Offre de thèse

Intitulé : Développement de modèles de gestion de clés post-quantique pour les réseaux d'Internet des Objets (IoT)

Mots-clés: Sécurité, Réseau, Gestion de clés, Post-quantique, Internet des Objets

Information générale
Etablissement d'accueil : ENSSAT, Lannion
Laboratoire et équipe d'accueil : IRISA, Equipe SOTERN
Durée de thèse : 36 mois
Période : 2026-2029

Liste des encadrants

Directeur de thèse: Gilles Guette
Email: gilles.guette@imt-atlantique.fr
Encadrant: Mohammed NAFI
Email: mohammed.nafi@irisa.fr
Co-encadrant: Renzo NAVAS
Email: renzo.navas@imt-atlantique.fr

Description du sujet de la thèse

Contexte

L'internet des objets (IoT) est un système composé d'une multitude d'objets qui sont autonomes, hétérogènes et accessibles depuis Internet. Ces objets sont capables de collecter et d'échanger des données à travers un réseau (5G, Wifi, etc). Ce paradigme est largement utilisé dans de nombreux domaines, notamment la santé, les transports, les maisons et villes intelligentes. Dans les applications sensibles telles que la santé, les données privées nécessitent d'être protégées contre les attaques de cybersécurité. À l'heure actuelle, la sécurité de ces données repose sur l'usage des protocoles de chiffrement *symétriques* (ex., AES), *asymétriques* (ex., RSA, courbes elliptiques, ElGamal, Diffie–Hellman), et fonctions de hachage (ex., SHA-3). Tous les systèmes cryptographiques actuels, notamment symétriques, reposent sur un système de gestion de clés fiable. En effet, la gestion de clés est au cœur de tout système sécurisé, et consiste en la génération, la distribution, le stockage, l'utilisation, le rafraîchissement, la révocation, et la destruction des clés cryptographiques.

Problématique

Avec l'avènement des ordinateurs quantiques, les mécanismes de gestion de clés utilisés dans les réseaux IoT deviendront vulnérables. Les protocoles actuels s'appuient majoritairement sur des primitives cryptographiques symétriques et asymétriques classiques. Or, la plupart de ces primitives, notamment asymétriques, ne sont pas résistantes aux nouvelles capacités de calcul des ordinateurs quantiques. A titre d'exemple, l'algorithme de Shor [1] est capable de compromettre les

mécanismes d'établissement et d'échange de clés basés sur la factorisation ou le logarithme discret, tandis que l'algorithme de Grover [2] réduit significativement le niveau de sécurité des schémas symétriques.

Dans les environnements IoT, les données sensibles (sanitaires, bancaires, économiques, etc) doivent rester confidentielles pendant plusieurs années. Or, les attaquants peuvent dès à présent intercepter et sauvegarder les communications chiffrées, afin de les déchiffrer ultérieurement lorsqu'ils disposeront d'ordinateurs quantiques. La fuite des données sensibles pourrait avoir des conséquences graves pour les systèmes cibles. Il convient alors à toute organisation ou entreprise de se protéger contre cette menace imminente. Par conséquent, il est essentiel de développer des solutions de sécurité post-quantiques, notamment de gestion de clés, capables d'être déployées sur des systèmes IoT actuels afin de se protéger à la fois contre les attaques classiques et quantiques.

La gestion de clés dans les réseaux IoT reste une tâche très difficile à assurer en raison, entre autres, de leurs fortes contraintes de ressources, hétérogénéité et forte mobilité des appareils IoT, et elle est d'autant plus problématique dans un environnement post-quantique où la taille des clés et des messages est nettement supérieure.

Etat de l'art

Plusieurs travaux de recherche ont été mis en place pour faire face aux attaques quantiques. Parmi ces travaux, on trouve les protocoles d'authentification et d'accord de clés [3,4,5,6,7], les protocoles d'échange et distribution de clés [8,9,10,11,12], les protocoles d'établissement et gestion de clés [13,14,15], les algorithmes de signatures numériques [16, 17], les protocoles hybrides [3] qui combinent les approches classiques et post-quantiques, et les autres modèles de sécurité [18,19, 20,21,22,1,2]. A titre d'exemple, IHKEM [14] est un protocole hiérarchique d'établissement et de gestion de clés dans les réseaux de capteurs sans fil. Ce protocole est conçu pour résister aux attaques quantiques tout en préservant les ressources des capteurs. L'article [19] explore les défis et les solutions pour la gestion de clés de groupe dans les réseaux IoT à l'ère de l'informatique quantique. Dans l'article [9], trois modèles d'échange de clés post-quantiques sont proposés. Les auteurs [3] ont proposé un framework hybride d'authentification et d'accord de clés pour un modèle client-serveur, qui se base à la fois sur les courbes elliptiques (ECC) et le mécanisme d'encapsulation de clés (KEM).

L'organisme de normalisation NIST a standardisé trois solutions post-quantiques : un modèle d'encapsulation de clés ML-KEM [13] et deux modèles de signature numérique ML-DSA [16] et SLH-DSA [17]. Au sein de l'IETF, le groupe de travail LAKE [23] cherche à adapter le protocole d'échange de clés EDHOC [12] aux exigences du post-quantique.

Bien que certains travaux de recherche aient déjà abordé le problème de sécurité des réseaux IoT dans un environnement post-quantique, très peu de solutions se sont intéressées à la gestion de clés dans sa globalité. En effet, les solutions actuelles ne traitent pas simultanément et de manière efficace toutes les phases de la gestion de clés ou tous le cycle de vie des clés.

Objectifs

L'objectif principal de cette thèse consiste en la mise en place de nouvelles approches de gestion de clés légères, robustes, efficaces qui remédient à cette problématique de sécurité critique des systèmes IoT dans un environnement quantique. Des caractéristiques des systèmes IoT doivent être prises en considération lors de la conception et du développement de nouvelles solutions.

Description des principaux verrous et travaux envisagés

Parmi les nombreuses approches de sécurité, nous nous intéresserons principalement à la gestion de clés. Plusieurs verrous de recherche doivent être levés, notamment :

- *Génération et stockage des clés*. Nous tenterons de répondre à la première question « *A quel niveau de l'architecture des systèmes IoT, les clés post-quantiques seront-elles établies ?* ». La taille des clés, le niveau de sécurité recherché, et la capacité des nœuds IoT seront pris en considération dans le processus de génération. La seconde question concerne le stockage des clés générées. En effet, les clés secrètes doivent être stockées de manière sûre pour diminuer l'impact des attaques de compromission de nœuds, ce qui nous amène à la question « *Où et comment seront-elles sauvegardées ?* ».
- *Distribution des clés*. Dans le cas où les clés cryptographiques sont générées par une tierce partie de confiance, nous tenterons d'apporter des réponses à la question « *Comment les clés seront-elle distribuées aux entités légitimes du système IoT à travers des canaux de communication publics ?* »
- *Rafraichissement et destruction des clés.* Pour contrer les attaques de sécurité, les clés nécessitent d'être rafraichies périodiquement. Nous essaierons de répondre à la question *« A quel moment et fréquence les clés seront-elles renouvelées ? »*

Approche méthodologique et critères de qualité des résultats obtenus

Les principaux travaux de cette thèse s'articuleront de la manière suivante :

- T0-T0+6 : Dans cette première partie, le doctorant devra effectuer une revue de la littérature pour élaborer un état de l'art exhaustif sur la gestion de clés post-quantiques dans les réseaux IoT. Une classification et une étude comparative des différentes approches seront également réalisées.
- T0+6-T0+22 : Le travail de cette seconde partie consistera en la mise en place des approches de gestion de clés post-quantiques originales, légères, robustes, et efficaces. Différentes pistes devront être explorées pour répondre à ce défi. Des approches empiriques basées sur des fondamentaux établis tant en crypto-primitives (NIST ML-KEM, HQC) qu'en protocoles réseaux (LAKE IETF, EDHOC, CBOR/COSE), seront prévues. L'implémentation, le test et l'évaluation des protocoles proposés sur de vrais réseaux et nœuds IoT seront envisagés. De plus, une validation formelle des approches proposées avec un outil comme TAMARIN ou Proverif devra aussi être réalisée.
- T0+22-T0+30 : Cette troisième partie se concentrera sur le passage à large échelle des solutions proposées. Des simulations devront être effectuées pour évaluer leurs performances en matière d'efficacité, de robustesse, et de consommation de ressources (énergie, mémoire, et calcul), avec une vision systémique. Pour ce faire, des simulateurs comme NS-3, pourront être utilisés, ou de nouvelles méthodes de simulation pourront être mises en place. Les résultats obtenus seront, par la suite, comparés avec ceux de certaines approches pertinentes de la littérature.
- T0+30 – T0+36 : le doctorant se concentrera sur la rédaction de son manuscrit de la thèse et la préparation de sa soutenance.

Les travaux réalisés dans le cadre de cette thèse, à savoir un état de l'art complet et approfondi et les nouvelles approches de gestion de clés, feront l'objet d'enquêtes/*Surveys* et d'articles scientifiques qui seront soumis dans des journaux et conférences de renommée internationale dans le domaine de la sécurité des réseaux tels que IEEE Internet of Things Journal, Future Generation Computer Systems, Computer Networks. Les protocoles développés pourront également être proposés à l'IETF pour suivre la procédure de standardisation.

Bibliographie

[1] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.

[2] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[3] Braeken, A. (2025). Flexible hybrid post-quantum bidirectional multi-factor authentication and key agreement framework using ECC and KEM. Future Generation Computer Systems, 166, 107634.

[4] Braeken, A. (2025). Ultra-lightweight post-quantum resistant 5G-AKA protocol. Computer Networks, 111444.

[5] Ghosh, H., Maurya, P. K., Bagchi, S., & Dwivedi, A. D. (2025). Lightweight RFID-enabled authentication protocol in post-quantum environment. Computers and Electrical Engineering, 124, 110367.

[6] Pursharthi, K., & Mishra, D. (2024). Towards post-quantum authenticated key agreement scheme for mobile devices. *Journal of Information Security and Applications*, *82*, 103754.

[7] Babu, P. R., Kumar, S. A., Reddy, A. G., & Das, A. K. (2024). Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges. Computer Science Review, 54, 100676.

[8] Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2025). Quantum Key Distribution Networks-Key Management: A Survey. ACM Computing Surveys, 57(10), 1-36.

[9] Fan, X., Zhao, F., & Xu, X. (2025). Multi-party post-quantum key exchange schemes. Journal of Information Security and Applications, 95, 104288.

[10] Dabra, V., Kumari, S., Bala, A., & Yadav, S. (2024). SL3PAKE: simple lattice-based three-party password authenticated key exchange for post-quantum world. Journal of Information Security and Applications, 84, 103826.

[11] Sekga, C., & Mafu, M. (2021). Security of quantum-key-distribution protocol by using the post-selection technique. Physics Open, 7, 100075.

[12] Selander, G., Mattsson, J., & Palombini, F. (2024). Ephemeral diffie-hellman over cose (edhoc). RFC 9528

[13] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European symposium on security and privacy (EuroS&P) (pp. 353-367). IEEE.

[14] Jain, K., & Singh, A. (2025). IHKEM: A Post-Quantum Ready Hierarchical Key Establishment and Management Scheme for Wireless Sensor Networks. Microprocessors and Microsystems, 105205.

[15] Samiullah, F., Gan, M. L., Akleylek, S., & Aun, Y. (2023, November). Post-quantum group key management in iots. In 2023 25th International Multitopic Conference (INMIC) (pp. 1-6). IEEE.

[16] National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204. https://doi.org/10.6028/NIST.FIPS.204

[17] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205

[18] Şafak, I., Alagöz, F., & Anarim, E. (2025). Post-quantum security measures for the internet of things. In Encyclopedia of Information Science and Technology, Sixth Edition (pp. 1-44). IGI Global Scientific Publishing.

[19] Hanna, Y., Bozhko, J., Tonyali, S., Harrilal-Parchment, R., Cebe, M., & Akkaya, K. (2025). A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. Internet of Things, 101650**.**

[20] Ma, C., Shankar, A., Kumari, S., & Chen, C. M. (2024). A lightweight BRLWE-based post-quantum cryptosystem with side-channel resilience for IoT security. Internet of Things, 28, 101391.

[21] Lohachab, A., Lohachab, A., & Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things, 9, 100174

[22] Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet of Things Journal, 7(7), 6457-6480.

[23] Lightweight Authenticated Key Exchange (LAKE) https://datatracker.ietf.org/doc/charter-ietf-lake/

Profil recherché

Un étudiant titulaire d'un diplôme de Master 2 ou équivalent dans le domaine de l'Informatique possédant des compétences avérées en réseaux et sécurité informatiques, cryptographie, intelligence artificielle, programmation et communication.

Candidature

Merci d'envoyer votre dossier de candidature par e-mail aux contacts indiqués ci-dessus, comprenant un CV, une lettre de motivation, les relevés de notes de Licence et de Master (avec votre classement), ainsi qu'une ou plusieurs lettre(s) de recommandation.