

RAPPORT DE VEILLE – MARS-AVRIL 2025

18/04/2025

Introduction

La communication quantique est un domaine de la physique appliquée et des technologies de l'information qui exploite les lois de la mécanique quantique pour transmettre de l'information de manière extrêmement sécurisée. Contrairement à la communication classique, la communication quantique utilise les propriétés des particules subatomiques, comme l'intrication ou la superposition, pour assurer une transmission inviolable. L'une de ses applications les plus concrètes est la distribution quantique de clés (QKD), qui permet de générer et échanger des clés de chiffrement impossibles à intercepter sans être détecté. En plus de cela, elle se base sur la génération de clés de chiffrement de manière réellement aléatoire et non en suivant un protocole. Accentuant ainsi de manière très significative la sécurité de la transmission d'information.

Les mois de mars et avril 2025 ont été riches en innovations dans ce domaine. Ce rapport propose une synthèse des événements marquants, allant de la sélection d'un nouvel algorithme post-quantique par le NIST, à la réalisation d'un record mondial de liaison quantique par satellite, en passant par des initiatives de cybersécurité d'entreprises privées et des démonstrations technologiques inédites au Royaume-Uni.

Développements récents

Le NIST sélectionne HQC comme cinquième algorithme pour le chiffrement post-quantique

Le 12 mars 2025, le NIST (National Institute of Standards and Technology) a annoncé la sélection de l'algorithme HQC (Hamming Quasi-Cyclic) comme solution de secours pour les opérations de chiffrement dans un monde post-quantique. Ce choix s'inscrit dans la démarche de standardisation entamée par le NIST depuis plusieurs années, visant à doter les États-Unis – et potentiellement le monde – d'outils cryptographiques résistants à de futures attaques par ordinateurs quantiques. L'adoption de HQC comme alternative robuste vient compléter les algorithmes déjà sélectionnés comme CRYSTALS-Kyber et Dilithium, et renforce la résilience du système global de cybersécurité face à un avenir incertain.

Source : <https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption>

Record de liaison satellite quantique de 12 900 km

Le 19 mars 2025, des chercheurs chinois ont établi un nouveau record mondial de liaison quantique par satellite, couvrant une distance de 12 900 km. Cette performance impressionnante a été réalisée à l'aide de la technologie de QKD à bord du satellite Micius,

permettant de sécuriser des communications intercontinentales entre l'Asie et l'Europe. Au-delà de la prouesse technique, cette démonstration confirme la faisabilité de réseaux quantiques à l'échelle planétaire, et constitue une étape stratégique dans la course à la domination technologique.

Source : <https://www.sciencedaily.com/releases/2025/03/250319142833.htm>

Lancement du premier service de cryptographie post-quantique par Unisys

Unisys, entreprise américaine spécialisée en cybersécurité, a lancé le 27 mars 2025 un service commercial de cryptographie post-quantique. Cette offre vise à évaluer la posture cryptographique des organisations, identifier les failles potentielles dans les systèmes existants, et mettre en place des algorithmes résistants aux attaques quantiques. Ce type d'initiative montre que le secteur privé anticipe déjà le basculement vers une ère post-quantique, et que la demande en solutions opérationnelles devient concrète.

Source : <https://www.unisys.com/news-release/unisys-launches-first-post-quantum-cryptography-service-to-block-future-security-threats>

Première communication quantique longue distance au Royaume-Uni

En avril 2025, des chercheurs britanniques ont réussi la première communication ultra-sécurisée à longue distance via un réseau quantique au Royaume-Uni. Cette transmission comprenait un appel vidéo entièrement chiffré par une technologie de QKD. Ce projet pilote, réalisé sur un réseau expérimental, prouve la viabilité d'une infrastructure nationale de communication quantique, et ouvre la voie à des applications gouvernementales, militaires, mais aussi commerciales dans les années à venir.

Source : <https://phys.org/news/2025-04-uk-distance-ultra-communication-quantum.html>

Journée mondiale de la science quantique

Le 14 avril 2025 a marqué la célébration du World Quantum Day, une journée internationale destinée à sensibiliser le grand public et les décideurs aux technologies quantiques. De nombreux événements ont souligné le lien entre avancées scientifiques et enjeux de cybersécurité, notamment l'importance de se préparer à l'arrivée des ordinateurs quantiques capables de casser les algorithmes classiques. Cette mobilisation mondiale est un signal fort du rôle croissant que jouera la physique quantique dans la société de demain.

Source : <https://www.tomsguide.com/computing/online-security/what-is-world-quantum-day>

Analyse

Les mois de mars et avril 2025 démontrent que l'anticipation des menaces post-quantiques est désormais une priorité non seulement pour les gouvernements, mais aussi pour les entreprises et la communauté scientifique internationale. La sélection d'un nouvel algorithme par le NIST montre la volonté d'élargir les standards et de renforcer la diversité algorithmique. Les démonstrations techniques (liaison satellite, réseaux longue distance) confirment que les infrastructures de communication quantique ne sont plus de simples

prototypes. Enfin, la sensibilisation du public et l'apparition de services privés marquent une transition vers l'industrialisation et la démocratisation des solutions post-quantiques.

Conclusion

Mars et avril 2025 marquent une nouvelle phase d'accélération dans le domaine de la cybersécurité quantique. La convergence entre standards internationaux, innovations techniques et initiatives industrielles donne forme à un écosystème cohérent. La prochaine étape résidera dans l'intégration à grande échelle de ces solutions, en parallèle d'un travail de normalisation et de formation des acteurs publics et privés aux nouveaux enjeux de sécurité numérique.

Sources

<https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption>

<https://www.sciencedaily.com/releases/2025/03/250319142833.htm>

<https://www.unisys.com/news-release/unisys-launches-first-post-quantum-cryptography-service-to-block-future-security-threats>

<https://phys.org/news/2025-04-uk-distance-ultra-communication-quantum.html>

<https://www.tomsguide.com/computing/online-security/what-is-world-quantum-day>

The screenshot shows the NIST website with the article "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption" dated March 11, 2025. The article text states that NIST has chosen HQC as a backup for ML-KEM, noting that HQC is based on different math and that NIST plans to issue a draft standard in 2025 and a finalized one in 2027. The page includes a media contact for Chad Boutin and lists the Information Technology Laboratory and Computer Security Division as the responsible organizations. A decorative banner at the bottom contrasts "OLD ENCRYPTION" with "NEW ENCRYPTION".

NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

March 11, 2025

- NIST has chosen a new algorithm for post-quantum encryption called HQC, which will serve as a backup for ML-KEM, the main algorithm for general encryption.
- HQC is based on different math than ML-KEM, which could be important if a weakness were discovered in ML-KEM.
- NIST plans to issue a draft standard incorporating the HQC algorithm in about a year, with a finalized standard expected in 2027.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division
Frontier and Quantum Technology Group

OLD ENCRYPTION | NEW ENCRYPTION

← → × scienceDaily.com/releases/2025/03/250319142833.htm

ScienceDaily
Your source for the latest research news

New! Sign up for our free email newsletter.

anglais français Google Translate

S D Health Tech Enviro Society Quirky Search

Science News from research organizations

Record-breaking 12,900 km ultra-secure quantum satellite link

This milestone marks the first-ever quantum satellite communication link established in the Southern Hemisphere.

Date: March 19, 2025
Source: Stellenbosch University

Summary: Scientists have successfully established the world's longest intercontinental ultra-secure quantum satellite link, spanning 12,900 km. Using the Chinese quantum microsatellite Jinan-1, launched into low Earth orbit, this milestone marks the first-ever quantum satellite communication link established in the Southern Hemisphere.

Share: f t p in

RELATED TOPICS FULL STORY

Breaking this hour

- > Mystery of Titan's Missing Deltas
- > Large Carbon Deposits Found On Mars
- > Barbarian Invasion of Roman Britain: Drought
- > California's Highest Tree
- > Brains Circuitry and Learning
- > Smart Insole Tracks How You Walk, Run and Stand
- > Colossal Squid Baby Discovered
- > Lasting Power of Affectionate Mothering
- > Hints of Alien Life Outside the Solar System
- > Cosmic Twist: The Universe Could Be Spinning

Trending Topics this week

Unisys Solutions Artificial Intelligence Resources About

5 MIN READ

Unisys Launches First Post-Quantum Cryptography Service to Block Future Security Threats

Unisys / Unisys Launches First Post-Quantum...

Cryptographic posture assessment is part of the company's cybersecurity portfolio and is designed to bolster global quantum resiliency

Share this in X f

BLUE BELL, Pa., March 27, 2025—[Unisys](#) (NYSE: UIS) has launched the first of several new [Post-Quantum Cryptography \(PQC\)](#) capabilities and services under its cybersecurity portfolio. The cryptographic posture assessment is part of a

← → phys.org/news/2025-04-uk-distance-ultra-communication-quantum.html

PHYS ORG Topics Week's top Latest news

Nanotechnology Physics Earth Astronomy & Space Chemistry Biology Other Sciences X Medicine Technology

It appears that you are currently using Ad Blocking software. What are the consequences?

Home / Physics / Optics & Photonics
Home / Physics / Quantum Physics

APRIL 8, 2025 The GIST Editors' notes

Researchers demonstrate the UK's first long-distance ultra-secure communication over a quantum network

by University of Cambridge



Featured Last Comments Popular

Microplastics discovered in caddisfly casings from the 1970s suggest long-term contamination
19 HOURS AGO 0

Astronomers confirm the existence of a lone black hole
21 HOURS AGO 0

Red, pink or white, all roses were once yellow says genomic analysis
22 HOURS AGO 0

Layered room-temperature altermagnet shows promise for advanced spintronics
APR 18, 2025 0

Indian astronomers investigate the behavior of X-ray binary SXP 138
APR 18, 2025 0

[Computing](#) > [Internet](#) > [Online Security](#)

What is World Quantum Day?

By Aleksandar Stevanović¹ Contributions from Olivia Powell published April 13, 2025

Why quantum science and technology are vital for your online security

 Comments (0)

When you purchase through links on our site, we may earn an affiliate commission. [Here's how it works.](#)

Jump to:

What is World Quantum Day?

Quantum technology and privacy

How quantum technology affects you



LATEST ARTICLES

- 1 Nintendo Switch 2 US pre-order date announced — console price stays same but accessories going up
- 2 Nintendo just quietly removed this Switch 2 feature from listing pages
- 3 This hidden Easter egg ingredient could be the reason you're having trouble sleeping this weekend
- 4 iPhone 18 just tipped for big price hike — and it has nothing to do with tariffs