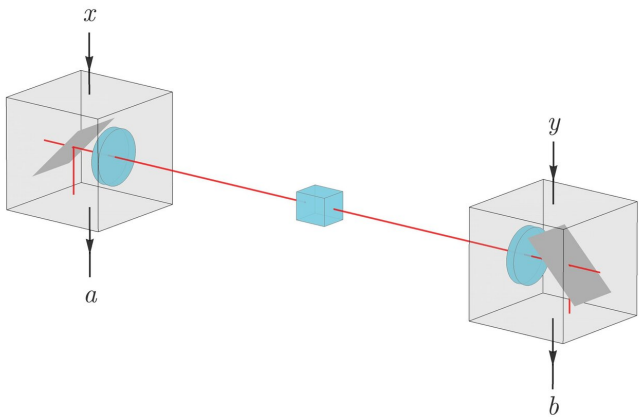
Applying advantage distillation to device-independent quantum key distribution (DIQKD)

4 February 2020, by Ingrid Fadelli



Standard QKD protocols require detailed knowledge of the internal workings of the devices. Credit: Tan, Lim & Renner.

Researchers at ETH Zürich and National University of Singapore have carried out a study investigating whether advantage distillation, a classical cryptography technique that has so far never been successfully implemented, can be applied to device-independent quantum key distribution (DIQKD) systems with the aim of creating a secret key for communication between different parties. The term DIQKD describes a novel form of quantum cryptography that allows honest users to certify information security using only the observed measurement statistics.

This means that security is based on the detection of quantum nonlocality, which guarantees that no other party, apart from the honest users, can be correlated to the generated key. DIQKD protocols, which are based on the laws of quantum physics, are an adaptation of more traditional quantum key distribution (QKD) approaches.

The key goal of conventional QKD approaches is to extract a key from correlations obtained by measuring a series of quantum systems. DIQKD protocols, on the other hand, are based on past observations suggesting that when these correlations violate a Bell inequality, a secure key can be extracted even if the different users devices are not fully characterized.

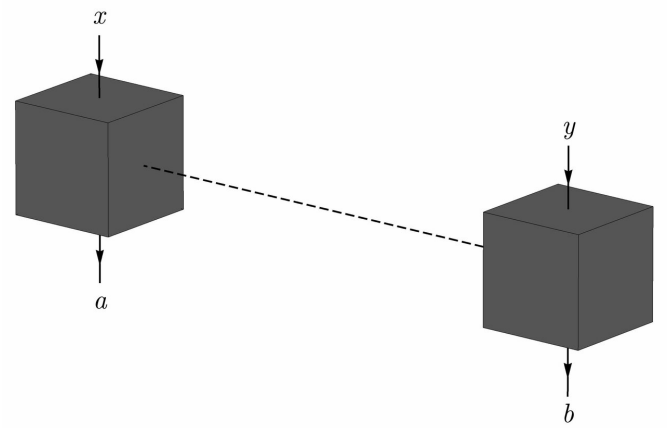
In other words, when assessing the security of DIQKD protocols, users do not need to assume that communicating devices are operating according to their specifications. This is in stark contrast with the device dependency observed in traditional QKD protocols, which typically assume that connected devices are implementing a specific range of quantum operations.

This unique characteristic of DIQKD can significantly enhance the security of communications and data exchanges, as it remains secure even if an attacker manages to influence the behavior of the users devices. This increased security, however, is often accompanied by a crucial limitation: To achieve positive keys rates, DIQKD protocols require low noise levels. In their paper, published in *Physical Review Letters*, Ernest Tan, Charles Lim and Renato Renner tried to overcome this limitation using a cryptography technique known as "advantage distillation."

"In the 1990s, classical cryptographers came up with the proposal to generate cryptographic keys from cosmic background radiation," Renner told Phys.org. "The idea was that the radiation can be measured everywhere, so two parties, say Alice and Bob, who would like to communicate secretly, can listen to the radiation and generate a common key from it, which they could then use for encrypting their communication channel. The (obvious) problem is, of course, that an adversary,

Eve, may listen to the same radiation, and hence infer the same key as well, so it wouldn't be secret."

To prevent a third party from accessing a private communication between two people, cryptographers introduced a technique known as advantage distillation. This technique allows two people who are communicating (e.g., Alice and Bob) to identify segments of cosmic background radiation where they have an advantage over an intruding party (e.g. Eve).



In contrast, with QKD, DIQKD can work with devices that are almost “black boxes”, required only to satisfy some minimal security assumptions. Credit: Tan, Lim & Renner.

This means that in these particular parts of radiation, Alice's measured signals are correlated more strongly to Bob's than they are to Eve's. As a consequence, these parts can be used to generate a secret key that Eve cannot access.

"While this idea seemed promising, it never made its way to practical applications," Renner said. "The reason for this is that the assumptions that have to be made about the radiation turned out to be unrealistic."

DIQKD and the scenario originally considered for advantage distillation share several similarities. In DIQKD, however, the radiation is replaced by a signal consisting of entangled particle pairs, distributed by an untrusted source, which may even be controlled by the third, intruding party. Based on this similarity, the researchers set out to explore whether the idea of advantage distillation is actually applicable to DIQKD and whether it can improve its tolerance against noise.

"A main challenge in DIQKD is that almost nothing is known about the information that the adversary Eve may have gathered," Renner explained. "In principle, that information could even consist of infinitely many qubits. We therefore had to use and further develop information-theoretic techniques that allow us to characterize such unstructured information."

Using the techniques they developed, the researchers were able to show that advantage distillation is possible even in extreme cryptography settings, such as in DIQKD. They found that their method allows for improvement of the noise tolerance thresholds beyond the previously known values, which should make it easier to achieve an experimental demonstration of DIQKD.

"The holy grail in the quantum cryptography community is to have a fully functioning and secure experimental demonstration of DIQKD," Renner said. "This, however, seems to be very challenging, and requires a joint effort from experimental and theoretical researchers."

Currently, several physicists are trying to improve existing DIQKD systems: experimentalists by reducing noise in communicating devices and theorists by developing protocols that are less demanding in terms of noise tolerance. The study carried out by Tan, Lim and Renner, which falls in the latter category, could ultimately pave the way to the development of new DIQKD frameworks that are both secure and fully effective.

"Our work shows that advantage distillation can improve the noise tolerance of DIQKD," Renner said. "However, our analysis is most likely quite far from optimal, as some of the (very powerful) methods from quantum information theory were not usable in the DI setting. This means that we now

need to explore whether the techniques we used can be generalized."

More information: Ernest Y.-Z. Tan et al. Advantage Distillation for Device-Independent Quantum Key Distribution, *Physical Review Letters* (2020). DOI: 10.1103/PhysRevLett.124.020502