Description de l'offre

Votre rôle est d'effectuer une thèse en cryptographie à clé secrète sur l'impact d'un attaquant quantique dans les télécommunications.

Il est aujourd'hui difficile de savoir quand les ordinateurs quantiques feront partie de notre quotidien. Néanmoins l'existence future de ces machines est largement admise et impose de s'attaquer dès à présent au bouleversement qu'elles vont entraîner. La cryptographie étant omniprésente dans notre quotidien (communications téléphoniques, navigations Internet, objets connectés), il est essentiel de comprendre l'impact des ordinateurs quantiques et trouver des alternatives aux mécanismes cryptographiques actuels viables dans un tel monde quantique.

En cryptographie à clé publique, l'état des lieux est relativement clair : l'algorithme de Shor permettrait à un ordinateur quantique de casser tous les mécanismes cryptographiques couramment utilisés aujourd'hui. Mais des alternatives post-quantiques existent et sont maintenant largement étudiées [12].

En cryptographie à clé secrète, si l'algorithme quantique de Grover [6] impose de doubler la taille des clés utilisées, la recherche a aussi montré qu'il était possible d'utiliser l'intrication et la superposition quantiques, mises en oeuvre par les algorithmes de Grover, Simon [14] ou Kuperberg [10], pour réaliser de nouvelles cryptanalyses.

Certains résultats récents s'appuient sur un tel attaquant quantique pour réaliser des cryptanalyses meet-in-the-middle [4], linéaires et différentielles [9], ou par collisions [3,7]. De plus, des attaques quantiques sur des algorithmes cryptographiques ou modes opératoires aujourd'hui déployés ont également été proposées : chiffrement par bloc Prince [11], chiffrement authentifié AEZ [8,13] ou le MAC Poly1305 [2]. Ces résultats sont obtenus soit par la transposition d'attaques classiques dans un contexte quantique, soit par de nouvelles approches qui prennent en compte les capacités nouvelles dont dispose l'attaquant. Dans le monde des télécommunications, de nombreux algorithmes cryptographiques (AES, Milenage, SNOW, ZUC, etc.) et modes opératoires (CBC, CTR, XTS, CCM, GCM, etc.) pourraient ainsi être susceptibles d'être attaqués.

Au-delà de l'existence d'une attaque quantique contre un algorithme de chiffrement ou d'intégrité, il est aussi primordial d'étudier la résistance des systèmes cryptographiques qui mettent en oeuvre ces algorithmes. Ce contexte plus global est étudié par le biais d'un modèle qui décrit le système analysé et les pouvoirs dont peut disposer l'attaquant. Il s'agit alors soit de montrer qu'une attaque est possible, soit de prouver la sécurité du système. Il existe à ce jour plusieurs modèles d'attaque quantique tels que l'attaque par superposition [5] ou l'attaque quantique à texte chiffré choisi [1]. Le lien possible entre attaquant classique et attaquant quantique est aussi une cible de recherche potentielle [15]. Dans le monde des

télécommunications, certains protocoles ont été attaqués (TLS 1.2, GP SCP02, LoRaWAN 1.0) et pour d'autres (TLS 1.3, GP SCP03, LoRaWAN 1.1, etc.), une preuve de sécurité a été proposée. Les preuves de sécurité existantes ne prennent pas en compte, la plupart du temps, les nouvelles fonctionnalités d'un tel attaquant (techniques de rembobinage ou tables de consultation à adapter, gestion différente des oracles, gestion des mesures quantiques, etc.). Elles doivent donc être revues et adaptées en conséquence.

L'objectif de la thèse sera d'étudier ces attaques et leurs impacts sur les protocoles et algorithmes du monde des télécommunications (réseaux 2G à 5G, protocole TLS, cartes multi-applicatives Global Platform, Internet des Objets LoRaWAN, etc.).

L'objectif de la thèse est d'étudier l'impact des ordinateurs quantiques sur les mécanismes cryptographiques à clé secrète utilisés par un opérateur de télécommunications. Plus précisément, la thèse devra porter sur :

· les modèles d'attaquants quantiques afin de trouver les plus pertinents par rapport aux protocoles mis en oeuvre par un opérateur de télécommunications ;
· les algorithmes quantiques permettant d'attaquer les algorithmes de cryptographie à clé secrète. Ces algorithmes pourront être soit déjà existants dans la littérature, soit adaptés d'un ou plusieurs algorithmes existants, soit créés pour le besoin de la thèse (voire à portée plus large) ;
· les cryptanalyses de primitives de cryptographie à clé secrète (à blocs ou à flot tels qu'AES, Milenage, SNOW ou ZUC) et de modes opératoires (ex : CBC, CTR, XTS, CCM, GCM). Ces cryptanalyses pourront être soit dédiées à un algorithme particulier, soit plus génériques en considérant un type d'attaque et de modèle d'attaquant relatif à une famille d'algorithmes. Ces cryptanalyses pourront aboutir à trois types de résultats au moins : (i) une variante plus efficace d'attaques existantes obtenue en considérant le contexte d'un attaquant quantique, (ii) une nouvelle attaque mettant en oeuvre des algorithmes quantiques dédiés, (iii) une argumentation montrant que les attaques existantes ne sont pas plus dévastatrices dans un monde post-quantique ;
· la façon dont il est possible de modifier un algorithme cryptographique ou un mode opératoire pour qu'il soit moins faillible (voire résistant) à une attaque quantique existante ;
· des constructions d'algorithmes ou de modes opératoires résistants aux attaques quantiques existantes dans la littérature ;
· les preuves de sécurité de protocoles cryptographiques dans le cas d'un attaquant quantique.

Ces différents éléments devront être menés de front, en fonction de la bibliographie qui est encore naissante dans ce domaine et qui sera certainement très active avant le démarrage et tout au long de la thèse

Références :

[1] Boneh, D., Zhandry, M.: Secure signatures and chosen ciphertext security in a quantum computing world. Crypto 2018.

[2] Bonnetain, X., Naya-Plasencia, M.: Hidden shift quantum cryptanalysis and implications. Asiacrypt 2018.

[3] Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An efficient quantum collision search algorithm and implications on symmetric cryptography. Asiacrypt 2017.

[4] Chevalier, C., Kaplan, M., Vu, Q.H.: On the Everlasting Security of Password Authenticated Quantum Key Exchange. CoRR abs/1904.

[5] Damgärd, I., Funder, J., Nielsen, J.B., Salvail, L.: Superposition attacks on cryptographic protocols. ICITS 2013.

[6] Grover, L.K.: A fast quantum mechanical algorithm for database search. STOC 1996.

[7] Hosoyamada, A., Sasaki, Y., Xagawa, K.: Quantum multicollision-finding algorithm. Asiacrypt 2017.

[8] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. Crypto 2016.

[9] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Quantum differential and linear cryptanalysis. IACR Trans. Symmetric Cryptol. 2016.

[10] Kuperberg, G.: Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. TQC 2013.

[11] Leander, G., May, A.: Grover meets Simon - quantumly attacking the FX-construction. Asiacrypt 2017.

[12] NIST: Post-Quantum Cryptography.

[13] Santoli, T., Schaffner, C.: Using Simon's Algorithm to Attack Symmetric-key Cryptographic Primitives. Quantum Info. Comput.

[14] Simon, D.R.: On the power of quantum cryptography. SIAM J. Comput.

[15] Zhandry, M.: How to construct quantum random functions. FOCS 2012.