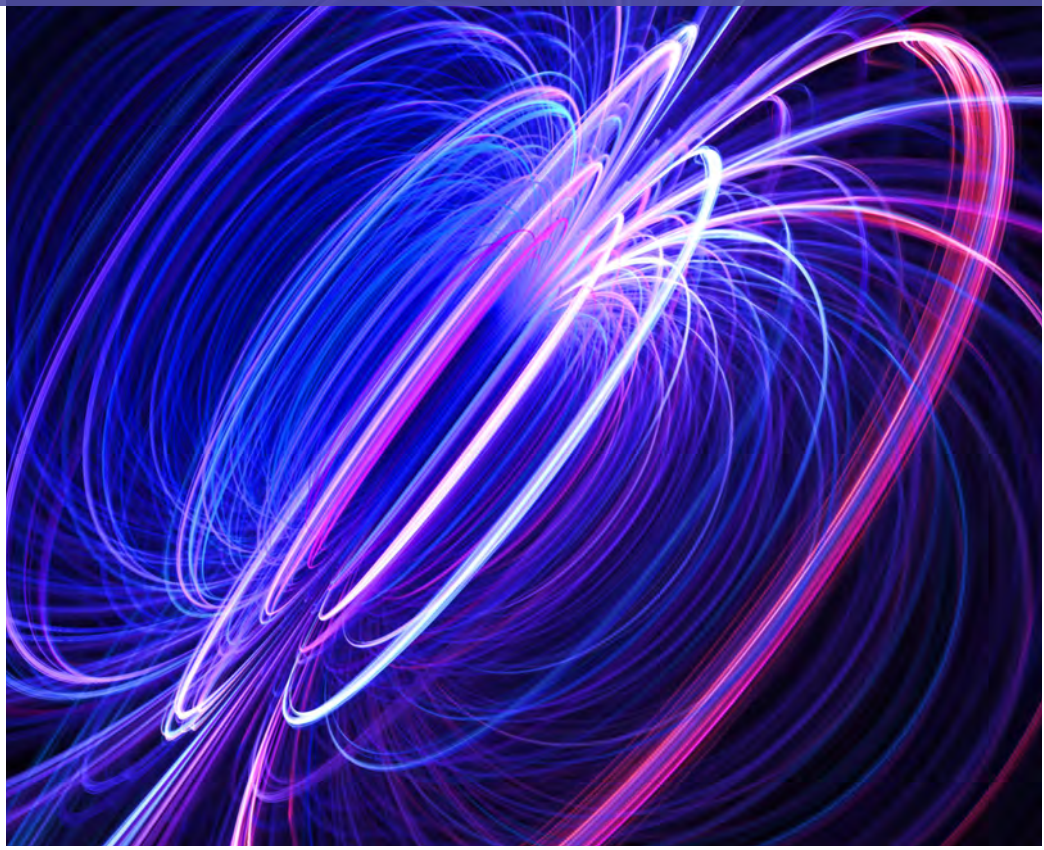
SCAUT

Side-channel Security for Authenticated Encryption



UCLouvain
University

worldline
e-payment services

ULB

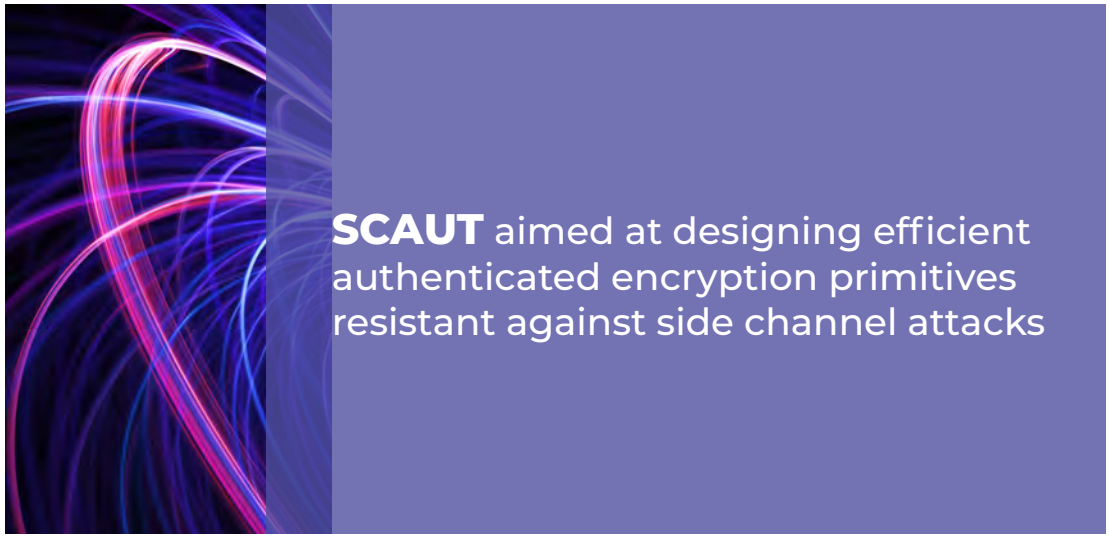
CRYPTO

QualSEC

Authenticated encryption

Authenticated encryption is a 2-in-1 primitive ensuring both that a message cannot be read by a third-party and that its content cannot be modified after it has been produced.
In addition to increased efficiency, authenticated encryption prevents unexpected issues that often arise when trying to combine encryption and authentication primitives.

Authenticated encryption is becoming more and more widespread nowadays, and is for example the only mode used in TLS 1.3.

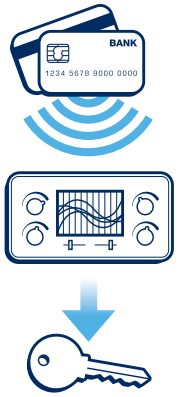


SCAUT aimed at designing efficient authenticated encryption primitives resistant against side channel attacks

Side-channel attacks

Side-channel attacks target a cryptographic device's physical characteristics, such as the power it consumes or the electromagnetic radiation it emits. They represent a very practical threat – sometimes needing only a few hundred measurements to break a secure token – and the industry devoted huge efforts to develop efficient countermeasures against them.

Initially focusing on embedded security devices such as smart cards, side-channel attacks now threaten an ever-increasing number of targets, with the advent of the IoT and the multiplication of tiny connected devices performing critical operations.



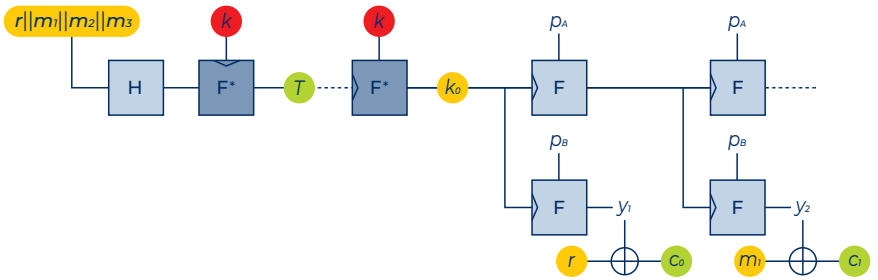
Project outcome

Thanks to Innoviris funding, this partnership between UCLouvain and ULB, with the technical support of Wordline who provided industrial feedback, achieved the following results

Re-keying: efficient generic modes

We designed several modes of operation achieving authenticated encryption and resistance against side-channel attacks. These modes rely on a protected implementation of a block cipher (in dark gray on the figure), but limit the use of this expensive component to the processing of one or two blocks, no matter the size of the message. The main payload can then be processed at full speed while still offering overall side-channel resistance.

Moreover, the security of these constructions has been formally analyzed, both regarding resistance to classical cryptanalysis and to side-channel attacks exploiting leakages.



SCREAM: a lightweight and easy-to-mask encryption algorithm

Although any cryptographic algorithm can in theory be protected against side-channel attacks, the cost of countermeasures can quickly become prohibitive. It is not enough to design a lightweight algorithm, that algorithm must be designed with side-channel protection in mind if we want to avoid losing all performance gains.
SCREAM is an authenticated encryption algorithm specifically designed to be lightweight and easy to protect against side-channel attacks. Its design focused on optimizing the AND complexity, allowing efficient masking-based protection.
This makes SCREAM suitable for secure implementation on low-end platforms, such as IoT devices.
Since the end of the SCAUT project we designed other primitives combining efficient lightweight implementation and resistance against side-channel attacks, such as the authenticated encryption algorithm Spook (**https://www spook dev**), which has been submitted to the US National Institute for Standards and technology (NIST) in the framework of their competition to select a new Lightweight Cryptography standard.

innoviris.brussels
empowering research

What we developed

With the support of Innoviris, we developed:

- Efficient and provably secure modes of operation achieving side-channel-resistant authenticated encryption. Side-channel resistance requires a fixed overhead, independent of the length of the message to be protected.
- Dedicated authenticated encryption primitives specifically designed to protect small embedded devices such as those required for the Internet of Things.

Partnership

We are looking for partners to produce and exploit this new technology

UCLouvain Crypto Group
Place du Levant, 3 – 1348 Louvain-la-Neuve | +32 10 47 81 41
uclcryptogroup@listes.uclouvain.be

Selected publications

Dobraunig, C., Koeune, F., Mangard, S., Mendel, F., Standaert F.: ***Towards fresh and hybrid rekeying schemes with beyond birthday security.*** *CARDIS 2015 – Lerman L., Bontempi G., Markowitch O.* ***The bias variance decomposition in profiled attacks.*** *Journal of Cryptographic Engineering Journault A., Standaert FX., Varici K.* ***Improving the Security and Efficiency of Block Ciphers Based on LS-Designs.*** *Designs, Codes and Cryptography, 2016 – Dziembowski S., Faust S., Herold G., Journault A., Masny D., Standaert FX.* ***Towards Sound Fresh Re keying with Hard (Physical) Learning Problems.*** *CRYPTO 2016 – Lerman L., Martinasek Z., Markowitch O.* ***Robust profiled attacks should the adversary trust the dataset?*** *IET Information Security 2017 – Lerman L., Markowitch O., Veshchikov N.* ***Comparing Sboxes of Ciphers from the Perspective of Side Channel Attacks.*** *AsianHOST 2016 – Barthe G., Dupressoir F., Faust S., Gregoire B., Standaert F.-X., Strub P.-Y.,* ***Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model.*** *EUROCRYPT 2017 – Lerman L., Veshchikov N., Picek S., Markowitch O.* ***On the Construction of Side-Channel Attack Resilient S-boxes.*** *COSADE 2017 – A. Journault, F.-X. Standaert,* ***Very High Order Masking: Efficient Implementation and Security Evaluation.*** *CHES 2017 – Lerman L., Poussier R., Markowitch O., Standaert F.-X.* ***Template attacks versus machine learning revisited and the curse of dimensionality in side channel analysis.*** *Journal of Cryptographic Engineering – Veshchikov N., Fernandes Medeiros S., Lerman L.* ***Variety of scalable shuffling countermeasures against side channel attacks.*** *Journal of Cyber Security and Mobility, 2017 – Lerman L., Veshchikov N., Markowitch O., Standaert F.-X.* ***Start Simple and then Refine Bias Variance Decomposition as a Diagnosis Tool for Leakage Profiling.*** *IEEE Transactions on Computers – Francesco Berti, François Koeune, Olivier Pereira, Thomas Peters, François Xavier Standaert:* ***Ciphertext Integrity with Misuse and Leakage Definition and Efficient Constructions with Symmetric Primitives.*** *AsiaCCS 2018.*