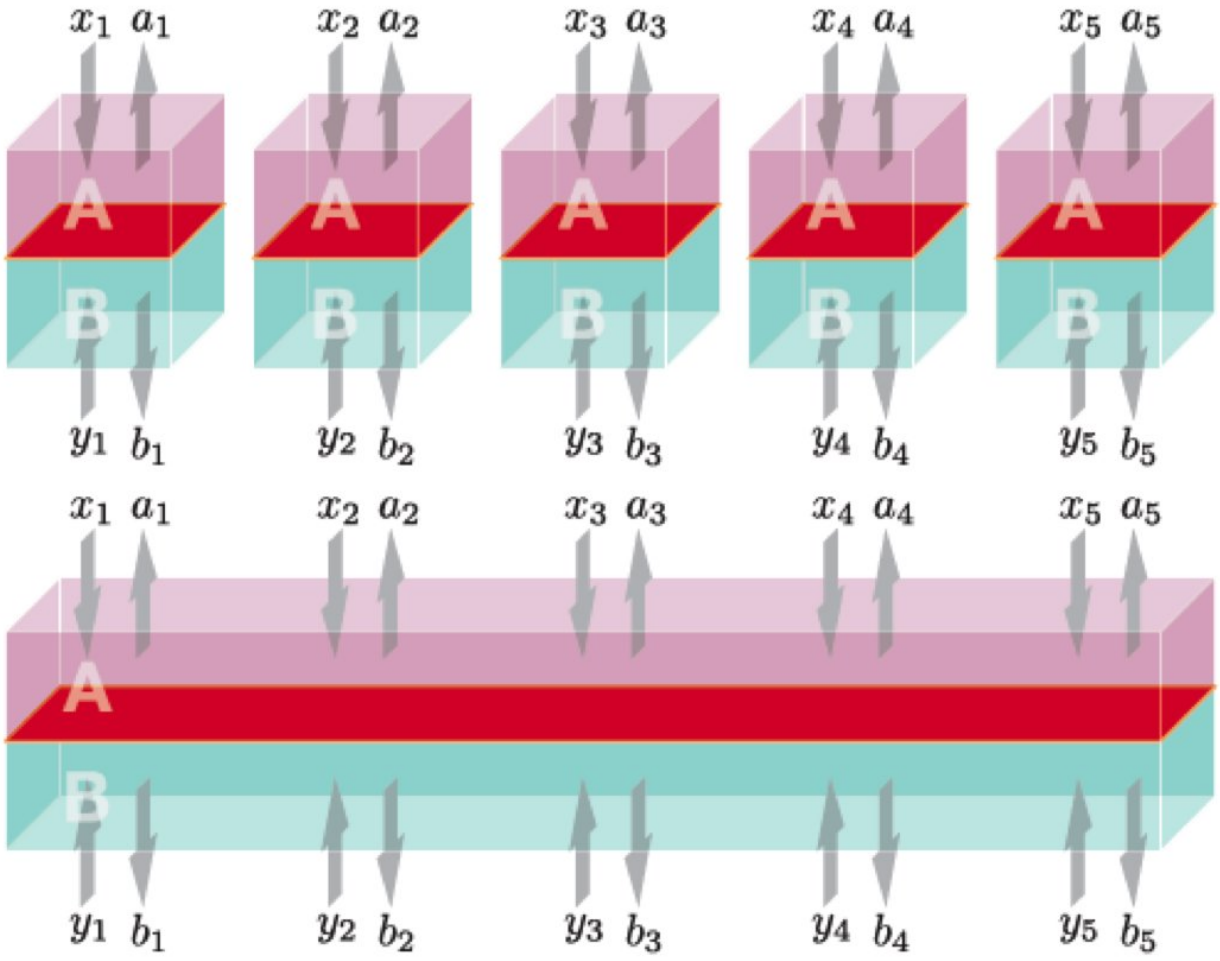
Trust is good, quantum trickery is better

February 1 2018



The key to proving the security of device-independent quantum cryptography in a regime that is attainable with state-of-the-art quantum technology is the realization that any attack strategy, no matter how complex (symbolized in the lower row), can be decomposed into a sequence of simple steps (upper row). Credit: (Image from Arnon-Friedman et al. *Nature Comms* 9, 459; 2018).

An international team of scientists has proven, for the first time, the security of so-called device-independent quantum cryptography in a regime that is attainable with state-of-the-art quantum technology, thus paving the way to practical realization of such schemes in which users don't have to worry whether their devices can be trusted or not.

In quantum cryptography, the laws of quantum mechanics are exploited to send messages with higher security than is possible in conventional cryptographic schemes based on classical physical phenomena. In principle, quantum communication enables absolute security—that is, no adversary can intercept messages or tinker with them. But in practice, such unconditional security is not currently possible. One main route for unauthorized access is advance manipulation of the communication devices that will be used later. Writing in *Nature Communications*, Rotem Arnon-Friedman and colleagues describe quantum-cryptographic protocols that ensure nearly optimal security, even if the devices are manipulated, and that such device-independent quantum cryptography should be possible with current quantum technology.

Device-independent quantum cryptography is the gold standard of quantum communication, as the advantages of quantum cryptography over its classical counterpart can be realized without having to worry whether the device can be trusted or not. This is an appealing prospect, but so far, device-independent quantum cryptography has been theoretical, with experimental requirements that are not achievable under realistic conditions.

Arnon-Friedman, a Ph.D. student in the group of Prof. Renato Renner in the Institute of Theoretical Physics at ETH Zurich, and co-workers in the U.S., France and the Czech Republic, developed a new theoretical concept called entropy accumulation, and applied it to quantum cryptography. They find that any attack strategy, no matter how complex, can be decomposed into a sequence of simple steps. This is

helpful for security proofs, which are notoriously difficult, because every possible attack strategy has to be taken into account. With their new approach, Arnon-Friedman and her colleagues have proven, for the first time, the security of device-independent quantum cryptography in a regime that is attainable with state-of-the-art quantum technology, thus paving the way to practical realization of such schemes.

More information: Rotem Arnon-Friedman et al, Practical device-independent quantum cryptography via entropy accumulation, *Nature Communications* (2018). DOI: 10.1038/s41467-017-02307-4

Provided by ETH Zurich