COMMUNIQUÉ DE PRESSE

Singapour, le 5 novembre 2024

La Banque de France et l'Autorité Monétaire de Singapour réalisent une expérimentation en matière de cryptographie post-quantique pour renforcer la sécurité des communications

La Banque de France (BDF) et l'Autorité Monétaire de Singapour (MAS) ont annoncé aujourd'hui le succès d'une expérimentation conjointe en matière de cryptographie post-quantique (PQC) menée sur plusieurs continents, en utilisant les technologies Internet conventionnelles. L'expérience PQC vise à renforcer la sécurité des communications et des données face aux avancées de l'informatique quantique. La réussite de cette expérimentation marque une étape cruciale dans l'évolution de la protection des communications électroniques internationales face aux menaces en matière de cybersécurité posées par l'informatique quantique.

L'initiative conjointe BDF-MAS a permis l'utilisation d'algorithmes cryptographiques résistant aux technologies quantiques pour la signature et le chiffrement d'e-mails. L'objectif est de maintenir le niveau de sécurité actuel des communications électroniques dans le futur, tout en conservant la compatibilité avec les normes, technologies et canaux de communication digitaux existants. Dans ce contexte, les e-mails sont particulièrement sensibles, puisqu'un e-mail chiffré est susceptible de transporter des informations confidentielles, ce qui en fait une cible privilégiée pour des cyberattaques. Cette initiative démontre non seulement la faisabilité pratique de ces nouvelles méthodes de sécurité, mais aussi leur efficacité dans des environnements applicatifs déjà largement adoptés.

Une approche hybride pour une sécurité maximale

Le projet a suivi une approche hybride, alliant la robustesse des algorithmes actuels à celle des algorithmes post-quantiques, afin d'assurer la sécurité et la compatibilité avec les systèmes existants tout en se préparant à l'arrivée de la menace quantique.

Une ambition de sécurité quantique

Un rapport technique détaillant les résultats et les enseignements de l'expérience a été publié aujourd'hui. Voici ci-dessous les principales conclusions du rapport :

a) En utilisant Microsoft Outlook comme client de messagerie associé à un plugin d'e-mail PQC, la BDF et la MAS ont réussi à échanger des e-mails signés numériquement et chiffrés à l'aide d'algorithmes PQC, à savoir CRYSTALS-Dilithium et CRYSTALS-Kyber.

b) La standardisation des algorithmes et bibliothèques cryptographiques PQC pour les signatures numériques et le chiffrement n'est pas suffisante. Les protocoles d'application et les normes actuelles, comme l'infrastructure à clé publique, les certificats numériques, les échanges de clés ou les e-mails sécurisés, doivent

également être standardisés pour intégrer les algorithmes cryptographiques PQC. Cela facilitera l'adoption et l'interopérabilité de la PQC.

c) Il existe un potentiel d'intégration de cette technologie dans les réseaux de paiement. En intégrant des algorithmes PQC dans les réseaux de paiement, les institutions financières peuvent préparer leurs mesures de sécurité face à la menace imminente de l'informatique quantique, garantissant l'intégrité et la confidentialité à long terme des données financières sensibles.

Un engagement fort pour la sécurité future des systèmes financiers

La BDF et la MAS continueront à collaborer lors de la prochaine étape de l'expérimentation, afin d'étendre la PQC aux transactions financières critiques, en particulier aux transactions transfrontalières sur les réseaux de paiement.
En collaborant pour cette expérimentation pionnière, la BDF et la MAS affirment leur engagement à anticiper les menaces futures et à garantir la sécurité des systèmes financiers mondiaux. Cette initiative souligne également l'importance de la coopération internationale pour faire face aux menaces cybernétiques émergentes.

Denis Beau, Premier Sous-gouverneur de la BDF, a déclaré : *« Bien que l'informatique quantique ouvre de nouvelles perspectives prometteuses dans divers domaines, elle représente également une menace en matière de sécurité numérique, notamment pour la protection de nos communications. C'est à ce titre que la Banque de France, en sa qualité de banque centrale, anticipe et multiplie les expérimentations sur la cryptographie post-quantique avec ses partenaires depuis 2022. Les résultats de cette première coopération avec l'Autorité Monétaire de Singapour dans le domaine de la cryptographie post-quantique sont de nature à nous rassurer sur notre capacité à rendre résilientes nos communications interinstitutionnelles. Nous nous félicitons que cette coopération puisse continuer dans une seconde phase. »*

Jacqueline Loh, Directrice Générale Adjointe (Développement Corporatif) de la MAS, a déclaré : *« La menace imminente du déchiffrement par des ordinateurs quantiques transforme les stratégies de cybersécurité dans les services financiers à l'échelle mondiale. L'accent est désormais mis sur l'agilité cryptographique et sur l'adaptation des systèmes en intégrant des algorithmes résistants aux technologies quantiques. Les institutions financières qui se préparent tôt à l'ère quantique ne se contenteront pas de réduire les risques futurs, elles se positionneront également pour maintenir la confiance du public dans les services financiers numériques. Les efforts de collaboration avec la BDF en matière de cryptographie post-quantique ont été extrêmement précieux pour la MAS. Nous sommes reconnaissants de cette opportunité de travailler ensemble sur une initiative aussi cruciale et nous sommes impatients de poursuivre notre collaboration pour renforcer la résilience quantique. »*

Qu'est-ce que l'information quantique ?

L'informatique quantique utilise les principes de mécanique quantique, des mathématiques avancées et d'ingénierie informatique pour réaliser certains types de calculs à une vitesse inatteignable par les ordinateurs conventionnels. Contrairement aux ordinateurs actuels, qui traitent l'information sous forme binaire (bits), les ordinateurs quantiques utilisent des qubits. Les principes mathématiques qui s'appliquent aux qubits permettent aux ordinateurs quantiques un parallélisme massif du traitement des informations. Les ordinateurs quantiques peuvent ainsi résoudre plus rapidement certains problèmes complexes. Bien que toujours en développement, cette technologie pourrait révolutionner de nombreux secteurs, mais aussi représenter une menace pour la sécurité des systèmes cryptographiques actuels.

Qu'est-ce que la cryptographie post-quantique ?

La cryptographie post-quantique désigne un ensemble de techniques et d'algorithmes cryptographiques conçus pour résister aux capacités des futurs ordinateurs quantiques. Ces machines, bien plus puissantes que les ordinateurs classiques, pourraient casser la cryptographie asymétrique, compromettant ainsi la sécurité des données et des communications. La cryptographie post-quantique vise à développer des méthodes de protection inviolables même par des technologies quantiques avancées.

À propos de la Banque de France. Institution indépendante, la Banque de France a trois grandes missions : la stratégie monétaire, la stabilité financière, les services à l'économie et à la société. Elle contribue à définir la politique monétaire de la zone euro et la met en œuvre en France ; elle contrôle banques et assurances et veille à la maîtrise des risques ; elle propose de nombreux services aux entreprises et aux particuliers.
Visitez notre site internet www.banque-france.fr
Suivez nous

À propos du Lab : Centre d'open innovation de la Banque de France, Le Lab agit comme un catalyseur pour détecter les opportunités, mener des expérimentations avec les experts de la DGSI et identifier les solutions qui permettront de co-construire la banque centrale de demain.

L'Autorité monétaire de Singapour (MAS) est la banque centrale de Singapour et l'organisme de régulation financière intégrée. En tant que banque centrale, la MAS promeut une croissance économique durable et non inflationniste par la conduite conjointe de la politique monétaire et de surveillances et analyses macroéconomiques. Elle gère le taux de change de Singapour, les réserves officielles de change et la liquidité du secteur bancaire. En tant que superviseur financier intégré, la MAS favorise un secteur des services financiers solide grâce à sa surveillance prudentielle de toutes les institutions financières à Singapour : banques, assureurs, intermédiaires de marchés financiers, conseillers financiers et infrastructures de marché. Elle est également responsable du bon fonctionnement des marchés financiers, d'une conduite saine et de l'éducation des investisseurs. La MAS collabore également avec l'industrie financière pour promouvoir Singapour en tant que centre financier international dynamique. Elle facilite le développement d'infrastructures, l'adoption de technologies et la montée en compétences dans le secteur financier. Pour plus d'informations, veuillez visiter https://www.mas.gov.sg

Contacts presse :

- Service de presse Banque de France

presse@banque-france.fr | +33 (0)1 42 92 39 00

- Monetary Authority of Singapore

Hidayah Rahim, Directrice Adjointe de la communication
hidayah_rahim@mas.gov.sg | +65 64225609