# Gemalto introduit la physique quantique dans ses appliances d'encodage

Gemalto vient d'annoncer le CN8000, une nouvelle appliance de sécurité dédiée à l'encodage des données informatiques. Conçu par les équipes de Safenet, société spécialisée dans les systèmes de gestion avancés des clés cryptographiques, le boitier s'appuie sur les solutions Multi-Link High Speed Encryptor (HSE) de l'entreprise rachetée en août 2014 par Gemalto.

Le CN8000 entend se distinguer sur l'échelle des performances en regard du volume de la solution. Dans un format 4U (430 x 460 x 175 mm), le boîtier permet d'agréger 10 ports Ethernet 10 Gbit/s full duplex pour un débit total encodé de 100 Gbits/s à faible latence (8 microseconde par carte d'encryption). Une solution susceptible, donc, de remplacer 10 encodeurs de 10 Gbit/s pour sécuriser les lignes tirées entre deux datacenters (privés ou publics). *« Nous pouvons protéger les données sensibles contre la surveillance et les interceptions visibles comme invisibles, à un coût abordable, de manière à les rendre inutilisables si elles tombent entre les mains de personnes non autorisées, tout en aidant les clients à réduire leur empreinte d'encodage »*, assure Todd Moore, vice-président pour la gestion des produits d'encodage chez Gemalto.

## Un générateur quantique de nombres aléatoire

Si le CN8000 se distingue par sa compacité et ses performances, il innove également par l'introduction de mécanismes basés sur la physique quantique pour générer les clés de chiffrement. La solution est apportée par l'entreprise suisse ID Quantique qui a développé le Quantis, un boîtier électronique de la taille d'une boîte d'allumettes et qui s'appuie sur la théorie probabiliste de la physique quantique pour générer des nombre de manière aléatoire. Le principe est le suivant : une générateur émet des particules de lumières (des photons) envoyées une par une sur un miroir semi réfléchissant. Selon que ces émissions de lumière sont reçues, ou non, par le détecteur de photons, le système génère un 0 ou un 1. *« Quantis est une fontaine de nombres aléatoires »*, schématise poétiquement Grégoire Ribordy, PDG de ID Quantique qui a intégré sa solution en collaboration avec la société américaine Senetas.

Le générateur de nombre aléatoire dédié à la production de clés de cryptage fonctionne à la fréquence de 4 Mbit/s. *« C'est largement suffisant pour les besoins actuels »*, assure le dirigeant. En l'occurrence, 2048 bits selon les standards en cours pour les clés publiques et 128 ou 256 bits pour les clés d'échange. Qui plus est, le système peut générer des clés en nombre infini puisque *« c'est une suite de tirages à pile ou face »*. De quoi répondre aux besoins d'évolution des clés de chiffrement alors que les performances toujours plus poussées des ordinateurs nécessitent des clés de cryptage toujours plus longues pour se protéger des attaques par force brute.

## Un distributeur quantique de clés de chiffrement

Au-delà de la cryptographie pure et dure, ID Quantique met également son moteur de nombres aléatoires au service d'une seconde application : la sécurisation de la distribution des clés. *« Le*

*chiffrement sera vulnérable à des attaques d'ordinateurs quantiques*, explique Grégoire Ribordy. *A plus long terme, la sécurité nécessitera des mécanismes non vulnérables de distribution de clés.* » ID Quantique propose alors un mécanisme de transmission des clés qui utilise le principe d'indétermination d'Heisenberg selon lequel l'observation d'un événement quantique perturbe cet événement. En appliquant ce principe sur une fibre optique, le système peut ainsi déterminer si la transmission d'une information entre deux points a été «observée» (donc attaquée), ou non, et émettre une alerte en conséquence.

« *Cette technologie répond à des besoins de sécurité à long terme, à l'horizon 2025, mais certains client prennent ce genre de menaces futures au sérieux et anticipent afin d'éviter que des données volées aujourd'hui ne soient déchiffrables en 2025* », justifie l'entrepreneur. Toujours est-il que, si l'offre n'est pas mise en avant par Gemalto, les boîtiers CN8000 sont de fait d'ores et déjà compatibles avec le modèle de distribution quantique de clés de chiffrement. Une solution taillée pour l'avenir, donc.

---

**Lire également**

Comprendre l'ordinateur quantique (infographie)
Mazyar Mirrahimi, Inria : « Un ordinateur quantique dans dix ans ? Impossible de l'affirmer »
Ordinateur quantique : IBM fait une percée sur les terres du qubit