SECURE-IC
THE SECURITY SCIENCE COMPANY

Side Channel Analysis of Xoodyak LWC NIST candidate

Secure-IC Security Science Factory
September 16^{th}, 2022
– Version 1.0 –

Contributor	Position
François FORLOT	Security Evaluation Engineer, Secure-IC
Nassim RIADI	R&D Engineer, Secure-IC
Khaled KARRAY	Threat Analysis Busines Line Director, Secure-IC
Sylvain GUILLEY	Chief Technical Officer (CTO), Secure-IC

Table 1: Contributors

Contents

Abstract

This report is part of the NIST lightweight cryptography algorithms standardization project. It presents the results of side channel analysis performed by Secure-IC Security Science Factory (SSF) team of the first order protected Xoodyak algorithm implemented by Cryptographic Engineering Research Group (CERG). The analyzed implementation was recovered from the public github repository of the CERG and was implemented on the Arty A7 (FPGA: Xilinx Artix 7, 100 Mhz) board and interfaced with the ANALYZR post-silicon side-channel and fault injection analysis tool [3]. The results show that up to 100k traces no leakages were detected using Ttest metrics and following ISO-17825 analysis methodology.

1 Target of evaluation

The target under analysis is the first order protected Xoodyak light weight algorithm implemented by the Cryptographic Engineering Research Group (CERG). Table 2 is a summary of the target under evaluation.

Algorithm	**Xoodyak**
Implementation	**Cryptographic Engineering Research Group (CERG)**
Variant	**Masked first order**
source code	https://github.com/GMUCERG/Xoodyak-SCA
protection method	**Domain Oriented Masking (DOM)**
Target board	**Arty A7 (FPGA: Xilinx Artix 7, 100 Mhz)**

Table 2: Target information summary.

2 Traces Acquisition framework and conditions

2.1 Evaluation bench

The evaluation bench used for the traces acquisition and analysis is showed in Figure 1. It is composed of a control PC with the ANALYZR solution [2, 3] that controls the target Arty A7 (FPGA: Xilinx Artix 7, 100 Mhz) as well as the oscilloscope. A UART-based communication between the target board and the control PC was implemented in order for the ANALYZR tool to send the cryptographic parameters (SDI, PDI, ..) to the be board to be processed. The result of the authenticated encryption is also recovered by the ANALYZR at the end of each cyrptogrpahic operation. In order to synchronize the traces and facilitate the vertical analysis a synchronisation trigger was added to the target (implemented outside the boundary of the cryptographic operation to be analysed) so as not to add any modification to the target of evaluation.

2.2 Bench configuration

- Osciloscope: **Tektronix MSO64**
- Osciloscope configuration: **6.25 GSa/s, 500Mhz bandwidth 12 bits resolution**
- Number of traces: **100 000 traces**
- Number of samples: **1 000 samples per trace**
- Trigger: **The trigger is synchronised with the beginning of the execution**
- Amplifier: **Langer PA 303 SMA Preamplifier 100 kHz up to 3 GHz**
- Probe type: **Langer RF-K 7-4 near-field probe, 30 Mhz to 3 Ghz bandwidth**

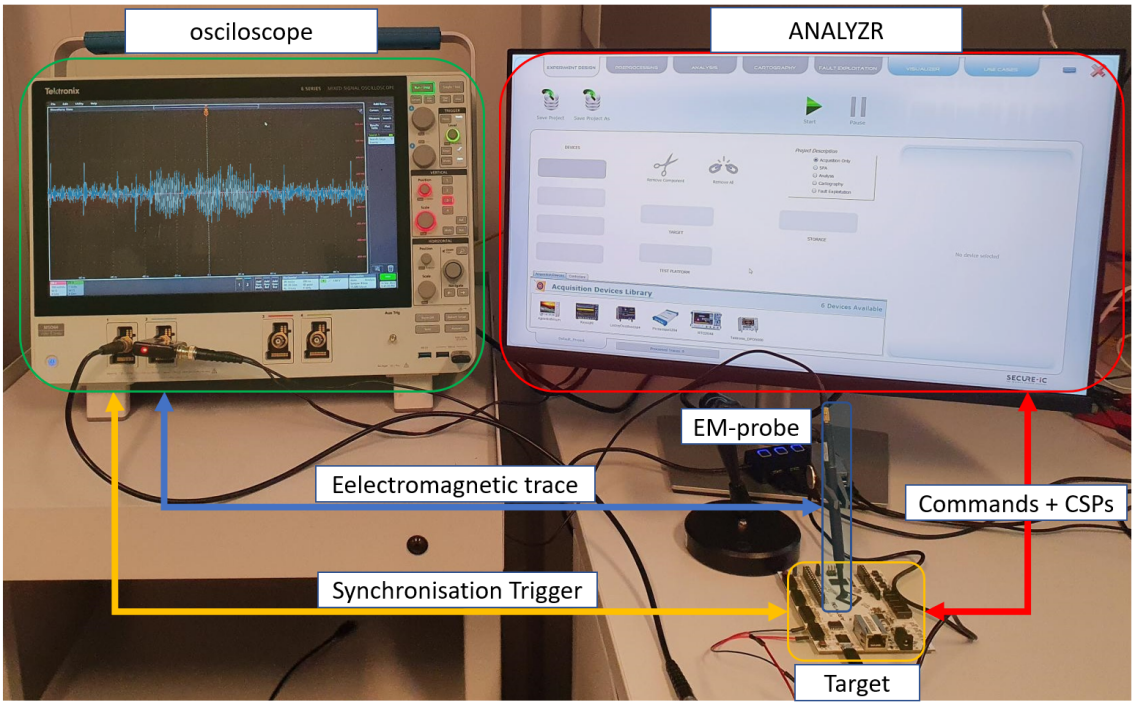

Figure 1: ANALYZR post-silicon side channel analysis bench

3 Leakage Assessment Methodology

100 000 traces are acquired from the setup, and are evaluated used the Welch's T-test [4]. The key for the encryption is fixed, the other parameters are variable. Figure 2 shows the execution of Xoodyak for the tested implementation.

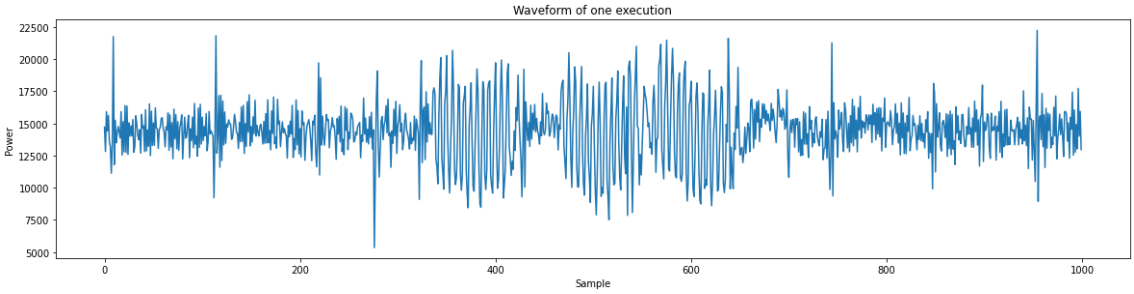

Figure 2: Trace of Xoodyak execution

From the side-channel trace of fig. 2 the Xoodoo permutation appears three times. Each Xoodoo pattern is composed of 12 rounds clearly identifiable on the Electromagnetic side-channel trace.

Following the ISO-17825 [1] recommendation, the evaluation will use the t-statistic. This preliminary analyses targets the plaintext. The traces are classified relative to the value of a bit of the plaintext and the t-statistic is computed between the two resulting sub datasets. A threshold of 4.5 is used to detected potential side-channel leakages. This threshold corresponds to a confidence level of 99.999%. The analysis is then extended to all the variable bits.

4 Leakage Assessment Results

The T-test is done for each variable bit of the plaintext, Figure 3 shows the evaluation for the 6^{th} bit of the last byte, chosen arbitrarily.

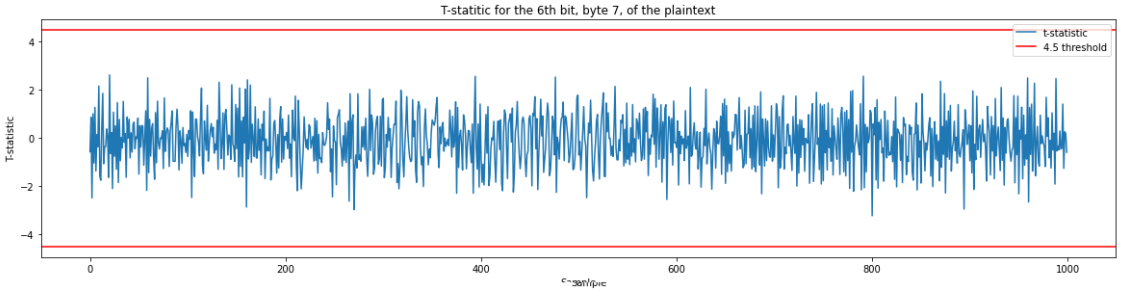

Figure 3: T-Test for one bit of plaintext

No Value exceeds the threshold of 4.5.

To extend to all the bits, see Figure 4. The shown data represents the maximum and the minimum t-statistic for each sample. To show the analysis on all bits of the plaintext,the t-statistics is the computed for each bit of the plaintext. The maximum (and the minimum) value of the t-statitics is then computed for each sample over all plaintext bits. The result is show in Figure 4. It show that the maximum t-statistics over all plaintext bit never exeeds the defined thresholds [-4.5:+4.5].

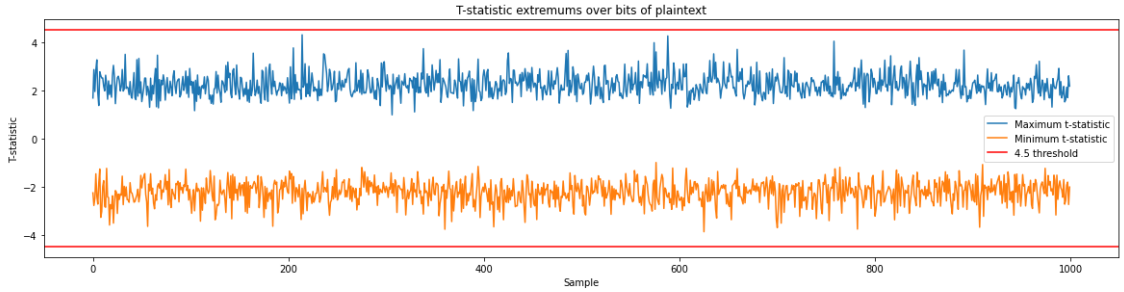

Figure 4: T-Test extremums for all bits of plaintext

In 100 000 traces of the given implementation, no t-statistic exceeds the 4.5 threshold for any of the bits.

References

[1] Information technology – Security techniques – Testing methods for the mitigation of non-invasive attack classes against cryptographic modules. Standard, International Organization for Standardization, Geneva, CH, 2016.

[2] Secure-IC. Cybersecurity evaluation tools. https://www.secure-ic.com/products/cybersecurity-evaluation-tools/, 2022.

[3] Secure-IC. Cybersecurity evaluation tools, post-silicon validation. https://www.secure-ic.com/products/cybersecurity-evaluation-tools/post-silicon-validation/, 2022.

[4] B. L. Welch. The generalization of 'student's'problem when several different population varlances are involved. *Biometrika*, 34(1-2):28–35, 1947.

CONTACT US

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

SECURE-IC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
ZAC des Champs Blancs
15, rue Claude Chappe
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 77 - contact@secure-ic.com