Comparaison des certificats hybrides PQC

Record number : OPR-1323

Overview

RESEARCH DIRECTION

Pierre Martin Tardif, Directeur de département - Department of Information Systems and Quantitative Management Methods

INFORMATION

pierre-martin.tardif@usherbrooke.ca

ADMINISTRATIVE UNIT(S)

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

LEVEL(S)

2e cycle

LOCATION(S)

Université de Sherbrooke, campus principal

Project Description

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) by sector

Sciences naturelles et génie

Génie informatique et génie logiciel, Informatique

Funding offered

To be discussed