-Beetle-v1	227.8	12	2,065	178	25
Saturnin-v1	180.5		1,725	215	305
ACE_UW-v1	98.5		1,229	200	130
Xoodyak_GMU-v2	83.0		1,234	168	259
Gimli_TUM-v1	39.2		933	241	786
Gimli_TUM-v2	21.2		905	244	1,474
Gimli_TUM-v3	11.4		838	253	2,850

Table 29: Intel Cyclone 10 LP Encryption PT Throughput for Long Messages

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	5,584.6	1	1,264	174.5	1
Subterranean_ST-v2	4,917.8		1,285	153.7	0.25
Ascon_GMU-v1	3,031.0	2	4,552	118.4	5
Gimli_GMU-v4	2,804.5	3	2,953	153.4	7
Xoodyak_GMU2-v2	2,665.8		**5,058**	97.2	7
Xoodyak_GMU2-v1	2,515.2	4	2,575	170.3	13
Ascon_GMU-v2	2,284.7		3,113	160.6	9
Ascon_GMU2-v2h	2,157.0		3,215	134.8	4
Gimli_GMU-v5	2,109.2		**5,576**	82.4	5
Ascon_GMU2-v3h	1,955.8		4,161	91.7	3
KNOT-v2x2h	1,921.8	5	2,792	140.1	14
KNOT-v2x2	1,902.4		2,472	138.7	14
Gimli_GT-v4	1,880.7		**5,010**	88.2	6
Gimli_GT-v5	1,874.6		**5,948**	58.6	4
Ascon_Graz-v4	1,738.4		3,730	108.7	8
Ascon_GMU2-v1h	1,605.4		2,415	175.6	7
GIFT-COFB_GMU-v4	1,575.5	6	2,609	110.8	9
GIFT-COFB_GMU-v3	1,533.7		2,523	131.8	11
Ascon_Graz-v2	1,529.1		2,634	143.3	12
Gimli_GMU-v2	1,515.5		2,158	153.9	13
KNOT-v2x4	1,507.2		3,519	102.0	13
KNOT-v2x4h	1,499.7		3,678	101.5	13
Gimli_GT-v6	1,447.4		4,820	45.2	4
AESGCM-v1	1,407.5		**8,754**	121.0	11
Ascon_Graz-v3	1,403.6		3,716	109.7	5
Xoodyak_XT-v1	1,377.7		2,231	136.3	19
Gimli_GT-v3	1,372.2		3,651	85.8	8
Xoodyak_XT-v8	1,328.5		3,630	90.0	13
Xoodyak_XT-v2	1,312.0		3,541	88.8	13
Xoodyak_XT-v7	1,298.8		2,272	128.5	19
Ascon_Graz-v5	1,281.9		4,905	80.1	4
Gimli_GT-v2	1,224.5		3,145	114.8	12
Ascon_VT-v2	1,223.1		2,695	172.0	9
Ascon_Graz-v1	1,131.0		2,517	141.4	8
Ascon_VT-v1	1,130.4		2,432	176.6	10
KNOT-v2x1	1,109.0		2,059	161.7	28
GIFT-COFB_GMU-v5	1,097.6		4,828	51.5	6
KNOT-v2x1h	1,093.1		2,532	159.4	28
Xoodyak_GMU-v1	1,079.1		3,135	106.8	19
Gimli_GT-v7	1,032.3		**6,379**	32.3	4
GIFT-COFB_GMU-v2	954.0		2,111	156.5	21
GIFT-COFB_GMU-v6	951.6		**6,630**	37.2	5
Elephant-v5	922.8	7	3,926	126.9	22
DryGASCON-v1	795.6	8	3,199	130.5	21
Gimli_GMU-v1	791.0		1,908	154.5	25
Gimli_GT-v1	761.5		2,378	142.8	24
TinyJAMBU_TJT-v3	638.8	9	1,021	159.7	8

Table 29 continued from previous page

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
Elephant-v4	600.4		3,050	157.6	42
Spook-v2-v2	578.8	10	3,188	108.5	48
COMET_VT-v1	569.0		**10,200**	88.9	20
Romulus-v2	566.8	11	2,086	141.7	32
Romulus-v3	563.9		2,407	79.3	18
GIFT-COFB_VT-v1	502.2		1,877	184.4	47
GIFT-COFB_GMU-v1	499.0		1,903	159.8	41
Saturnin-v2	495.7	12	3,892	104.6	54
PHOTON-Beetle-v1	486.6	13	3,602	125.4	33
Romulus-v4	469.6		3,409	40.4	11
SCHWAEMM-v2	467.0		**5,773**	85.7	47
AESGCM-v2	460.5	14*	**7,711**	118.7	33
ISAP-v3	452.3	15	3,767	131.9	42
ISAP-v4	450.9		3,026	155.0	22
SCHWAEMM-v1	445.3	16	4,713	81.8	47
ISAP-v1	434.1		4,589	126.6	42
Elephant-v2	421.0		2,729	113.2	43
Elephant-v3	386.6		2,504	123.2	51
SPIX-v1	350.4	17	3,525	82.1	15
ISAP-v2	335.7		3,852	136.4	26
Romulus-v1	305.6		1,735	143.2	60
SKINNY-AEAD-v1	276.3	18	3,672	144.6	67
ACE_GMU-v1	274.0	19	4,473	77.0	18
SKINNY-AEAD-v2	266.5		3,532	139.5	67
COMET_CI-v3	222.7	20	4,379	114.8	66
SPIX-v2x4	212.2		2,310	132.6	40
COMET_CI-v1	211.7		4,663	115.8	70
TinyJAMBU_TJT-v2	190.3		777	196.2	33
TinyJAMBU_GMU-v1	185.2		856	196.8	34
Oribatida-v1	173.5	21	2,512	185.7	137
ESTATE-v1	171.6	22	3,839	118.0	88
mixFeed-v1	164.3	23*	**5,363**	73.2	57
Oribatida-v2	159.5		2,221	174.5	105
COMET_VT-v2	159.1		**5,204**	110.6	89
SpoC_IIT-v1	156.5	24	2,250	182.2	149
ForkAE-v2	154.1	25	3,200	148.1	123
Elephant-v1	152.6		2,056	163.1	171
SPIX-v2x2	148.6		1,993	134.7	58
LOCUS-v2	141.2	26	2,828	132.4	60
Pyjamask-v2	113.7		**8,692**	90.6	102
LOTUS-v2	106.3		2,445	99.6	60
SpoC_VT-v1	96.7		1,696	167.7	111
TinyJAMBU_GMU-v2	95.1		841	196.2	66
Saturnin-v1	94.2		3,802	145.0	394
WAGE-v1	89.6	27	1,774	159.6	114
SPIX-v2	88.9		1,864	130.6	94
LOCUS-v1	70.6		2,978	125.8	114
LOTUS-v1	58.1		2,642	103.5	114

Table 29 continued from previous page

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
COMET_CI-v2	57.3		2,629	132.9	297
Xoodyak_GMU-v2	56.7		**5,871**	77.0	261
ESTATE-v3	56.5		2,279	180.2	408
Pyjamask-v1	53.6	28*	**8,599**	109.7	262
ACE_UW-v1	52.4		1,903	106.5	130
TinyJAMBU_TJT-v1	49.8		686	200.8	129
ESTATE-v2	49.4		1,946	174.3	452
ESTATE-v4	18.4		1,572	200.1	1,392
Gimli_TUM-v1	16.4		2,044	101.3	789
Romulus-v5	12.8		1,960	130.2	1,304
Gimli_TUM-v2	8.4		2,074	97.3	1,481
TinyJAMBU_GMU-v3	6.0		817	191.1	1,026
ForkAE-v1	5.4		2,129	135.7	3,194
Gimli_TUM-v3	4.5		2,115	100.5	2,865

Table 30: Intel Cyclone 10 LP Encryption AD Throughput for Long Messages

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	5,584.6	1	1,264	174.5	1
Subterranean_ST-v2	4,917.8		1,285	153.7	0.25
Xoodyak_GMU2-v1	4,611.2	2	2,575	170.3	13
Ascon_GMU-v1	3,031.0	3	4,552	118.4	5
Xoodyak_GMU2-v2	2,850.9		**5,058**	97.2	12
Gimli_GMU-v4	2,804.5	4	2,953	153.4	7
KNOT-v2x4	2,799.1	5	3,519	102.0	7
KNOT-v2x4h	2,785.1		3,678	101.5	7
Ascon_GMU-v2	2,284.7		3,113	160.6	9
Ascon_GMU2-v2h	2,157.0		3,215	134.8	4
Gimli_GMU-v5	2,109.2		**5,576**	82.4	5
Xoodyak_XT-v1	1,999.5		2,231	136.3	24
Ascon_GMU2-v3h	1,955.8		4,161	91.7	3
KNOT-v2x2h	1,921.8		2,792	140.1	14
KNOT-v2x2	1,902.4		2,472	138.7	14
Xoodyak_XT-v7	1,885.1		2,272	128.5	24
Gimli_GT-v4	1,880.7		**5,010**	88.2	6
Gimli_GT-v5	1,874.6		**5,948**	58.6	4
Xoodyak_XT-v8	1,759.0		3,630	90.0	18
Ascon_Graz-v4	1,738.4		3,730	108.7	8
Xoodyak_XT-v2	1,737.1		3,541	88.8	18
AESGCM-v1	1,720.3		**8,754**	121.0	9
TinyJAMBU_TJT-v3	1,703.4	6	1,021	159.7	3
Ascon_GMU2-v1h	1,605.4		2,415	175.6	7
GIFT-COFB_GMU-v4	1,575.5	7	2,609	110.8	9
Xoodyak_GMU-v1	1,566.3		3,135	106.8	24
GIFT-COFB_GMU-v3	1,533.7		2,523	131.8	11
Ascon_Graz-v2	1,529.1		2,634	143.3	12
Gimli_GMU-v2	1,515.5		2,158	153.9	13
Gimli_GT-v6	1,447.4		4,820	45.2	4
Ascon_Graz-v3	1,403.6		3,716	109.7	5
Gimli_GT-v3	1,372.2		3,651	85.8	8
Ascon_Graz-v5	1,281.9		4,905	80.1	4
Gimli_GT-v2	1,224.5		3,145	114.8	12
Ascon_Graz-v1	1,131.0		2,517	141.4	8
Ascon_VT-v1	1,130.4		2,432	176.6	10
KNOT-v2x1	1,109.0		2,059	161.7	28
Ascon_VT-v2	1,100.8		2,695	172.0	10
GIFT-COFB_GMU-v5	1,097.6		4,828	51.5	6
KNOT-v2x1h	1,093.1		2,532	159.4	28
Gimli_GT-v7	1,032.3		**6,379**	32.3	4
Romulus-v2	1,007.6	8	2,086	141.7	18
Saturnin-v2	991.4	9	3,892	104.6	27
GIFT-COFB_GMU-v2	954.0		2,111	156.5	21
GIFT-COFB_GMU-v6	951.6		**6,630**	37.2	5
Romulus-v3	922.8		2,407	79.3	11
Elephant-v5	882.7	10	3,926	126.9	23

Table 30 continued from previous page

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
DryGASCON-v1	795.6	11	3,199	130.5	21
Gimli_GMU-v1	791.0		1,908	154.5	25
Gimli_GT-v1	761.5		2,378	142.8	24
ISAP-v3	759.8	12	3,767	131.9	25
Elephant-v2	754.3		2,729	113.2	24
ISAP-v1	729.2		4,589	126.6	25
COMET_VT-v1	711.2		**10,200**	88.9	16
ISAP-v4	708.5		3,026	155.0	14
Elephant-v3	704.2		2,504	123.2	28
Romulus-v4	688.8		3,409	40.4	7.5
Elephant-v4	586.4		3,050	157.6	43
Spook-v2-v2	578.8	13	3,188	108.5	48
SCHWAEMM-v2	577.6		**5,773**	85.7	38
PHOTON-Beetle-v1	573.4	14	3,602	125.4	28
Romulus-v1	573.0		1,735	143.2	32
SCHWAEMM-v1	550.7	15	4,713	81.8	38
ISAP-v2	545.6		3,852	136.4	16
GIFT-COFB_GMU-v1	499.0		1,903	159.8	41
TinyJAMBU_TJT-v2	483.0		777	196.2	13
GIFT-COFB_VT-v1	481.7		1,877	184.4	49
AESGCM-v2	460.5	16*	**7,711**	118.7	33
TinyJAMBU_GMU-v1	449.9		856	196.8	14
SPIX-v1	404.3	17	3,525	82.1	13
Oribatida-v1	344.4	18	2,512	185.7	69
ESTATE-v1	343.2	19	3,839	118.0	44
Oribatida-v2	316.1		2,221	174.5	53
Elephant-v1	296.5		2,056	163.1	88
SKINNY-AEAD-v1	293.9	20	3,672	144.6	63
SKINNY-AEAD-v2	283.4		3,532	139.5	63
LOCUS-v2	282.5	21	2,828	132.4	30
ACE_GMU-v1	274.0	22	4,473	77.0	18
COMET_CI-v3	262.5	23	4,379	114.8	56
COMET_CI-v1	246.9		4,663	115.8	60
TinyJAMBU_GMU-v2	241.4		841	196.2	26
LOTUS-v2	212.6		2,445	99.6	30
SPIX-v2x4	212.2		2,310	132.6	40
Saturnin-v1	188.4		3,802	145.0	197
ForkAE-v2	178.8	24	3,200	148.1	106
mixFeed-v1	176.7	25*	**5,363**	73.2	53
COMET_VT-v2	166.6		**5,204**	110.6	85
SpoC_IIT-v1	160.9	26	2,250	182.2	145
SPIX-v2x2	148.6		1,993	134.7	58
LOCUS-v1	141.2		2,978	125.8	57
TinyJAMBU_TJT-v1	131.2		686	200.8	49
Pyjamask-v2	118.4		**8,692**	90.6	98
LOTUS-v1	116.2		2,642	103.5	57
ESTATE-v3	113.1		2,279	180.2	204
Xoodyak_GMU-v2	102.0		**5,871**	77.0	266

Table 30 continued from previous page

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
ESTATE-v2	98.7		1,946	174.3	226
SpoC_VT-v1	98.5		1,696	167.7	109
WAGE-v1	89.6	27	1,774	159.6	114
SPIX-v2	88.9		1,864	130.6	94
COMET_CI-v2	64.5		2,629	132.9	264
Pyjamask-v1	54.4	28*	**8,599**	109.7	258
ACE_UW-v1	52.4		1,903	106.5	130
ESTATE-v4	36.8		1,572	200.1	696
Romulus-v5	25.3		1,960	130.2	660
Gimli_TUM-v1	16.5		2,044	101.3	786
TinyJAMBU_GMU-v3	15.8		817	191.1	386
ForkAE-v1	14.4		2,129	135.7	1,209
Gimli_TUM-v2	8.5		2,074	97.3	1,474
Gimli_TUM-v3	4.5		2,115	100.5	2,850

Table 31: Intel Cyclone 10 LP Encryption AD+PT Throughput for Long Messages

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	5,584.6	1	1,264	174.5	2
Subterranean_ST-v2	4,917.8		1,285	153.7	0.5
Xoodyak_GMU2-v1	3,563.2	2	2,575	170.3	26
Ascon_GMU-v1	3,031.0	3	4,552	118.4	10
Gimli_GMU-v4	2,804.5	4	2,953	153.4	14
Xoodyak_GMU2-v2	2,782.7		**5,058**	97.2	19
Ascon_GMU-v2	2,284.7		3,113	160.6	18
Ascon_GMU2-v2h	2,157.0		3,215	134.8	8
Gimli_GMU-v5	2,109.2		**5,576**	82.4	10
KNOT-v2x4	1,959.4	5	3,519	102.0	20
Ascon_GMU2-v3h	1,955.8		4,161	91.7	6
KNOT-v2x4h	1,949.6		3,678	101.5	20
KNOT-v2x2h	1,921.8		2,792	140.1	28
KNOT-v2x2	1,902.4		2,472	138.7	28
Gimli_GT-v4	1,880.7		**5,010**	88.2	12
Gimli_GT-v5	1,874.6		**5,948**	58.6	8
Ascon_Graz-v4	1,738.4		3,730	108.7	16
Xoodyak_XT-v1	1,724.7		2,231	136.3	43
Xoodyak_XT-v7	1,626.1		2,272	128.5	43
Ascon_GMU2-v1h	1,605.4		2,415	175.6	14
Xoodyak_XT-v8	1,578.5		3,630	90.0	31
GIFT-COFB_GMU-v4	1,575.5	6	2,609	110.8	18
Xoodyak_XT-v2	1,558.8		3,541	88.8	31
AESGCM-v1	1,548.3		**8,754**	121.0	20
GIFT-COFB_GMU-v3	1,533.7		2,523	131.8	22
Ascon_Graz-v2	1,529.1		2,634	143.3	24
Gimli_GMU-v2	1,515.5		2,158	153.9	26
Gimli_GT-v6	1,447.4		4,820	45.2	8
Ascon_Graz-v3	1,403.6		3,716	109.7	10
Gimli_GT-v3	1,372.2		3,651	85.8	16
Xoodyak_GMU-v1	1,351.0		3,135	106.8	43
Ascon_Graz-v5	1,281.9		4,905	80.1	8
Gimli_GT-v2	1,224.5		3,145	114.8	24
Ascon_VT-v2	1,158.7		2,695	172.0	19
Ascon_Graz-v1	1,131.0		2,517	141.4	16
Ascon_VT-v1	1,130.4		2,432	176.6	20
KNOT-v2x1	1,109.0		2,059	161.7	56
GIFT-COFB_GMU-v5	1,097.6		4,828	51.5	12
KNOT-v2x1h	1,093.1		2,532	159.4	56
Gimli_GT-v7	1,032.3		**6,379**	32.3	8
GIFT-COFB_GMU-v2	954.0		2,111	156.5	42
GIFT-COFB_GMU-v6	951.6		**6,630**	37.2	10
TinyJAMBU_TJT-v3	929.1	7	1,021	159.7	11
Elephant-v5	902.3	8	3,926	126.9	45
DryGASCON-v1	795.6	9	3,199	130.5	42
Gimli_GMU-v1	791.0		1,908	154.5	50
Gimli_GT-v1	761.5		2,378	142.8	48

Table 31 continued from previous page

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
Romulus-v2	725.5	10	2,086	141.7	50
Romulus-v3	700.0		2,407	79.3	29
Saturnin-v2	660.9	11	3,892	104.6	81
COMET_VT-v1	632.2		**10,200**	88.9	36
Elephant-v4	593.3		3,050	157.6	85
Spook-v2-v2	578.8	12	3,188	108.5	96
ISAP-v3	567.0	13	3,767	131.9	67
Romulus-v4	558.5		3,409	40.4	18.5
ISAP-v4	551.1		3,026	155.0	36
ISAP-v1	544.2		4,589	126.6	67
Elephant-v2	540.4		2,729	113.2	67
PHOTON-Beetle-v1	526.4	14	3,602	125.4	61
SCHWAEMM-v2	516.5		**5,773**	85.7	85
Elephant-v3	499.2		2,504	123.2	79
GIFT-COFB_GMU-v1	499.0		1,903	159.8	82
SCHWAEMM-v1	492.4	15	4,713	81.8	85
GIFT-COFB_VT-v1	491.7		1,877	184.4	96
AESGCM-v2	460.5	16*	**7,711**	118.7	66
ISAP-v2	415.7		3,852	136.4	42
Romulus-v1	398.6		1,735	143.2	92
SPIX-v1	375.4	17	3,525	82.1	28
SKINNY-AEAD-v1	284.8	18	3,672	144.6	130
SKINNY-AEAD-v2	274.7		3,532	139.5	130
ACE_GMU-v1	274.0	19	4,473	77.0	36
TinyJAMBU_TJT-v2	273.0		777	196.2	46
TinyJAMBU_GMU-v1	262.4		856	196.8	48
COMET_CI-v3	241.0	20	4,379	114.8	122
Oribatida-v1	230.7	21	2,512	185.7	206
ESTATE-v1	228.8	22	3,839	118.0	132
COMET_CI-v1	227.9		4,663	115.8	130
SPIX-v2x4	212.2		2,310	132.6	80
Oribatida-v2	212.0		2,221	174.5	158
Elephant-v1	201.5		2,056	163.1	259
LOCUS-v2	188.3	23	2,828	132.4	90
mixFeed-v1	170.2	24*	**5,363**	73.2	110
ForkAE-v2	165.5	25	3,200	148.1	229
COMET_VT-v2	162.8		**5,204**	110.6	174
SpoC_IIT-v1	158.7	26	2,250	182.2	294
SPIX-v2x2	148.6		1,993	134.7	116
LOTUS-v2	141.7		2,445	99.6	90
TinyJAMBU_GMU-v2	136.5		841	196.2	92
Saturnin-v1	125.6		3,802	145.0	591
Pyjamask-v2	116.0		**8,692**	90.6	200
SpoC_VT-v1	97.6		1,696	167.7	220
LOCUS-v1	94.1		2,978	125.8	171
WAGE-v1	89.6	27	1,774	159.6	228
SPIX-v2	88.9		1,864	130.6	188
Xoodyak_GMU-v2	79.5		**5,871**	77.0	527

Table 31 continued from previous page

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
LOTUS-v1	77.5		2,642	103.5	171
ESTATE-v3	75.4		2,279	180.2	612
TinyJAMBU_TJT-v1	72.2		686	200.8	178
ESTATE-v2	65.8		1,946	174.3	678
COMET_CI-v2	60.7		2,629	132.9	561
Pyjamask-v1	54.0	28*	**8,599**	109.7	520
ACE_UW-v1	52.4		1,903	106.5	260
ESTATE-v4	24.5		1,572	200.1	2,088
Romulus-v5	17.0		1,960	130.2	1,964
Gimli_TUM-v1	16.5		2,044	101.3	1,575
TinyJAMBU_GMU-v3	8.7		817	191.1	1,412
Gimli_TUM-v2	8.4		2,074	97.3	2,955
ForkAE-v1	7.9		2,129	135.7	4,403
Gimli_TUM-v3	4.5		2,115	100.5	5,715

Table 32: Intel Cyclone 10 LP Hash Throughput for Long Messages

Variant	**Throughput HM [Mbit/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per Block**
Gimli_GMU-v4	2,804.5	1	2,953	153.4	7
Gimli_GMU-v5	2,109.2		**5,576**	82.4	5
Gimli_GT-v4	1,880.7		**5,010**	88.2	6
Gimli_GT-v5	1,874.6		**5,948**	58.6	4
Xoodyak_GMU2-v2	1,777.2		**5,058**	97.2	7
Xoodyak_GMU2-v1	1,676.8	2	2,575	170.3	13
Gimli_GMU-v2	1,515.5		2,158	153.9	13
Gimli_GT-v6	1,447.4		4,820	45.2	4
Gimli_GT-v3	1,372.2		3,651	85.8	8
Ascon_GMU2-v2h	1,232.5	3	3,215	134.8	7
Gimli_GT-v2	1,224.5		3,145	114.8	12
Ascon_GMU2-v3h	1,173.5		4,161	91.7	5
Xoodyak_XT-v8	1,046.7		3,630	90.0	11
Gimli_GT-v7	1,032.3		**6,379**	32.3	4
Xoodyak_XT-v7	967.8		2,272	128.5	17
SHA2-v1	934.4	4	2,139	118.6	65
Ascon_Graz-v3	877.3		3,716	109.7	8
Ascon_Graz-v4	869.2		3,730	108.7	8
Ascon_GMU2-v1h	864.4		2,415	175.6	13
Ascon_Graz-v5	854.6		4,905	80.1	6
Saturnin-v2	811.1	5	3,892	104.6	33
Xoodyak_GMU-v1	804.1		3,135	106.8	17
DryGASCON-v1	795.6	6	3,199	130.5	21
Gimli_GMU-v1	791.0		1,908	154.5	25
Gimli_GT-v1	761.5		2,378	142.8	24
Ascon_VT-v2	733.9		2,695	172.0	15
Ascon_Graz-v2	655.3		2,634	143.3	14
KNOT-v2x4h	649.9	7	3,678	101.5	20
Ascon_Graz-v1	646.3		2,517	141.4	14
Subterranean_ST-v2	614.7	8	1,285	153.7	2
KNOT-v2x2h	448.4		2,792	140.1	40
SHA3-v1	394.3	9*	**5,417**	84.5	233
SCHWAEMM-v2	322.8	10*	**5,773**	85.7	34
ACE_GMU-v1	274.0	11	4,473	77.0	18
KNOT-v2x1h	255.1		2,532	159.4	80
PHOTON-Beetle-v1	160.6	12	3,602	125.4	25
Saturnin-v1	121.7		3,802	145.0	305
ACE_UW-v1	52.4		1,903	106.5	130
Xoodyak_GMU-v2	38.1		**5,871**	77.0	259
Gimli_TUM-v1	16.5		2,044	101.3	786
Gimli_TUM-v2	8.5		2,074	97.3	1,474
Gimli_TUM-v3	4.5		2,115	100.5	2,850

Table 33: Lattice ECP5 Encryption PT Throughput for Long Messages

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	3,840.1	1	1,471	120.0	1
Subterranean_ST-v2	3,063.4		1,342	95.7	0.25
Xoodyak_GMU2-v1	2,222.5	2	3,248	150.5	13
Ascon_GMU-v1	2,158.1		**5,909**	84.3	5
Xoodyak_GMU2-v2	1,911.0		4,058	69.7	7
Gimli_GMU-v4	1,735.9	3	3,223	94.9	7
Ascon_GMU-v2	1,666.3	4	4,641	117.2	9
Ascon_GMU2-v2h	1,427.5		3,764	89.2	4
Gimli_GMU-v5	1,344.8		4,586	52.5	5
Ascon_GMU2-v3h	1,305.6		4,925	61.2	3
Gimli_GT-v4	1,295.6		4,027	60.7	6
AESGCM-v1	1,258.6		**6,740**	108.2	11
KNOT-v2x2	1,239.9	5	3,287	90.4	14
Xoodyak_XT-v8	1,053.0		4,121	71.3	13
Xoodyak_XT-v2	1,038.8		4,077	70.3	13
KNOT-v2x2h	1,032.7		3,373	75.3	14
Gimli_GMU-v2	1,014.0		2,617	103.0	13
Gimli_GT-v6	1,008.0		**6,341**	31.5	4
Ascon_GMU2-v1h	1,006.3		2,928	110.1	7
Ascon_Graz-v4	989.6		3,379	61.9	8
Xoodyak_XT-v1	967.1		2,402	95.7	19
KNOT-v2x4	933.6		3,984	63.2	13
KNOT-v2x4h	899.0		4,283	60.9	13
Xoodyak_XT-v7	893.5		2,489	88.4	19
Gimli_GT-v3	890.4		4,451	55.6	8
Ascon_Graz-v5	889.8		4,646	55.6	4
GIFT-COFB_GMU-v3	869.6	6	3,059	74.7	11
Ascon_Graz-v6	827.9		**5,346**	38.8	6
Ascon_Graz-v3	815.0		3,305	63.7	5
Gimli_GT-v2	812.8		2,852	76.2	12
GIFT-COFB_GMU-v4	812.7		3,311	57.1	9
GIFT-COFB_GMU-v5	777.9		3,821	36.5	6
Xoodyak_GMU-v1	747.8		3,172	74.0	19
Gimli_GT-v5	745.6		**5,738**	23.3	4
Ascon_Graz-v2	683.1		2,603	64.0	12
Elephant-v5	655.2	7	4,145	90.1	22
GIFT-COFB_GMU-v2	639.9		2,628	105.0	21
COMET_VT-v1	630.0		**5,266**	98.4	20
DryGASCON-v1	612.8	8	3,801	100.5	21
KNOT-v2x1	586.0		2,275	85.5	28
Ascon_VT-v1	543.4		3,130	84.9	10
KNOT-v2x1h	541.2		2,446	78.9	28
Ascon_VT-v2	536.3		3,041	75.4	9
Gimli_GT-v7	526.4		**8,238**	16.4	4
Gimli_GMU-v1	522.4		2,328	102.0	25
Ascon_Graz-v1	474.2		2,544	59.3	8
TinyJAMBU_TJT-v3	461.6	9	1,092	115.4	8

Table 33 continued from previous page

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Gimli_GT-v1	417.3		2,537	78.2	24
AESGCM-v2	413.8	10*	**5,507**	106.7	33
Spook-v2-v2	410.7	11	3,662	77.0	48
PHOTON-Beetle-v1	393.5	12	3,294	101.4	33
Saturnin-v2	374.5	13	3,648	79.0	54
Elephant-v4	372.0		3,157	97.6	42
SCHWAEMM-v1	361.3	14	4,685	66.3	47
SCHWAEMM-v2	347.4		**5,947**	63.8	47
GIFT-COFB_GMU-v1	332.3		2,727	106.5	41
Romulus-v2	328.0	15	2,353	82.0	32
Romulus-v3	320.0		3,847	45.0	18
Elephant-v2	318.1		3,073	85.5	43
GIFT-COFB_VT-v1	311.3		2,214	114.3	47
SPIX-v1	295.9	16	2,432	69.3	15
Elephant-v3	277.2		2,901	88.3	51
ACE_GMU-v1	263.9	17	2,784	74.2	18
Romulus-v4	251.3		**5,086**	21.6	11
ISAP-v3	225.1		**5,703**	65.6	42
ISAP-v1	209.5		**6,701**	61.1	42
ISAP-v4	195.5	18	3,623	67.2	22
SKINNY-AEAD-v1	193.2	19	3,174	101.1	67
SKINNY-AEAD-v2	188.0		3,182	98.4	67
Romulus-v1	171.8		1,998	80.5	60
ISAP-v2	167.3		**5,708**	68.0	26
Oribatida-v1	164.9	20	1,671	176.5	137
COMET_VT-v2	160.3	21	2,353	111.5	89
ESTATE-v1	158.6	22	2,855	109.0	88
COMET_CI-v3	155.2		3,443	80.0	66
COMET_CI-v1	147.9		3,255	80.9	70
SPIX-v2x4	138.7		2,265	86.7	40
TinyJAMBU_TJT-v2	121.6		689	125.4	33
TinyJAMBU_GMU-v1	117.5		720	124.8	34
SpoC_IIT-v1	113.5	23	2,153	132.2	149
Oribatida-v2	104.4		2,497	114.2	105
ForkAE-v2	93.6	24	3,571	90.0	123
Pyjamask-v2	91.9	25	4,162	73.2	102
Elephant-v1	91.2		2,368	97.5	171
SPIX-v2x2	88.5		2,107	80.2	58
mixFeed-v1	87.4	26	3,479	38.9	57
LOCUS-v2	77.3	27	2,950	72.5	60
TinyJAMBU_GMU-v2	62.2		908	128.3	66
SPIX-v2	60.7		2,078	89.2	94
Saturnin-v1	60.2		3,070	92.6	394
WAGE-v1	57.0	28	2,081	101.6	114
SpoC_VT-v1	56.6		2,049	98.2	111
LOTUS-v2	56.2		2,208	52.7	60
Xoodyak_GMU-v2	55.0		2,316	74.8	261
Pyjamask-v1	45.3		3,897	92.7	262

Table 33 continued from previous page

Variant	Throughput PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
LOCUS-v1	41.0		2,857	73.0	114
COMET_CI-v2	40.7		1,974	94.3	297
ACE_UW-v1	36.3		2,156	73.8	130
ESTATE-v3	33.6		1,820	107.1	408
ESTATE-v2	32.7		1,689	115.4	452
LOTUS-v1	30.6		2,413	54.6	114
TinyJAMBU_TJT-v1	27.6		580	111.3	129
Gimli_TUM-v1	12.6		1,767	78.0	789
ESTATE-v4	10.9		1,329	118.1	1,392
Romulus-v5	7.5		1,961	76.5	1,304
Gimli_TUM-v2	6.4		1,767	73.5	1,481
Gimli_TUM-v3	3.5		1,772	78.5	2,865
TinyJAMBU_GMU-v3	3.4		1,277	108.1	1,026
ForkAE-v1	2.7		2,022	67.9	3,194

Table 34: Lattice ECP5 Encryption AD Throughput for Long Messages

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Xoodyak_GMU2-v1	4,074.5	1	3,248	150.5	13
Subterranean_GMU-v1	3,840.1	2	1,471	120.0	1
Subterranean_ST-v2	3,063.4		1,342	95.7	0.25
Ascon_GMU-v1	2,158.1		**5,909**	84.3	5
Xoodyak_GMU2-v2	2,043.7		4,058	69.7	12
Gimli_GMU-v4	1,735.9	3	3,223	94.9	7
KNOT-v2x4	1,733.8	4	3,984	63.2	7
KNOT-v2x4h	1,669.6		4,283	60.9	7
Ascon_GMU-v2	1,666.3	5	4,641	117.2	9
AESGCM-v1	1,538.3		**6,740**	108.2	9
Ascon_GMU2-v2h	1,427.5		3,764	89.2	4
Xoodyak_XT-v1	1,403.6		2,402	95.7	24
Xoodyak_XT-v8	1,394.3		4,121	71.3	18
Xoodyak_XT-v2	1,375.4		4,077	70.3	18
Gimli_GMU-v5	1,344.8		4,586	52.5	5
Ascon_GMU2-v3h	1,305.6		4,925	61.2	3
Xoodyak_XT-v7	1,296.8		2,489	88.4	24
Gimli_GT-v4	1,295.6		4,027	60.7	6
KNOT-v2x2	1,239.9		3,287	90.4	14
TinyJAMBU_TJT-v3	1,230.8	6	1,092	115.4	3
Xoodyak_GMU-v1	1,085.3		3,172	74.0	24
KNOT-v2x2h	1,032.7		3,373	75.3	14
Gimli_GMU-v2	1,014.0		2,617	103.0	13
Gimli_GT-v6	1,008.0		**6,341**	31.5	4
Ascon_GMU2-v1h	1,006.3		2,928	110.1	7
Ascon_Graz-v4	989.6		3,379	61.9	8
Gimli_GT-v3	890.4		4,451	55.6	8
Ascon_Graz-v5	889.8		4,646	55.6	4
GIFT-COFB_GMU-v3	869.6	7	3,059	74.7	11
Ascon_Graz-v6	827.9		**5,346**	38.8	6
Ascon_Graz-v3	815.0		3,305	63.7	5
Gimli_GT-v2	812.8		2,852	76.2	12
GIFT-COFB_GMU-v4	812.7		3,311	57.1	9
COMET_VT-v1	787.4		**5,266**	98.4	16
GIFT-COFB_GMU-v5	777.9		3,821	36.5	6
Saturnin-v2	749.0	8	3,648	79.0	27
Gimli_GT-v5	745.6		**5,738**	23.3	4
Ascon_Graz-v2	683.1		2,603	64.0	12
GIFT-COFB_GMU-v2	639.9		2,628	105.0	21
Elephant-v5	626.7	9	4,145	90.1	23
DryGASCON-v1	612.8	10	3,801	100.5	21
KNOT-v2x1	586.0		2,275	85.5	28
Romulus-v2	583.1	11	2,353	82.0	18
Elephant-v2	570.0		3,073	85.5	24
Ascon_VT-v1	543.4		3,130	84.9	10
KNOT-v2x1h	541.2		2,446	78.9	28
Gimli_GT-v7	526.4		**8,238**	16.4	4

Table 34 continued from previous page

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Romulus-v3	523.6		3,847	45.0	11
Gimli_GMU-v1	522.4		2,328	102.0	25
Elephant-v3	504.8		2,901	88.3	28
Ascon_VT-v2	482.7		3,041	75.4	10
Ascon_Graz-v1	474.2		2,544	59.3	8
PHOTON-Beetle-v1	463.7	12	3,294	101.4	28
SCHWAEMM-v1	446.9	13	4,685	66.3	38
SCHWAEMM-v2	429.7		**5,947**	63.8	38
Gimli_GT-v1	417.3		2,537	78.2	24
AESGCM-v2	413.8	14*	**5,507**	106.7	33
Spook-v2-v2	410.7	15	3,662	77.0	48
ISAP-v3	378.1		**5,703**	65.6	25
Romulus-v4	368.6		**5,086**	21.6	7.5
Elephant-v4	363.3		3,157	97.6	43
ISAP-v1	351.9		**6,701**	61.1	25
SPIX-v1	341.4	16	2,432	69.3	13
GIFT-COFB_GMU-v1	332.3		2,727	106.5	41
Oribatida-v1	327.3	17	1,671	176.5	69
Romulus-v1	322.0		1,998	80.5	32
ESTATE-v1	317.1	18	2,855	109.0	44
TinyJAMBU_TJT-v2	308.7		689	125.4	13
ISAP-v4	307.2	19	3,623	67.2	14
GIFT-COFB_VT-v1	298.6		2,214	114.3	49
TinyJAMBU_GMU-v1	285.3		720	124.8	14
ISAP-v2	271.9		**5,708**	68.0	16
ACE_GMU-v1	263.9	20	2,784	74.2	18
Oribatida-v2	206.9		2,497	114.2	53
SKINNY-AEAD-v1	205.5	21	3,174	101.1	63
SKINNY-AEAD-v2	200.0		3,182	98.4	63
COMET_CI-v3	182.9	22	3,443	80.0	56
Elephant-v1	177.3		2,368	97.5	88
COMET_CI-v1	172.6		3,255	80.9	60
COMET_VT-v2	167.8		2,353	111.5	85
TinyJAMBU_GMU-v2	157.9		908	128.3	26
LOCUS-v2	154.7	23	2,950	72.5	30
SPIX-v2x4	138.7		2,265	86.7	40
Saturnin-v1	120.3		3,070	92.6	197
SpoC_IIT-v1	116.7	24	2,153	132.2	145
LOTUS-v2	112.4		2,208	52.7	30
ForkAE-v2	108.7	25	3,571	90.0	106
Xoodyak_GMU-v2	99.0		2,316	74.8	266
Pyjamask-v2	95.6	26	4,162	73.2	98
mixFeed-v1	93.9	27	3,479	38.9	53
SPIX-v2x2	88.5		2,107	80.2	58
LOCUS-v1	81.9		2,857	73.0	57
TinyJAMBU_TJT-v1	72.7		580	111.3	49
ESTATE-v3	67.2		1,820	107.1	204
ESTATE-v2	65.4		1,689	115.4	226

Table 34 continued from previous page

Variant	Throughput AD [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
LOTUS-v1	61.3		2,413	54.6	57
SPIX-v2	60.7		2,078	89.2	94
SpoC_VT-v1	57.7		2,049	98.2	109
WAGE-v1	57.0	28	2,081	101.6	114
Pyjamask-v1	46.0		3,897	92.7	258
COMET_CI-v2	45.7		1,974	94.3	264
ACE_UW-v1	36.3		2,156	73.8	130
ESTATE-v4	21.7		1,329	118.1	696
Romulus-v5	14.8		1,961	76.5	660
Gimli_TUM-v1	12.7		1,767	78.0	786
TinyJAMBU_GMU-v3	9.0		1,277	108.1	386
ForkAE-v1	7.2		2,022	67.9	1,209
Gimli_TUM-v2	6.4		1,767	73.5	1,474
Gimli_TUM-v3	3.5		1,772	78.5	2,850

Table 35: Lattice ECP5 Encryption AD+PT Throughput for Long Messages

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Subterranean_GMU-v1	3,840.1	1	1,471	120.0	2
Xoodyak_GMU2-v1	3,148.5	2	3,248	150.5	26
Subterranean_ST-v2	3,063.4		1,342	95.7	0.5
Ascon_GMU-v1	2,158.1		**5,909**	84.3	10
Xoodyak_GMU2-v2	1,994.8		4,058	69.7	19
Gimli_GMU-v4	1,735.9	3	3,223	94.9	14
Ascon_GMU-v2	1,666.3	4	4,641	117.2	18
Ascon_GMU2-v2h	1,427.5		3,764	89.2	8
AESGCM-v1	1,384.4		**6,740**	108.2	20
Gimli_GMU-v5	1,344.8		4,586	52.5	10
Ascon_GMU2-v3h	1,305.6		4,925	61.2	6
Gimli_GT-v4	1,295.6		4,027	60.7	12
Xoodyak_XT-v8	1,251.2		4,121	71.3	31
KNOT-v2x2	1,239.9	5	3,287	90.4	28
Xoodyak_XT-v2	1,234.2		4,077	70.3	31
KNOT-v2x4	1,213.6		3,984	63.2	20
Xoodyak_XT-v1	1,210.7		2,402	95.7	43
KNOT-v2x4h	1,168.7		4,283	60.9	20
Xoodyak_XT-v7	1,118.6		2,489	88.4	43
KNOT-v2x2h	1,032.7		3,373	75.3	28
Gimli_GMU-v2	1,014.0		2,617	103.0	26
Gimli_GT-v6	1,008.0		**6,341**	31.5	8
Ascon_GMU2-v1h	1,006.3		2,928	110.1	14
Ascon_Graz-v4	989.6		3,379	61.9	16
Xoodyak_GMU-v1	936.2		3,172	74.0	43
Gimli_GT-v3	890.4		4,451	55.6	16
Ascon_Graz-v5	889.8		4,646	55.6	8
GIFT-COFB_GMU-v3	869.6	6	3,059	74.7	22
Ascon_Graz-v6	827.9		**5,346**	38.8	12
Ascon_Graz-v3	815.0		3,305	63.7	10
Gimli_GT-v2	812.8		2,852	76.2	24
GIFT-COFB_GMU-v4	812.7		3,311	57.1	18
GIFT-COFB_GMU-v5	777.9		3,821	36.5	12
Gimli_GT-v5	745.6		**5,738**	23.3	8
COMET_VT-v1	699.9		**5,266**	98.4	36
Ascon_Graz-v2	683.1		2,603	64.0	24
TinyJAMBU_TJT-v3	671.4	7	1,092	115.4	11
Elephant-v5	640.6	8	4,145	90.1	45
GIFT-COFB_GMU-v2	639.9		2,628	105.0	42
DryGASCON-v1	612.8	9	3,801	100.5	42
KNOT-v2x1	586.0		2,275	85.5	56
Ascon_VT-v1	543.4		3,130	84.9	20
KNOT-v2x1h	541.2		2,446	78.9	56
Gimli_GT-v7	526.4		**8,238**	16.4	8
Gimli_GMU-v1	522.4		2,328	102.0	50
Ascon_VT-v2	508.1		3,041	75.4	19
Saturnin-v2	499.4	10	3,648	79.0	81

Table 35 continued from previous page

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Ascon_Graz-v1	474.2		2,544	59.3	16
PHOTON-Beetle-v1	425.7	11	3,294	101.4	61
Romulus-v2	419.8	12	2,353	82.0	50
Gimli_GT-v1	417.3		2,537	78.2	48
AESGCM-v2	413.8	13*	**5,507**	106.7	66
Spook-v2-v2	410.7	14	3,662	77.0	96
Elephant-v2	408.4		3,073	85.5	67
SCHWAEMM-v1	399.6	15	4,685	66.3	85
Romulus-v3	397.2		3,847	45.0	29
SCHWAEMM-v2	384.2		**5,947**	63.8	85
Elephant-v4	367.6		3,157	97.6	85
Elephant-v3	357.9		2,901	88.3	79
GIFT-COFB_GMU-v1	332.3		2,727	106.5	82
SPIX-v1	317.0	16	2,432	69.3	28
GIFT-COFB_VT-v1	304.8		2,214	114.3	96
Romulus-v4	298.9		**5,086**	21.6	18.5
ISAP-v3	282.2		**5,703**	65.6	67
ACE_GMU-v1	263.9	17	2,784	74.2	36
ISAP-v1	262.6		**6,701**	61.1	67
ISAP-v4	238.9	18	3,623	67.2	36
Romulus-v1	224.0		1,998	80.5	92
Oribatida-v1	219.3	19	1,671	176.5	206
ESTATE-v1	211.4	20	2,855	109.0	132
ISAP-v2	207.1		**5,708**	68.0	42
SKINNY-AEAD-v1	199.1	21	3,174	101.1	130
SKINNY-AEAD-v2	193.8		3,182	98.4	130
TinyJAMBU_TJT-v2	174.5		689	125.4	46
COMET_CI-v3	167.9	22	3,443	80.0	122
TinyJAMBU_GMU-v1	166.4		720	124.8	48
COMET_VT-v2	164.0		2,353	111.5	174
COMET_CI-v1	159.3		3,255	80.9	130
Oribatida-v2	138.8		2,497	114.2	158
SPIX-v2x4	138.7		2,265	86.7	80
Elephant-v1	120.5		2,368	97.5	259
SpoC_IIT-v1	115.1	23	2,153	132.2	294
LOCUS-v2	103.1	24	2,950	72.5	90
ForkAE-v2	100.6	25	3,571	90.0	229
Pyjamask-v2	93.7	26	4,162	73.2	200
mixFeed-v1	90.5	27	3,479	38.9	110
TinyJAMBU_GMU-v2	89.3		908	128.3	92
SPIX-v2x2	88.5		2,107	80.2	116
Saturnin-v1	80.2		3,070	92.6	591
Xoodyak_GMU-v2	77.2		2,316	74.8	527
LOTUS-v2	74.9		2,208	52.7	90
SPIX-v2	60.7		2,078	89.2	188
SpoC_VT-v1	57.1		2,049	98.2	220
WAGE-v1	57.0	28	2,081	101.6	228
LOCUS-v1	54.6		2,857	73.0	171

Table 35 continued from previous page

Variant	Throughput AD+PT [Mbit/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Pyjamask-v1	45.6		3,897	92.7	520
ESTATE-v3	44.8		1,820	107.1	612
ESTATE-v2	43.6		1,689	115.4	678
COMET_CI-v2	43.0		1,974	94.3	561
LOTUS-v1	40.9		2,413	54.6	171
TinyJAMBU_TJT-v1	40.0		580	111.3	178
ACE_UW-v1	36.3		2,156	73.8	260
ESTATE-v4	14.5		1,329	118.1	2,088
Gimli_TUM-v1	12.7		1,767	78.0	1,575
Romulus-v5	10.0		1,961	76.5	1,964
Gimli_TUM-v2	6.4		1,767	73.5	2,955
TinyJAMBU_GMU-v3	4.9		1,277	108.1	1,412
ForkAE-v1	3.9		2,022	67.9	4,403
Gimli_TUM-v3	3.5		1,772	78.5	5,715

Table 36: Lattice ECP5 Hash Throughput for Long Messages

Variant	**Throughput HM [Mbit/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per Block**
Gimli_GMU-v4	1,735.9	1	3,223	94.9	7
Xoodyak_GMU2-v1	1,481.6	2	3,248	150.5	13
Gimli_GMU-v5	1,344.8		4,586	52.5	5
Gimli_GT-v4	1,295.6		4,027	60.7	6
Xoodyak_GMU2-v2	1,274.0		4,058	69.7	7
Gimli_GMU-v2	1,014.0		2,617	103.0	13
Gimli_GT-v6	1,008.0		**6,341**	31.5	4
SHA2-v1	927.4	3	2,001	117.7	65
Gimli_GT-v3	890.4		4,451	55.6	8
Xoodyak_XT-v8	829.7		4,121	71.3	11
Ascon_GMU2-v2h	815.7	4	3,764	89.2	7
Gimli_GT-v2	812.8		2,852	76.2	12
Ascon_GMU2-v3h	783.4		4,925	61.2	5
Gimli_GT-v5	745.6		**5,738**	23.3	4
Xoodyak_XT-v7	665.7		2,489	88.4	17
Saturnin-v2	612.8	5	3,648	79.0	33
DryGASCON-v1	612.8	6	3,801	100.5	21
Ascon_Graz-v5	593.2		4,646	55.6	6
Xoodyak_GMU-v1	557.2		3,172	74.0	17
Ascon_GMU2-v1h	541.8		2,928	110.1	13
Gimli_GT-v7	526.4		**8,238**	16.4	4
Gimli_GMU-v1	522.4		2,328	102.0	25
Ascon_Graz-v3	509.4		3,305	63.7	8
Ascon_Graz-v6	496.8		**5,346**	38.8	5
Ascon_Graz-v4	494.8		3,379	61.9	8
SHA3-v1	421.9	7	1,804	90.3	233
Gimli_GT-v1	417.3		2,537	78.2	24
KNOT-v2x4h	389.6	8	4,283	60.9	20
Subterranean_ST-v2	382.9	9	1,342	95.7	2
Ascon_VT-v2	321.8		3,041	75.4	15
Ascon_Graz-v2	292.8		2,603	64.0	14
Ascon_Graz-v1	271.0		2,544	59.3	14
ACE_GMU-v1	263.9	10	2,784	74.2	18
KNOT-v2x2h	241.0		3,373	75.3	40
SCHWAEMM-v2	240.1	11*	**5,947**	63.8	34
PHOTON-Beetle-v1	129.8	12	3,294	101.4	25
KNOT-v2x1h	126.3		2,446	78.9	80
Saturnin-v1	77.7		3,070	92.6	305
Xoodyak_GMU-v2	37.0		2,316	74.8	259
ACE_UW-v1	36.3		2,156	73.8	130
Gimli_TUM-v1	12.7		1,767	78.0	786
Gimli_TUM-v2	6.4		1,767	73.5	1,474
Gimli_TUM-v3	3.5		1,772	78.5	2,850

Table 37: Xilinx Artix-7 Encryption PT Throughput for 1536 Byte Messages

Variant	Through-put 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	8,636.4	91%	1	848	298	424
Ascon_GMU-v1	5,813.2	92%	2	2,410	246	520
Subterranean_ST-v2	5,392.0	89%		891	190	433
Xoodyak_GMU2-v2	4,960.1	91%	3	2,322	199	493
Xoodyak_GMU2-v1	4,325.6	93%		1,608	314	892
Gimli_GMU-v4	4,147.4	94%	4	2,357	242	717
Ascon_GMU-v2	4,118.4	94%		1,790	307	916
Ascon_GMU2-v2h	3,563.1	95%		2,126	234	807
Ascon_Graz-v4	3,144.5	95%		2,249	206	805
KNOT-v2x2	2,954.7	92%	5	1,873	233	969
GIFT-COFB_GMU-v4	2,901.7	96%	6	1,730	213	902
Ascon_GMU2-v3h	2,855.8	94%		2,493	142	611
KNOT-v2x2h	2,815.2	92%		2,112	222	969
Gimli_GT-v4	2,791.8	92%		2,510	142	625
GIFT-COFB_GMU-v3	2,786.6	96%		1,641	249	1,098
Gimli_GT-v5	2,771.9	89%		**3,907**	97	430
GIFT-COFB_GMU-v5	2,768.8	95%		2,051	137	608
Xoodyak_XT-v2	2,655.3	96%		2,025	188	870
GIFT-COFB_GMU-v6	2,645.2	94%		2,363	110	511
Gimli_GT-v6	2,612.6	90%		**3,937**	91	428
Xoodyak_XT-v8	2,556.5	96%		2,143	181	870
Ascon_Graz-v3	2,477.3	96%		2,142	201	997
Gimli_GMU-v2	2,437.0	95%		1,678	260	1,311
Ascon_GMU2-v1h	2,431.2	96%		1,375	276	1,395
KNOT-v2x4	2,309.2	95%		**2,797**	165	878
Ascon_Graz-v5	2,301.1	96%		**2,797**	150	801
Xoodyak_XT-v1	2,260.5	96%		1,355	234	1,272
Xoodyak_XT-v7	2,183.2	96%		1,392	226	1,272
Ascon_Graz-v2	2,179.3	96%		1,541	213	1,201
Gimli_GT-v3	1,958.3	93%		**2,678**	131	822
KNOT-v2x4h	1,917.4	95%		2,438	137	878
Gimli_GT-v7	1,899.3	90%		**5,347**	66	427
Gimli_GT-v2	1,765.5	95%		1,909	175	1,218
Xoodyak_GMU-v1	1,642.3	96%		1,808	170	1,272
KNOT-v2x1	1,607.2	93%		1,620	251	1,919
GIFT-COFB_GMU-v2	1,543.4	97%		1,380	261	2,078
Ascon_VT-v2	1,517.0	97%		1,928	219	1,774
KNOT-v2x1h	1,511.2	93%		1,684	236	1,919
Elephant-v5	1,503.1	95%		**2,645**	217	1,774
Ascon_Graz-v1	1,480.8	97%		1,465	191	1,585
Ascon_VT-v1	1,457.1	98%		1,913	233	1,965
DryGASCON-v1	1,414.9	98%	7	2,074	238	2,067
COMET_VT-v1	1,309.0	98%	8	2,449	209	1,962
Gimli_GMU-v1	1,253.9	96%		1,435	255	2,499
Spook-v2-v2	1,055.6	96%	9	2,033	206	2,398
Elephant-v4	957.8	96%	10	1,901	263	3,374
TinyJAMBU_TJT-v3	946.4	99%	11	576	240	3,116

Table 37 continued from previous page

Variant	Through-put 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Gimli_GT-v1	893.8	96%		1,747	175	2,406
Romulus-v3	855.8	98%	12	1,824	123	1,766
Romulus-v2	841.8	98%		1,280	214	3,124
GIFT-COFB_GMU-v1	800.3	97%		1,223	263	4,038
Saturnin-v2	742.7	94%	13	2,321	167	2,763
GIFT-COFB_VT-v1	731.9	98%		1,041	275	4,617
SCHWAEMM-v1	708.6	96%	14*	**3,071**	135	2,341
SCHWAEMM-v2	682.4	96%		**3,740**	130	2,341
PHOTON-Beetle-v1	680.3	99%	15	2,065	178	3,215
Elephant-v2	661.4	98%		1,884	181	3,363
Romulus-v4	655.7	97%		**2,602**	58	1,087
SPIX-v1	638.1	96%	16	1,533	156	3,004
Elephant-v3	616.4	98%		1,717	200	3,987
ISAP-v1	598.6	90%		**3,491**	193	3,962
ISAP-v3	581.2	90%	17	2,182	188	3,975
ACE_GMU-v1	491.9	97%	18	1,847	143	3,572
Romulus-v1	481.8	99%		953	229	5,840
ISAP-v2	456.5	93%		2,157	200	5,384
SKINNY-AEAD-v2	452.9	99%	19	2,337	240	6,511
SKINNY-AEAD-v1	452.9	99%		2,333	240	6,512
COMET_CI-v3	409.9	98%		1,841	215	6,446
COMET_CI-v1	400.8	98%		1,884	223	6,837
COMET_VT-v2	329.6	98%		1,703	234	8,725
mixFeed-v1	328.9	97%	20	1,343	151	5,641
ESTATE-v1	320.5	99%	21	1,351	222	8,512
TinyJAMBU_TJT-v2	302.3	99%		461	315	12,803
SPIX-v2x4	267.0	95%		1,332	176	8,099
Pyjamask-v2	255.0	95%	22	2,308	213	10,263
Oribatida-v1	255.0	99%	23	1,450	276	13,301
Oribatida-v2	250.0	99%		1,450	276	13,564
TinyJAMBU_GMU-v1	247.8	99%		591	266	13,189
ForkAE-v2	235.9	99%	24	2,466	228	11,878
LOCUS-v2	221.0	99%	25	1,628	209	11,619
Elephant-v1	210.8	98%		1,291	229	13,347
SpoC_IIT-v1	199.6	99%	26	1,512	235	14,468
SPIX-v2x2	195.5	95%		1,267	187	11,755
WAGE-v1	151.7	97%	27	1,150	279	22,600
LOTUS-v2	149.1	99%		1,487	141	11,619
Saturnin-v1	134.8	97%		1,725	215	19,593
SpoC_VT-v1	131.2	99%		1,079	230	21,545
TinyJAMBU_GMU-v2	128.7	99%		564	268	25,589
LOCUS-v1	120.3	99%		1,824	216	22,068
Xoodyak_GMU-v2	118.0	95%		1,234	168	17,495
SPIX-v2	117.4	95%		1,181	182	19,057
Pyjamask-v1	107.7	96%		1,979	229	26,131
ACE_UW-v1	95.4	97%		1,229	200	25,756
COMET_CI-v2	94.0	98%		1,096	222	29,031
ESTATE-v3	80.8	99%		1,130	259	39,392

Table 37 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
LOTUS-v1	80.7	99%		1,652	145	22,068
ESTATE-v2	75.4	99%		907	268	43,668
TinyJAMBU_TJT-v1	71.2	99%		446	290	50,030
Gimli_TUM-v1	37.9	97%		933	241	78,117
ESTATE-v4	25.3	99%		944	277	134,378
Romulus-v5	20.8	99%		887	214	126,575
Gimli_TUM-v2	20.4	97%		905	244	146,617
Gimli_TUM-v3	11.0	97%		838	253	283,617
TinyJAMBU_GMU-v3	8.6	99%		537	278	397,589
ForkAE-v1	8.3	100%		1,191	208	306,694
Minimum		**89%**				
Average		**96%**				
Maximum		**100%**				

Table 38: Xilinx Artix-7 Encryption PT Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	2,724.6	29%	1	848	298	56
Ascon_GMU-v1	2,099.2	33%	2	2,410	246	60
Ascon_GMU-v2	1,786.2	41%		1,790	307	88
Gimli_GMU-v4	1,697.3	38%	3	2,357	242	73
Ascon_GMU2-v2h	1,687.4	45%		2,126	234	71
Xoodyak_GMU2-v1	1,623.9	35%	4	1,608	314	99
Xoodyak_GMU2-v2	1,543.8	28%		2,322	199	66
Ascon_Graz-v4	1,528.6	46%		2,249	206	69
Subterranean_ST-v2	1,496.6	25%		891	190	65
GIFT-COFB_GMU-v3	1,482.4	51%	5	1,641	249	86
GIFT-COFB_GMU-v4	1,473.7	49%		1,730	213	74
Ascon_Graz-v3	1,336.5	52%		2,142	201	77
Ascon_GMU2-v1h	1,320.7	52%		1,375	276	107
Xoodyak_XT-v2	1,283.4	46%		2,025	188	75
GIFT-COFB_GMU-v5	1,252.6	43%		2,051	137	56
Xoodyak_XT-v8	1,235.6	46%		2,143	181	75
Ascon_GMU2-v3h	1,232.3	41%		2,493	142	59
Ascon_Graz-v5	1,181.5	49%		**2,797**	150	65
KNOT-v2x2	1,181.1	37%	6	1,873	233	101
KNOT-v2x4	1,173.3	48%		**2,797**	165	72
Gimli_GMU-v2	1,157.6	45%		1,678	260	115
KNOT-v2x2h	1,125.4	37%		2,112	222	101
Ascon_Graz-v2	1,124.3	49%		1,541	213	97
GIFT-COFB_GMU-v6	1,104.3	39%		2,363	110	51
Xoodyak_XT-v1	1,079.4	46%		1,355	234	111
Xoodyak_XT-v7	1,042.5	46%		1,392	226	111
Gimli_GT-v4	995.9	33%		2,510	142	73
KNOT-v2x4h	974.2	48%		2,438	137	72
Ascon_VT-v1	954.4	64%		1,913	233	125
Ascon_VT-v2	950.2	61%		1,928	219	118
GIFT-COFB_GMU-v2	915.3	58%		1,380	261	146
DryGASCON-v1	902.6	62%	7	2,074	238	135
COMET_VT-v1	877.1	66%	8	2,449	209	122
Ascon_Graz-v1	865.4	57%		1,465	191	113
Gimli_GT-v5	801.0	26%		**3,907**	97	62
Gimli_GT-v2	786.0	42%		1,909	175	114
Xoodyak_GMU-v1	784.1	46%		1,808	170	111
Gimli_GT-v3	779.9	37%		**2,678**	131	86
Gimli_GT-v6	776.5	27%		**3,937**	91	60
TinyJAMBU_TJT-v3	714.4	74%	9	576	240	172
KNOT-v2x1	702.3	41%		1,620	251	183
Elephant-v5	661.3	42%		**2,645**	217	168
KNOT-v2x1h	660.3	41%		1,684	236	183
Gimli_GMU-v1	656.1	50%		1,435	255	199
Romulus-v2	608.7	71%	10	1,280	214	180
Gimli_GT-v7	572.7	27%		**5,347**	66	59
Romulus-v3	572.5	65%		1,824	123	110

Table 38 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Spook-v2-v2	555.1	51%	11	2,033	206	190
PHOTON-Beetle-v1	509.1	74%	12	2,065	178	179
GIFT-COFB_GMU-v1	506.2	62%		1,223	263	266
GIFT-COFB_VT-v1	480.5	64%		1,041	275	293
Gimli_GT-v1	452.5	48%		1,747	175	198
Elephant-v4	437.2	44%	13	1,901	263	308
Elephant-v2	413.7	61%		1,884	181	224
Romulus-v4	395.9	59%		**2,602**	58	75
Elephant-v3	387.9	62%		1,717	200	264
SCHWAEMM-v1	386.1	53%	14*	**3,071**	135	179
SCHWAEMM-v2	371.8	53%		**3,740**	130	179
Romulus-v1	366.4	75%		953	229	320
SKINNY-AEAD-v2	354.1	77%	15	2,337	240	347
SKINNY-AEAD-v1	353.1	77%		2,333	240	348
SPIX-v1	327.3	49%	16	1,533	156	244
Saturnin-v2	306.5	39%	17	2,321	167	279
COMET_CI-v3	294.3	71%		1,841	215	374
COMET_CI-v1	287.6	71%		1,884	223	397
ACE_GMU-v1	281.6	55%	18	1,847	143	260
ESTATE-v1	273.2	85%	19	1,351	222	416
TinyJAMBU_TJT-v2	244.7	80%		461	315	659
COMET_VT-v2	223.1	66%		1,703	234	537
ForkAE-v2	207.7	88%	20	2,466	228	562
Oribatida-v1	202.7	79%	21	1,450	276	697
TinyJAMBU_GMU-v1	201.2	80%		591	266	677
mixFeed-v1	194.7	57%	22	1,343	151	397
ISAP-v1	189.3	29%		**3,491**	193	522
Oribatida-v2	187.4	74%		1,450	276	754
LOCUS-v2	184.8	83%	23	1,628	209	579
ISAP-v3	179.9	28%	24	2,182	188	535
ISAP-v2	171.0	35%		2,157	200	599
SpoC_IIT-v1	158.3	78%	25	1,512	235	760
Elephant-v1	135.7	63%		1,291	229	864
LOTUS-v2	124.7	83%		1,487	141	579
Pyjamask-v2	124.1	46%	26	2,308	213	879
SPIX-v2x4	121.9	43%		1,332	176	739
TinyJAMBU_GMU-v2	105.5	81%		564	268	1,301
SpoC_VT-v1	105.0	79%		1,079	230	1,121
LOCUS-v1	101.3	84%		1,824	216	1,092
SPIX-v2x2	88.4	43%		1,267	187	1,083
WAGE-v1	88.0	56%	27	1,150	279	1,624
Saturnin-v1	74.9	54%		1,725	215	1,469
ESTATE-v3	71.4	88%		1,130	259	1,856
LOTUS-v1	68.0	84%		1,652	145	1,092
COMET_CI-v2	66.6	70%		1,096	222	1,707
ESTATE-v2	65.8	87%		907	268	2,084
TinyJAMBU_TJT-v1	58.0	81%		446	290	2,558
Pyjamask-v1	57.8	52%		1,979	229	2,027

Table 38 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
ACE_UW-v1	55.8	57%		1,229	200	1,836
Xoodyak_GMU-v2	54.7	44%		1,234	168	1,572
SPIX-v2	52.9	43%		1,181	182	1,761
ESTATE-v4	22.5	88%		944	277	6,314
Gimli_TUM-v1	22.3	57%		933	241	5,529
Romulus-v5	16.6	79%		887	214	6,607
Gimli_TUM-v2	12.1	57%		905	244	10,365
ForkAE-v1	8.3	99%		1,191	208	12,846
TinyJAMBU_GMU-v3	7.1	82%		537	278	20,021
Gimli_TUM-v3	6.5	57%		838	253	20,037
Minimum		**25%**				
Average		**56%**				
Maximum		**99%**				

Table 39: Xilinx Artix-7 Encryption PT Throughput for 16 Byte Messages

Variant	Throughput 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	866.9	9%	1	848	298	44
Ascon_GMU-v1	699.7	11%	2	2,410	246	45
Ascon_GMU-v2	644.2	15%		1,790	307	61
Ascon_GMU2-v2h	637.3	17%		2,126	234	47
GIFT-COFB_GMU-v3	601.4	21%	3	1,641	249	53
Gimli_GMU-v4	595.7	13%	4	2,357	242	52
Ascon_Graz-v4	586.0	18%		2,249	206	45
GIFT-COFB_GMU-v4	580.1	19%		1,730	213	47
Xoodyak_GMU2-v1	550.6	12%	5	1,608	314	73
Ascon_Graz-v3	547.4	21%		2,142	201	47
Ascon_GMU2-v1h	543.5	22%		1,375	276	65
Xoodyak_XT-v2	491.1	18%		2,025	188	49
Xoodyak_GMU2-v2	489.8	9%		2,322	199	52
Xoodyak_XT-v8	472.8	18%		2,143	181	49
Ascon_Graz-v5	468.3	20%		**2,797**	150	41
GIFT-COFB_GMU-v5	461.5	16%		2,051	137	38
KNOT-v2x4	459.1	19%		**2,797**	165	46
Subterranean_ST-v2	458.9	8%		891	190	53
Ascon_VT-v1	458.8	31%		1,913	233	65
Ascon_Graz-v2	447.0	20%		1,541	213	61
Ascon_GMU2-v3h	443.3	15%		2,493	142	41
Ascon_VT-v2	438.0	28%		1,928	219	64
Gimli_GMU-v2	437.9	17%		1,678	260	76
COMET_VT-v1	431.5	32%	6	2,449	209	62
DryGASCON-v1	423.1	29%	7	2,074	238	72
Xoodyak_XT-v1	410.3	17%		1,355	234	73
KNOT-v2x2	408.5	13%	8	1,873	233	73
TinyJAMBU_TJT-v3	404.2	42%	9	576	240	76
GIFT-COFB_GMU-v2	402.5	25%		1,380	261	83
Xoodyak_XT-v7	396.3	17%		1,392	226	73
GIFT-COFB_GMU-v6	391.1	14%		2,363	110	36
KNOT-v2x2h	389.3	13%		2,112	222	73
KNOT-v2x4h	381.2	19%		2,438	137	46
Ascon_Graz-v1	376.1	25%		1,465	191	65
Gimli_GT-v4	330.5	11%		2,510	142	55
Romulus-v2	326.1	38%	10	1,280	214	84
Xoodyak_GMU-v1	298.1	17%		1,808	170	73
Gimli_GT-v2	287.2	15%		1,909	175	78
PHOTON-Beetle-v1	284.8	41%	11	2,065	178	80
Romulus-v3	281.1	32%		1,824	123	56
Elephant-v5	272.3	17%		**2,645**	217	102
Gimli_GT-v3	270.5	13%		**2,678**	131	62
Gimli_GMU-v1	263.2	20%		1,435	255	124
KNOT-v2x1	253.0	15%		1,620	251	127
Gimli_GT-v5	248.3	8%		**3,907**	97	50
Elephant-v2	243.9	36%	12	1,884	181	95
Gimli_GT-v6	242.7	8%		**3,937**	91	48

Table 39 continued from previous page

Variant	Through-put 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
KNOT-v2x1h	237.9	15%		1,684	236	127
GIFT-COFB_GMU-v1	235.4	29%		1,223	263	143
GIFT-COFB_VT-v1	231.6	31%		1,041	275	152
Elephant-v3	230.6	37%		1,717	200	111
SKINNY-AEAD-v2	210.4	46%	13	2,337	240	146
Romulus-v1	209.4	43%		953	229	140
SKINNY-AEAD-v1	209.0	46%		2,333	240	147
ESTATE-v1	186.9	58%	14	1,351	222	152
Spook-v2-v2	185.7	17%	15	2,033	206	142
Elephant-v4	185.0	18%		1,901	263	182
Gimli_GT-v7	179.7	9%		**5,347**	66	47
Gimli_GT-v1	177.8	19%		1,747	175	126
Romulus-v4	176.8	26%		**2,602**	58	42
COMET_CI-v3	156.4	38%		1,841	215	176
TinyJAMBU_TJT-v2	153.3	50%		461	315	263
COMET_CI-v1	152.6	37%		1,884	223	187
ForkAE-v2	151.2	64%	16	2,466	228	193
SCHWAEMM-v1	135.0	18%	17*	**3,071**	135	128
SCHWAEMM-v2	130.0	18%		**3,740**	130	128
SPIX-v1	129.7	19%	18	1,533	156	154
TinyJAMBU_GMU-v1	126.6	51%		591	266	269
Oribatida-v1	123.5	48%	19	1,450	276	286
LOCUS-v2	122.2	55%	20	1,628	209	219
ACE_GMU-v1	120.4	24%	21	1,847	143	152
Saturnin-v2	117.5	15%	22	2,321	167	182
COMET_VT-v2	110.9	33%		1,703	234	270
Oribatida-v2	105.8	42%		1,450	276	334
SpoC_IIT-v1	96.1	48%	23	1,512	235	313
mixFeed-v1	85.5	25%	24	1,343	151	226
Elephant-v1	83.5	39%		1,291	229	351
LOTUS-v2	82.4	55%		1,487	141	219
LOCUS-v1	67.8	56%		1,824	216	408
TinyJAMBU_GMU-v2	67.4	52%		564	268	509
SpoC_VT-v1	64.7	49%		1,079	230	455
ISAP-v1	61.5	9%		**3,491**	193	402
ISAP-v3	58.0	9%	25	2,182	188	415
ISAP-v2	57.8	12%		2,157	200	443
ESTATE-v3	52.5	65%		1,130	259	632
Pyjamask-v2	47.6	18%	26	2,308	213	573
ESTATE-v2	47.1	62%		907	268	728
LOTUS-v1	45.5	56%		1,652	145	408
SPIX-v2x4	45.1	16%		1,332	176	499
WAGE-v1	38.0	24%	27	1,150	279	940
TinyJAMBU_TJT-v1	36.8	51%		446	290	1,010
COMET_CI-v2	34.8	36%		1,096	222	816
SPIX-v2x2	32.6	16%		1,267	187	735
Saturnin-v1	31.9	23%		1,725	215	862
ACE_UW-v1	24.2	25%		1,229	200	1,056

Table 39 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Pyjamask-v1	23.6	21%		1,979	229	1,241
Xoodyak_GMU-v2	20.5	17%		1,234	168	1,050
SPIX-v2	19.5	16%		1,181	182	1,197
ESTATE-v4	16.6	65%		944	277	2,138
Romulus-v5	10.2	48%		887	214	2,695
Gimli_TUM-v1	9.8	25%		933	241	3,162
ForkAE-v1	8.2	98%		1,191	208	3,264
Gimli_TUM-v2	5.3	25%		905	244	5,922
TinyJAMBU_GMU-v3	4.6	53%		537	278	7,709
Gimli_TUM-v3	2.8	25%		838	253	11,442
Minimum		**8%**				
Average		**28%**				
Maximum		**98%**				

Table 40: Xilinx Artix-7 Encryption AD Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	8,636.4	91%	1	848	298	424
Xoodyak_GMU2-v1	7,492.1	88%	2	1,608	314	515
Ascon_GMU-v1	5,813.2	92%	3	2,410	246	520
Subterranean_ST-v2	5,404.4	89%		891	190	432
Xoodyak_GMU2-v2	5,315.9	91%		2,322	199	460
Gimli_GMU-v4	4,147.4	94%	4	2,357	242	717
Ascon_GMU-v2	4,104.9	94%		1,790	307	919
KNOT-v2x4	4,055.0	90%		**2,797**	165	500
Ascon_GMU2-v2h	3,563.1	95%		2,126	234	807
Xoodyak_XT-v2	3,468.7	94%		2,025	188	666
KNOT-v2x4h	3,366.9	90%	5	2,438	137	500
Xoodyak_XT-v8	3,339.5	94%		2,143	181	666
Xoodyak_XT-v1	3,216.3	94%		1,355	234	894
Ascon_Graz-v4	3,129.0	95%		2,249	206	809
Xoodyak_XT-v7	3,106.4	94%		1,392	226	894
GIFT-COFB_GMU-v4	2,924.4	97%	6	1,730	213	895
KNOT-v2x2	2,915.6	91%		1,873	233	982
Ascon_GMU2-v3h	2,860.5	94%		2,493	142	610
GIFT-COFB_GMU-v3	2,809.7	97%		1,641	249	1,089
Gimli_GT-v4	2,796.3	92%		2,510	142	624
GIFT-COFB_GMU-v5	2,787.2	95%		2,051	137	604
KNOT-v2x2h	2,777.9	91%		2,112	222	982
Gimli_GT-v5	2,771.9	89%		**3,907**	97	430
GIFT-COFB_GMU-v6	2,660.8	94%		2,363	110	508
Gimli_GT-v6	2,612.6	90%		**3,937**	91	428
Ascon_Graz-v3	2,469.9	96%		2,142	201	1,000
TinyJAMBU_TJT-v3	2,467.9	96%	7	576	240	1,195
Gimli_GMU-v2	2,437.0	95%		1,678	260	1,311
Ascon_GMU2-v1h	2,426.0	96%		1,375	276	1,398
Xoodyak_GMU-v1	2,334.0	94%		1,808	170	895
Ascon_Graz-v5	2,295.4	96%		**2,797**	150	803
Ascon_Graz-v2	2,164.9	95%		1,541	213	1,209
Gimli_GT-v3	1,958.3	93%		**2,678**	131	822
Gimli_GT-v7	1,903.8	90%		**5,347**	66	426
Gimli_GT-v2	1,765.5	95%		1,909	175	1,218
COMET_VT-v1	1,627.5	97%	8	2,449	209	1,578
KNOT-v2x1	1,584.9	92%		1,620	251	1,946
GIFT-COFB_GMU-v2	1,557.6	98%		1,380	261	2,059
KNOT-v2x1h	1,490.2	92%		1,684	236	1,946
Ascon_Graz-v1	1,475.2	97%		1,465	191	1,591
Romulus-v2	1,451.2	95%	9	1,280	214	1,812
Ascon_VT-v1	1,451.1	97%		1,913	233	1,973
Elephant-v5	1,423.6	94%		**2,645**	217	1,873
DryGASCON-v1	1,414.9	98%	10	2,074	238	2,067
Saturnin-v2	1,414.3	89%	11	2,321	167	1,451
Ascon_VT-v2	1,363.9	97%		1,928	219	1,973
Romulus-v3	1,359.2	95%		1,824	123	1,112

Table 40 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Gimli_GMU-v1	1,253.9	96%		1,435	255	2,499
Elephant-v2	1,144.7	95%	12	1,884	181	1,943
Elephant-v3	1,084.1	95%		1,717	200	2,267
Spook-v2-v2	1,055.6	96%	13	2,033	206	2,398
ISAP-v1	1,003.2	90%		**3,491**	193	2,364
ISAP-v3	971.9	90%	14	2,182	188	2,377
Romulus-v4	935.3	94%		**2,602**	58	762
Elephant-v4	925.2	95%		1,901	263	3,493
Gimli_GT-v1	893.8	96%		1,747	175	2,406
Romulus-v1	876.1	96%		953	229	3,212
SCHWAEMM-v1	869.0	96%	15*	**3,071**	135	1,909
SCHWAEMM-v2	836.8	96%		**3,740**	130	1,909
GIFT-COFB_GMU-v1	808.1	98%		1,223	263	3,999
PHOTON-Beetle-v1	799.1	98%	16	2,065	178	2,737
TinyJAMBU_TJT-v2	755.7	97%		461	315	5,122
ISAP-v2	741.8	93%		2,157	200	3,313
SPIX-v1	728.6	95%	17	1,533	156	2,631
GIFT-COFB_VT-v1	709.3	99%		1,041	275	4,764
ESTATE-v1	636.9	99%	18	1,351	222	4,283
TinyJAMBU_GMU-v1	593.4	98%		591	266	5,508
Oribatida-v1	495.8	97%	19	1,450	276	6,841
ACE_GMU-v1	489.7	96%	20	1,847	143	3,588
Oribatida-v2	487.3	97%		1,450	276	6,960
COMET_CI-v3	481.6	98%		1,841	215	5,486
SKINNY-AEAD-v2	481.5	99%	21	2,337	240	6,125
SKINNY-AEAD-v1	481.4	99%		2,333	240	6,126
COMET_CI-v1	466.3	98%		1,884	223	5,877
LOCUS-v2	438.3	98%	22	1,628	209	5,859
Elephant-v1	394.8	95%		1,291	229	7,127
mixFeed-v1	353.0	97%	23	1,343	151	5,256
COMET_VT-v2	344.7	98%		1,703	234	8,341
TinyJAMBU_GMU-v2	322.0	98%		564	268	10,228
LOTUS-v2	295.7	98%		1,487	141	5,859
ForkAE-v2	273.6	99%	24	2,466	228	10,239
SPIX-v2x4	265.8	94%		1,332	176	8,137
Pyjamask-v2	264.7	95%	25	2,308	213	9,887
Saturnin-v1	261.0	93%		1,725	215	10,121
LOCUS-v1	238.6	98%		1,824	216	11,124
SpoC_IIT-v1	205.0	99%	26	1,512	235	14,084
Xoodyak_GMU-v2	204.4	92%		1,234	168	10,100
SPIX-v2x2	194.6	94%		1,267	187	11,811
TinyJAMBU_TJT-v1	184.6	97%		446	290	19,306
ESTATE-v3	160.7	99%		1,130	259	19,803
LOTUS-v1	160.2	98%		1,652	145	11,124
WAGE-v1	150.9	96%	27	1,150	279	22,713
ESTATE-v2	149.9	99%		907	268	21,967
SpoC_VT-v1	133.6	99%		1,079	230	21,161
SPIX-v2	116.8	94%		1,181	182	19,149

Table 40 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Pyjamask-v1	109.3	96%		1,979	229	25,755
COMET_CI-v2	105.5	98%		1,096	222	25,863
ACE_UW-v1	94.9	96%		1,229	200	25,885
ESTATE-v4	50.4	99%		944	277	67,557
Romulus-v5	39.8	96%		887	214	66,055
Gimli_TUM-v1	38.1	97%		933	241	77,829
TinyJAMBU_GMU-v3	22.5	98%		537	278	151,828
ForkAE-v1	22.0	100%		1,191	208	116,127
Gimli_TUM-v2	20.5	97%		905	244	145,945
Gimli_TUM-v3	11.0	97%		838	253	282,177
Minimum		**88%**				
Average		**95%**				
Maximum		**100%**				

Table 41: Xilinx Artix-7 Encryption AD Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	2,724.6	29%	1	848	298	56
Ascon_GMU-v1	2,099.2	33%	2	2,410	246	60
Xoodyak_GMU2-v1	1,869.4	22%	3	1,608	314	86
Ascon_GMU-v2	1,727.3	40%		1,790	307	91
Gimli_GMU-v4	1,697.3	38%	4	2,357	242	73
Ascon_GMU2-v2h	1,687.4	45%		2,126	234	71
GIFT-COFB_GMU-v3	1,655.7	57%	5	1,641	249	77
GIFT-COFB_GMU-v4	1,627.7	54%		1,730	213	67
Xoodyak_GMU2-v2	1,592.0	27%		2,322	199	64
Subterranean_ST-v2	1,520.0	25%		891	190	64
Ascon_Graz-v4	1,444.8	44%		2,249	206	73
Xoodyak_XT-v2	1,436.7	39%		2,025	188	67
Xoodyak_XT-v8	1,383.2	39%		2,143	181	67
TinyJAMBU_TJT-v3	1,350.3	53%	6	576	240	91
GIFT-COFB_GMU-v5	1,348.9	46%		2,051	137	52
Ascon_Graz-v3	1,286.4	50%		2,142	201	80
Ascon_GMU2-v1h	1,284.7	51%		1,375	276	110
KNOT-v2x4	1,280.0	28%		**2,797**	165	66
Ascon_GMU2-v3h	1,253.5	41%		2,493	142	58
Xoodyak_XT-v1	1,235.1	36%		1,355	234	97
Xoodyak_XT-v7	1,192.9	36%		1,392	226	97
GIFT-COFB_GMU-v6	1,173.3	42%		2,363	110	48
Gimli_GMU-v2	1,157.6	45%		1,678	260	115
Ascon_Graz-v5	1,146.3	48%		**2,797**	150	67
KNOT-v2x4h	1,062.8	28%	7	2,438	137	66
GIFT-COFB_GMU-v2	1,052.2	66%		1,380	261	127
KNOT-v2x2	1,046.5	33%		1,873	233	114
Ascon_Graz-v2	1,038.6	46%		1,541	213	105
Gimli_GT-v4	1,009.8	33%		2,510	142	72
COMET_VT-v1	1,009.5	60%	8	2,449	209	106
KNOT-v2x2h	997.1	33%		2,112	222	114
DryGASCON-v1	902.6	62%	9	2,074	238	135
Ascon_VT-v1	897.0	60%		1,913	233	133
Xoodyak_GMU-v1	888.2	36%		1,808	170	98
Ascon_VT-v2	843.1	60%		1,928	219	133
Ascon_Graz-v1	821.8	54%		1,465	191	119
Gimli_GT-v5	801.0	26%		**3,907**	97	62
Gimli_GT-v2	786.0	42%		1,909	175	114
Gimli_GT-v3	779.9	37%		**2,678**	131	86
Gimli_GT-v6	776.5	27%		**3,937**	91	60
Romulus-v2	702.4	46%	10	1,280	214	156
Gimli_GMU-v1	656.1	50%		1,435	255	199
Elephant-v5	649.7	43%		**2,645**	217	171
Romulus-v3	629.8	44%		1,824	123	100
KNOT-v2x1	612.0	36%		1,620	251	210
GIFT-COFB_GMU-v1	593.2	72%		1,223	263	227
Gimli_GT-v7	582.6	28%		**5,347**	66	58

Table 41 continued from previous page

Variant	Through-put 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
KNOT-v2x1h	575.4	36%		1,684	236	210
PHOTON-Beetle-v1	566.1	70%	11	2,065	178	161
Spook-v2-v2	555.1	51%	12	2,033	206	190
Elephant-v2	554.9	46%	13	1,884	181	167
GIFT-COFB_VT-v1	550.0	77%		1,041	275	256
Elephant-v3	525.1	46%		1,717	200	195
ESTATE-v1	483.7	75%	14	1,351	222	235
TinyJAMBU_TJT-v2	477.2	62%		461	315	338
Gimli_GT-v1	452.5	48%		1,747	175	198
Romulus-v1	437.5	48%		953	229	268
Elephant-v4	433.0	44%		1,901	263	311
SCHWAEMM-v1	429.3	47%	15*	**3,071**	135	161
SCHWAEMM-v2	413.4	47%		**3,740**	130	161
Romulus-v4	412.4	42%		**2,602**	58	72
Saturnin-v2	409.1	26%	16	2,321	167	209
TinyJAMBU_GMU-v1	382.6	63%		591	266	356
SKINNY-AEAD-v2	373.5	77%	17	2,337	240	329
SKINNY-AEAD-v1	372.4	76%		2,333	240	330
SPIX-v1	334.2	44%	18	1,533	156	239
COMET_CI-v3	329.6	67%		1,841	215	334
COMET_CI-v1	319.8	67%		1,884	223	357
LOCUS-v2	315.7	71%	19	1,628	209	339
ISAP-v1	312.7	28%		**3,491**	193	316
ISAP-v3	292.6	27%	20	2,182	188	329
Oribatida-v1	286.6	56%	21	1,450	276	493
Oribatida-v2	286.1	57%		1,450	276	494
ISAP-v2	277.5	35%		2,157	200	369
ACE_GMU-v1	265.3	52%	22	1,847	143	276
ForkAE-v2	239.7	87%	23	2,466	228	487
COMET_VT-v2	230.0	65%		1,703	234	521
LOTUS-v2	213.0	71%		1,487	141	339
TinyJAMBU_GMU-v2	207.9	63%		564	268	660
mixFeed-v1	203.5	56%	24	1,343	151	380
Elephant-v1	190.6	46%		1,291	229	615
LOCUS-v1	173.9	72%		1,824	216	636
SpoC_IIT-v1	161.7	78%	25	1,512	235	744
ESTATE-v3	128.1	79%		1,130	259	1,035
Pyjamask-v2	125.2	45%	26	2,308	213	871
ESTATE-v2	116.8	77%		907	268	1,175
LOTUS-v1	116.7	72%		1,652	145	636
TinyJAMBU_TJT-v1	116.5	62%		446	290	1,274
SPIX-v2x4	116.0	41%		1,332	176	777
SpoC_VT-v1	106.6	79%		1,079	230	1,105
Saturnin-v1	103.9	37%		1,725	215	1,059
SPIX-v2x2	84.1	41%		1,267	187	1,139
WAGE-v1	82.2	53%	27	1,150	279	1,737
COMET_CI-v2	72.2	67%		1,096	222	1,575
Xoodyak_GMU-v2	65.3	29%		1,234	168	1,317

Table 41 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Pyjamask-v1	58.1	51%		1,979	229	2,019
ACE_UW-v1	52.1	53%		1,229	200	1,965
SPIX-v2	50.3	41%		1,181	182	1,853
ESTATE-v4	40.2	79%		944	277	3,525
Gimli_TUM-v1	22.4	57%		933	241	5,517
ForkAE-v1	21.7	99%		1,191	208	4,899
Romulus-v5	20.5	49%		887	214	5,335
TinyJAMBU_GMU-v3	14.6	63%		537	278	9,780
Gimli_TUM-v2	12.1	57%		905	244	10,337
Gimli_TUM-v3	6.5	57%		838	253	19,977
Minimum		**22%**				
Average		**50%**				
Maximum		**99%**				

Table 42: Xilinx Artix-7 Encryption AD Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	866.9	9%	1	848	298	44
GIFT-COFB_GMU-v3	724.4	25%	2	1,641	249	44
Ascon_GMU-v1	699.7	11%	3	2,410	246	45
GIFT-COFB_GMU-v4	681.6	22%		1,730	213	40
Ascon_GMU2-v2h	637.3	17%		2,126	234	47
Ascon_GMU-v2	614.0	14%		1,790	307	64
Gimli_GMU-v4	595.7	13%	4	2,357	242	52
TinyJAMBU_TJT-v3	558.5	22%	5	576	240	55
Xoodyak_GMU2-v1	550.6	6%	6	1,608	314	73
Ascon_Graz-v4	538.1	16%		2,249	206	49
GIFT-COFB_GMU-v2	522.0	33%		1,380	261	64
Ascon_GMU2-v1h	519.5	21%		1,375	276	68
GIFT-COFB_GMU-v5	515.8	18%		2,051	137	34
Ascon_Graz-v3	514.6	20%		2,142	201	50
Xoodyak_XT-v2	501.3	14%		2,025	188	48
Xoodyak_GMU2-v2	489.8	8%		2,322	199	52
Xoodyak_XT-v8	482.7	14%		2,143	181	48
Subterranean_ST-v2	467.7	8%		891	190	52
COMET_VT-v1	461.2	28%	7	2,449	209	58
Ascon_GMU2-v3h	454.4	15%		2,493	142	40
Ascon_Graz-v5	446.5	19%		**2,797**	150	43
Gimli_GMU-v2	437.9	17%		1,678	260	76
GIFT-COFB_GMU-v6	426.7	15%		2,363	110	33
DryGASCON-v1	423.1	29%	8	2,074	238	72
Xoodyak_XT-v1	416.0	12%		1,355	234	72
Ascon_VT-v1	408.5	27%		1,913	233	73
KNOT-v2x4	406.2	9%		**2,797**	165	52
Xoodyak_XT-v7	401.8	12%		1,392	226	72
Ascon_Graz-v2	395.1	17%		1,541	213	69
Ascon_VT-v2	384.0	27%		1,928	219	73
KNOT-v2x2	346.8	11%	9	1,873	233	86
Ascon_Graz-v1	344.3	23%		1,465	191	71
KNOT-v2x4h	337.2	9%		2,438	137	52
Gimli_GT-v4	336.6	11%		2,510	142	54
KNOT-v2x2h	330.4	11%		2,112	222	86
Romulus-v2	326.1	21%	10	1,280	214	84
GIFT-COFB_GMU-v1	323.7	39%		1,223	263	104
GIFT-COFB_VT-v1	322.9	45%		1,041	275	109
Xoodyak_GMU-v1	298.1	12%		1,808	170	73
PHOTON-Beetle-v1	295.9	36%	11	2,065	178	77
Gimli_GT-v2	287.2	15%		1,909	175	78
Romulus-v3	281.1	20%		1,824	123	56
ESTATE-v1	275.9	43%	12	1,351	222	103
Gimli_GT-v3	270.5	13%		**2,678**	131	62
Gimli_GMU-v1	263.2	20%		1,435	255	124
Gimli_GT-v5	248.3	8%		**3,907**	97	50
Gimli_GT-v6	242.7	8%		**3,937**	91	48

Table 42 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Elephant-v5	222.2	15%		**2,645**	217	125
TinyJAMBU_TJT-v2	221.5	29%		461	315	182
SKINNY-AEAD-v2	219.4	45%	13	2,337	240	140
SKINNY-AEAD-v1	217.9	45%		2,333	240	141
Romulus-v1	209.4	23%		953	229	140
KNOT-v2x1	208.6	12%		1,620	251	154
KNOT-v2x1h	196.2	12%		1,684	236	154
Elephant-v2	194.7	16%	14	1,884	181	119
Spook-v2-v2	185.7	17%	15	2,033	206	142
Elephant-v3	184.2	16%		1,717	200	139
Gimli_GT-v7	183.7	9%		**5,347**	66	46
TinyJAMBU_GMU-v1	181.1	30%		591	266	188
Gimli_GT-v1	177.8	19%		1,747	175	126
Romulus-v4	176.8	18%		**2,602**	58	42
ForkAE-v2	172.7	63%	16	2,466	228	169
LOCUS-v2	168.3	38%	17	1,628	209	159
COMET_CI-v3	165.8	34%		1,841	215	166
COMET_CI-v1	161.3	34%		1,884	223	177
Elephant-v4	149.6	15%		1,901	263	225
SCHWAEMM-v1	140.5	15%	18*	**3,071**	135	123
Saturnin-v2	137.9	9%	19	2,321	167	155
SCHWAEMM-v2	135.3	15%		**3,740**	130	123
Oribatida-v2	125.3	25%	20	1,450	276	282
SPIX-v1	124.0	16%	21	1,533	156	161
Oribatida-v1	123.5	24%		1,450	276	286
LOTUS-v2	113.5	38%		1,487	141	159
COMET_VT-v2	112.6	32%		1,703	234	266
ACE_GMU-v1	109.0	21%	22	1,847	143	168
ISAP-v1	101.2	9%		**3,491**	193	244
TinyJAMBU_GMU-v2	98.6	30%		564	268	348
SpoC_IIT-v1	97.3	47%	23	1,512	235	309
LOCUS-v1	94.0	39%		1,824	216	294
ISAP-v2	93.8	12%	24	2,157	200	273
ISAP-v3	93.6	9%		2,182	188	257
mixFeed-v1	87.5	24%	25	1,343	151	221
ESTATE-v3	78.4	48%		1,130	259	423
ESTATE-v2	69.0	45%		907	268	497
Elephant-v1	66.8	16%		1,291	229	439
SpoC_VT-v1	65.3	48%		1,079	230	451
LOTUS-v1	63.1	39%		1,652	145	294
TinyJAMBU_TJT-v1	54.1	29%		446	290	686
Pyjamask-v2	47.3	17%	26	2,308	213	577
SPIX-v2x4	42.0	15%		1,332	176	537
Saturnin-v1	41.4	15%		1,725	215	665
COMET_CI-v2	36.3	34%		1,096	222	783
WAGE-v1	33.9	22%	27	1,150	279	1,053
SPIX-v2x2	30.3	15%		1,267	187	791
ESTATE-v4	24.7	48%		944	277	1,437

Table 42 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Pyjamask-v1	23.5	21%		1,979	229	1,245
ACE_UW-v1	21.6	22%		1,229	200	1,185
ForkAE-v1	20.9	95%		1,191	208	1,272
Xoodyak_GMU-v2	20.5	9%		1,234	168	1,050
SPIX-v2	18.1	15%		1,181	182	1,289
Romulus-v5	10.2	24%		887	214	2,695
Gimli_TUM-v1	9.8	25%		933	241	3,159
TinyJAMBU_GMU-v3	6.9	30%		537	278	5,148
Gimli_TUM-v2	5.3	25%		905	244	5,915
Gimli_TUM-v3	2.8	25%		838	253	11,427
Minimum		**6%**				
Average		**23%**				
Maximum		**95%**				

Table 43: Xilinx Artix-7 Encryption AD+PT Throughput for 1536 Byte Messages

Variant	Through-put 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	4,526.4	47%	1	848	298	809
Ascon_GMU-v1	3,022.8	48%	2	2,410	246	1,000
Xoodyak_GMU2-v1	2,892.4	44%	3	1,608	314	1,334
Subterranean_ST-v2	2,861.2	47%		891	190	816
Xoodyak_GMU2-v2	2,714.0	48%		2,322	199	901
Gimli_GMU-v4	2,140.9	48%	4	2,357	242	1,389
Ascon_GMU-v2	2,115.8	48%		1,790	307	1,783
Ascon_GMU2-v2h	1,825.6	49%		2,126	234	1,575
Ascon_Graz-v4	1,605.2	49%		2,249	206	1,577
Xoodyak_XT-v2	1,549.4	47%		2,025	188	1,491
KNOT-v2x2	1,523.7	48%	5	1,873	233	1,879
KNOT-v2x4	1,521.0	48%		**2,797**	165	1,333
Xoodyak_XT-v8	1,491.7	47%		2,143	181	1,491
GIFT-COFB_GMU-v4	1,489.7	49%	6	1,730	213	1,757
Ascon_GMU2-v3h	1,470.0	49%		2,493	142	1,187
Gimli_GT-v5	1,466.1	47%		**3,907**	97	813
Gimli_GT-v4	1,454.1	48%		2,510	142	1,200
KNOT-v2x2h	1,451.8	48%		2,112	222	1,879
GIFT-COFB_GMU-v5	1,429.1	49%		2,051	137	1,178
GIFT-COFB_GMU-v3	1,427.8	49%		1,641	249	2,143
Gimli_GT-v6	1,380.5	47%		**3,937**	91	810
Xoodyak_XT-v1	1,371.2	46%		1,355	234	2,097
GIFT-COFB_GMU-v6	1,369.5	49%		2,363	110	987
Xoodyak_XT-v7	1,324.3	46%		1,392	226	2,097
KNOT-v2x4h	1,262.9	48%		2,438	137	1,333
Ascon_Graz-v3	1,260.1	49%		2,142	201	1,960
Gimli_GMU-v2	1,248.5	49%		1,678	260	2,559
Ascon_GMU2-v1h	1,236.9	49%		1,375	276	2,742
Ascon_Graz-v5	1,173.3	49%		**2,797**	150	1,571
Ascon_Graz-v2	1,108.6	49%		1,541	213	2,361
Gimli_GT-v3	1,012.4	48%		**2,678**	131	1,590
Gimli_GT-v7	1,003.7	48%		**5,347**	66	808
Xoodyak_GMU-v1	996.2	46%		1,808	170	2,097
Gimli_GT-v2	907.3	49%		1,909	175	2,370
KNOT-v2x1	824.9	48%		1,620	251	3,739
GIFT-COFB_GMU-v2	787.4	49%		1,380	261	4,073
KNOT-v2x1h	775.6	48%		1,684	236	3,739
Elephant-v5	752.2	49%		**2,645**	217	3,545
Ascon_Graz-v1	752.0	49%		1,465	191	3,121
Ascon_VT-v1	735.4	49%		1,913	233	3,893
COMET_VT-v1	734.2	49%	7	2,449	209	3,498
Ascon_VT-v2	726.9	49%		1,928	219	3,702
DryGASCON-v1	716.3	49%	8	2,074	238	4,083
TinyJAMBU_TJT-v3	691.1	49%	9	576	240	4,267
Gimli_GMU-v1	639.6	49%		1,435	255	4,899
Romulus-v2	542.0	49%	10	1,280	214	4,852
Spook-v2-v2	538.4	49%	11	2,033	206	4,702

Table 43 continued from previous page

Variant	Through-put 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Romulus-v3	535.6	49%		1,824	123	2,822
Saturnin-v2	505.6	48%	12	2,321	167	4,059
Elephant-v4	483.4	49%	13	1,901	263	6,685
Gimli_GT-v1	456.6	49%		1,747	175	4,710
Elephant-v2	426.8	49%		1,884	181	5,211
GIFT-COFB_GMU-v1	407.4	50%		1,223	263	7,933
Elephant-v3	400.1	49%		1,717	200	6,143
SCHWAEMM-v1	396.8	49%	14*	**3,071**	135	4,181
Romulus-v4	394.4	49%		**2,602**	58	1,807
ISAP-v1	389.4	47%		**3,491**	193	6,091
SCHWAEMM-v2	382.1	49%		**3,740**	130	4,181
ISAP-v3	378.5	47%	15	2,182	188	6,104
PHOTON-Beetle-v1	370.4	50%	16	2,065	178	5,905
GIFT-COFB_VT-v1	364.3	50%		1,041	275	9,276
SPIX-v1	347.8	49%	17	1,533	156	5,512
Romulus-v1	315.7	50%		953	229	8,912
ISAP-v2	290.6	48%		2,157	200	8,456
ACE_GMU-v1	249.5	49%	18	1,847	143	7,044
SKINNY-AEAD-v2	234.9	50%	19	2,337	240	12,557
SKINNY-AEAD-v1	234.8	50%		2,333	240	12,558
COMET_CI-v3	223.5	50%		1,841	215	11,822
COMET_CI-v1	217.5	50%		1,884	223	12,597
TinyJAMBU_TJT-v2	217.5	50%		461	315	17,795
ESTATE-v1	214.2	50%	20	1,351	222	12,736
TinyJAMBU_GMU-v1	176.1	50%		591	266	18,564
mixFeed-v1	172.2	49%	21	1,343	151	10,778
COMET_VT-v2	170.3	49%		1,703	234	16,885
Oribatida-v1	169.6	49%	22	1,450	276	19,995
Oribatida-v2	166.2	50%		1,450	276	20,400
LOCUS-v2	147.8	50%	23	1,628	209	17,379
Elephant-v1	139.8	49%		1,291	229	20,123
SPIX-v2x4	136.7	49%		1,332	176	15,818
Pyjamask-v2	133.0	49%	24	2,308	213	19,680
ForkAE-v2	127.1	50%	25	2,466	228	22,050
SpoC_IIT-v1	101.7	50%	26	1,512	235	28,388
SPIX-v2x2	100.1	49%		1,267	187	22,948
LOTUS-v2	99.7	50%		1,487	141	17,379
TinyJAMBU_GMU-v2	92.6	50%		564	268	35,572
Saturnin-v1	90.9	49%		1,725	215	29,049
LOCUS-v1	80.4	50%		1,824	216	33,012
Xoodyak_GMU-v2	77.8	45%		1,234	168	26,548
WAGE-v1	76.9	49%	27	1,150	279	44,601
SpoC_VT-v1	66.5	50%		1,079	230	42,473
SPIX-v2	60.1	49%		1,181	182	37,198
Pyjamask-v1	55.3	49%		1,979	229	50,908
LOTUS-v1	54.0	50%		1,652	145	33,012
ESTATE-v3	54.0	50%		1,130	259	58,976
TinyJAMBU_TJT-v1	51.8	50%		446	290	68,846

Table 43 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
ESTATE-v2	50.4	50%		907	268	65,364
COMET_CI-v2	50.2	50%		1,096	222	54,375
ACE_UW-v1	48.3	49%		1,229	200	50,845
Gimli_TUM-v1	19.3	49%		933	241	153,573
ESTATE-v4	16.9	50%		944	277	201,194
Romulus-v5	13.8	50%		887	214	189,935
Gimli_TUM-v2	10.4	49%		905	244	288,121
TinyJAMBU_GMU-v3	6.3	50%		537	278	545,812
ForkAE-v1	6.0	50%		1,191	208	422,754
Gimli_TUM-v3	5.6	49%		838	253	557,217
Minimum		**44%**				
Average		**49%**				
Maximum		**50%**				

Table 44: Xilinx Artix-7 Encryption AD+PT Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	2,090.1	22%	1	848	298	73
Ascon_GMU-v1	1,574.4	25%	2	2,410	246	80
Xoodyak_GMU2-v1	1,435.4	22%	3	1,608	314	112
Xoodyak_GMU2-v2	1,306.3	23%		2,322	199	78
Ascon_GMU-v2	1,237.7	28%		1,790	307	127
Gimli_GMU-v4	1,226.8	28%	4	2,357	242	101
Subterranean_ST-v2	1,216.0	20%		891	190	80
Ascon_GMU2-v2h	1,163.2	31%		2,126	234	103
GIFT-COFB_GMU-v4	1,079.8	36%	5	1,730	213	101
GIFT-COFB_GMU-v3	1,071.3	37%		1,641	249	119
Ascon_Graz-v4	1,004.5	30%		2,249	206	105
Xoodyak_XT-v2	992.3	30%		2,025	188	97
Xoodyak_XT-v8	955.4	30%		2,143	181	97
GIFT-COFB_GMU-v5	947.9	32%		2,051	137	74
KNOT-v2x4	908.4	29%		**2,797**	165	93
Ascon_GMU2-v3h	876.0	29%		2,493	142	83
Xoodyak_XT-v1	861.9	29%		1,355	234	139
Ascon_Graz-v3	857.6	33%		2,142	201	120
Ascon_GMU2-v1h	851.3	34%		1,375	276	166
GIFT-COFB_GMU-v6	840.6	30%		2,363	110	67
KNOT-v2x2	834.2	26%	6	1,873	233	143
Xoodyak_XT-v7	832.5	29%		1,392	226	139
Gimli_GMU-v2	797.1	31%		1,678	260	167
KNOT-v2x2h	794.9	26%		2,112	222	143
Ascon_Graz-v5	775.8	32%		**2,797**	150	99
Gimli_GT-v4	757.3	25%		2,510	142	96
KNOT-v2x4h	754.2	29%		2,438	137	93
Ascon_Graz-v2	712.8	31%		1,541	213	153
Gimli_GT-v5	645.0	21%		**3,907**	97	77
GIFT-COFB_GMU-v2	639.4	40%		1,380	261	209
Gimli_GT-v6	629.6	22%		**3,937**	91	74
Xoodyak_GMU-v1	626.2	29%		1,808	170	139
COMET_VT-v1	575.3	39%	7	2,449	209	186
Gimli_GT-v3	568.4	27%		**2,678**	131	118
TinyJAMBU_TJT-v3	561.1	40%	8	576	240	219
Ascon_VT-v1	560.1	38%		1,913	233	213
DryGASCON-v1	556.4	38%	9	2,074	238	219
Gimli_GT-v2	553.1	30%		1,909	175	162
Ascon_Graz-v1	552.5	36%		1,465	191	177
Ascon_VT-v2	544.3	37%		1,928	219	206
KNOT-v2x1	481.3	28%		1,620	251	267
Gimli_GT-v7	469.3	22%		**5,347**	66	72
Elephant-v5	468.8	30%		**2,645**	217	237
KNOT-v2x1h	452.6	28%		1,684	236	267
Gimli_GMU-v1	436.7	33%		1,435	255	299
Romulus-v2	434.8	40%	10	1,280	214	252
Romulus-v3	408.9	38%		1,824	123	154

Table 44 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Spook-v2-v2	368.8	34%	11	2,033	206	286
GIFT-COFB_GMU-v1	346.2	42%		1,223	263	389
GIFT-COFB_VT-v1	317.1	43%		1,041	275	444
Elephant-v2	313.1	36%	12	1,884	181	296
PHOTON-Beetle-v1	311.0	42%	13	2,065	178	293
Elephant-v4	308.1	31%		1,901	263	437
Gimli_GT-v1	304.8	33%		1,747	175	294
Elephant-v3	294.3	36%		1,717	200	348
Romulus-v4	282.8	35%		**2,602**	58	105
Romulus-v1	261.7	41%		953	229	448
Saturnin-v2	256.8	24%	14	2,321	167	333
SCHWAEMM-v1	255.1	31%	15*	**3,071**	135	271
SCHWAEMM-v2	245.6	31%		**3,740**	130	271
SPIX-v1	221.9	31%	16	1,533	156	360
SKINNY-AEAD-v2	205.8	44%	17	2,337	240	597
SKINNY-AEAD-v1	205.5	43%		2,333	240	598
ESTATE-v1	192.0	45%	18	1,351	222	592
TinyJAMBU_TJT-v2	186.0	42%		461	315	867
COMET_CI-v3	184.1	41%		1,841	215	598
COMET_CI-v1	179.2	41%		1,884	223	637
ACE_GMU-v1	174.3	34%	19	1,847	143	420
ISAP-v1	163.9	20%		**3,491**	193	603
ISAP-v3	156.3	19%	20	2,182	188	616
TinyJAMBU_GMU-v1	151.3	43%		591	266	900
ISAP-v2	140.7	23%		2,157	200	728
COMET_VT-v2	136.6	40%		1,703	234	877
Oribatida-v1	135.5	40%	21	1,450	276	1,043
LOCUS-v2	130.7	44%	22	1,628	209	819
Oribatida-v2	125.7	37%		1,450	276	1,124
ForkAE-v2	118.9	47%	23	2,466	228	982
mixFeed-v1	117.5	33%	24	1,343	151	658
Elephant-v1	103.9	37%		1,291	229	1,128
SpoC_IIT-v1	89.8	44%	25	1,512	235	1,340
LOTUS-v2	88.1	44%		1,487	141	819
Pyjamask-v2	85.2	31%	26	2,308	213	1,280
SPIX-v2x4	82.1	29%		1,332	176	1,098
TinyJAMBU_GMU-v2	80.0	43%		564	268	1,716
LOCUS-v1	71.4	44%		1,824	216	1,548
SPIX-v2x2	59.7	29%		1,267	187	1,604
Saturnin-v1	59.1	32%		1,725	215	1,863
SpoC_VT-v1	59.1	44%		1,079	230	1,993
WAGE-v1	53.9	34%	27	1,150	279	2,649
ESTATE-v3	49.6	46%		1,130	259	2,672
LOTUS-v1	48.0	44%		1,652	145	1,548
Xoodyak_GMU-v2	46.7	27%		1,234	168	1,842
ESTATE-v2	45.9	45%		907	268	2,988
TinyJAMBU_TJT-v1	44.4	43%		446	290	3,342
COMET_CI-v2	41.1	41%		1,096	222	2,763

Table 44 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Pyjamask-v1	38.2	34%		1,979	229	3,068
SPIX-v2	35.8	29%		1,181	182	2,606
ACE_UW-v1	34.1	35%		1,229	200	3,005
ESTATE-v4	15.6	46%		944	277	9,098
Gimli_TUM-v1	14.2	36%		933	241	8,673
Romulus-v5	11.8	42%		887	214	9,247
Gimli_TUM-v2	7.7	36%		905	244	16,261
ForkAE-v1	6.0	50%		1,191	208	17,678
TinyJAMBU_GMU-v3	5.4	43%		537	278	26,196
Gimli_TUM-v3	4.1	36%		838	253	31,437
Minimum		**19%**				
Average		**34%**				
Maximum		**50%**				

Table 45: Xilinx Artix-7 Encryption AD+PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	778.4	8%	1	848	298	49
Ascon_GMU-v1	629.8	10%	2	2,410	246	50
GIFT-COFB_GMU-v3	601.4	21%	3	1,641	249	53
GIFT-COFB_GMU-v4	580.1	19%		1,730	213	47
Xoodyak_GMU2-v1	550.6	8%	4	1,608	314	73
Ascon_GMU2-v2h	544.6	15%		2,126	234	55
Ascon_GMU-v2	538.3	12%		1,790	307	73
Gimli_GMU-v4	525.0	12%	5	2,357	242	59
Xoodyak_GMU2-v2	489.8	9%		2,322	199	52
Xoodyak_XT-v2	462.8	14%		2,025	188	52
Ascon_Graz-v4	462.6	14%		2,249	206	57
GIFT-COFB_GMU-v5	461.5	16%		2,051	137	38
Xoodyak_XT-v8	445.5	14%		2,143	181	52
Subterranean_ST-v2	434.3	7%		891	190	56
Ascon_GMU2-v1h	430.8	17%		1,375	276	82
Ascon_Graz-v3	428.8	17%		2,142	201	60
GIFT-COFB_GMU-v2	402.5	25%		1,380	261	83
KNOT-v2x4	398.5	13%		**2,797**	165	53
Xoodyak_XT-v1	394.1	13%		1,355	234	76
Ascon_GMU2-v3h	386.7	13%		2,493	142	47
Xoodyak_XT-v7	380.6	13%		1,392	226	76
GIFT-COFB_GMU-v6	380.5	14%		2,363	110	37
Ascon_Graz-v5	376.5	16%		**2,797**	150	51
Gimli_GMU-v2	373.9	15%		1,678	260	89
TinyJAMBU_TJT-v3	353.1	25%	6	576	240	87
COMET_VT-v1	343.0	23%	7	2,449	209	78
KNOT-v2x2	342.8	11%	8	1,873	233	87
Ascon_Graz-v2	336.6	15%		1,541	213	81
KNOT-v2x4h	330.9	13%		2,438	137	53
DryGASCON-v1	327.6	23%	9	2,074	238	93
KNOT-v2x2h	326.6	11%		2,112	222	87
Romulus-v2	326.1	30%	10	1,280	214	84
Ascon_VT-v1	320.7	22%		1,913	233	93
Ascon_VT-v2	304.7	21%		1,928	219	92
Gimli_GT-v4	302.9	10%		2,510	142	60
Ascon_Graz-v1	301.8	20%		1,465	191	81
Xoodyak_GMU-v1	286.3	13%		1,808	170	76
Romulus-v3	281.1	26%		1,824	123	56
Gimli_GT-v2	248.9	13%		1,909	175	90
Gimli_GT-v3	239.5	11%		**2,678**	131	70
GIFT-COFB_GMU-v1	235.4	29%		1,223	263	143
Gimli_GT-v5	234.3	8%		**3,907**	97	53
Gimli_GT-v6	233.0	8%		**3,937**	91	50
GIFT-COFB_VT-v1	225.6	31%		1,041	275	156
Elephant-v5	222.2	14%		**2,645**	217	125
Gimli_GMU-v1	219.1	17%		1,435	255	149
Romulus-v1	209.4	33%		953	229	140

Table 45 continued from previous page

Variant	Through-put 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
KNOT-v2x1	207.3	12%		1,620	251	155
PHOTON-Beetle-v1	207.1	28%	11	2,065	178	110
KNOT-v2x1h	194.9	12%		1,684	236	155
Elephant-v2	194.7	23%	12	1,884	181	119
Elephant-v3	184.2	23%		1,717	200	139
Romulus-v4	176.8	22%		**2,602**	58	42
Gimli_GT-v7	176.0	8%		**5,347**	66	48
Elephant-v4	149.6	15%		1,901	263	225
Gimli_GT-v1	149.3	16%		1,747	175	150
SKINNY-AEAD-v2	148.4	31%	13	2,337	240	207
SKINNY-AEAD-v1	147.7	31%		2,333	240	208
ESTATE-v1	145.0	34%	14	1,351	222	196
Spook-v2-v2	138.8	13%	15	2,033	206	190
TinyJAMBU_TJT-v2	128.0	29%		461	315	315
COMET_CI-v3	118.6	26%		1,841	215	232
Saturnin-v2	117.5	11%	16	2,321	167	182
COMET_CI-v1	115.6	26%		1,884	223	247
TinyJAMBU_GMU-v1	105.1	30%		591	266	324
SPIX-v1	104.0	15%	17	1,533	156	192
ForkAE-v2	98.9	39%	18	2,466	228	295
LOCUS-v2	95.9	32%	19	1,628	209	279
SCHWAEMM-v1	94.9	12%	20*	**3,071**	135	182
SCHWAEMM-v2	91.4	12%		**3,740**	130	182
ACE_GMU-v1	89.7	18%	21	1,847	143	204
COMET_VT-v2	84.4	25%		1,703	234	355
Oribatida-v1	83.1	24%	22	1,450	276	425
Oribatida-v2	71.8	21%		1,450	276	492
Elephant-v1	66.8	24%		1,291	229	439
SpoC_IIT-v1	65.7	32%	23	1,512	235	458
LOTUS-v2	64.7	32%		1,487	141	279
ISAP-v1	60.1	7%		**3,491**	193	411
mixFeed-v1	58.9	17%	24	1,343	151	328
ISAP-v3	56.8	7%	25	2,182	188	424
TinyJAMBU_GMU-v2	56.1	30%		564	268	612
ISAP-v2	53.8	9%		2,157	200	476
LOCUS-v1	53.0	33%		1,824	216	522
SpoC_VT-v1	43.7	33%		1,079	230	673
Pyjamask-v2	40.1	15%	26	2,308	213	680
ESTATE-v3	39.7	37%		1,130	259	836
SPIX-v2x4	36.5	13%		1,332	176	618
ESTATE-v2	36.0	36%		907	268	954
LOTUS-v1	35.6	33%		1,652	145	522
Saturnin-v1	31.9	17%		1,725	215	862
TinyJAMBU_TJT-v1	30.8	30%		446	290	1,206
WAGE-v1	27.9	18%	27	1,150	279	1,281
SPIX-v2x2	26.4	13%		1,267	187	908
COMET_CI-v2	26.3	26%		1,096	222	1,080
Xoodyak_GMU-v2	20.4	12%		1,234	168	1,053

Table 45 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Pyjamask-v1	19.4	17%		1,979	229	1,508
ACE_UW-v1	17.7	18%		1,229	200	1,445
SPIX-v2	15.8	13%		1,181	182	1,478
ESTATE-v4	12.5	37%		944	277	2,834
Romulus-v5	10.2	36%		887	214	2,695
Gimli_TUM-v1	7.8	20%		933	241	3,948
ForkAE-v1	6.0	49%		1,191	208	4,469
Gimli_TUM-v2	4.2	20%		905	244	7,396
TinyJAMBU_GMU-v3	3.8	31%		537	278	9,252
Gimli_TUM-v3	2.3	20%		838	253	14,292
Minimum		**7%**				
Average		**20%**				
Maximum		**49%**				

Table 46: Xilinx Artix-7 Hash Throughput for 1536 Byte Messages

Variant	**Through-put 1536B [Mbit/s]**	**Thr HM 1536B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 1536B**
Gimli_GMU-v4	4,254.2	96%	1	2,357	242	699
Xoodyak_GMU2-v2	3,523.5	97%	2	2,322	199	694
Xoodyak_GMU2-v1	3,012.0	97%		1,608	314	1,281
Gimli_GT-v5	2,921.4	94%		**3,907**	97	408
Gimli_GT-v4	2,888.9	95%		2,510	142	604
Gimli_GT-v6	2,754.2	95%		**3,937**	91	406
Gimli_GMU-v2	2,482.4	97%		1,678	260	1,287
Ascon_GMU2-v2h	2,077.6	97%	3	2,126	234	1,384
Xoodyak_XT-v8	2,070.9	98%		2,143	181	1,074
Gimli_GT-v3	2,012.2	96%		**2,678**	131	800
Gimli_GT-v7	2,007.4	95%		**5,347**	66	404
Gimli_GT-v2	1,804.0	97%		1,909	175	1,192
Ascon_GMU2-v3h	1,762.5	97%		2,493	142	990
Xoodyak_XT-v7	1,677.0	99%		1,392	226	1,656
Ascon_Graz-v4	1,603.1	97%		2,249	206	1,579
SHA2-v1	1,572.2	99%	4	1,051	201	1,571
Ascon_Graz-v3	1,564.2	97%		2,142	201	1,579
Ascon_Graz-v5	1,555.4	97%		**2,797**	150	1,185
DryGASCON-v1	1,434.3	99%	5	2,074	238	2,039
Ascon_GMU2-v1h	1,321.7	97%		1,375	276	2,566
Gimli_GMU-v1	1,272.2	97%		1,435	255	2,463
Xoodyak_GMU-v1	1,261.4	99%		1,808	170	1,656
Saturnin-v2	1,241.4	96%	6	2,321	167	1,653
Ascon_Graz-v2	948.0	97%		1,541	213	2,761
Ascon_VT-v2	910.4	97%		1,928	219	2,956
Gimli_GT-v1	908.1	97%		1,747	175	2,368
KNOT-v2x4h	852.0	97%	7	2,438	137	1,976
Ascon_Graz-v1	850.1	97%		1,465	191	2,761
Subterranean_ST-v2	753.6	99%	8	891	190	3,098
KNOT-v2x2h	693.1	98%		2,112	222	3,936
ACE_GMU-v1	495.3	97%	9	1,847	143	3,548
SCHWAEMM-v2	481.2	98%	10*	**3,740**	130	3,320
KNOT-v2x1h	369.1	98%		1,684	236	7,856
PHOTON-Beetle-v1	228.6	100%	11	2,065	178	9,566
Saturnin-v1	176.4	98%		1,725	215	14,981
ACE_UW-v1	96.0	97%		1,229	200	25,608
Xoodyak_GMU-v2	82.1	99%		1,234	168	25,142
Gimli_TUM-v1	38.4	98%		933	241	77,046
Gimli_TUM-v2	20.8	98%		905	244	144,482
Gimli_TUM-v3	11.1	98%		838	253	279,354
Minimum		**94%**				
Average		**97%**				
Maximum		**100%**				

Table 47: Xilinx Artix-7 Hash Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr HM 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Gimli_GMU-v4	2,252.8	51%	1	2,357	242	55
Xoodyak_GMU2-v2	2,037.8	56%	2	2,322	199	50
Xoodyak_GMU2-v1	1,891.4	61%		1,608	314	85
Xoodyak_XT-v8	1,494.7	71%		2,143	181	62
Gimli_GMU-v2	1,462.9	57%		1,678	260	91
Gimli_GT-v4	1,398.2	46%		2,510	142	52
SHA2-v1	1,354.1	86%	3	1,051	201	76
Xoodyak_XT-v7	1,257.7	74%		1,392	226	92
Ascon_GMU2-v2h	1,248.0	58%	4	2,126	234	96
Gimli_GT-v5	1,241.6	40%		**3,907**	97	40
Gimli_GT-v6	1,226.1	42%		**3,937**	91	38
DryGASCON-v1	1,138.8	79%	5	2,074	238	107
Gimli_GT-v3	1,048.0	50%		**2,678**	131	64
Ascon_GMU2-v3h	1,038.6	57%		2,493	142	70
Gimli_GT-v2	1,018.2	55%		1,909	175	88
Ascon_Graz-v4	985.7	60%		2,249	206	107
Ascon_Graz-v3	961.8	60%		2,142	201	107
Ascon_Graz-v5	948.1	59%		**2,797**	150	81
Xoodyak_GMU-v1	946.1	74%		1,808	170	92
Gimli_GT-v7	938.7	44%		**5,347**	66	36
Ascon_GMU2-v1h	812.1	60%		1,375	276	174
Gimli_GMU-v1	801.0	61%		1,435	255	163
Saturnin-v2	633.4	49%	6	2,321	167	135
Subterranean_ST-v2	631.7	83%	7	891	190	154
Ascon_Graz-v2	589.5	61%		1,541	213	185
Ascon_VT-v2	572.1	61%		1,928	219	196
Gimli_GT-v1	560.0	60%		1,747	175	160
Ascon_Graz-v1	528.6	61%		1,465	191	185
KNOT-v2x4h	515.8	59%	8	2,438	137	136
KNOT-v2x2h	444.0	62%		2,112	222	256
SCHWAEMM-v2	346.7	71%	9*	**3,740**	130	192
ACE_GMU-v1	310.2	61%	10	1,847	143	236
PHOTON-Beetle-v1	249.0	109%	11	2,065	178	366
KNOT-v2x1h	243.6	65%		1,684	236	496
Saturnin-v1	115.8	64%		1,725	215	951
Xoodyak_GMU-v2	65.5	79%		1,234	168	1,314
ACE_UW-v1	60.7	62%		1,229	200	1,688
Gimli_TUM-v1	26.1	66%		933	241	4,734
Gimli_TUM-v2	14.1	66%		905	244	8,874
Gimli_TUM-v3	7.6	66%		838	253	17,154
Minimum		**40%**				
Average		**63%**				
Maximum		**109%**				

Table 48: Xilinx Artix-7 Hash Throughput for 16 Byte Messages

Variant	**Through-put 16B [Mbit/s]**	**Thr HM 16B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 16B**
Gimli_GMU-v4	911.1	21%	1	2,357	242	34
Xoodyak_GMU2-v2	878.3	24%	2	2,322	199	29
Xoodyak_GMU2-v1	873.7	28%		1,608	314	46
Xoodyak_XT-v8	798.9	38%		2,143	181	29
Xoodyak_XT-v7	705.6	41%		1,392	226	41
DryGASCON-v1	692.4	48%	3	2,074	238	44
Gimli_GMU-v2	640.0	25%		1,678	260	52
Ascon_GMU2-v2h	554.7	26%	4	2,126	234	54
Gimli_GT-v4	534.6	18%		2,510	142	34
Xoodyak_GMU-v1	530.7	41%		1,808	170	41
Ascon_GMU2-v3h	454.4	25%		2,493	142	40
Gimli_GT-v6	448.0	15%		**3,937**	91	26
Ascon_Graz-v4	446.9	27%		2,249	206	59
Gimli_GT-v5	443.4	14%		**3,907**	97	28
Ascon_Graz-v3	436.1	27%		2,142	201	59
Gimli_GT-v2	430.8	23%		1,909	175	52
Ascon_Graz-v5	426.7	27%		**2,797**	150	45
Subterranean_ST-v2	419.3	55%	5	891	190	58
Gimli_GT-v3	419.2	20%		**2,678**	131	40
Gimli_GMU-v1	370.9	28%		1,435	255	88
Ascon_GMU2-v1h	368.0	27%		1,375	276	96
Gimli_GT-v7	352.0	17%		**5,347**	66	24
PHOTON-Beetle-v1	345.2	152%	6	2,065	178	66
SHA2-v1	338.5	21%	7	1,051	201	76
Saturnin-v2	309.8	24%	8	2,321	167	69
Ascon_Graz-v2	269.9	28%		1,541	213	101
Ascon_VT-v2	264.5	28%		1,928	219	106
Gimli_GT-v1	254.5	27%		1,747	175	88
Ascon_Graz-v1	242.1	28%		1,465	191	101
KNOT-v2x4h	230.7	26%	9	2,438	137	76
KNOT-v2x2h	208.9	29%		2,112	222	136
SCHWAEMM-v2	184.9	38%	10*	**3,740**	130	90
ACE_GMU-v1	143.0	28%	11	1,847	143	128
KNOT-v2x1h	118.0	31%		1,684	236	256
Saturnin-v1	80.7	45%		1,725	215	341
Xoodyak_GMU-v2	40.0	48%		1,234	168	537
ACE_UW-v1	28.2	29%		1,229	200	908
Gimli_TUM-v1	13.0	33%		933	241	2,376
Gimli_TUM-v2	7.0	33%		905	244	4,452
Gimli_TUM-v3	3.8	33%		838	253	8,604
Minimum		**14%**				
Average		**32%**				
Maximum		**152%**				

Table 49: Intel Cyclone 10 LP Encryption PT Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	5,057.8	91%	1	1,264	174.5	424
Subterranean_ST-v2	4,361.2	89%		1,285	153.7	433
Ascon_GMU-v1	2,797.9	92%	2	4,552	118.4	520
Gimli_GMU-v4	2,628.5	94%	3	2,953	153.4	717
Xoodyak_GMU2-v2	2,422.5	91%		**5,058**	97.2	493
Xoodyak_GMU2-v1	2,346.0	93%	4	2,575	170.3	892
Ascon_GMU-v2	2,155.0	94%		3,113	160.6	916
Ascon_GMU2-v2h	2,052.7	95%		3,215	134.8	807
Gimli_GMU-v5	1,946.9	92%		**5,576**	82.4	520
Ascon_GMU2-v3h	1,843.8	94%		4,161	91.7	611
KNOT-v2x2h	1,777.0	92%	5	2,792	140.1	969
KNOT-v2x2	1,759.1	92%		2,472	138.7	969
Gimli_GT-v4	1,733.3	92%		**5,010**	88.2	625
Gimli_GT-v5	1,674.0	89%		**5,948**	58.6	430
Ascon_Graz-v4	1,658.5	95%		3,730	108.7	805
Ascon_GMU2-v1h	1,546.7	96%		2,415	175.6	1,395
GIFT-COFB_GMU-v4	1,509.2	96%	6	2,609	110.8	902
GIFT-COFB_GMU-v3	1,475.0	96%		2,523	131.8	1,098
Ascon_Graz-v2	1,466.7	96%		2,634	143.3	1,201
Gimli_GMU-v2	1,442.7	95%		2,158	153.9	1,311
KNOT-v2x4	1,428.2	95%		3,519	102.0	878
KNOT-v2x4h	1,421.1	95%		3,678	101.5	878
Ascon_Graz-v3	1,351.6	96%		3,716	109.7	997
Xoodyak_XT-v1	1,317.0	96%		2,231	136.3	1,272
Gimli_GT-v6	1,298.6	90%		4,820	45.2	428
Gimli_GT-v3	1,282.0	93%		3,651	85.8	822
Xoodyak_XT-v8	1,270.5	96%		3,630	90.0	870
Xoodyak_XT-v2	1,254.6	96%		3,541	88.8	870
Xoodyak_XT-v7	1,241.6	96%		2,272	128.5	1,272
Ascon_Graz-v5	1,229.1	96%		4,905	80.1	801
Ascon_VT-v2	1,191.4	97%		2,695	172.0	1,774
Gimli_GT-v2	1,158.2	95%		3,145	114.8	1,218
Ascon_VT-v1	1,104.5	98%		2,432	176.6	1,965
Ascon_Graz-v1	1,096.1	97%		2,517	141.4	1,585
GIFT-COFB_GMU-v5	1,039.8	95%		4,828	51.5	608
KNOT-v2x1	1,035.6	93%		2,059	161.7	1,919
Xoodyak_GMU-v1	1,031.6	96%		3,135	106.8	1,272
KNOT-v2x1h	1,020.8	93%		2,532	159.4	1,919
Gimli_GT-v7	928.4	90%		**6,379**	32.3	427
GIFT-COFB_GMU-v2	925.6	97%		2,111	156.5	2,078
GIFT-COFB_GMU-v6	893.8	94%		**6,630**	37.2	511
Elephant-v5	878.9	95%	7	3,926	126.9	1,774
DryGASCON-v1	776.0	98%	8	3,199	130.5	2,067
Gimli_GMU-v1	759.7	96%		1,908	154.5	2,499
Gimli_GT-v1	729.2	96%		2,378	142.8	2,406
TinyJAMBU_TJT-v3	629.7	99%	9	1,021	159.7	3,116
Elephant-v4	574.0	96%		3,050	157.6	3,374

Table 49 continued from previous page

Variant	Through-put 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Romulus-v2	557.4	98%	10	2,086	141.7	3,124
COMET_VT-v1	556.8	98%		**10,200**	88.9	1,962
Spook-v2-v2	556.1	96%	11	3,188	108.5	2,398
Romulus-v3	551.8	98%		2,407	79.3	1,766
GIFT-COFB_VT-v1	490.8	98%		1,877	184.4	4,617
GIFT-COFB_GMU-v1	486.4	97%		1,903	159.8	4,038
PHOTON-Beetle-v1	479.4	99%	12	3,602	125.4	3,215
Saturnin-v2	465.0	94%	13	3,892	104.6	2,763
Romulus-v4	456.2	97%		3,409	40.4	1,087
SCHWAEMM-v2	450.1	96%		**5,773**	85.7	2,341
SCHWAEMM-v1	429.1	96%	14	4,713	81.8	2,341
ISAP-v4	414.0	92%	15	3,026	155.0	4,600
Elephant-v2	413.4	98%		2,729	113.2	3,363
ISAP-v3	407.8	90%		3,767	131.9	3,975
ISAP-v1	392.6	90%		4,589	126.6	3,962
Elephant-v3	379.8	98%		2,504	123.2	3,987
SPIX-v1	335.9	96%	16	3,525	82.1	3,004
ISAP-v2	311.3	93%		3,852	136.4	5,384
Romulus-v1	301.4	99%		1,735	143.2	5,840
SKINNY-AEAD-v1	272.9	99%	17	3,672	144.6	6,512
ACE_GMU-v1	265.1	97%	18	4,473	77.0	3,572
SKINNY-AEAD-v2	263.3	99%		3,532	139.5	6,511
COMET_CI-v3	218.9	98%	19	4,379	114.8	6,446
COMET_CI-v1	208.0	98%		4,663	115.8	6,837
SPIX-v2x4	201.2	95%		2,310	132.6	8,099
TinyJAMBU_TJT-v2	188.3	99%		777	196.2	12,803
TinyJAMBU_GMU-v1	183.4	99%		856	196.8	13,189
Oribatida-v1	171.5	99%	20	2,512	185.7	13,301
ESTATE-v1	170.3	99%	21	3,839	118.0	8,512
mixFeed-v1	159.3	97%	22*	**5,363**	73.2	5,641
Oribatida-v2	158.1	99%		2,221	174.5	13,564
COMET_VT-v2	155.8	98%		**5,204**	110.6	8,725
SpoC_IIT-v1	154.8	99%	23	2,250	182.2	14,468
ForkAE-v2	153.2	99%	24	3,200	148.1	11,878
Elephant-v1	150.1	98%		2,056	163.1	13,347
SPIX-v2x2	140.8	95%		1,993	134.7	11,755
LOCUS-v2	140.0	99%	25	2,828	132.4	11,619
Pyjamask-v2	108.5	95%		**8,692**	90.6	10,263
LOTUS-v2	105.4	99%		2,445	99.6	11,619
SpoC_VT-v1	95.7	99%		1,696	167.7	21,545
TinyJAMBU_GMU-v2	94.2	99%		841	196.2	25,589
Saturnin-v1	90.9	97%		3,802	145.0	19,593
WAGE-v1	86.8	97%	26	1,774	159.6	22,600
SPIX-v2	84.2	95%		1,864	130.6	19,057
LOCUS-v1	70.0	99%		2,978	125.8	22,068
LOTUS-v1	57.6	99%		2,642	103.5	22,068
COMET_CI-v2	56.3	98%		2,629	132.9	29,031
ESTATE-v3	56.2	99%		2,279	180.2	39,392

Table 49 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Xoodyak_GMU-v2	54.1	95%		**5,871**	77.0	17,495
Pyjamask-v1	51.6	96%	27*	**8,599**	109.7	26,131
ACE_UW-v1	50.8	97%		1,903	106.5	25,756
TinyJAMBU_TJT-v1	49.3	99%		686	200.8	50,030
ESTATE-v2	49.1	99%		1,946	174.3	43,668
ESTATE-v4	18.3	99%		1,572	200.1	134,378
Gimli_TUM-v1	15.9	97%		2,044	101.3	78,117
Romulus-v5	12.6	99%		1,960	130.2	126,575
Gimli_TUM-v2	8.2	97%		2,074	97.3	146,617
TinyJAMBU_GMU-v3	5.9	99%		817	191.1	397,589
ForkAE-v1	5.4	100%		2,129	135.7	306,694
Gimli_TUM-v3	4.4	97%		2,115	100.5	283,617
Minimum		**89%**				
Average		**96%**				
Maximum		**100%**				

Table 50: Intel Cyclone 10 LP Encryption PT Throughput for 64 Byte Messages

Variant	Throughput 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	1,595.6	29%	1	1,264	174.5	56
Subterranean_ST-v2	1,210.5	25%		1,285	153.7	65
Gimli_GMU-v4	1,075.7	38%	2	2,953	153.4	73
Ascon_GMU-v1	1,010.3	33%	3	4,552	118.4	60
Ascon_GMU2-v2h	972.2	45%		3,215	134.8	71
Ascon_GMU-v2	934.6	41%		3,113	160.6	88
Xoodyak_GMU2-v1	880.7	35%	4	2,575	170.3	99
Ascon_GMU2-v1h	840.2	52%		2,415	175.6	107
Ascon_Graz-v4	806.2	46%		3,730	108.7	69
Ascon_GMU2-v3h	795.6	41%		4,161	91.7	59
GIFT-COFB_GMU-v3	784.7	51%	5	2,523	131.8	86
GIFT-COFB_GMU-v4	766.5	49%		2,609	110.8	74
Ascon_Graz-v2	756.7	49%		2,634	143.3	97
Xoodyak_GMU2-v2	754.0	28%		**5,058**	97.2	66
Ascon_VT-v2	746.3	61%		2,695	172.0	118
Ascon_Graz-v3	729.2	52%		3,716	109.7	77
KNOT-v2x4	725.7	48%	6	3,519	102.0	72
Ascon_VT-v1	723.4	64%		2,432	176.6	125
KNOT-v2x4h	722.1	48%		3,678	101.5	72
KNOT-v2x2h	710.4	37%		2,792	140.1	101
KNOT-v2x2	703.2	37%		2,472	138.7	101
Gimli_GMU-v5	703.1	33%		**5,576**	82.4	60
Gimli_GMU-v2	685.3	45%		2,158	153.9	115
Ascon_Graz-v1	640.6	57%		2,517	141.4	113
Ascon_Graz-v5	631.1	49%		4,905	80.1	65
Xoodyak_XT-v1	628.8	46%		2,231	136.3	111
Gimli_GT-v4	618.3	33%		**5,010**	88.2	73
Xoodyak_XT-v8	614.1	46%		3,630	90.0	75
Xoodyak_XT-v2	606.4	46%		3,541	88.8	75
Xoodyak_XT-v7	592.9	46%		2,272	128.5	111
GIFT-COFB_GMU-v2	548.9	58%		2,111	156.5	146
Gimli_GT-v2	515.6	42%		3,145	114.8	114
Gimli_GT-v3	510.6	37%		3,651	85.8	86
DryGASCON-v1	495.0	62%	7	3,199	130.5	135
Xoodyak_GMU-v1	492.6	46%		3,135	106.8	111
Gimli_GT-v5	483.8	26%		**5,948**	58.6	62
TinyJAMBU_TJT-v3	475.4	74%	8	1,021	159.7	172
GIFT-COFB_GMU-v5	470.4	43%		4,828	51.5	56
KNOT-v2x1	452.5	41%		2,059	161.7	183
KNOT-v2x1h	446.0	41%		2,532	159.4	183
Romulus-v2	403.1	71%	9	2,086	141.7	180
Gimli_GMU-v1	397.5	50%		1,908	154.5	199
Elephant-v5	386.7	42%	10	3,926	126.9	168
Gimli_GT-v6	386.0	27%		4,820	45.2	60
GIFT-COFB_GMU-v6	373.2	39%		**6,630**	37.2	51
COMET_VT-v1	373.1	66%		**10,200**	88.9	122
Gimli_GT-v1	369.2	48%		2,378	142.8	198

Table 50 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Romulus-v3	369.1	65%		2,407	79.3	110
PHOTON-Beetle-v1	358.8	74%	11	3,602	125.4	179
GIFT-COFB_VT-v1	322.2	64%		1,877	184.4	293
GIFT-COFB_GMU-v1	307.7	62%		1,903	159.8	266
Spook-v2-v2	292.4	51%	12	3,188	108.5	190
Gimli_GT-v7	280.0	27%		**6,379**	32.3	59
Romulus-v4	275.5	59%		3,409	40.4	75
Elephant-v4	262.0	44%		3,050	157.6	308
Elephant-v2	258.6	61%		2,729	113.2	224
SCHWAEMM-v2	245.2	53%		**5,773**	85.7	179
Elephant-v3	239.0	62%		2,504	123.2	264
SCHWAEMM-v1	233.8	53%	13	4,713	81.8	179
Romulus-v1	229.2	75%		1,735	143.2	320
SKINNY-AEAD-v1	212.8	77%	14	3,672	144.6	348
SKINNY-AEAD-v2	205.8	77%		3,532	139.5	347
Saturnin-v2	191.9	39%	15	3,892	104.6	279
SPIX-v1	172.3	49%	16	3,525	82.1	244
COMET_CI-v3	157.2	71%	17	4,379	114.8	374
TinyJAMBU_TJT-v2	152.5	80%		777	196.2	659
ACE_GMU-v1	151.7	55%	18	4,473	77.0	260
COMET_CI-v1	149.3	71%		4,663	115.8	397
TinyJAMBU_GMU-v1	148.8	80%		856	196.8	677
ESTATE-v1	145.2	85%	19	3,839	118.0	416
ISAP-v4	143.8	32%	20	3,026	155.0	552
Oribatida-v1	136.4	79%	21	2,512	185.7	697
ForkAE-v2	134.9	88%	22	3,200	148.1	562
ISAP-v3	126.2	28%		3,767	131.9	535
ISAP-v1	124.2	29%		4,589	126.6	522
SpoC_IIT-v1	122.8	78%	23	2,250	182.2	760
Oribatida-v2	118.5	74%		2,221	174.5	754
LOCUS-v2	117.1	83%	24	2,828	132.4	579
ISAP-v2	116.6	35%		3,852	136.4	599
COMET_VT-v2	105.5	66%		**5,204**	110.6	537
Elephant-v1	96.6	63%		2,056	163.1	864
mixFeed-v1	94.3	57%	25*	**5,363**	73.2	397
SPIX-v2x4	91.9	43%		2,310	132.6	739
LOTUS-v2	88.1	83%		2,445	99.6	579
TinyJAMBU_GMU-v2	77.2	81%		841	196.2	1,301
SpoC_VT-v1	76.6	79%		1,696	167.7	1,121
SPIX-v2x2	63.7	43%		1,993	134.7	1,083
LOCUS-v1	59.0	84%		2,978	125.8	1,092
Pyjamask-v2	52.8	46%		**8,692**	90.6	879
Saturnin-v1	50.5	54%		3,802	145.0	1,469
WAGE-v1	50.3	56%	26	1,774	159.6	1,624
ESTATE-v3	49.7	88%		2,279	180.2	1,856
LOTUS-v1	48.5	84%		2,642	103.5	1,092
ESTATE-v2	42.8	87%		1,946	174.3	2,084
TinyJAMBU_TJT-v1	40.2	81%		686	200.8	2,558

Table 50 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
COMET_CI-v2	39.9	70%		2,629	132.9	1,707
SPIX-v2	38.0	43%		1,864	130.6	1,761
ACE_UW-v1	29.7	57%		1,903	106.5	1,836
Pyjamask-v1	27.7	52%	27*	**8,599**	109.7	2,027
Xoodyak_GMU-v2	25.1	44%		**5,871**	77.0	1,572
ESTATE-v4	16.2	88%		1,572	200.1	6,314
Romulus-v5	10.1	79%		1,960	130.2	6,607
Gimli_TUM-v1	9.4	57%		2,044	101.3	5,529
ForkAE-v1	5.4	99%		2,129	135.7	12,846
TinyJAMBU_GMU-v3	4.9	82%		817	191.1	20,021
Gimli_TUM-v2	4.8	57%		2,074	97.3	10,365
Gimli_TUM-v3	2.6	57%		2,115	100.5	20,037
Minimum		**25%**				
Average		**56%**				
Maximum		**99%**				

Table 51: Intel Cyclone 10 LP Encryption PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	507.7	9%	1	1,264	174.5	44
Gimli_GMU-v4	377.5	13%	2	2,953	153.4	52
Subterranean_ST-v2	371.2	8%		1,285	153.7	53
Ascon_GMU2-v2h	367.1	17%	3	3,215	134.8	47
Ascon_VT-v1	347.8	31%		2,432	176.6	65
Ascon_GMU2-v1h	345.8	22%		2,415	175.6	65
Ascon_VT-v2	344.0	28%		2,695	172.0	64
Ascon_GMU-v2	337.1	15%		3,113	160.6	61
Ascon_GMU-v1	336.8	11%		4,552	118.4	45
GIFT-COFB_GMU-v3	318.3	21%	4	2,523	131.8	53
Ascon_Graz-v4	309.0	18%		3,730	108.7	45
GIFT-COFB_GMU-v4	301.7	19%		2,609	110.8	47
Ascon_Graz-v2	300.8	20%		2,634	143.3	61
Ascon_Graz-v3	298.6	21%		3,716	109.7	47
Xoodyak_GMU2-v1	298.6	12%	5	2,575	170.3	73
Ascon_GMU2-v3h	286.2	15%		4,161	91.7	41
KNOT-v2x4	284.0	19%	6	3,519	102.0	46
KNOT-v2x4h	282.5	19%		3,678	101.5	46
Ascon_Graz-v1	278.4	25%		2,517	141.4	65
TinyJAMBU_TJT-v3	269.0	42%	7	1,021	159.7	76
Gimli_GMU-v2	259.2	17%		2,158	153.9	76
Ascon_Graz-v5	250.1	20%		4,905	80.1	41
KNOT-v2x2h	245.7	13%		2,792	140.1	73
KNOT-v2x2	243.2	13%		2,472	138.7	73
GIFT-COFB_GMU-v2	241.4	25%		2,111	156.5	83
Xoodyak_GMU2-v2	239.2	9%		**5,058**	97.2	52
Xoodyak_XT-v1	239.0	17%		2,231	136.3	73
Xoodyak_XT-v8	235.0	18%		3,630	90.0	49
Gimli_GMU-v5	234.4	11%		**5,576**	82.4	45
DryGASCON-v1	232.1	29%	8	3,199	130.5	72
Xoodyak_XT-v2	232.0	18%		3,541	88.8	49
Xoodyak_XT-v7	225.4	17%		2,272	128.5	73
Romulus-v2	215.9	38%	9	2,086	141.7	84
Gimli_GT-v4	205.2	11%		**5,010**	88.2	55
PHOTON-Beetle-v1	200.7	41%	10	3,602	125.4	80
Gimli_GT-v2	188.4	15%		3,145	114.8	78
Xoodyak_GMU-v1	187.2	17%		3,135	106.8	73
COMET_VT-v1	183.5	32%		**10,200**	88.9	62
Romulus-v3	181.3	32%		2,407	79.3	56
Gimli_GT-v3	177.1	13%		3,651	85.8	62
GIFT-COFB_GMU-v5	173.3	16%		4,828	51.5	38
KNOT-v2x1	163.0	15%		2,059	161.7	127
KNOT-v2x1h	160.7	15%		2,532	159.4	127
Gimli_GMU-v1	159.5	20%		1,908	154.5	124
Elephant-v5	159.2	17%	11	3,926	126.9	102
GIFT-COFB_VT-v1	155.3	31%		1,877	184.4	152
Elephant-v2	152.5	36%		2,729	113.2	95

Table 51 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
Gimli_GT-v5	150.0	8%		**5,948**	58.6	50
Gimli_GT-v1	145.0	19%		2,378	142.8	126
GIFT-COFB_GMU-v1	143.1	29%		1,903	159.8	143
Elephant-v3	142.1	37%		2,504	123.2	111
GIFT-COFB_GMU-v6	132.2	14%		**6,630**	37.2	36
Romulus-v1	131.0	43%		1,735	143.2	140
SKINNY-AEAD-v1	125.9	46%	12	3,672	144.6	147
Romulus-v4	123.0	26%		3,409	40.4	42
SKINNY-AEAD-v2	122.3	46%		3,532	139.5	146
Gimli_GT-v6	120.6	8%		4,820	45.2	48
Elephant-v4	110.8	18%		3,050	157.6	182
ESTATE-v1	99.4	58%	13	3,839	118.0	152
ForkAE-v2	98.2	64%	14	3,200	148.1	193
Spook-v2-v2	97.8	17%	15	3,188	108.5	142
TinyJAMBU_TJT-v2	95.5	50%		777	196.2	263
TinyJAMBU_GMU-v1	93.6	51%		856	196.8	269
Gimli_GT-v7	87.9	9%		**6,379**	32.3	47
SCHWAEMM-v2	85.7	18%		**5,773**	85.7	128
COMET_CI-v3	83.5	38%	16	4,379	114.8	176
Oribatida-v1	83.1	48%	17	2,512	185.7	286
SCHWAEMM-v1	81.8	18%	18	4,713	81.8	128
COMET_CI-v1	79.2	37%		4,663	115.8	187
LOCUS-v2	77.4	55%	19	2,828	132.4	219
SpoC_IIT-v1	74.5	48%	20	2,250	182.2	313
Saturnin-v2	73.5	15%	21	3,892	104.6	182
SPIX-v1	68.3	19%	22	3,525	82.1	154
Oribatida-v2	66.9	42%		2,221	174.5	334
ACE_GMU-v1	64.9	24%	23	4,473	77.0	152
Elephant-v1	59.5	39%		2,056	163.1	351
LOTUS-v2	58.2	55%		2,445	99.6	219
COMET_VT-v2	52.4	33%		**5,204**	110.6	270
TinyJAMBU_GMU-v2	49.3	52%		841	196.2	509
ISAP-v4	47.2	10%	24	3,026	155.0	420
SpoC_VT-v1	47.2	49%		1,696	167.7	455
mixFeed-v1	41.4	25%	25*	**5,363**	73.2	226
ISAP-v3	40.7	9%		3,767	131.9	415
ISAP-v1	40.3	9%		4,589	126.6	402
LOCUS-v1	39.5	56%		2,978	125.8	408
ISAP-v2	39.4	12%		3,852	136.4	443
ESTATE-v3	36.5	65%		2,279	180.2	632
SPIX-v2x4	34.0	16%		2,310	132.6	499
LOTUS-v1	32.5	56%		2,642	103.5	408
ESTATE-v2	30.7	62%		1,946	174.3	728
TinyJAMBU_TJT-v1	25.5	51%		686	200.8	1,010
SPIX-v2x2	23.5	16%		1,993	134.7	735
WAGE-v1	21.7	24%	26	1,774	159.6	940
Saturnin-v1	21.5	23%		3,802	145.0	862
COMET_CI-v2	20.9	36%		2,629	132.9	816

Table 51 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
Pyjamask-v2	20.2	18%		**8,692**	90.6	573
SPIX-v2	14.0	16%		1,864	130.6	1,197
ACE_UW-v1	12.9	25%		1,903	106.5	1,056
ESTATE-v4	12.0	65%		1,572	200.1	2,138
Pyjamask-v1	11.3	21%	27*	**8,599**	109.7	1,241
Xoodyak_GMU-v2	9.4	17%		**5,871**	77.0	1,050
Romulus-v5	6.2	48%		1,960	130.2	2,695
ForkAE-v1	5.3	98%		2,129	135.7	3,264
Gimli_TUM-v1	4.1	25%		2,044	101.3	3,162
TinyJAMBU_GMU-v3	3.2	53%		817	191.1	7,709
Gimli_TUM-v2	2.1	25%		2,074	97.3	5,922
Gimli_TUM-v3	1.1	25%		2,115	100.5	11,442
Minimum		**8%**				
Average		**28%**				
Maximum		**98%**				

Table 52: Intel Cyclone 10 LP Encryption AD Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	5,057.8	91%	1	1,264	174.5	424
Subterranean_ST-v2	4,371.3	89%		1,285	153.7	432
Xoodyak_GMU2-v1	4,063.4	88%	2	2,575	170.3	515
Ascon_GMU-v1	2,797.9	92%	3	4,552	118.4	520
Gimli_GMU-v4	2,628.5	94%	4	2,953	153.4	717
Xoodyak_GMU2-v2	2,596.2	91%		**5,058**	97.2	460
KNOT-v2x4	2,508.0	90%	5	3,519	102.0	500
KNOT-v2x4h	2,495.4	90%		3,678	101.5	500
Ascon_GMU-v2	2,147.9	94%		3,113	160.6	919
Ascon_GMU2-v2h	2,052.7	95%		3,215	134.8	807
Gimli_GMU-v5	1,946.9	92%		**5,576**	82.4	520
Xoodyak_XT-v1	1,873.9	94%		2,231	136.3	894
Ascon_GMU2-v3h	1,846.8	94%		4,161	91.7	610
Xoodyak_XT-v7	1,766.6	94%		2,272	128.5	894
KNOT-v2x2h	1,753.5	91%		2,792	140.1	982
Gimli_GT-v4	1,736.1	92%		**5,010**	88.2	624
KNOT-v2x2	1,735.8	91%		2,472	138.7	982
Gimli_GT-v5	1,674.0	89%		**5,948**	58.6	430
Xoodyak_XT-v8	1,659.6	94%		3,630	90.0	666
Ascon_Graz-v4	1,650.3	95%		3,730	108.7	809
TinyJAMBU_TJT-v3	1,642.1	96%	6	1,021	159.7	1,195
Xoodyak_XT-v2	1,639.0	94%		3,541	88.8	666
Ascon_GMU2-v1h	1,543.4	96%		2,415	175.6	1,398
GIFT-COFB_GMU-v4	1,521.0	97%	7	2,609	110.8	895
GIFT-COFB_GMU-v3	1,487.2	97%		2,523	131.8	1,089
Xoodyak_GMU-v1	1,466.2	94%		3,135	106.8	895
Ascon_Graz-v2	1,457.0	95%		2,634	143.3	1,209
Gimli_GMU-v2	1,442.7	95%		2,158	153.9	1,311
Ascon_Graz-v3	1,347.5	96%		3,716	109.7	1,000
Gimli_GT-v6	1,298.6	90%		4,820	45.2	428
Gimli_GT-v3	1,282.0	93%		3,651	85.8	822
Ascon_Graz-v5	1,226.0	96%		4,905	80.1	803
Gimli_GT-v2	1,158.2	95%		3,145	114.8	1,218
Ascon_VT-v1	1,100.0	97%		2,432	176.6	1,973
Ascon_Graz-v1	1,091.9	97%		2,517	141.4	1,591
Ascon_VT-v2	1,071.2	97%		2,695	172.0	1,973
GIFT-COFB_GMU-v5	1,046.7	95%		4,828	51.5	604
KNOT-v2x1	1,021.2	92%		2,059	161.7	1,946
KNOT-v2x1h	1,006.6	92%		2,532	159.4	1,946
Romulus-v2	960.9	95%	8	2,086	141.7	1,812
GIFT-COFB_GMU-v2	934.1	98%		2,111	156.5	2,059
Gimli_GT-v7	930.5	90%		**6,379**	32.3	426
GIFT-COFB_GMU-v6	899.1	94%		**6,630**	37.2	508
Saturnin-v2	885.5	89%	9	3,892	104.6	1,451
Romulus-v3	876.3	95%		2,407	79.3	1,112
Elephant-v5	832.5	94%	10	3,926	126.9	1,873
DryGASCON-v1	776.0	98%	11	3,199	130.5	2,067

Table 52 continued from previous page

Variant	Through-put 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Gimli_GMU-v1	759.7	96%		1,908	154.5	2,499
Gimli_GT-v1	729.2	96%		2,378	142.8	2,406
Elephant-v2	715.6	95%		2,729	113.2	1,943
COMET_VT-v1	692.3	97%		**10,200**	88.9	1,578
ISAP-v3	681.9	90%	12	3,767	131.9	2,377
Elephant-v3	668.0	95%		2,504	123.2	2,267
ISAP-v1	658.1	90%		4,589	126.6	2,364
ISAP-v4	653.8	92%		3,026	155.0	2,913
Romulus-v4	650.8	94%		3,409	40.4	762
PHOTON-Beetle-v1	563.2	98%	13	3,602	125.4	2,737
Spook-v2-v2	556.1	96%	14	3,188	108.5	2,398
Elephant-v4	554.4	95%		3,050	157.6	3,493
SCHWAEMM-v2	551.9	96%		**5,773**	85.7	1,909
Romulus-v1	548.0	96%		1,735	143.2	3,212
SCHWAEMM-v1	526.2	96%	15	4,713	81.8	1,909
ISAP-v2	505.9	93%		3,852	136.4	3,313
GIFT-COFB_GMU-v1	491.2	98%		1,903	159.8	3,999
GIFT-COFB_VT-v1	475.6	99%		1,877	184.4	4,764
TinyJAMBU_TJT-v2	470.8	97%		777	196.2	5,122
TinyJAMBU_GMU-v1	439.1	98%		856	196.8	5,508
SPIX-v1	383.5	95%	16	3,525	82.1	2,631
ESTATE-v1	338.5	99%	17	3,839	118.0	4,283
Oribatida-v1	333.5	97%	18	2,512	185.7	6,841
Oribatida-v2	308.1	97%		2,221	174.5	6,960
SKINNY-AEAD-v1	290.1	99%	19	3,672	144.6	6,126
Elephant-v1	281.1	95%		2,056	163.1	7,127
SKINNY-AEAD-v2	279.9	99%		3,532	139.5	6,125
LOCUS-v2	277.7	98%	20	2,828	132.4	5,859
ACE_GMU-v1	263.9	96%	21	4,473	77.0	3,588
COMET_CI-v3	257.2	98%	22	4,379	114.8	5,486
COMET_CI-v1	242.0	98%		4,663	115.8	5,877
TinyJAMBU_GMU-v2	235.7	98%		841	196.2	10,228
LOTUS-v2	209.0	98%		2,445	99.6	5,859
SPIX-v2x4	200.3	94%		2,310	132.6	8,137
ForkAE-v2	177.7	99%	23	3,200	148.1	10,239
Saturnin-v1	176.0	93%		3,802	145.0	10,121
mixFeed-v1	171.0	97%	24*	**5,363**	73.2	5,256
COMET_VT-v2	163.0	98%		**5,204**	110.6	8,341
SpoC_IIT-v1	159.0	99%	25	2,250	182.2	14,084
SPIX-v2x2	140.1	94%		1,993	134.7	11,811
LOCUS-v1	138.9	98%		2,978	125.8	11,124
TinyJAMBU_TJT-v1	127.8	97%		686	200.8	19,306
LOTUS-v1	114.3	98%		2,642	103.5	11,124
Pyjamask-v2	112.7	95%		**8,692**	90.6	9,887
ESTATE-v3	111.8	99%		2,279	180.2	19,803
ESTATE-v2	97.5	99%		1,946	174.3	21,967
SpoC_VT-v1	97.4	99%		1,696	167.7	21,161
Xoodyak_GMU-v2	93.7	92%		**5,871**	77.0	10,100

Table 52 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
WAGE-v1	86.3	96%	26	1,774	159.6	22,713
SPIX-v2	83.8	94%		1,864	130.6	19,149
COMET_CI-v2	63.2	98%		2,629	132.9	25,863
Pyjamask-v1	52.3	96%	27*	**8,599**	109.7	25,755
ACE_UW-v1	50.6	96%		1,903	106.5	25,885
ESTATE-v4	36.4	99%		1,572	200.1	67,557
Romulus-v5	24.2	96%		1,960	130.2	66,055
Gimli_TUM-v1	16.0	97%		2,044	101.3	77,829
TinyJAMBU_GMU-v3	15.5	98%		817	191.1	151,828
ForkAE-v1	14.4	100%		2,129	135.7	116,127
Gimli_TUM-v2	8.2	97%		2,074	97.3	145,945
Gimli_TUM-v3	4.4	97%		2,115	100.5	282,177
Minimum		**88%**				
Average		**95%**				
Maximum		**100%**				

Table 53: Intel Cyclone 10 LP Encryption AD Throughput for 64 Byte Messages

Variant	Throughput 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	1,595.6	29%	1	1,264	174.5	56
Subterranean_ST-v2	1,229.4	25%		1,285	153.7	64
Gimli_GMU-v4	1,075.7	38%	2	2,953	153.4	73
Xoodyak_GMU2-v1	1,013.9	22%	3	2,575	170.3	86
Ascon_GMU-v1	1,010.3	33%	4	4,552	118.4	60
Ascon_GMU2-v2h	972.2	45%		3,215	134.8	71
Ascon_GMU-v2	903.8	40%		3,113	160.6	91
TinyJAMBU_TJT-v3	898.5	53%	5	1,021	159.7	91
GIFT-COFB_GMU-v3	876.4	57%	6	2,523	131.8	77
GIFT-COFB_GMU-v4	846.6	54%		2,609	110.8	67
Ascon_GMU2-v1h	817.3	51%		2,415	175.6	110
Ascon_GMU2-v3h	809.3	41%		4,161	91.7	58
KNOT-v2x4	791.7	28%	7	3,519	102.0	66
KNOT-v2x4h	787.7	28%		3,678	101.5	66
Xoodyak_GMU2-v2	777.5	27%		**5,058**	97.2	64
Ascon_Graz-v4	762.0	44%		3,730	108.7	73
Xoodyak_XT-v1	719.6	36%		2,231	136.3	97
Gimli_GMU-v5	703.1	33%		**5,576**	82.4	60
Ascon_Graz-v3	701.8	50%		3,716	109.7	80
Ascon_Graz-v2	699.0	46%		2,634	143.3	105
Xoodyak_XT-v8	687.4	39%		3,630	90.0	67
Gimli_GMU-v2	685.3	45%		2,158	153.9	115
Ascon_VT-v1	679.9	60%		2,432	176.6	133
Xoodyak_XT-v2	678.8	39%		3,541	88.8	67
Xoodyak_XT-v7	678.4	36%		2,272	128.5	97
Ascon_VT-v2	662.1	60%		2,695	172.0	133
GIFT-COFB_GMU-v2	631.0	66%		2,111	156.5	127
KNOT-v2x2h	629.4	33%		2,792	140.1	114
Gimli_GT-v4	626.9	33%		**5,010**	88.2	72
KNOT-v2x2	623.0	33%		2,472	138.7	114
Ascon_Graz-v5	612.3	48%		4,905	80.1	67
Ascon_Graz-v1	608.3	54%		2,517	141.4	119
Xoodyak_GMU-v1	557.9	36%		3,135	106.8	98
Gimli_GT-v2	515.6	42%		3,145	114.8	114
Gimli_GT-v3	510.6	37%		3,651	85.8	86
GIFT-COFB_GMU-v5	506.6	46%		4,828	51.5	52
DryGASCON-v1	495.0	62%	8	3,199	130.5	135
Gimli_GT-v5	483.8	26%		**5,948**	58.6	62
Romulus-v2	465.1	46%	9	2,086	141.7	156
COMET_VT-v1	429.4	60%		**10,200**	88.9	106
Romulus-v3	406.0	44%		2,407	79.3	100
PHOTON-Beetle-v1	398.9	70%	10	3,602	125.4	161
Gimli_GMU-v1	397.5	50%		1,908	154.5	199
GIFT-COFB_GMU-v6	396.5	42%		**6,630**	37.2	48
KNOT-v2x1	394.3	36%		2,059	161.7	210
KNOT-v2x1h	388.7	36%		2,532	159.4	210
Gimli_GT-v6	386.0	27%		4,820	45.2	60

Table 53 continued from previous page

Variant	Through-put 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Elephant-v5	379.9	43%	11	3,926	126.9	171
Gimli_GT-v1	369.2	48%		2,378	142.8	198
GIFT-COFB_VT-v1	368.8	77%		1,877	184.4	256
GIFT-COFB_GMU-v1	360.5	72%		1,903	159.8	227
Elephant-v2	346.9	46%		2,729	113.2	167
Elephant-v3	323.6	46%		2,504	123.2	195
TinyJAMBU_TJT-v2	297.2	62%		777	196.2	338
Spook-v2-v2	292.4	51%	12	3,188	108.5	190
Romulus-v4	287.0	42%		3,409	40.4	72
Gimli_GT-v7	284.8	28%		**6,379**	32.3	58
TinyJAMBU_GMU-v1	283.1	63%		856	196.8	356
Romulus-v1	273.7	48%		1,735	143.2	268
SCHWAEMM-v2	272.7	47%		**5,773**	85.7	161
SCHWAEMM-v1	260.0	47%	13	4,713	81.8	161
Elephant-v4	259.5	44%		3,050	157.6	311
ESTATE-v1	257.0	75%	14	3,839	118.0	235
Saturnin-v2	256.1	26%	15	3,892	104.6	209
ISAP-v4	235.5	33%	16	3,026	155.0	337
SKINNY-AEAD-v1	224.4	76%	17	3,672	144.6	330
SKINNY-AEAD-v2	217.1	77%		3,532	139.5	329
ISAP-v3	205.3	27%		3,767	131.9	329
ISAP-v1	205.1	28%		4,589	126.6	316
LOCUS-v2	200.0	71%	18	2,828	132.4	339
Oribatida-v1	192.8	56%	19	2,512	185.7	493
ISAP-v2	189.2	35%		3,852	136.4	369
Oribatida-v2	180.8	57%		2,221	174.5	494
COMET_CI-v3	176.0	67%	20	4,379	114.8	334
SPIX-v1	175.9	44%	21	3,525	82.1	239
COMET_CI-v1	166.0	67%		4,663	115.8	357
ForkAE-v2	155.7	87%	22	3,200	148.1	487
TinyJAMBU_GMU-v2	152.2	63%		841	196.2	660
LOTUS-v2	150.5	71%		2,445	99.6	339
ACE_GMU-v1	142.9	52%	23	4,473	77.0	276
Elephant-v1	135.7	46%		2,056	163.1	615
SpoC_IIT-v1	125.4	78%	24	2,250	182.2	744
COMET_VT-v2	108.7	65%		**5,204**	110.6	521
LOCUS-v1	101.2	72%		2,978	125.8	636
mixFeed-v1	98.6	56%	25*	**5,363**	73.2	380
ESTATE-v3	89.1	79%		2,279	180.2	1,035
SPIX-v2x4	87.4	41%		2,310	132.6	777
LOTUS-v1	83.3	72%		2,642	103.5	636
TinyJAMBU_TJT-v1	80.7	62%		686	200.8	1,274
SpoC_VT-v1	77.7	79%		1,696	167.7	1,105
ESTATE-v2	76.0	77%		1,946	174.3	1,175
Saturnin-v1	70.1	37%		3,802	145.0	1,059
SPIX-v2x2	60.5	41%		1,993	134.7	1,139
Pyjamask-v2	53.3	45%		**8,692**	90.6	871
WAGE-v1	47.0	53%	26	1,774	159.6	1,737

Table 53 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
COMET_CI-v2	43.2	67%		2,629	132.9	1,575
SPIX-v2	36.1	41%		1,864	130.6	1,853
Xoodyak_GMU-v2	30.0	29%		**5,871**	77.0	1,317
ESTATE-v4	29.1	79%		1,572	200.1	3,525
Pyjamask-v1	27.8	51%	27*	**8,599**	109.7	2,019
ACE_UW-v1	27.8	53%		1,903	106.5	1,965
ForkAE-v1	14.2	99%		2,129	135.7	4,899
Romulus-v5	12.5	49%		1,960	130.2	5,335
TinyJAMBU_GMU-v3	10.0	63%		817	191.1	9,780
Gimli_TUM-v1	9.4	57%		2,044	101.3	5,517
Gimli_TUM-v2	4.8	57%		2,074	97.3	10,337
Gimli_TUM-v3	2.6	57%		2,115	100.5	19,977
Minimum		**22%**				
Average		**50%**				
Maximum		**99%**				

Table 54: Intel Cyclone 10 LP Encryption AD Throughput for 16 Byte Messages

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	507.7	9%	1	1,264	174.5	44
GIFT-COFB_GMU-v3	383.4	25%	2	2,523	131.8	44
Subterranean_ST-v2	378.3	8%		1,285	153.7	52
Gimli_GMU-v4	377.5	13%	3	2,953	153.4	52
TinyJAMBU_TJT-v3	371.6	22%	4	1,021	159.7	55
Ascon_GMU2-v2h	367.1	17%	5	3,215	134.8	47
GIFT-COFB_GMU-v4	354.5	22%		2,609	110.8	40
Ascon_GMU-v1	336.8	11%		4,552	118.4	45
Ascon_GMU2-v1h	330.5	21%		2,415	175.6	68
Ascon_GMU-v2	321.3	14%		3,113	160.6	64
GIFT-COFB_GMU-v2	313.0	33%		2,111	156.5	64
Ascon_VT-v1	309.7	27%		2,432	176.6	73
Ascon_VT-v2	301.6	27%		2,695	172.0	73
Xoodyak_GMU2-v1	298.6	6%	6	2,575	170.3	73
Ascon_GMU2-v3h	293.4	15%		4,161	91.7	40
Ascon_Graz-v4	283.8	16%		3,730	108.7	49
Ascon_Graz-v3	280.7	20%		3,716	109.7	50
Ascon_Graz-v2	265.9	17%		2,634	143.3	69
Gimli_GMU-v2	259.2	17%		2,158	153.9	76
Ascon_Graz-v1	254.9	23%		2,517	141.4	71
KNOT-v2x4	251.2	9%	7	3,519	102.0	52
KNOT-v2x4h	249.9	9%		3,678	101.5	52
Xoodyak_XT-v1	242.4	12%		2,231	136.3	72
Xoodyak_XT-v8	239.9	14%		3,630	90.0	48
Xoodyak_GMU2-v2	239.2	8%		**5,058**	97.2	52
Ascon_Graz-v5	238.5	19%		4,905	80.1	43
Xoodyak_XT-v2	236.9	14%		3,541	88.8	48
Gimli_GMU-v5	234.4	11%		**5,576**	82.4	45
DryGASCON-v1	232.1	29%	8	3,199	130.5	72
Xoodyak_XT-v7	228.5	12%		2,272	128.5	72
GIFT-COFB_VT-v1	216.5	45%		1,877	184.4	109
Romulus-v2	215.9	21%	9	2,086	141.7	84
Gimli_GT-v4	209.0	11%		**5,010**	88.2	54
KNOT-v2x2h	208.6	11%		2,792	140.1	86
PHOTON-Beetle-v1	208.5	36%	10	3,602	125.4	77
KNOT-v2x2	206.5	11%		2,472	138.7	86
GIFT-COFB_GMU-v1	196.7	39%		1,903	159.8	104
COMET_VT-v1	196.2	28%		**10,200**	88.9	58
GIFT-COFB_GMU-v5	193.7	18%		4,828	51.5	34
Gimli_GT-v2	188.4	15%		3,145	114.8	78
Xoodyak_GMU-v1	187.2	12%		3,135	106.8	73
Romulus-v3	181.3	20%		2,407	79.3	56
Gimli_GT-v3	177.1	13%		3,651	85.8	62
Gimli_GMU-v1	159.5	20%		1,908	154.5	124
Gimli_GT-v5	150.0	8%		**5,948**	58.6	50
ESTATE-v1	146.6	43%	11	3,839	118.0	103
Gimli_GT-v1	145.0	19%		2,378	142.8	126

Table 54 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
GIFT-COFB_GMU-v6	144.2	15%		**6,630**	37.2	33
TinyJAMBU_TJT-v2	138.0	29%		777	196.2	182
KNOT-v2x1	134.4	12%		2,059	161.7	154
TinyJAMBU_GMU-v1	134.0	30%		856	196.8	188
KNOT-v2x1h	132.5	12%		2,532	159.4	154
SKINNY-AEAD-v1	131.3	45%	12	3,672	144.6	141
Romulus-v1	131.0	23%		1,735	143.2	140
Elephant-v5	129.9	15%	13	3,926	126.9	125
SKINNY-AEAD-v2	127.6	45%		3,532	139.5	140
Romulus-v4	123.0	18%		3,409	40.4	42
Elephant-v2	121.7	16%		2,729	113.2	119
Gimli_GT-v6	120.6	8%		4,820	45.2	48
Elephant-v3	113.5	16%		2,504	123.2	139
ForkAE-v2	112.2	63%	14	3,200	148.1	169
LOCUS-v2	106.6	38%	15	2,828	132.4	159
Spook-v2-v2	97.8	17%	16	3,188	108.5	142
Gimli_GT-v7	89.8	9%		**6,379**	32.3	46
Elephant-v4	89.7	15%		3,050	157.6	225
SCHWAEMM-v2	89.2	15%		**5,773**	85.7	123
COMET_CI-v3	88.6	34%	17	4,379	114.8	166
Saturnin-v2	86.3	9%	18	3,892	104.6	155
SCHWAEMM-v1	85.1	15%	19	4,713	81.8	123
COMET_CI-v1	83.7	34%		4,663	115.8	177
Oribatida-v1	83.1	24%	20	2,512	185.7	286
LOTUS-v2	80.2	38%		2,445	99.6	159
Oribatida-v2	79.2	25%		2,221	174.5	282
ISAP-v4	78.4	11%	21	3,026	155.0	253
SpoC_IIT-v1	75.5	47%	22	2,250	182.2	309
TinyJAMBU_GMU-v2	72.2	30%		841	196.2	348
ISAP-v1	66.4	9%		4,589	126.6	244
ISAP-v3	65.7	9%		3,767	131.9	257
SPIX-v1	65.3	16%	23	3,525	82.1	161
ISAP-v2	63.9	12%		3,852	136.4	273
ACE_GMU-v1	58.7	21%	24	4,473	77.0	168
LOCUS-v1	54.8	39%		2,978	125.8	294
ESTATE-v3	54.5	48%		2,279	180.2	423
COMET_VT-v2	53.2	32%		**5,204**	110.6	266
SpoC_VT-v1	47.6	48%		1,696	167.7	451
Elephant-v1	47.5	16%		2,056	163.1	439
LOTUS-v1	45.1	39%		2,642	103.5	294
ESTATE-v2	44.9	45%		1,946	174.3	497
mixFeed-v1	42.4	24%	25*	**5,363**	73.2	221
TinyJAMBU_TJT-v1	37.5	29%		686	200.8	686
SPIX-v2x4	31.6	15%		2,310	132.6	537
Saturnin-v1	27.9	15%		3,802	145.0	665
SPIX-v2x2	21.8	15%		1,993	134.7	791
COMET_CI-v2	21.7	34%		2,629	132.9	783
Pyjamask-v2	20.1	17%		**8,692**	90.6	577

Table 54 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
WAGE-v1	19.4	22%	26	1,774	159.6	1,053
ESTATE-v4	17.8	48%		1,572	200.1	1,437
ForkAE-v1	13.7	95%		2,129	135.7	1,272
SPIX-v2	13.0	15%		1,864	130.6	1,289
ACE_UW-v1	11.5	22%		1,903	106.5	1,185
Pyjamask-v1	11.3	21%	27*	**8,599**	109.7	1,245
Xoodyak_GMU-v2	9.4	9%		**5,871**	77.0	1,050
Romulus-v5	6.2	24%		1,960	130.2	2,695
TinyJAMBU_GMU-v3	4.8	30%		817	191.1	5,148
Gimli_TUM-v1	4.1	25%		2,044	101.3	3,159
Gimli_TUM-v2	2.1	25%		2,074	97.3	5,915
Gimli_TUM-v3	1.1	25%		2,115	100.5	11,427
Minimum		**6%**				
Average		**23%**				
Maximum		**95%**				

Table 55: Intel Cyclone 10 LP Encryption AD+PT Throughput for 1536 Byte Messages

Variant	Through-put 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	2,650.8	47%	1	1,264	174.5	809
Subterranean_ST-v2	2,314.2	47%		1,285	153.7	816
Xoodyak_GMU2-v1	1,568.7	44%	2	2,575	170.3	1,334
Ascon_GMU-v1	1,454.9	48%	3	4,552	118.4	1,000
Gimli_GMU-v4	1,356.8	48%	4	2,953	153.4	1,389
Xoodyak_GMU2-v2	1,325.5	48%		**5,058**	97.2	901
Ascon_GMU-v2	1,107.1	48%		3,113	160.6	1,783
Ascon_GMU2-v2h	1,051.8	49%		3,215	134.8	1,575
Gimli_GMU-v5	1,011.4	48%		**5,576**	82.4	1,001
Ascon_GMU2-v3h	949.1	49%		4,161	91.7	1,187
KNOT-v2x4	940.7	48%	5	3,519	102.0	1,333
KNOT-v2x4h	936.0	48%		3,678	101.5	1,333
KNOT-v2x2h	916.4	48%		2,792	140.1	1,879
KNOT-v2x2	907.2	48%		2,472	138.7	1,879
Gimli_GT-v4	902.8	48%		**5,010**	88.2	1,200
Gimli_GT-v5	885.4	47%		**5,948**	58.6	813
Ascon_Graz-v4	846.6	49%		3,730	108.7	1,577
Xoodyak_XT-v1	798.9	46%		2,231	136.3	2,097
Ascon_GMU2-v1h	786.9	49%		2,415	175.6	2,742
GIFT-COFB_GMU-v4	774.8	49%	6	2,609	110.8	1,757
GIFT-COFB_GMU-v3	755.7	49%		2,523	131.8	2,143
Xoodyak_XT-v7	753.2	46%		2,272	128.5	2,097
Ascon_Graz-v2	746.1	49%		2,634	143.3	2,361
Xoodyak_XT-v8	741.3	47%		3,630	90.0	1,491
Gimli_GMU-v2	739.1	49%		2,158	153.9	2,559
Xoodyak_XT-v2	732.1	47%		3,541	88.8	1,491
Ascon_Graz-v3	687.5	49%		3,716	109.7	1,960
Gimli_GT-v6	686.2	47%		4,820	45.2	810
Gimli_GT-v3	662.8	48%		3,651	85.8	1,590
Ascon_Graz-v5	626.7	49%		4,905	80.1	1,571
Xoodyak_GMU-v1	625.8	46%		3,135	106.8	2,097
Gimli_GT-v2	595.2	49%		3,145	114.8	2,370
Ascon_VT-v2	570.9	49%		2,695	172.0	3,702
Ascon_VT-v1	557.5	49%		2,432	176.6	3,893
Ascon_Graz-v1	556.6	49%		2,517	141.4	3,121
GIFT-COFB_GMU-v5	536.7	49%		4,828	51.5	1,178
KNOT-v2x1	531.5	48%		2,059	161.7	3,739
KNOT-v2x1h	523.9	48%		2,532	159.4	3,739
Gimli_GT-v7	490.6	48%		**6,379**	32.3	808
GIFT-COFB_GMU-v2	472.2	49%		2,111	156.5	4,073
GIFT-COFB_GMU-v6	462.8	49%		**6,630**	37.2	987
TinyJAMBU_TJT-v3	459.9	49%	7	1,021	159.7	4,267
Elephant-v5	439.8	49%	8	3,926	126.9	3,545
DryGASCON-v1	392.8	49%	9	3,199	130.5	4,083
Gimli_GMU-v1	387.5	49%		1,908	154.5	4,899
Gimli_GT-v1	372.5	49%		2,378	142.8	4,710
Romulus-v2	358.9	49%	10	2,086	141.7	4,852

Table 55 continued from previous page

Variant	Through-put 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Romulus-v3	345.3	49%		2,407	79.3	2,822
Saturnin-v2	316.5	48%	11	3,892	104.6	4,059
COMET_VT-v1	312.3	49%		**10,200**	88.9	3,498
Elephant-v4	289.7	49%		3,050	157.6	6,685
Spook-v2-v2	283.6	49%	12	3,188	108.5	4,702
Romulus-v4	274.5	49%		3,409	40.4	1,807
Elephant-v2	266.8	49%		2,729	113.2	5,211
ISAP-v3	265.5	47%	13	3,767	131.9	6,104
ISAP-v4	261.3	47%		3,026	155.0	7,289
PHOTON-Beetle-v1	261.0	50%	14	3,602	125.4	5,905
ISAP-v1	255.4	47%		4,589	126.6	6,091
SCHWAEMM-v2	252.0	49%		**5,773**	85.7	4,181
GIFT-COFB_GMU-v1	247.6	50%		1,903	159.8	7,933
Elephant-v3	246.5	49%		2,504	123.2	6,143
GIFT-COFB_VT-v1	244.3	50%		1,877	184.4	9,276
SCHWAEMM-v1	240.3	49%	15	4,713	81.8	4,181
ISAP-v2	198.2	48%		3,852	136.4	8,456
Romulus-v1	197.5	50%		1,735	143.2	8,912
SPIX-v1	183.1	49%	16	3,525	82.1	5,512
SKINNY-AEAD-v1	141.5	50%	17	3,672	144.6	12,558
SKINNY-AEAD-v2	136.5	50%		3,532	139.5	12,557
TinyJAMBU_TJT-v2	135.5	50%		777	196.2	17,795
ACE_GMU-v1	134.4	49%	18	4,473	77.0	7,044
TinyJAMBU_GMU-v1	130.3	50%		856	196.8	18,564
COMET_CI-v3	119.4	50%	19	4,379	114.8	11,822
Oribatida-v1	114.1	49%	20	2,512	185.7	19,995
ESTATE-v1	113.8	50%	21	3,839	118.0	12,736
COMET_CI-v1	112.9	50%		4,663	115.8	12,597
Oribatida-v2	105.1	50%		2,221	174.5	20,400
SPIX-v2x4	103.0	49%		2,310	132.6	15,818
Elephant-v1	99.6	49%		2,056	163.1	20,123
LOCUS-v2	93.6	50%	22	2,828	132.4	17,379
mixFeed-v1	83.4	49%	23*	**5,363**	73.2	10,778
ForkAE-v2	82.5	50%	24	3,200	148.1	22,050
COMET_VT-v2	80.5	49%		**5,204**	110.6	16,885
SpoC_IIT-v1	78.9	50%	25	2,250	182.2	28,388
SPIX-v2x2	72.1	49%		1,993	134.7	22,948
LOTUS-v2	70.5	50%		2,445	99.6	17,379
TinyJAMBU_GMU-v2	67.8	50%		841	196.2	35,572
Saturnin-v1	61.3	49%		3,802	145.0	29,049
Pyjamask-v2	56.6	49%		**8,692**	90.6	19,680
SpoC_VT-v1	48.5	50%		1,696	167.7	42,473
LOCUS-v1	46.8	50%		2,978	125.8	33,012
WAGE-v1	44.0	49%	26	1,774	159.6	44,601
SPIX-v2	43.1	49%		1,864	130.6	37,198
LOTUS-v1	38.5	50%		2,642	103.5	33,012
ESTATE-v3	37.5	50%		2,279	180.2	58,976
TinyJAMBU_TJT-v1	35.8	50%		686	200.8	68,846

Table 55 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Xoodyak_GMU-v2	35.7	45%		**5,871**	77.0	26,548
ESTATE-v2	32.8	50%		1,946	174.3	65,364
COMET_CI-v2	30.0	50%		2,629	132.9	54,375
Pyjamask-v1	26.5	49%	27*	**8,599**	109.7	50,908
ACE_UW-v1	25.7	49%		1,903	106.5	50,845
ESTATE-v4	12.2	50%		1,572	200.1	201,194
Romulus-v5	8.4	50%		1,960	130.2	189,935
Gimli_TUM-v1	8.1	49%		2,044	101.3	153,573
TinyJAMBU_GMU-v3	4.3	50%		817	191.1	545,812
Gimli_TUM-v2	4.2	49%		2,074	97.3	288,121
ForkAE-v1	3.9	50%		2,129	135.7	422,754
Gimli_TUM-v3	2.2	49%		2,115	100.5	557,217
Minimum		**44%**				
Average		**49%**				
Maximum		**50%**				

Table 56: Intel Cyclone 10 LP Encryption AD+PT Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	1,224.0	22%	1	1,264	174.5	73
Subterranean_ST-v2	983.6	20%		1,285	153.7	80
Xoodyak_GMU2-v1	778.5	22%	2	2,575	170.3	112
Gimli_GMU-v4	777.5	28%	3	2,953	153.4	101
Ascon_GMU-v1	757.8	25%	4	4,552	118.4	80
Ascon_GMU2-v2h	670.1	31%		3,215	134.8	103
Ascon_GMU-v2	647.6	28%		3,113	160.6	127
Xoodyak_GMU2-v2	638.0	23%		**5,058**	97.2	78
GIFT-COFB_GMU-v3	567.1	37%	5	2,523	131.8	119
Ascon_GMU2-v3h	565.5	29%		4,161	91.7	83
KNOT-v2x4	561.8	29%	6	3,519	102.0	93
GIFT-COFB_GMU-v4	561.6	36%		2,609	110.8	101
KNOT-v2x4h	559.0	29%		3,678	101.5	93
Ascon_GMU2-v1h	541.6	34%		2,415	175.6	166
Ascon_Graz-v4	529.8	30%		3,730	108.7	105
Gimli_GMU-v5	520.8	25%		**5,576**	82.4	81
Xoodyak_XT-v1	502.2	29%		2,231	136.3	139
KNOT-v2x2h	501.7	26%		2,792	140.1	143
KNOT-v2x2	496.7	26%		2,472	138.7	143
Ascon_Graz-v2	479.7	31%		2,634	143.3	153
Xoodyak_XT-v8	474.8	30%		3,630	90.0	97
Xoodyak_XT-v7	473.4	29%		2,272	128.5	139
Gimli_GMU-v2	471.9	31%		2,158	153.9	167
Gimli_GT-v4	470.2	25%		**5,010**	88.2	96
Xoodyak_XT-v2	468.9	30%		3,541	88.8	97
Ascon_Graz-v3	467.9	33%		3,716	109.7	120
Ascon_VT-v2	427.5	37%		2,695	172.0	206
Ascon_VT-v1	424.6	38%		2,432	176.6	213
Ascon_Graz-v5	414.4	32%		4,905	80.1	99
Ascon_Graz-v1	409.0	36%		2,517	141.4	177
Xoodyak_GMU-v1	393.4	29%		3,135	106.8	139
Gimli_GT-v5	389.5	21%		**5,948**	58.6	77
GIFT-COFB_GMU-v2	383.4	40%		2,111	156.5	209
TinyJAMBU_TJT-v3	373.3	40%	7	1,021	159.7	219
Gimli_GT-v3	372.1	27%		3,651	85.8	118
Gimli_GT-v2	362.8	30%		3,145	114.8	162
GIFT-COFB_GMU-v5	356.0	32%		4,828	51.5	74
Gimli_GT-v6	312.9	22%		4,820	45.2	74
KNOT-v2x1	310.1	28%		2,059	161.7	267
KNOT-v2x1h	305.7	28%		2,532	159.4	267
DryGASCON-v1	305.2	38%	8	3,199	130.5	219
Romulus-v2	287.9	40%	9	2,086	141.7	252
GIFT-COFB_GMU-v6	284.0	30%		**6,630**	37.2	67
Elephant-v5	274.1	30%	10	3,926	126.9	237
Gimli_GMU-v1	264.5	33%		1,908	154.5	299
Romulus-v3	263.6	38%		2,407	79.3	154
Gimli_GT-v1	248.7	33%		2,378	142.8	294

Table 56 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
COMET_VT-v1	244.7	39%		**10,200**	88.9	186
Gimli_GT-v7	229.4	22%		**6,379**	32.3	72
PHOTON-Beetle-v1	219.2	42%	11	3,602	125.4	293
GIFT-COFB_VT-v1	212.6	43%		1,877	184.4	444
GIFT-COFB_GMU-v1	210.4	42%		1,903	159.8	389
Romulus-v4	196.8	35%		3,409	40.4	105
Elephant-v2	195.7	36%		2,729	113.2	296
Spook-v2-v2	194.3	34%	12	3,188	108.5	286
Elephant-v4	184.6	31%		3,050	157.6	437
Elephant-v3	181.3	36%		2,504	123.2	348
Romulus-v1	163.7	41%		1,735	143.2	448
SCHWAEMM-v2	162.0	31%		**5,773**	85.7	271
Saturnin-v2	160.8	24%	13	3,892	104.6	333
SCHWAEMM-v1	154.5	31%	14	4,713	81.8	271
SKINNY-AEAD-v1	123.8	43%	15	3,672	144.6	598
SKINNY-AEAD-v2	119.6	44%		3,532	139.5	597
ISAP-v4	119.3	22%	16	3,026	155.0	665
SPIX-v1	116.8	31%	17	3,525	82.1	360
TinyJAMBU_TJT-v2	115.9	42%		777	196.2	867
TinyJAMBU_GMU-v1	112.0	43%		856	196.8	900
ISAP-v3	109.6	19%		3,767	131.9	616
ISAP-v1	107.5	20%		4,589	126.6	603
ESTATE-v1	102.0	45%	18	3,839	118.0	592
COMET_CI-v3	98.3	41%	19	4,379	114.8	598
ISAP-v2	95.9	23%		3,852	136.4	728
ACE_GMU-v1	93.9	34%	20	4,473	77.0	420
COMET_CI-v1	93.0	41%		4,663	115.8	637
Oribatida-v1	91.1	40%	21	2,512	185.7	1,043
LOCUS-v2	82.8	44%	22	2,828	132.4	819
Oribatida-v2	79.5	37%		2,221	174.5	1,124
ForkAE-v2	77.2	47%	23	3,200	148.1	982
Elephant-v1	74.0	37%		2,056	163.1	1,128
SpoC_IIT-v1	69.6	44%	24	2,250	182.2	1,340
COMET_VT-v2	64.6	40%		**5,204**	110.6	877
LOTUS-v2	62.3	44%		2,445	99.6	819
SPIX-v2x4	61.9	29%		2,310	132.6	1,098
TinyJAMBU_GMU-v2	58.5	43%		841	196.2	1,716
mixFeed-v1	56.9	33%	25*	**5,363**	73.2	658
SpoC_VT-v1	43.1	44%		1,696	167.7	1,993
SPIX-v2x2	43.0	29%		1,993	134.7	1,604
LOCUS-v1	41.6	44%		2,978	125.8	1,548
Saturnin-v1	39.8	32%		3,802	145.0	1,863
Pyjamask-v2	36.3	31%		**8,692**	90.6	1,280
ESTATE-v3	34.5	46%		2,279	180.2	2,672
LOTUS-v1	34.2	44%		2,642	103.5	1,548
WAGE-v1	30.8	34%	26	1,774	159.6	2,649
TinyJAMBU_TJT-v1	30.8	43%		686	200.8	3,342
ESTATE-v2	29.9	45%		1,946	174.3	2,988

Table 56 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
SPIX-v2	25.6	29%		1,864	130.6	2,606
COMET_CI-v2	24.6	41%		2,629	132.9	2,763
Xoodyak_GMU-v2	21.4	27%		**5,871**	77.0	1,842
Pyjamask-v1	18.3	34%	27*	**8,599**	109.7	3,068
ACE_UW-v1	18.1	35%		1,903	106.5	3,005
ESTATE-v4	11.3	46%		1,572	200.1	9,098
Romulus-v5	7.2	42%		1,960	130.2	9,247
Gimli_TUM-v1	6.0	36%		2,044	101.3	8,673
ForkAE-v1	3.9	50%		2,129	135.7	17,678
TinyJAMBU_GMU-v3	3.7	43%		817	191.1	26,196
Gimli_TUM-v2	3.1	36%		2,074	97.3	16,261
Gimli_TUM-v3	1.6	36%		2,115	100.5	31,437
Minimum		**19%**				
Average		**34%**				
Maximum		**50%**				

Table 57: Intel Cyclone 10 LP Encryption AD+PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	455.9	8%	1	1,264	174.5	49
Subterranean_ST-v2	351.3	7%		1,285	153.7	56
Gimli_GMU-v4	332.7	12%	2	2,953	153.4	59
GIFT-COFB_GMU-v3	318.3	21%	3	2,523	131.8	53
Ascon_GMU2-v2h	313.7	15%	4	3,215	134.8	55
Ascon_GMU-v1	303.1	10%		4,552	118.4	50
GIFT-COFB_GMU-v4	301.7	19%		2,609	110.8	47
Xoodyak_GMU2-v1	298.6	8%	5	2,575	170.3	73
Ascon_GMU-v2	281.7	12%		3,113	160.6	73
Ascon_GMU2-v1h	274.1	17%		2,415	175.6	82
Ascon_GMU2-v3h	249.7	13%		4,161	91.7	47
KNOT-v2x4	246.5	13%	6	3,519	102.0	53
KNOT-v2x4h	245.2	13%		3,678	101.5	53
Ascon_Graz-v4	244.0	14%		3,730	108.7	57
Ascon_VT-v1	243.1	22%		2,432	176.6	93
GIFT-COFB_GMU-v2	241.4	25%		2,111	156.5	83
Ascon_VT-v2	239.3	21%		2,695	172.0	92
Xoodyak_GMU2-v2	239.2	9%		**5,058**	97.2	52
TinyJAMBU_TJT-v3	234.9	25%	7	1,021	159.7	87
Ascon_Graz-v3	233.9	17%		3,716	109.7	60
Xoodyak_XT-v1	229.6	13%		2,231	136.3	76
Ascon_Graz-v2	226.5	15%		2,634	143.3	81
Ascon_Graz-v1	223.4	20%		2,517	141.4	81
Xoodyak_XT-v8	221.4	14%		3,630	90.0	52
Gimli_GMU-v2	221.4	15%		2,158	153.9	89
Xoodyak_XT-v2	218.7	14%		3,541	88.8	52
Xoodyak_XT-v7	216.5	13%		2,272	128.5	76
Romulus-v2	215.9	30%	8	2,086	141.7	84
Gimli_GMU-v5	206.8	10%		**5,576**	82.4	51
KNOT-v2x2h	206.2	11%		2,792	140.1	87
KNOT-v2x2	204.1	11%		2,472	138.7	87
Ascon_Graz-v5	201.1	16%		4,905	80.1	51
Gimli_GT-v4	188.1	10%		**5,010**	88.2	60
Romulus-v3	181.3	26%		2,407	79.3	56
Xoodyak_GMU-v1	179.9	13%		3,135	106.8	76
DryGASCON-v1	179.7	23%	9	3,199	130.5	93
GIFT-COFB_GMU-v5	173.3	16%		4,828	51.5	38
Gimli_GT-v2	163.3	13%		3,145	114.8	90
Gimli_GT-v3	156.8	11%		3,651	85.8	70
GIFT-COFB_VT-v1	151.3	31%		1,877	184.4	156
PHOTON-Beetle-v1	146.0	28%	10	3,602	125.4	110
COMET_VT-v1	145.9	23%		**10,200**	88.9	78
GIFT-COFB_GMU-v1	143.1	29%		1,903	159.8	143
Gimli_GT-v5	141.5	8%		**5,948**	58.6	53
KNOT-v2x1	133.6	12%		2,059	161.7	155
Gimli_GMU-v1	132.7	17%		1,908	154.5	149
KNOT-v2x1h	131.6	12%		2,532	159.4	155

Table 57 continued from previous page

Variant	Through-put 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
Romulus-v1	131.0	33%		1,735	143.2	140
Elephant-v5	129.9	14%	11	3,926	126.9	125
GIFT-COFB_GMU-v6	128.6	14%		**6,630**	37.2	37
Romulus-v4	123.0	22%		3,409	40.4	42
Gimli_GT-v1	121.8	16%		2,378	142.8	150
Elephant-v2	121.7	23%		2,729	113.2	119
Gimli_GT-v6	115.8	8%		4,820	45.2	50
Elephant-v3	113.5	23%		2,504	123.2	139
Elephant-v4	89.7	15%		3,050	157.6	225
SKINNY-AEAD-v1	89.0	31%	12	3,672	144.6	208
SKINNY-AEAD-v2	86.3	31%		3,532	139.5	207
Gimli_GT-v7	86.0	8%		**6,379**	32.3	48
TinyJAMBU_TJT-v2	79.7	29%		777	196.2	315
TinyJAMBU_GMU-v1	77.8	30%		856	196.8	324
ESTATE-v1	77.0	34%	13	3,839	118.0	196
Saturnin-v2	73.5	11%	14	3,892	104.6	182
Spook-v2-v2	73.1	13%	15	3,188	108.5	190
ForkAE-v2	64.3	39%	16	3,200	148.1	295
COMET_CI-v3	63.4	26%	17	4,379	114.8	232
LOCUS-v2	60.8	32%	18	2,828	132.4	279
SCHWAEMM-v2	60.3	12%		**5,773**	85.7	182
COMET_CI-v1	60.0	26%		4,663	115.8	247
SCHWAEMM-v1	57.5	12%	19	4,713	81.8	182
Oribatida-v1	55.9	24%	20	2,512	185.7	425
SPIX-v1	54.7	15%	21	3,525	82.1	192
SpoC_IIT-v1	50.9	32%	22	2,250	182.2	458
ACE_GMU-v1	48.3	18%	23	4,473	77.0	204
Elephant-v1	47.5	24%		2,056	163.1	439
LOTUS-v2	45.7	32%		2,445	99.6	279
Oribatida-v2	45.4	21%		2,221	174.5	492
ISAP-v4	44.2	8%	24	3,026	155.0	449
TinyJAMBU_GMU-v2	41.0	30%		841	196.2	612
COMET_VT-v2	39.9	25%		**5,204**	110.6	355
ISAP-v3	39.8	7%		3,767	131.9	424
ISAP-v1	39.4	7%		4,589	126.6	411
ISAP-v2	36.7	9%		3,852	136.4	476
SpoC_VT-v1	31.9	33%		1,696	167.7	673
LOCUS-v1	30.8	33%		2,978	125.8	522
mixFeed-v1	28.5	17%	25*	**5,363**	73.2	328
ESTATE-v3	27.6	37%		2,279	180.2	836
SPIX-v2x4	27.5	13%		2,310	132.6	618
LOTUS-v1	25.4	33%		2,642	103.5	522
ESTATE-v2	23.4	36%		1,946	174.3	954
Saturnin-v1	21.5	17%		3,802	145.0	862
TinyJAMBU_TJT-v1	21.3	30%		686	200.8	1,206
SPIX-v2x2	19.0	13%		1,993	134.7	908
Pyjamask-v2	17.1	15%		**8,692**	90.6	680
WAGE-v1	15.9	18%	26	1,774	159.6	1,281

Table 57 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
COMET_CI-v2	15.8	26%		2,629	132.9	1,080
SPIX-v2	11.3	13%		1,864	130.6	1,478
ACE_UW-v1	9.4	18%		1,903	106.5	1,445
Xoodyak_GMU-v2	9.4	12%		**5,871**	77.0	1,053
Pyjamask-v1	9.3	17%	27*	**8,599**	109.7	1,508
ESTATE-v4	9.0	37%		1,572	200.1	2,834
Romulus-v5	6.2	36%		1,960	130.2	2,695
ForkAE-v1	3.9	49%		2,129	135.7	4,469
Gimli_TUM-v1	3.3	20%		2,044	101.3	3,948
TinyJAMBU_GMU-v3	2.6	31%		817	191.1	9,252
Gimli_TUM-v2	1.7	20%		2,074	97.3	7,396
Gimli_TUM-v3	0.9	20%		2,115	100.5	14,292
Minimum		**7%**				
Average		**20%**				
Maximum		**49%**				

Table 58: Intel Cyclone 10 LP Hash Throughput for 1536 Byte Messages

Variant	**Through-put 1536B [Mbit/s]**	**Thr HM 1536B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 1536B**
Gimli_GMU-v4	2,696.2	96%	1	2,953	153.4	699
Gimli_GMU-v5	2,012.7	95%		**5,576**	82.4	503
Gimli_GT-v4	1,793.6	95%		**5,010**	88.2	604
Gimli_GT-v5	1,764.3	94%		**5,948**	58.6	408
Xoodyak_GMU2-v2	1,720.9	97%		**5,058**	97.2	694
Xoodyak_GMU2-v1	1,633.6	97%	2	2,575	170.3	1,281
Gimli_GMU-v2	1,469.6	97%		2,158	153.9	1,287
Gimli_GT-v6	1,368.9	95%		4,820	45.2	406
Gimli_GT-v3	1,317.3	96%		3,651	85.8	800
Ascon_GMU2-v2h	1,196.9	97%	3	3,215	134.8	1,384
Gimli_GT-v2	1,183.4	97%		3,145	114.8	1,192
Ascon_GMU2-v3h	1,137.9	97%		4,161	91.7	990
Xoodyak_XT-v8	1,029.1	98%		3,630	90.0	1,074
Gimli_GT-v7	981.2	95%		**6,379**	32.3	404
Xoodyak_XT-v7	953.7	99%		2,272	128.5	1,656
SHA2-v1	927.8	99%	4	2,139	118.6	1,571
Ascon_Graz-v3	853.4	97%		3,716	109.7	1,579
Ascon_Graz-v4	845.5	97%		3,730	108.7	1,579
Ascon_GMU2-v1h	840.9	97%		2,415	175.6	2,566
Ascon_Graz-v5	830.8	97%		4,905	80.1	1,185
Xoodyak_GMU-v1	792.4	99%		3,135	106.8	1,656
DryGASCON-v1	786.6	99%	5	3,199	130.5	2,039
Saturnin-v2	777.3	96%	6	3,892	104.6	1,653
Gimli_GMU-v1	770.8	97%		1,908	154.5	2,463
Gimli_GT-v1	740.9	97%		2,378	142.8	2,368
Ascon_VT-v2	715.0	97%		2,695	172.0	2,956
Ascon_Graz-v2	638.0	97%		2,634	143.3	2,761
KNOT-v2x4h	631.4	97%	7	3,678	101.5	1,976
Ascon_Graz-v1	629.2	97%		2,517	141.4	2,761
Subterranean_ST-v2	609.6	99%	8	1,285	153.7	3,098
KNOT-v2x2h	437.5	98%		2,792	140.1	3,936
SCHWAEMM-v2	317.3	98%	9*	**5,773**	85.7	3,320
ACE_GMU-v1	266.9	97%	10	4,473	77.0	3,548
KNOT-v2x1h	249.3	98%		2,532	159.4	7,856
PHOTON-Beetle-v1	161.1	100%	11	3,602	125.4	9,566
Saturnin-v1	118.9	98%		3,802	145.0	14,981
ACE_UW-v1	51.1	97%		1,903	106.5	25,608
Xoodyak_GMU-v2	37.7	99%		**5,871**	77.0	25,142
Gimli_TUM-v1	16.2	98%		2,044	101.3	77,046
Gimli_TUM-v2	8.3	98%		2,074	97.3	144,482
Gimli_TUM-v3	4.4	98%		2,115	100.5	279,354
Minimum		**94%**				
Average		**97%**				
Maximum		**100%**				

Table 59: Intel Cyclone 10 LP Hash Throughput for 64 Byte Messages

Variant	Throughput 64B [Mbit/s]	Thr HM 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Gimli_GMU-v4	1,427.7	51%	1	2,953	153.4	55
Xoodyak_GMU2-v1	1,025.8	61%	2	2,575	170.3	85
Xoodyak_GMU2-v2	995.2	56%		**5,058**	97.2	50
Gimli_GMU-v5	981.0	47%		**5,576**	82.4	43
Gimli_GT-v4	868.0	46%		**5,010**	88.2	52
Gimli_GMU-v2	866.0	57%		2,158	153.9	91
SHA2-v1	799.1	86%	3	2,139	118.6	76
Gimli_GT-v5	749.8	40%		**5,948**	58.6	40
Xoodyak_XT-v8	742.8	71%		3,630	90.0	62
Ascon_GMU2-v2h	719.0	58%	4	3,215	134.8	96
Xoodyak_XT-v7	715.3	74%		2,272	128.5	92
Gimli_GT-v3	686.1	50%		3,651	85.8	64
Ascon_GMU2-v3h	670.6	57%		4,161	91.7	70
Gimli_GT-v2	667.9	55%		3,145	114.8	88
DryGASCON-v1	624.6	79%	5	3,199	130.5	107
Gimli_GT-v6	609.4	42%		4,820	45.2	38
Xoodyak_GMU-v1	594.3	74%		3,135	106.8	92
Ascon_Graz-v3	524.7	60%		3,716	109.7	107
Ascon_Graz-v4	519.9	60%		3,730	108.7	107
Ascon_GMU2-v1h	516.7	60%		2,415	175.6	174
Subterranean_ST-v2	510.9	83%	6	1,285	153.7	154
Ascon_Graz-v5	506.4	59%		4,905	80.1	81
Gimli_GMU-v1	485.3	61%		1,908	154.5	163
Gimli_GT-v7	458.8	44%		**6,379**	32.3	36
Gimli_GT-v1	456.9	60%		2,378	142.8	160
Ascon_VT-v2	449.3	61%		2,695	172.0	196
Ascon_Graz-v2	396.7	61%		2,634	143.3	185
Saturnin-v2	396.6	49%	7	3,892	104.6	135
Ascon_Graz-v1	391.3	61%		2,517	141.4	185
KNOT-v2x4h	382.3	59%	8	3,678	101.5	136
KNOT-v2x2h	280.3	62%		2,792	140.1	256
SCHWAEMM-v2	228.6	71%	9*	**5,773**	85.7	192
PHOTON-Beetle-v1	175.5	109%	10	3,602	125.4	366
ACE_GMU-v1	167.2	61%	11	4,473	77.0	236
KNOT-v2x1h	164.6	65%		2,532	159.4	496
Saturnin-v1	78.0	64%		3,802	145.0	951
ACE_UW-v1	32.3	62%		1,903	106.5	1,688
Xoodyak_GMU-v2	30.0	79%		**5,871**	77.0	1,314
Gimli_TUM-v1	11.0	66%		2,044	101.3	4,734
Gimli_TUM-v2	5.6	66%		2,074	97.3	8,874
Gimli_TUM-v3	3.0	66%		2,115	100.5	17,154
Minimum		**40%**				
Average		**62%**				
Maximum		**109%**				

Table 60: Intel Cyclone 10 LP Hash Throughput for 16 Byte Messages

Variant	**Throughput 16B [Mbit/s]**	**Thr HM 16B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 16B**
Gimli_GMU-v4	577.4	21%	1	2,953	153.4	34
Xoodyak_GMU2-v1	473.9	28%	2	2,575	170.3	46
Xoodyak_GMU2-v2	429.0	24%		**5,058**	97.2	29
Xoodyak_XT-v7	401.3	41%		2,272	128.5	41
Xoodyak_XT-v8	397.0	38%		3,630	90.0	29
DryGASCON-v1	379.7	48%	3	3,199	130.5	44
Gimli_GMU-v2	378.9	25%		2,158	153.9	52
Gimli_GMU-v5	376.6	18%		**5,576**	82.4	28
Subterranean_ST-v2	339.2	55%	4	1,285	153.7	58
Xoodyak_GMU-v1	333.4	41%		3,135	106.8	41
Gimli_GT-v4	331.9	18%		**5,010**	88.2	34
Ascon_GMU2-v2h	319.5	26%	5	3,215	134.8	54
Ascon_GMU2-v3h	293.4	25%		4,161	91.7	40
Gimli_GT-v2	282.6	23%		3,145	114.8	52
Gimli_GT-v3	274.4	20%		3,651	85.8	40
Gimli_GT-v5	267.8	14%		**5,948**	58.6	28
PHOTON-Beetle-v1	243.3	152%	6	3,602	125.4	66
Ascon_Graz-v3	237.9	27%		3,716	109.7	59
Ascon_Graz-v4	235.7	27%		3,730	108.7	59
Ascon_GMU2-v1h	234.1	27%		2,415	175.6	96
Ascon_Graz-v5	227.9	27%		4,905	80.1	45
Gimli_GMU-v1	224.7	28%		1,908	154.5	88
Gimli_GT-v6	222.7	15%		4,820	45.2	26
Ascon_VT-v2	207.7	28%		2,695	172.0	106
Gimli_GT-v1	207.7	27%		2,378	142.8	88
SHA2-v1	199.8	21%	7	2,139	118.6	76
Saturnin-v2	194.0	24%	8	3,892	104.6	69
Ascon_Graz-v2	181.7	28%		2,634	143.3	101
Ascon_Graz-v1	179.2	28%		2,517	141.4	101
Gimli_GT-v7	172.1	17%		**6,379**	32.3	24
KNOT-v2x4h	171.0	26%	9	3,678	101.5	76
KNOT-v2x2h	131.9	29%		2,792	140.1	136
SCHWAEMM-v2	121.9	38%	10*	**5,773**	85.7	90
KNOT-v2x1h	79.7	31%		2,532	159.4	256
ACE_GMU-v1	77.0	28%	11	4,473	77.0	128
Saturnin-v1	54.4	45%		3,802	145.0	341
Xoodyak_GMU-v2	18.4	48%		**5,871**	77.0	537
ACE_UW-v1	15.0	29%		1,903	106.5	908
Gimli_TUM-v1	5.5	33%		2,044	101.3	2,376
Gimli_TUM-v2	2.8	33%		2,074	97.3	4,452
Gimli_TUM-v3	1.5	33%		2,115	100.5	8,604
Minimum		**14%**				
Average		**32%**				
Maximum		**152%**				

Table 61: Lattice ECP5 Encryption PT Throughput for 1536 Byte Messages

Variant	Through-put 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	3,477.9	91%	1	1,471	120.0	424
Subterranean_ST-v2	2,716.7	89%		1,342	95.7	433
Xoodyak_GMU2-v1	2,073.0	93%	2	3,248	150.5	892
Ascon_GMU-v1	1,992.1	92%		**5,909**	84.3	520
Xoodyak_GMU2-v2	1,736.5	91%		4,058	69.7	493
Gimli_GMU-v4	1,626.9	94%	3	3,223	94.9	717
Ascon_GMU-v2	1,571.7	94%	4	4,641	117.2	916
Ascon_GMU2-v2h	1,358.5	95%		3,764	89.2	807
Gimli_GMU-v5	1,241.3	92%		4,586	52.5	520
Ascon_GMU2-v3h	1,230.8	94%		4,925	61.2	611
Gimli_GT-v4	1,194.0	92%		4,027	60.7	625
KNOT-v2x2	1,146.5	92%	5	3,287	90.4	969
Xoodyak_XT-v8	1,007.1	96%		4,121	71.3	870
Xoodyak_XT-v2	993.4	96%		4,077	70.3	870
Ascon_GMU2-v1h	969.5	96%		2,928	110.1	1,395
Gimli_GMU-v2	965.2	95%		2,617	103.0	1,311
KNOT-v2x2h	954.9	92%		3,373	75.3	969
Ascon_Graz-v4	944.1	95%		3,379	61.9	805
Xoodyak_XT-v1	924.5	96%		2,402	95.7	1,272
Gimli_GT-v6	904.4	90%		**6,341**	31.5	428
KNOT-v2x4	884.7	95%		3,984	63.2	878
Xoodyak_XT-v7	854.1	96%		2,489	88.4	1,272
Ascon_Graz-v5	853.1	96%		4,646	55.6	801
KNOT-v2x4h	851.9	95%		4,283	60.9	878
GIFT-COFB_GMU-v3	836.3	96%	6	3,059	74.7	1,098
Gimli_GT-v3	831.9	93%		4,451	55.6	822
Ascon_Graz-v6	785.7	95%		**5,346**	38.8	607
Ascon_Graz-v3	784.7	96%		3,305	63.7	997
GIFT-COFB_GMU-v4	778.4	96%		3,311	57.1	902
Gimli_GT-v2	768.8	95%		2,852	76.2	1,218
GIFT-COFB_GMU-v5	736.9	95%		3,821	36.5	608
Xoodyak_GMU-v1	714.9	96%		3,172	74.0	1,272
Gimli_GT-v5	665.8	89%		**5,738**	23.3	430
Ascon_Graz-v2	655.2	96%		2,603	64.0	1,201
Elephant-v5	624.0	95%	7	4,145	90.1	1,774
GIFT-COFB_GMU-v2	620.8	97%		2,628	105.0	2,078
COMET_VT-v1	616.5	98%		**5,266**	98.4	1,962
DryGASCON-v1	597.6	98%	8	3,801	100.5	2,067
KNOT-v2x1	547.2	93%		2,275	85.5	1,919
Ascon_VT-v1	530.9	98%		3,130	84.9	1,965
Ascon_VT-v2	522.4	97%		3,041	75.4	1,774
KNOT-v2x1h	505.4	93%		2,446	78.9	1,919
Gimli_GMU-v1	501.7	96%		2,328	102.0	2,499
Gimli_GT-v7	473.4	90%		**8,238**	16.4	427
Ascon_Graz-v1	459.6	97%		2,544	59.3	1,585
TinyJAMBU_TJT-v3	455.0	99%	9	1,092	115.4	3,116
Gimli_GT-v1	399.6	96%		2,537	78.2	2,406

Table 61 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Spook-v2-v2	394.6	96%	10	3,662	77.0	2,398
PHOTON-Beetle-v1	387.7	99%	11	3,294	101.4	3,215
Elephant-v4	355.6	96%		3,157	97.6	3,374
Saturnin-v2	351.3	94%	12	3,648	79.0	2,763
SCHWAEMM-v1	348.2	96%	13	4,685	66.3	2,341
SCHWAEMM-v2	334.8	96%		**5,947**	63.8	2,341
GIFT-COFB_GMU-v1	323.9	97%		2,727	106.5	4,038
Romulus-v2	322.5	98%	14	2,353	82.0	3,124
Romulus-v3	313.1	98%		3,847	45.0	1,766
Elephant-v2	312.4	98%		3,073	85.5	3,363
GIFT-COFB_VT-v1	304.2	98%		2,214	114.3	4,617
SPIX-v1	283.6	96%	15	2,432	69.3	3,004
Elephant-v3	272.3	98%		2,901	88.3	3,987
ACE_GMU-v1	255.3	97%	16	2,784	74.2	3,572
Romulus-v4	244.2	97%		**5,086**	21.6	1,087
ISAP-v3	202.9	90%		**5,703**	65.6	3,975
SKINNY-AEAD-v1	190.8	99%	17	3,174	101.1	6,512
ISAP-v1	189.5	90%		**6,701**	61.1	3,962
SKINNY-AEAD-v2	185.7	99%		3,182	98.4	6,511
ISAP-v4	179.5	92%	18	3,623	67.2	4,600
Romulus-v1	169.4	99%		1,998	80.5	5,840
Oribatida-v1	163.0	99%	19	1,671	176.5	13,301
ESTATE-v1	157.4	99%	20	2,855	109.0	8,512
COMET_VT-v2	157.0	98%	21	2,353	111.5	8,725
ISAP-v2	155.1	93%		**5,708**	68.0	5,384
COMET_CI-v3	152.5	98%		3,443	80.0	6,446
COMET_CI-v1	145.4	98%		3,255	80.9	6,837
SPIX-v2x4	131.5	95%		2,265	86.7	8,099
TinyJAMBU_TJT-v2	120.4	99%		689	125.4	12,803
TinyJAMBU_GMU-v1	116.3	99%		720	124.8	13,189
SpoC_IIT-v1	112.3	99%	22	2,153	132.2	14,468
Oribatida-v2	103.5	99%		2,497	114.2	13,564
ForkAE-v2	93.1	99%	23	3,571	90.0	11,878
Elephant-v1	89.8	98%		2,368	97.5	13,347
Pyjamask-v2	87.6	95%	24	4,162	73.2	10,263
mixFeed-v1	84.7	97%	25	3,479	38.9	5,641
SPIX-v2x2	83.8	95%		2,107	80.2	11,755
LOCUS-v2	76.7	99%	26	2,950	72.5	11,619
TinyJAMBU_GMU-v2	61.6	99%		908	128.3	25,589
Saturnin-v1	58.1	97%		3,070	92.6	19,593
SPIX-v2	57.5	95%		2,078	89.2	19,057
SpoC_VT-v1	56.0	99%		2,049	98.2	21,545
LOTUS-v2	55.7	99%		2,208	52.7	11,619
WAGE-v1	55.2	97%	27	2,081	101.6	22,600
Xoodyak_GMU-v2	52.5	95%		2,316	74.8	17,495
Pyjamask-v1	43.6	96%		3,897	92.7	26,131
LOCUS-v1	40.6	99%		2,857	73.0	22,068
COMET_CI-v2	39.9	98%		1,974	94.3	29,031

Table 61 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
ACE_UW-v1	35.2	97%		2,156	73.8	25,756
ESTATE-v3	33.4	99%		1,820	107.1	39,392
ESTATE-v2	32.5	99%		1,689	115.4	43,668
LOTUS-v1	30.4	99%		2,413	54.6	22,068
TinyJAMBU_TJT-v1	27.3	99%		580	111.3	50,030
Gimli_TUM-v1	12.3	97%		1,767	78.0	78,117
ESTATE-v4	10.8	99%		1,329	118.1	134,378
Romulus-v5	7.4	99%		1,961	76.5	126,575
Gimli_TUM-v2	6.2	97%		1,767	73.5	146,617
Gimli_TUM-v3	3.4	97%		1,772	78.5	283,617
TinyJAMBU_GMU-v3	3.3	99%		1,277	108.1	397,589
ForkAE-v1	2.7	100%		2,022	67.9	306,694
Minimum		**89%**				
Average		**96%**				
Maximum		**100%**				

Table 62: Lattice ECP5 Encryption PT Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	1,097.2	29%	1	1,471	120.0	56
Xoodyak_GMU2-v1	778.2	35%	2	3,248	150.5	99
Subterranean_ST-v2	754.1	25%		1,342	95.7	65
Ascon_GMU-v1	719.4	33%		**5,909**	84.3	60
Ascon_GMU-v2	681.7	41%	3	4,641	117.2	88
Gimli_GMU-v4	665.8	38%	4	3,223	94.9	73
Ascon_GMU2-v2h	643.4	45%		3,764	89.2	71
Xoodyak_GMU2-v2	540.5	28%		4,058	69.7	66
Ascon_GMU2-v3h	531.1	41%		4,925	61.2	59
Ascon_GMU2-v1h	526.6	52%		2,928	110.1	107
Xoodyak_XT-v8	486.7	46%		4,121	71.3	75
Xoodyak_XT-v2	480.1	46%		4,077	70.3	75
Ascon_Graz-v4	458.9	46%		3,379	61.9	69
Gimli_GMU-v2	458.5	45%		2,617	103.0	115
KNOT-v2x2	458.3	37%	5	3,287	90.4	101
KNOT-v2x4	449.5	48%		3,984	63.2	72
Gimli_GMU-v5	448.3	33%		4,586	52.5	60
GIFT-COFB_GMU-v3	444.9	51%	6	3,059	74.7	86
Xoodyak_XT-v1	441.4	46%		2,402	95.7	111
Ascon_Graz-v5	438.0	49%		4,646	55.6	65
KNOT-v2x4h	432.9	48%		4,283	60.9	72
Gimli_GT-v4	425.9	33%		4,027	60.7	73
Ascon_Graz-v3	423.4	52%		3,305	63.7	77
COMET_VT-v1	413.1	66%		**5,266**	98.4	122
Xoodyak_XT-v7	407.8	46%		2,489	88.4	111
GIFT-COFB_GMU-v4	395.3	49%		3,311	57.1	74
KNOT-v2x2h	381.7	37%		3,373	75.3	101
DryGASCON-v1	381.3	62%	7	3,801	100.5	135
GIFT-COFB_GMU-v2	368.1	58%		2,628	105.0	146
Ascon_Graz-v6	361.3	44%		**5,346**	38.8	55
Ascon_VT-v1	347.8	64%		3,130	84.9	125
TinyJAMBU_TJT-v3	343.5	74%	8	1,092	115.4	172
Gimli_GT-v2	342.2	42%		2,852	76.2	114
Xoodyak_GMU-v1	341.3	46%		3,172	74.0	111
Ascon_Graz-v2	338.0	49%		2,603	64.0	97
GIFT-COFB_GMU-v5	333.4	43%		3,821	36.5	56
Gimli_GT-v3	331.3	37%		4,451	55.6	86
Ascon_VT-v2	327.2	61%		3,041	75.4	118
PHOTON-Beetle-v1	290.2	74%	9	3,294	101.4	179
Elephant-v5	274.6	42%	10	4,145	90.1	168
Gimli_GT-v6	268.8	27%		**6,341**	31.5	60
Ascon_Graz-v1	268.6	57%		2,544	59.3	113
Gimli_GMU-v1	262.5	50%		2,328	102.0	199
KNOT-v2x1	239.1	41%		2,275	85.5	183
Romulus-v2	233.2	71%	11	2,353	82.0	180
KNOT-v2x1h	220.8	41%		2,446	78.9	183
Romulus-v3	209.5	65%		3,847	45.0	110

Table 62 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Spook-v2-v2	207.5	51%	12	3,662	77.0	190
GIFT-COFB_GMU-v1	204.9	62%		2,727	106.5	266
Gimli_GT-v1	202.3	48%		2,537	78.2	198
GIFT-COFB_VT-v1	199.7	64%		2,214	114.3	293
Elephant-v2	195.4	61%		3,073	85.5	224
Gimli_GT-v5	192.4	26%		**5,738**	23.3	62
SCHWAEMM-v1	189.8	53%	13	4,685	66.3	179
SCHWAEMM-v2	182.4	53%		**5,947**	63.8	179
Elephant-v3	171.3	62%		2,901	88.3	264
Elephant-v4	162.3	44%		3,157	97.6	308
SKINNY-AEAD-v1	148.8	77%	14	3,174	101.1	348
Romulus-v4	147.5	59%		**5,086**	21.6	75
ACE_GMU-v1	146.2	55%	15	2,784	74.2	260
SPIX-v1	145.5	49%	16	2,432	69.3	244
SKINNY-AEAD-v2	145.2	77%		3,182	98.4	347
Saturnin-v2	145.0	39%	17	3,648	79.0	279
Gimli_GT-v7	142.8	27%		**8,238**	16.4	59
ESTATE-v1	134.2	85%	18	2,855	109.0	416
Oribatida-v1	129.6	79%	19	1,671	176.5	697
Romulus-v1	128.8	75%		1,998	80.5	320
COMET_CI-v3	109.5	71%	20	3,443	80.0	374
COMET_VT-v2	106.3	66%		2,353	111.5	537
COMET_CI-v1	104.3	71%		3,255	80.9	397
TinyJAMBU_TJT-v2	97.4	80%		689	125.4	659
TinyJAMBU_GMU-v1	94.4	80%		720	124.8	677
SpoC_IIT-v1	89.0	78%	21	2,153	132.2	760
ForkAE-v2	82.0	88%	22	3,571	90.0	562
Oribatida-v2	77.5	74%		2,497	114.2	754
LOCUS-v2	64.1	83%	23	2,950	72.5	579
ISAP-v3	62.8	28%		**5,703**	65.6	535
ISAP-v4	62.3	32%	24	3,623	67.2	552
SPIX-v2x4	60.1	43%		2,265	86.7	739
ISAP-v1	59.9	29%		**6,701**	61.1	522
ISAP-v2	58.1	35%		**5,708**	68.0	599
Elephant-v1	57.8	63%		2,368	97.5	864
TinyJAMBU_GMU-v2	50.5	81%		908	128.3	1,301
mixFeed-v1	50.2	57%	25	3,479	38.9	397
LOTUS-v2	46.6	83%		2,208	52.7	579
SpoC_VT-v1	44.9	79%		2,049	98.2	1,121
Pyjamask-v2	42.6	46%	26	4,162	73.2	879
SPIX-v2x2	37.9	43%		2,107	80.2	1,083
LOCUS-v1	34.2	84%		2,857	73.0	1,092
Saturnin-v1	32.3	54%		3,070	92.6	1,469
WAGE-v1	32.0	56%	27	2,081	101.6	1,624
ESTATE-v3	29.6	88%		1,820	107.1	1,856
ESTATE-v2	28.3	87%		1,689	115.4	2,084
COMET_CI-v2	28.3	70%		1,974	94.3	1,707
SPIX-v2	25.9	43%		2,078	89.2	1,761

Table 62 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
LOTUS-v1	25.6	84%		2,413	54.6	1,092
Xoodyak_GMU-v2	24.4	44%		2,316	74.8	1,572
Pyjamask-v1	23.4	52%		3,897	92.7	2,027
TinyJAMBU_TJT-v1	22.3	81%		580	111.3	2,558
ACE_UW-v1	20.6	57%		2,156	73.8	1,836
ESTATE-v4	9.6	88%		1,329	118.1	6,314
Gimli_TUM-v1	7.2	57%		1,767	78.0	5,529
Romulus-v5	5.9	79%		1,961	76.5	6,607
Gimli_TUM-v2	3.6	57%		1,767	73.5	10,365
TinyJAMBU_GMU-v3	2.8	82%		1,277	108.1	20,021
ForkAE-v1	2.7	99%		2,022	67.9	12,846
Gimli_TUM-v3	2.0	57%		1,772	78.5	20,037
Minimum		**25%**				
Average		**56%**				
Maximum		**99%**				

Table 63: Lattice ECP5 Encryption PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	349.1	9%	1	1,471	120.0	44
Xoodyak_GMU2-v1	263.9	12%	2	3,248	150.5	73
Ascon_GMU-v2	245.9	15%	3	4,641	117.2	61
Ascon_GMU2-v2h	243.0	17%		3,764	89.2	47
Ascon_GMU-v1	239.8	11%		**5,909**	84.3	45
Gimli_GMU-v4	233.7	13%	4	3,223	94.9	52
Subterranean_ST-v2	231.2	8%		1,342	95.7	53
Ascon_GMU2-v1h	216.7	22%		2,928	110.1	65
COMET_VT-v1	203.2	32%		**5,266**	98.4	62
TinyJAMBU_TJT-v3	194.3	42%	5	1,092	115.4	76
Ascon_GMU2-v3h	191.1	15%		4,925	61.2	41
Xoodyak_XT-v8	186.3	18%		4,121	71.3	49
Xoodyak_XT-v2	183.7	18%		4,077	70.3	49
GIFT-COFB_GMU-v3	180.5	21%	6	3,059	74.7	53
DryGASCON-v1	178.7	29%	7	3,801	100.5	72
Ascon_Graz-v4	175.9	18%		3,379	61.9	45
KNOT-v2x4	175.9	19%	8	3,984	63.2	46
Ascon_Graz-v5	173.6	20%		4,646	55.6	41
Gimli_GMU-v2	173.4	17%		2,617	103.0	76
Ascon_Graz-v3	173.4	21%		3,305	63.7	47
Xoodyak_GMU2-v2	171.5	9%		4,058	69.7	52
KNOT-v2x4h	169.4	19%		4,283	60.9	46
Xoodyak_XT-v1	167.8	17%		2,402	95.7	73
Ascon_VT-v1	167.2	31%		3,130	84.9	65
PHOTON-Beetle-v1	162.3	41%	9	3,294	101.4	80
GIFT-COFB_GMU-v2	161.9	25%		2,628	105.0	83
KNOT-v2x2	158.5	13%		3,287	90.4	73
GIFT-COFB_GMU-v4	155.6	19%		3,311	57.1	47
Xoodyak_XT-v7	155.0	17%		2,489	88.4	73
Ascon_VT-v2	150.8	28%		3,041	75.4	64
Gimli_GMU-v5	149.4	11%		4,586	52.5	45
Gimli_GT-v4	141.3	11%		4,027	60.7	55
Ascon_Graz-v2	134.4	20%		2,603	64.0	61
Ascon_Graz-v6	134.3	16%		**5,346**	38.8	37
KNOT-v2x2h	132.0	13%		3,373	75.3	73
Xoodyak_GMU-v1	129.8	17%		3,172	74.0	73
Gimli_GT-v2	125.0	15%		2,852	76.2	78
Romulus-v2	125.0	38%	10	2,353	82.0	84
GIFT-COFB_GMU-v5	122.8	16%		3,821	36.5	38
Ascon_Graz-v1	116.7	25%		2,544	59.3	65
Elephant-v2	115.2	36%	11	3,073	85.5	95
Gimli_GT-v3	114.9	13%		4,451	55.6	62
Elephant-v5	113.1	17%		4,145	90.1	102
Gimli_GMU-v1	105.3	20%		2,328	102.0	124
Romulus-v3	102.9	32%		3,847	45.0	56
Elephant-v3	101.9	37%		2,901	88.3	111
GIFT-COFB_VT-v1	96.3	31%		2,214	114.3	152

Table 63 continued from previous page

Variant	Through-put 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
GIFT-COFB_GMU-v1	95.3	29%		2,727	106.5	143
ESTATE-v1	91.8	58%	12	2,855	109.0	152
SKINNY-AEAD-v1	88.1	46%	13	3,174	101.1	147
SKINNY-AEAD-v2	86.3	46%		3,182	98.4	146
KNOT-v2x1	86.1	15%		2,275	85.5	127
Gimli_GT-v6	84.0	8%		**6,341**	31.5	48
KNOT-v2x1h	79.6	15%		2,446	78.9	127
Gimli_GT-v1	79.5	19%		2,537	78.2	126
Oribatida-v1	79.0	48%	14	1,671	176.5	286
Romulus-v1	73.6	43%		1,998	80.5	140
Spook-v2-v2	69.4	17%	15	3,662	77.0	142
Elephant-v4	68.7	18%		3,157	97.6	182
SCHWAEMM-v1	66.3	18%	16	4,685	66.3	128
Romulus-v4	65.8	26%		**5,086**	21.6	42
SCHWAEMM-v2	63.8	18%		**5,947**	63.8	128
ACE_GMU-v1	62.5	24%	17	2,784	74.2	152
TinyJAMBU_TJT-v2	61.0	50%		689	125.4	263
ForkAE-v2	59.7	64%	18	3,571	90.0	193
Gimli_GT-v5	59.6	8%		**5,738**	23.3	50
TinyJAMBU_GMU-v1	59.4	51%		720	124.8	269
COMET_CI-v3	58.2	38%	19	3,443	80.0	176
SPIX-v1	57.6	19%	20	2,432	69.3	154
Saturnin-v2	55.6	15%	21	3,648	79.0	182
COMET_CI-v1	55.4	37%		3,255	80.9	187
SpoC_IIT-v1	54.1	48%	22	2,153	132.2	313
COMET_VT-v2	52.8	33%		2,353	111.5	270
Gimli_GT-v7	44.8	9%		**8,238**	16.4	47
Oribatida-v2	43.8	42%		2,497	114.2	334
LOCUS-v2	42.4	55%	23	2,950	72.5	219
Elephant-v1	35.6	39%		2,368	97.5	351
TinyJAMBU_GMU-v2	32.3	52%		908	128.3	509
LOTUS-v2	30.8	55%		2,208	52.7	219
SpoC_VT-v1	27.6	49%		2,049	98.2	455
LOCUS-v1	22.9	56%		2,857	73.0	408
SPIX-v2x4	22.2	16%		2,265	86.7	499
mixFeed-v1	22.0	25%	24	3,479	38.9	226
ESTATE-v3	21.7	65%		1,820	107.1	632
ISAP-v4	20.5	10%	25	3,623	67.2	420
ESTATE-v2	20.3	62%		1,689	115.4	728
ISAP-v3	20.2	9%		**5,703**	65.6	415
ISAP-v2	19.6	12%		**5,708**	68.0	443
ISAP-v1	19.5	9%		**6,701**	61.1	402
LOTUS-v1	17.1	56%		2,413	54.6	408
Pyjamask-v2	16.4	18%	26	4,162	73.2	573
COMET_CI-v2	14.8	36%		1,974	94.3	816
TinyJAMBU_TJT-v1	14.1	51%		580	111.3	1,010
SPIX-v2x2	14.0	16%		2,107	80.2	735
WAGE-v1	13.8	24%	27	2,081	101.6	940

Table 63 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Saturnin-v1	13.7	23%		3,070	92.6	862
Pyjamask-v1	9.6	21%		3,897	92.7	1,241
SPIX-v2	9.5	16%		2,078	89.2	1,197
Xoodyak_GMU-v2	9.1	17%		2,316	74.8	1,050
ACE_UW-v1	8.9	25%		2,156	73.8	1,056
ESTATE-v4	7.1	65%		1,329	118.1	2,138
Romulus-v5	3.6	48%		1,961	76.5	2,695
Gimli_TUM-v1	3.2	25%		1,767	78.0	3,162
ForkAE-v1	2.7	98%		2,022	67.9	3,264
TinyJAMBU_GMU-v3	1.8	53%		1,277	108.1	7,709
Gimli_TUM-v2	1.6	25%		1,767	73.5	5,922
Gimli_TUM-v3	0.9	25%		1,772	78.5	11,442
Minimum		**8%**				
Average		**28%**				
Maximum		**98%**				

Table 64: Lattice ECP5 Encryption AD Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Xoodyak_GMU2-v1	3,590.5	88%	1	3,248	150.5	515
Subterranean_GMU-v1	3,477.9	91%	2	1,471	120.0	424
Subterranean_ST-v2	2,723.0	89%		1,342	95.7	432
Ascon_GMU-v1	1,992.1	92%		**5,909**	84.3	520
Xoodyak_GMU2-v2	1,861.1	91%		4,058	69.7	460
Gimli_GMU-v4	1,626.9	94%	3	3,223	94.9	717
Ascon_GMU-v2	1,566.6	94%	4	4,641	117.2	919
KNOT-v2x4	1,553.4	90%	5	3,984	63.2	500
KNOT-v2x4h	1,495.9	90%		4,283	60.9	500
Ascon_GMU2-v2h	1,358.5	95%		3,764	89.2	807
Xoodyak_XT-v8	1,315.5	94%		4,121	71.3	666
Xoodyak_XT-v1	1,315.4	94%		2,402	95.7	894
Xoodyak_XT-v2	1,297.7	94%		4,077	70.3	666
Gimli_GMU-v5	1,241.3	92%		4,586	52.5	520
Ascon_GMU2-v3h	1,232.8	94%		4,925	61.2	610
Xoodyak_XT-v7	1,215.3	94%		2,489	88.4	894
Gimli_GT-v4	1,195.9	92%		4,027	60.7	624
TinyJAMBU_TJT-v3	1,186.5	96%	6	1,092	115.4	1,195
KNOT-v2x2	1,131.3	91%		3,287	90.4	982
Xoodyak_GMU-v1	1,016.0	94%		3,172	74.0	895
Ascon_GMU2-v1h	967.4	96%		2,928	110.1	1,398
Gimli_GMU-v2	965.2	95%		2,617	103.0	1,311
KNOT-v2x2h	942.2	91%		3,373	75.3	982
Ascon_Graz-v4	939.4	95%		3,379	61.9	809
Gimli_GT-v6	904.4	90%		**6,341**	31.5	428
Ascon_Graz-v5	851.0	96%		4,646	55.6	803
GIFT-COFB_GMU-v3	843.2	97%	7	3,059	74.7	1,089
Gimli_GT-v3	831.9	93%		4,451	55.6	822
GIFT-COFB_GMU-v4	784.5	97%		3,311	57.1	895
Ascon_Graz-v6	783.1	95%		**5,346**	38.8	609
Ascon_Graz-v3	782.4	96%		3,305	63.7	1,000
Gimli_GT-v2	768.8	95%		2,852	76.2	1,218
COMET_VT-v1	766.5	97%		**5,266**	98.4	1,578
GIFT-COFB_GMU-v5	741.8	95%		3,821	36.5	604
Saturnin-v2	669.0	89%	8	3,648	79.0	1,451
Gimli_GT-v5	665.8	89%		**5,738**	23.3	430
Ascon_Graz-v2	650.9	95%		2,603	64.0	1,209
GIFT-COFB_GMU-v2	626.5	98%		2,628	105.0	2,059
DryGASCON-v1	597.6	98%	9	3,801	100.5	2,067
Elephant-v5	591.0	94%	10	4,145	90.1	1,873
Romulus-v2	556.1	95%	11	2,353	82.0	1,812
Elephant-v2	540.7	95%		3,073	85.5	1,943
KNOT-v2x1	539.6	92%		2,275	85.5	1,946
Ascon_VT-v1	528.8	97%		3,130	84.9	1,973
Gimli_GMU-v1	501.7	96%		2,328	102.0	2,499
KNOT-v2x1h	498.4	92%		2,446	78.9	1,946
Romulus-v3	497.3	95%		3,847	45.0	1,112

Table 64 continued from previous page

Variant	Through-put 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Elephant-v3	478.9	95%		2,901	88.3	2,267
Gimli_GT-v7	474.5	90%		**8,238**	16.4	426
Ascon_VT-v2	469.7	97%		3,041	75.4	1,973
Ascon_Graz-v1	457.8	97%		2,544	59.3	1,591
PHOTON-Beetle-v1	455.4	98%	12	3,294	101.4	2,737
SCHWAEMM-v1	427.0	96%	13	4,685	66.3	1,909
SCHWAEMM-v2	410.5	96%		**5,947**	63.8	1,909
Gimli_GT-v1	399.6	96%		2,537	78.2	2,406
Spook-v2-v2	394.6	96%	14	3,662	77.0	2,398
Romulus-v4	348.3	94%		**5,086**	21.6	762
Elephant-v4	343.5	95%		3,157	97.6	3,493
ISAP-v3	339.3	90%		**5,703**	65.6	2,377
GIFT-COFB_GMU-v1	327.1	98%		2,727	106.5	3,999
SPIX-v1	323.9	95%	15	2,432	69.3	2,631
ISAP-v1	317.6	90%		**6,701**	61.1	2,364
Oribatida-v1	317.0	97%	16	1,671	176.5	6,841
ESTATE-v1	312.8	99%	17	2,855	109.0	4,283
Romulus-v1	308.0	96%		1,998	80.5	3,212
TinyJAMBU_TJT-v2	300.9	97%		689	125.4	5,122
GIFT-COFB_VT-v1	294.8	99%		2,214	114.3	4,764
ISAP-v4	283.5	92%	18	3,623	67.2	2,913
TinyJAMBU_GMU-v1	278.4	98%		720	124.8	5,508
ACE_GMU-v1	254.2	96%	19	2,784	74.2	3,588
ISAP-v2	252.1	93%		**5,708**	68.0	3,313
SKINNY-AEAD-v1	202.9	99%	20	3,174	101.1	6,126
Oribatida-v2	201.6	97%		2,497	114.2	6,960
SKINNY-AEAD-v2	197.5	99%		3,182	98.4	6,125
COMET_CI-v3	179.2	98%	21	3,443	80.0	5,486
COMET_CI-v1	169.2	98%		3,255	80.9	5,877
Elephant-v1	168.1	95%		2,368	97.5	7,127
COMET_VT-v2	164.2	98%		2,353	111.5	8,341
TinyJAMBU_GMU-v2	154.1	98%		908	128.3	10,228
LOCUS-v2	152.1	98%	22	2,950	72.5	5,859
SPIX-v2x4	130.9	94%		2,265	86.7	8,137
SpoC_IIT-v1	115.3	99%	23	2,153	132.2	14,084
Saturnin-v1	112.4	93%		3,070	92.6	10,121
LOTUS-v2	110.5	98%		2,208	52.7	5,859
ForkAE-v2	108.0	99%	24	3,571	90.0	10,239
Xoodyak_GMU-v2	91.0	92%		2,316	74.8	10,100
Pyjamask-v2	91.0	95%	25	4,162	73.2	9,887
mixFeed-v1	90.9	97%	26	3,479	38.9	5,256
SPIX-v2x2	83.4	94%		2,107	80.2	11,811
LOCUS-v1	80.6	98%		2,857	73.0	11,124
TinyJAMBU_TJT-v1	70.8	97%		580	111.3	19,306
ESTATE-v3	66.5	99%		1,820	107.1	19,803
ESTATE-v2	64.5	99%		1,689	115.4	21,967
LOTUS-v1	60.3	98%		2,413	54.6	11,124
SPIX-v2	57.2	94%		2,078	89.2	19,149

Table 64 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
SpoC_VT-v1	57.0	99%		2,049	98.2	21,161
WAGE-v1	54.9	96%	27	2,081	101.6	22,713
COMET_CI-v2	44.8	98%		1,974	94.3	25,863
Pyjamask-v1	44.2	96%		3,897	92.7	25,755
ACE_UW-v1	35.0	96%		2,156	73.8	25,885
ESTATE-v4	21.5	99%		1,329	118.1	67,557
Romulus-v5	14.2	96%		1,961	76.5	66,055
Gimli_TUM-v1	12.3	97%		1,767	78.0	77,829
TinyJAMBU_GMU-v3	8.7	98%		1,277	108.1	151,828
ForkAE-v1	7.2	100%		2,022	67.9	116,127
Gimli_TUM-v2	6.2	97%		1,767	73.5	145,945
Gimli_TUM-v3	3.4	97%		1,772	78.5	282,177
Minimum		**88%**				
Average		**95%**				
Maximum		**100%**				

Table 65: Lattice ECP5 Encryption AD Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	1,097.2	29%	1	1,471	120.0	56
Xoodyak_GMU2-v1	895.9	22%	2	3,248	150.5	86
Subterranean_ST-v2	765.8	25%		1,342	95.7	64
Ascon_GMU-v1	719.4	33%		**5,909**	84.3	60
Gimli_GMU-v4	665.8	38%	3	3,223	94.9	73
Ascon_GMU-v2	659.2	40%	4	4,641	117.2	91
TinyJAMBU_TJT-v3	649.2	53%	5	1,092	115.4	91
Ascon_GMU2-v2h	643.4	45%		3,764	89.2	71
Xoodyak_GMU2-v2	557.4	27%		4,058	69.7	64
Xoodyak_XT-v8	544.9	39%		4,121	71.3	67
Ascon_GMU2-v3h	540.2	41%		4,925	61.2	58
Xoodyak_XT-v2	537.5	39%		4,077	70.3	67
Ascon_GMU2-v1h	512.3	51%		2,928	110.1	110
Xoodyak_XT-v1	505.1	36%		2,402	95.7	97
GIFT-COFB_GMU-v3	496.9	57%	6	3,059	74.7	77
KNOT-v2x4	490.4	28%	7	3,984	63.2	66
COMET_VT-v1	475.4	60%		**5,266**	98.4	106
KNOT-v2x4h	472.2	28%		4,283	60.9	66
Xoodyak_XT-v7	466.7	36%		2,489	88.4	97
Gimli_GMU-v2	458.5	45%		2,617	103.0	115
Gimli_GMU-v5	448.3	33%		4,586	52.5	60
GIFT-COFB_GMU-v4	436.7	54%		3,311	57.1	67
Ascon_Graz-v4	433.8	44%		3,379	61.9	73
Gimli_GT-v4	431.9	33%		4,027	60.7	72
Ascon_Graz-v5	425.0	48%		4,646	55.6	67
GIFT-COFB_GMU-v2	423.2	66%		2,628	105.0	127
Ascon_Graz-v3	407.5	50%		3,305	63.7	80
KNOT-v2x2	406.1	33%		3,287	90.4	114
Xoodyak_GMU-v1	386.6	36%		3,172	74.0	98
DryGASCON-v1	381.3	62%	8	3,801	100.5	135
GIFT-COFB_GMU-v5	359.0	46%		3,821	36.5	52
Ascon_Graz-v6	348.6	42%		**5,346**	38.8	57
Gimli_GT-v2	342.2	42%		2,852	76.2	114
KNOT-v2x2h	338.2	33%		3,373	75.3	114
Gimli_GT-v3	331.3	37%		4,451	55.6	86
Ascon_VT-v1	326.8	60%		3,130	84.9	133
PHOTON-Beetle-v1	322.6	70%	9	3,294	101.4	161
Ascon_Graz-v2	312.3	46%		2,603	64.0	105
Ascon_VT-v2	290.3	60%		3,041	75.4	133
Elephant-v5	269.7	43%	10	4,145	90.1	171
Romulus-v2	269.1	46%	11	2,353	82.0	156
Gimli_GT-v6	268.8	27%		**6,341**	31.5	60
Gimli_GMU-v1	262.5	50%		2,328	102.0	199
Elephant-v2	262.1	46%		3,073	85.5	167
Ascon_Graz-v1	255.1	54%		2,544	59.3	119
GIFT-COFB_GMU-v1	240.1	72%		2,727	106.5	227
ESTATE-v1	237.5	75%	12	2,855	109.0	235

Table 65 continued from previous page

Variant	Through-put 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Elephant-v3	232.0	46%		2,901	88.3	195
Romulus-v3	230.4	44%		3,847	45.0	100
GIFT-COFB_VT-v1	228.6	77%		2,214	114.3	256
SCHWAEMM-v1	211.0	47%	13	4,685	66.3	161
KNOT-v2x1	208.4	36%		2,275	85.5	210
Spook-v2-v2	207.5	51%	14	3,662	77.0	190
SCHWAEMM-v2	202.8	47%		**5,947**	63.8	161
Gimli_GT-v1	202.3	48%		2,537	78.2	198
Saturnin-v2	193.5	26%	15	3,648	79.0	209
KNOT-v2x1h	192.4	36%		2,446	78.9	210
Gimli_GT-v5	192.4	26%		**5,738**	23.3	62
TinyJAMBU_TJT-v2	190.0	62%		689	125.4	338
Oribatida-v1	183.3	56%	16	1,671	176.5	493
TinyJAMBU_GMU-v1	179.5	63%		720	124.8	356
Elephant-v4	160.7	44%		3,157	97.6	311
SKINNY-AEAD-v1	156.9	76%	17	3,174	101.1	330
Romulus-v1	153.8	48%		1,998	80.5	268
Romulus-v4	153.6	42%		**5,086**	21.6	72
SKINNY-AEAD-v2	153.2	77%		3,182	98.4	329
SPIX-v1	148.5	44%	18	2,432	69.3	239
Gimli_GT-v7	145.2	28%		**8,238**	16.4	58
ACE_GMU-v1	137.7	52%	19	2,784	74.2	276
COMET_CI-v3	122.6	67%	20	3,443	80.0	334
Oribatida-v2	118.4	57%		2,497	114.2	494
COMET_CI-v1	116.0	67%		3,255	80.9	357
COMET_VT-v2	109.5	65%		2,353	111.5	521
LOCUS-v2	109.5	71%	21	2,950	72.5	339
ISAP-v3	102.2	27%		**5,703**	65.6	329
ISAP-v4	102.1	33%	22	3,623	67.2	337
TinyJAMBU_GMU-v2	99.5	63%		908	128.3	660
ISAP-v1	99.0	28%		**6,701**	61.1	316
ForkAE-v2	94.6	87%	23	3,571	90.0	487
ISAP-v2	94.3	35%		**5,708**	68.0	369
SpoC_IIT-v1	91.0	78%	24	2,153	132.2	744
Elephant-v1	81.2	46%		2,368	97.5	615
LOTUS-v2	79.5	71%		2,208	52.7	339
LOCUS-v1	58.7	72%		2,857	73.0	636
SPIX-v2x4	57.1	41%		2,265	86.7	777
ESTATE-v3	53.0	79%		1,820	107.1	1,035
mixFeed-v1	52.4	56%	25	3,479	38.9	380
ESTATE-v2	50.3	77%		1,689	115.4	1,175
SpoC_VT-v1	45.5	79%		2,049	98.2	1,105
Saturnin-v1	44.8	37%		3,070	92.6	1,059
TinyJAMBU_TJT-v1	44.7	62%		580	111.3	1,274
LOTUS-v1	43.9	72%		2,413	54.6	636
Pyjamask-v2	43.0	45%	26	4,162	73.2	871
SPIX-v2x2	36.1	41%		2,107	80.2	1,139
COMET_CI-v2	30.7	67%		1,974	94.3	1,575

Table 65 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
WAGE-v1	29.9	53%	27	2,081	101.6	1,737
Xoodyak_GMU-v2	29.1	29%		2,316	74.8	1,317
SPIX-v2	24.6	41%		2,078	89.2	1,853
Pyjamask-v1	23.5	51%		3,897	92.7	2,019
ACE_UW-v1	19.2	53%		2,156	73.8	1,965
ESTATE-v4	17.2	79%		1,329	118.1	3,525
Romulus-v5	7.3	49%		1,961	76.5	5,335
Gimli_TUM-v1	7.2	57%		1,767	78.0	5,517
ForkAE-v1	7.1	99%		2,022	67.9	4,899
TinyJAMBU_GMU-v3	5.7	63%		1,277	108.1	9,780
Gimli_TUM-v2	3.6	57%		1,767	73.5	10,337
Gimli_TUM-v3	2.0	57%		1,772	78.5	19,977
Minimum		**22%**				
Average		**50%**				
Maximum		**99%**				

Table 66: Lattice ECP5 Encryption AD Throughput for 16 Byte Messages

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	349.1	9%	1	1,471	120.0	44
TinyJAMBU_TJT-v3	268.5	22%	2	1,092	115.4	55
Xoodyak_GMU2-v1	263.9	6%	3	3,248	150.5	73
Ascon_GMU2-v2h	243.0	17%	4	3,764	89.2	47
Ascon_GMU-v1	239.8	11%		**5,909**	84.3	45
Subterranean_ST-v2	235.6	8%		1,342	95.7	52
Ascon_GMU-v2	234.3	14%		4,641	117.2	64
Gimli_GMU-v4	233.7	13%	5	3,223	94.9	52
GIFT-COFB_GMU-v3	217.4	25%	6	3,059	74.7	44
COMET_VT-v1	217.2	28%		**5,266**	98.4	58
GIFT-COFB_GMU-v2	210.0	33%		2,628	105.0	64
Ascon_GMU2-v1h	207.2	21%		2,928	110.1	68
Ascon_GMU2-v3h	195.8	15%		4,925	61.2	40
Xoodyak_XT-v8	190.1	14%		4,121	71.3	48
Xoodyak_XT-v2	187.6	14%		4,077	70.3	48
GIFT-COFB_GMU-v4	182.8	23%		3,311	57.1	40
DryGASCON-v1	178.7	29%	7	3,801	100.5	72
Gimli_GMU-v2	173.4	17%		2,617	103.0	76
Xoodyak_GMU2-v2	171.5	8%		4,058	69.7	52
Xoodyak_XT-v1	170.1	12%		2,402	95.7	72
PHOTON-Beetle-v1	168.6	36%	8	3,294	101.4	77
Ascon_Graz-v5	165.5	19%		4,646	55.6	43
Ascon_Graz-v3	163.0	20%		3,305	63.7	50
Ascon_Graz-v4	161.6	16%		3,379	61.9	49
Xoodyak_XT-v7	157.2	12%		2,489	88.4	72
KNOT-v2x4	155.6	9%	9	3,984	63.2	52
KNOT-v2x4h	149.8	9%		4,283	60.9	52
Gimli_GMU-v5	149.4	11%		4,586	52.5	45
Ascon_VT-v1	148.9	27%		3,130	84.9	73
Gimli_GT-v4	144.0	11%		4,027	60.7	54
GIFT-COFB_GMU-v5	137.3	18%		3,821	36.5	34
ESTATE-v1	135.5	43%	10	2,855	109.0	103
KNOT-v2x2	134.6	11%		3,287	90.4	86
GIFT-COFB_VT-v1	134.2	45%		2,214	114.3	109
Ascon_VT-v2	132.2	27%		3,041	75.4	73
GIFT-COFB_GMU-v1	131.0	39%		2,727	106.5	104
Xoodyak_GMU-v1	129.8	12%		3,172	74.0	73
Ascon_Graz-v6	127.4	15%		**5,346**	38.8	39
Gimli_GT-v2	125.0	15%		2,852	76.2	78
Romulus-v2	125.0	21%	11	2,353	82.0	84
Ascon_Graz-v2	118.8	17%		2,603	64.0	69
Gimli_GT-v3	114.9	13%		4,451	55.6	62
KNOT-v2x2h	112.1	11%		3,373	75.3	86
Ascon_Graz-v1	106.9	23%		2,544	59.3	71
Gimli_GMU-v1	105.3	20%		2,328	102.0	124
Romulus-v3	102.9	20%		3,847	45.0	56
Elephant-v5	92.3	15%	12	4,145	90.1	125

Table 66 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Elephant-v2	92.0	16%		3,073	85.5	119
SKINNY-AEAD-v1	91.8	45%	13	3,174	101.1	141
SKINNY-AEAD-v2	90.0	45%		3,182	98.4	140
TinyJAMBU_TJT-v2	88.2	29%		689	125.4	182
TinyJAMBU_GMU-v1	85.0	30%		720	124.8	188
Gimli_GT-v6	84.0	8%		**6,341**	31.5	48
Elephant-v3	81.4	16%		2,901	88.3	139
Gimli_GT-v1	79.5	19%		2,537	78.2	126
Oribatida-v1	79.0	24%	14	1,671	176.5	286
Romulus-v1	73.6	23%		1,998	80.5	140
KNOT-v2x1	71.0	12%		2,275	85.5	154
Spook-v2-v2	69.4	17%	15	3,662	77.0	142
SCHWAEMM-v1	69.0	15%	16	4,685	66.3	123
ForkAE-v2	68.2	63%	17	3,571	90.0	169
SCHWAEMM-v2	66.4	15%		**5,947**	63.8	123
Romulus-v4	65.8	18%		**5,086**	21.6	42
KNOT-v2x1h	65.6	12%		2,446	78.9	154
Saturnin-v2	65.2	9%	18	3,648	79.0	155
COMET_CI-v3	61.7	34%	19	3,443	80.0	166
Gimli_GT-v5	59.6	8%		**5,738**	23.3	50
COMET_CI-v1	58.5	34%		3,255	80.9	177
LOCUS-v2	58.4	38%	20	2,950	72.5	159
ACE_GMU-v1	56.5	21%	21	2,784	74.2	168
Elephant-v4	55.5	15%		3,157	97.6	225
SPIX-v1	55.1	16%	22	2,432	69.3	161
SpoC_IIT-v1	54.8	47%	23	2,153	132.2	309
COMET_VT-v2	53.6	32%		2,353	111.5	266
Oribatida-v2	51.8	25%		2,497	114.2	282
TinyJAMBU_GMU-v2	47.2	30%		908	128.3	348
Gimli_GT-v7	45.8	9%		**8,238**	16.4	46
LOTUS-v2	42.4	38%		2,208	52.7	159
ISAP-v4	34.0	11%	24	3,623	67.2	253
ISAP-v3	32.7	9%		**5,703**	65.6	257
ESTATE-v3	32.4	48%		1,820	107.1	423
ISAP-v1	32.1	9%		**6,701**	61.1	244
ISAP-v2	31.9	12%		**5,708**	68.0	273
LOCUS-v1	31.8	39%		2,857	73.0	294
ESTATE-v2	29.7	45%		1,689	115.4	497
Elephant-v1	28.4	16%		2,368	97.5	439
SpoC_VT-v1	27.9	48%		2,049	98.2	451
LOTUS-v1	23.8	39%		2,413	54.6	294
mixFeed-v1	22.5	24%	25	3,479	38.9	221
TinyJAMBU_TJT-v1	20.8	29%		580	111.3	686
SPIX-v2x4	20.7	15%		2,265	86.7	537
Saturnin-v1	17.8	15%		3,070	92.6	665
Pyjamask-v2	16.2	17%	26	4,162	73.2	577
COMET_CI-v2	15.4	34%		1,974	94.3	783
SPIX-v2x2	13.0	15%		2,107	80.2	791

Table 66 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
WAGE-v1	12.3	22%	27	2,081	101.6	1,053
ESTATE-v4	10.5	48%		1,329	118.1	1,437
Pyjamask-v1	9.5	21%		3,897	92.7	1,245
Xoodyak_GMU-v2	9.1	9%		2,316	74.8	1,050
SPIX-v2	8.9	15%		2,078	89.2	1,289
ACE_UW-v1	8.0	22%		2,156	73.8	1,185
ForkAE-v1	6.8	95%		2,022	67.9	1,272
Romulus-v5	3.6	24%		1,961	76.5	2,695
Gimli_TUM-v1	3.2	25%		1,767	78.0	3,159
TinyJAMBU_GMU-v3	2.7	30%		1,277	108.1	5,148
Gimli_TUM-v2	1.6	25%		1,767	73.5	5,915
Gimli_TUM-v3	0.9	25%		1,772	78.5	11,427
Minimum		**6%**				
Average		**23%**				
Maximum		**95%**				

Table 67: Lattice ECP5 Encryption AD+PT Throughput for 1536 Byte Messages

Variant	Through-put 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean_GMU-v1	1,822.8	47%	1	1,471	120.0	809
Subterranean_ST-v2	1,441.6	47%		1,342	95.7	816
Xoodyak_GMU2-v1	1,386.1	44%	2	3,248	150.5	1,334
Ascon_GMU-v1	1,035.9	48%		**5,909**	84.3	1,000
Xoodyak_GMU2-v2	950.2	48%		4,058	69.7	901
Gimli_GMU-v4	839.8	48%	3	3,223	94.9	1,389
Ascon_GMU-v2	807.5	48%	4	4,641	117.2	1,783
Ascon_GMU2-v2h	696.1	49%		3,764	89.2	1,575
Gimli_GMU-v5	644.8	48%		4,586	52.5	1,001
Ascon_GMU2-v3h	633.6	49%		4,925	61.2	1,187
Gimli_GT-v4	621.9	48%		4,027	60.7	1,200
KNOT-v2x2	591.2	48%	5	3,287	90.4	1,879
Xoodyak_XT-v8	587.6	47%		4,121	71.3	1,491
KNOT-v2x4	582.7	48%		3,984	63.2	1,333
Xoodyak_XT-v2	579.6	47%		4,077	70.3	1,491
KNOT-v2x4h	561.1	48%		4,283	60.9	1,333
Xoodyak_XT-v1	560.8	46%		2,402	95.7	2,097
Xoodyak_XT-v7	518.1	46%		2,489	88.4	2,097
Gimli_GMU-v2	494.5	49%		2,617	103.0	2,559
Ascon_GMU2-v1h	493.2	49%		2,928	110.1	2,742
KNOT-v2x2h	492.4	48%		3,373	75.3	1,879
Ascon_Graz-v4	481.9	49%		3,379	61.9	1,577
Gimli_GT-v6	477.9	47%		**6,341**	31.5	810
Ascon_Graz-v5	435.0	49%		4,646	55.6	1,571
Xoodyak_GMU-v1	433.6	46%		3,172	74.0	2,097
Gimli_GT-v3	430.1	48%		4,451	55.6	1,590
GIFT-COFB_GMU-v3	428.5	49%	6	3,059	74.7	2,143
Ascon_Graz-v6	402.4	49%		**5,346**	38.8	1,185
GIFT-COFB_GMU-v4	399.6	49%		3,311	57.1	1,757
Ascon_Graz-v3	399.2	49%		3,305	63.7	1,960
Gimli_GT-v2	395.1	49%		2,852	76.2	2,370
GIFT-COFB_GMU-v5	380.4	49%		3,821	36.5	1,178
Gimli_GT-v5	352.2	47%		**5,738**	23.3	813
COMET_VT-v1	345.8	49%		**5,266**	98.4	3,498
Ascon_Graz-v2	333.3	49%		2,603	64.0	2,361
TinyJAMBU_TJT-v3	332.3	49%	7	1,092	115.4	4,267
GIFT-COFB_GMU-v2	316.7	49%		2,628	105.0	4,073
Elephant-v5	312.3	49%	8	4,145	90.1	3,545
DryGASCON-v1	302.6	49%	9	3,801	100.5	4,083
KNOT-v2x1	280.9	48%		2,275	85.5	3,739
Ascon_VT-v1	268.0	49%		3,130	84.9	3,893
KNOT-v2x1h	259.4	48%		2,446	78.9	3,739
Gimli_GMU-v1	255.9	49%		2,328	102.0	4,899
Ascon_VT-v2	250.3	49%		3,041	75.4	3,702
Gimli_GT-v7	250.2	48%		**8,238**	16.4	808
Saturnin-v2	239.2	48%	10	3,648	79.0	4,059
Ascon_Graz-v1	233.4	49%		2,544	59.3	3,121

Table 67 continued from previous page

Variant	Through-put 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
PHOTON-Beetle-v1	211.1	50%	11	3,294	101.4	5,905
Romulus-v2	207.7	49%	12	2,353	82.0	4,852
Gimli_GT-v1	204.1	49%		2,537	78.2	4,710
Elephant-v2	201.6	49%		3,073	85.5	5,211
Spook-v2-v2	201.2	49%	13	3,662	77.0	4,702
Romulus-v3	195.9	49%		3,847	45.0	2,822
SCHWAEMM-v1	195.0	49%	14	4,685	66.3	4,181
SCHWAEMM-v2	187.5	49%		**5,947**	63.8	4,181
Elephant-v4	179.5	49%		3,157	97.6	6,685
Elephant-v3	176.7	49%		2,901	88.3	6,143
GIFT-COFB_GMU-v1	164.9	50%		2,727	106.5	7,933
SPIX-v1	154.6	49%	15	2,432	69.3	5,512
GIFT-COFB_VT-v1	151.4	50%		2,214	114.3	9,276
Romulus-v4	146.9	49%		**5,086**	21.6	1,807
ISAP-v3	132.1	47%		**5,703**	65.6	6,104
ACE_GMU-v1	129.5	49%	16	2,784	74.2	7,044
ISAP-v1	123.3	47%		**6,701**	61.1	6,091
ISAP-v4	113.3	47%	17	3,623	67.2	7,289
Romulus-v1	111.0	50%		1,998	80.5	8,912
Oribatida-v1	108.4	49%	18	1,671	176.5	19,995
ESTATE-v1	105.2	50%	19	2,855	109.0	12,736
SKINNY-AEAD-v1	99.0	50%	20	3,174	101.1	12,558
ISAP-v2	98.8	48%		**5,708**	68.0	8,456
SKINNY-AEAD-v2	96.3	50%		3,182	98.4	12,557
TinyJAMBU_TJT-v2	86.6	50%		689	125.4	17,795
COMET_CI-v3	83.2	50%	21	3,443	80.0	11,822
TinyJAMBU_GMU-v1	82.6	50%		720	124.8	18,564
COMET_VT-v2	81.1	49%		2,353	111.5	16,885
COMET_CI-v1	78.9	50%		3,255	80.9	12,597
Oribatida-v2	68.8	50%		2,497	114.2	20,400
SPIX-v2x4	67.4	49%		2,265	86.7	15,818
Elephant-v1	59.5	49%		2,368	97.5	20,123
SpoC_IIT-v1	57.2	50%	22	2,153	132.2	28,388
LOCUS-v2	51.3	50%	23	2,950	72.5	17,379
ForkAE-v2	50.1	50%	24	3,571	90.0	22,050
Pyjamask-v2	45.7	49%	25	4,162	73.2	19,680
mixFeed-v1	44.3	49%	26	3,479	38.9	10,778
TinyJAMBU_GMU-v2	44.3	50%		908	128.3	35,572
SPIX-v2x2	42.9	49%		2,107	80.2	22,948
Saturnin-v1	39.2	49%		3,070	92.6	29,049
LOTUS-v2	37.2	50%		2,208	52.7	17,379
Xoodyak_GMU-v2	34.6	45%		2,316	74.8	26,548
SPIX-v2	29.4	49%		2,078	89.2	37,198
SpoC_VT-v1	28.4	50%		2,049	98.2	42,473
WAGE-v1	28.0	49%	27	2,081	101.6	44,601
LOCUS-v1	27.2	50%		2,857	73.0	33,012
Pyjamask-v1	22.4	49%		3,897	92.7	50,908
ESTATE-v3	22.3	50%		1,820	107.1	58,976

Table 67 continued from previous page

Variant	Throughput 1536B [Mbit/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
ESTATE-v2	21.7	50%		1,689	115.4	65,364
COMET_CI-v2	21.3	50%		1,974	94.3	54,375
LOTUS-v1	20.3	50%		2,413	54.6	33,012
TinyJAMBU_TJT-v1	19.9	50%		580	111.3	68,846
ACE_UW-v1	17.8	49%		2,156	73.8	50,845
ESTATE-v4	7.2	50%		1,329	118.1	201,194
Gimli_TUM-v1	6.2	49%		1,767	78.0	153,573
Romulus-v5	4.9	50%		1,961	76.5	189,935
Gimli_TUM-v2	3.1	49%		1,767	73.5	288,121
TinyJAMBU_GMU-v3	2.4	50%		1,277	108.1	545,812
ForkAE-v1	2.0	50%		2,022	67.9	422,754
Gimli_TUM-v3	1.7	49%		1,772	78.5	557,217
Minimum		**44%**				
Average		**49%**				
Maximum		**50%**				

Table 68: Lattice ECP5 Encryption AD+PT Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean_GMU-v1	841.7	22%	1	1,471	120.0	73
Xoodyak_GMU2-v1	687.9	22%	2	3,248	150.5	112
Subterranean_ST-v2	612.7	20%		1,342	95.7	80
Ascon_GMU-v1	539.5	25%		**5,909**	84.3	80
Gimli_GMU-v4	481.2	28%	3	3,223	94.9	101
Ascon_GMU-v2	472.3	28%	4	4,641	117.2	127
Xoodyak_GMU2-v2	457.3	23%		4,058	69.7	78
Ascon_GMU2-v2h	443.5	31%		3,764	89.2	103
Ascon_GMU2-v3h	377.5	29%		4,925	61.2	83
Xoodyak_XT-v8	376.3	30%		4,121	71.3	97
Xoodyak_XT-v2	371.2	30%		4,077	70.3	97
Xoodyak_XT-v1	352.5	29%		2,402	95.7	139
KNOT-v2x4	348.0	29%	5	3,984	63.2	93
Ascon_GMU2-v1h	339.5	34%		2,928	110.1	166
KNOT-v2x4h	335.1	29%		4,283	60.9	93
Gimli_GMU-v5	332.0	25%		4,586	52.5	81
Xoodyak_XT-v7	325.7	29%		2,489	88.4	139
Gimli_GT-v4	323.9	25%		4,027	60.7	96
KNOT-v2x2	323.7	26%		3,287	90.4	143
GIFT-COFB_GMU-v3	321.5	37%	6	3,059	74.7	119
Gimli_GMU-v2	315.7	31%		2,617	103.0	167
Ascon_Graz-v4	301.6	30%		3,379	61.9	105
GIFT-COFB_GMU-v4	289.7	36%		3,311	57.1	101
Ascon_Graz-v5	287.6	32%		4,646	55.6	99
Xoodyak_GMU-v1	272.6	29%		3,172	74.0	139
Ascon_Graz-v3	271.7	33%		3,305	63.7	120
COMET_VT-v1	270.9	39%		**5,266**	98.4	186
TinyJAMBU_TJT-v3	269.8	40%	7	1,092	115.4	219
KNOT-v2x2h	269.6	26%		3,373	75.3	143
GIFT-COFB_GMU-v2	257.2	40%		2,628	105.0	209
GIFT-COFB_GMU-v5	252.3	32%		3,821	36.5	74
Ascon_Graz-v6	245.3	30%		**5,346**	38.8	81
Gimli_GT-v3	241.5	27%		4,451	55.6	118
Gimli_GT-v2	240.8	30%		2,852	76.2	162
DryGASCON-v1	235.0	38%	8	3,801	100.5	219
Gimli_GT-v6	217.9	22%		**6,341**	31.5	74
Ascon_Graz-v2	214.3	31%		2,603	64.0	153
Ascon_VT-v1	204.1	38%		3,130	84.9	213
Elephant-v5	194.6	30%	9	4,145	90.1	237
Ascon_VT-v2	187.5	37%		3,041	75.4	206
PHOTON-Beetle-v1	177.3	42%	10	3,294	101.4	293
Gimli_GMU-v1	174.7	33%		2,328	102.0	299
Ascon_Graz-v1	171.5	36%		2,544	59.3	177
Romulus-v2	166.6	40%	11	2,353	82.0	252
KNOT-v2x1	163.9	28%		2,275	85.5	267
Gimli_GT-v5	154.9	21%		**5,738**	23.3	77
KNOT-v2x1h	151.4	28%		2,446	78.9	267

Table 68 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Romulus-v3	149.6	38%		3,847	45.0	154
Elephant-v2	147.9	36%		3,073	85.5	296
GIFT-COFB_GMU-v1	140.1	42%		2,727	106.5	389
Spook-v2-v2	137.8	34%	12	3,662	77.0	286
Gimli_GT-v1	136.3	33%		2,537	78.2	294
GIFT-COFB_VT-v1	131.8	43%		2,214	114.3	444
Elephant-v3	130.0	36%		2,901	88.3	348
SCHWAEMM-v1	125.3	31%	13	4,685	66.3	271
Saturnin-v2	121.5	24%	14	3,648	79.0	333
SCHWAEMM-v2	120.5	31%		**5,947**	63.8	271
Gimli_GT-v7	117.0	22%		**8,238**	16.4	72
Elephant-v4	114.4	31%		3,157	97.6	437
Romulus-v4	105.3	35%		**5,086**	21.6	105
SPIX-v1	98.6	31%	15	2,432	69.3	360
ESTATE-v1	94.3	45%	16	2,855	109.0	592
Romulus-v1	92.0	41%		1,998	80.5	448
ACE_GMU-v1	90.5	34%	17	2,784	74.2	420
Oribatida-v1	86.6	40%	18	1,671	176.5	1,043
SKINNY-AEAD-v1	86.6	43%	19	3,174	101.1	598
SKINNY-AEAD-v2	84.4	44%		3,182	98.4	597
TinyJAMBU_TJT-v2	74.1	42%		689	125.4	867
TinyJAMBU_GMU-v1	71.0	43%		720	124.8	900
COMET_CI-v3	68.5	41%	20	3,443	80.0	598
COMET_VT-v2	65.1	40%		2,353	111.5	877
COMET_CI-v1	65.0	41%		3,255	80.9	637
ISAP-v3	54.6	19%		**5,703**	65.6	616
Oribatida-v2	52.0	37%		2,497	114.2	1,124
ISAP-v1	51.9	20%		**6,701**	61.1	603
ISAP-v4	51.7	22%	21	3,623	67.2	665
SpoC_IIT-v1	50.5	44%	22	2,153	132.2	1,340
ISAP-v2	47.8	23%		**5,708**	68.0	728
ForkAE-v2	46.9	47%	23	3,571	90.0	982
LOCUS-v2	45.3	44%	24	2,950	72.5	819
Elephant-v1	44.3	37%		2,368	97.5	1,128
SPIX-v2x4	40.4	29%		2,265	86.7	1,098
TinyJAMBU_GMU-v2	38.3	43%		908	128.3	1,716
LOTUS-v2	32.9	44%		2,208	52.7	819
mixFeed-v1	30.3	33%	25	3,479	38.9	658
Pyjamask-v2	29.3	31%	26	4,162	73.2	1,280
SPIX-v2x2	25.6	29%		2,107	80.2	1,604
Saturnin-v1	25.4	32%		3,070	92.6	1,863
SpoC_VT-v1	25.2	44%		2,049	98.2	1,993
LOCUS-v1	24.1	44%		2,857	73.0	1,548
Xoodyak_GMU-v2	20.8	27%		2,316	74.8	1,842
ESTATE-v3	20.5	46%		1,820	107.1	2,672
ESTATE-v2	19.8	45%		1,689	115.4	2,988
WAGE-v1	19.6	34%	27	2,081	101.6	2,649
LOTUS-v1	18.1	44%		2,413	54.6	1,548

Table 68 continued from previous page

Variant	Throughput 64B [Mbit/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
SPIX-v2	17.5	29%		2,078	89.2	2,606
COMET_CI-v2	17.5	41%		1,974	94.3	2,763
TinyJAMBU_TJT-v1	17.0	43%		580	111.3	3,342
Pyjamask-v1	15.5	34%		3,897	92.7	3,068
ACE_UW-v1	12.6	35%		2,156	73.8	3,005
ESTATE-v4	6.6	46%		1,329	118.1	9,098
Gimli_TUM-v1	4.6	36%		1,767	78.0	8,673
Romulus-v5	4.2	42%		1,961	76.5	9,247
Gimli_TUM-v2	2.3	36%		1,767	73.5	16,261
TinyJAMBU_GMU-v3	2.1	43%		1,277	108.1	26,196
ForkAE-v1	2.0	50%		2,022	67.9	17,678
Gimli_TUM-v3	1.3	36%		1,772	78.5	31,437
Minimum		**19%**				
Average		**34%**				
Maximum		**50%**				

Table 69: Lattice ECP5 Encryption AD+PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Subterranean_GMU-v1	313.5	8%	1	1,471	120.0	49
Xoodyak_GMU2-v1	263.9	8%	2	3,248	150.5	73
Subterranean_ST-v2	218.8	7%		1,342	95.7	56
Ascon_GMU-v1	215.8	10%		**5,909**	84.3	50
Ascon_GMU2-v2h	207.6	15%	3	3,764	89.2	55
Gimli_GMU-v4	205.9	12%	4	3,223	94.9	59
Ascon_GMU-v2	205.4	12%		4,641	117.2	73
GIFT-COFB_GMU-v3	180.5	21%	5	3,059	74.7	53
Xoodyak_XT-v8	175.5	14%		4,121	71.3	52
Xoodyak_XT-v2	173.1	14%		4,077	70.3	52
Ascon_GMU2-v1h	171.8	17%		2,928	110.1	82
Xoodyak_GMU2-v2	171.5	9%		4,058	69.7	52
TinyJAMBU_TJT-v3	169.8	25%	6	1,092	115.4	87
Ascon_GMU2-v3h	166.7	13%		4,925	61.2	47
GIFT-COFB_GMU-v2	161.9	25%		2,628	105.0	83
COMET_VT-v1	161.5	23%		**5,266**	98.4	78
Xoodyak_XT-v1	161.2	13%		2,402	95.7	76
GIFT-COFB_GMU-v4	155.6	19%		3,311	57.1	47
KNOT-v2x4	152.7	13%	7	3,984	63.2	53
Xoodyak_XT-v7	148.9	13%		2,489	88.4	76
Gimli_GMU-v2	148.1	15%		2,617	103.0	89
KNOT-v2x4h	147.0	13%		4,283	60.9	53
Ascon_Graz-v5	139.6	16%		4,646	55.6	51
Ascon_Graz-v4	138.9	14%		3,379	61.9	57
DryGASCON-v1	138.4	23%	8	3,801	100.5	93
Ascon_Graz-v3	135.8	17%		3,305	63.7	60
KNOT-v2x2	133.0	11%		3,287	90.4	87
Gimli_GMU-v5	131.8	10%		4,586	52.5	51
Gimli_GT-v4	129.6	10%		4,027	60.7	60
Romulus-v2	125.0	30%	9	2,353	82.0	84
Xoodyak_GMU-v1	124.6	13%		3,172	74.0	76
GIFT-COFB_GMU-v5	122.8	16%		3,821	36.5	38
PHOTON-Beetle-v1	118.0	28%	10	3,294	101.4	110
Ascon_VT-v1	116.9	22%		3,130	84.9	93
KNOT-v2x2h	110.8	11%		3,373	75.3	87
Ascon_Graz-v6	110.4	13%		**5,346**	38.8	45
Gimli_GT-v2	108.4	13%		2,852	76.2	90
Ascon_VT-v2	104.9	21%		3,041	75.4	92
Romulus-v3	102.9	26%		3,847	45.0	56
Gimli_GT-v3	101.8	11%		4,451	55.6	70
Ascon_Graz-v2	101.2	15%		2,603	64.0	81
GIFT-COFB_GMU-v1	95.3	29%		2,727	106.5	143
GIFT-COFB_VT-v1	93.8	31%		2,214	114.3	156
Ascon_Graz-v1	93.7	20%		2,544	59.3	81
Elephant-v5	92.3	14%	11	4,145	90.1	125
Elephant-v2	92.0	23%		3,073	85.5	119
Gimli_GMU-v1	87.6	17%		2,328	102.0	149

Table 69 continued from previous page

Variant	Through-put 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Elephant-v3	81.4	23%		2,901	88.3	139
Gimli_GT-v6	80.6	8%		**6,341**	31.5	50
Romulus-v1	73.6	33%		1,998	80.5	140
ESTATE-v1	71.2	34%	12	2,855	109.0	196
KNOT-v2x1	70.6	12%		2,275	85.5	155
Gimli_GT-v1	66.8	16%		2,537	78.2	150
Romulus-v4	65.8	22%		**5,086**	21.6	42
KNOT-v2x1h	65.2	12%		2,446	78.9	155
SKINNY-AEAD-v1	62.2	31%	13	3,174	101.1	208
SKINNY-AEAD-v2	60.9	31%		3,182	98.4	207
Gimli_GT-v5	56.3	8%		**5,738**	23.3	53
Saturnin-v2	55.6	11%	14	3,648	79.0	182
Elephant-v4	55.5	15%		3,157	97.6	225
Oribatida-v1	53.1	24%	15	1,671	176.5	425
Spook-v2-v2	51.9	13%	16	3,662	77.0	190
TinyJAMBU_TJT-v2	51.0	29%		689	125.4	315
TinyJAMBU_GMU-v1	49.3	30%		720	124.8	324
SCHWAEMM-v1	46.7	12%	17	4,685	66.3	182
ACE_GMU-v1	46.6	18%	18	2,784	74.2	204
SPIX-v1	46.2	15%	19	2,432	69.3	192
SCHWAEMM-v2	44.9	12%		**5,947**	63.8	182
COMET_CI-v3	44.1	26%	20	3,443	80.0	232
Gimli_GT-v7	43.9	8%		**8,238**	16.4	48
COMET_CI-v1	41.9	26%		3,255	80.9	247
COMET_VT-v2	40.2	25%		2,353	111.5	355
ForkAE-v2	39.0	39%	21	3,571	90.0	295
SpoC_IIT-v1	36.9	32%	22	2,153	132.2	458
LOCUS-v2	33.3	32%	23	2,950	72.5	279
Oribatida-v2	29.7	21%		2,497	114.2	492
Elephant-v1	28.4	24%		2,368	97.5	439
TinyJAMBU_GMU-v2	26.8	30%		908	128.3	612
LOTUS-v2	24.2	32%		2,208	52.7	279
ISAP-v3	19.8	7%		**5,703**	65.6	424
ISAP-v4	19.2	8%	24	3,623	67.2	449
ISAP-v1	19.0	7%		**6,701**	61.1	411
SpoC_VT-v1	18.7	33%		2,049	98.2	673
ISAP-v2	18.3	9%		**5,708**	68.0	476
SPIX-v2x4	18.0	13%		2,265	86.7	618
LOCUS-v1	17.9	33%		2,857	73.0	522
ESTATE-v3	16.4	37%		1,820	107.1	836
ESTATE-v2	15.5	36%		1,689	115.4	954
mixFeed-v1	15.2	17%	25	3,479	38.9	328
Pyjamask-v2	13.8	15%	26	4,162	73.2	680
Saturnin-v1	13.7	17%		3,070	92.6	862
LOTUS-v1	13.4	33%		2,413	54.6	522
TinyJAMBU_TJT-v1	11.8	30%		580	111.3	1,206
SPIX-v2x2	11.3	13%		2,107	80.2	908
COMET_CI-v2	11.2	26%		1,974	94.3	1,080

Table 69 continued from previous page

Variant	Throughput 16B [Mbit/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
WAGE-v1	10.1	18%	27	2,081	101.6	1,281
Xoodyak_GMU-v2	9.1	12%		2,316	74.8	1,053
Pyjamask-v1	7.9	17%		3,897	92.7	1,508
SPIX-v2	7.7	13%		2,078	89.2	1,478
ACE_UW-v1	6.5	18%		2,156	73.8	1,445
ESTATE-v4	5.3	37%		1,329	118.1	2,834
Romulus-v5	3.6	36%		1,961	76.5	2,695
Gimli_TUM-v1	2.5	20%		1,767	78.0	3,948
ForkAE-v1	1.9	49%		2,022	67.9	4,469
TinyJAMBU_GMU-v3	1.5	31%		1,277	108.1	9,252
Gimli_TUM-v2	1.3	20%		1,767	73.5	7,396
Gimli_TUM-v3	0.7	20%		1,772	78.5	14,292
Minimum		**7%**				
Average		**20%**				
Maximum		**49%**				

Table 70: Lattice ECP5 Hash Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbit/s]	Thr HM 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Gimli_GMU-v4	1,668.8	96%	1	3,223	94.9	699
Xoodyak_GMU2-v1	1,443.5	97%	2	3,248	150.5	1,281
Gimli_GMU-v5	1,283.3	95%		4,586	52.5	503
Gimli_GT-v4	1,235.5	95%		4,027	60.7	604
Xoodyak_GMU2-v2	1,233.6	97%		4,058	69.7	694
Gimli_GMU-v2	983.2	97%		2,617	103.0	1,287
Gimli_GT-v6	953.4	95%		**6,341**	31.5	406
SHA2-v1	920.9	99%	3	2,001	117.7	1,571
Gimli_GT-v3	854.8	96%		4,451	55.6	800
Xoodyak_XT-v8	815.8	98%		4,121	71.3	1,074
Ascon_GMU2-v2h	792.1	97%	4	3,764	89.2	1,384
Gimli_GT-v2	785.5	97%		2,852	76.2	1,192
Ascon_GMU2-v3h	759.6	97%		4,925	61.2	990
Gimli_GT-v5	701.7	94%		**5,738**	23.3	408
Xoodyak_XT-v7	656.1	99%		2,489	88.4	1,656
DryGASCON-v1	605.8	99%	5	3,801	100.5	2,039
Saturnin-v2	587.3	96%	6	3,648	79.0	1,653
Ascon_Graz-v5	576.7	97%		4,646	55.6	1,185
Xoodyak_GMU-v1	549.1	99%		3,172	74.0	1,656
Ascon_GMU2-v1h	527.1	97%		2,928	110.1	2,566
Gimli_GMU-v1	509.0	97%		2,328	102.0	2,463
Gimli_GT-v7	500.3	95%		**8,238**	16.4	404
Ascon_Graz-v3	495.5	97%		3,305	63.7	1,579
Ascon_Graz-v6	482.7	97%		**5,346**	38.8	988
Ascon_Graz-v4	481.3	97%		3,379	61.9	1,579
Gimli_GT-v1	406.0	97%		2,537	78.2	2,368
Subterranean_ST-v2	379.7	99%	7	1,342	95.7	3,098
KNOT-v2x4h	378.5	97%	8	4,283	60.9	1,976
Ascon_VT-v2	313.5	97%		3,041	75.4	2,956
Ascon_Graz-v2	285.0	97%		2,603	64.0	2,761
Ascon_Graz-v1	263.8	97%		2,544	59.3	2,761
ACE_GMU-v1	257.1	97%	9	2,784	74.2	3,548
SCHWAEMM-v2	236.1	98%	10*	**5,947**	63.8	3,320
KNOT-v2x2h	235.1	98%		3,373	75.3	3,936
PHOTON-Beetle-v1	130.3	100%	11	3,294	101.4	9,566
KNOT-v2x1h	123.5	98%		2,446	78.9	7,856
Saturnin-v1	75.9	98%		3,070	92.6	14,981
Xoodyak_GMU-v2	36.5	99%		2,316	74.8	25,142
ACE_UW-v1	35.4	97%		2,156	73.8	25,608
Gimli_TUM-v1	12.4	98%		1,767	78.0	77,046
Gimli_TUM-v2	6.2	98%		1,767	73.5	144,482
Gimli_TUM-v3	3.5	98%		1,772	78.5	279,354
Minimum		**94%**				
Average		**97%**				
Maximum		**100%**				

Table 71: Lattice ECP5 Hash Throughput for 64 Byte Messages

Variant	Throughput 64B [Mbit/s]	Thr HM 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Xoodyak_GMU2-v1	906.4	61%	1	3,248	150.5	85
Gimli_GMU-v4	883.7	51%	2	3,223	94.9	55
SHA2-v1	793.2	86%	3	2,001	117.7	76
Xoodyak_GMU2-v2	713.4	56%		4,058	69.7	50
Gimli_GMU-v5	625.5	47%		4,586	52.5	43
Gimli_GT-v4	598.0	46%		4,027	60.7	52
Xoodyak_XT-v8	588.8	71%		4,121	71.3	62
Gimli_GMU-v2	579.4	57%		2,617	103.0	91
Xoodyak_XT-v7	492.1	74%		2,489	88.4	92
DryGASCON-v1	481.0	79%	4	3,801	100.5	107
Ascon_GMU2-v2h	475.8	58%	5	3,764	89.2	96
Ascon_GMU2-v3h	447.6	57%		4,925	61.2	70
Gimli_GT-v3	445.2	50%		4,451	55.6	64
Gimli_GT-v2	443.3	55%		2,852	76.2	88
Gimli_GT-v6	424.4	42%		**6,341**	31.5	38
Xoodyak_GMU-v1	411.8	74%		3,172	74.0	92
Ascon_Graz-v5	351.5	59%		4,646	55.6	81
Ascon_GMU2-v1h	323.9	60%		2,928	110.1	174
Gimli_GMU-v1	320.5	61%		2,328	102.0	163
Subterranean_ST-v2	318.3	83%	6	1,342	95.7	154
Ascon_Graz-v3	304.7	60%		3,305	63.7	107
Saturnin-v2	299.6	49%	7	3,648	79.0	135
Gimli_GT-v5	298.2	40%		**5,738**	23.3	40
Ascon_Graz-v4	296.0	60%		3,379	61.9	107
Ascon_Graz-v6	292.2	59%		**5,346**	38.8	68
Gimli_GT-v1	250.4	60%		2,537	78.2	160
Gimli_GT-v7	234.0	44%		**8,238**	16.4	36
KNOT-v2x4h	229.2	59%	8	4,283	60.9	136
Ascon_VT-v2	197.0	61%		3,041	75.4	196
Ascon_Graz-v2	177.2	61%		2,603	64.0	185
SCHWAEMM-v2	170.1	71%	9*	**5,947**	63.8	192
Ascon_Graz-v1	164.1	61%		2,544	59.3	185
ACE_GMU-v1	161.0	61%	10	2,784	74.2	236
KNOT-v2x2h	150.6	63%		3,373	75.3	256
PHOTON-Beetle-v1	141.9	109%	11	3,294	101.4	366
KNOT-v2x1h	81.5	65%		2,446	78.9	496
Saturnin-v1	49.8	64%		3,070	92.6	951
Xoodyak_GMU-v2	29.1	79%		2,316	74.8	1,314
ACE_UW-v1	22.4	62%		2,156	73.8	1,688
Gimli_TUM-v1	8.4	66%		1,767	78.0	4,734
Gimli_TUM-v2	4.2	66%		1,767	73.5	8,874
Gimli_TUM-v3	2.3	66%		1,772	78.5	17,154
Minimum		**40%**				
Average		**62%**				
Maximum		**109%**				

Table 72: Lattice ECP5 Hash Throughput for 16 Byte Messages

Variant	**Throughput 16B [Mbit/s]**	**Thr HM 16B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 16B**
Xoodyak_GMU2-v1	418.7	28%	1	3,248	150.5	46
Gimli_GMU-v4	357.4	21%	2	3,223	94.9	34
Xoodyak_XT-v8	314.7	38%		4,121	71.3	29
Xoodyak_GMU2-v2	307.5	24%		4,058	69.7	29
DryGASCON-v1	292.5	48%	3	3,801	100.5	44
Xoodyak_XT-v7	276.0	41%		2,489	88.4	41
Gimli_GMU-v2	253.5	25%		2,617	103.0	52
Gimli_GMU-v5	240.1	18%		4,586	52.5	28
Xoodyak_GMU-v1	231.0	41%		3,172	74.0	41
Gimli_GT-v4	228.6	18%		4,027	60.7	34
Ascon_GMU2-v2h	211.5	26%	4	3,764	89.2	54
Subterranean_ST-v2	211.3	55%	5	1,342	95.7	58
SHA2-v1	198.3	21%	6	2,001	117.7	76
PHOTON-Beetle-v1	196.7	152%	7	3,294	101.4	66
Ascon_GMU2-v3h	195.8	25%		4,925	61.2	40
Gimli_GT-v2	187.6	23%		2,852	76.2	52
Gimli_GT-v3	178.1	20%		4,451	55.6	40
Ascon_Graz-v5	158.2	27%		4,646	55.6	45
Gimli_GT-v6	155.1	15%		**6,341**	31.5	26
Gimli_GMU-v1	148.4	28%		2,328	102.0	88
Ascon_GMU2-v1h	146.7	27%		2,928	110.1	96
Saturnin-v2	146.6	24%	8	3,648	79.0	69
Ascon_Graz-v3	138.1	27%		3,305	63.7	59
Ascon_Graz-v4	134.2	27%		3,379	61.9	59
Ascon_Graz-v6	130.7	26%		**5,346**	38.8	38
Gimli_GT-v1	113.8	27%		2,537	78.2	88
Gimli_GT-v5	106.5	14%		**5,738**	23.3	28
KNOT-v2x4h	102.5	26%	9	4,283	60.9	76
Ascon_VT-v2	91.1	28%		3,041	75.4	106
SCHWAEMM-v2	90.7	38%	10*	**5,947**	63.8	90
Gimli_GT-v7	87.7	17%		**8,238**	16.4	24
Ascon_Graz-v2	81.2	28%		2,603	64.0	101
Ascon_Graz-v1	75.1	28%		2,544	59.3	101
ACE_GMU-v1	74.2	28%	11	2,784	74.2	128
KNOT-v2x2h	70.9	29%		3,373	75.3	136
KNOT-v2x1h	39.5	31%		2,446	78.9	256
Saturnin-v1	34.8	45%		3,070	92.6	341
Xoodyak_GMU-v2	17.8	48%		2,316	74.8	537
ACE_UW-v1	10.4	29%		2,156	73.8	908
Gimli_TUM-v1	4.2	33%		1,767	78.0	2,376
Gimli_TUM-v2	2.1	33%		1,767	73.5	4,452
Gimli_TUM-v3	1.2	33%		1,772	78.5	8,604
Minimum		**14%**				
Average		**32%**				
Maximum		**152%**				

B Power and Energy – Design Space Exploration

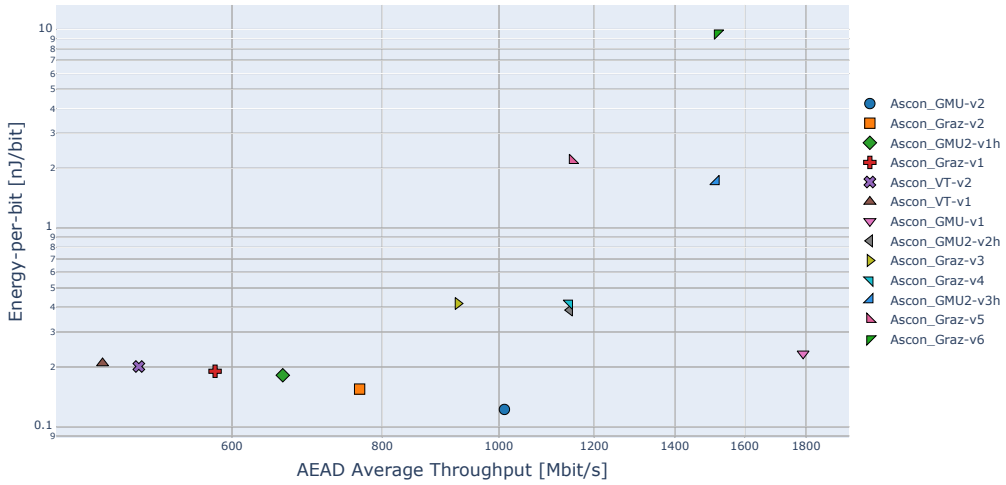

Figure 58: Design-space exploration of Ascon variants for AEAD of long messages: Energy-per-bit vs. Throughput

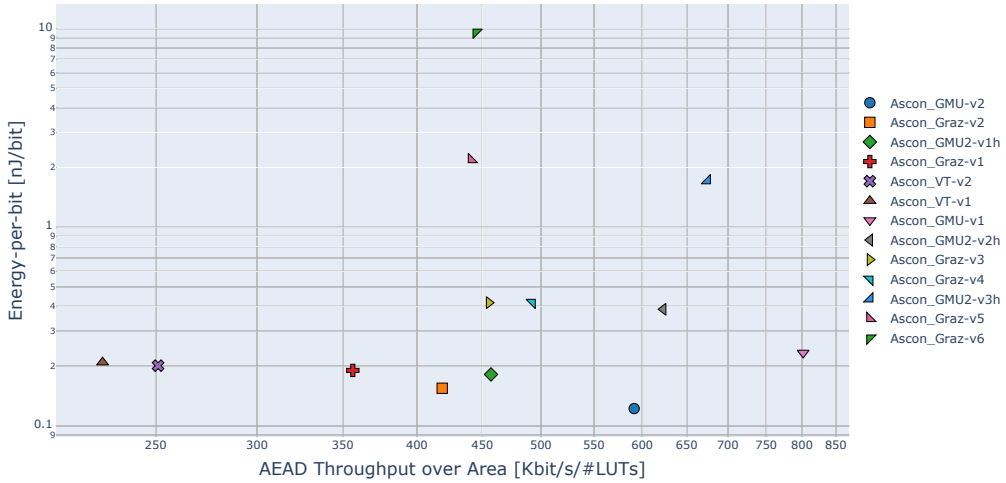

Figure 59: Design-space exploration of Ascon variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

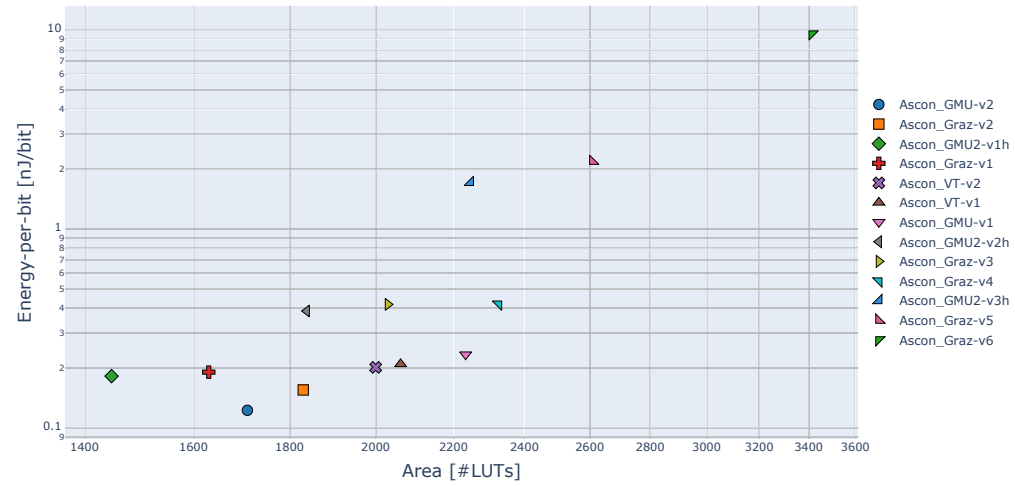

Figure 60: Design-space exploration of Ascon variants for AEAD of long messages: Energy-per-bit vs. Area

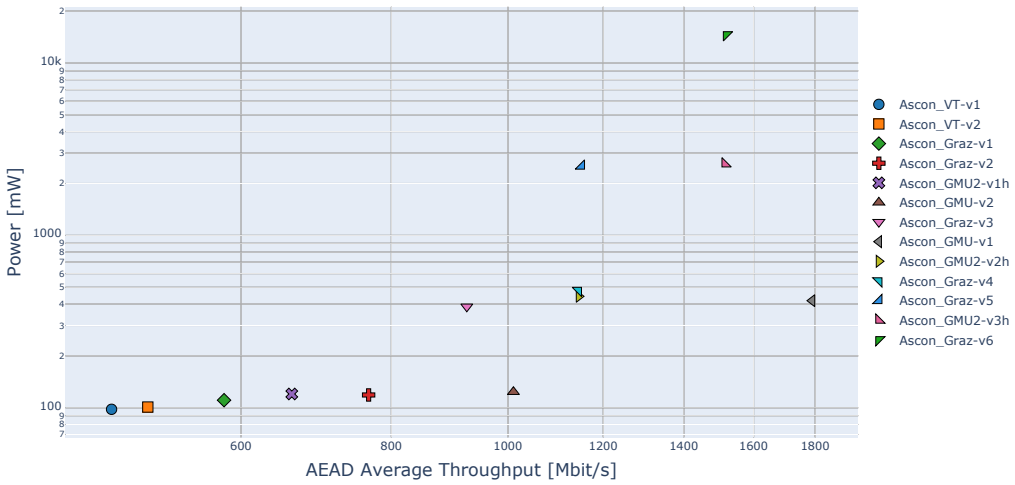

Figure 61: Design-space exploration of Ascon variants for AEAD of long messages: Power vs. Throughput

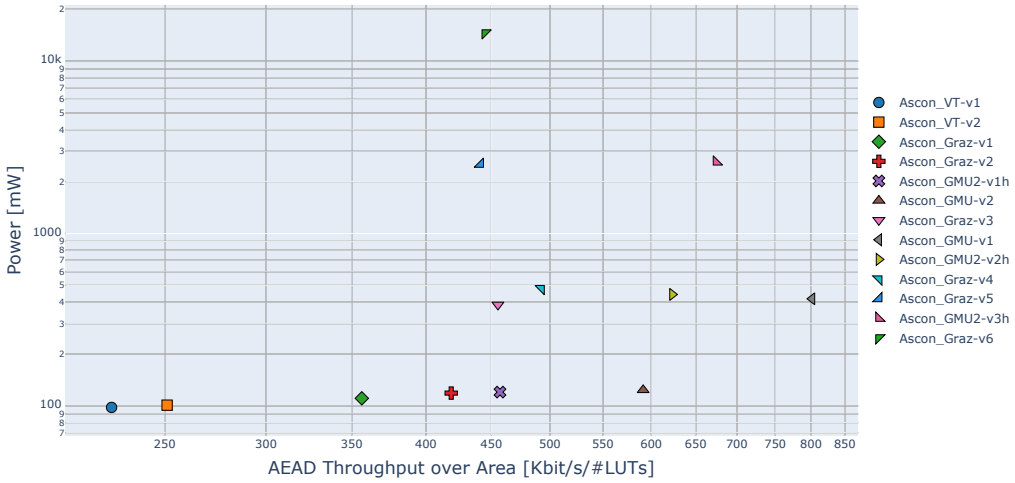

Figure 62: Design-space exploration of Ascon variants for AEAD of long messages: Power vs. Throughput-over-Area

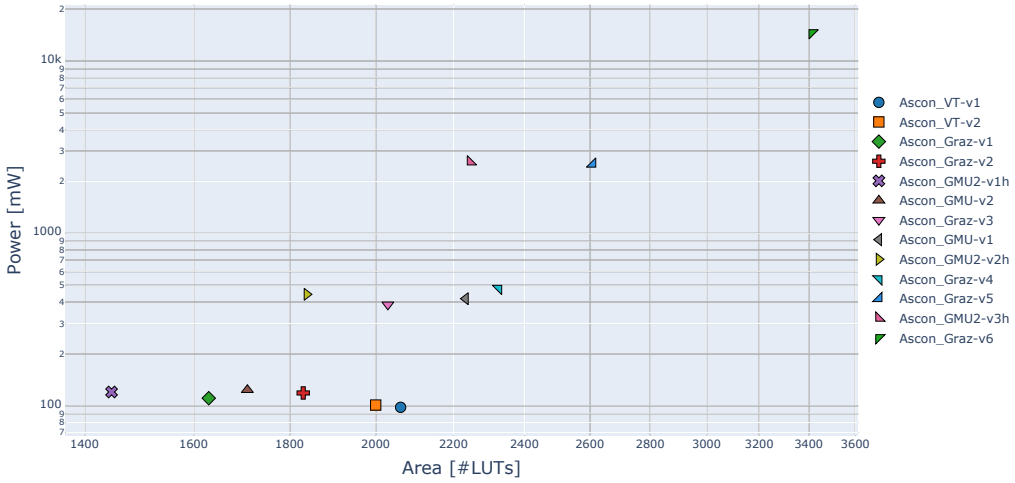

Figure 63: Design-space exploration of Ascon variants for AEAD of long messages: Power vs. Area

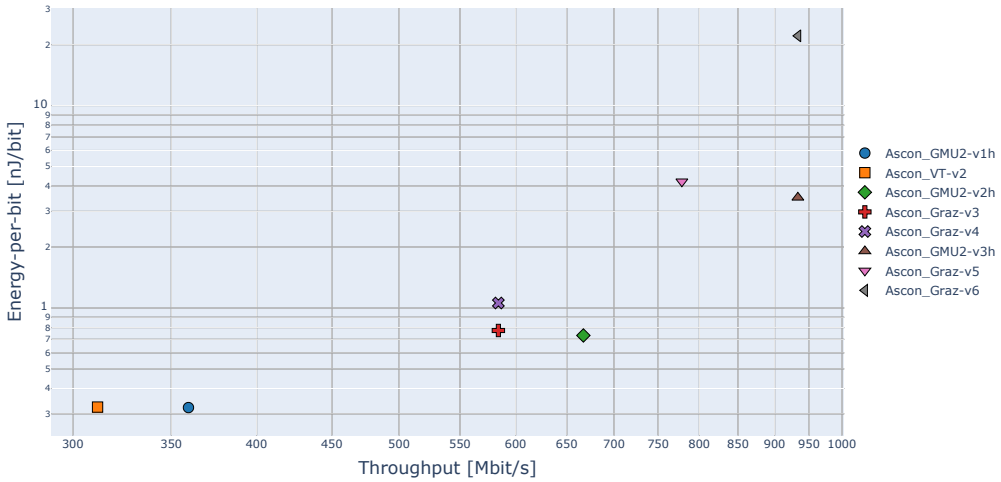

Figure 64: Design-space exploration of Ascon variants for hashing of long messages: Energy-per-bit vs. Throughput

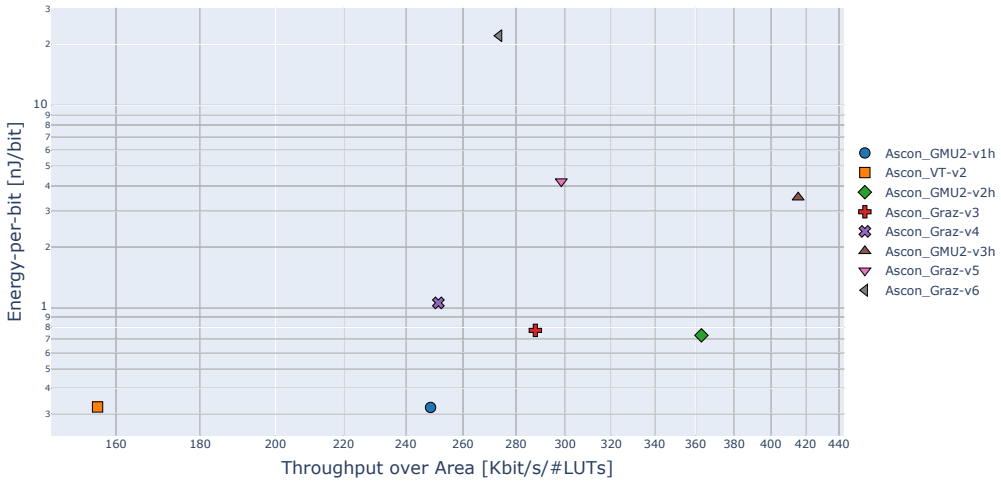

Figure 65: Design-space exploration of Ascon variants for hashing of long messages: Energy-per-bit vs. Throughput-over-Area

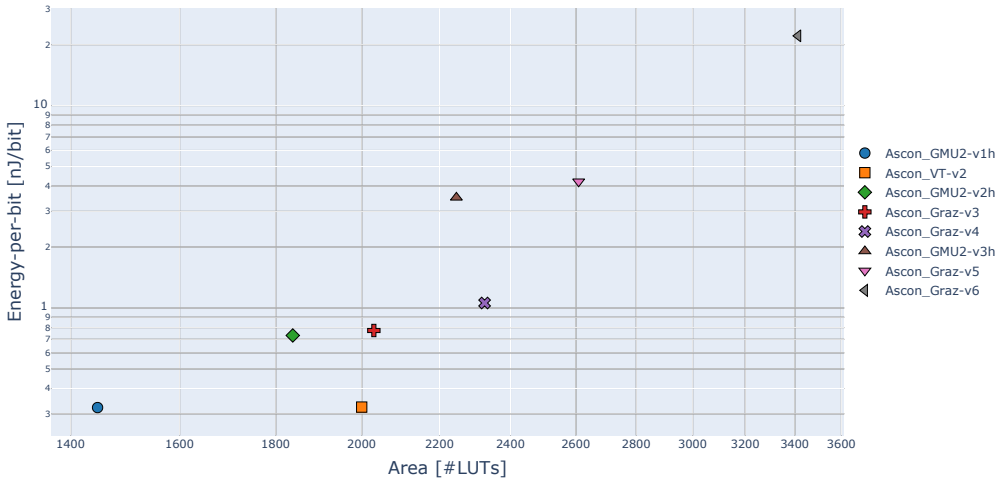

Figure 66: Design-space exploration of Ascon variants for hashing of long messages: Energy-per-bit vs. Area

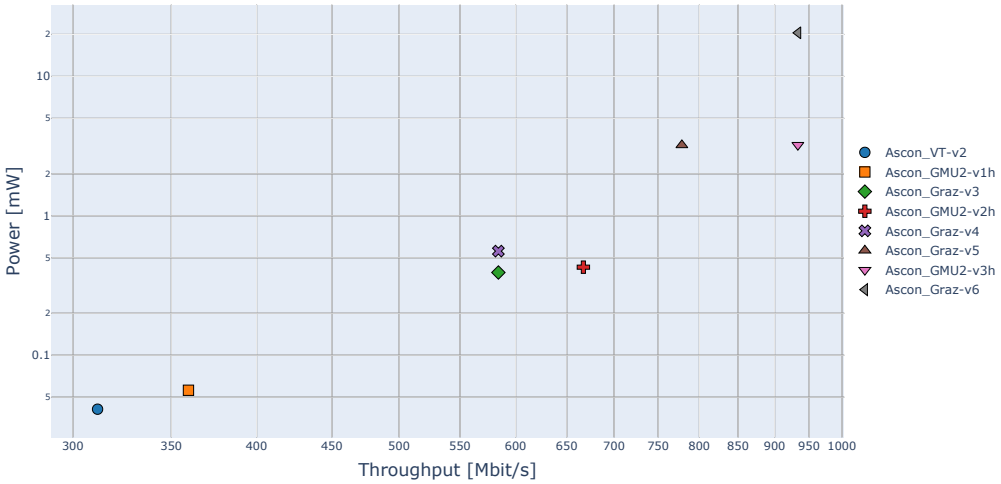

Figure 67: Design-space exploration of Ascon variants for hashing long messages: Power vs. Throughput

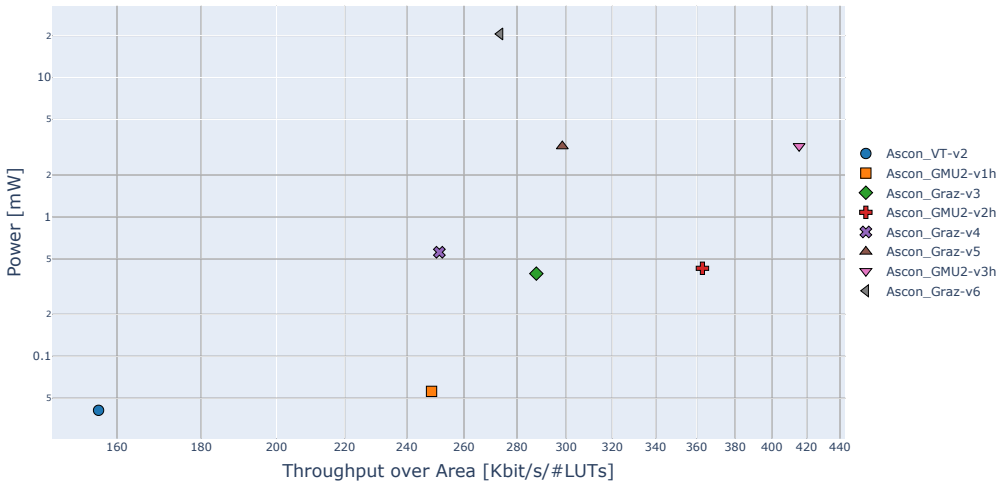

Figure 68: Design-space exploration of Ascon variants for hashing long messages: Power vs. Throughput-over-Area

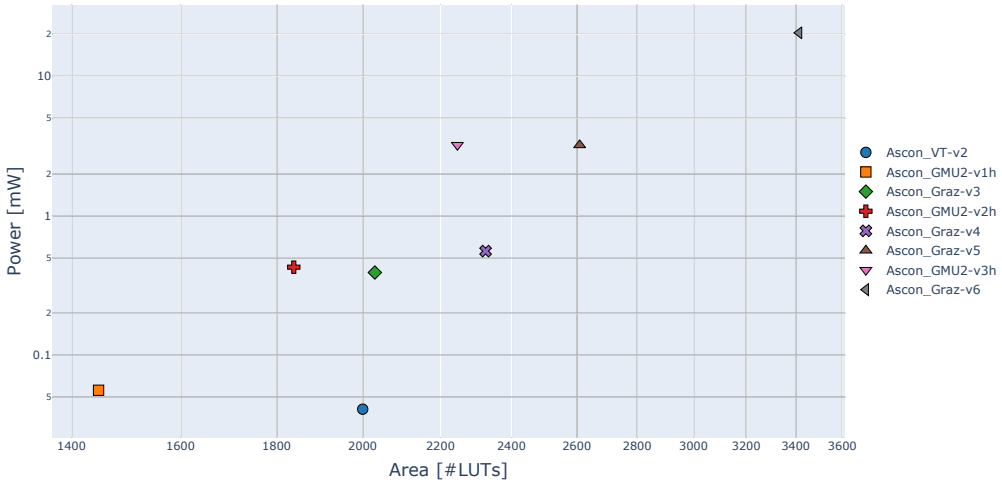

Figure 69: Design-space exploration of Ascon variants for hashing long messages: Power vs. Area

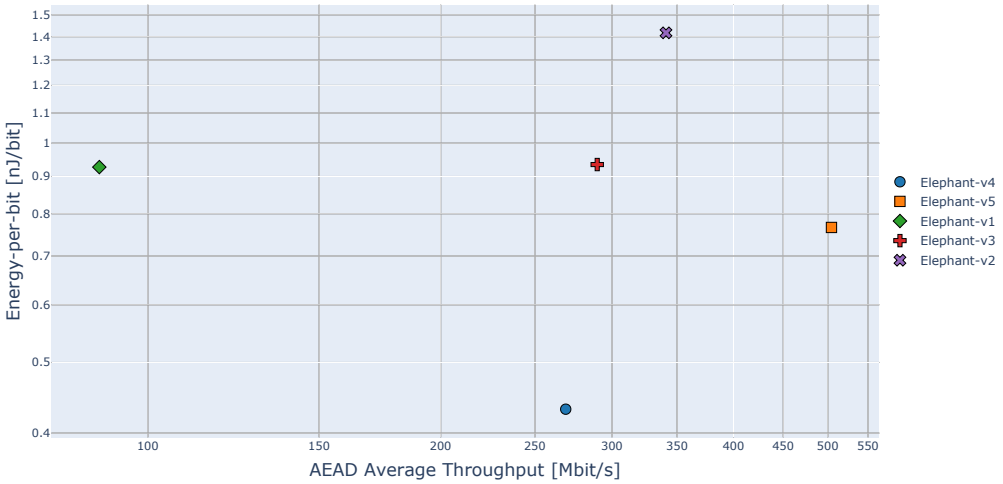

Figure 70: Design-space exploration of Elephant variants for AEAD of long messages: Energy-per-bit vs. Throughput

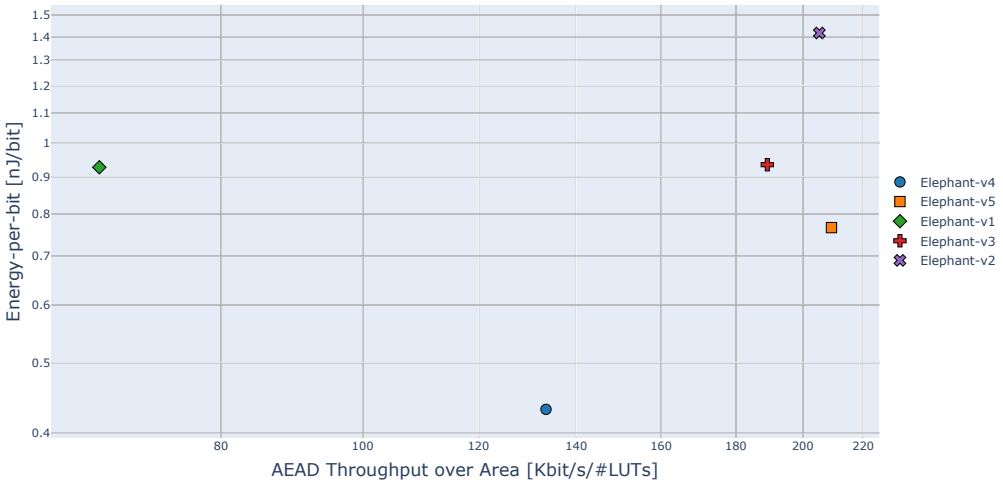

Figure 71: Design-space exploration of Elephant variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

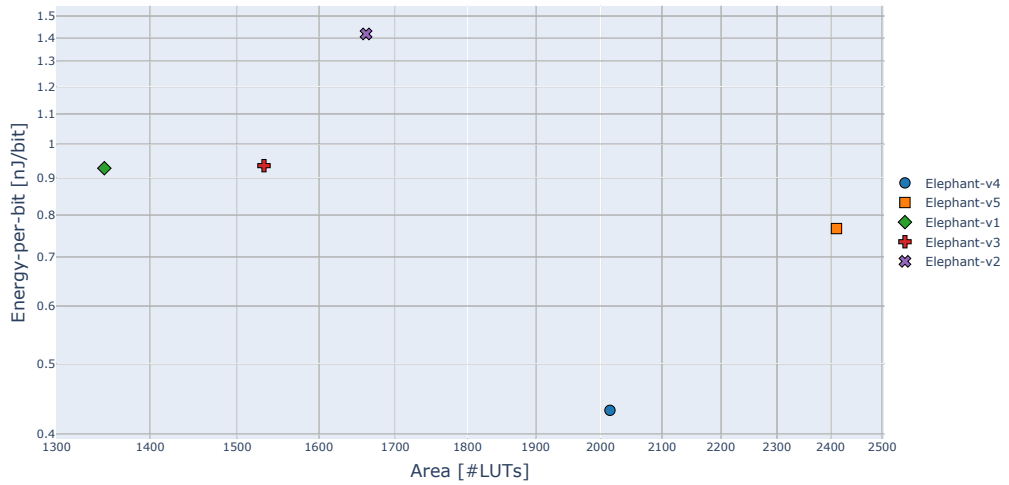

Figure 72: Design-space exploration of Elephant variants for AEAD of long messages: Energy-per-bit vs. Area

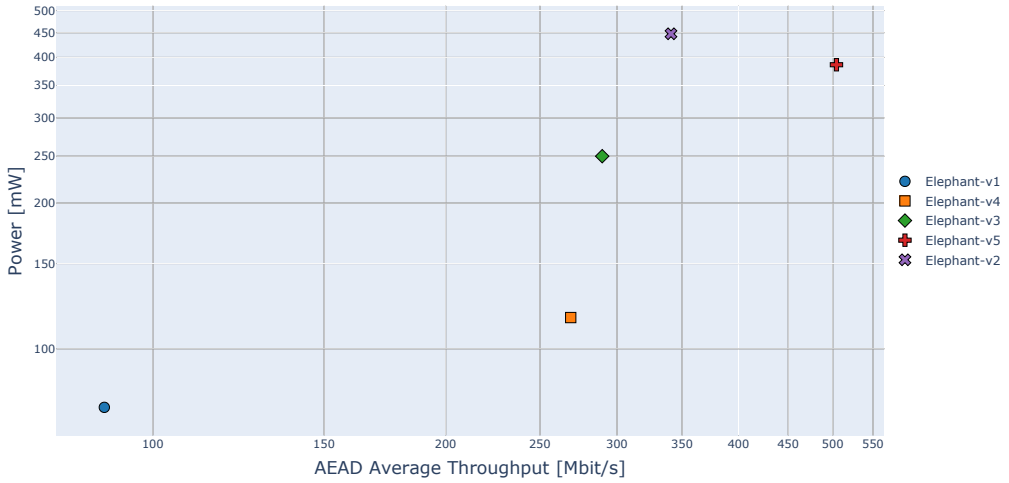

Figure 73: Design-space exploration of Elephant variants for AEAD of long messages: Power vs. Throughput

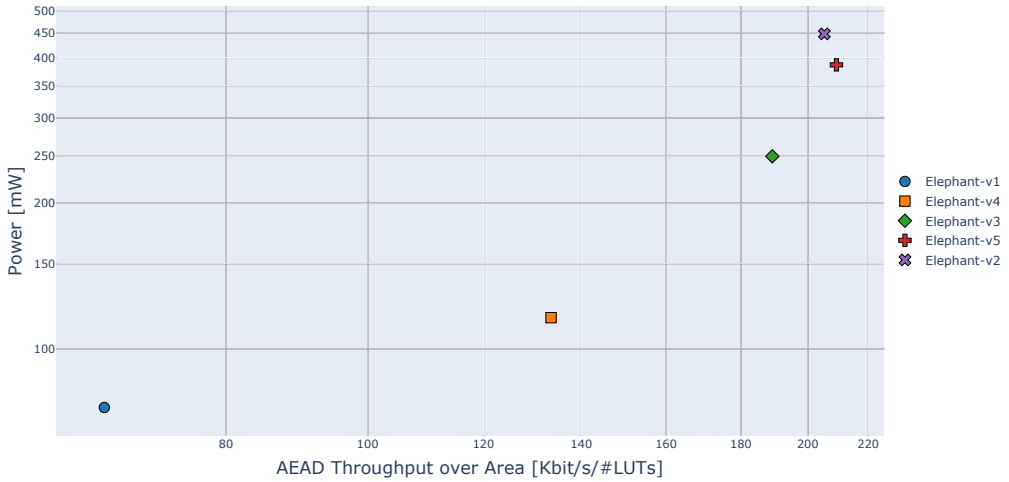

Figure 74: Design-space exploration of Elephant variants for AEAD of long messages: Power vs. Throughput-over-Area

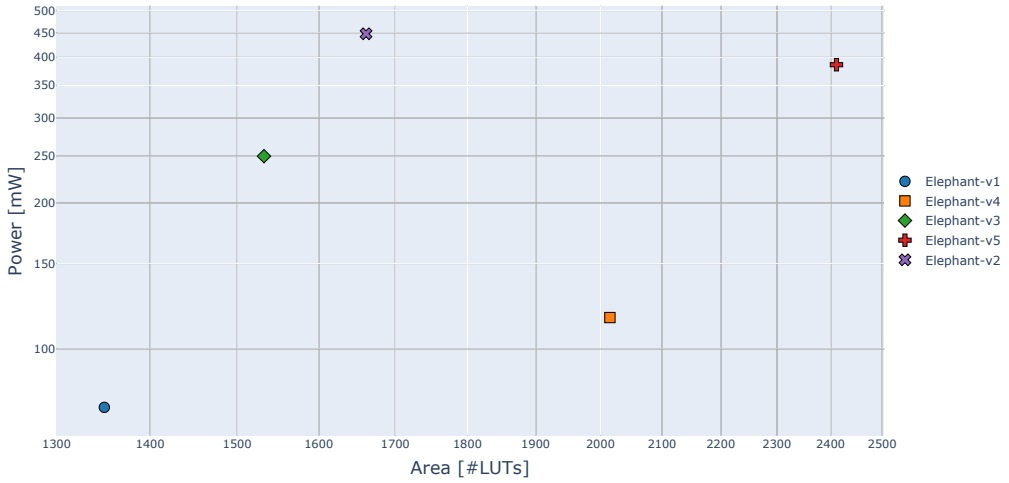

Figure 75: Design-space exploration of Elephant variants for AEAD of long messages: Power vs. Area

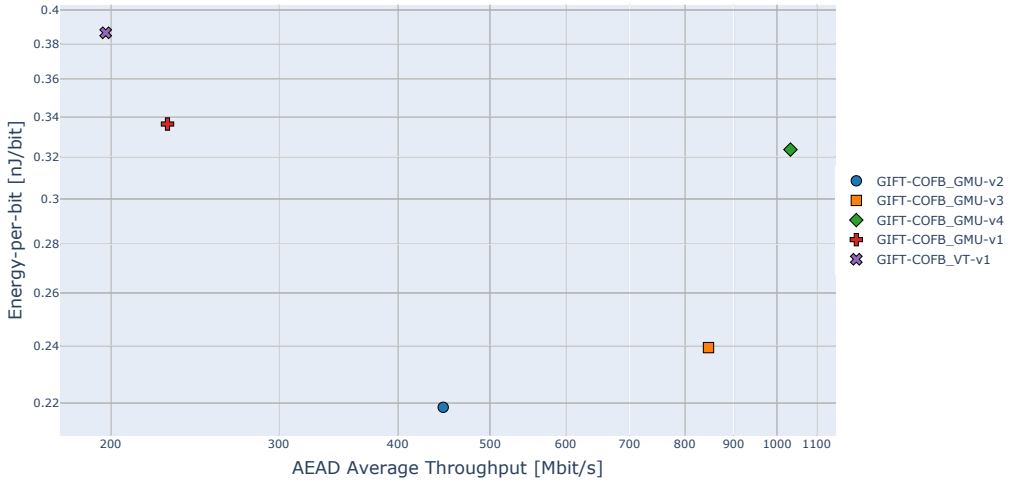

Figure 76: Design-space exploration of GIFT-COFB variants for AEAD of long messages: Energy-per-bit vs. Throughput

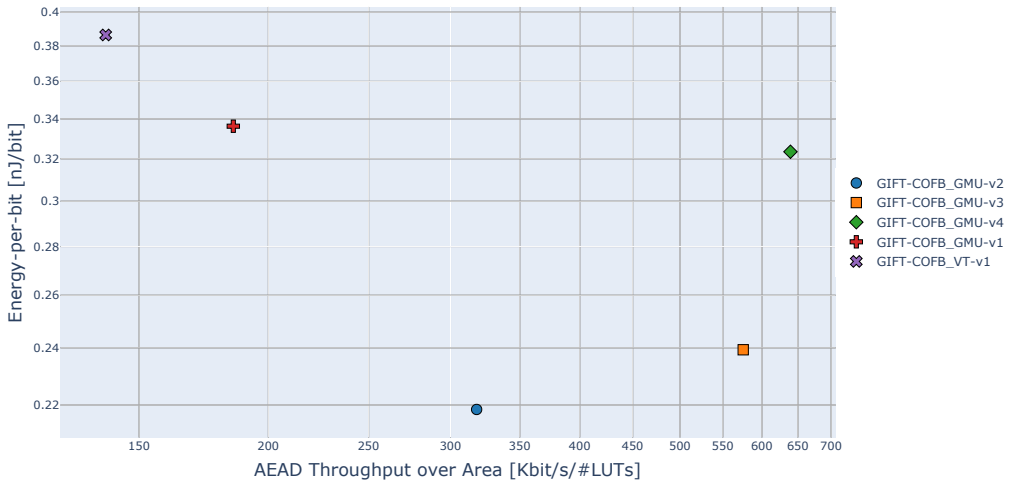

Figure 77: Design-space exploration of GIFT-COFB variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

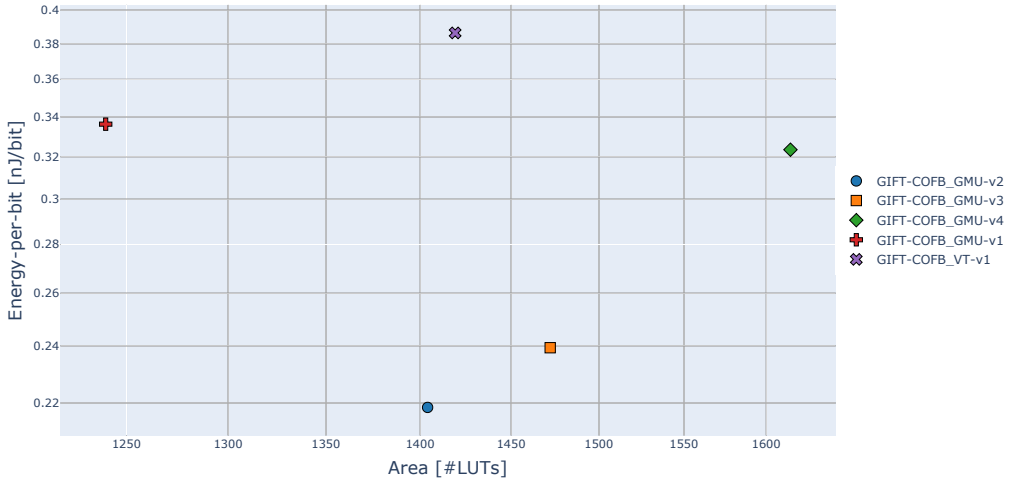

Figure 78: Design-space exploration of GIFT-COFB variants for AEAD of long messages: Energy-per-bit vs. Area

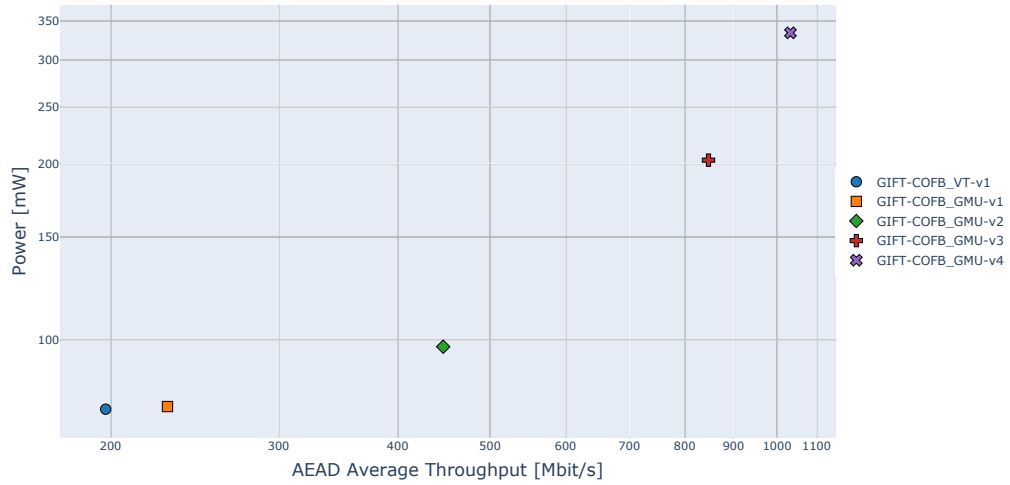

Figure 79: Design-space exploration of GIFT-COFB variants for AEAD of long messages: Power vs. Throughput

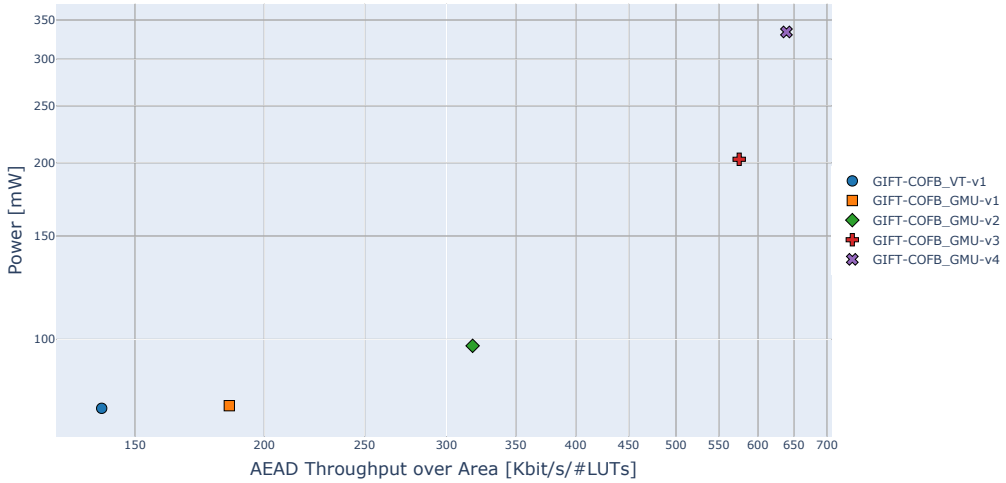

Figure 80: Design-space exploration of GIFT-COFB variants for AEAD of long messages: Power vs. Throughput-over-Area

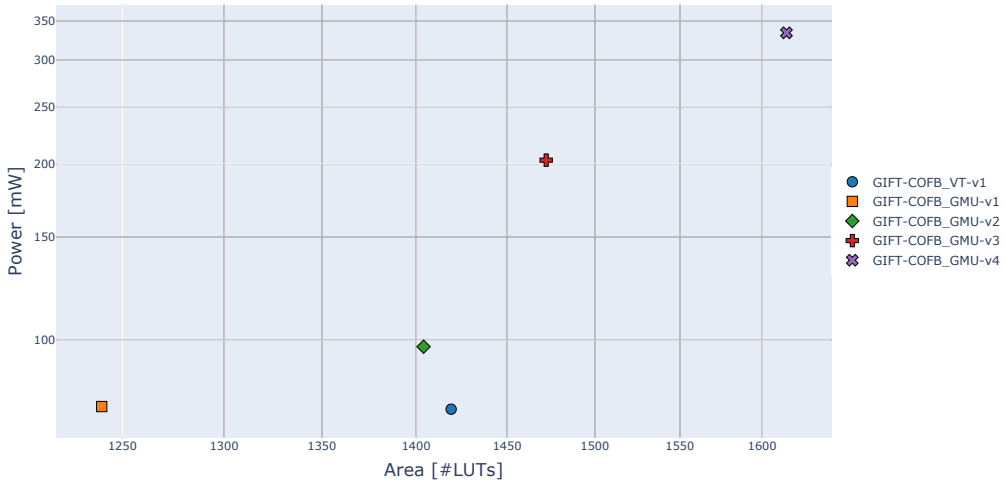

Figure 81: Design-space exploration of GIFT-COFB variants for AEAD of long messages: Power vs. Area

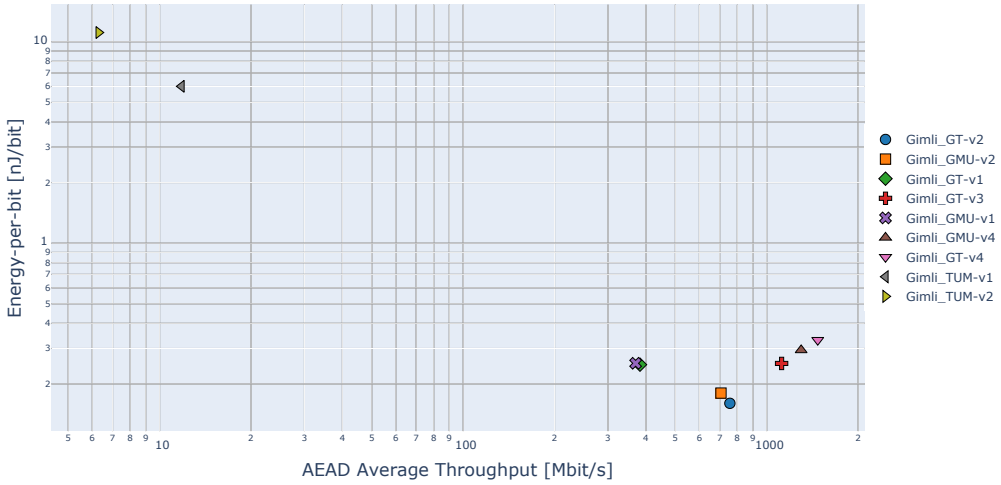

Figure 82: Design-space exploration of Gimli variants for AEAD of long messages: Energy-per-bit vs. Throughput

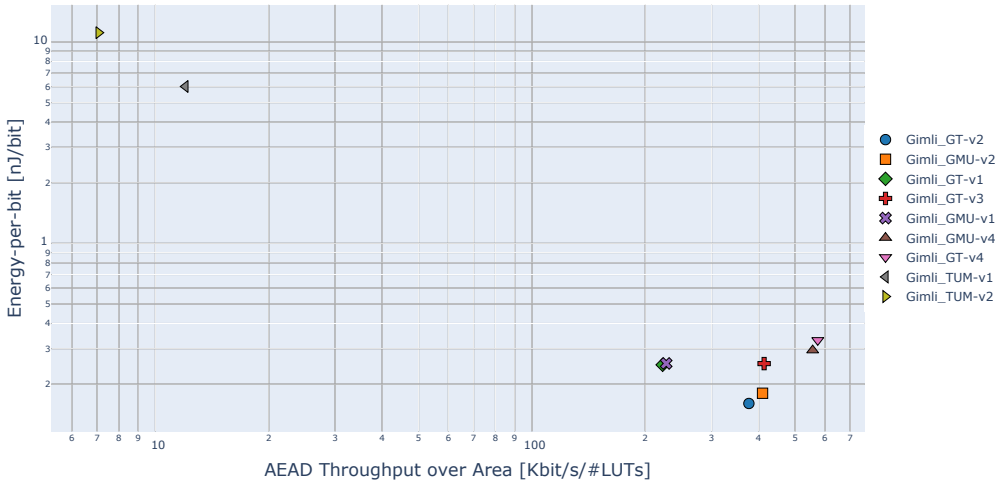

Figure 83: Design-space exploration of Gimli variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

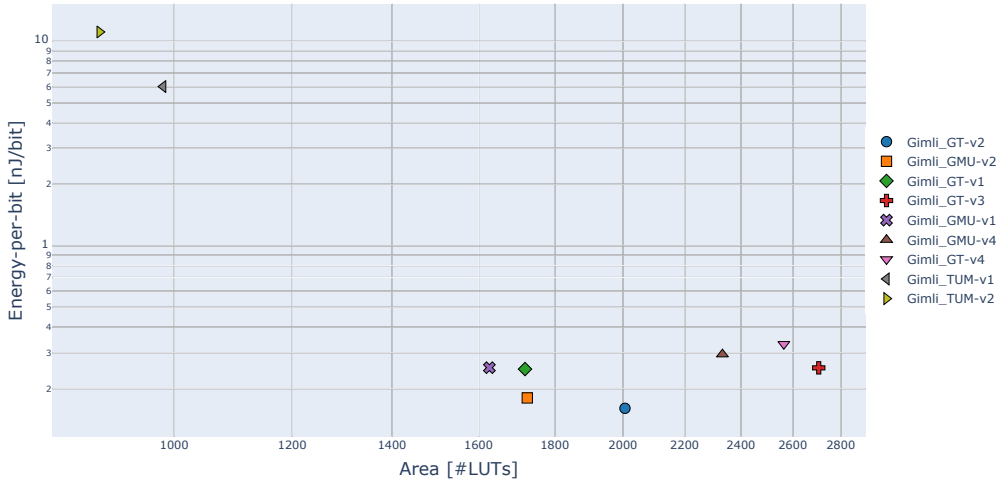

Figure 84: Design-space exploration of Gimli variants for AEAD of long messages: Energy-per-bit vs. Area

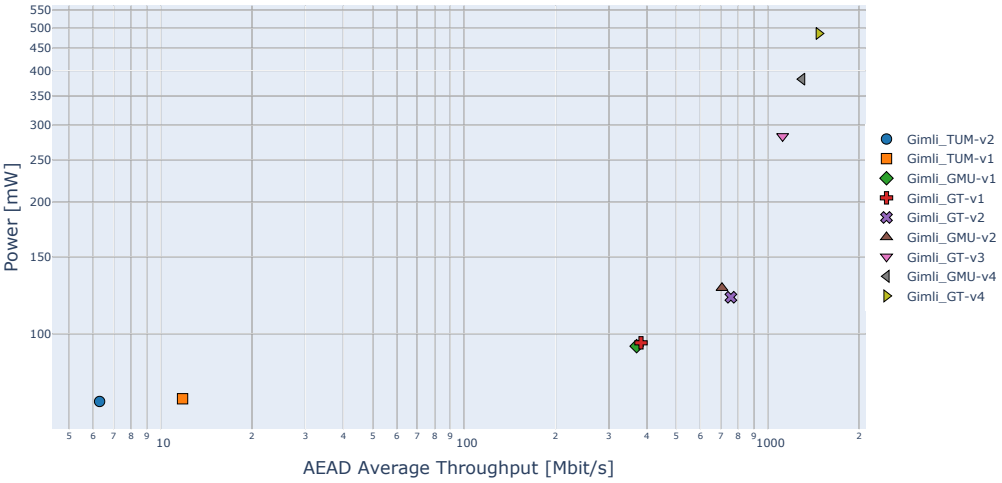

Figure 85: Design-space exploration of Gimli variants for AEAD of long messages: Power vs. Throughput

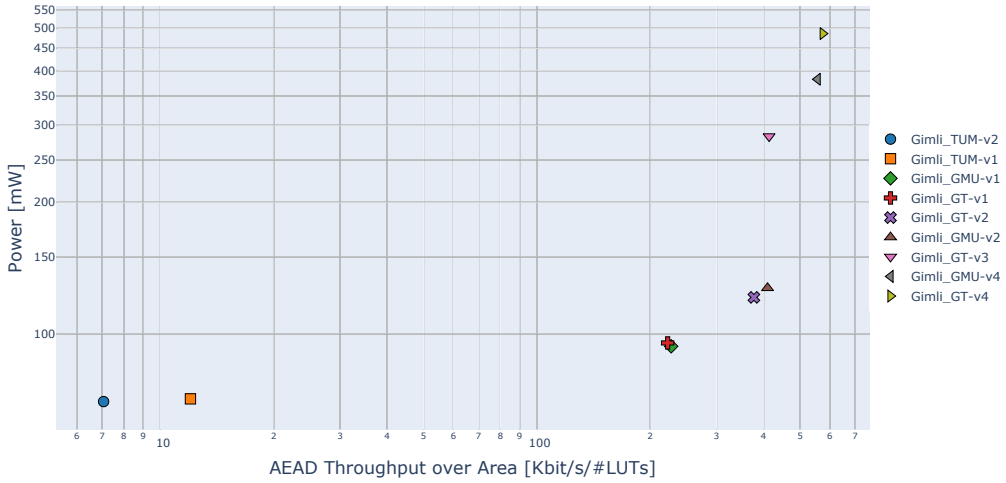

Figure 86: Design-space exploration of Gimli variants for AEAD of long messages: Power vs. Throughput-over-Area

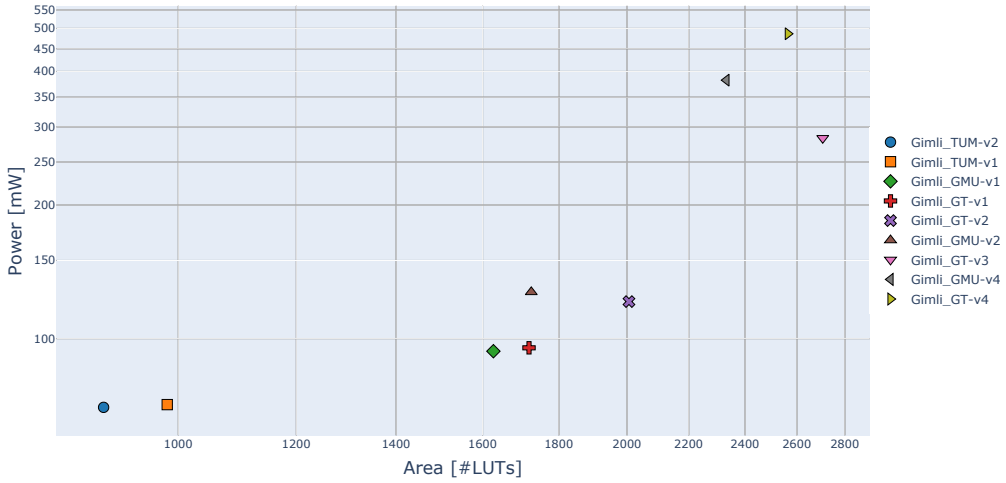

Figure 87: Design-space exploration of Gimli variants for AEAD of long messages: Power vs. Area

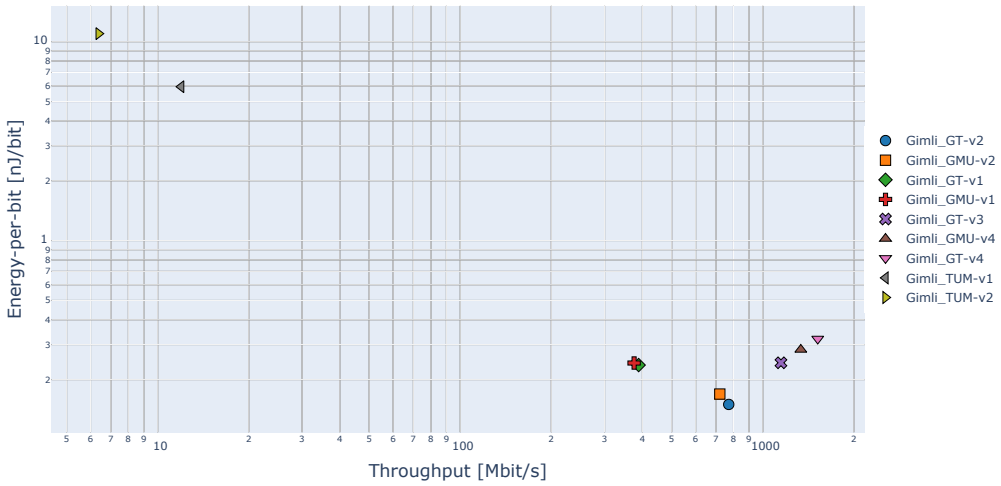

Figure 88: Design-space exploration of Gimli variants for hashing of long messages: Energy-per-bit vs. Throughput

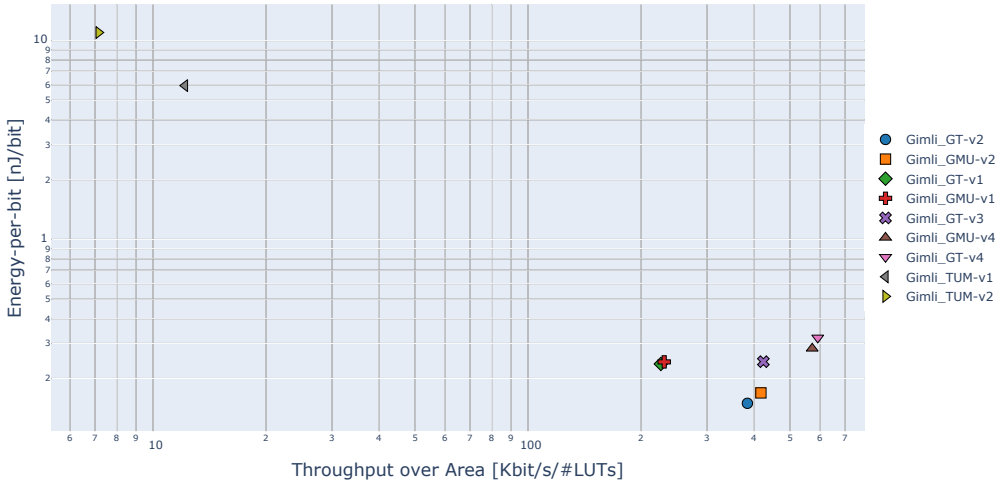

Figure 89: Design-space exploration of Gimli variants for hashing of long messages: Energy-per-bit vs. Throughput-over-Area

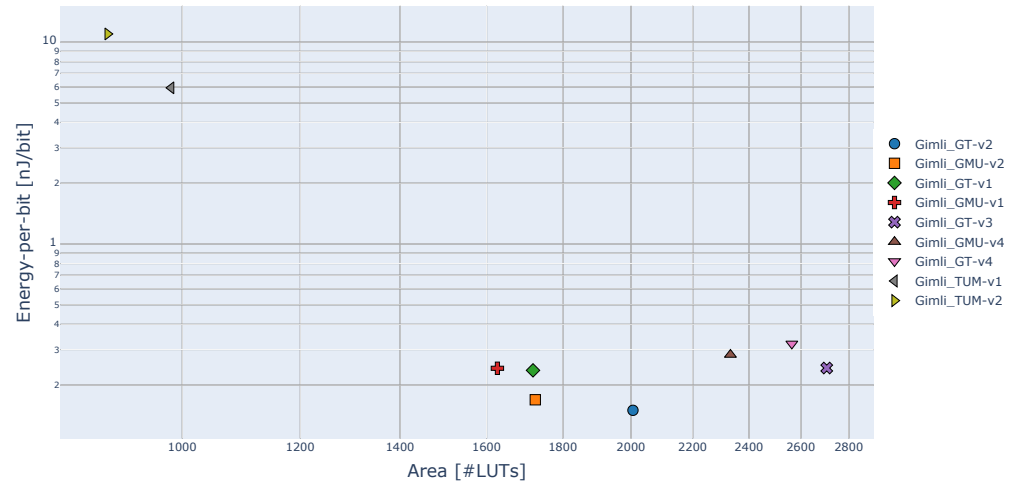

Figure 90: Design-space exploration of Gimli variants for hashing of long messages: Energy-per-bit vs. Area

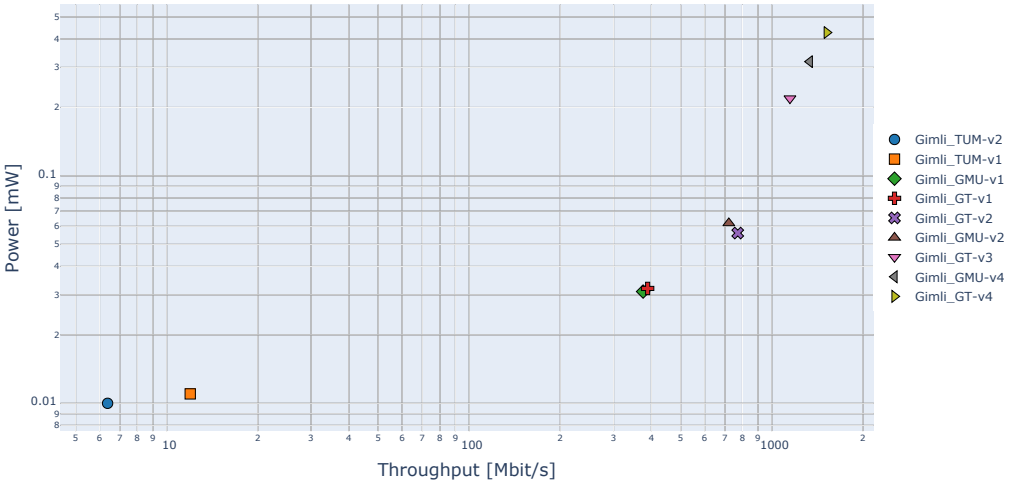

Figure 91: Design-space exploration of Gimli variants for hashing long messages: Power vs. Throughput

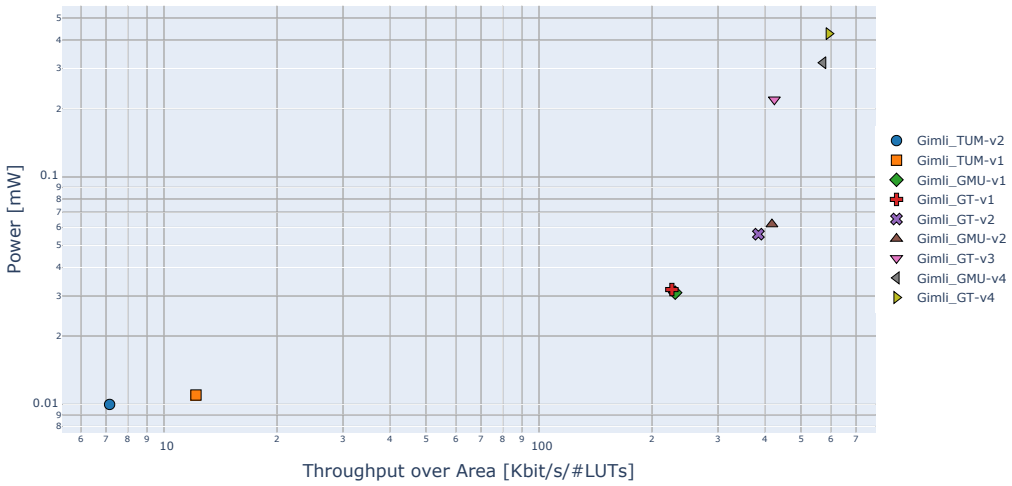

Figure 92: Design-space exploration of Gimli variants for hashing long messages: Power vs. Throughput-over-Area

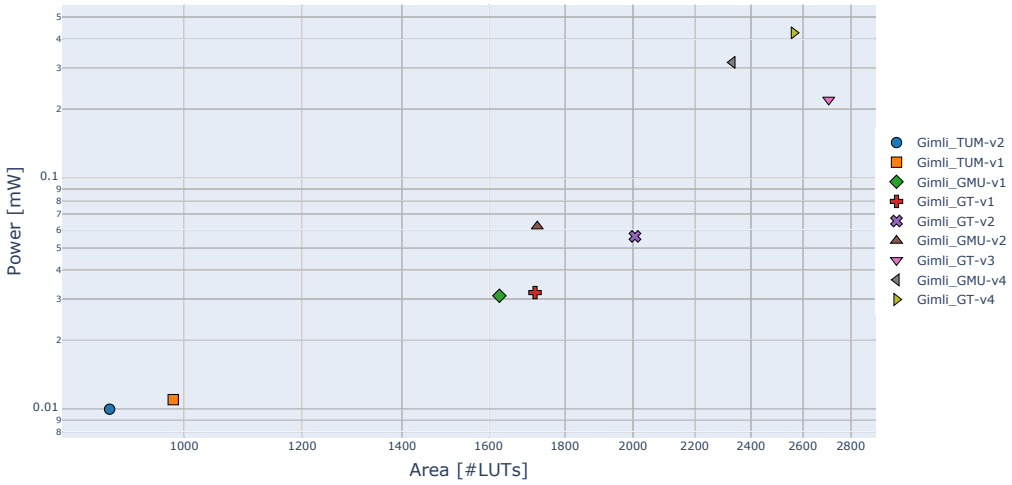

Figure 93: Design-space exploration of Gimli variants for hashing long messages: Power vs. Area

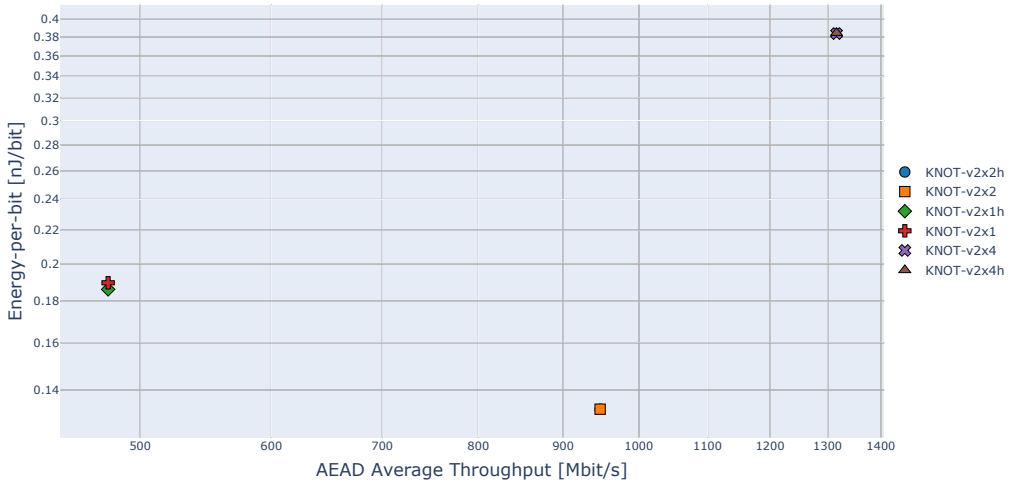

Figure 94: Design-space exploration of KNOT variants for AEAD of long messages: Energy-per-bit vs. Throughput

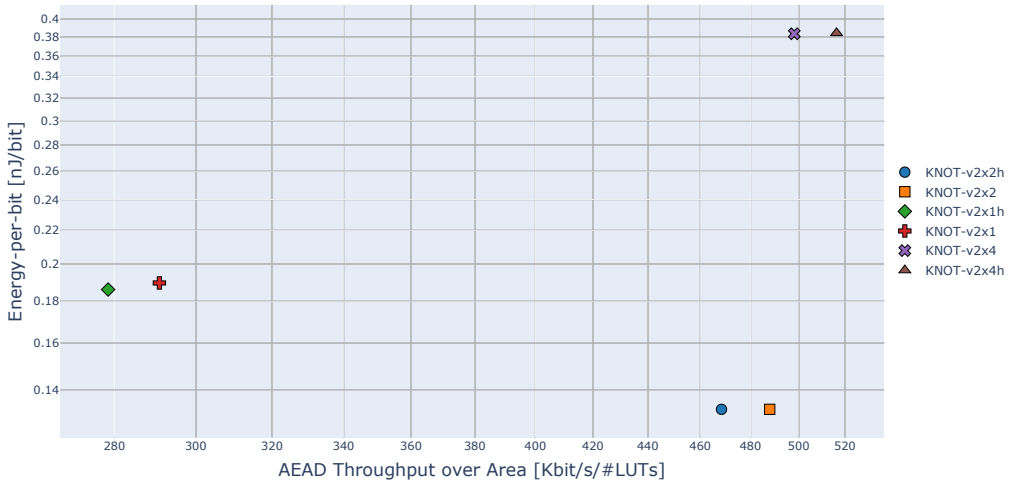

Figure 95: Design-space exploration of KNOT variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

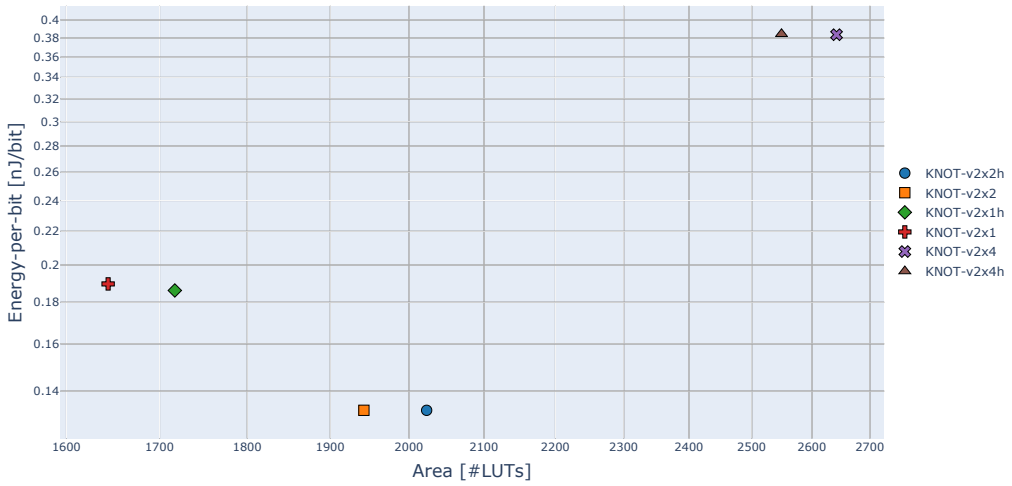

Figure 96: Design-space exploration of KNOT variants for AEAD of long messages: Energy-per-bit vs. Area

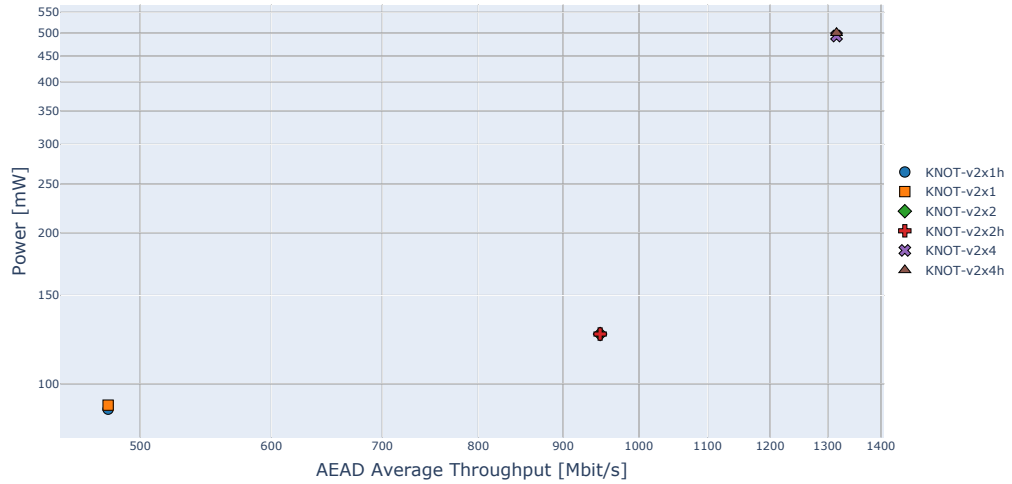

Figure 97: Design-space exploration of KNOT variants for AEAD of long messages: Power vs. Throughput

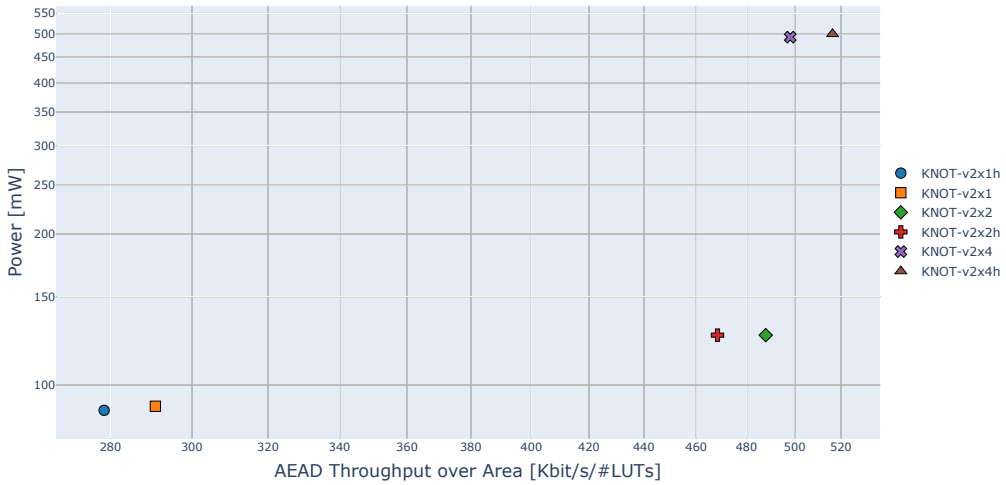

Figure 98: Design-space exploration of KNOT variants for AEAD of long messages: Power vs. Throughput-over-Area

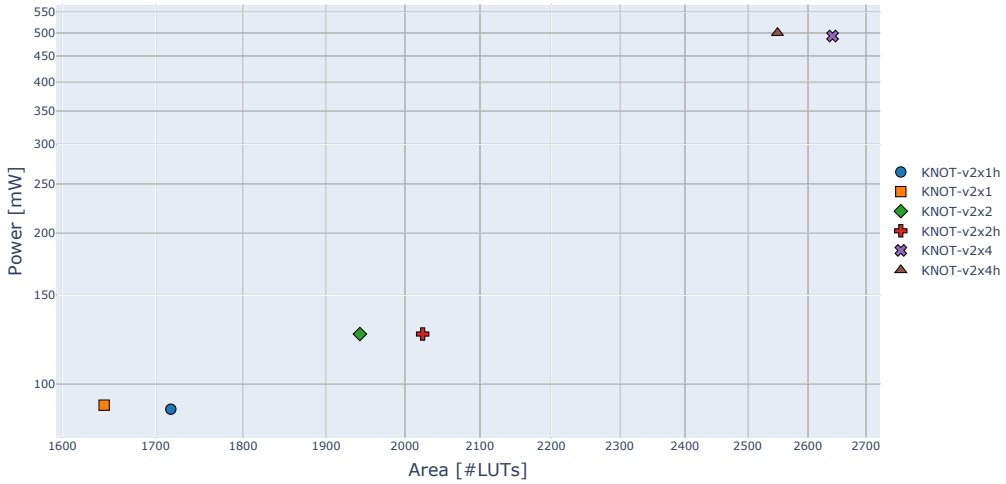

Figure 99: Design-space exploration of KNOT variants for AEAD of long messages: Power vs. Area

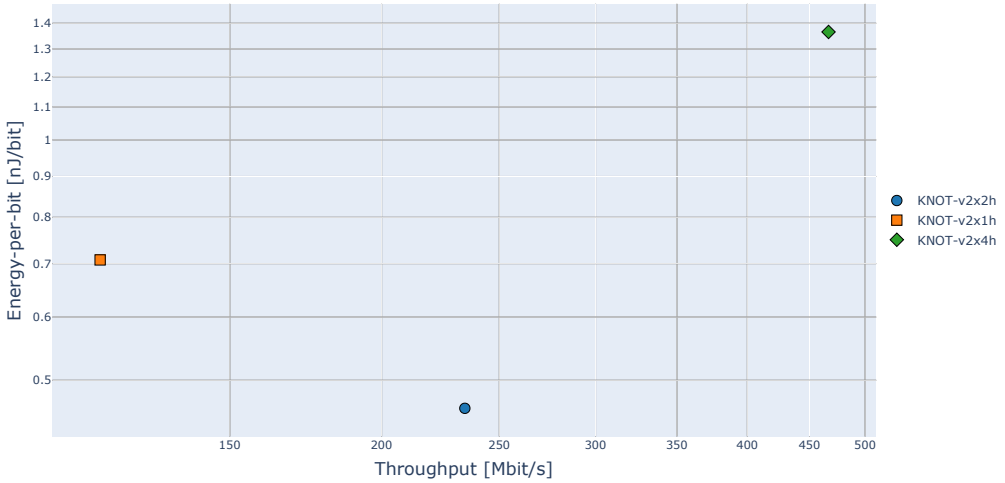

Figure 100: Design-space exploration of KNOT variants for hashing of long messages: Energy-per-bit vs. Throughput

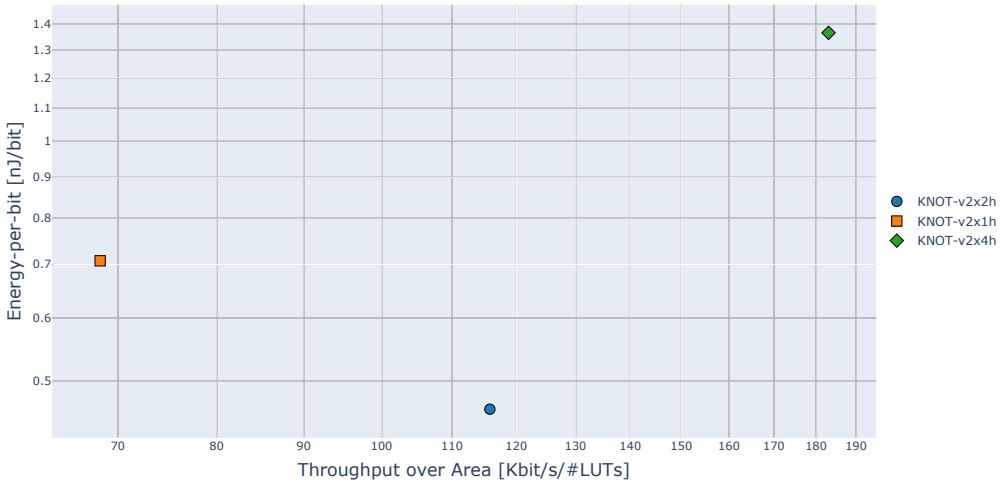

Figure 101: Design-space exploration of KNOT variants for hashing of long messages: Energy-per-bit vs. Throughput-over-Area

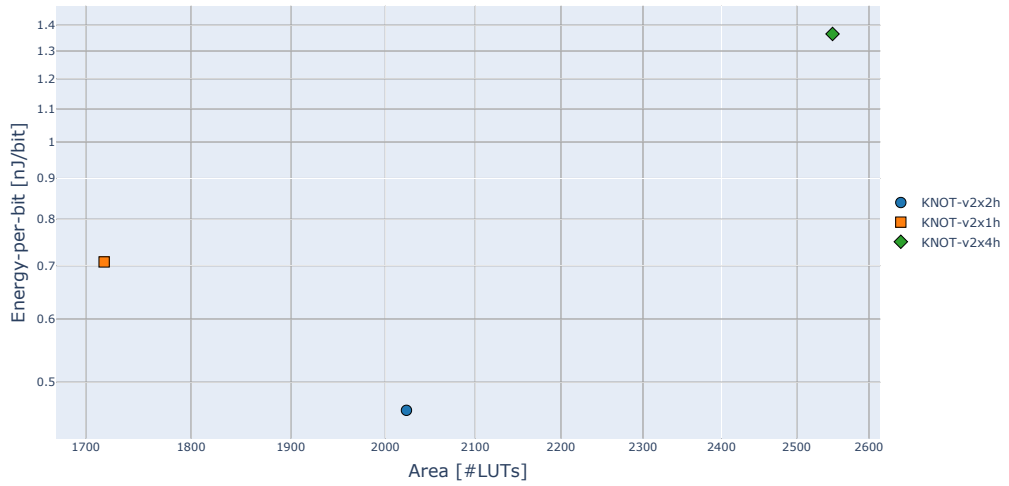

Figure 102: Design-space exploration of KNOT variants for hashing of long messages: Energy-per-bit vs. Area

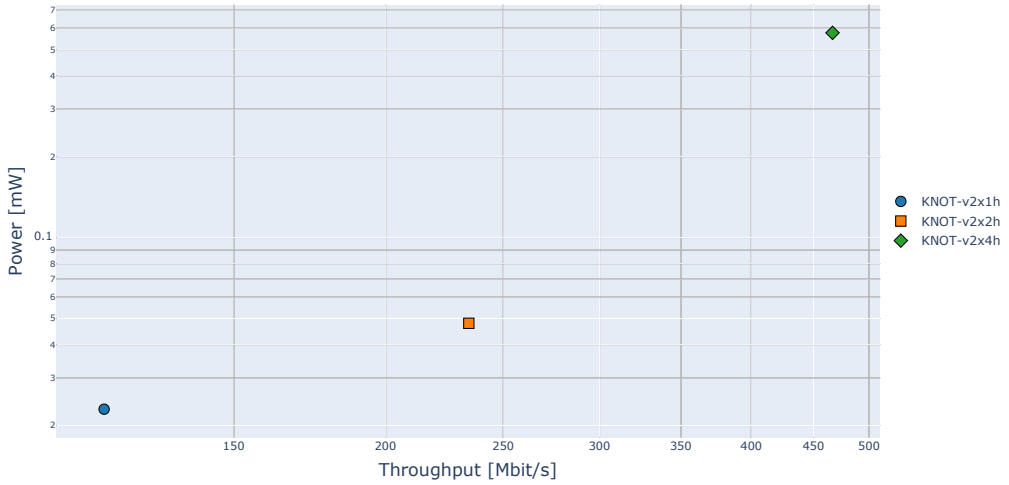

Figure 103: Design-space exploration of KNOT variants for hashing long messages: Power vs. Throughput

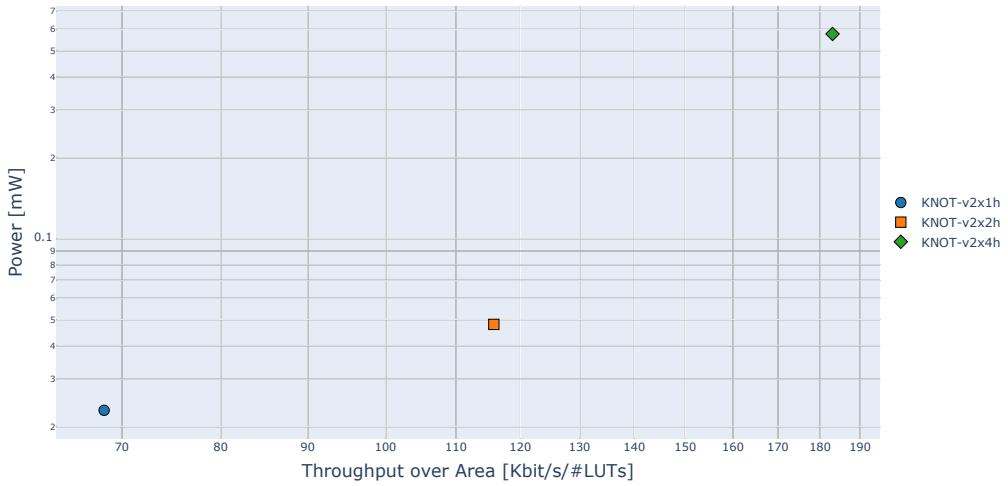

Figure 104: Design-space exploration of KNOT variants for hashing long messages: Power vs. Throughput-over-Area

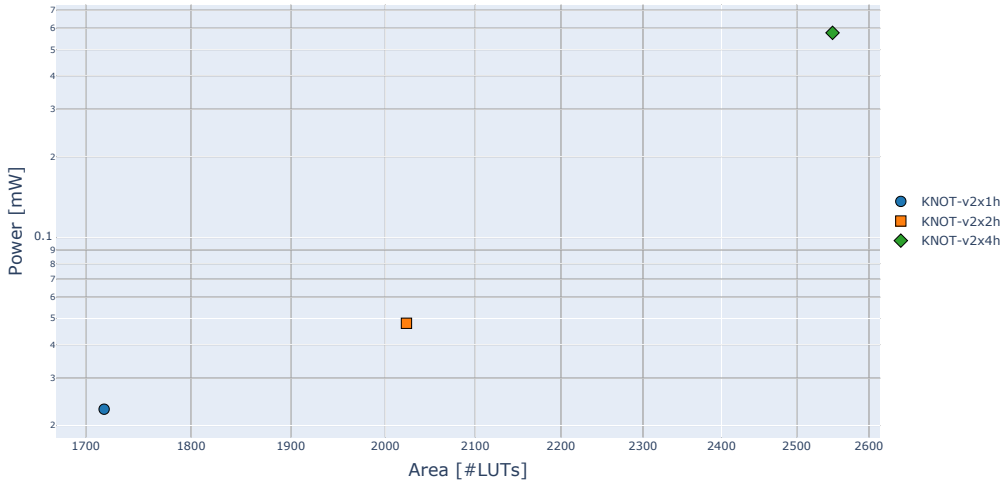

Figure 105: Design-space exploration of KNOT variants for hashing long messages: Power vs. Area

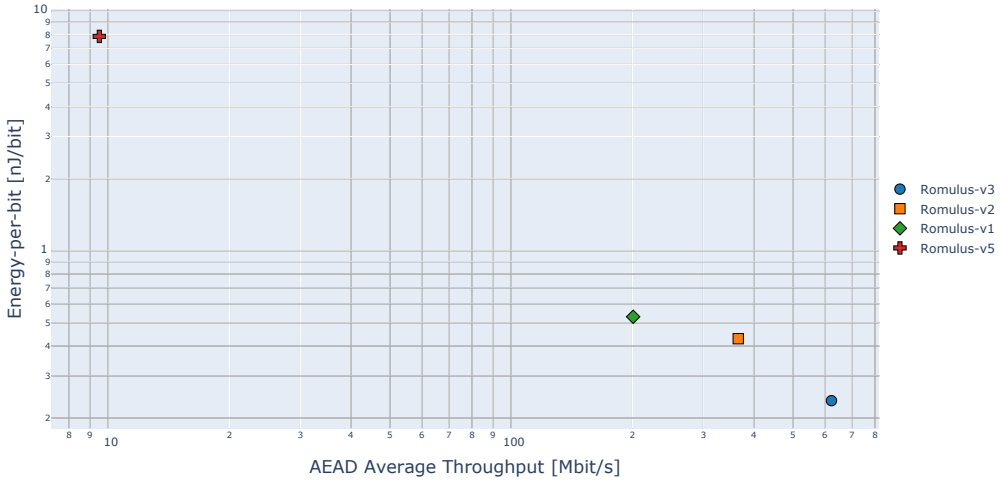

Figure 106: Design-space exploration of Romulus variants for AEAD of long messages: Energy-per-bit vs. Throughput

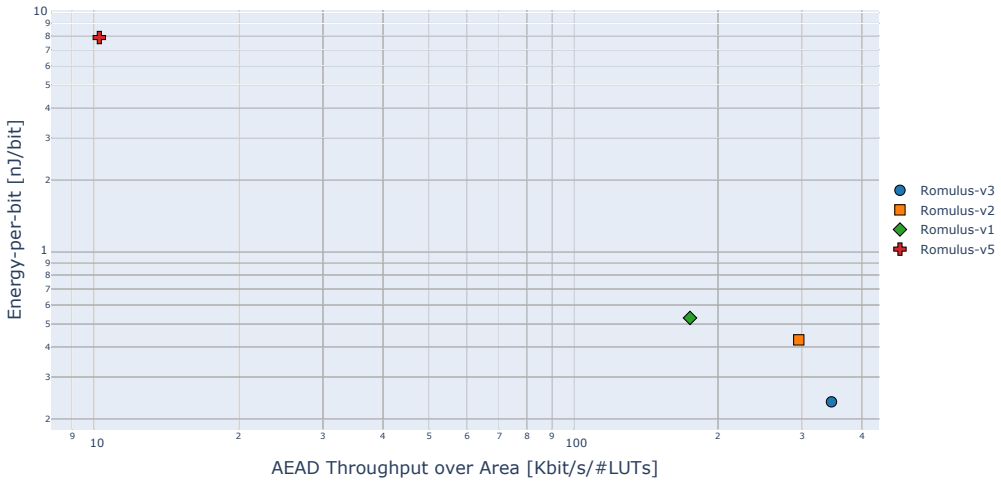

Figure 107: Design-space exploration of Romulus variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

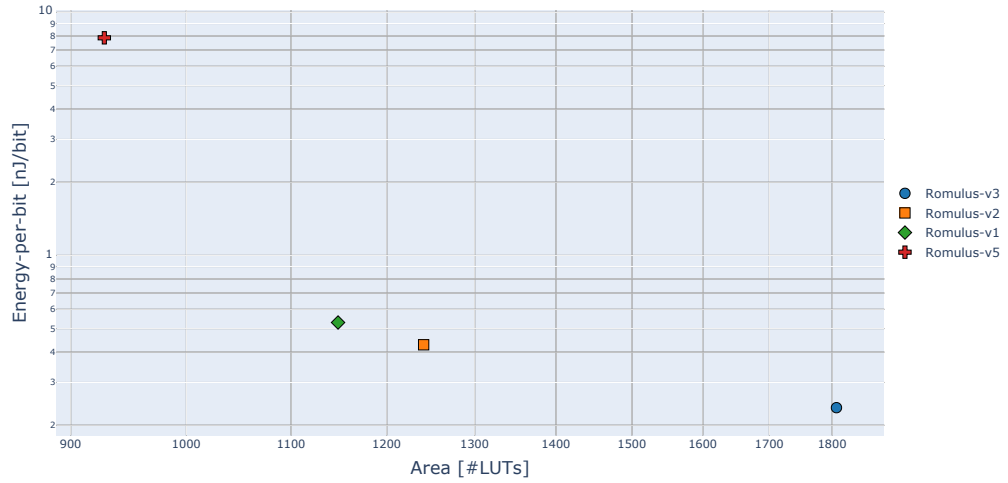

Figure 108: Design-space exploration of Romulus variants for AEAD of long messages: Energy-per-bit vs. Area

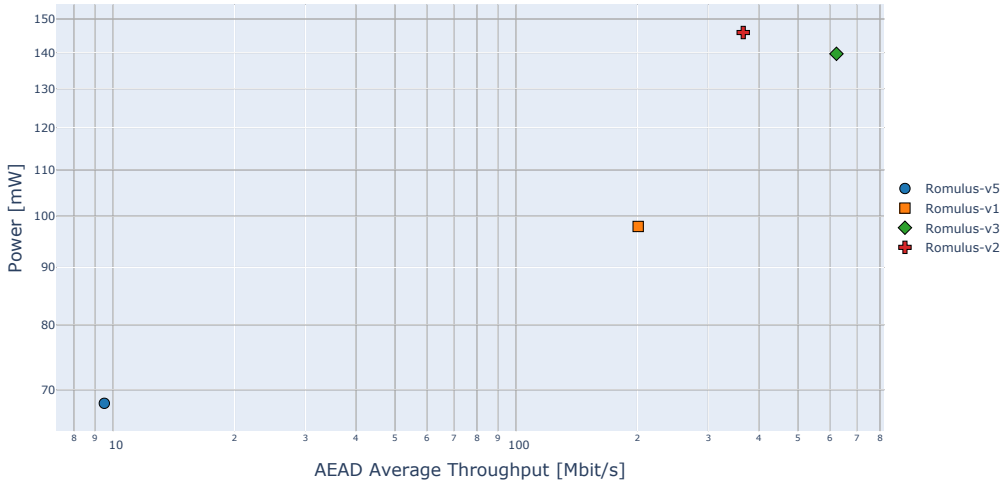

Figure 109: Design-space exploration of Romulus variants for AEAD of long messages: Power vs. Throughput

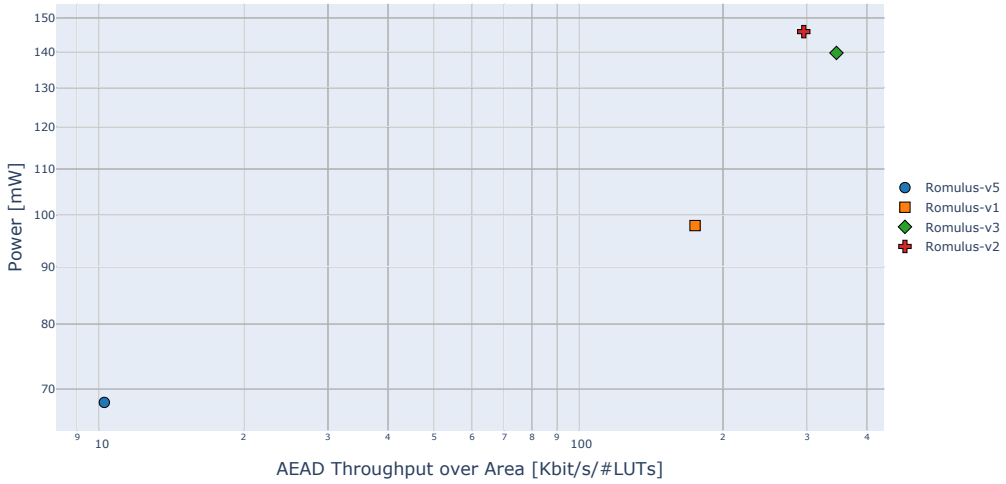

Figure 110: Design-space exploration of Romulus variants for AEAD of long messages: Power vs. Throughput-over-Area

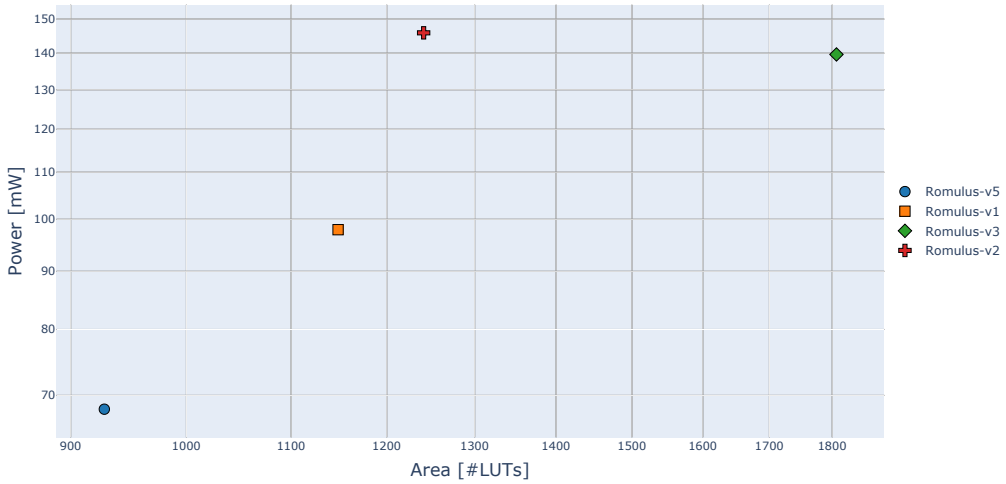

Figure 111: Design-space exploration of Romulus variants for AEAD of long messages: Power vs. Area

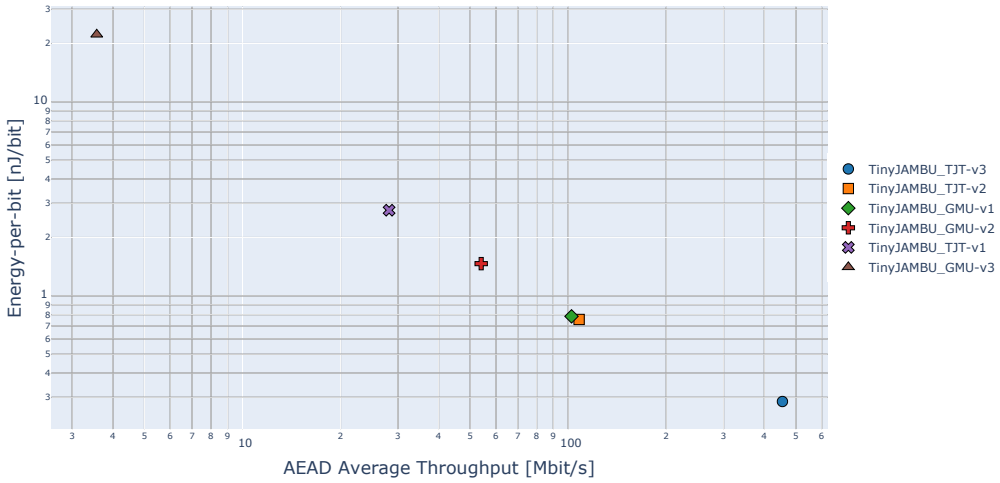

Figure 112: Design-space exploration of TinyJAMBU variants for AEAD of long messages: Energy-per-bit vs. Throughput

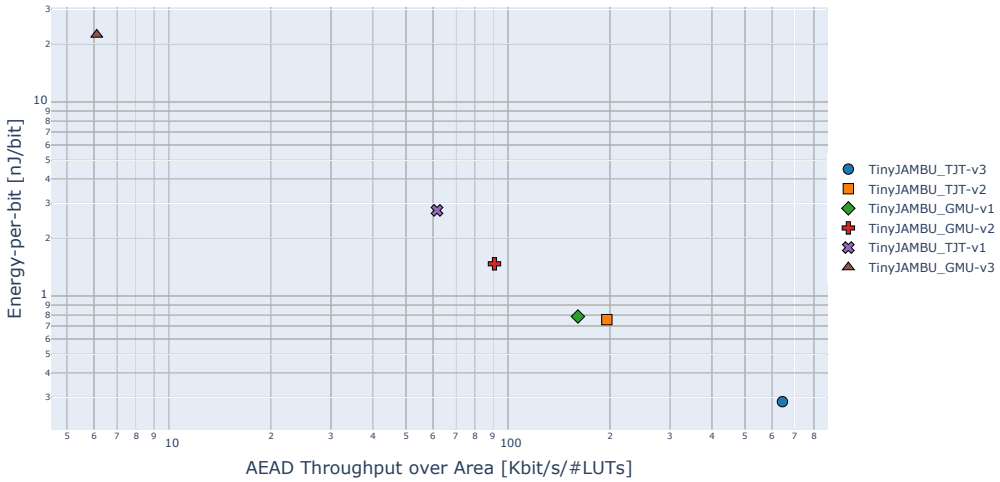

Figure 113: Design-space exploration of TinyJAMBU variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

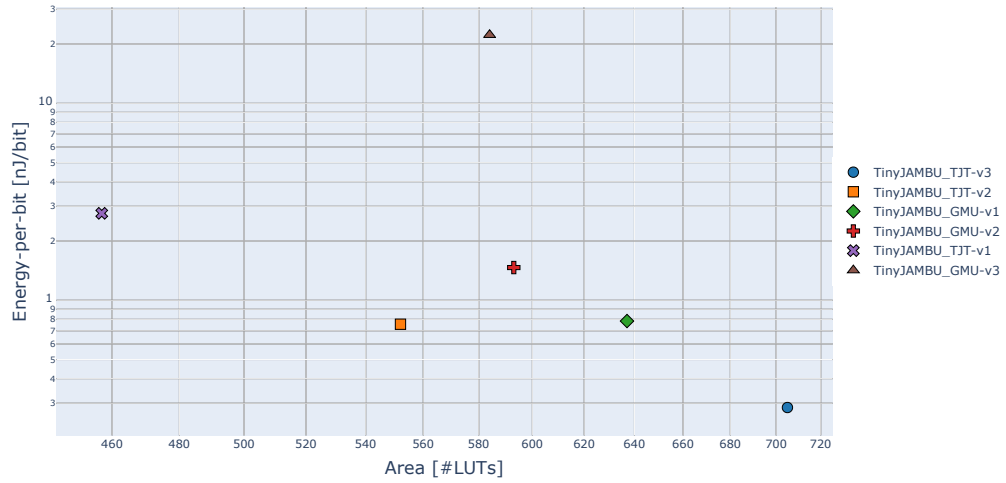

Figure 114: Design-space exploration of TinyJAMBU variants for AEAD of long messages: Energy-per-bit vs. Area

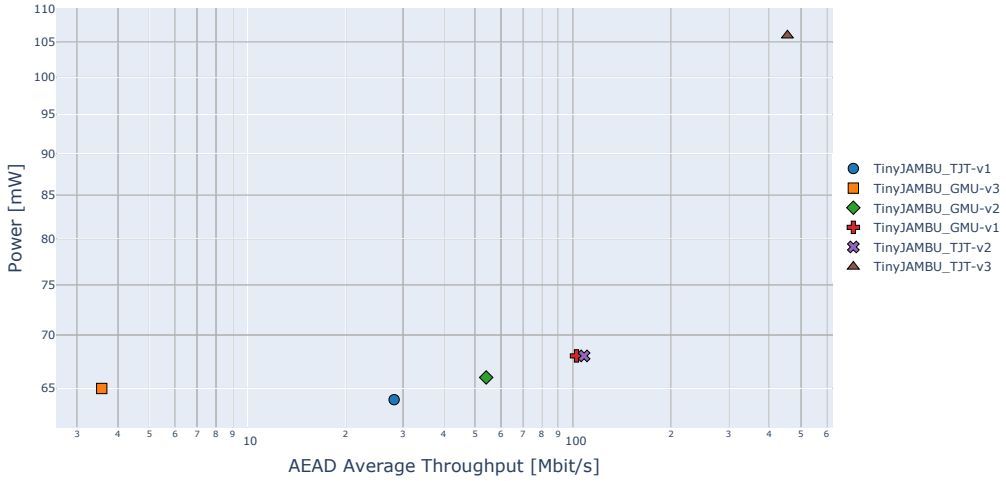

Figure 115: Design-space exploration of TinyJAMBU variants for AEAD of long messages: Power vs. Throughput

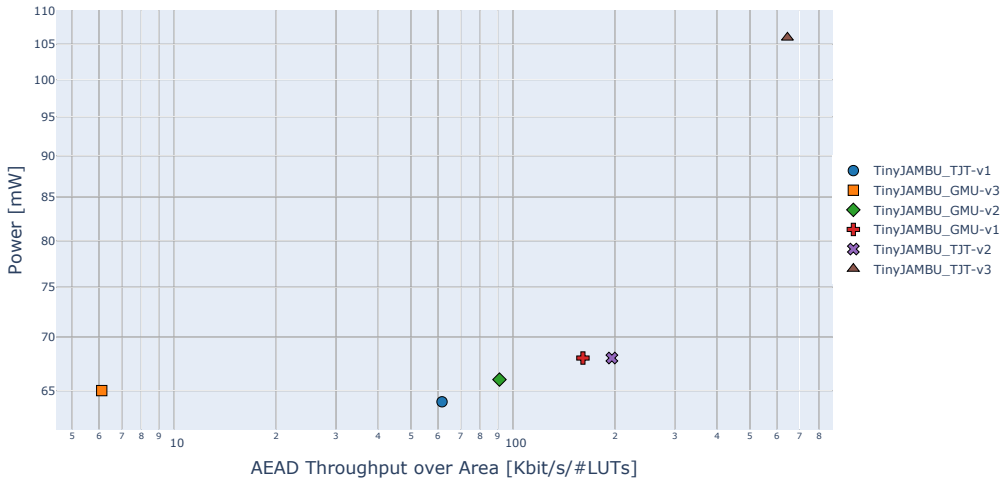

Figure 116: Design-space exploration of TinyJAMBU variants for AEAD of long messages: Power vs. Throughput-over-Area

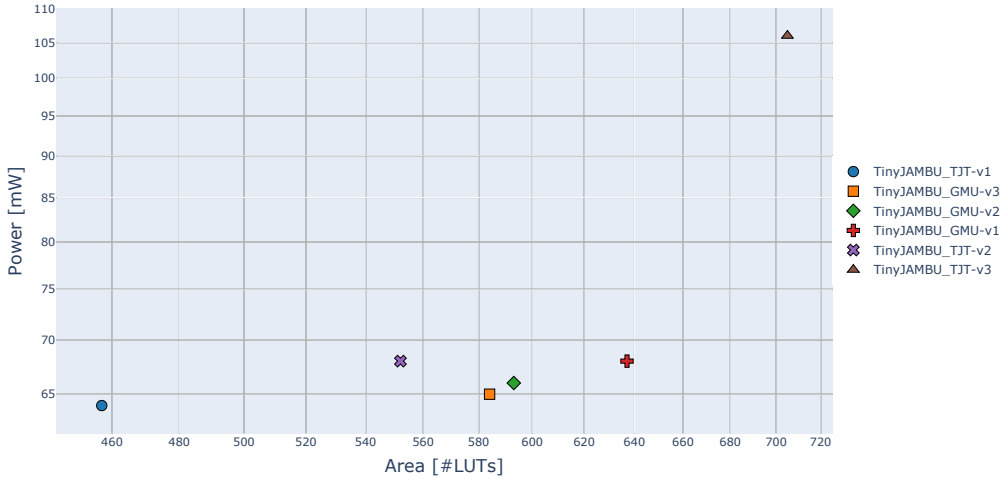

Figure 117: Design-space exploration of TinyJAMBU variants for AEAD of long messages: Power vs. Area

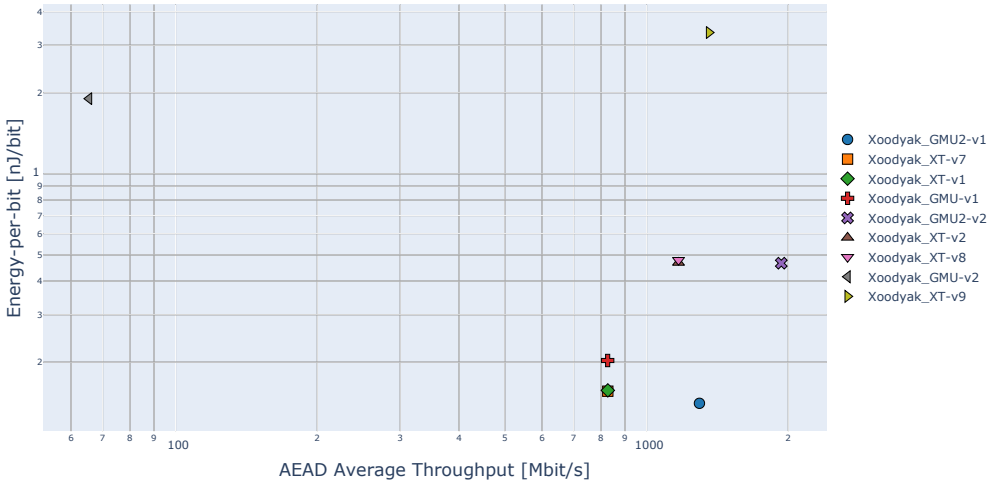

Figure 118: Design-space exploration of Xoodyak variants for AEAD of long messages: Energy-per-bit vs. Throughput

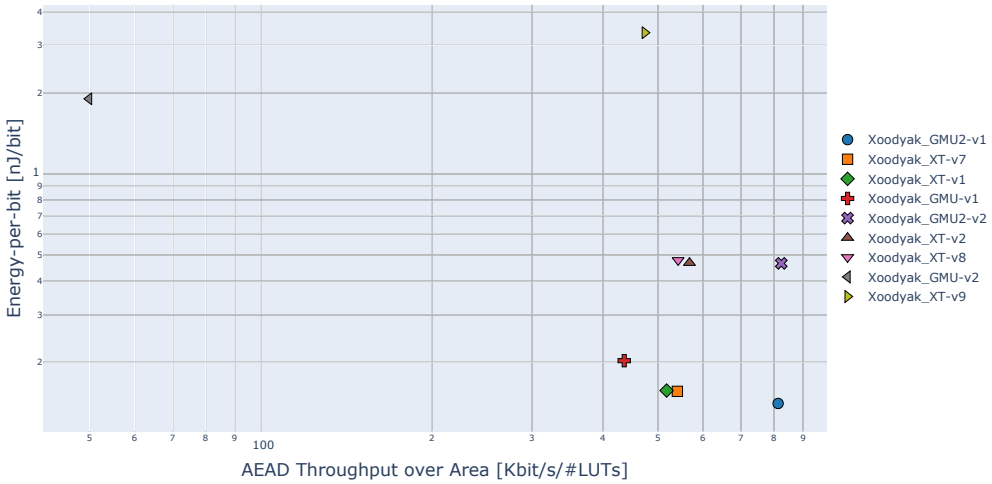

Figure 119: Design-space exploration of Xoodyak variants for AEAD of long messages: Energy-per-bit vs. Throughput-over-Area

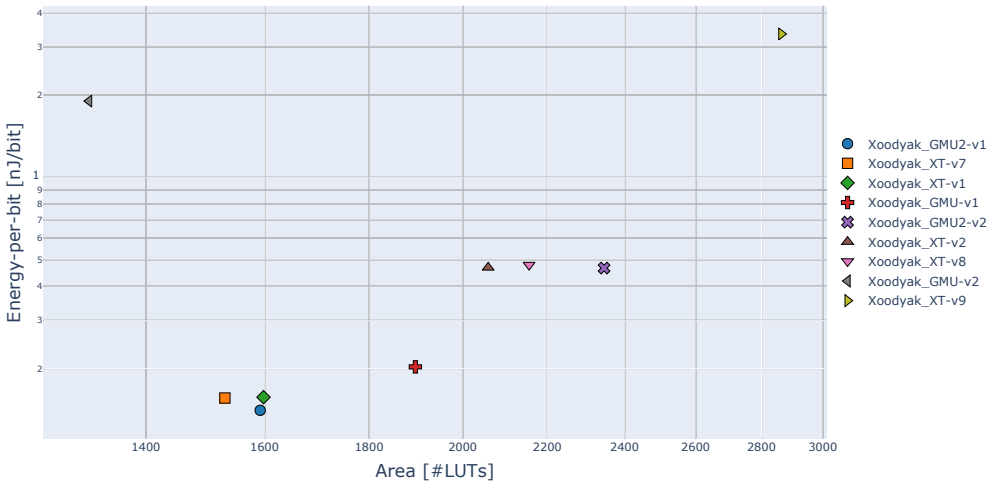

Figure 120: Design-space exploration of Xoodyak variants for AEAD of long messages: Energy-per-bit vs. Area

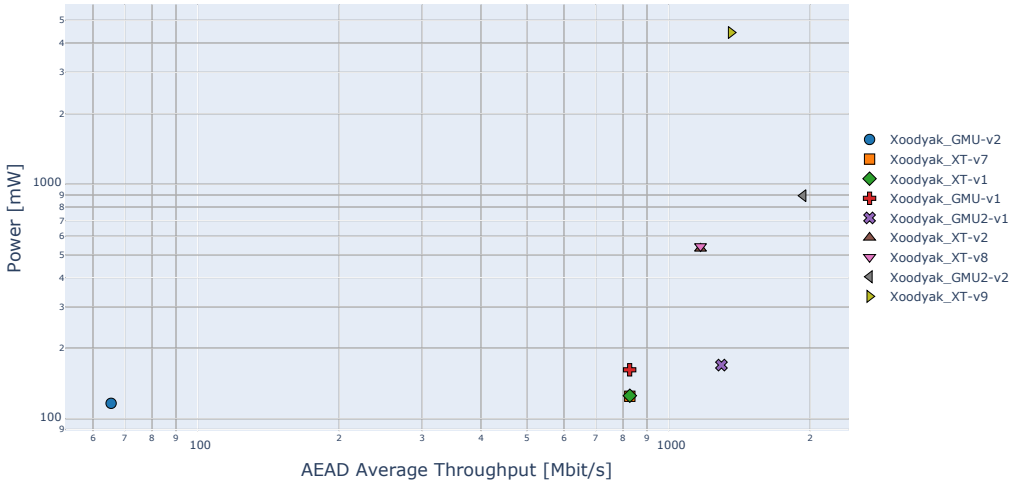

Figure 121: Design-space exploration of Xoodyak variants for AEAD of long messages: Power vs. Throughput

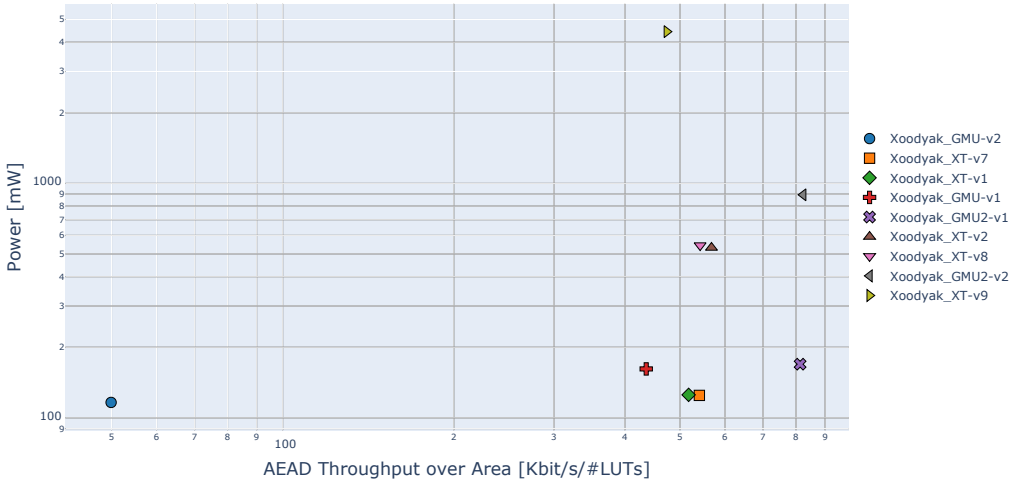

Figure 122: Design-space exploration of Xoodyak variants for AEAD of long messages: Power vs. Throughput-over-Area

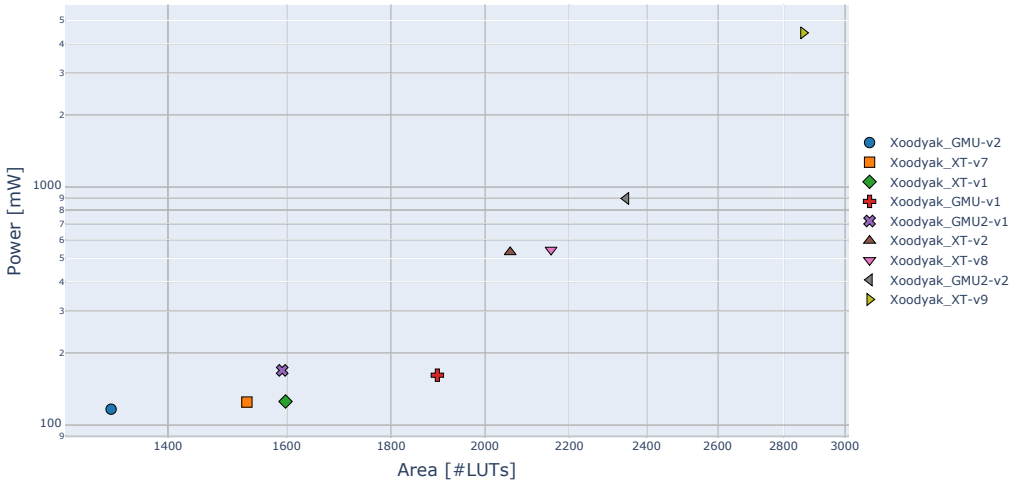

Figure 123: Design-space exploration of Xoodyak variants for AEAD of long messages: Power vs. Area

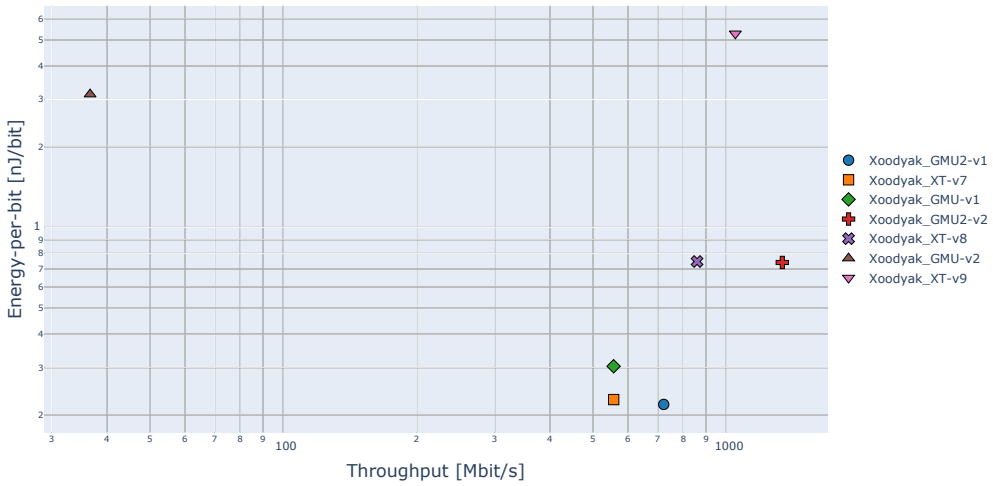

Figure 124: Design-space exploration of Xoodyak variants for hashing of long messages: Energy-per-bit vs. Throughput

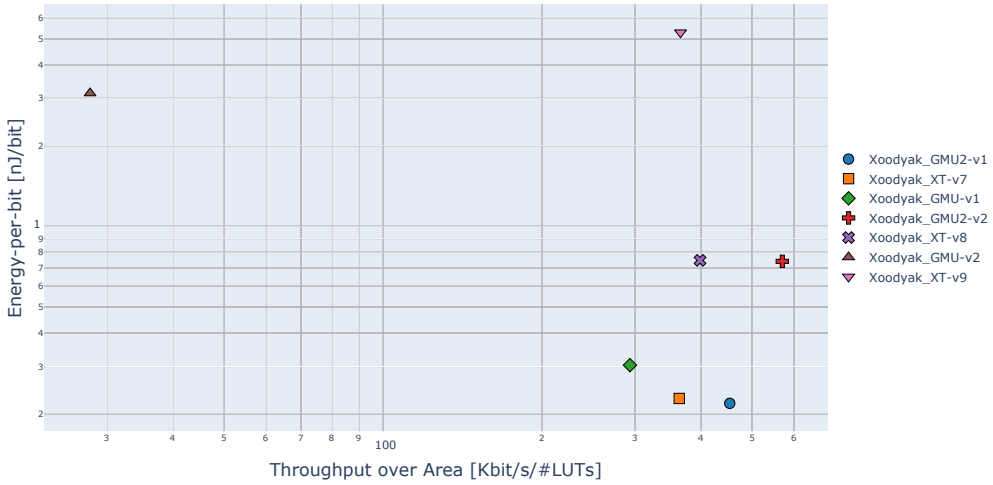

Figure 125: Design-space exploration of Xoodyak variants for hashing of long messages: Energy-per-bit vs. Throughput-over-Area

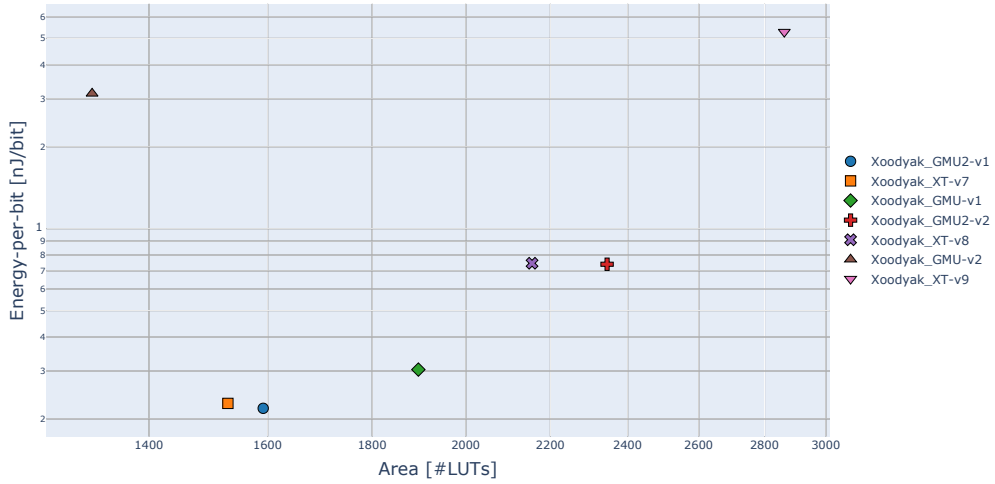

Figure 126: Design-space exploration of Xoodyak variants for hashing of long messages: Energy-per-bit vs. Area

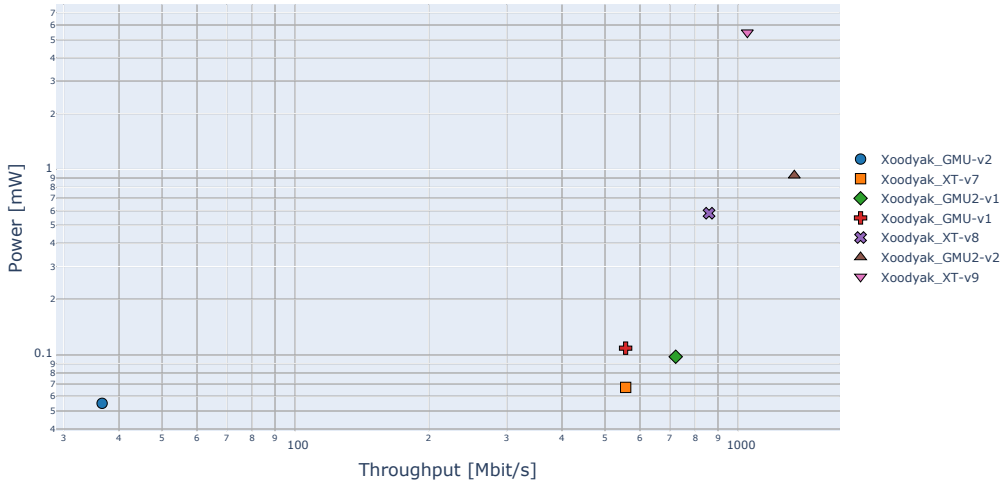

Figure 127: Design-space exploration of Xoodyak variants for hashing long messages: Power vs. Throughput

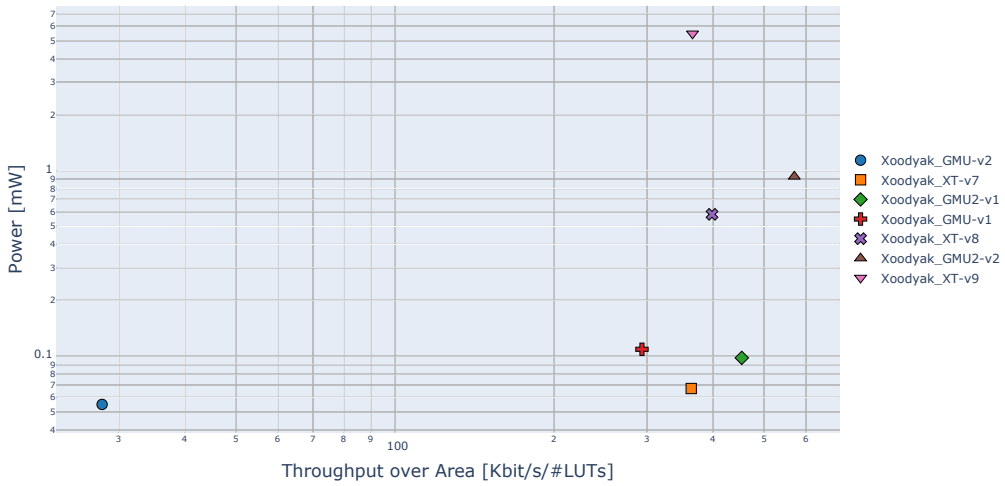

Figure 128: Design-space exploration of Xoodyak variants for hashing long messages: Power vs. Throughput-over-Area

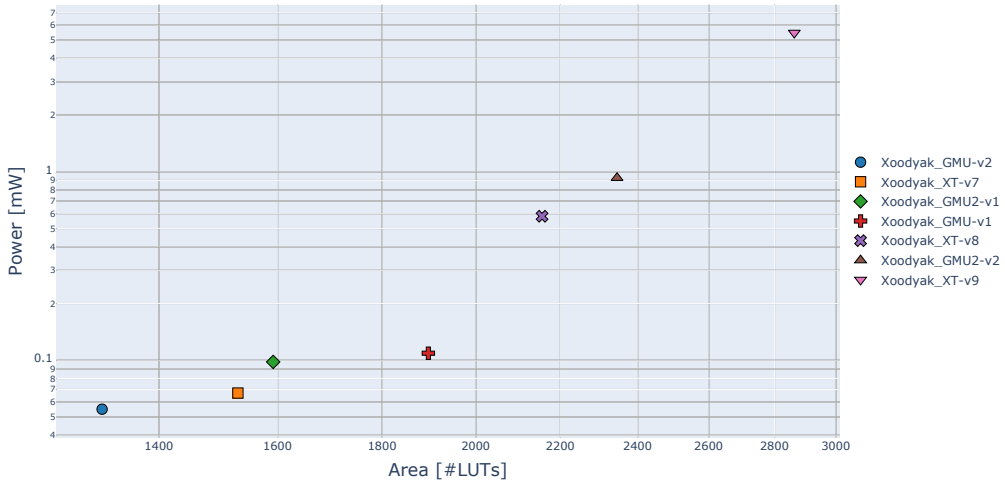

Figure 129: Design-space exploration of Xoodyak variants for hashing long messages: Power vs. Area

C List of Tables and Figures

Table 73: List of Tables included in Appendix A

Metric	Artix-7	Cyclone 10 LP	ECP5
Resource Usage and Maximum Frequency	Table 22	Table 23	Table 24
PT Throughput for Long Messages	Table 25	Table 29	Table 33
AD Throughput for Long Messages	Table 26	Table 30	Table 34
AD+PT Throughput for Long Messages	Table 27	Table 31	Table 35
Hash Throughput for Long Messages	Table 28	Table 32	Table 36
PT Throughput for 1536 Byte Messages	Table 37	Table 49	Table 61
PT Throughput for 64 Byte Messages	Table 38	Table 50	Table 62
PT Throughput for 16 Byte Messages	Table 39	Table 51	Table 63
AD Throughput for 1536 Byte Messages	Table 40	Table 52	Table 64
AD Throughput for 64 Byte Messages	Table 41	Table 53	Table 65
AD Throughput for 16 Byte Messages	Table 42	Table 54	Table 66
AD+PT Throughput for 1536 Byte Messages	Table 43	Table 55	Table 67
AD+PT Throughput for 64 Byte Messages	Table 44	Table 56	Table 68
AD+PT Throughput for 16 Byte Messages	Table 45	Table 57	Table 69
Hash Throughput for 1536 Byte Messages	Table 46	Table 58	Table 70
Hash Throughput for 64 Byte Messages	Table 47	Table 59	Table 71
Hash Throughput for 16 Byte Messages	Table 48	Table 60	Table 72

Table 74: List of Figures included in Section 5

Metric	Artix-7	Cyclone 10 LP	ECP5
PT Throughput for Long Messages vs. Area	Figure 2	Figure 6	Figure 10
AD Throughput for Long Messages vs. Area	Figure 3	Figure 7	Figure 11
AD+PT Throughput for Long Messages vs. Area	Figure 4	Figure 8	Figure 12
Hash Throughput for Long Messages vs. Area	Figure 5	Figure 9	Figure 13

Changelog

1.0.0 (September 26, 2020) — First version of the paper published

1.0.1 (September 29, 2020)

Fixed

- Table 1: HDL of SpoC changed from VHDL to Verilog (CryptoCore)
  REASON: Mistake in the original version

Added

- Section 5.3: DryGASCON added to the list of algorithms that rank higher for short messages than for long messages
  REASON: Omission in the original version

1.0.2 (September 30, 2020)

Changed

- Table 2: Max Length [bytes] for Spook-v1 changed from $2^{16} - 1$ to unlimited
  REASON: Correction by the Spook Team

Removed

- Section 4: "The designers of Spook-v1 declared the maximum length as unlimited from the implementation point of view, but constrained to $2^{16} - 1$ due to the security bounds derived in [1]."
  REASON: Correction by the Spook Team

1.0.3 (October 2, 2020)

Changed

- Spook-v1 replaced by Spook-v2-v1
  REASON: v2 indicates a new version of the Spook algorithm announced on March 15, 2020

Added

- Figures 6 to 8 and Tables 4, 5, 12 to 14, 23, 29 to 31 and 49 to 57: Added results for ISAP-v2 on Cyclone 10 LP
  REASON: Miscommunication regarding the source list for ISAP-v2

1.0.4 (October 4, 2020)

Removed

- Section 3.6: WAGE removed from the list of algorithms that did not pass all tests.
  REASON: Miscommunication regarding the version of reference software implementation to be used for generating test vectors

1.0.5 (October 23, 2020)

Added

- New hardware design submissions: Gimli_GT (12 variants), Saturnin (2 variants), and TinyJAMBU_TJT (3 variants). The previous submissions renamed: Gimli to Gimli_TUM and TinyJAMBU to TinyJAMBU_GMU.
  REASON: Phase 2 Submissions

- New variants: Romulus-v5 and Oribatida-v2.
  Reason: Phase 2 Submissions
- New design-space exploration diagrams for Gimli and TinyJAMBU.
  Reason: Phase 2 Submissions
- Average, minimum, and maximum values added in Tables 22-51.
  Reason: Additional information helpful in analysis of results

Changed

- The fully-debugged code submitted for ESTATE and SpoC. Improved code submitted for LOCUS-v1.
  Reason: Phase 2 Submissions
- Listing of results in the ranking by throughput tables limited to the best two per hardware design submission.
  Reason: Attempt to limit each result table to one page.
- Section 1 Introduction is split into two sections: Section 1: Introduction and Section 2: Previous Work.
  Reason: Improve readability.

1.0.6 (October 25, 2020)

Fixed

- Added missing hashing throughput results for SCHWAEMM-v2 in Figures 9 and 13
  Reason: Results were missing due to a bug in the table and figure generation script.

1.0.7 (December 23, 2020)

Added

- New hardware design submissions: ACE (1 variant), ForkAE (2 variants), mixFeed (1 variant), and Xoodyak_GMU2 (2 variants).
  Reason: Phase 3 Submissions
- New variants replacing previous variants: KNOT (16 new variants replacing previous 4 variants). New variants added on top of previous variants: COMET_CI-v3, LOCUS-v2, and LOTUS-v2.
  Reason: Phase 3 Submissions
- Results reported for the implementations of the current standards: AES-GCM (2 variants), SHA-2 (SHA-256, 1 variant), and SHA-3 (SHA3-256, 1 variant).
  Reason: The first attempt at the comparison with the current standards
- New sections: 4.1 Implementations of current standards, 6 Conclusions and Future Work.
  Reason: The first attempt at comparison with the current standards. Conclusions from Phases 1-3.

Changed

- The fully-debugged code submitted for COMET_VT-v1. Improved code submitted for Gimli (7 new variants replacing previous variants with the same names), Spook-v2-v2 (replacing Spook-v2-v1), and Subterranean-v2 (replacing Subterranean-v2)
  Reason: Phase 3 Submissions

- Revised space-exploration graphs for COMET, Gimli, KNOT, and Xoodyak.
  Reason: Phase 3 Submissions
- Revised sections: 4 Hardware Designs, 5 Results and Their Analysis, Appendix A Additional Results
  Reason: Phase 3 Submissions. Comparison with the current standards.

1.0.7 (February 15, 2021)

Added

- New Section 6, titled Power and Energy Evaluation
  Reason: Extended evaluation using different performance metrics
- New Appendix B, titled Power and Energy Design-space Exploration
  Reason: Extended evaluation using different performance metrics
- New hardware design submissions: ACE_GMU (1 variant), Ascon_GMU (2 variants), Ascon_GMU2 (3 variants), GIFT-COFB_GMU (6 variants), Gimli_GMU (4 variants), SKINNY-AEAD (2 variants), SPIX (2 variants), and Subterranean_GMU (1 variant).
  Reason: Phase 4 Submissions
- New variants added on top of previous variants: ISAP (v3 and v4), Elephant (v3–v5)
  Reason: Phase 4 Submissions
- Added new tables: Table 7: FPGA Rankings based on Hash Throughput for Long Messages and Table 11: Xilinx Artix-7 Hash Throughput Rankings.
  Reason: Extended analysis

Changed

- Previous Section 5, renamed from Results and Their Analysis to Throughput and Area Analysis
  Reason: Extended evaluation using different performance metrics added in Section 6 and Appendix B
- New variants replacing previous variants: Ascon_Graz (6 new variants replacing previous 2 variants), mixFeed (1 variant), Saturnin (2 variants), Xoodyak_XT (12 variants).
  Reason: Phase 4 Submissions
- Corrected numbers of clock cycles for some variants of KNOT
  Reason: The use of incorrect test vectors in previous timing measurements
- Modified names of the following designs due to the submission of a new design package for the same candidate: ACE changed to ACE_UW, GIFT-COFB changed to GIFT-COFB_VT, Subterranean changed to Subterranean_ST.
  Reason: Phase 4 Submissions
- Modified space exploration graphs for Ascon, Gimli, and Xoodyak in Section 5.2.3 Initial Design Space Explorations
  Reason: Phase 4 Submissions

1.0.7 (February 24, 2021)

Added

- New energy-per-bit and power results for TinyJAMBU_TJT-v2 and TinyJAMBU_TJT-v3, significantly improving TinyJAMBU positions in the energy-per-bit rankings
  Reason: Minor revisions required in the source code

- A new hardware design submission: SpoC_IIT (1 variant)
  Reason: A Phase 4 Submission. First submission supporting SpoC-128.
- New variants added on top of previous variants: SPIX-v2x2 and SPIX-v2x4
  Reason: Phase 4 Submissions. Variants superior in terms of energy per bit.
- Table of contents at the beginning of the report
  Reason: Ease of access to all sections
- New Appendix C: List of Tables and Figures, with a tabular representation of selected tables and figures
  Reason: Ease of access to all tables and graphs.

Changed

- Introduced consistent symbols representing each candidate in all two-dimensional graphs other than the space exploration graphs
  Reason: Increased readability of graphs
- Moved all tables containing detailed results from Section 5 to Appendix A
  Reason: Grouping all detailed results in a single appendix. Large sizes of tables.
- Removed the limitation according to which only the best two variants per each hardware design submission were included in the majority of result tables in Appendix A
  Reason: Completeness. Potential for extended analysis.