Comparaison des certificats hybrides PQC

Numéro de la fiche : OPR-1323

Sommaire

DIRECTION DE RECHERCHE

Pierre Martin Tardif, Directeur de département - Département des systèmes d'information et méthodes quantitatives de gestion

RENSEIGNEMENTS

pierre-martin.tardif@usherbrooke.ca

UNITÉ(S) ADMINISTRATIVE(S)

École de gestion
Département des systèmes d'information et méthodes quantitatives de gestion
Faculté des sciences
Faculté de génie

CYCLE(S)

2e cycle

LIEU(X)

Université de Sherbrooke, campus principal

Description du projet

À mesure que l'informatique quantique progresse, elle menace de briser les méthodes de cryptage actuellement utilisées pour sécuriser les communications numériques, telles que RSA et ECDSA. En réponse, de nouveaux algorithmes « résistants à l'informatique quantique » ont été développés, mais ils sont nettement plus volumineux et complexes, ce qui pose des défis majeurs pour leur intégration dans les infrastructures actuelles, en particulier les certificats numériques qui reposent sur la norme X.509 largement utilisée. Afin de gérer cette transition de manière sécurisée et progressive, des certificats hybrides combinant des méthodes traditionnelles et des méthodes résistantes à l'informatique quantique ont été proposés. Cependant, peu de recherches ont évalué et comparé leurs performances réelles et leur impact sur les communications sécurisées telles que les communications de la NSA. Afin de gérer cette transition de manière sûre et progressive, des certificats hybrides combinant des méthodes traditionnelles et des méthodes résistantes aux ordinateurs quantiques ont été proposés. Cependant, peu de recherches ont évalué et comparé leurs performances réelles et leur impact sur la sécurité des communications telles que le protocole TLS.

Discipline(s) par secteur

Sciences naturelles et génie

Génie informatique et génie logiciel, Informatique

Financement offert

À discuter

La dernière mise à jour a été faite le 22 juin 2026. L'Université se réserve le droit de modifier ses projets sans préavis.