Proposition de thèse

Cryptographie Post-Quantique pour l'Aéronautique

1. Objet de la thèse

Nous souhaiterions proposer un sujet de thèse autour de la cryptographie post-quantique en cours de standardisation par le NIST en se focalisant sur :

- l'étude des différentes solutions proposées dans le contexte aéronautique ;
- la proposition de variantes, ou nouvelles solutions créées pour l'aéronautique ;
- l'analyse de modèles d'attaquant adaptés aux contraintes de l'aéronautique.

2. Descriptif de la thèse

Cette thèse est en lien avec le thématique « Prise en compte de la menace de l'algorithmique quantique » dans le sous-thème 1 « Cryptographie ».

La transition vers des systèmes cryptographiques résistants à un ordinateur quantique risque d'être imposée sous peu. Le NIST a en effet le pouvoir d'imposer ce passage à toute entreprise travaillant avec le gouvernement américain, et par voie de conséquence de forcer en pratique cette transition sur le marché mondial. En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) préconise d'ailleurs l'utilisation de tels mécanismes pour les applications nécessitant une sécurité sur le long terme [LRANSSI].

Le domaine de l'aéronautique, avec des cycles de vie qui peuvent s'étendre sur plusieurs décennies, se prépare à cette transition. Un exemple, sur le site toulousain, sont les R&T R-S3/RE-0003-011 et R-S16/RE-0003-011 proposées par le CNES où il était demandé de traiter explicitement le cas de la cryptographie post-quantique pour l'injection de clés à distance dans un contexte satellitaire. L'un des futurs encadrants a été l'expert scientifique portant ces deux R&T.

Le NIST prévoit de standardiser des protocoles d'échanges de clés (permettant à deux entités échangeant sur un canal non sûr d'obtenir un secret commun) et de signature (permettant à une entité de prouver son identité). La compétition vient de passer en phase 2, et deux des futurs encadrants (Carlos Aguilar, ISAE, et Jean-Christophe Deneuville, ENAC) portent 4 parmi les 17 propositions restantes [NISTR2].

Certaines de ces propositions ont une sécurité fondée sur des problèmes réputés difficiles dans la théorie des codes correcteurs. Nous souhaiterions proposer un sujet de thèse autour de :

- l'étude des différentes solutions proposées dans le contexte aéronautique ;
- la proposition de variantes, ou nouvelles solutions créées pour l'aéronautique ;
- l'analyse fine de modèles d'attaquant quantique adaptés aux contraintes de l'aéronautique.

[NISTR2] https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

[LRANSSI] https://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-%C3%A0-laide-de-m%C3%A9canismes

3. Programme de la thèse

La grande majorité des travaux autour de la standardisation de la cryptographie post-quantique cible le monde IT avec des implémentations software. Certains travaux traitent des implémentations hardware, mais pas dans le contexte des contraintes habituelles de l'aéronautique.

Par ailleurs le modèle d'attaquant généralement retenu est celui d'un attaquant ayant accès à un ordinateur quantique idéal (grand nombre de qu-bits, pas de problèmes de cohérence dans le temps, etc.) et pouvant réaliser un grand nombre de calculs même si ceux-ci demandent un temps considérable (e.g. des années). Ce modèle est intéressant pour les candidats à la standardisation du NIST car il permet de proposer des standards qui sont utilisables même dans les contextes les plus adverses. En revanche, cette approche impose d'utiliser des mécanismes plus complexes et des clés de plus grande taille que ce qui est nécessaire dans certaines applications.

L'objectif de cette thèse, par opposition aux travaux mentionnés, est d'étudier la question de la transition vers une cryptographie résistante à l'ordinateur quantique, dans le contexte de l'aéronautique.

Pour cela nous étudierons quel protocole serait optimal tant au niveau de la signature que de l'échange de clés pour des applications diverses : satellites, avions, drones. Une première question qui est majeure dans l'aéronautique, et tout particulièrement pour le contexte satellite, est les performances (temps et taille occupée) d'une implémentation FPGA (incluant un encodage des clés dans le FPGA pour qu'elles soient inaccessibles au système d'exploitation). Cette contrainte n'a absolument pas été prise en compte pour le moment et il est intéressant d'étudier quelle pourrait être la meilleure approche dans un tel contexte.

Ainsi, dans un premier temps nous trierons les candidats en fonction de la complexité estimée pour une implémentation hardware incluant un encodage des clés. Nous réaliserons des premières implémentations simples en FPGA pour les candidats plus prometteurs et étudierons les implémentations existantes.

Dans un deuxième temps, forts de cette première expérience et de nos connaissances des divers candidats à la standardisation, nous nous intéresserons aux choix qui auraient été faits pour optimiser les algorithmes dans le contexte IT et qui auraient un impact négatif dans le contexte FPGA. Par exemple, pour le candidat HQC[1] que nous avons proposé à la

[1] https://pqc-hqc.org/

standardisation, la dernière phase de l'échange de clé correspond au décodage d'un code tenseur entre un code à répétition et un code BCH. Ce choix permet d'optimiser la taille des clés tout en permettant une analyse formelle de la propagation des erreurs. Des résultats récents (non publiés) d'une partie de l'équipe portant HQC montrent qu'il est possible d'optimiser encore plus la taille des clés si on utilise des codes plus élaborés (mélange de Reed-Solomon et de Reed-Muller). Ceci est sans doute un mauvais choix pour une implémentation FPGA car le gain en taille de clé ne compensera certainement pas l'augmentation de la surface utilisée pour traiter de tels codes. Inversement, un pur code de répétition (avec décodage par majorité) fera grandir significativement les clés mais simplifiera tellement la phase de décodage qu'il est très crédible que l'empreinte FPGA se voit réduite. Nous mettons en relief HQC étant donné que c'est l'un des candidats que nous portons mais des questions équivalentes se posent pour la majorité des candidats.

Dans un troisième temps, nous passerons en revue des choix plus génériques qui ont été faits par la communauté ou par le NIST pour atteindre des standards de sécurité les plus hauts possibles. Par exemple on peut citer l'utilisation d'algorithmes en temps constant[2] ou les transformations génériques IND-CCA. Focalisons-nous sur le temps constant, qui permet d'assurer que les fuites d'information locales sur le temps d'exécution des algorithmes cryptographiques ne donneront pas lieu à des attaques. Ceci est important tout particulièrement quand différentes applications, dont certaines hostiles, utilisent le même cache mémoire. Dans un satellite en orbite, avec un algorithme en dur dans un FPGA, on peut remettre en question la crédibilité d'un tel contexte et donc l'utilisation des algorithmes temps constant, souvent coûteux, et il est intéressant d'étudier quels seraient les gains possibles en renonçant à cette propriété.

Enfin au niveau de la modélisation de l'attaquant il est possible de reprendre l'analyse de sécurité des différents protocoles si on remet en question certaines des contraintes qu'il est courant d'accepter dans le modèle IT. Par exemple, au niveau des signatures, le NIST demande à ce que les candidats résistent à des attaquants ayant accès à 2^{64} signatures. Dans un contexte satellite on peut considérer qu'un nombre bien moindre si on contraint le signataire à ne pas réaliser plus de par exemple 2^{32} = 4 milliards de signatures, voire 2^{10} = 1024 signatures si par exemple l'objectif est de signer des mises à jour du firmware du satellite.

Un autre exemple est celui des transformations utilisées par de nombreux candidats pour résister à un attaquant dans le modèle QROM (oracle aléatoire quantique). Classiquement, on se contente du modèle ROM (oracle aléatoire classique) ce qui donne lieu à des transformations moins coûteuses, mais il a été prouvé qu'un attaquant quantique est strictement plus puissant que l'attaquant considéré dans le modèle ROM, d'où l'utilisation du modèle QROM qui prend en compte ce pouvoir supplémentaire de l'attaquant quantique. Ceci étant, il n'existe aucune attaque quantique connue efficace contre un candidat à la

---

[2] Pour une description de la problématique du temps constant voir https://www.bearssl.org/constanttime.html

standardisation qui utiliserait une transformation prouvée dans le modèle ROM. Il est donc intéressant d'étudier le surcoût des transformations QROM et envisager les alternatives.

4. Références

1. AGUILAR MELCHOR C., GABORIT P,. "Procédé et dispositifs cryptographiques de protection de données privées", brevet mondial, référence en France n°09/58598 du 2 décembre 2009
2. AGUILAR MELCHOR C., BLAZY O., DENEUVILLE JC., GABORIT P., ZEMOR G., "Efficient Encryption From Random Quasi-Cyclic Codes", IEEE Trans. Information Theory 64(5): 3927-3943 (2018)

Ces deux premières références correspondent au mécanisme générique d'échange de clés utilisé par l'ample majorité des candidats à la standardisation du NIST pour un échange de clés post-quantique (qu'ils soient fondés sur les réseaux euclidiens ou sur les codes). La publication de 2008 est un brevet décrivant ce mécanisme et celle de 2018 une preuve formelle de la sécurité que ce mécanisme apporte dans le cas particulier des codes correcteurs.

3. Carlos Aguilar Melchor, Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, Gilles Zemor ; BIKE: Bit Flipping Key Encapsulation ; NIST Candidate ; https://bikesuite.org/
4. Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jurjen Bos, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor ; HQC (Hamming Quasi-Cyclic) ; NIST Candidate ; https://pqc-hqc.org/
5. Carlos Aguilar Melchor, Nicolas Aragon, Magali Bardet, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Ayoub Otmani, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zemor ; ROLLO (Rank-Ouroboros, LAKE and LOCKER ; NIST Candidate ; https://pqc-rollo.org/
6. Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Alain Couvreur, Jean-Christophe Deneuville, Phillippe Gaborit, Adrien Hauteville, Gilles Zemor ; RQC (Rank Quasi-Cyclic) ; NIST Candidate ; http://pqc-rqc.org/

Ces quatre références correspondent à 4 des 17 candidats encore en lice pour la standardisation post-quantique (échanges de clés) pour lesquelles les encadrants forment partie des porteurs.

Enfin, le directeur de thèse a été le responsable scientifique des R&T R-S3/RE-0003-011 et R-S16/RE-0003-011 proposées par le CNES où il était demandé de traiter explicitement le cas de la cryptographie post-quantique pour l'injection de clés à distance dans un contexte satellitaire.