QUÉBEC QUANTIQUE

Catalyseur de l'écosystème quantique du Québec

quebec-quantique.ca

CAS D'USAGE

Cryptographie quantique

FILIÈRE

Assurances finances gouvernement

*Le marché mondial de la cryptographie quantique passera de **347 millions de dollars en 2019 à 1,3 milliard de dollars en 2024**, un taux de croissance de 30 % par année.*

Opportunité La cryptographie (chiffrement) quantique (*quantum cryptography*) rend les données inviolables, car il faudrait enfreindre les lois de la physique pour les décrypter[1].

Menace La capacité de calcul accrue des ordinateurs quantiques compromet l'intégrité et la sécurité des données encryptées sous les protocoles actuels[2,3].

Technologies quantiques applicables

- Distribution de clés quantiques (QKD)
- Cryptographie sécuritaire quantique (QSC)
- Réseaux optimisés quantiques
- Cryptographie post-quantique

Applications commerciales

- Protection des réseaux locaux de communication pour les banques, grandes entreprises, bureaux gouvernementaux et centres de données médicales et hôpitaux
- Transmissions de données de façon sécuritaire pour la défense
- Protection éventuelle pour tous les réseaux de communication, avant l'arrivée de l'ordinateur quantique[4]

Exemples d'acteurs dans la chaîne d'innovation

DÉVELOPPEURS

Ki3PHOTONICS Technologies
ISARA
agnostiq
IDQ
quantropi
CRYPTO4A

ÉCOSYSTÈME

TELUS
Bell
IBM
ERICSSON
VIDÉOTRON

UTILISATEURS

KPMG
HSBC
CHUM
RBC
intact
Québec

Fiche créée en collaboration avec NUMANA

Partenaire public Québec

CAS D'USAGE : cryptographie quantique

FILIÈRE

Assurances - finances - gouvernement

Freins à l'adoption

Les technologies de cryptographie quantiques sont prêtes pour des projets pilotes de petite échelle, mais ne sont pas encore capables de pleinement remplacer le chiffrement classique. Notamment, la distance de communication des technologies de chiffrement quantiques est limitée pour le moment[5].

Risques du statu quo

L'ordinateur quantique changera le paradigme de la cryptographie et les avancées technologiques sur le sujet ne sont pas exposées publiquement. Par conséquent, les capacités de cette technologie ne seront connues que lorsqu'il sera trop tard[6].

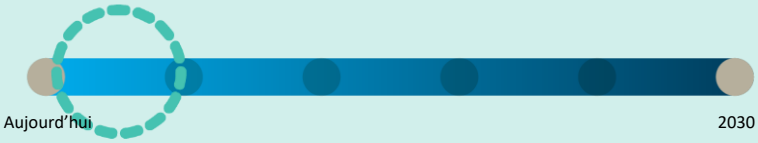
Si les investissements en cryptographie quantique tardent, le retard technologique deviendra presque impossible à combler, peu importe la quantité d'investissements subséquents[7].

Qui plus est, les données actuelles sont déjà vulnérables à une méthode de vol de données où les données chiffrées sont copiées aujourd'hui et ne seront déchiffrées que lorsque la puissance de calcul de l'ordinateur quantique sera déployée (*harvest and decrypt*)[8,9,10].

Cette menace présente un grand danger lorsque les données volées restent confidentielles au fil du temps, par exemple de l'information sur la défense nationale ou les secrets d'État[11,12].

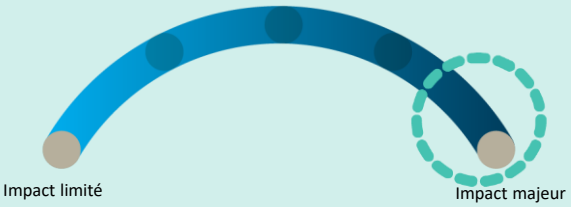
Le marché mondial de la cryptographie quantique passera de **347 millions de dollars en 2019 à 1,3 milliard de dollars en 2024,** un taux de croissance de 30% par année[13].

Fenêtre d'OPPORTUNITÉ



Vu la vitesse de développement de l'ordinateur quantique, il est important de se munir d'une stratégie de protection des données avant qu'il ne soit trop tard. Les investissements doivent être accordés dès maintenant pour garantir une protection en amont, et pour éviter d'accuser un retard technologique[14,15].

POTENTIEL d'impact pour les entreprises



Les algorithmes de déchiffrement quantiques seront, sans équivoque, une technologie de rupture. Il est du devoir corporatif d'assurer une protection adéquate des données de ses clients et utilisateurs, en plus de ses propres données.

1. https://www.orange-business.com/en/blogs/can-quantum-cryptography-secure-internet-quantum-computer-age
2. https://www.orange-business.com/en/blogs/can-quantum-cryptography-secure-internet-quantum-computer-age
3. https://builtin.com/cybersecurity/how-neutralize-quantum-security-threats
4. https://www.ibm.com/blogs/industries/quantum-computing-cybersecurity-risks-quantum-safe-cryptography/
5. https://newatlas.com/quantum-computing/toshiba-quantum-communication-record-optical-fibers/
6. https://www.ibm.com/blogs/industries/quantum-computing-cybersecurity-risks-quantum-safe-cryptography/
7. https://builtin.com/cybersecurity/how-neutralize-quantum-security-threats
8. https://www.linkedin.com/pulse/perfect-harvest-now-decrypt-later-attack-how-steal-10-baumhof/
9. https://www.zdnet.com/article/quantum-computers-could-one-day-reveal-all-of-our-secrets/
10. https://www.forbes.com/sites/forbestechcouncil/2019/09/24/is-the-quantum-computing-revolution-riskier-than-you-realize/?sh=56914c9bae23
11. https://www.ibm.com/thought-leadership/institute-business-value/report/quantumsecurity
12. https://www.ibm.com/blogs/industries/quantum-computing-cybersecurity-risks-quantum-safe-cryptography/
13. https://www.bccresearch.com/market-research/information-technology/global-market-of-quantum-cryptography-market-report.html
14. https://www.helpnetsecurity.com/2020/11/06/quantum-computers-threat/
15. https://builtin.com/cybersecurity/how-neutralize-quantum-security-threats

QUÉBEC QUANTIQUE

Québec Quantique vise à favoriser l'adoption des technologies quantiques par les entreprises et organisations québécoises.

info@quebec-quantique.ca

Rejoignez-nous sur LinkedIn

Inscrivez-vous à notre infolettre

quebec-quantique.ca