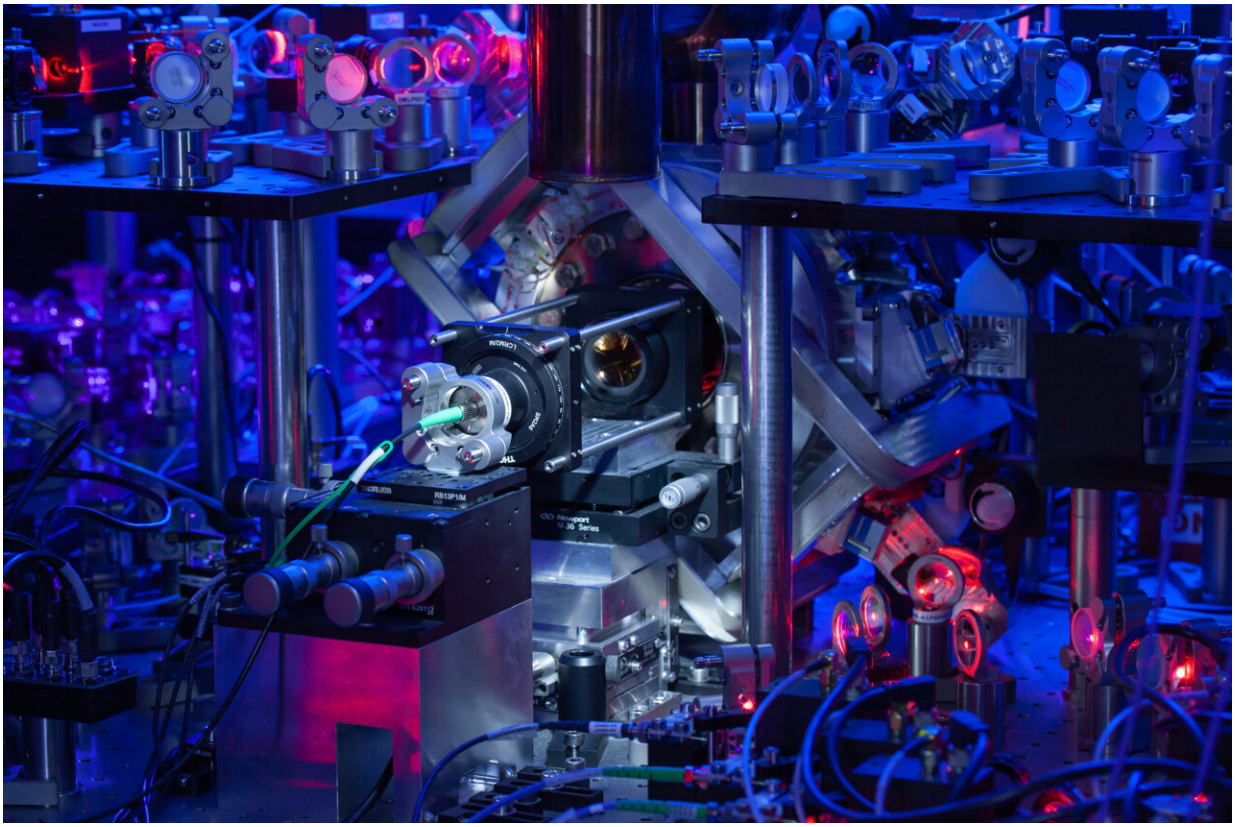
Quantum key distribution based on high-quality quantum entanglement

July 27 2022



One of the two ion traps used, seen in the center of the image. Around the trap run a number of laser beam lines for the preparation and manipulation of the ions. At the front of the trap, the end of the quantum network link to the other trap—an optical fiber—is visible. Credit: David Nadlinger/ University of Oxford

A method known as quantum key distribution has long held the promise

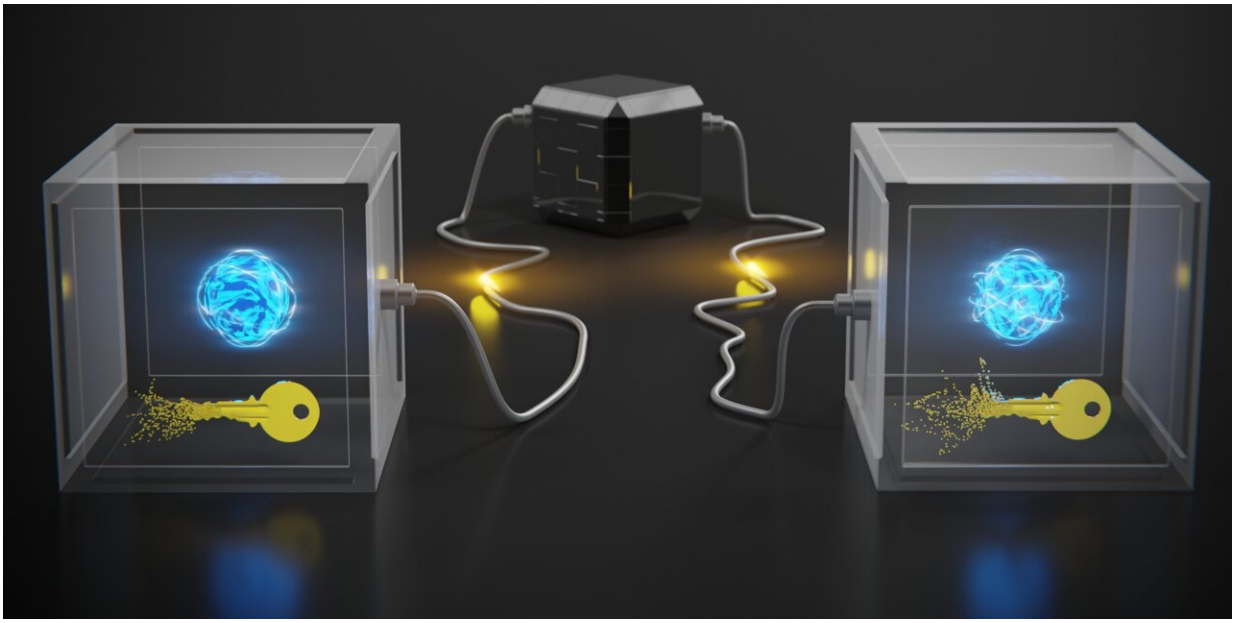
of communication security unattainable in conventional cryptography. An international team of scientists has now demonstrated experimentally, for the first time, an approach to quantum key distribution that is based on high-quality quantum entanglement—offering much broader security guarantees than previous schemes.

The art of cryptography is to skillfully transform messages so that they become meaningless to everyone but the intended recipients. Modern cryptographic schemes, such as those underpinning digital commerce, prevent adversaries from illegitimately deciphering messages—say, credit-card information—by requiring them to perform mathematical operations that consume a prohibitively large amount of computational power. Starting from the 1980s, however, ingenious theoretical concepts have been introduced in which security does not depend on the eavesdropper's finite number-crunching capabilities. Instead, basic laws of quantum physics limit how much information, if any, an adversary can ultimately intercept. In one such concept, security can be guaranteed with only a few general assumptions about the physical apparatus used. Implementations of such "device-independent" schemes have long been sought after, but remained out of reach. Until now, that is. Writing in *Nature*, an international team of researchers from the University of Oxford, EPFL, ETH Zurich, the University of Geneva and CEA report the first demonstration of this sort of protocol—taking a decisive step towards practical devices offering such exquisite security.

The key is a secret

Secure communication is all about keeping information private. It might be surprising, therefore, that in real-world applications large parts of the transactions between legitimate users are played out in public. The key is that sender and receiver do not have to keep their entire communication hidden. In essence, they only have to share one "secret"; in practice, this

secret is string of bits, known as a cryptographic key, that enables everyone in its possession to turn coded messages into meaningful information. Once the legitimate parties have ensured for a given round of communication that they, and only they, share such a key, pretty much all the other communication can happen in plain view, for everyone to see. The question, then, is how to ensure that only the legitimate parties share a secret key. The process of accomplishing this is known as "key distribution."



Artistic representation of device-independent quantum key distribution (DIQKD). Credit: Scixel/Enrique Sahagú

In the cryptographic algorithms underlying, for instance, RSA—one of the most widely used cryptographic systems—key distribution is based on the (unproven) conjecture that certain mathematical functions are easy to compute but hard to revert. More specifically, RSA relies on the

fact that for today's computers it is hard to find the prime factors of a large number, whereas it is easy for them to multiply known prime factors to obtain that number. Secrecy is therefore ensured by mathematical difficulty. But what is impossibly difficult today might be easy tomorrow. Famously, quantum computers can find prime factors significantly more efficiently than classical computers. Once quantum computers with a sufficiently large number of qubits become available, RSA encoding is destined to become penetrable.

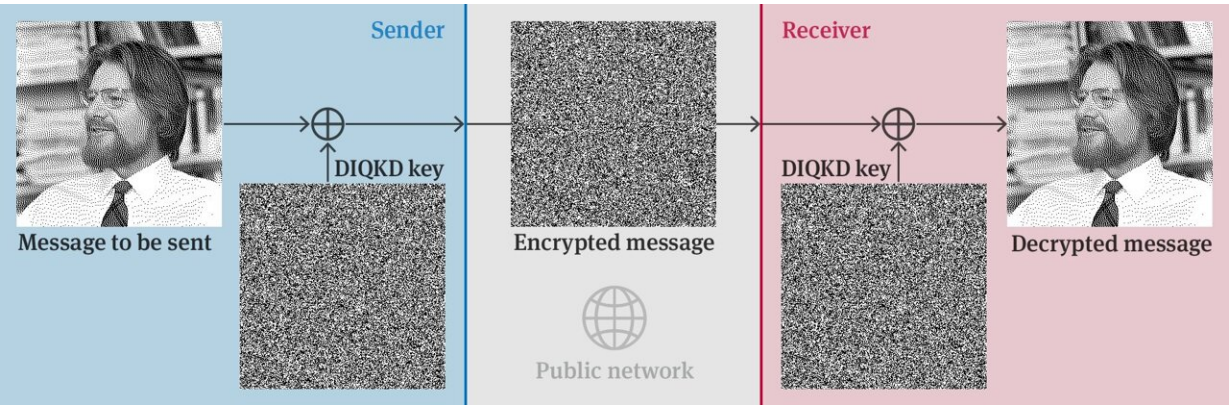
But quantum theory provides the basis not only for cracking the cryptosystems at the heart of digital commerce, but also for a potential solution to the problem: a way entirely different from RSA for distributing cryptographic keys—one that has nothing to do with the hardness of performing mathematical operations, but with fundamental physical laws. Enter quantum key distribution, or QKD for short.

Quantum-certified security

In 1991, the Polish-British physicist Artur Ekert showed in a seminal paper that the security of the key-distribution process can be guaranteed by directly exploiting a property that is unique to quantum systems, with no equivalent in classical physics: quantum entanglement. Quantum entanglement refers to certain types of correlations in the outcomes of measurements performed on separate quantum systems. Importantly, quantum entanglement between two systems is exclusive, in that nothing else can be correlated to these systems. In the context of cryptography this means that sender and receiver can produce between them shared outcomes through entangled quantum systems, without a third party being able to secretly gain knowledge about these outcomes. Any eavesdropping leaves traces that clearly flag the intrusion. In short: the legitimate parties can interact with one another in ways that are—thanks to quantum theory—fundamentally beyond any adversary's control. In classical cryptography, an equivalent security guarantee is provably

impossible.

Over the years, it was realized that QKD schemes based on the ideas introduced by Ekert can have a further remarkable benefit: users have to make only very general assumptions regarding the devices employed in the process. By contrast, earlier forms of QKD based on other basic principles require detailed knowledge about the inner workings of the devices used. The novel form of QKD is now generally known as device-independent QKD (DIQKD), and an experimental implementation thereof became a major goal in the field. Hence the excitement as such a breakthrough experiment has now finally been achieved.



Once two parties have obtained a secret key using device-independent quantum key distribution (DIQKD), they can use it for provably secure communication. Illustrating this in the experiment, the sender transmits to receiver an encrypted picture of John Stewart Bell, whose theoretical arguments about the limits to correlations in nature lie at the heart of device-independent security. Credit: David Nadlinger/ University of Oxford, original photo of J. S. Bell: CERN

Culmination of years of work

The scale of the challenge is reflected in the breadth of the team, which combines leading experts in theory and experiment. The experiment involved two single ions—one for the sender and one for the receiver—confined in separate traps that were connected with an optical-fiber link. In this basic quantum network, entanglement between the ions was generated with record-high fidelity over millions of runs. Without such a sustained source of high-quality entanglement, the protocol could not have been run in a practically meaningful manner. Equally important was to certify that the entanglement is suitably exploited, which is done by showing that conditions known as Bell inequalities are violated. Moreover, for the analysis of the data and an efficient extraction of the cryptographic key, significant advances in the theory were needed.

In the experiment, the "legitimate parties"—the ions—were located in one and the same laboratory. But there is a clear route to extending the distance between them to kilometers and beyond. With that perspective, together with further recent progress made in related experiments in Germany and China, there is now a real prospect of turning the theoretical concept of Ekert into practical technology.

More information: Jean-Daniel Bancal, Experimental quantum key distribution certified by Bell's theorem, *Nature* (2022). DOI: 10.1038/s41586-022-04941-5.
www.nature.com/articles/s41586-022-04941-5

Provided by ETH Zurich