SIMPLE-Crypto Yearly Report

Final Version, June 2025.

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. The post-workshop version is an update based on sponsor's feedback. It lists potential plans for the next year. The final version integrates the priorities determined by the scientific council.

1 SIMPLE-Crypto progresses

Following the conclusions of the 2023 sponsor's workshop, and given the limited resources of the association, development efforts were oriented towards extensions of the SMAesH implementation. We followed two tracks of improvements: first, optimizing the architecture, aiming for reduced area and increased throughput; second, extending the core's features. Regarding the core's performances improvement, we decided to integrate a new optimized S-box masked implementation from CHES 2024 [2], allowing us to reduce the overall area by at least 27% (this area gain increases with the masking order) and the latency by 19% (i.e., from 106 to 86 cycles). Regarding features extensions, we modified the core to support the three AES variants (i.e., handling 128, 192 and 256-bit key sizes), both in encryption and decryption, chosen dynamically at run-time. Besides, these modifications come with some adaptations of the core's API in order to support the storage of a (configurable) long-term key inside the core, re-used by sequential executions. The resulting package implementing these modifications was released under the version 2.0.0 of the SMAesH implementation, publicly available on the SMAesH's Github repository.[1] We leveraged this release to reorganize the latter in order to facilitate the handling of the IP, by adding a continuous integration flow that includes revised functional tests, formal tests, and HDL code linting.

We also organized the SCALE-I training in June 2024, which gathered 14 participants. The purpose of this training was to explain the theoretical background and the classical evaluation tools commonly encountered in the context of side-channel security evaluations (e.g., SNR, T-test, Template Attacks, ...). The training lasted 3 days, during which classical courses focusing on the theoretical parts were interleaved with practical sessions using an unprotected software AES implementation as practical case study. All the resources used during this training are publicly available, in the form of a book for the theoretical part, complemented by an exercise session in Python using the SCALib evaluation library developed by the association.[2,3]

In parallel, we extended the SCALib evaluation library towards the support of recent Python releases (e.g., Python 3.12) as well as improving the robustness of the existing belief propagation implementation (i.e., fixing numerical instabilities). We also progressed towards improving the user experience of the library by removing unnecessary parameters from initializers of common tools, therefore resulting in a breaking modification of the API starting with SCALib v0.6.0.

[1] See https://github.com/simple-crypto/SMAesH
[2] See https://perso.uclouvain.be/fstandae/book.html
[3] See https://github.com/simple-crypto/scale-one

2 Sponsor's workshop conclusions

Overall, the SCALE-I training organized in 2024 in Louvain-la-Neuve was appreciated by the sponsors. It was therefore suggested to re-organize it (in 2025) and to extend it to secure implementations (in 2026). Sponsors have been contacted in January 2025 with a training date.

The development of open source IP was also discussed with, as last year, a remaining gap between sponsors interested in this IP as relevant training material and sponsors interested in the IP for potential integration. It was observe that this gap is probably inherent to the goal of SIMPLE-Crypto to develop upon scientifically mature solutions. The latter may indeed create a phase delay with the market demand whenever there is a need to deploy before full scientific maturity, as we currently experience with post-quantum cryptography. As last year, it was concluded that this gap for now does not hurt SIMPLE-Crypto developments which, besides their interest as training material, may serve in product updates or be handy for some market players.

More precisely, we next list topics of interest identified during discussions:

- *SCALE-I.* Organization of a new edition of SCALE-I, covering the same subjects as the first edition, but revised to incorporate the feedback from the first edition. These modifications should include the revision of the training material in order to make exercises more accessible (e.g., by adding supporting slides and subdivide the exercises into simpler sub-steps). We also plan to clarify pre-requisites for practical part by announcing these in advance and pointing to useful resources. The target period is the end of May/beginning of June.

- *Fault-resistance.* While the subject is broad and currently lacks the scientific maturity of leakage-resistance, a first track could be to develop IPs with provable threshold fault security against DFA and basic injections into the control logic. It could directly lead to an extension of the existing SMAesH IP with sound countermeasures (and become a systematic addition to future developments). Security against other classes of attacks (e.g., SIFA) will not be considered at first due to the lack of accurate understanding. Besides, the development of setups, evaluation methodologies and training material, again focused on DFA and control faults is encouraged, as a natural starting point towards building expertise on the topic.

- *SCAlib extensions.* Adding more features to SCAlib such as efficient Correlation Power Analysis implementation would be interesting. Trace alignment techniques could also be implemented, but the choice of which techniques to implement is not as clear and depends on the existence of a "one-size-fits-most" algorithm which would be privileged.

- *SMAesH modes.*: A natural extension for the SMAesH IP is the support of common AES modes of operation, which would increase its interest in the integration of an industrial flow. Alternatively, an IP core for the recently standardized Ascon would fit similar requirements (but there does not seem to be a clear market demand in that direction for now).

- *Protected HW Keccak IP.* A masked hardware implementation of Keccak, to support efficient (protected) implementation of the recently standardized Kyber and Dilithium, would be interesting to have (and also be a starting point for the next item).

- *Protected SW Dilithium and Kyber*: Masked implementations of Kyber and Dilithium, targeted for embedded devices, remain among the sponsor's priorities. Despite not reaching the same scientific maturity as symmetric algorithms, they could be used as a common

ground to benchmark state-of-the-art attacks. It is agreed that releasing a masked implementation of Dilithium based on [1], or a masked implementation of Kyber based on https://github.com/uclcrypto/pqm4_masked could be useful steps in this direction.

We insist that this list of topics is at this stage preliminary. The concrete directions that will be privileged will be driven by available funding and discussion with the scientific council.

3 Scientific council's feedback

The scientific council deems all the potential developments listed above as valuable. The extension of the SCALE training towards countermeasures and the continuous development of the SCALib library are encouraged. For the latter, the addition of synchronization/alignment methods is confirmed as an interesting direction. When moving towards protected implementations, mutual information estimation tools and multivariate / high-order leakage detection tools could be interesting additions. As for priorities regarding the development of new IP blocks, the ones that look the most appealing given the philosophy of SIMPLE-Crypto are mature building blocks for post-quantum cryptography applications (e.g., hardware coprocessors for the NTT or masked Keccak). Baseline implementations of (masked) Kyber and Dilithium, despite not directly ensuring strong security guarantees (hence, seen more as research objects in order to stimulate research on the physical security evaluation of such algorithms) are recognized as useful as well.

4 Administrative updates

SIMPLE-Crypto's sponsorship levels remained the same for the last 3 years. As the association is based in Belgium, automatic salary indexation ideally requires to update these levels accordingly, which the sponsors agreed to do on a regular basis. We will apply a 20% increase for the last 3 years, applicable from 2025 for all sponsorship's not covered by a pre-established agreement.

References

[1] M. Azouaoui, O. Bronchain, G. Cassiers, C. Hoffmann, Y. Kuzovkova, J. Renes, T. Schneider, M. Schönauer, F. Standaert, and C. van Vredendaal, *Protecting dilithium against leakage revisited sensitivity analysis and improved implementations*, IACR Trans. Cryptogr. Hardw. Embed. Syst., 2023 (2023), pp. 58–79.

[2] G. Cassiers, B. Gigerl, S. Mangard, C. Momin, and R. Nagpal, *Compress: Generate small and fast masked pipelined circuits*, IACR Trans. Cryptogr. Hardw. Embed. Syst., 2024 (2024), pp. 500–529.