ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

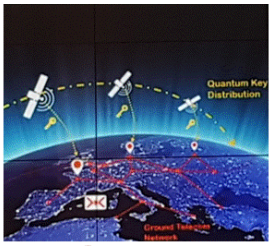
Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité » n°63
Lundi 20 Novembre 2023

Quand tout devient quantique : ordinateurs, communications, algorithmes résistants

Par **webinaire** Zoom

Lundi 20 novembre
18h00-20h00



Quand tout devient quantique : ordinateurs, communications, algorithmes résistants.

Professeur Jean-Jacques Quisquater
Université de Louvain (Belgique)
Docteur d'État en science informatique

Compte-rendu rédigé par Clarisse Veron,
étudiante en Master 1 Cybersécurité et E-santé - Université Paris Cité

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 1 Cybersécurité et E-santé

SOMMAIRE

Introduction

Le "Lundi de la Cybersécurité" n°63, intitulé "Quand tout devient quantique : ordinateurs, communications, algorithmes résistants," s'est tenu à un moment où l'urgence de sécuriser les données sensibles émises hier et aujourd'hui est devenue une priorité mondiale. Dans un paysage technologique où les avancées en cryptographie quantique évoluent rapidement, l'industrie européenne se trouve face à un défi majeur pour rester compétitive et sécurisée. Une veille importante pour tous les acteurs du domaine est essentielle pour anticiper et s'adapter aux évolutions, notamment en réponse à des initiatives telles que le développement de standards propres par la Chine.

L'événement, orchestré par des experts de renom tels que le Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks, a rassemblé une communauté engagée de professionnels et de chercheurs pour explorer ces questions urgentes. L'objectif était de démystifier la technologie quantique et ses implications pour la cryptologie, et de souligner l'importance d'une réponse proactive et informée aux défis posés par ces technologies émergentes.

Objectif de la Conférence :

L'objectif principal de cette conférence est d'explorer et de démystifier le monde en rapide évolution de la technologie quantique et ses implications dans le domaine de la cryptologie. La conférence vise à établir une compréhension claire des différences et des liens entre trois domaines clés : les technologies quantiques appliquées à la cryptologie, les calculateurs quantiques, et la cryptologie post-quantique. Chaque domaine présente des défis uniques et des opportunités potentielles dans notre paysage technologique en mutation.

Contexte et Intervenants :

Nous sommes à une époque où la maturité croissante des calculateurs quantique présente à la fois des opportunités et des menaces pour les systèmes de chiffrement existant. Ces systèmes, y compris les algorithmes de chiffrement asymétriques comme le RSA, sont menacés par la puissance de calcul des calculateurs quantiques. Parallèlement, la cryptologie post-quantique

se profile comme une évolution indispensable, offrant une résistance aux tentatives de décryptement par ces puissants calculateurs.

D'autre part, les technologies quantiques offrent des innovations significatives dans la distribution quantique de clés (QKD) et la génération de nombres aléatoires, exploitant les propriétés uniques de l'intrication quantique pour améliorer la sécurité dans le chiffrement symétrique.

La conférence accueille le professeur Jean-Jacques Quisquater, un cryptologue belge de renom, comme principal intervenant. Professeur à l'université catholique de Louvain et membre de l'ARCSI, M. Quisquater apporte une expertise considérable à cette discussion. Avec un doctorat en science informatique de l'université d'Orsay et une affiliation à l'IEEE, il est également co-inventeur du schéma d'identification Guillou-Quisquater et membre de l'académie royale de Belgique. Sa vaste expérience en cryptographie à l'ENS-Ulm et en tant que chercheur associé au MIT lui permet d'offrir des perspectives uniques et approfondies sur les sujets abordés.

Cette conférence promet d'être une exploration exhaustive des derniers développements dans le domaine de la cryptologie quantique et post-quantique, mettant en lumière les défis, les opportunités et les implications géopolitiques de ces avancées technologiques. Avec la contribution d'éminents experts, dont plusieurs Prix Nobel, elle se positionne comme une ressource essentielle pour comprendre l'état actuel et futur de la cryptographie dans un monde où "tout devient quantique".

I. Aperçu de la mécanique quantique et ses applications

Dans son discours, Jean-Jacques Quisquater met en lumière l'importance de la mécanique quantique et ses applications pratiques dans divers domaines. Selon l'intervenant, bien que la mécanique quantique ait été perçue comme un domaine largement théorique, elle a trouvé des applications concrètes dans plusieurs secteurs technologiques.

Le Pr Quisquater souligne que les transistors, éléments fondamentaux de l'électronique moderne, sont une application directe de la mécanique quantique. Ces composants utilisent des principes quantiques pour réguler le flux électrique dans les circuits, illustrant ainsi l'impact des phénomènes quantiques sur la technologie quotidienne.

L'intervenant aborde ensuite la communication quantique, un domaine où la mécanique quantique joue un rôle crucial. Il explique que la distribution quantique de clés (QKD) s'appuie sur l'intrication quantique pour assurer une sécurité accrue dans l'échange de clés de chiffrement symétriques. Cette technologie représente un progrès majeur dans la sécurisation des communications.

En ce qui concerne le calcul quantique, l'intervenant décrit comment les ordinateurs quantiques, utilisant des qubits capables de superposer plusieurs états « O » et « 1 », offrent des capacités de traitement d'informations bien au-delà de celles des ordinateurs classiques. Ces systèmes ont

le potentiel de transformer radicalement des domaines variés, allant de la cryptographie à la recherche pharmaceutique.

En conclusion, Jean-Jacques Quisquater affirme que la mécanique quantique a dépassé les limites des laboratoires de physique pour devenir un moteur d'innovation dans de nombreux secteurs technologiques. Ses applications dans les transistors, la communication et le calcul quantique témoignent de son rôle essentiel dans le développement de technologies avancées.

II. La cryptographie quantique

Dans la deuxième partie de sa conférence, Jean-Jacques Quisquater se concentre sur les défis et les opportunités offerts par la cryptographie quantique. Il met en évidence deux aspects cruciaux de cette technologie : la distribution de clés sécurisées et la génération de clés secrètes.

L'un des points forts abordés par l'intervenant concerne la distribution quantique de clés (QKD). Selon le Pr Quisquater, cette technologie représente une avancée majeure dans le domaine de la sécurité des communications. La QKD utilise les propriétés uniques de l'intrication quantique pour garantir qu'une clé de chiffrement partagée entre deux parties ne peut être compromise sans que cela soit détecté. Cette méthode de distribution de clés offre une sécurité nettement supérieure à celle des méthodes classiques, rendant toute interception ou écoute indiscernable pratiquement impossible car les qubits subissent une décorrélation.

En outre, l’expert discute de la capacité des systèmes quantiques à générer des nombres réellement aléatoires, ce qui est essentiel pour la création de clés secrètes robustes. Contrairement aux ordinateurs classiques, qui ne peuvent produire que des nombres pseudo-aléatoires, les systèmes quantiques exploitent les phénomènes d'intrication et de décorrélation pour produire des séquences de nombres véritablement aléatoires. Cette caractéristique est cruciale pour la cryptographie, car la force d'une clé de chiffrement repose en grande partie sur son caractère imprévisible et donc aléatoire.

En conclusion, cette partie de la conférence de Jean-Jacques Quisquater souligne l'importance croissante de la cryptographie quantique dans un monde où la sécurité des informations devient de plus en plus critique. Les avancées dans la distribution de clés sécurisées et la génération de clés secrètes ouvrent de nouvelles perspectives pour la protection des données dans diverses applications, allant de la communication sécurisée aux transactions financières. Ces développements indiquent un changement de paradigme dans la manière dont la confidentialité et la sécurité des données sont abordées à l'ère de l'informatique.

III. Algorithmes quantiques et leur impact sur la cryptographie

Dans la troisième partie de sa conférence, Jean-Jacques Quisquater se penche sur l'impact significatif des ordinateurs quantiques sur les algorithmes cryptographiques actuels. Il aborde en particulier les algorithmes de Shor pour les clés asymétriques et de Grover pour les clés symétriques, qui jouent un rôle central dans le domaine de la cryptanalyse.

L'intervenant commence par discuter de l'algorithme de Shor, connu pour sa capacité à factoriser de grands nombres en un temps polynomial, une tâche extrêmement difficile pour les ordinateurs classiques. Mr Quisquater souligne que cet algorithme pose une menace sérieuse pour les systèmes de chiffrement à clé publique comme le RSA, actuellement largement utilisés pour sécuriser les communications sur Internet. Avec la mise en œuvre effective de l'algorithme de Shor sur des ordinateurs quantiques suffisamment puissants, ces systèmes de chiffrement pourraient devenir obsolètes, rendant nécessaire le développement de nouvelles méthodes de chiffrement résistantes aux attaques quantiques.

Ensuite, l'intervenant se concentre sur l'algorithme de Grover, qui offre un moyen d'accélérer de manière significative la recherche dans une base de données non triée. Cet algorithme a des implications importantes pour la cryptographie symétrique, car il permet de réduire de moitié la longueur effective de la clé de chiffrement. Par exemple, une clé symétrique de 128 bits, considérée comme sûre dans le cadre classique, pourrait être compromise en utilisant l'algorithme de Grover, nécessitant donc potentiellement le doublement de la longueur des clés pour maintenir un niveau de sécurité équivalent face aux attaques quantiques.

Mr Quisquater conclut cette partie en soulignant l'urgence pour la communauté cryptographique de développer et d'adopter de nouveaux algorithmes résistant aux attaques quantiques. L'avènement des ordinateurs quantiques performants ne rendra pas seulement certains algorithmes actuels vulnérables, mais ouvrira également la voie à de nouvelles méthodes de cryptanalyse. Cette réalité conduit à une course entre le développement de la technologie quantique et la mise en place de systèmes de chiffrement capables de résister à ces nouveaux défis, les chiffrements dits « post-quantiques ». Enfin, l'intervenant insiste sur l'importance de la collaboration internationale et de la recherche continue pour assurer la sécurité des données à l'ère quantique.

IV. Migration vers la cryptographie post-quantique

Dans la quatrième partie de sa conférence, Jean-Jacques Quisquater aborde la transition nécessaire vers la cryptographie post-quantique. Cette section met l'accent sur la nécessité impérieuse d'adopter de nouveaux algorithmes cryptographiques capables de résister aux attaques menées par des ordinateurs quantiques.

Jean-Jacques Quisquater souligne d'abord l'urgence avec laquelle la communauté cryptographique doit répondre à la menace que représentent les ordinateurs quantiques pour les systèmes de chiffrement actuels. Il explique que les algorithmes de chiffrement traditionnels, tels que le RSA et l'ECC (Elliptic Curve Cryptography), ne sont pas suffisamment robustes face à des attaques quantiques. Par conséquent, il devient crucial de développer et d'implémenter des systèmes cryptographiques dits "post-quantiques" qui peuvent garantir la sécurité des données même dans un contexte où les capacités de calcul quantique sont pleinement exploitées.

L'intervenant aborde ensuite les défis associés à cette transition. Un des principaux défis est la complexité accrue et les exigences de performance des nouveaux algorithmes

cryptographiques. Ces algorithmes doivent être conçus non seulement pour résister aux attaques quantiques, mais aussi pour être efficaces et pratiques à utiliser dans diverses applications.

L'intervenant examine aussi les stratégies pour une transition réussie vers la cryptographie post-quantique. Il évoque l'importance de la recherche et du développement continus pour identifier et valider des algorithmes sécurisés. En outre, il souligne la nécessité d'une coopération internationale pour établir des normes et des protocoles communs, garantissant ainsi une transition harmonieuse et sécurisée vers des systèmes cryptographiques adaptés à l'ère quantique.

La partie se conclut sur l'assertion que la migration vers la cryptographie post-quantique n'est pas seulement une mesure de précaution, mais une nécessité impérative pour l'avenir de la sécurité des données. Jean-Jacques insiste sur le fait que cette transition doit être abordée avec diligence et prudence, en tenant compte des dernières avancées en cryptographie quantique et en adaptant continuellement les approches pour contrer les menaces émergentes. Cette démarche proactive est essentielle pour assurer la protection des données à l'ère de l'informatique quantique.

V. Aspects géopolitiques

Dans la cinquième et dernière partie de sa conférence, Jean-Jacques Quisquater explore les aspects géopolitiques de la cryptographie quantique, mettant en lumière son importance pour la sécurité nationale et internationale.

Mr Quisquater souligne que la cryptographie quantique n'est pas seulement une question technique, mais aussi un enjeu géopolitique majeur. Avec la montée en puissance des ordinateurs quantiques, les nations du monde entier reconnaissent l'importance stratégique de maîtriser cette technologie. La capacité à protéger ou à craquer des systèmes cryptographiques a des implications directes pour la sécurité nationale, notamment dans les domaines du renseignement, de la défense et de la diplomatie.

L'intervenant aborde la course à la suprématie quantique entre les grandes puissances mondiales, en particulier entre les États-Unis et la Chine. Cette course a des ramifications profondes, car la domination dans le domaine quantique pourrait offrir un avantage significatif en matière de cybersécurité et de capacités de renseignement. Mr Quisquater note que l'Europe, bien que participant à cette course, semble pour l'instant être un acteur moins proéminent.

L’expert met en avant la dualité entre la nécessité de collaboration internationale pour le développement de normes et de protocoles en cryptographie quantique, et la compétition géopolitique pour le leadership technologique. Il souligne que, bien que la collaboration soit essentielle pour garantir une sécurité globale, les enjeux de souveraineté nationale et de puissance stratégique mènent souvent à une compétition intense.

En conclusion, Jean-Jacques Quisquater appelle à une prise de conscience de l'importance géopolitique de la cryptographie quantique. Il souligne que les progrès dans ce domaine ne sont pas seulement des réussites scientifiques et techniques, mais aussi des facteurs qui influencent le paysage géopolitique mondial. La capacité à naviguer dans cet équilibre délicat entre

coopération et compétition définira la manière dont les nations abordent la sécurité et la diplomatie à l'ère quantique.

Conclusion

La conférence, orchestrée par l'expert en cryptographie Jean-Jacques Quisquater, s'est achevée sur une note d'urgence et d'appel à la préparation proactive face aux progrès fulgurants dans le domaine de la cryptographie quantique. Cette clôture a mis en lumière la nécessité pour les gouvernements et les industries de s'adapter rapidement aux nouvelles réalités de la sécurité de l'information dans un monde où la technologie quantique prend une place de plus en plus centrale.

La séance interactive de questions-réponses a constitué un point culminant de la conférence, permettant un échange direct et dynamique entre le public et l'expert. Cette session, introduite par Gérard, l'organisateur de la conférence, a permis de plonger plus profondément dans les complexités et les nuances de la cryptographie quantique et post-quantique. Les participants, alliant professionnels et passionnés éclairés, ont soulevé des questions variées, abordant les défis techniques, les implications géopolitiques, et les perspectives dans le domaine de la sécurité des données.

Les réponses fournies par Jean-Jacques Quisquater ont non seulement clarifié plusieurs points complexes mais ont aussi enrichi la discussion avec des anecdotes et des informations complémentaires. Cette interaction a souligné la pertinence et l'intérêt des sujets traités, démontrant l'importance de la diffusion des connaissances en cryptographie dans un contexte technologique en évolution.

En conclusion, la conférence a offert une perspective précieuse et approfondie sur les défis et les opportunités que présente la cryptographie quantique et post-quantique. Elle a rappelé l'importance d'une approche proactive et adaptée pour garantir la sécurité de l'information à l'ère de l'informatique quantique. Les échanges lors de la séance de questions-réponses ont renforcé l'engagement de la communauté vers une compréhension plus profonde et une préparation efficace face à ces changements imminents. Gérard Peliks, en concluant la séance, a non seulement remercié Jean-Jacques pour sa contribution significative mais a aussi souligné l'importance des futures rencontres organisées par l'ARCSI, encourageant la participation active pour continuer à explorer ces sujets cruciaux.