

# REASSURE

Robust and Efficient Approaches to  
Evaluating Side Channel and Fault Attack Resilience

<https://reassure.eu/>



 **UCLouvain**  
University

 **SGDSN**


 **University of  
BRISTOL**

 **UNIVERSITÄT  
KLAGENFURT**

 **IDEMIA**  
augmented identity

 **riscure**

 **NXP**

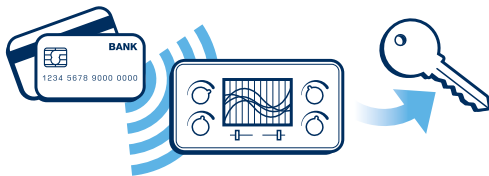


**REASSURE** tackles the problem of assessing the resistance against side-channel attacks, aiming at more efficient, more reliable evaluation practices

## 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 design countermeasures against them.

In parallel, sophisticated security certification and evaluation methods (Common Criteria, EMVCo, FIPS...) have been established to give users assurance that security claims have withstood independent evaluation and testing.



## Challenges in evaluation processes

Evaluating the efficiency of countermeasures is of course paramount, both for the designer who wants to confirm he reached his goal and for the independent evaluator.

**Yet, several challenges remain in the current state of the art:**

How can we gain confidence that a given countermeasure (or combination thereof) does achieve the required security level?

How can we compare the relative merits of different countermeasures?

Can we optimize the (very important) evaluation effort without losing reliability?

Can we extrapolate reliable estimates from limited data?

And how about newcomers to the field, such as Internet-of-Things (IoT) developers, who also need physical security, but lack the equipment and 20+ years of expertise of well-established actors such as smart card manufacturers.

## Our team

**Funded by the European Union through the H2020 program, REASSURE gathered 7 actors representative of all steps of side-channel evaluation:**

- Three universities – UCLouvain, University of Bristol, Universität Klagenfurt – active in academic research in the field.
- Two companies – NXP and IDEMIA – specialized in producing secure products.
- One evaluation lab – Riscure – performing independent assessment of secure implementations.
- One governmental body – SGDSN – certifying secure devices.

## Our goals

**REASSURE pursued 4 objectives:**

- To increase the quality, reliability and efficiency of vulnerability analysis, through a novel approach improving the assurance we get in evaluation outcomes and the comparability of independently conducted evaluations.
- To cater for emerging areas such as the IoT, by exploring the automation of leakage assessment practices and developing leakage simulators, so that IoT developers could early on assess leakage properties of their code without needing immediate access to a testing lab.
- To deliver practical tools, data sets and shared best-practice within the community of stakeholders, with the expectation that this will improve the quality of the assessment and characterization provided for newly-discovered attacks.
- To get existing stakeholders to adopt the novel technologies and methodologies emerging from this project as well as to provide input into new standardization efforts to ensure that they benefit from the knowledge created by this project.

# HORIZON 2020

## What we developed

Through **REASSURE**, we developed

- A novel evaluation strategy that works “backwards”, starting from a well-defined worst-case adversary. This approach increases the assurance level of our evaluations.
- Several automated methods, as well as shortcut formulas allowing much more efficient evaluations with limited (and quantified) impact on accuracy.
- Various software toolboxes to help with the analysis of side-channel resistance.
- Reference leakage traces on various platforms, as well as leakage simulators allowing to predict the leakage of an implementation.
- Live and online trainings for beginners and at more advanced levels.
- More than 30 scientific papers and 5 white papers.

Do not hesitate to visit our website <https://reassure.eu/> to access the project's material.

## Selected publications

Azouaoui M., Bellizia D., Buhan I., Debande N., Duval S., Giraud C., Jaulmes E., Koeune F., Oswald E., Standaert F.-X., Whytnall C., A Systematic Appraisal of Side-Channel Evaluation Strategies. *SSR 2020* – Whitnall C., Oswald E., A Critical Analysis of ISO 17825 ('Testing methods for the mitigation of non-invasive attack classes against cryptographic modules'). *Asiacrypt 2019*.

Bronchain O., Standaert F.-X., Side-Channel Countermeasures' Dissection and the Limits of Closed Source Security Evaluations. *TCHES 2020*.

Bronchain O., Hendrickx J. M., Massart C., Olshevsky A., Standaert F.-X., Leakage Certification Revisited: Bounding Model Errors in Side-Channel Security Evaluations. *CRYPTO 2019*.

Masure L., Dumas C., Prouff E., A Comprehensive Study of Deep Learning for Side-Channel Analysis. *TCHES 2020*.

Azouaoui M., Poussier R., Standaert F.-X., Verneuil V., Key Enumeration from the Adversarial Viewpoint When to Stop Measuring and Start Enumerating? *CARDIS 2019*.

McCann D., Oswald E., Whitnall C. Towards Practical Tools for Side Channel Aware Software Engineering: 'Grey Box' Modelling for Instruction Leakages. *USENIX Security Symposium 2017*.

## Partnership

Do not hesitate to contact us if you are interested in collaborating on any of these aspects.



**UCLouvain Crypto Group**

Place du Levant, 3 – 1348 Louvain-la-Neuve | +32 10 47 81 41  
[uclcryptogroup@listes.uclouvain.be](mailto:uclcryptogroup@listes.uclouvain.be)