Defence-related Research Action - DEFRA

ACRONYME: INES

Titre: INtegrated Embedded Security

Durée du projet: 01/12/2025 – 01/03/2030

Budget: 2 448 000€

dont contribution IRSD: 2 000 000 €

Mots-clés: canaux auxiliaires, injection de fautes, cryptographie post-quantique

DESCRIPTION DU PROJET

Contexte

INES répond au besoin urgent d'une sécurité embarquée robuste pour les implémentations cryptographiques face aux attaques par canaux auxiliaires (SCAs) et aux attaques par injection de fautes (FIAs), avec un accent particulier sur la cryptographie post-quantique (PQC). Bien que les schémas PQC (par ex. ML-KEM/Kyber et ML-DSA/Dilithium) soient en cours de normalisation, leur conception a rarement pris en compte les menaces physiques au niveau de l'implémentation, laissant les systèmes de sécurité nationale exposés lorsqu'ils sont déployés dans des environnements hostiles. Le consortium INES — UCLouvain (coord.), NXP, STMicroelectronics, Thales Belgium et l'École Royale Militaire — ambitionne de fournir une réponse holistique couvrant la conception, l'implémentation, la mesure et l'évaluation.

Objectifs généraux

Le projet s'articule autour de quatre objectifs SMART :

1. Améliorer les protections contre les SCAs et FIAs pour la PQC grâce à des analyses de sensibilité et des implémentations à niveaux (par ex. concentrer les contre-mesures là où les fuites sont les plus critiques).
2. Préserver les propriétés de sécurité lors de la compilation/synthèse pour les logiciels et le matériel (FPGA), y compris l'exploration des SCAs à distance sur des processeurs généralistes.
3. Construire des bancs d'essai fiables et harmonisés pour les mesures locales de fuite et l'insertion de fautes, ainsi que des environnements VM pour les attaques à distance.
4. Faire progresser l'évaluation de la sécurité, en combinant l'étude des attaques dans le pire des cas avec des extrapolations simplifiées pour estimer la résistance au-delà des limites expérimentales et enrichir les outils (par ex. SCALib - https://www.simple-crypto.org/activities/scalib).

Méthodologie

INES suit un flux de travail intégré et itératif :

- **WP1 (Conception)** : Sélectionner les schémas PQC prioritaires ; réaliser une analyse de sensibilité des sous-composants (par ex. NTT, étapes de ré-encryption) et spécifier des contre-mesures au niveau algorithmique.
- **WP2 (Compilation & synthèse)** : Traduire les contre-mesures en implémentations protégées — logiciels (systèmes embarqués & processeurs généralistes) et matériels (FPGA) — en veillant à ce que le compilateur/synthétiseur conserve la sécurité. Une implémentation publique sera publiée sous forme de défi à la communauté.
- **WP3 (Bancs d'essai)** : Définir des laboratoires de référence pour SCAs et FIAs et construire des réseaux de VM pour évaluer la faisabilité et les conditions des SCAs à distance.
- **WP4 (Évaluation)** : Renforcer les méthodologies d'évaluation (approche du pire cas, extrapolation) et enrichir SCALib avec des fonctionnalités orientées industrie. Le consortium développera des résultats open source lorsque possible (jeux de données, code) et des implémentations propriétaires pour soutenir l'exploitation industrielle et l'usage Défense.

Impact potentiel pour la Défense

INES soutient directement les priorités CYBER de la Défense en :

- **Développement de capacités** : Équiper la Défense belge (via ERM, Cyber Command, NSA/NVO) avec des tests reproductibles, des méthodes d'évaluation améliorées et le savoir-faire pour évaluer et produire des produits cryptographiques sécurisés résistant aux SCAs/FIAs — même en cas de capture sur le terrain ou de manipulation hostile.
- **Optimisation des processus** : Fournir des laboratoires harmonisés et des raccourcis d'évaluation quantitative pour accélérer les flux de certification et les analyses de risque dans les achats.
- **Produits commercialisables & emplois** : Les partenaires industriels intégreront les résultats pour renforcer les dispositifs utilisés par la Défense ; le transfert de connaissances et les nouvelles tâches d'évaluation favoriseront la création de rôles spécialisés au sein des organisations de Défense.

Résultats finaux attendus & valorisation à court/moyen terme

- **Implémentations protégées** : Au moins trois implémentations (≥1 logiciel, ≥1 matériel, ≥1 open source), incluant une version publique pour défi communautaire (M42) et des livrables propriétaires pour la Défense (M48).
- **Démonstrations de SCAs à distance** : Deux attaques reproduites sur des environnements réseau réalistes, avec recommandations sur leur pertinence et les contre-mesures (M24).
- **Bancs d'essai de référence** : Conception documentée d'un laboratoire de mesure et d'injection de fautes permettant la reproductibilité et une adoption rentable (M42).
- **Outils d'évaluation** : SCALib enrichi d'au moins deux nouvelles fonctionnalités, plus des rapports d'évaluation et des formules simplifiées pour extrapolation fiable (M48).

- **Publications & diffusion** : ≥6 articles scientifiques évalués par les pairs ; jeux de données et code partagés lorsqu'ils ne sont pas sensibles ; ateliers et présentations ciblées pour les acteurs Défense (Cyber Command, NSA/NVO).

Perspectives de valorisation

Court terme (pendant le projet) :

- Adoption des processus et outils d'évaluation par les évaluateurs Défense et les laboratoires industriels ; utilisation immédiate de SCALib amélioré et du réseau VM pour attaques à distance.

Moyen terme (3–5 ans) :

- Intégration des contre-mesures dans des produits de niveau Défense chez Thales Belgium, NXP et ST ; renforcement de l'approche nationale vers la certification en sécurité embarquée; formation continue via jeux de données ouverts et plateformes de "challenge".

COORDONNÉES

Coordinateur

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

Partenaires

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

LIEN(S) DU PROJET

Non encore disponible