Migration des systèmes d'information à la cryptographie post-quantique

Numéro de la fiche : OPR-1206

Sommaire

DIRECTION DE RECHERCHE

Aref Meddeb, Professeur - Département de génie électrique et de génie informatique

RENSEIGNEMENTS

aref.meddeb@usherbrooke.ca

UNITÉ(S) ADMINISTRATIVE(S)

Faculté de génie
Département de génie électrique et de génie informatique

CYCLE(S)

2e cycle
3e cycle

LIEU(X)

Campus principal
Pôle d'expertise en cybersécurité

Description du projet

Face à l'évolution rapide de l'informatique quantique, la recherche en cryptographie post-quantique (PQC) a souligné l'urgence pour les organisations d'adapter leurs protocoles cryptographiques avant que les ordinateurs quantiques ne soient capables de casser les schémas de chiffrement largement utilisés.

Les objectifs sont les suivants :

1 – (MScA) Élaboration d'un horizon de préparation stratégique pour l'adoption des normes PQC
Objectif : Protéger les infrastructures des organisations contre les futures menaces quantiques.
Méthodologie : i) Évaluer les cryptosystèmes déployés et identifier leurs vulnérabilités ii) Définir un calendrier : avec des étapes clés pour une transition en douceur vers les normes PQC. iii) Fournir des outils pour évaluer les investissements dans les technologies PQC en fonction des évaluations des risques et des besoins opérationnels.
Résultat : Une feuille de route stratégique avec des solutions sur mesure, permettant de garder une longueur d'avance sur les perturbations quantiques tout en optimisant l'efficacité des ressources.

2 – (PhD) Conception et mise en œuvre d'approches de migration hybrides
Objectif : Assurer une transition en douceur vers les normes PQC tout en maintenant l'interopérabilité avec les systèmes existants.
Méthodologie : i) Développer des modèles de chiffrement hybrides : combinant algorithmes classiques et PQC. ii) Simuler et tester : les performances, l'évolutivité et la sécurité de ces modèles dans des scénarios réels. iii) Mettre en œuvre des systèmes hybrides : de manière incrémentale, en commençant par les applications à faible risque avant un déploiement plus large.
Résultat : un cadre cryptographique hybride robuste minimisant les perturbations opérationnelles et favorisant l'adoption progressive du PQC.

3 – (MScA) Évaluations des risques, priorisation et revues de conformité

Objectif : identifier et atténuer les risques associés aux menaces quantiques tout en garantissant une conformité réglementaire minimale

pendant le processus de migration du PQC.
Méthodologie : i) Évaluer les risques liés au PQC : comprendre l'impact de l'informatique quantique sur les systèmes critiques et les données clients. ii) Élaborer des stratégies PQC : garantir la conformité aux normes et réglementations. iii) Élaborer des plans d'urgence : relever les défis imprévus pendant la transition.
Résultat : amélioration de la résilience opérationnelle et de l'alignement réglementaire, renforcement de la confiance des clients et garantie d'une conformité transparente.

Discipline(s) par secteur

Sciences naturelles et génie

Génie électrique et génie électronique

Financement offert

Oui

Partenaire(s)

Intact

La dernière mise à jour a été faite le 28 March 2025. L'Université se réserve le droit de modifier ses projets sans préavis.