Comments

Nicolai Müller
Ruhr University Bochum, Horst Görtz Institute for IT Security, Germany
E-Mail: nicolai.mueller@rub.de

Amir Moradi
University of Cologne, Institute for Computer Science, Germany
E-Mail: amir.moradi@uni-koeln.de

September 16, 2022

1 Summary

This reply concerns the present report on `TinyJAMBU_first_order` by Abdulgadir et al. The authors have indicated that they have detected first-order leakage with the help of TVLA. We were able to reproduce the detected leakage with PROLEAD and fixed the issue. The updated version can be found on GitHub.

2 Changes

By analyzing the leaking points in time, it turns out that the leakage occurs if `rdi_ready` is set to zero, i.e. if the fresh masks are applied during multiple clock cycles. This is visualized in Figure 1.

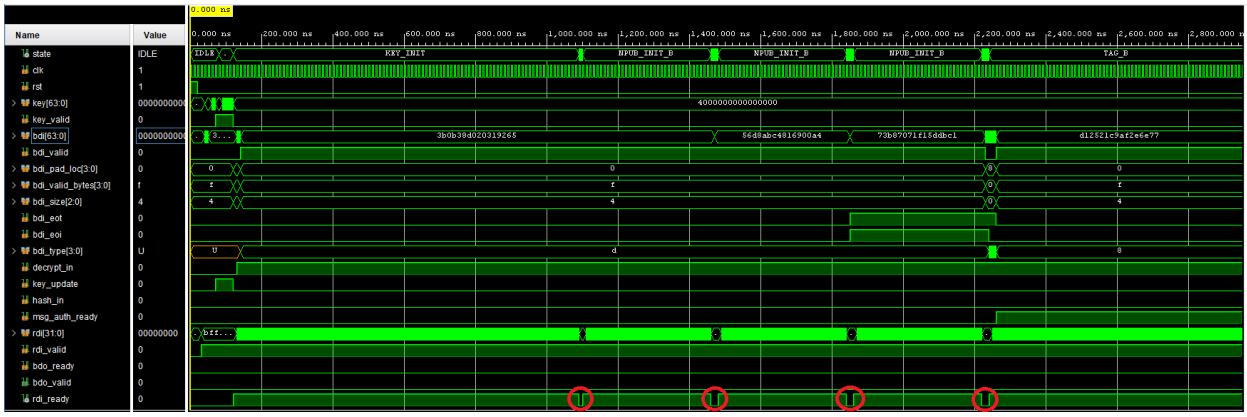

Figure 1: Simulation results of the leakging version encompassing the first key load and the first encryption procedure.

To fix the the implementation, we change the control logic in a way that `rdi_ready` is also set to one during the leakging points in time. In particular, the fresh masks are updated during every clock cycle.

3 Evaluation

We evaluate the robust probing security of the old and the new design, including the combined occurrence of glitches and transitions [1] by applying PROLEAD [4]. PROLEAD, a leakage detection tool publicly available at GitHub[1], performs logic simulations at the gate level and applies

[1] `https://github.com/ChairImpSec/PROLEAD`

statistical methods to evaluate the robust probing security of a circuit. For more information regarding PROLEAD, we refer to the PROLEAD wiki[2] and the original paper [4]. In short, we were able to reproduce the detected leakage for the old version. After updating the implementation, no leakage was detected. For more information, we refer to the additional report files.

[2] https://github.com/ChairImpSec/PROLEAD/wiki

References

[1] Faust, S., Grosso, V., Pozo, S. M. D., Paglialonga, C., and Standaert, F. Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. *IACR TCHES 2018*, 3 (2018), 89–120.

[2] Gigerl, B., Hadzic, V., Primas, R., Mangard, S., and Bloem, R. Coco: Co-Design and Co-Verification of Masked Software Implementations on CPUs. In *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021* (2021), USENIX Association, pp. 1469–1468.

[3] Gross, H., Mangard, S., and Korak, T. Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. In *TIS@CCS 2016* (2016), B. Bilgin, S. Nikova, and V. Rijmen, Eds., ACM, p. 3.

[4] Müller, N., and Moradi, A. PROLEAD - A Probing-Based Hardware Leakage Detection Tool. Cryptology ePrint Archive, Paper 2022/965, 2022. `https://eprint.iacr.org/2022/965`.