A FOOLPROOF METHOD OF PRESERVING DATA SECURITY

In the battle to protect the security of digital information, a Swiss company has used quantum mechanics to develop a new form of cryptography which makes decoding data impossible – even as computers become much faster

The increasing processing power of computers is making it easier for hackers to decipher encrypted information by finding the keys at the heart of traditional coding techniques. That task will become much easier when quantum computers arrive, hugely accelerating processing speeds and making it possible to break codes very quickly.

However, the quantum mechanics science behind the new generation of super-fast computers has already generated a new form of cryptography which is impossible to decode – not least because any attempt to intercept changes the data. A leader in the field is ID Quantique, a company created in 2001 by four scientists at the University of Geneva who had identified the potential of quantum cryptography to revolutionise data security.

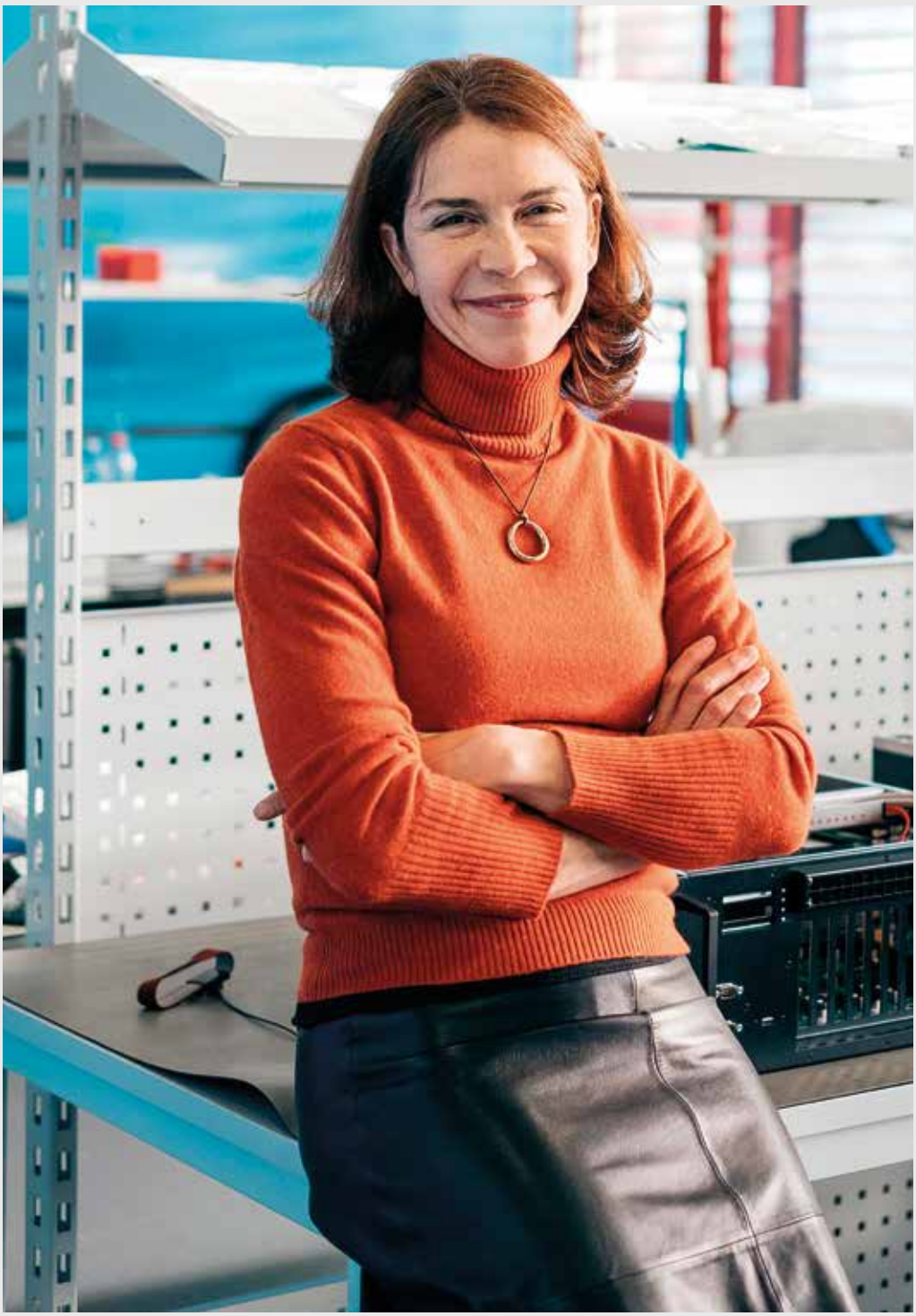
'Quantum encryption technology has been around for a while,' says Grégoire Ribordy, a physicist who was one of the founders and became the company's chief executive in 2001. 'But all the big IT groups have begun to enter the quantum computing field in the last two years. And the US National Security Agency (NSA) announced in 2015 that it was planning to upgrade its cryptography techniques to make them quantum safe.

'We may have been early into the field, but people now understand the challenge. Quantum computing is no longer science any more, but engineering – it's not a question of if, but when. So quantum encryption has become a priority for protecting the security of data when today's conventional coding techniques become too vulnerable.'

The development of quantum mechanics came in the first 30 years of the 20th century when physicists found discrepancies between the results of their experiments and the then theory. Quantum mechanics described a new way of looking at the world of atoms, particles and other very small things. It was initially purely theoretical, but gradually led to the first quantum revolution with the development of lasers, microchips and other new technologies.

This first wave did not use the full potential of quantum physics, says Dr Ribordy. But a second quantum revolution has begun as it has become possible to use much smaller devices and control individual elements. And the emergence of quantum computing is one consequence of that, because it will be able to process the calculations needed to break cryptographic codes so fast that traditional encryption techniques will be ineffective.

‘Quantum encryption has become a priority for protecting the security of data when today’s conventional coding techniques become too vulnerable’



‘The idea of quantum cryptography is not to use quantum physics to create a problem, but to solve this problem by improving the security of communications.’

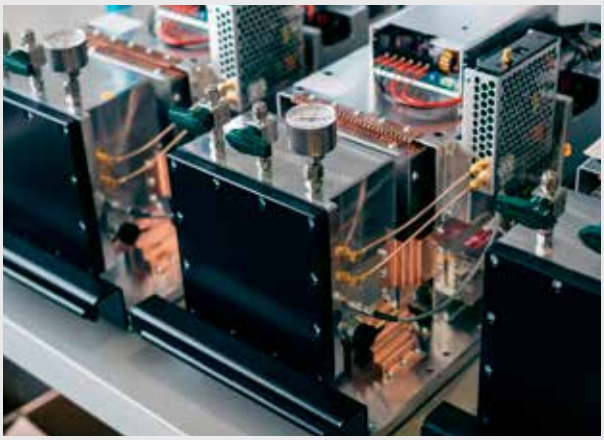
Even before quantum computing has developed, far-sighted organisations are already using quantum-safe cryptography techniques to provide long-term security of their data. An adversary can record information encrypted using traditional codes today and decrypt it in the future when quantum computing becomes available. Using quantum cryptography now protects critical data such as client portfolios, as well as information about clients and the employees of the organisation.

A more common use today of ID Quantique’s quantum-safe techniques is to secure communications between data centres – between head office computers and back-up facilities, for example. An attraction for users is that the information cannot be decrypted when quantum computers arrive, because of the Heisenberg Uncertainty Principle. This central tenet of quantum mechanics, says that if you try to read and measure a quantum object such as a photon that carries the encryption key, you change its state.

Kelly Richdale, a seasoned entrepreneurial executive brought in to help transform ID Quantique into a more commercially minded organisation, sees this as a strong selling point. ‘If someone tries to intercept information sent over optical fibres – for example between two data centres – it creates physical proof of the attempt. It is an anti-eavesdropping mechanism, as well as giving protection in the future world of quantum computing.’

The company has other products using quantum mechanics principles, such as the Quantis, a small random number generator, which harnesses the random nature of the universe to generate encryption keys for security products. It is also used in the online gaming industry, which is highly regulated and needs to be able to demonstrate that its games use genuinely random numbers.

‘In times of uncertainty people buy Swiss francs, and they also buy Swiss encryption devices’



An attraction of ID Quantique’s security encryption products for potential customers is that it is a Swiss company. ‘One of our logos is Swiss Quantum,’ says Kelly Richdale. ‘The most famous examples of security breaches were those highlighted by the whistle-blower Edward Snowden, who revealed the surveillance of digital communications by governments and their insistence that manufacturers install back doors in devices to give them access to transmissions of encrypted data.

‘Switzerland doesn’t have that kind of strong government pressure – indeed, we have data protection and privacy as fundamental rights. When countries such as the US force disclosure through back doors, it hugely undermines trust in their products. It’s a bit like the flight to the Swiss franc: in times of uncertainty people buy Swiss francs, and they also buy Swiss encryption devices.’

Dr Ribordy says he hopes to broaden the company’s range of products, to position it as the leader in quantum-safe long-term security. These include new solutions for email encryption and storage encryption, where he expects demand to grow as the arrival of quantum computers approaches.

‘We are looking for partners to bring our quantum products into completely different markets, such as smartphones. You could just take a picture on your smartphone which would generate high quality random numbers for codes and encryption keys for security purposes.’

The company has started to grow fast, doubling its staff to 50 in the last year. One factor that is increasing demand is the new focus on cyber attacks. Traditionally it has been on data theft, and that is expected to continue. But increasingly cyber attacks are being used for political purposes, such as influencing elections or attacking critical infrastructure.

'If you look at what happened in Ukraine, the Russians hacked into the electricity grid,' says Kelly Richdale. 'They took out part of it and the only thing that saved the Ukrainians was the age of their grid and its poor connectivity which stopped the whole network from being brought down.

The beauty of quantum-safe encryption is that it has guaranteed forward security built in

'The first such attack came in Estonia, which has now become a leader in developing cyber defences. And Switzerland is a good example of how organisations can work together to defend their critical infrastructure, which includes the banks as well as the electricity industry, the water grid and other networks. There is a very strong coordinated response if there's an attack on a Swiss infrastructure company, but there are countries where cyber defence is not so well coordinated.'

And the beauty of quantum-safe encryption is that it has guaranteed forward security built in, says Grégoire Ribordy. 'It's based on the laws of physics and they can't be changed. Quantum cryptography has the potential to end the race between code-makers and code-breakers. We can improve the performance of our system, reduce its cost and maybe its size, and move into new application areas. But the security of quantum cryptography will not change – and that's what makes the technology interesting.'●