

New quantum transmission protocol has higher data transmission rate, robustness against interference

September 22 2021



Marcus Huber. Credit: Vienna University of Technology

Quantum cryptography is one of the most promising quantum technologies of our time: Exactly the same information is generated at two different locations, and the laws of quantum physics guarantee that no third party can intercept this information. This creates a code with which information can be perfectly encrypted.

The team of Prof. Marcus Huber from the Atomic Institute of TU Wien developed a new type of [quantum cryptography](#) protocol, which has now been tested in practice in cooperation with Chinese research groups: While up to now one normally used photons that can be in two different states, the situation here is more complicated: Eight different paths can be taken by each of the photons. As the team has now been able to show, this makes the generation of the quantum cryptographic key faster and also significantly more robust against interference. The results have now been published in the scientific journal *Physical Review Letters*.

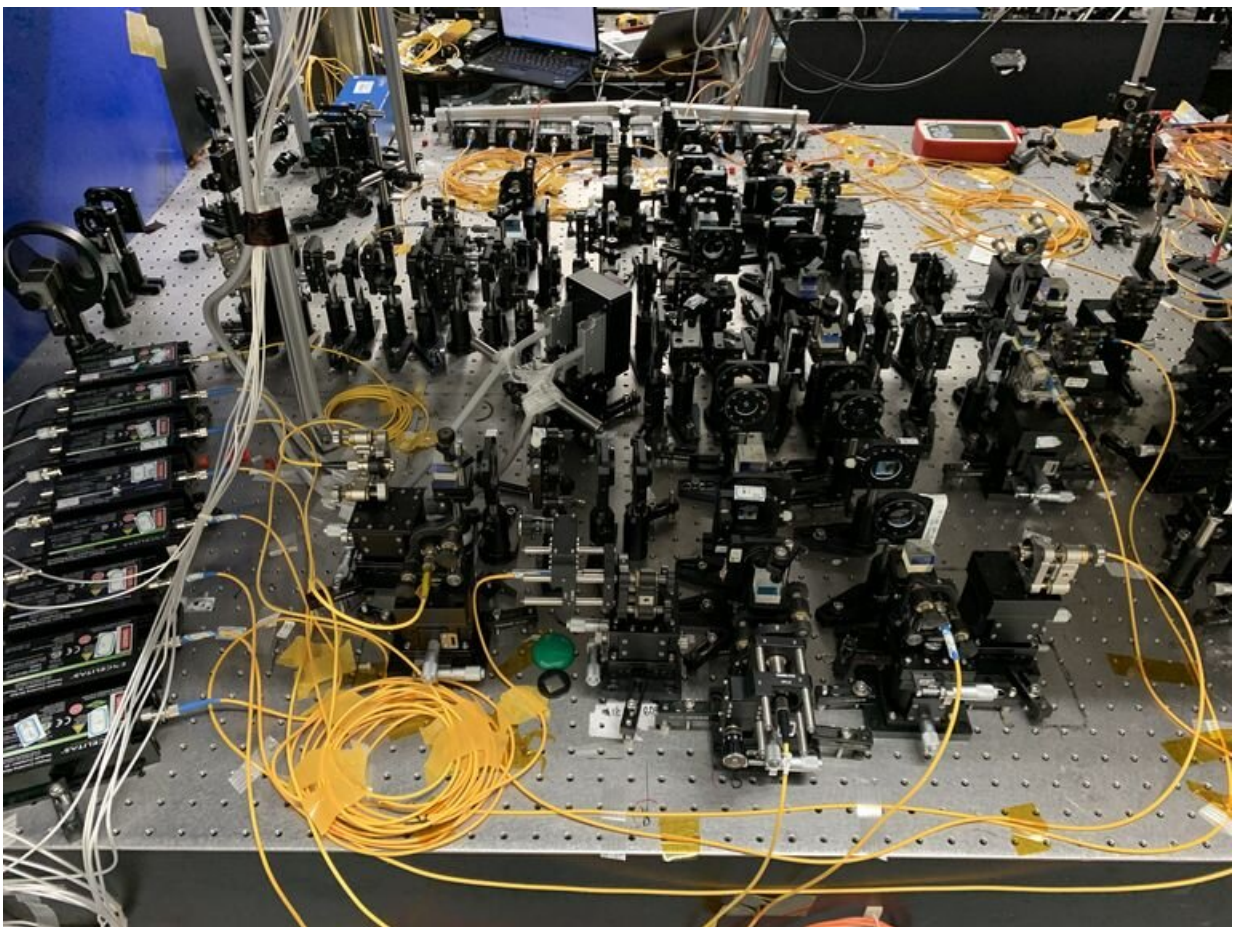
Two states, two dimensions

"There are many different ways of using photons to transmit [information](#)," says Marcus Huber. "Often, experiments focus on their photons' polarization. For example, whether they oscillate horizontally or vertically—or whether they are in a quantum-mechanical superposition state in which, in a sense, they assume both states simultaneously. Similar to how you can describe a point on a two-dimensional plane with two coordinates, the state of the photon can be represented as a point in a two-dimensional space."

But a photon can also carry information independently of the direction of polarization. One can, for example, use the information about which [path](#) the photon is currently traveling on. This is exactly what has now been exploited: "A [laser beam](#) generates photon pairs in a special kind of crystal. There are eight different points in the crystal where this can happen," explains Marcus Huber. Depending on the point at which the

photon pair was created, each of the two photons can move along eight different paths—or along several paths at the same time, which is also permitted according to the laws of quantum theory.

These two photons can be directed to completely different places and analyzed there. One of the eight possibilities is measured, completely at random—but as the two photons are quantum-physically entangled, the same result is always obtained at both places. Whoever is standing at the first measuring device knows what another person is currently detecting at the second measuring device—and no one else in the universe can get hold of this information.



Credit: Vienna University of Technology

Eight states, eight dimensions

"The fact that we use eight possible paths here, and not two different polarization directions as it is usually the case, makes a big difference," says Marcus Huber. "The space of possible quantum states becomes much larger. The photon can no longer be described by a point in two dimensions, mathematically it now exists in eight dimensions."

This has several advantages: First, it allows more information to be generated: At 8307 bits per second and over 2.5 bits per [photon](#) pair, a new record has been set in entanglement-based quantum cryptography key generation. And secondly, it can be shown that this makes the process less susceptible to interference.

"With all quantum technologies, you have to deal with the problem of decoherence," says Marcus Huber. "No quantum system can be perfectly shielded from disturbances. But if it comes into contact with disturbances, then it can lose its quantum properties very easily: The quantum entanglements are destroyed." Higher-dimensional quantum states, however, are less likely to lose their entanglement even in the presence of disturbances.

Moreover, sophisticated quantum error-correction mechanisms can be used to compensate for the influence of external perturbations. "In the experiments, additional light was switched on in the laboratory to deliberately cause disturbances—and the protocol still worked," says Marcus Huber. "But only if we actually used eight different paths. We were able to show that with a mere two-dimensional encoding a cryptographic key can no longer be generated in this case."

In principle, it should be possible to improve the new, faster and more reliable quantum cryptography protocol further by using additional degrees of freedom or an even larger number of different paths.

"However, this not only increases the space of possible states, it also becomes increasingly difficult at some point to read out the states correctly," says Marcus Huber. "We seem to have found a good compromise here, at least within the range of what is currently technically possible."

More information: Xiao-Min Hu et al, Pathways for Entanglement-Based Quantum Communication in the Face of High Noise, *Physical Review Letters* (2021). [DOI: 10.1103/PhysRevLett.127.110505](https://doi.org/10.1103/PhysRevLett.127.110505)

Provided by Vienna University of Technology

Citation: New quantum transmission protocol has higher data transmission rate, robustness against interference (2021, September 22) retrieved 28 April 2024 from <https://phys.org/news/2021-09-quantum-transmission-protocol-higher-robustness.html>

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