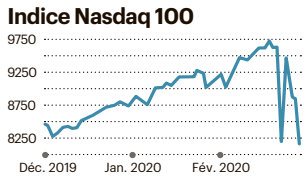
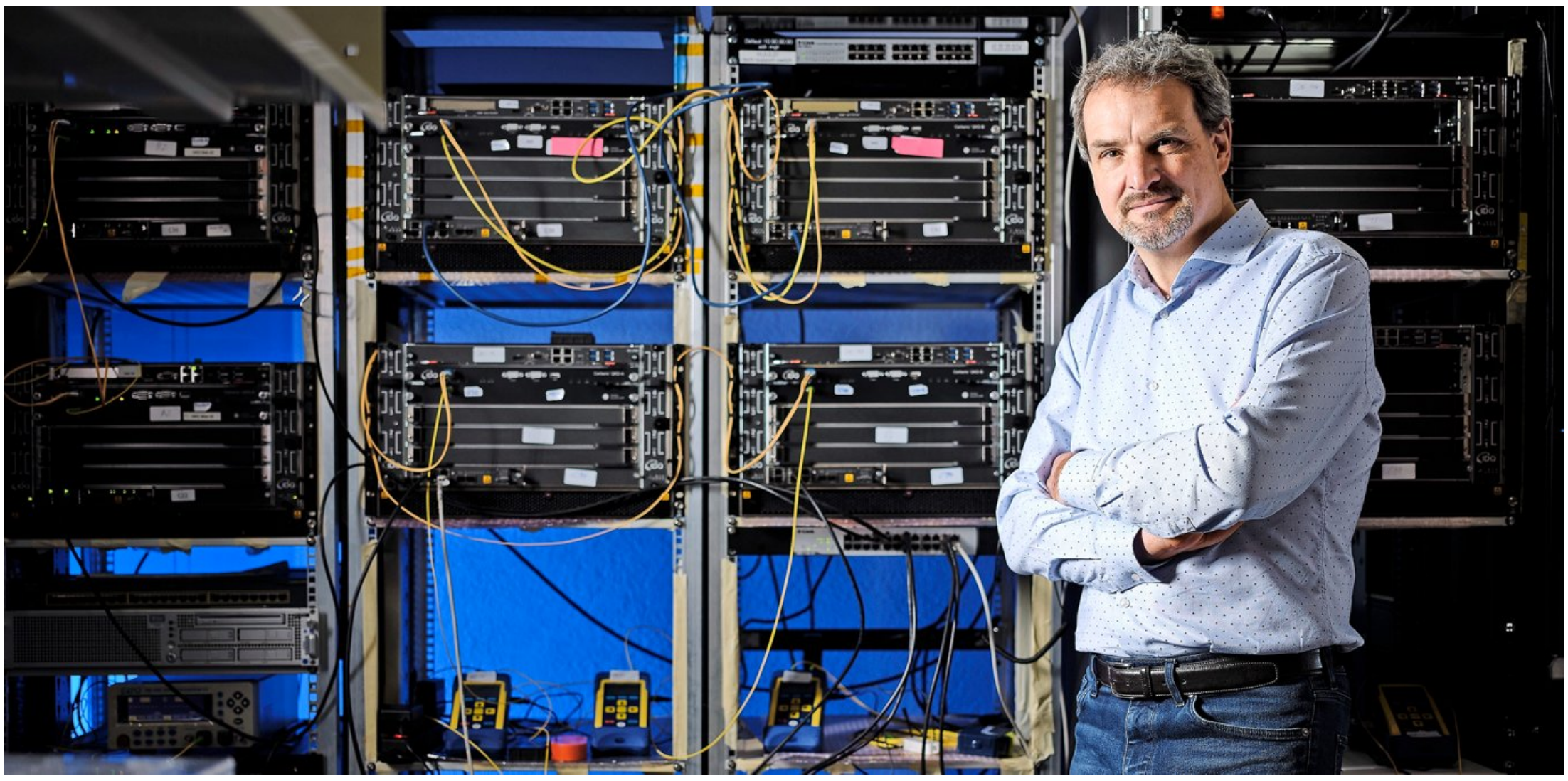
Economie

Lauréat de la semaine
Avec Pascal Kiener à sa tête et au vu de ses solides résultats 2019, la BCV entame en pleine forme sa 175e année

Indice Nasdaq 100



Le graphique
Empoisonné par le Covid-19, le Nasdaq a sombré avec les autres places boursières



Grégoire Ribordy, CEO d'ID Quantique, dans la zone de fabrication et de test. *Yvain Genevay / LMD*

La physique quantique garantira l'inviolabilité de nos données

CYBERSÉCURITÉ Depuis bientôt vingt ans, la société genevoise ID Quantique s'illustre dans la cryptographie quantique, un système jugé inviolable.

OLIVIER WURLOD
olivier.wurlod@lematindimanche.ch

«La mécanique quantique force le respect. Mais une petite voix intérieure me dit que ce n'est pas encore la juste vérité. En tout cas je suis convaincu que Dieu ne joue pas aux dés.» Dans les années 1920, Einstein ne voulait pas y croire. Aux yeux du père de la relativité, la propriété aléatoire de la physique quantique n'était pas réaliste. Un siècle plus tard, son interprétation erronée du phénomène est en train de bouleverser le monde de la cryptographie.

Depuis le début du XXIe siècle, une petite société genevoise fait partie des principaux précurseurs à avoir compris tout le potentiel de la physique quantique dans le domaine de la sécurité informatique. Issue des laboratoires de physique appliquée de l'Université de Genève, ID Quantique est parvenue à se faire sa place dans un marché de la cryptographie quantique encore restreint mais en plein essor depuis quelques années (la banque Morgan Stanley l'évalue à 10 milliards de dollars en 2025).

L'arrivée actuelle des ordinateurs quantiques donne des ailes à cette technologie étant donné que les experts prédisent que la puissance de calculs de ces nouvelles machines parviendra à briser les solutions de cryptage les plus élaborées. «Dans les années à venir, même les clés les plus perfectionnées finiront par être «craquées» au vu des capacités générées par ces nouveaux ordinateurs et la facilité de conserver des données. Pour protéger des informations sur le long terme, la cryptographie quantique supprime ce risque», assure Grégoire Ribordy, CEO et cofondateur d'ID Quantique.

Comment ça marche?
Sans trop entrer dans des détails techniques et physiques aussi complexes que laborieux, comment fonctionne cette technologie que les experts estiment inviolable? La première chose à savoir en parlant de la solution développée par ID Quantique est qu'elle ne protège pas le message, mais la clé qui servira à le décrypter.

Générée aléatoirement, cette clé s'échange par fibre optique entre deux appareils (un émetteur A et un récepteur B) à l'aide de photons, dont la particularité est que ces infimes particules de lumière sont très sensibles et ne peuvent être «observées» sans en changer leurs caractéristiques. «Imaginez-les sous la forme d'une bulle de savon. À la moindre perturbation constatée lors de leur trajet entre les deux boîtiers, ces dernières explosent et empêchent toutes tentatives d'interception de la clé par des personnes malintentionnées», explique son patron.

Ce dernier confirme toutefois que si cette solution est inviolable selon les lois de la physique quantique, elle n'est pas à l'abri des faiblesses humaines puisque les émetteurs et récepteurs peuvent comprendre des failles installées volontairement pour avoir accès aux clés échangées. «Cette vulnérabilité est certes possible, mais me paraît très compliquée. Non seulement elle nécessiterait la complicité de plus d'une personne, mais en plus il faudrait qu'elle ne soit pas détectée lors d'évaluations de plus en plus courammentpratiquées pour vérifierqu'il n'y a pas de portes d'entrée dérobées similaires à celles installées par la société Crypto AG.»

> **«Dans les années à venir, même les clés les plus perfectionnées finiront par être «craquées». Pour protéger des informations sur le long terme, la cryptographie quantique supprime ce risque»**
> Grégoire Ribordy, CEO et cofondateur d'ID Quantique

Autre principale limite à ce jour: la nécessité d'avoir un réseau en fibre optique ainsi que la distance maximale encore restreinte entre émetteur et récepteur. Si certains tests ont permis d'atteindre les 400 kilomètres, cette solution reste à dimension locale. Mais dans les années à venir, la cryptographie quantique pourrait voir son champ d'application s'étendre géographiquement à l'aide de satellites quantiques.

Dans les pages du «Figaro», Anton Zeilinger, le professeur à l'origine de cette percée, expliquait que l'astuce avait été d'envoyer une première clé quantique au moment où le satellite survolait Pékin, puis une autre quelques heures plus tard une fois l'engin proche de l'Autriche. «Par une opération mathématique simple, il sera possible de reconstruire une clé commune utilisable entre Pékin et Vienne», expliquait le scientifique. À ce jour, seule la Chine dispose d'un tel engin lancé dans l'espace en 2016.

Marché en pleine croissance
À Genève, où l'entreprise est active depuis sa création en 2001, l'attention se porte sur certains secteurs comme ceux de la finance, de la pharma ou pour toute autre industrie souhaitant protéger sa propriété intellectuelle et ayant les moyens de payer une technologie encore coûteuse (100 000 francs par appareil).

En plus de tout le pan «sécurisation des données», ID Quantique utilise sa technologie pour se diversifier et commercialiser des instruments scientifiques tels que des générateurs de nombres aléatoires utilisés par exemple par les sociétés de loterie. L'entreprise genevoise s'est également creusé un sillon dans le domaine des capteurs quantiques, outils indispensables pour les futures voitures autonomes puisqu'ils devraient leur permettre de mieux analyser leur environnement.

Il y a deux ans, pour accélérer sa croissance et rester l'un des leaders du marché au côté de géants tels que Toshiba ou Huawei, ID Quantique signait une alliance avec le groupe coréen SK Telecom et levait 65 millions de dollars. Des fonds ayant permis à l'entreprise de quasi doubler ses effectifs en deux ans (passant d'une soixantaine de personnes à plus de 110 salariés actuellement).

La Suisse réfléchit à soutenir les groupes actifs dans les technologies quantiques

En février 2018, contre un investissement de 65 millions, ID Quantique cède le contrôle d'une part majoritaire de son capital à SK Telecom, le géant des télécoms coréen. Si cette alliance est une victoire pour la PME genevoise, pour la Suisse elle l'est moins et cela même si ID Quantique continue d'assembler ses boîtiers à Carouge.

Vingt mois plus tard, une prise de conscience semble heureusement émerger du côté de Berne en ce qui concerne les technologies quantiques et le fait que d'autres pays sont beaucoup plus actifs et enclins à en soutenir le développement. Ces dernières sont en effet clairement prises en compte dans le dernier rapport du Conseil suisse de la science (CSS) où elles arrivent en tête du plan d'action pour les années 2021 à 2024. Et parmi les recommandations apparaît celle d'identifier, puis de développer des niches prometteuses dans les technologies quantiques, y compris dans le domaine de la cybersécurité.

Et pour une fois, la question monétaire n'y est plus taboue. «Comme les investisseurs suisses sont peu enclins à prendre des risques lorsqu'il s'agit du domaine des technologies quantiques, il faudrait favoriser la création d'un fonds de capital-risque ou d'une communauté d'investisseurs pour les start-up actives dans ce marché et entrées dans cette phase dangereuse baptisée «Vallée de la mort», indique le rapport.

En agissant de la sorte, la Suisse s'inscrit dans une tendance globale où la protection des données se transforme en enjeux nationaux sur le plan sécuritaire certes, mais aussi sur celui des droits de l'homme. Dans un rapport paru ces derniers jours, l'Unesco rappelle que «le cryptage est une pièce importante du puzzle pour la réalisation d'un internet libre, ouvert et digne de confiance».