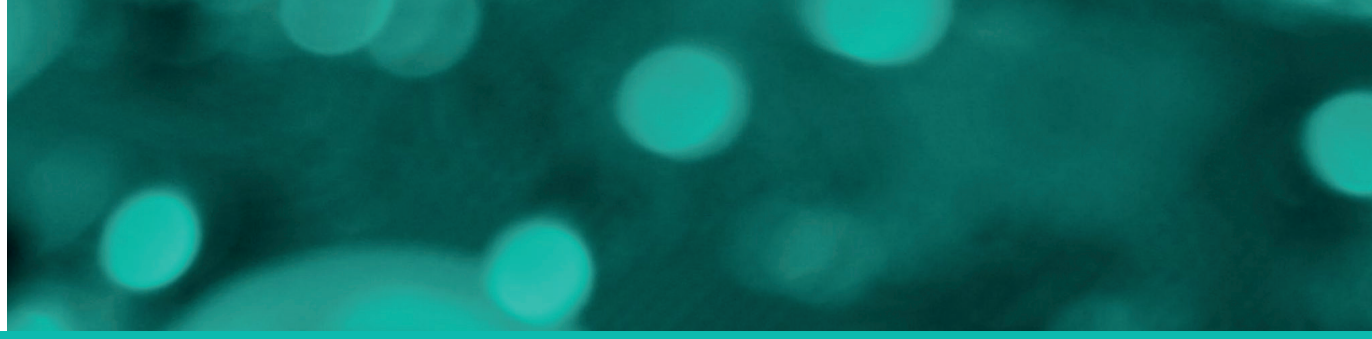
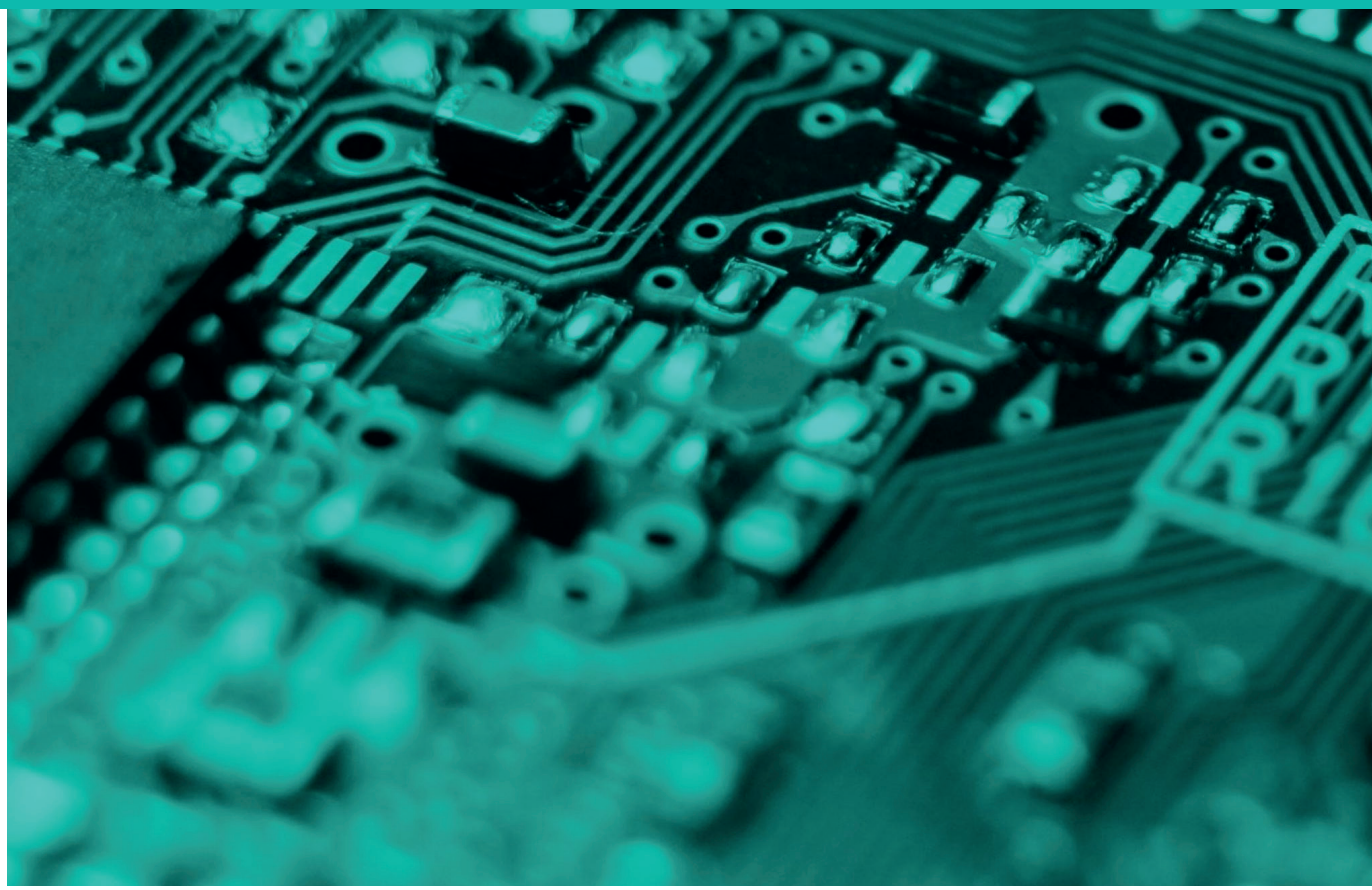


PIRATE

Protected Implementations, Resilient Algorithms, Test and Evaluation for Side-Channel Security



UCLouvain

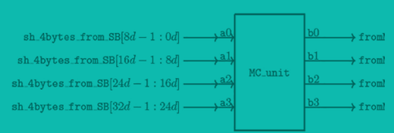
GROUPE CRYPTO

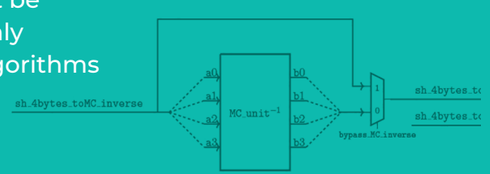
Wallonie service public SPW

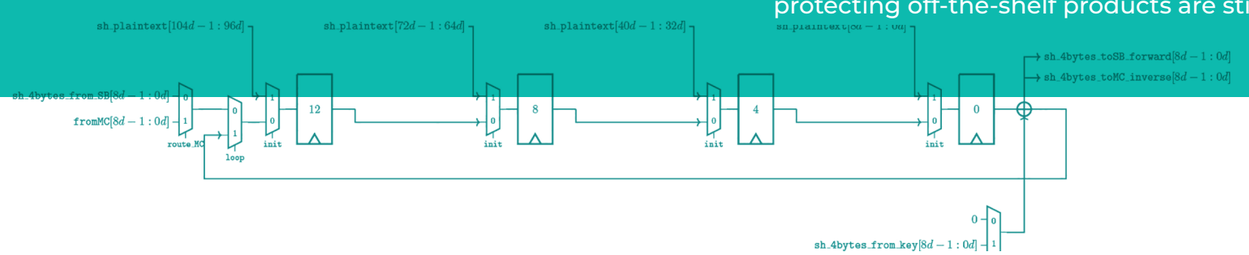
THALES
Construisons ensemble un avenir de confiance

Kerckhoffs's principle: security without obcurity

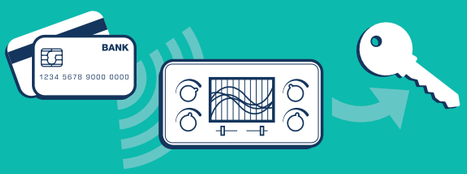
Unlike popular belief, cryptography is generally not about building secret schemes full of undisclosed details. On the contrary, Kerckhoffs's principle states that the security of a cryptosystem should not be based on its secrecy. This principle is commonly adopted today, and modern cryptographic algorithms are all based on public designs.







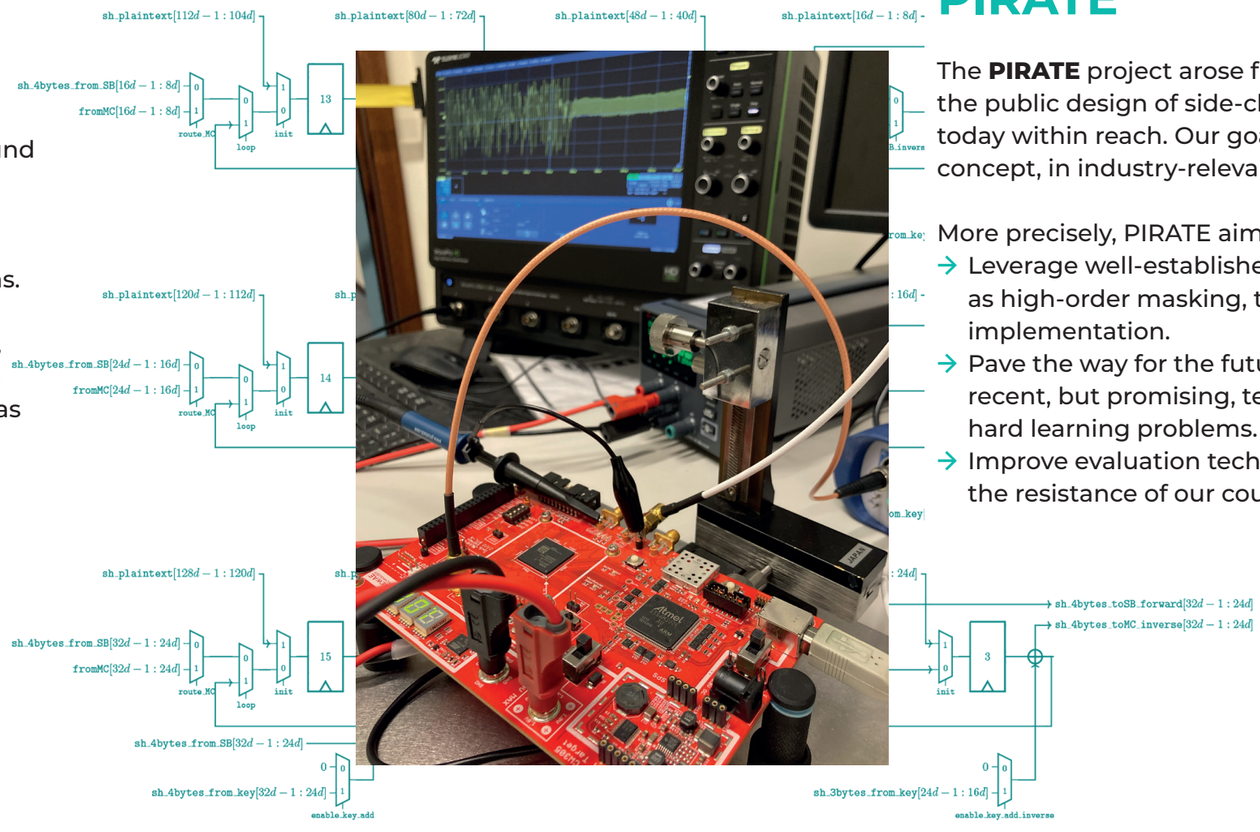
The side-channel attack exception



Side-channel attacks exploit, not only the specifications of a cryptographic algorithm, but also the physical characteristics of its execution on a real device, such as the energy consumed, or its electromagnetic emanations. Discovered in the late nineties, these attacks proved devastating against existing secure devices, and huge effort has been devoted since then in designing cost-effective countermeasures against them. Although based on public underlying principles, countermeasures have so far escaped Kerckhoffs's principle: nowadays, details of countermeasures protecting off-the-shelf products are still mostly confidential.

The benefits of public scrutiny

Yet, Kerckhoffs's principle is not a mere academic caprice: by allowing a wide analysis by experts around the world, the public disclosure of cryptosystems proved invaluable in improving their strength and developing a wide scientific consensus on the respective figures of merit of different constructions. After a transitory period due to the lack of a good theoretical understanding of the underlying issues, side-channel countermeasures would benefit from following a similar path. And we believe the time has come.



PIRATE

The **PIRATE** project arose from our conviction that the public design of side-channel countermeasures is today within reach. Our goal was to design proofs of concept, in industry-relevant environments.

More precisely, PIRATE aimed to:

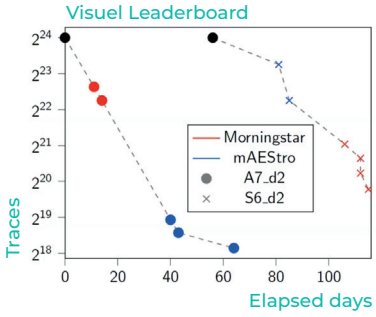
- Leverage well-established countermeasures, such as high-order masking, to develop a public secured implementation.
- Pave the way for the future, by analysing more recent, but promising, techniques, e.g. based on hard learning problems.
- Improve evaluation techniques in order to assess the resistance of our countermeasures.

Wallonie service public SPW

The **PIRATE** project was funded by the Walloon Region in the framework of the WIN²WAL programme (project 1910082)

CHES 2023
SMAesH challenge

- 5 teams:
- 112 submissions
- **A7_d2** ●
  - > 77 submissions
  - > 5 successful attacks
- **S6_d2** X
  - > 35 submissions
  - > 6 successful attacks
- Peak rates
  - > 2 submissions/h/team
  - > 12 submissions/day



What we developed

Thanks to Walloon Region funding, and in synergy with other projects, **PIRATE** developed:

- → An open-source FPGA implementation of the Advanced Encryption Standard (AES), protected against side-channel attacks and relying only on public countermeasures. This implementation was released as open source through the non-profit association SIMPLE CRYPTO, and submitted to the community as the CHES 2023 SMAesH challenge, inviting researchers from all over the world to submit their best attacks against it.
- → A proprietary implementation delivered to the project sponsor, Thales Belgium, for integration in some of their commercial products.
- → Various research papers describing this implementation and our approach based on hard learning problems.

Selected publications

SMAesH core, available at https://github.com/simple-crypto/SMAesH.

The SMAesH Challenge, available at https://smaesh-challenge.simple-crypto.org/.

C. Momin, G. Cassiers, F.-X. Standaert, Handcrafting: Improving Automated Masking in Hardware with Manual Optimizations, in the proceedings of COSADE 2021, LNCS, vol 13211, pp 257-275, Leuven, Belgium, April 2022, Springer

G. Cassiers, L. Masure, C. Momin, T. Moos, A. Moradi, F.-X. Standaert, Randomness Generation for Secure Hardware Masking – Unrolled Trivium to the Rescue. IACR CIC, vol. 1, no. 2, Jul 08, 2024.

S. Duval, P. Méaux, C. Momin, F.-X. Standaert, Exploring Crypto-Physical Dark Matter and Learning with Physical Rounding: Towards Secure and Efficient Fresh Re-Keying. IACR TCHES, 2021(1), 373-401.

D. Bellizia, C. Hoffmann, D. Kamel, P. Meaux, F.-X. Standaert, When Bad News Become Good News: Towards Usable Instances of Learning with Physical Errors, in IACR TCHES, vol 2022, num 4, pp 1-24.

C. Hoffmann, B. Libert, C. Momin, T. Peters, F.-X. Standaert, Polka: Towards Leakage-Resistant Post-Quantum CCA-Secure Public Key Encryption, in the proceedings of PKC 2023, LNCS, vol 13940, pp 114-144, Atlanta, USA, May 2023, Springer.

C. Hoffmann, P. Meaux, C. Momin, Y. Rotella, F.-X. Standaert, B. Udvarhelyi, Learning With Physical Rounding for Linear and Quadratic Leakage Functions, Crypto 2023, Lecture Notes in Computer Science, vol 14083, pp 410-439, Santa Barbara, California, USA, August 2023, Springer.

Interested ? Do not hesitate to contact us.
UCLouvain Crypto Group
Place du Levant, 3, 1348 Louvain-la-Neuve, Belgium
(+32)10 47 81 41
uclcryptogroup@listes.uclouvain.be