

# Maintaining cryptographic security in the quantum age



**Behind the scenes, cryptographic technologies underpin a great deal of the security that we take for granted. Yet with ever more powerful computers, the encryption and decryption methods that underpin secure communications are under threat. IST researchers are identifying new ways of shoring up defences through advanced quantum computing.**

**Since Moore's law predicts the doubling of transistor density every 18 months it will become increasingly easy to break cryptographic keys as computational power doubles. For example, the 512 bit RSA public-key cryptosystem developed in 1977, can be broken by university research groups within a few months. Even though keys of 2048 bits are considered by many to be secure for decades, if the huge processing power of futuristic [quantum computers](#) can be implemented, then most public key cryptography will become history.**

Against such a threat the IST project STORK built a core European research effort in cryptography. It provided a platform for the exchange of ideas on key issues facing cryptography, and proposed a roadmap for future research. "We produced a directory of the key European players and their areas of expertise, listed the outstanding issues, and suggested an agenda for the next five years," says project coordinator Bart Preneel of the University of Leuven.

"It's a very small research community, only about a thousand people worldwide. Most of them know about the STORK project and refer to our site." The project's work lead directly to ECRYPT, an IST Network of Excellence project in cryptology, which began in February 2004, under the Sixth Framework Programme.

The challenge now is to find a way to make cryptographic techniques available and economic for industry and commerce at large.

## **New cryptographic protocols**

Rising to this challenge the IST project PROSECCO has the task of developing new quantum cryptographic protocols with particular emphasis on protocols that are presently or will soon be practical.

PROSECCO began on 1 January 2003, and is now just over halfway to completion. The project aims to develop a practical method for distributed yet secure processing of quantum computations, a fundamentally new mode of information processing that uses discrete, indivisible units of energy called quanta.

The project is attempting to develop new distributed quantum applications and to analyse their security against quantum attacks. Such protocols will probably be among the first applications of quantum technology. The development of new quantum protocols is also likely to yield further data on a key

problem in the field - distinguishing between tasks which can be securely implemented with quantum protocols but not with classical cryptography, and tasks for which physical security guarantees are impossible.

According to project coordinator Joern Mueller-Quade of Karlsruhe University in Germany, “New technology like quantum computing endangers classical cryptography. So we are trying to find new quantum cryptographic applications that offer higher levels of security than classical cryptography, and also if classical cryptography can be made more secure against quantum attacks.”

“In PROSECCO, we are not so interested in methods of key exchange, but more in digital signatures,” he continues. “For example how to make them more secure than classical digital signatures. We think it may be possible to develop cryptographic methods that are more secure for authentication purposes, such as ‘zero-knowledge proofs’ for auctions.”

### **Developing methods of quantum key exchange**

While some EU researchers are focusing on quantum protocols, SECOQC, a four-year IST project launched on 1 April 2004, is working on a tool based on quantum technologies that will enable organisations to exchange critical information with guaranteed security, knowing that their vital knowledge assets are secure from industrial espionage and other forms of illegal activity.

SECOQC is lead by Seibersdorf Research, the research organisation that was involved in the world’s first successful bank transfer encoded via quantum cryptography. Project coordinator Christian Monyk of Seibersdorf says, “To date, quantum cryptography has only been carried out in the universities and experimental projects. We plan to develop the technology to meet the real needs of future users.”

“How we encrypt and decrypt the data is an issue of classical cryptography,” says Monyk. “What we are focusing on is managing the generation and distribution of the cryptographic keys, which is where quantum technology comes in.” He elaborates, “With existing high-security cryptography, you have to distribute the key beforehand, which is a weakness in the system. With quantum distribution you don’t have to transport or store the key, so it is far more secure than existing methods.”

One of the challenges for SECOQC researchers, he says, is to develop optical devices capable of generating, detecting and guiding single photons; devices that are affordable within a commercial environment. “At the moment, they are the size of a table – so what we are about is a normal development process.”

### **Understanding quantum computing**

In quantum computing, the fundamental unit of information adheres to the laws of quantum mechanics which differ radically from the laws of classical physics. Therefore, quantum computers can be programmed in a qualitatively new way. As a result new algorithms for solving problems can turn difficult mathematical problems, such as factorisation, into easy ones, making traditional key breaking simpler.

Quantum information exchange makes use of the properties of light to underpin a method of encryption that is theoretically unbreakable. Typically, a sending optical device puts photons into a particular state, which is then observed by the recipient. Since it is impossible to intercept a light transmission without changing it, important information can be exchanged with great security.

Quantum cryptography makes use of an optical communication protocol to transfer data across an optical network. Transmission of the quantum cryptographic key relies on single photons transmitted over an optical channel to transfer the secret key. Any attempt to interrupt or break into such a system inevitably

disrupts the sequence of photons, rendering any attempt to read the key immediately detectable.

Such cryptography has been proposed as the obvious answer to protecting cryptographic codes from quantum-level attacks. The most straightforward application of quantum cryptography is in the distribution of the secret keys that are used to encrypt and decrypt transmitted data. While classical cryptography employs mathematical techniques to maintain the security of encrypted messages, in quantum mechanics the information is protected by the laws of physics.

Quantum encryption and decryption are therefore inherently safer than classical cryptographic methods because any observation or monitoring of an optical system automatically disturbs the light stream. If anyone tries to access a photon stream, this very measurement will disturb the system and the legal recipient will see an error.

So, while scientists across Europe are working frantically to resolve the technical issues, of one thing you can be sure. That there is going to be no shortage of applications for the results. Christian Monyk of SECOQC points to some likely users, “All institutions that need secure data exchange – the police, banks, hospitals, patent attorneys and companies of all kinds. Anyone with data to transfer that must remain secure. The possibilities for practical application are quite high!”

Source: [IST Results](#)

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.*