07 Generating absolutely secure shared secret keys

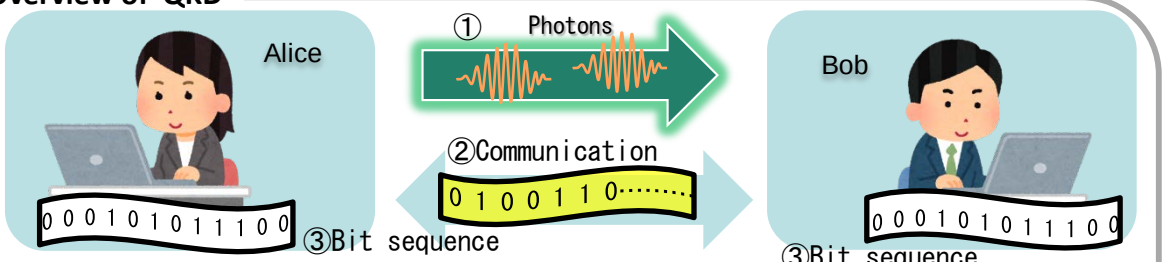
- Quantum key distribution using practical devices -

Abstract

Quantum key distribution (QKD) is a procedure to generate a secure bit string using very weak light and a public communication channel. The secure bit string supports many types of secure communication, and the security of QKD has already been theoretically proven. However, in the existing theories, some severe conditions are required, which may not always hold under realistic circumstances. Consequently, users of a QKD system cannot but trust its manufacturer, in the sense that they themselves cannot check whether or not the system satisfies those strict conditions. Here, we present our recent theoretical progress regarding relaxation of those conditions. We believe that this is a significant step toward a QKD system that allows users themselves to transparently verify its secureness without solely depending on a third party.

Genuinely secure communication is realized by sharing a secret bit string.

Overview of QKD



① Alice sends many photons to Bob.

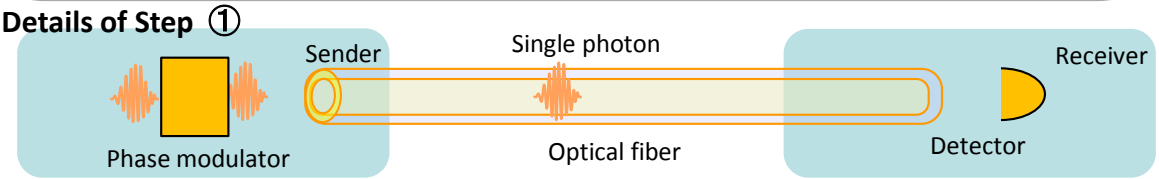
② They communicate with each other regarding the observed status of those photons.

③ Based on the communication, bit strings with guaranteed randomness are created that only Alice and Bob can share.

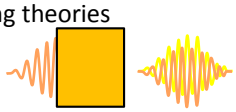
Key

- Secure random bit strings are generated.
- Procedure ① is done under quantum dynamics.

Details of Step ①

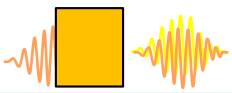


Existing theories



Degree of photonic phase shift (which encodes information) must be strictly precise.

Our theory



A certain amount of fluctuation in the phase shift is allowed.

Existing theories

Number of photons must be counted.

Our theory

Only the existence of photons matters.

Quantum dynamics plays an important role here.

References

[1] K. Tamaki, M. Curty, G. Kato, H. K. Lo, K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," Physical Review A, 90, 052314, 2014.

[2] G. Kato, K. Tamaki, "Security of six-state quantum key distribution protocol with threshold detector," Scientific Reports, 6, Article number: 30044, 2016.

Contact

Go Kato Computing Theory Research Group, Media Information Science Laboratory
E-mail: kato.go(at)lab.ntt.co.jp