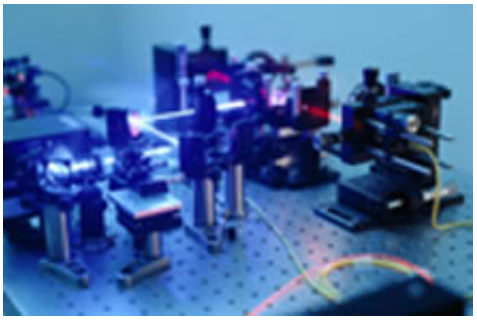
Cryptic messages boost data security

November 29 2007



The Swiss national elections in October 2007 provided the opportunity to witness quantum cryptography in 'real-life' action for the first time. Geneva was first in line to test the unbreakable data code developed by Swiss start-up company id Quantique, paving the way for a new era in data security.

The canton of Geneva became a world pioneer when it decided to use quantum cryptography to protect the dedicated line used for counting votes in the October national elections. The world's first commercial quantum random number generator and quantum cryptography system was developed by the Swiss company id Quantique – a spin-off company of the University of Geneva – so the choice of Geneva to test the system in action was only appropriate.

The firm was founded in 2001 by four researchers from the University

of Geneva: Nicolas Gisin, Grégoire Ribordy, Olivier Guinnard and Hugo Zbinden. According to Gisin: “Protection of the federal elections is of historical importance in the sense that, after several years of development and experimentation, this will be the first use of a 1 GHz quantum encrypter, which is transparent for the user, and an ordinary fibre-optic line to send data endowed with relevance and purpose. So this occasion marks quantum technology’s real-world debut.”

All about Eve

Quantum cryptography, or quantum key distribution (QKD), enables two communicating parties to produce a shared random bit string know only to them, which can be used as a key to crypt and decrypt messages. An important and unique feature of quantum cryptography is the ability of the two communicating parties to quickly detect the presence of any third party trying to gain access to the key. This third party, the eavesdropper if you like, is commonly known as Eve among cryptographers. Quantum cryptography then is essentially all about cutting Eve out of the equation.

The use of the system developed by id Quantique makes it possible to detect Eve’s presence almost immediately and to take counter measures. The system works, however, not only when there is an eavesdropper on the line but also when data become corrupted accidentally. Which, in the case of the Swiss elections, is an equally important feature.

For Robert Hensler, the Geneva State Chancellor, the application of quantum cryptography will go a long way towards alleviating concerns over eVoting. “In this context, the value added by quantum cryptography concerns not so much protection from outside attempts to interfere as the ability to verify that the data have not been corrupted in transit between entry and storage,” he is quoted as saying.

SwissQuantum, a new standard for data security

The Swiss elections are an important milestone for id Quantique, but they are just the initial phase of a wider-ranging plan which is expected to lead to the creation of a pilot quantum communications network in Geneva similar to the nascent internet network in the United States back in the 1970s. Known as SwissQuantum, this next stage in the project aims to provide a platform for testing and validating the quantum technologies that will help to protect the communications networks of the future.

The project's plans, however, extend beyond the Geneva region with a longer-term view of expanding the network throughout the country and beyond. This technology will appeal in particular to certain core industries of the economy which depend particularly on data security – banks, insurance companies, high-tech businesses,… In this regard, it is hoped that the SwissQuantum name will come to be seen as the best guarantee for reassuring potential clients of the soundness of this scientific innovation.

id Quantique is a partner in the European project SECOQC which began in April 2004. "The SECOQC project makes it possible for id Quantique's engineers to interact with some of the best groups worldwide in the field of quantum cryptography," observes Ribordy. Together, the project partners intend to lay the foundations for a long-range, high-security communication network that combines the entirely novel technology of quantum key distribution with components of classical computer science and cryptography.

Ensuring effective data security is the next challenge for global data networks. SECOCQ will provide European citizens, companies and institutions with a tool that allows them to face the threats of future interception technologies, thus creating significant advantages for the

European economy.

Source: ICT Results