Secure Gadgets for Post-Quantum Cryptography

For real world deployment, cryptographic devices must be protected against physical attacks. Against power-side channels, masking in its different flavors (e.g., Boolean, arithmetic masking) is a common approach. To implement masked cryptographic schemes, secure gadgets that are proven to be secure in certain probing models are typically used.

The first part of this work aims at explaining security notions like non-interference (NI), strong non-interference (SNI) [1], that are used within the context of secure gadgets. Afterwards, the work should investigate and explain some secure gadgets and procedures that are commonly used in post-quantum cryptography, as for example proposed in [2].

References

- [1]: https://dl.acm.org/doi/abs/10.1145/2976749.2978427
- [2]: https://link.springer.com/chapter/10.1007/978-3-030-21568-2_17

Contact

Request Topic

Advisors

Patrick Karl