Figure : iStock

Assurer la cybersécurité à long terme

La cryptographie quantique au service des réseaux électriques | Le développement rapide de l'ordinateur quantique rendra obsolètes les protocoles de sécurisation des données utilisés dans les réseaux de communication critiques, privés comme publics. Heureusement, la cryptographie quantique offre des solutions dès aujourd'hui.

JEAN-SÉBASTIEN PEGON

Les risques de failles de sécurité dans les réseaux d'infrastructures électriques et autres réseaux critiques augmentent chaque année. Or, cette tendance va encore s'accélérer ces prochaines années, et ce, pour plusieurs raisons.

Premièrement, les tensions géopolitiques et économiques contribuent à accroître les risques pesant sur la sécurité. En effet, les cyberattaques font partie intégrante des stratégies que certaines organisations publiques ou privées influentes ont développées pour affecter des pays ou d'autres organisations. Ceci est clairement visible dans les rapports répertoriant ce type de risques.[1]

Ensuite, la transformation numérique qui s'opère dans le monde influence aussi l'évolution des réseaux électriques et autres infrastructures critiques en général. Cette transformation est devenue indispensable, car elle présente énormément d'avantages opérationnels et financiers, tout en améliorant l'expérience utilisateur. Toutefois, elle augmente aussi le nombre de points d'accès et d'interfaces accessibles depuis l'extérieur des infrastructures et, parfois, même depuis Internet. La surface d'attaque des réseaux d'infrastructures critiques est donc, elle aussi, en pleine expansion.[2]

Finalement, l'augmentation de la performance des outils utilisés pour le piratage, et la cybercriminalité en général, constitue aussi un facteur aggravant.

Une évolution des solutions de sécurité est nécessaire

Comme l'indiquait Solange Ghernaouti, professeure à l'Université de Lausanne et experte internationale en cybersécurité et cyberdéfense, dans un

précédent article paru dans le Bulletin [3], la cybersécurité des réseaux électriques est identifiée en tant qu'enjeu stratégique de souveraineté nationale. Des réponses ont déjà été apportées pour améliorer la sécurité de ces réseaux grâce à l'élaboration de nouveaux standards **(figure 1)**, entre autres la norme ISO/IEC 31000 dédiée au management du risque, les normes de la série ISO/IEC 27000 dont la norme 27019:2017 spécifique au secteur de l'énergie [4], ou encore de nouvelles recommandations de l'Union européenne (telles que la recommandation 2019/553 de la Commission du 3 avril 2019 relative à la cybersécurité dans le secteur de l'énergie [5]). Bien que ces normes et recommandations constituent une avancée nécessaire et importante, cela ne suffira pas, car elles ne traitent pas encore spécifiquement de l'impact des attaques à venir qui utiliseront la puissance des ordinateurs quantiques.

Les ordinateurs quantiques sont en effet capables d'effectuer des calculs complexes avec un gain de temps exponentiel par rapport aux ordinateurs utilisés de nos jours. Cette nouvelle génération d'ordinateur permettra, probablement déjà d'ici une dizaine d'années, de décrypter les informations chiffrées actuellement par des moyens conventionnels de cryptographie classique (scénario d'attaque « harvest now, decrypt later »).[6]

Cela signifie qu'une évolution majeure des solutions de sécurité – aussi bien en ce qui concerne la génération de clés cryptographiques que leur distribution – est nécessaire aujourd'hui pour assurer la sécurité des données sur le long terme. Ce travail a d'ailleurs commencé puisque le National Institute of Standards and Technology (NIST) a lancé une consultation et effectué une sélection de nouveaux algorithmes dits « post-quantiques », dont la standardisation est prévue dans 2 ou 3 ans.[7]

Alors, comment protéger les données efficacement sur le long terme ?

Un chiffrement efficace des données est essentiel

Afin de protéger les données informatiques, une pratique essentielle et reconnue consiste à chiffrer les informations, en particulier lorsqu'elles transitent dans des réseaux déployés

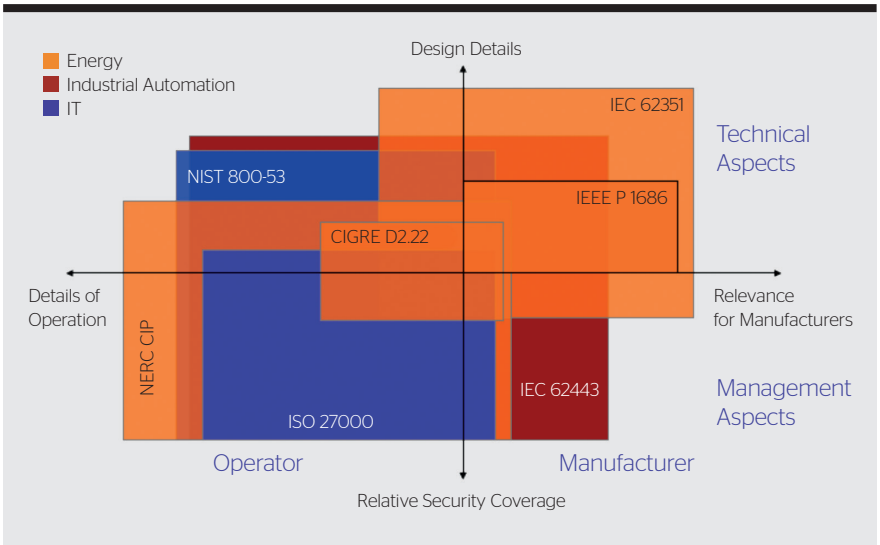

Figure 1 Standards de cybersécurité par secteur industriel.

dans l'espace public. En effet, une sécurité physique le long des fibres ou câbles du réseau ne peut être garantie. Par conséquent, ces réseaux de communication peuvent être victimes d'écoutes par le biais de techniques d'interception sur les fibres optiques ou d'espionnage à distance. La confidentialité, voire l'intégrité des données, peut alors être impactée avec des conséquences dramatiques, comme le montre le cas bien connu de l'Ukraine dont le réseau électrique a été piraté en 2015 et en 2016. Cet incident a entraîné d'importantes coupures électriques de plusieurs heures pour des centaines de milliers de personnes.

Le chiffrement des données est particulièrement recommandé dans les différents éléments de communication du réseau électrique, et notamment dans la partie de contrôle SCADA (Supervisory Control And Data Acquisition) ou DCS (Distributed Control System).

Pour être pleinement efficace, la cryptographie doit s'appuyer sur des sources d'aléa d'excellente qualité permettant de générer des clés imprédictibles même pour des algorithmes avancés, eux-mêmes implémentés sur de puissants ordinateurs de type HPC (High Power Computer) ou, bientôt, sur des ordinateurs quantiques. Comme ces derniers peuvent traiter une grande quantité de données très rapidement et efficacement, ils seront capables, par exemple, de détecter un biais dans une source supposée aléatoire. Une source d'aléa peu fiable peut donc être à l'origine d'une faille dans la génération de clés cryptographiques, ce qui représente un risque majeur pour la sécurité des données.

Générer une clé quantique pour une sécurité accrue

Pour protéger les données sensibles, la cryptographie classique doit être combinée à un générateur de nombres aléatoires aussi peu prédictibles que possible. Il en existe plusieurs types :

- Les générateurs pseudo-aléatoires reposent sur des programmes informatiques déterministes. Ces générateurs sont en fait des amplificateurs d'aléa, basés sur une graine aléatoire. Ils ne permettent donc pas de générer de l'aléa directement.
- Les générateurs hardware s'appuient quant à eux sur les principes de la physique classique. Ces phénomènes sont régis par des lois physiques déterministes et sont donc partiellement prédictibles. Leur qualité diminue avec l'augmentation de la puissance de calcul disponible.
- Finalement, les générateurs de nombres aléatoires hardware QRNG (Quantum Random Number Generator) utilisent les principes de la physique quantique, qui est elle-même de nature probabiliste. Ces générateurs sont désormais disponibles sous forme de puces et ont la propriété de fournir un aléa instantané, de haut débit, dont l'excellente qualité est reconnue par les organismes de normalisation et de sécurité (Metas, AIS31, BSI). Les puces QRNG suivent les recommandations

Figures : Hitachi ABB Power Grids

NIST SP800 90A/B/C et passent les tests IID, non-IID, DieHarder et suite de test NIST SP800-22. Ces générateurs sont intégrés dans certaines cartes de chiffrement des équipements de communication, ou même dans des terminaux mobiles ou IoT.

Afin d'améliorer la sécurité des réseaux électriques et des infrastructures critiques, les sociétés ID Quantique et Hitachi-ABB Power Grids ont développé une carte cryptographique intégrant la puce QRNG produite par ID Quantique. Cette carte de chiffrement, appelée SENC1, fait partie de la gamme de produits FOX615 d'Hitachi-ABB Power Grids. En 2019, le réseau électrique du Sultanat d'Oman a été l'un des premiers à bénéficier de cette innovation technologique. Depuis, d'autres réseaux critiques en Suisse, comme celui de la société CKW, utilisent cette technologie pour chiffrer leur réseau de communication et bénéficier d'une sécurité renforcée dès aujourd'hui, mais aussi sur l'ensemble de la longue durée de vie du réseau électrique.

Dans un autre domaine, l'an dernier, la société Samsung a lancé sur le marché sud-coréen le smartphone Galaxy A Quantum muni d'une puce QRNG d'ID Quantique, rendant ainsi cette technologie accessible au grand public. Cette puce peut aussi être intégrée dans des équipements IoT utilisés dans les réseaux smart grid pour améliorer la sécurité de leur authentification ou de leur connexion chiffrée.

Les ordinateurs quantiques n'ont pas que des avantages

Les prototypes d'ordinateurs quantiques déjà disponibles – certains dans le cloud, comme ceux d'IBM, Google, Microsoft, ou Honeywell – utilisent les propriétés de la physique quantique pour offrir une nouvelle génération d'ordinateurs exponentiellement plus puissants que les ordinateurs classiques. Ils sont développés afin d'effectuer certains types de calculs, notamment probabilistes, et permettront dans les années à venir des avancées majeures dans les secteurs pharmaceutiques, chimiques, du traitement des données ou encore de la finance. Cependant, ils vont aussi avoir un impact majeur et néfaste sur la sécurité des données, puisque la cryptographie actuelle va être, en partie, rendue caduque par ce nouveau type d'ordinateur révolutionnaire.

En effet, les ordinateurs quantiques pourront prochainement casser les protocoles d'échanges de clés asymétriques – Diffie-Hellman (DH), Rivest, Shamir and Adleman (RSA), ou basés sur les courbes elliptiques (EC) – employés pour protéger les données sensibles échangées dans les réseaux de communication, notamment dans les réseaux électriques. La cryptographie asymétrique utilisée pour échanger des clés de chiffrement symétriques est unanimement reconnue aujourd'hui comme étant à risque dans l'ère quantique. En effet, l'algorithme de Shor, bien connu des cryptographes, peut être implémenté assez facilement sur un ordinateur quantique universel pour décoder des algorithmes RSA, DH ou EC, eux-mêmes implémentés dans des protocoles de communications sécurisées bien connus tels que IPSec, TLS, SSL ou https.

La distribution quantique de clé pour une cybersécurité pérenne

En revanche, les solutions de cryptographie symétrique, AES256 par exemple, sont considérées comme résistantes aux attaques d'ordinateurs quantiques. Malgré tout, il est primordial de trouver une solution d'échange de clés symétriques ne pouvant pas être interceptée et décryptée dans un second temps. Une technique, elle aussi reposant sur la physique quantique, a été conçue en 1984 et permet d'offrir un niveau de sécurité universel pour l'échange de clés symétriques. Elle est connue sous le nom de distribution quantique de clé ou QKD (Quantum Key Distribution).

Cette technologie a été implémentée pour la première fois en 2003 dans des équipements commerciaux de cryptographie conçus et produits par ID Quantique, société basée à Genève.[8] À la différence des communications sécuri-

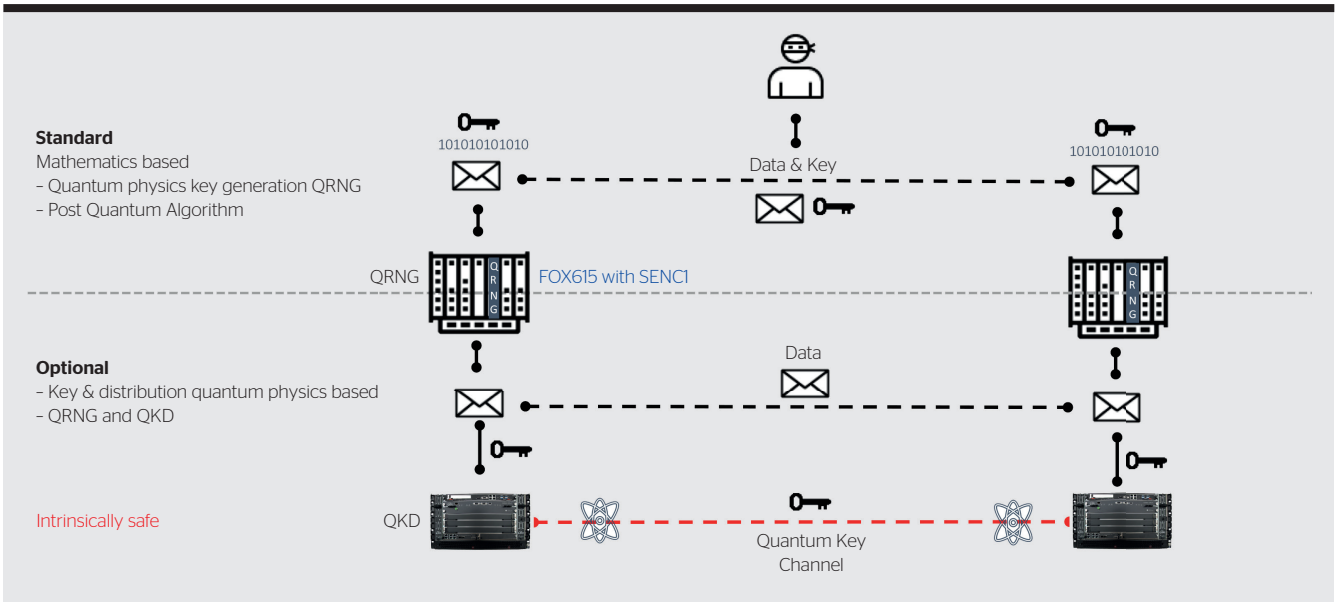

Figure 2 Pour sécuriser les données, il est possible d'utiliser une clé quantique (QRNG) en combinaison avec un algorithme post-quantique (solution standard) ou, en option, une clé quantique dont la distribution est également basée sur la physique quantique (QKD).

sées utilisées aujourd'hui dans les réseaux publics ou privés, les communications quantiques ne peuvent être interceptées sans être modifiées. De plus, la fiabilité de la QKD n'est pas remise en cause par les évolutions technologiques au fil du temps. Ce principe de communication offre, par conséquent, un niveau de sécurité ultime pour l'échange d'informations ultrasensibles telles que les clés de chiffrement.

Premières applications dans les réseaux électriques

La distribution quantique de clé est déjà utilisée dans certains réseaux d'infrastructures critiques et électriques. Par exemple, en 2020, ID Quantique a commencé à sécuriser le réseau électrique de la société Kepco, entre les deux sous-stations d'Anmyeon et de Taen, en Corée du Sud. D'autres déploiements sont prévus dans un avenir proche pour la même société, notamment entre leurs centres de données principaux.

En 2020, les Services Industriels de Genève (SIG) ont aussi implémenté un lien QKD, combiné à la solution de chiffrement de la société Adva (FSP3000) afin de démontrer la possibilité d'utiliser des clés quantiques en complément des clés classiques, et ce, dans le cadre d'un projet européen appelé OpenQKD [9]. Ainsi, il a pu être validé que la technologie QKD s'intégrait facilement dans des réseaux existants pour sécuriser un lien en production entre des centres de données sur lequel un volume très important d'informations sensibles est échangé quotidiennement.

Les sociétés ID Quantique et Hitachi-ABB Power Grids continuent aussi de travailler ensemble pour pouvoir proposer la technologie QKD en option de la gamme FOX615, afin de garantir un niveau de sécurité supplémentaire résistant aux attaques plus sophistiquées utilisant la puissance des ordinateurs quantiques **(figure 2)**.

Assurer la sécurité à long terme dès aujourd'hui

Même si, à priori, les ordinateurs quantiques existants ne sont pas encore assez puissants pour déchiffrer nos données, la confidentialité de ces dernières est déjà à risque. En effet, une organisation malicieuse qui prélèverait et sauvegarderait des données chiffrées aujourd'hui serait capable de les exploiter plus tard, dès l'arrivée de l'ordinateur quantique, exposant ainsi l'organisation visée à un risque qui peut s'avérer critique. Par conséquent, toute donnée dont la durée de confidentialité requise s'élève à plus de 5 ou 10 ans devrait être protégée dès aujourd'hui. Pour ce faire, des solutions de cryptographie quantique existent et celles-ci commencent à être déployées dans des réseaux opérationnels afin d'anticiper un risque majeur de cyberattaque augmentant chaque année.

Références

[1] R. I. Ogie, « Cyber Security Incidents on Critical Infrastructure and Industrial Networks », Proceedings of the 9th International Conference on Computer and Automation Engineering ICCAE'17, p. 254-258, New York, USA, 2017. ro.uow.edu.au/cgi/viewcontent.cgi?article=1217&context=smartpapers.

[2] Gabrielle Desarnaud, « Cyber Attacks and Energy Infrastructures : Anticipating Risks », Études de l'Ifri, janvier 2017. ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf.

[3] S. Ghernaouti, « La cybersécurité des infrastructures électriques », Bulletin SEV/VSE 12/2019, p. 46-48, 2019. bulletin.ch/fr/news-detail/la-cybersecurite-des-infrastructures-electriques.html.

[4] ISO/IEC 27019:2017 Technologies de l'information – Techniques de sécurité – Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie. iso.org/fr/standard/68091.html.

[5] « Recommandation (UE) 2019/553 de la Commission du 3 avril 2019 relative à la cybersécurité dans le secteur de l'énergie », Journal officiel de l'Union européenne, 5 avril 2019. eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019H0553&from=ES.

[6] S. Buchholz, J. Mariani, A. Routh, A. Keyal, P. Kamleshkumar Kishnani, « The realist's guide to quantum technology and national security », Deloitte Insights, 2020. www2.deloitte.com/uk/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html.

[7] NIST Post-Quantum Cryptography program. csrc.nist.gov/projects/post-quantum-cryptography.

[8] G. Ribordy, P. Trinkler, «Physique quantique et cryptographie», Bulletin SEV/VSE 7/2011, p. 27-31, 2011. doi.org/10.5169/seals-856830.

[9] Projet européen OpenQKD. openqkd.eu.

Auteur

Jean-Sébastien Pegon est directeur des ventes pour les secteurs Marchés Télécom, Finances et Infrastructures critiques chez ID Quantique.

→ ID Quantique SA, 1227 Carouge

→ jean-sebastien.pegon@idquantique.com

IN KÜRZE

Langfristige Cybersicherheit gewährleisten

Quantenkryptografie für Stromnetze

Die Cybersicherheit von Stromnetzen ist eine strategische Frage der nationalen Souveränität. Das Risiko von Sicherheitsverletzungen steigt jedoch jedes Jahr. Quantencomputer, von denen einige Prototypen bereits in der Cloud verfügbar sind, werden es wahrscheinlich schon in zehn Jahren ermöglichen, Informationen zu entschlüsseln, die derzeit mit konventionellen Mitteln der Kryptografie verschlüsselt sind (das Angriffsszenario «harvest now, decrypt later»). Eine umfassende Weiterentwicklung der Sicherheitslösungen – sowohl bezüglich der kryptografischen Schlüsselerzeugung als auch der Verteilung – ist daher heute nötig, um die Datensicherheit langfristig zu gewährleisten.

Glücklicherweise gibt es bereits Lösungen für die Quantenkryptografie. Neuerdings werden sie auch in betrieblichen Netzwerken eingesetzt, beispielsweise bei den Services Industriels de Genève (SIG). Einerseits sind Hardware-QRNG (Quantum Random Number Generator), die ebenfalls auf den Prinzipien der Quantenphysik basieren, in der Lage, selbst für einen Quantencomputer unvorhersehbare Kodierungsschlüssel zu erzeugen. Andererseits bietet die Quantum Key Distribution (QKD) eine sichere Langzeitlösung für den symmetrischen Schlüsselaustausch. Da Quantenkommunikation nicht abgefangen werden kann, ohne modifiziert zu werden, wird die Zuverlässigkeit von QKD nicht durch technologische Entwicklungen im Laufe der Zeit beeinträchtigt werden. CHE