Secret Code **in a Laser Pulse**

Soon, the NSA and other secret services may no longer be able to secretly eavesdrop on our communications without being detected – at least if quantum cryptography becomes popular. A team headed by **Christoph Marquardt** and **Gerd Leuchs** at the **Max Planck Institute for the Science of Light** in Erlangen is laying the foundations for the tap-proof distribution of cryptographic keys even via satellite. For the time being, the researchers have brought quantum communication into the light of day.

TEXT **ROLAND WENGENMAYR**

Secret services probably wouldn't like what they'd find on the top floor of the Max Planck Institute for the Science of Light. The experiment set up in front of us represents the only guaranteed way of communicating without being intercepted. To this end, quantum cryptography – the enigmatic name given to this technology – uses quantum physics in a very targeted way. There are even commercial systems already on the market, but the technology is still in its infancy. It is still far removed from making global communication possible.

The Erlangen-based physicists have now succeeded in making a quantum leap, so to speak, in this field. They are the first research team in the world to be able to send particularly sensitive quantum information in broad daylight through shimmering, streaky, hazy air. This means they have no need for fiber optic cables, which aren't yet suitable for global quantum communication.

We're standing next to the sender station, traditionally called Alice, because A as in Alice communicates with B as in Bob. Bettina Heim points through the opening in front of us to the computer science building of Friedrich-Alexander University Erlangen-Nuremberg (FAU), which hovers on the horizon in the haze of this sunny February afternoon. There, 1.6 kilometers away, is the receiving station known as Bob. It can't be seen with the naked eye. Bob collects the laser light arriving from Alice with its 15-centimeter-diameter telescopic lens and focuses it into a receiver. The transmission works even under conditions as hazy as those at the moment, explains Christian Peuntinger with pride. The successful experimental setup, which the physicist helped develop, is currently being retrofitted for further experiments.

THE TOUGHEST TEST FOR SIGNAL TRANSMISSION

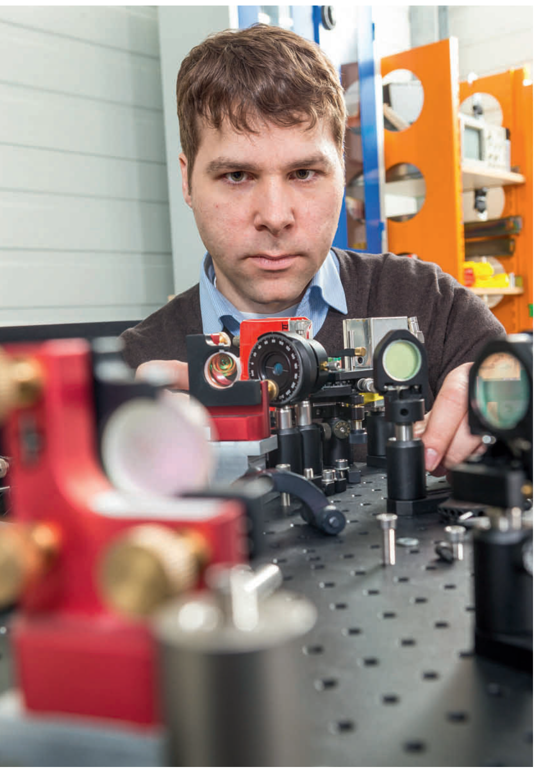
We're in the department of Gerd Leuchs, one of the Founding Directors of the Max Planck Institute for the Science of Light, which is a mere five years old. "The various groups in my department investigate different aspects of light," explains Leuchs: "And Christoph Marquardt's group focuses on quantum information processing, which includes quantum cryptography." Bettina Heim and Christian Peuntinger are doing their doctorates in the team. Marquardt explains how surprisingly well the experiment in Erlangen works – after all, the quantum information it sends out is hypersensitive. "This transmission path is almost the toughest test for signal transmission there is, because the path is very close to ground," explains the physicist: "Trees, heated streets and buildings create extremely disruptive air turbulences."

This has consequences: The laser beam expands to a diameter of more than 15 centimeters en route. "Without these perturbations, it would be just 4 centimeters," says the physicist. The special quality of the laser light suffers, as well. It is characterized by the fact that the light waves of the individual light quanta, the photons, propagate to the same beat. Undisturbed laser light thus has clean wave fronts – like the crests of ocean waves travelling nicely in parallel. "But the air turbulences distort these wave fronts," explains Marquardt: "And this is also bad for the quantum information being carried along."

But the team in Gerd Leuchs' department has found a smart way to embed the quantum information in the laser light so that it is so well protected that it survives these distortions.

Photo: Axel Griesch

Alice in eye contact with Bob: The researchers use bright laser pulses from a sender station called Alice, in the Max Planck Institute for the Science of Light, to transmit quantum information to a receiver named Bob, which is installed 1.6 kilometers away in a building at Friedrich-Alexander University Erlangen-Nuremberg.



Christoph Marquardt aligns the setup of a new sender station.

How exactly this works will occupy us throughout the afternoon. Here, looking out of the small window into the February sun, Bettina Heim points out a further advantage of their approach. The researchers in Erlangen were the first to succeed in imprinting the quantum information onto relatively bright laser pulses.

Previous open-air experiments, in contrast, used individual photons as information carriers. The price for this is extremely weak light, which makes it necessary to have particularly sensitive receivers. Owing to their special design, these receivers also have a very difficult time filtering out the tiny light quanta with the information sought from the photons beating down in the glaring sunlight.

This explains why such open-air experiments in bright daylight are a challenge. In the experiment in Erlangen, on the other hand, it isn't only the light pulses that are robustly bright compared to the background: the information is also embedded in them so intelligently that the bright background light causes no problems when it is read out. But why do researchers want to send information through the open air at all? Quantum information can also be sent via optical fibers, which provide a well-protected transport path for light.

"Transmitting through the air makes us less dependent on the infrastructure," emphasizes Bettina Heim. And there is an additional, as yet unsolved problem for fiber optic transmission: After around a hundred kilometers, the laser pulses in the fibers are attenuated to such an extent that they must be refreshed for longer distances. In today's optical fiber networks, the light is thus regenerated at regular intervals for the transmission of conventional digital information.

However, the sensitive quantum information is destroyed by today's amplifier technology. While so-called quantum repeaters should one day be able to pass on quantum information over greater distances, such repeaters don't yet exist. Open-air transmission, in comparison, can overcome great distances even without a repeater. With the sensitive individual photons, European researchers have already achieved 144 kilometers – albeit in the clear night air on the Canary Islands.

"But we can also communicate over much larger distances – with satellites," says Christoph Marquardt, explaining a further advantage. And this is precisely what is involved in the exciting race in which research groups from China, Japan, Canada, the US and Europe are currently competing. The objective: Who is most successful at transmitting the highly sensitive quantum information between a satellite and Earth? With their new technique based on bright laser pulses, the researchers in Erlangen have attained a good position for themselves in this race and are now preparing experiments with satellites.

SECURE CONNECTIONS AROUND THE GLOBE

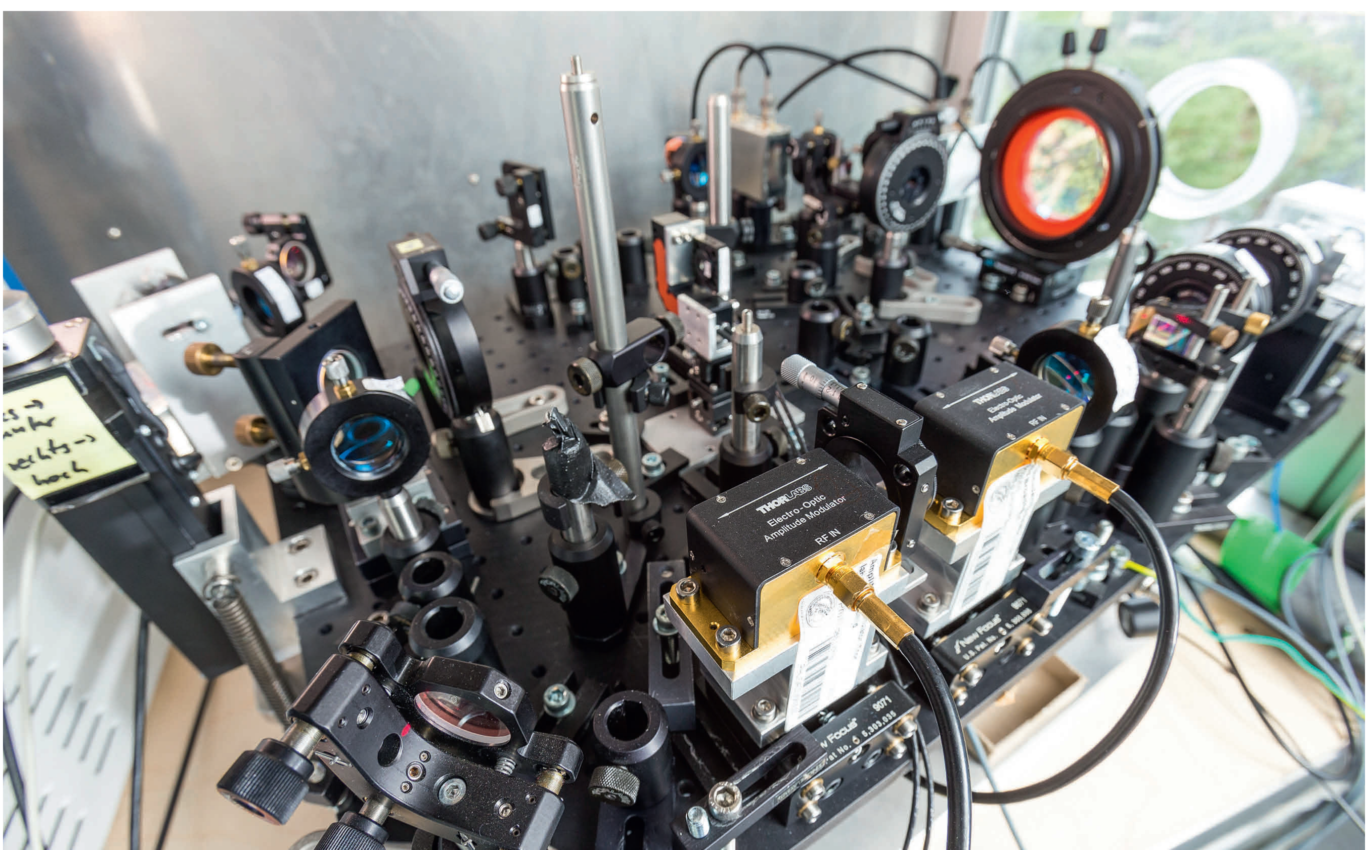
Functioning quantum communication with a satellite is a huge technical challenge. For this project, the Max Planck researchers are conducting basic research. But everybody knows, of course, that a technical breakthrough would allow connections around the globe that can't be intercepted. Chinese physicists recently received the equivalent of around one hundred million dollars for such a project. "China has classified this as one of five strategically particularly important space missions," emphasizes satellite expert Dominique Elser. "This news subsequently set something in motion politically in other countries as well," adds Marquardt.

A few floors below, Imran Khan demonstrates the Erlangen receiver that is currently being built for satellite communication. Sat-Bob is as compact as the experiment on the roof and would fit into a shoebox. "We are currently testing several different versions," says the doctoral student. Lenses and many other components are mounted on breadboards, solid metal plates with holes. The instrument looks surprisingly unspectacular, considering the fact that it is to communicate over a distance of more than 36,000 kilometers. This is the orbital altitude of the geostationary satellite that will be involved. Geostationary satellites have the advantage that they orbit Earth's surface synchronously: from the ground, they appear to be nailed to the sky. >

Photo: Axel Griesch

Right: In a porch of a technical services room on the institute's roof, the researchers in Erlangen have installed the sender they use to transmit quantum information through the air in bright daylight.

Below: The researchers use the two black and gold boxes as a kind of typewriter for quantum information. These are modulators in the sender station with which the researchers generate the signals for their experiments.



Photos: Axel Griesch (2)

Ready to receive: Bettina Heim and Christian Peuntinger prepare the receiver Bob, which is set up for the experiment in the computer science building at Friedrich-Alexander University Erlangen-Nuremberg.

Suitable satellite technology does actually already exist – and comes from Backnang, near Stuttgart. This is where the company Tesat-Spacecom has its headquarters. The company developed a laser communication system for the Sentinel Earth observation satellites of the European Space Agency (ESA) and for other satellites.

The Sentinel satellites fly low, which is why they are visible to the ground station for only a brief period. "Their data is therefore not transmitted directly to the ground, but to satellites in the geostationary orbit that also have Tesat laser communication systems on board," says Dominique Elser: "These laser communication terminals (LCTs) serve as communication relays because they are always at the same point in the sky as seen from the ground station." Elser, who works on the satellite project, explains that the LCTs already contain a large portion of the technology that is necessary for quantum communication via laser beam. They therefore already satisfy the technical requirements for quantum cryptography.

Fundamentally, quantum cryptography requires two channels. Alice and Bob exchange quantum signals via one channel. This channel must be secure, and quantum physics can guarantee just that. Through a second channel, which may even be public, the two can then exchange some of their measured quantum signals as a check.

ONLY QUANTUM PHYSICS KNOWS REAL RANDOMNESS

The key based on the exchanged quantum signals must also be secure, of course. Quantum physics can provide crucial help here as well: only it knows real randomness, the perfect roll of the dice. From a technical point of view it is surprisingly difficult to generate randomness. A roll of the dice or the drawing of lottery numbers could be computed if the original condition of the dice or the lottery balls were known precisely enough, and if there were sufficient computational power to rigorously calculate the effect of the physical laws on them.

Even today's computers can generate only pseudo-random numbers that always contain a systematic, predictable part. Marquardt's team is thus working also with Austrian colleagues on a quantum mechanical random number generator that is to fit onto a USB stick. Alice can use such a device to generate a chain of guaranteed true random numbers.

The word cryptography comes from Ancient Greek and means "secret writing." Quantum cryptography, however, actually deals with the secure exchange of a key. The term quantum key distribution is therefore closer to what happens. But how does quantum physics provide security in the quantum channel?

This is where Eve comes into play. "Eve" is derived from the word eavesdropper. And this spy does exactly that. With messages that aren't quantum encrypted, it is technically no problem for her to split off a little of the light and thus eavesdrop completely unnoticed. But this changes as soon as Alice and Bob exchange true quantum information. Now any eavesdropping attempt by Eve unavoidably leaves trac-

Photo: Axel Griesch

es. Alice and Bob can detect this by using the public channel to compare a portion of the signal sent by Alice with the one received by Bob.

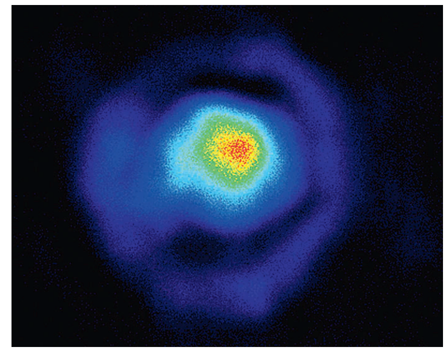
The reason for Eve's problem is that quantum information can't be perfectly copied – it can only be transmitted. In science, this is called the no-cloning theorem. Reading quantum information corresponds to a measurement on the information carrier, such as a photon. According to quantum mechanics, any measurement inevitably changes the object measured. Reading quantum information can be imagined to be a bit like a letter that is written in light-sensitive secret ink that quickly fades when the letter is opened.

Conventional information, such as digital zeroes and ones, can be copied only because quantum effects are of no consequence here. Usually such information is carried by very large numbers of photons or electrons that behave like objects of classical physics in these quantities. Quantum information can actually be transferred from one carrier to another by means of what is known as quantum teleportation – for example from a photon, as the so-called flying quantum bit (qubit), to an atom, as a qubit resting in a memory. However, this process doesn't amount to copying, because the quantum information is deleted in the original information carrier. Eve can therefore never copy quantum information undetected in order to read it.

A METHOD FROM CONVENTIONAL RADAR TECHNOLOGY

By transferring sensitive quantum information to bright laser pulses, the Erlangen-based researchers have pulled off a remarkable technical feat. What they needed here was special light and a method from conventional radar technology. This homodyne method uses the wave properties of the signal carrier in a clever way. In simple terms: it mixes a very weak signal that contains the actual information with a very strong carrier signal.

If we imagine this signal as water waves, it corresponds to a fine, regular ripple on a heavy swell. With the aid of this method, the receiver can detect the weak signal wave – figuratively speaking the ripple on the swell – with great sensitivity. Even after an arduous journey through a disturbing environment,



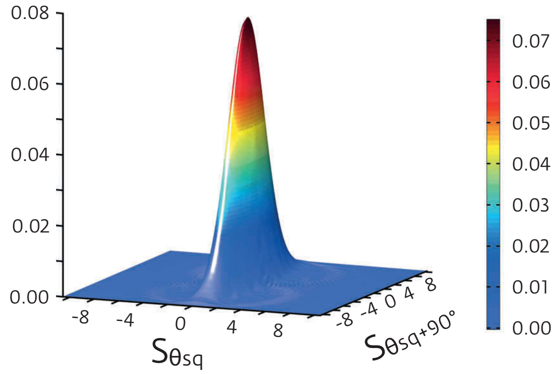
Distorted by turbulences: The intensity profile of the transmitted beam (blue – low intensity; red – high intensity) shows that, after being transmitted through air, the beam is no longer symmetric with respect to the axis of the direction of propagation. The Erlangen-based researchers therefore write the quantum information into the polarization of the light, which the turbulences don't affect.

it still reliably finds the signal. The physicists in Erlangen use precisely this by imprinting the sensitive quantum state onto a bright laser transport beam.

Quantum communication can be carried out particularly well with “squeezed light.” This is a form of light that is not known in nature. It can be produced artificially from laser light. A further characteristic of the quantum world comes into play here: Heisenberg's uncertainty principle. This states that, in the quantum world, pairs of physical quantities that have a special mutual relationship can't be determined at the same time with arbitrary precision. In physics, this special pair relationship is called complementary. One example is the velocity and the position of a quantum object. It is a fundamental principle that the two quantities can't be exactly determined simultaneously. >

Bob's eye: This lens enables the receiver to collect the light signals that Alice sends. The receiving station is located in the center of the lens, upside down.

Photos: MPI for the Science of Light (top), Axel Griesch (bottom)



Profile of the squeezed light: In quantum mechanics, two quantities of a pair of characteristics can't be measured with arbitrary precision. Although physicists can increase the precision of one quantity ($S_{\theta sq}$), they lose precision in the other quantity ($S_{\theta sq+90°}$) in the process. Researchers in Erlangen have successfully transmitted such a squeezed state through the atmosphere, as this reconstruction shows.

So in the quantum world, the quantum traffic police would have a problem. They could either measure the speed of a potential traffic offender with their radar precisely enough for a ticket – but then the license plate on the photo would be out of focus; or they could take a photo that is in focus, but then they wouldn't obtain enough information about the speed.

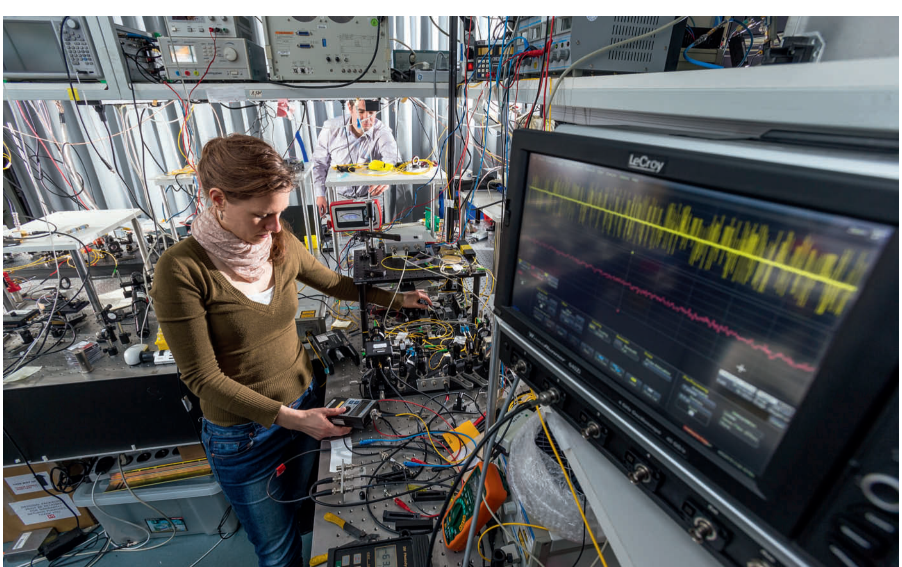
Nevertheless, quantum physicists can make a trade-off with the precision of the two complementary quantities: They can render one quantity, which characterizes one quantum state, more precisely at the expense of the complementary quantity. The state is then referred to as "squeezed". In their laser light, the researchers in Erlangen squeeze a different pair of characteristics than position and velocity. They use the polarization of the light. This quantity describes the direction in which the light wave oscillates up and down, so to speak. A light wave traveling through space fundamentally has complementary directions of oscillation that can't simultaneously be determined with arbitrary precision. Marquardt's group squeezes these polarization pairs.

MORE INFORMATION IN A LASER PULSE

The method has the advantage that the polarization robustly survives perturbations in the air. "Even if the turbulences completely distort the wave fronts of a laser pulse, the polarization in the pulse is maintained," says Marquardt. The quantum information therefore has a smooth journey from Alice to Bob. And the Erlangen technology provides even more advantages. The methods used so far are based on a kind of Morse code of light with individual photons from which Bob's receiver generates individual clicks. In the method used in Erlangen, the quantum information can be packaged not just in clicks, but also continuously. Significantly more information thus fits into a laser pulse, paving the way for faster and more efficient transmission of information.

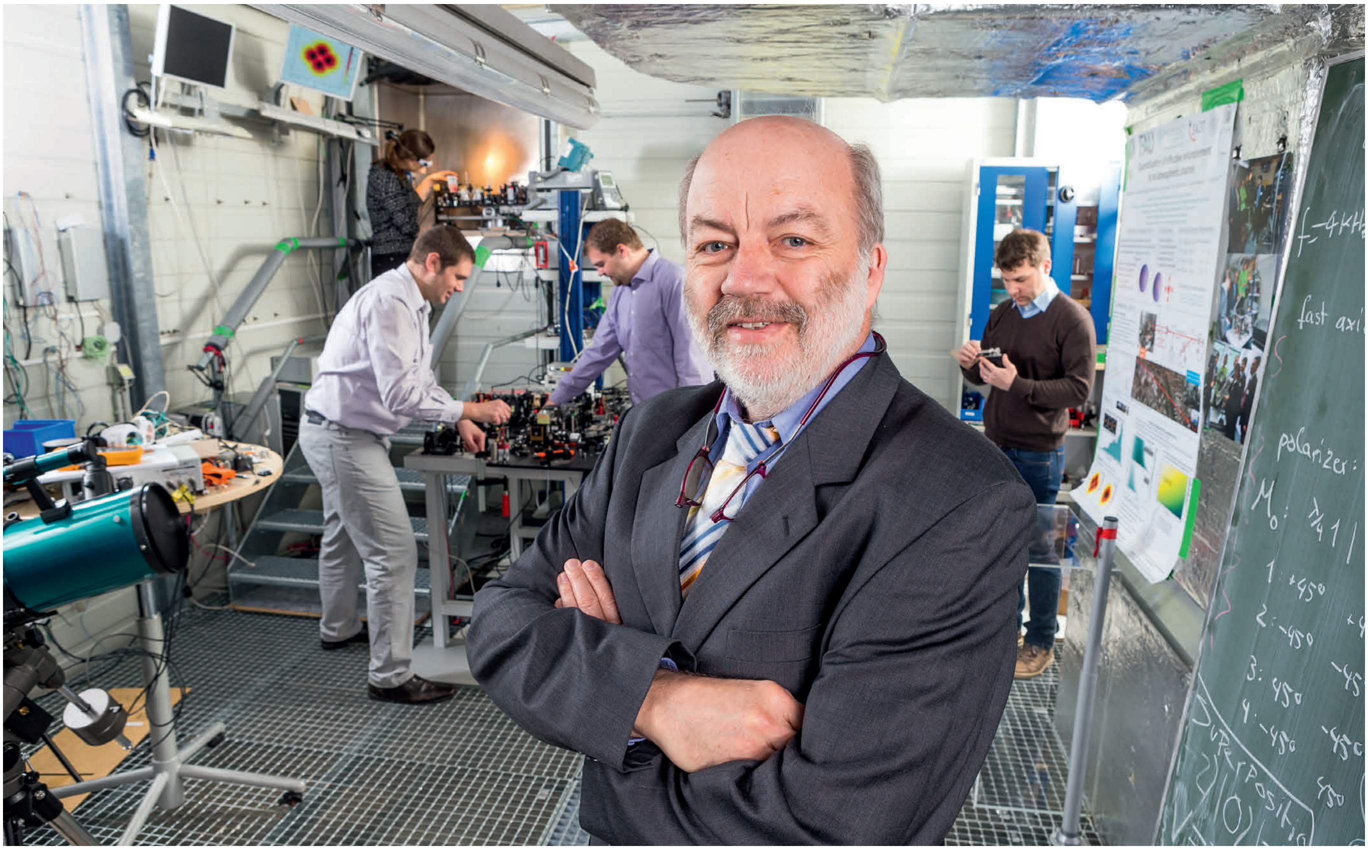
The satellite experiment, with the participation of the Erlangen-based researchers, also has a "nice secondary aspect," explains Marquardt in conclusion. This is an understatement, as it involves one of the greatest unanswered questions in physics: "It would be the first time that such a quantum state is transmitted over such a large distance through Earth's gravitational field," explains the physicist. According to Einstein's general theory of relativity, which celebrates its 100th birthday in 2015, a clock on the Earth's surface ticks more slowly than one on a satellite at an altitude of 36,000 kilometers.

If a highly sensitive quantum state travels between space and Earth, it should experience the effects of the general theory of relativity. At present, no one can precisely predict what will happen to the state, because no one has yet succeeded in unifying the general theory of relativity with quantum theory to produce a unified theory of physics. Although theoretical physicists have put forward competing proposals



Quantum information about to leap into space: Birgit Stiller tests a receiver for laser pulses from satellites.

Graphic: Phys. Rev. Lett. 113, 060502 (2014), http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.113.060502; photo: Axel Griesch



Team work for secure communication: Gerd Leuchs (in the foreground), Bettina Heim, Dominique Elser, Christian Peuntinger and Christoph Marquardt (behind, from left) want to enable new applications for quantum communication, such as secure data exchange via satellites.

that describe how such quantum gravitation could work, none have been confirmed as yet.

The satellite experiment could perhaps shed some light on this. "The measurable effects would certainly be minuscule, but it might be possible to explore limits," says Marquardt cautiously. This could lead to some of the current models of quantum gravitation being dropped, and theoretical physics would have new clues to continue its research.

It's surprising how closely basic research is linked to its technical application in quantum information technology. "As we are a Max Planck Institute, application doesn't have top priority," explains Gerd Leuchs. "But sometimes direct connections to new technologies just come about, which makes it all very nice." It is important to the Director that young people in Erlangen also have a chance to learn about fascinating new technologies that have their roots in basic research. "After all, the general public funds our basic research through taxes, and this is the best service we can offer them." ◂

TO THE POINT

- **Quantum cryptography allows information to be transmitted with absolute security. To this end, researchers at the Max Planck Institute for the Science of Light use the fact that quantum information can't be copied without errors, and that the quantum world knows true randomness.**
- **Over large distances, quantum information can be transmitted better through free space than through a fiber optic cable, as it can't yet be refreshed, unlike conventional information. Moreover, transmission through air is a necessary condition for quantum-encrypted satellite communication.**
- **Quantum communication has thus far used mainly individual photons as the information carriers, which are transmitted less efficiently during daylight. Now, for the first time, Max Planck physicists in Erlangen have sent quantum information through a turbulent atmosphere using bright pulses of light in daylight, and have thus helped expand the possible applications of quantum information to data exchange with satellites.**

GLOSSARY

Quantum communication: A subdomain of quantum information processing involving the transmission of quantum information, which differs fundamentally from conventional information: it can't be copied perfectly.

Quantum cryptography: An encryption technique in which information can be transmitted with absolute security. Various effects found in quantum physics are suitable for this, such as the fact that quantum information can't be copied without error.

Quantum repeater: A component that is currently the subject of intense research. The aim is to use it to teleport quantum information with the aid of quantum mechanical entanglement. Quantum repeaters can therefore avoid losses that occur in fiber optic cables when information is transmitted over great distances.

Photo: Axel Griesch