ETH zürich

NO. 2/2016

GLOBE

NEW THINKING

Key technologies and what we use them for

PAGE 14

Materials research: better and cheaper

PAGE 10

Why animal models are important for research

PAGE 42

Ulrich Graf – flying ace and pragmatist

PAGE 50

A new idea bears late fruit

Physicist Renato Renner wants to demonstrate the conditions that must be met for quantum cryptography to be secure. The fundamentals that he must first define open up a door to a whole new world.

Text Felix Würsten

When Renato Renner talks to laypeople about his work, they quickly feel that they have been plunged into a highly abstract world. As a professor of quantum information theory, Renner conducts research in many fields, including the foundations of quantum cryptography. The hope is that this area will open up possibilities for data transmission processes that offer more security. In contrast to today's encryption processes, which are based on the laws of classical physics, quantum cryptography is based on the laws of quantum mechanics. The basic concept underlying it is that sender and receiver exchange individual entangled photons or specially prepared light particles. What makes this exchange secure is the fact that, thanks to quantum-mechanical entanglement, both sender and receiver will notice immediately if an unauthorized third party "eavesdrops" on the data.

Although this exchange of photons sounds terribly futuristic, there are already commercial devices on the market that can quantum encrypt information. However, the process still has one major drawback: since only individual photons are exchanged, the physical distance is limited to a maximum of 100 kilometres. Large data networks would therefore require relay stations that can boost the signal en route.

ETH's special situation

These relay stations are called "quantum repeaters", and are currently the subject of intense research. "The challenge is not only to transmit quantum information, but also to store it for a brief period of time," Renner explains. At the moment, there are various competing approaches to exactly how to do this. The reason research in this area is so intensive is that, one day, these approaches will also be used for building what are known as quantum computers. Meanwhile, ETH Zurich is in a unique position: "Research in our department covers all the relevant approaches," Renner says.

Renner himself doesn't research any one individual technology, but instead is more concerned with the theoretical foundations. For him, the crucial question is how to use maths and physics to prove that quantum cryptography is truly secure. Answering this question calls for a new kind of thinking. You have to show not only that quantum mechanics correctly explains the exchange of photons, but also that this theory is complete; in other words, that it can sufficiently explain all conceivable results.

In an ideal world, the photons will be so entangled that an attacker from the outside has no chance of eavesdropping on the information un- ›

INFORMATION AND QUANTUM PHYSICS

The Group for Quantum Information Theory at ETH Zurich is concerned with the issue of how the processing and transmission of information relates to the laws of physics. One of the group's research goals is to investigate what options quantum physics opens up for information processing and how these opportunities are specifically to be used. Another goal is to achieve a deeper understanding of the physical relationships by studying quantum-mechanical phenomena from the perspective of information processing.

Renato Renner is Professor for Theoretical Physics and head of the research group for Quantum Information Theory. After earning his doctorate at ETH Zurich, he was a research fellow at the University of Cambridge. In 2007 he returned to ETH as an Assistant Professor.

noticed. In the real world, how- ever, the devices do not function perfectly. For example, it may be that the sender sends off not a series of single photons but batches of them instead. It would then be theoretically possible for an attacker to intercept individual photons without being noticed, thus accessing the information. With the help of complex statistical calculations, Renner hopes to show the requirements that must be met in order for data to be transmitted securely, even with imperfect devices.

On the threshold of a new world

At any rate, for Renner, quantum cryptography is "just" a means to an end. "What I'm aiming for is a fundamental understanding of the physics. We are working to open up the doors to a whole new world – one that we barely know. Opening these doors will expand our awareness of how the world works."

Renner sees quantum physics as a prime example of how investment in basic research pays off. The foundations of quantum mechanics were developed about a century ago, and for a long time the theory remained a largely abstract proposition for describing microcosmic phenomena. It was not until technological advances in several areas made it possible to investigate and manipulate materials down to the atomic level that people began to imagine concrete applications for it.

Renner is confident that "once we understand the basic principles, the applications will arise of their own accord. Quantum cryptography wasn't there at the beginning; rather, it was our understanding of quantum physics that later inspired the idea of using quantum mechanics to encrypt data." And there is no end in sight: high-precision measuring devices and powerful quantum computers that can solve certain tasks much more efficiently than today's computers are just two examples of how quantum mechanics might change our everyday lives. "Back when the first vacuum tubes were developed, no one could possibly have imagined how we would be communicating today with mobile phones," he says, "and we're currently in a comparable situation in quantum sciences."

It is also clear to Renner that, ultimately, it will not be technology that determines which of the applications will actually be realized. "Setting up a quantum cryptographic data network requires major investment," he says, "but the decision on whether or not to make this investment in order to enable secure data transmission lies not with physicists, but society." ○

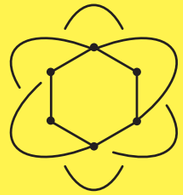
Group for Quantum Information Theory:
→ www.qit.ethz.ch

Photo: Daniel Winkler

How quantum mechanics is changing our world

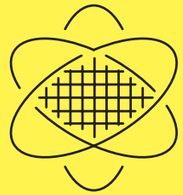
The basic principles of quantum mechanics were developed between 1925 and 1936, as classical physics was unable to correctly describe the behaviour of atoms and molecules. Quantum mechanics uses terms and concepts that fundamentally contradict classical physics, and that are therefore difficult for the layperson to grasp. Nevertheless, quantum mechanics now impacts many areas of our everyday lives in very tangible ways.

Compiled by Felix Würsten



Chemistry

Using quantum mechanics as a basis, it's possible to predict precisely how atoms and molecules will behave. This makes it an important foundation for computer models that simulate chemical reactions.



Materials research

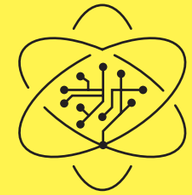
Today, we can analyse and modify materials right down to the atomic level – thanks, in part, to the scanning tunnelling microscope developed at IBM's research laboratory in Rüschlikon, near Zurich, in the early 1980s. The microscope is based on an important quantum mechanical phenomenon known as the tunnel effect.

Cryptography

A concrete technological application of quantum mechanics that is on the horizon is data encryption (see main article). Quantum cryptography enables data to be transmitted in such a way that no adversary can possibly intercept the information, regardless of how powerful their computing resources may be.

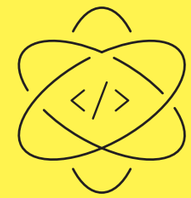
Metrology

Atomic clocks are exceedingly precise chronometers – but physicists are already thinking beyond this: they aim to develop nuclear clocks that are even more precise. These, too, are based on quantum mechanical phenomena, and would make the GPS we use for positioning in our day-to-day lives much more accurate.



Electronics

Electronic components are becoming ever smaller, but this miniaturisation will soon reach its limits. When transistors are only a few atomic layers thick, they no longer function according to the laws of classical physics – they follow the rules of quantum mechanics.



Computer science

It's the great dream of many physicists: to build a computer that works according to the laws of quantum mechanics. Such a computer could be used to solve certain computer science problems more efficiently than is currently possible, such as searching extremely large databases and factorising exceptionally long numbers.