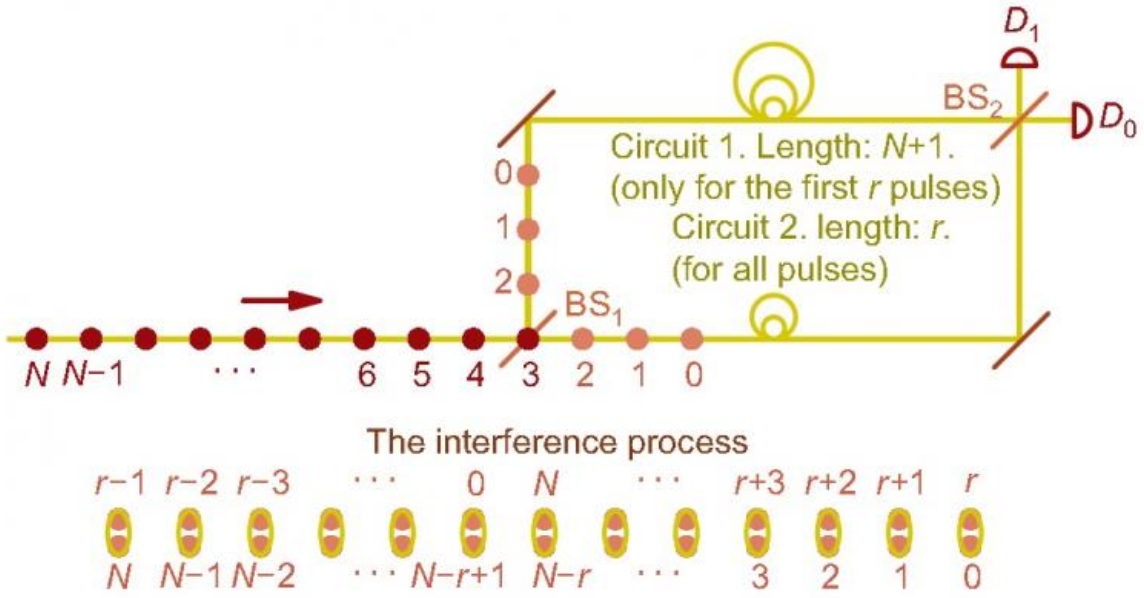
Scientists design a QKD-based quantum private query with no failure

November 30 2015



The interference wiring diagram of the newly proposed QPQ protocol, where the database generates a single-photon signal with N optical pulses and shifts the phase of each pulse randomly by 0 or π, then the user extracts the phase differential of two pulses of them by the circuits on the right side and a random number r. Credit: © Science China Press

Cryptography protects data secrecy in public environment. Certain cryptographic communications require not only the security of the

transmitted message against eavesdropping from an outside adversary, but also the communicators' individual privacy against each other. Symmetrically private information retrieval (SPIR), which deals with the problem of private user queries to a database, is an example of such communication protocols. In a SPIR protocol, Alice can obtain one item (i.e. one secret) from Bob's secret database in such a manner that Bob does not know which item Alice has obtained and, simultaneously, Alice cannot get additional items except the one she wanted in the database.

With the advantage of unconditional security, quantum cryptography has attracted a great deal of attention recently. Quantum private query (QPQ) is the quantum scheme for the SPIR problem. Since the first QPQ protocol was proposed by Vittorio Giovannetti et al in 2008, quite a few scholars have participated in the study of this interesting and important field. The original QPQ protocols are based on oracle operations. Though those protocols have significant advantages in theory, they are difficult to implement because the dimension of the oracle operation would be exceedingly high for a large database.

In 2011, to overcome this drawback, scholars proposed a new type of QPQ: quantum-key-distribution (QKD)-based QPQ. Based on the mature technology of QKD, this new kind of QPQ has the advantages of being easy to realize and loss tolerant. Therefore, as a practical model, QKD-based QPQ is overwhelmingly attractive and has become a research hotspot.

However, QKD-based QPQ seems somewhat unreliable in the sense that all the existing protocols would fail with a non-zero probability. Besides, the database would generally reveal some additional secrets to the honest user. Even worse, to reduce the failure probability, one must increase the expectation of the number of the revealed secrets. And improving the security of the database makes the protocol more likely to fail. It seems incompatible to mitigate these disadvantages of QKD-based QPQ.

However, researchers have removed these obstacles with a differential phase-shift (DPS) QKD protocol.

The DPS-QKD protocol was proposed by Toshihiko Sasaki et al. in the journal *Nature* in 2014. In this QKD protocol, participants no longer need to monitor signal disturbance. It can tolerate up to a 50 percent bit error rate by setting a parameter large enough, while the generally used BB84 protocol can only tolerate 11 percent. Additionally, the DPS-QKD protocol is naturally immune to the photon-number-splitting attack in which the adversary utilizes the imperfection of the photon source in practice. The technology of DPS has greatly promoted the development of QKD and captured a lot of research attention. Recently, researchers found that DPS is also beneficial for QKD-based QPQ.

Based on the DPS-QKD, a new QPQ protocol was proposed by Bin Liu, Fei Gao, Wei Huang and Qiaoyan Wen, scientists at the Beijing University of Posts and Telecommunications in Beijing. "It maintains the advantages of the QKD-based QPQ, being easy to implement and loss tolerant," according to the four scholars.

They revealed in the study, which was published in *Science China-Physics, Mechanics & Astronomy*, that it is the randomness in the dilution of the oblivious key, one of the main processes in such protocols, that caused the possible failure of previous QKD-based QPQ. By utilizing the features of DPS, their protocol successfully avoids the process of dilution.

Without the process of dilution, this new protocol becomes more reliable and reasonable, compared with the previous QKD-based QPQ protocols. Just as the scholars stated in their article: "Different from the situations in the previous QKD-based QPQ protocols, the number of the items an honest user will obtain is always one and the failure probability is always zero."

They also calculated an upper bound for the leaked information of the database in theory, and claimed that when the number of the database items "becomes larger, the advantage of our protocol's bound would be highlighted compared with the other QKD-based QPQ protocols."

What's more, just like the DPS-QKD, the QKD-based QPQ protocol proposed by the four scholars is also naturally immune to the photon-number-splitting attacks. Other QKD-based QPQ protocols without a perfect photon source would leak more database secrets than expected to both outside adversaries and dishonest users.

At the end of this article, the authors noted that "the proposed protocol is the first QKD-based QPQ protocol without the process of the oblivious key dilution, and, therefore, it is the first QKD-based one with no failure probability and no information reveal for the database when the user is honest." They add that "the proposed protocol initiates a new branch of QKD-based QPQ."

More information: Bin Liu et al. QKD-based quantum private query without a failure probability, *Science China Physics, Mechanics & Astronomy* (2015). DOI: 10.1007/s11433-015-5714-3

Provided by Science China Press