SIMPLE-Crypto Yearly Report

Researcher's Version, March 2023.

Foreword. This document is the annual report of the SIMPLE-Crypto association. As per the association's organization (see https://www.simple-crypto.org/organization), this report comes in three versions. The researcher's version describes progresses of year i-1 and lists potential plans (with a tentative time budget) for the next year. The post-workshop version is an update based on sponsor's feedback. The final version integrates the priorities determined by the scientific council.

1 SIMPLE-Crypto progresses

Following the conclusions of the 2022 sponsor's workshop, development efforts were oriented towards a hardware implementation of the AES masked at arbitrary security orders. We selected the Hardware Private Circuits (HPC) scheme for this purpose. It is a generic technique to protect cryptographic implementations against side-channel attacks thanks to masking (aka secret sharing), which provides state-of-the-art guarantees in terms of resistance against physical defaults (e.g., glitches) and composability [1]. The AES-HPC implementation package is a generic HDL code that describes a 32-bit hardware implementation of the AES protected with arbitrary number of shares [2]. This code project will move from "under development" to "under public evaluation" on the SIMPLE-Crypto website in the coming days. It will come with a detailed documentation and a succint preliminary evaluation report about which feedback is welcome. The instances of the AES-HPC with two shares will serve as a CHES 2023 challenge. The datasets of the challenge will remain open for continuous evaluation until final release, and possibly be extended towards more shares as the security level of our implementations becomes more tightly estimated.

In parallel, we progressed towards the development of theoretical and practical teaching/training material. As a first target, we aim to cover the basics of side-channel analysis and security evaluations. We aim to organize a training based on this material end of 2023 or early 2024.

2 Potential developments plans

Topics of potential interest identified by the SIMPLE-Crypto developers are listed next:

- *Masked hardware implementation of Ascon.* The NIST just selected Ascon in their effort towards standardizing a lightweight cryptography standard.[1] As part if its good implementation features, Ascon inherits from some leakage-resistance properties. In particular, it can offer strong ciphertext integrity in a leveled implementation context where only two calls to its permutation require strong side-channel protections [3]. A uniformly protected implementation could also be designed for contexts where strong confidentiality guarantees with leakage in decryption are needed. Such a project could in part leverage the AES-HPC project (e.g., re-use some gadgets) while also requiring Ascon-specific optimizations.

[1] https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon.

- *Side-channel protected implementations of CRYSTALS-Kyber or CRYSTALS-Dilithium.* The NIST selected CRYSTALS-Kyber and CRYSTALS-Dilithium as primary candidates for post-quantum encryption and signature in 2022.[2] There is already a vast literature witnessing the challenges in protecting such implementations, with a growing number of attack paths to consider, implying the need of increasingly expensive countermeasures. A natural though more prospective development project could analyze the state-of-the-art side-channel protected implementations of these algorithms. In view of the lower maturity of the topic, a possible preliminary goal (before the development of a full-fledged protected implementation) could be to benchmark the implementations in the literature coming with source code and restrict candidate approaches for protecting CRYSTALS-Kyber or CRYSTALS-Dilithium.

- *Extension of SCALib.* The continuous development of a library enabling worst-case side-channel security evaluations is a recurrent goal of the SIMPLE-Crypto association. The extension of SCALib towards more functionalities, with applicability to more targets, is therefore always in scope for internship topics. Examples include of improvements include optimization of the SNR and T-test computations, multivariate leakage detection, extension of soft analytical side-channel attacks and the modeling of large target intermediate values.

All three topics would be intended for internships of a few months (3 typically, up to 6 if needed).

We insist that this list of topics is at this stage preliminary. Concrete proposals of internships will be driven by available funding, sponsors' feedback and discussion with the scientific council.

References

[1] G. Cassiers, B. Grégoire, I. Levi, and F. Standaert, *Hardware private circuits: From trivial composition to full verification*, IEEE Trans. Computers, 70 (2021), pp. 1677–1690.

[2] C. Momin, G. Cassiers, and F. Standaert, *Handcrafting: Improving automated masking in hardware with manual optimizations*, in COSADE, vol. 13211 of Lecture Notes in Computer Science, Springer, 2022, pp. 257–275.

[3] C. Verhamme, G. Cassiers, and F. Standaert, *Analyzing the leakage resistance of the nist's lightweight crypto competition's finalists*, in CARDIS, vol. 13820 of Lecture Notes in Computer Science, Springer, 2022, pp. 290–308.

[2] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.