

Projet d'Initiation à la Recherche ou Projet d'Innovation-Recherche (barrer)

Nom du laboratoire ou de l'entreprise/établissement :

Collaboration avec Actia

TUTEUR(S)

- GRUYER Pierre. Mel : pierre.gruyer@actia.fr

Tuteurs INSA si projet industriel :

- Vincent Migliore. Mel: vincent.migliore@insa-toulouse.fr

TITRE DU PROJET

Cryptographie post-quantique pour systèmes embarqués automobiles

MOT-CLES

Cryptographie Post-Quantique, systèmes embarqués, implémentation logicielle

DESCRIPTIF (RESUME), indiquer l'enjeu sociétal de l'INSA de Toulouse s'il y a lieu

Objectifs du projet

L'objectif du PIR est de réaliser une étude exploratoire accompagnée d'un démonstrateur logiciel simplifié. Le projet ne vise pas à développer un produit industriel complet, mais à produire une première base technique permettant d'évaluer les impacts et les compromis liés à l'intégration de mécanismes post-quantiques dans un contexte embarqué.

Contexte

Les véhicules modernes intègrent de plus en plus de fonctions connectées : mises à jour logicielles à distance, diagnostic sécurisé, authentification de calculateurs, échanges avec le cloud ou gestion de certificats. Ces fonctions reposent aujourd'hui sur des mécanismes cryptographiques classiques.

À moyen ou long terme, l'arrivée d'ordinateurs quantiques suffisamment puissants pourrait remettre en cause une partie de ces mécanismes. Les industriels doivent donc anticiper la transition vers la cryptographie post-quantique, c'est-à-dire des algorithmes conçus pour rester robustes face à cette nouvelle menace.

ACTIA souhaite comprendre ce que signifie concrètement être « post-quantum ready » dans un contexte embarqué automobile : quels impacts sur les performances, la mémoire, les certificats, la mise à jour logicielle et l'architecture globale d'un calculateur ?

Problématique

Comment préparer un système embarqué automobile à l'arrivée de la cryptographie post-quantique, tout en conservant une architecture réaliste et compatible avec les contraintes industrielles ?

Travail demandé

- **Étude bibliographique :** Comprendre les principes de la cryptographie post-quantique, ses familles d'algorithmes, ses usages possibles et les contraintes spécifiques aux systèmes embarqués automobiles. Se renseigner notamment sur les méthodes d'hybridation (entre PQC et mécanismes crypto classiques RSA)

- **Choix d'un cas d'usage simple :** Définir un scénario représentatif, par exemple la vérification d'une signature avant mise à jour logicielle, l'authentification d'un message ou une transition simplifiée entre cryptographie classique et post-quantique.

- **Faire la comparaison entre plusieurs algorithmes Post-Quantique avec l'utilisation actuelle basé sur :**

- Paire de clés asymétrique basé sur RSA2048.

- Signature SHA256-RSA2048-PKCS1.5 algorithm.

- **Benchmark expérimental :** Mettre en place un environnement de test sur Raspberry Pi (ou sur Arduino qu'on préférera pour travailler sur des environnements temps réels avec librairie PQCMicro) afin de mesurer des critères comme le temps de calcul, la taille des clés, la taille des signatures et, si possible, l'empreinte mémoire.

- **Démonstrateur logiciel** : Réaliser une maquette simple illustrant le fonctionnement étudié : génération de clés, signature, vérification, comparaison classique/post-quantique ou simulation d'une étape de mise à jour sécurisée.
- **Analyse et recommandations** : Interpréter les résultats obtenus et proposer des recommandations pour une future intégration industrielle : points forts, limites, risques techniques et travaux complémentaires nécessaires.

Livrables attendus

- Rapport d'état de l'art synthétique sur la cryptographie post-quantique et ses enjeux pour l'automobile.
- Description du cas d'usage étudié, des hypothèses retenues et des limites du périmètre.
- Démonstrateur logiciel simplifié avec procédure d'exécution.
- Résultats de benchmark : temps d'exécution (Durée précise à la milliseconde), tailles de clés/signatures, observations mémoire si disponibles.
- Synthèse de recommandations à destination d'ACTIA pour préparer une suite en projet, stage ou PoC industriel.

Compétences développées

- Cybersécurité embarquée
- Cryptographie appliquée
- Systèmes embarqués automobiles
- Benchmark et analyse de performances
- Architecture logicielle
- Rédaction technique et vulgarisation

PROFIL DES ETUDIANTS SOUHAITE (1 seul choix par projet)

- ☐ IR-SI : spécialité Informatique parcours Systèmes Informatiques

PRIORITE : si vous posez plusieurs sujets, indiquer ici la priorité de ce sujet (1= plus prioritaire)