Defence-related Research Action - DEFRA

ACRONYM: INES

Title: INtegrated Embedded Security

Duration of the project: 01/12/2025 – 01/03/2030

Key words: side-channel, fault injection, post-quantum cryptography

Budget: 2 448 000€

of which RHID contribution: 2 000 000€

PROJECT DESCRIPTION

Context

INES addresses the urgent need for robust embedded security of cryptographic implementations against side-channel attacks (SCAs) and fault injection attacks (FIAs), with a special focus on post-quantum cryptography (PQC). While PQC schemes (e.g., ML-KEM/Kyber and ML-DSA/Dilithium) are being standardized, their design rarely considered implementation-level physical threats, leaving national-security systems exposed when deployed in adversarial environments. The INES consortium —UCLouvain (coord.), NXP, STMicroelectronics, Thales Belgium, and the Royal Military Academy — ambitions to deliver a holistic response spanning design, implementation, measurement, and evaluation.

General objectives

The project is structured around four SMART goals:

1. Improve protections against SCAs and FIAs for PQC through sensitivity analyses and levelled implementations (e.g., focusing countermeasures where leakage is most critical).
2. Preserve security properties during compilation/synthesis for software and hardware (FPGAs), including the exploration of remote SCAs on general-purpose processors.
3. Build sound, harmonised test benches for local leakage measurements and fault insertion, plus VM-based setups for remote attacks.
4. Advance sound security assessment, combining worst-case attack studies with shortcut extrapolation to estimate resistance beyond in-lab limits and extend tooling (e.g. SCALib - https://www.simple-crypto.org/activities/scalib).

Methodology

INES follows an integrated, iterative workflow:

- **WP1 (Design):** Select priority PQC schemes; perform sensitivity analysis of subcomponents (e.g., NTT, re-encryption steps) and specify algorithmic-level countermeasures.
- **WP2 (Compilation & synthesis):** Translate countermeasures into protected implementations—software (embedded & general-purpose CPUs) and hardware (FPGAs)—ensuring that compiler/synthesizer preserves security. A public challenge implementation will be released to the community.
- **WP3 (Setups):** Define reference labs for SCAs and FIAs and construct VM networks to assess feasibility and conditions of remote SCAs.
- **WP4 (Assessment):** Strengthen evaluation methodologies (worst-case vectors, extrapolation) and expand SCALib with industry-driven features.
  The consortium will develop open-source results possible (datasets, code), and proprietary implementations supporting industrial exploitation and Defence use.

Potential impact on Defence

INES directly supports Defence CYBER priorities by:

- **Capability development:** Equipping Belgian Defence (via RMA, Cyber Command, NSA/NVO) with reproducible testing, improved assessment methods, and know-how to evaluate and produce secure cryptographic products resilient to SCAs/FIAs—even under field capture or adversarial manipulation.
- **Process optimisation:** Providing harmonised labs and quantitative evaluation shortcuts to accelerate certification-like workflows and procurement risk assessments.
- **Marketable products & jobs:** Industrial partners integrate results to harden devices used by Defence; knowledge transfer and new evaluation tasks will grow specialised roles within Defence organisations.

Expected final results & short/medium-term valorisation

- **Protected implementations:** At least three implementations (≥1 software, ≥1 hardware, ≥1 open source), including a community challenge release (M42) and proprietary deliverables for Defence supply (M48).
- **Remote SCA demonstrations:** Two attacks shown on realistic networked settings, with guidance on practical relevance and mitigations (M24).
- **Reference test benches:** Documented measurement and fault-injection lab design enabling reproducibility and cost-effective adoption (M42).
- **Evaluation tooling:** SCALib enriched with ≥2 new functionalities, plus evaluation reports and shortcut formulas for reliable extrapolation (M48).
- **Publications & dissemination:** ≥6 peer-reviewed papers; datasets and code shared where non-sensitive; workshops and focused briefings to Defence stakeholders (Cyber Command, NSA/NVO).

Valorisation perspectives

Short term (within project):

- Adoption of assessment processes and tooling by Defence evaluators and industrial labs; immediate use of improved SCALib and remote-attack VM network.

Medium term (3–5 years):

- Integration of countermeasures into Defence-grade products from Thales Belgium, NXP, and ST; strengthened national pathway toward embedded-security certification; sustained training using open datasets and challenge platforms.

CONTACT INFORMATION

Coordinator

UCLouvain / ICTEAM – Crypto Group
François-Xavier Standaert
francois-xavier.standaert@uclouvain.be

Partners

STMicroelectronics Belgium / Connected Security, SW development, Security architecture
Jean-François Dhem
Jean-francois.dhem@st.com

NXP Semiconductors Belgium NV / Competence Center Crypto & Security
Joppe Bos
joppe.bos@nxp.com

Thales Belgium / Innovation & Product Policy
Jonathan Pisane
jonathan.pisane@be.thalesgroup.com

Royal Military Academy / ALICE (cryptography group), MWMW (mathematics)
Julien Petit
julien.petit@mil.be

LINK(S)

Not available yet.