SIMPLE-Crypto Yearly Report

Post-workshop Version, November 2025.

Foreword. This document is the annual report of the SIMPLE-Crypto association. As per the association's organisation (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 (with a tentative time budget) for the next year. The final version integrates the priorities determined by the scientific council.

1 SIMPLE-Crypto progresses

Following the conclusions of the 2024 sponsor's workshop, and given the limited resources of the association, development efforts were oriented towards the organisation of a revised version of the SCALE-I training. The second edition took place from June 02 to 04 2025 in Louvain-la-Neuve and gathered 12 participants. We took the Sponsors' comments into account and reorganised the training in order to make the latter more accessible. In particular, the agenda, topics covered and logistics were revised to ensure a smoother transition between sessions[1],[2]. More details:

- We revised the content of the training, removed parts considered as too advanced in last edition's feedback and consolidated the remaining ones with complementary exercises;
- We created a *'getting started'* session that was sent to the participants prior to the training, of which the purpose was to check if the Notebook environment used during the training was well configured on their machine, to avoid losing time at the beginning of the training;
- We reduced the amount of pure implementation tasks in the practical sessions to the profit of the interpretation of phenomenons based on (controllable) parameter values;
- We split the remaining implementations tasks in sub-parts with unitary tests for the key functions to implement and provided solutions for all these sub-implementation sub-tasks;
- We created a different Jupyter Notebook for the practical sessions, with a more direct link to the topics covered during the theoretical sessions allowing improved discussions;
- We created a new introduction session, combining practical background to help participants gaining intuition about side-channel analysis through the basic manipulation and visualisation of real traces and statistical background to help assessing the results of the experiments;
- We created a new practical session introducing the typical non-idealities that may occur during the acquisition process and that may be the source of statistical bias.

[1] See https://perso.uclouvain.be/fstandae/book.html

[2] See https://github.com/simple-crypto/scale-one

The updated training received positive reviews globally, with more balanced feedbacks with respect to the difficulty and more appreciation regarding the quality of the sessions. Besides, it comes out of the received reviews that 100% of the attendees would recommend the formation and would be interested in a SCALE-II training focusing on countermeasures.

In parallel, we extended the SCALib evaluation library towards the support of new functionalities such as a new tool to perform Correlation Power Analysis (as suggested by sponsors), a new API separation between the fit and the prediction steps of the LDA models (together with a more efficient multi-variable LDA) and a new histogram-based rank estimation tool.

We also concluded an open source baseline masked software implementation of Dilithium (as also suggested by sponsors), following the descriptions in [1].[3] This implementation (currently) does not come with the strong worst-case security guarantees that the association targets, but was seen as a useful common ground to benchmark attacks proposed in the literature.

Finally, we progressed towards extending SMAesH with modes (ECB, CBC, CTR and GCM) and making the interface of the core compliant with Tilelink-UL v1.9.3 bus architecture. This project is under progress. A top-level draft of the architecture and FSM is already available.[4]

2 Sponsor's workshop conclusions

The sponsors marked their interest in a SCALE-II training, following the same model of SCALE-I but covering side-channel countermeasures. It was therefore suggested to organise it in 2026, and that a 2026 edition of SCALE-I would depend on the sponsors interest. It was however mentioned that SCALE-I should be organised on a periodic basis.

As of previous years, development projects were discussed to identify the priorities taking into account the limited resources of the association. Similarly to last year, the protection of post-quantum algorithms appeared to be of global interest, and more specifically for hardware implementations, for which there seems to be a lack of references implementations in the research community and for the industry. In parallel, the progress made on SCALib were appreciated and are encouraged. As a side request to leakage assessment/analysis tools, some interest was raised about having a tool enabling the efficient vizualisation of large measurement traces.

More precisely, we next list the topics identified as interesting for further development:

- *SCALE-II training*: The organization of a new training denoted SCALE-II, focusing on understanding the working principles of leakage resistance and countermeasures (leaving concrete implementation constraints and physical defaults for a later training), was encouraged. As for SCALE-I, the SCALE-II training will combine theoretical background, paper-and-pencil exercises and the analysis of power traces in the presence of countermeasures (e.g., masking or shuffling). The target period is the end of May / beginning of June.
- *SCAlib extensions*: Adding more features to SCAlib such as improved tools for MI estimation and tools for the efficient visualization of long traces is encouraged too.
- *Masked SHA3 in hardware*: Developing a masked SHA3, as a hardware module should be prioritized. This core could be used as a standalone co-processor, or as the basis block of a hardware/hybrid implementation of the ML-DSA signature scheme (which would be a

[3] https://github.com/simple-crypto/pqm4_masked/tree/master/crypto_sign/dilithium3/m4f_masked

[4] https://github.com/simple-crypto/SMAesH/tree/smaesh-mode

project in itself). Similarly to the SMAesH IP, it should come with detailed documentation, continuous test framework and preliminary side-channel security evaluation.

- *SMAesH-mode*: As mentioned last year, 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. This project is currently ongoing and it could be finalized it in the coming year. Together with the Verilog implementation in itself, this project involves the creation of a detailed implementation related to the API used as well as the top-level architecture.
- *Masked Ascon in hardware*: Developing a masked Ascon as a hardware module was suggested as well. While there does not seem to be a market demand in that direction for now, a protected hardware module of a recently standardized mode could be of interest in the future. As for our other development projects, this IP should come with detailed documentation, continuous test framework and preliminary side-channel security evaluation.

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.