SIMPLE-Crypto Yearly Report

Final Version, January 2024.

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 contributors' 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 [2]. The SMAesH implementation package, which compiles our results, is a generic HDL code that describes a 32-bit hardware implementation of the AES protected with arbitrary number of shares [3].[1] This code project has moved from "under development" to "under public evaluation" on the SIMPLE-Crypto website. It comes with a detailed documentation and a succint preliminary evaluation report about which feedback is welcome. The instances of SMAesH with two shares serve as a CHES 2023 challenge.[2] 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 thanks to the challenge.

In parallel, we extended our evaluation library (SCALib) towards optimizations of the SNR and T-test computations, multivariate leakage detection and improved soft analytical side-channel attacks. We also 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 in 2024 (dates announced soon).

2 Potential developments plans

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

- *Extensions of the SMAesH implementation.* Towards decrytion & other architectures. Making a dataset using threee shares public could also be interesting for the community.
- *Masked hardware implementation of Ascon.* The NIST just selected Ascon in their effort towards standardizing a lightweight cryptography standard.[3] As part if its good implementation features, Ascon inherits from some leakage-resistance properties. In particular, it can

[1] https://www.simple-crypto.org/activities/smaesh/
[2] https://smaesh-challenge.simple-crypto.org/
[3] https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon.

offer strong ciphertext integrity in a leveled implementation context where only two calls to its permutation require strong side-channel protections [4]. 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.

More generally, moving from primitives like block ciphers (or permutations) to modes of operation is deemed useful by sponsors. An alternative to Ascon could be to integrate the masked AES in GCM version. But such standardized modes do not have nice features for leakage-resistance as Ascon does (and will therefore be less efficient).

- *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.[4] 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.

  Despite this topic does not directly fall in the association's main goals (i.e., it is still a topic of intense research and current solutions are unlikely to provide high security levels in a worst-case setting), sponsors suggest that developing reference implementations for training purposes only (i.e., with clear cautionary note that they are not aimed for practical use) should not always be excluded and the decision whether there is sufficient interest for this could be let to the appreciation of the scientific council. If full-fledge secure implementations of CRYSTALS-Kyber or CRYSTALS-Dilithium are too difficult based on current knowledge, developing pieces of it could be worthy. For example, a side-channel secure implementation of SHA3 (in software preferably, in hardware possibly) could be of interest as a first step.

- *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 further improvements of soft analytical side-channel attacks and the modeling of large target intermediate values. Another direction would be to include alignment tools (that are under-discussed in the literature).

- *Leakage-resistant mode of operation for embedded software with AES coprocessors.* Leakage-resistant modes of operation offer an alternative to masking in order to provide secure authenticated encryption in low-end (now-noise) embedded software microcontrollers. They deviate from standard modes of operation but benefit from good security with lower expertise [1]. Sponsors nevertheless show limited interest as long as such modes are not standardized.

- *Dual-rail logic styles* were mentioned as another topic of interest to be revisited based on our current understanding of masking, although it probably requires academic research first.

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

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

After discussion with the scientific council, it is concluded that two topics should be prioritized for internships in 2024 (given funding constraints). On the hardware implementation side, a masked implementation of Ascon, that could be the basis for a challenge in 2025, is suggested. It would directly match the association's goals and be a timely development. On the software implementation side, a masked implementation of CRYSTALS-Dilithium, consolidating the emerging literature on the topic, is suggested. While such an implementation will most likely not come with strong security guarantees in the worst-case evaluation setting promoted by the association, there is a consensus that it would be a useful ingredient to improve the community's understanding of the different side-channel attack paths against CRYSTALS-Dilithium. Eventually, it is suggested to maintain the SMAesH dataset and, in case of improved attacks, to extend it to more shares. Despite not prioritary, the extension of the SMAesH implementation towards more functionalities (e.g., decryption, 256-bit keys, shuffling) is listed as a useful project that we keep in reserve list.

References

[1] O. Bronchain, C. Momin, T. Peters, and F. Standaert, *Improved leakage-resistant authenticated encryption based on hardware AES coprocessors*, IACR Trans. Cryptogr. Hardw. Embed. Syst., 2021 (2021), pp. 641–676.

[2] 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.

[3] 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.

[4] 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.