IDEMIA annonce la première technologie SIM 5G résistante à l'ordinateur quantique au monde

IDEMIA est fière d'annoncer l'utilisation d'un algorithme résistant à l'ordinateur quantique dans une carte SIM 5G pour protéger les données et la vie privée des abonnés face au danger que représente l'ordinateur quantique.

 # CONNECTIVITÉ

POSTÉ LE 17.12.21

IDEMIA est fière d'annoncer l'utilisation d'un **algorithme post-quantique** dans une **carte SIM 5G** pour **protéger les données et la vie privée** des abonnés face au danger que représente l'ordinateur quantique.

Première mondiale dans le domaine des télécommunications, cette carte SIM 5G post-quantique utilise un algorithme cryptographique à clé publique sélectionné par le NIST comme candidat à la première norme de protection contre la menace d'une attaque quantique.

Portée à l'attention du public il y a plus de 20 ans, la révolution quantique va bientôt décupler ce risque. Imaginez un ordinateur en mesure d'exécuter des algorithmes en s'appuyant sur un système quantique pour déchiffrer instantanément des secrets qui, autrement, resteraient totalement inviolables. Cette hypothèse se concrétisera inéluctablement dans les prochaines années. IDEMIA, en tant que leader dans les domaines de la sécurité et de la cryptographie, travaille assidûment pour anticiper la menace quantique et développer les défenses nécessaires à une sécurité sans faille. Les ordinateurs quantiques sont en effet en passe de pénétrer tout ce qui semble aujourd'hui impénétrable, notamment les systèmes de chiffrement.

La révolution quantique est une formidable opportunité. Elle est très prometteuse pour de nombreuses industries, à condition d'anticiper les risques. Nous préparons aujourd'hui les vaccins technologiques de demain, notamment pour maintenir la sécurité des systèmes critiques et la protection des données chiffrées.

Marc BERTIN, CTO SET chez IDEMIA

La technologie 5G est déjà à la pointe en termes de protection de la vie privé des abonnés en chiffrant l'identifiant

international d'abonnement mobile (IMSI). En ajoutant des algorithmes post-quantiques, IDEMIA en fait **un bouclier absolu pour la protection de la vie privée**.

Pourquoi maintenant ? L'informatique quantique fait des progrès à pas de géants pour décupler la puissance de calcul disponible, permettant de résoudre des problèmes complexes en quelques secondes ou minutes, au lieu d'un milliard d'années avec les technologies classiques pour déchiffrer la cryptographie asymétrique. Ce type d'ordinateur représente un nouveau danger pour la sécurité des données et une menace pour la vie privée des citoyens car, à l'ère quantique, toutes les données traitées, stockées et sécurisées avec la cryptographie actuelle pourront être piratées. La révolution quantique pourrait devenir une réalité d'ici 5 à 10 ans, il est donc important de s'y préparer dès aujourd'hui. Tout se joue maintenant, notamment pour les secrets transmis par les réseaux de télécommunications qui auront encore de la valeur dans les 10 prochaines années, comme par exemple les informations personnelles.

IDEMIA travaille actuellement avec certains des principaux opérateurs mobiles mondiaux sur les sujets de recherche et le développement de solutions pour protéger l'industrie des télécommunications contre les attaques quantiques.

À la pointe de l'innovation en matière de protection des données sensibles, le département Recherche & Développement d'IDEMIA travaille depuis longtemps sur des solutions pour défendre la société face au défi quantique et identifier les innovations technologiques qui prépareront l'industrie au monde de demain.

---

* National Institute of Standards and Technology
