TechAndComputer (Aug. 7, 2012) — Researchers at Tamagawa University announced August 10 that they had demonstrated the incompleteness and limit of the security theory in quantum key distribution. The present theory cannot guarantee unconditional security. Details will be given at the SPIE conference on Quantum Communication and Quantum Imaging on August 15, 2012.

Share This: **See Also:** **Computers & Math**

- Hacking
- Encryption
- Information Technology
- Quantum Computers
- Spintronics Research
- Statistics

Reference

- Security engineering
- Random variable
- Probability theory
- Cyber security standards

Many papers claim that the trace distance, d, guarantees unconditional security in quantum key distribution (QKD). In our paper, first we explain explicitly the main misconception in the claim of unconditional security for QKD theory. In general terms, the cause of the misunderstanding in the security claim is the Lemma in Renner's paper. It suggests that the generation of a perfect random key is assured by the probability (1-d), and that its failure probability is d. Thus, it concludes that the generated key provides a perfect random key sequence when the protocol succeeds. In this way QKD provides perfect secrecy (unconditional security) to a type of encryption termed 'the one-time pad'.

H. P. Yuen at Northwestern University proved that the trace distance quantity does not give the probability of such an event. If d is not small enough, the generated key sequence is never perfectly random. The evaluation of the trace distance now requires reconstruction if it is to be used. However, QKD theory groups have not accepted this criticism, and have invented many upper-bound evaluation theories for the trace distance.

We clarified that the most recent upper bound theories for the trace distance are constructed again by the reasoning of Renner, who originally introduced the concept. It is thus unsuitable to quantify the information theoretic security of QKD, and the unconditional security defined by

Shannon is not satisfied.

Consequently, Yuen's theory is correct, and at present there is no theoretical proof of the unconditional security for any QKD.

Background

Quantum information science holds enormous promise for entirely new kinds of computing and communications, including important problems that are intractable using conventional digital technology. The most expected field is quantum cryptography. But realizing that promise will depend on theoretical guarantee of the security and the ability to transfer an extremely fragile quantum condition. Recently it has been pointed out sometimes that, in general, scientists are not familiar with practical applications. The quantum cryptography (quantum key distribution: QKD) is a typical example of the stern realities.

Now, despite enormous progress in theoretical QKD, many theory groups are still discussing the security proof for QKD based on Renner's trace distance theory. One of reasons is that H.P.Yuen (Northwestern University) pointed out that the present theory does not guarantee the security of the real QKD system [1,2].

Recently, Renner et al announced that in any practical implementation, the generated key length is limited by the available resources, and the present security proofs are not established rigorously in such a situation. And they published own improvement result in Nature Communication in 2012 [3]. However, without the review of the incompleteness of the theory, it is repeatedly and persistently claimed that a specific trace distance criterion would guarantee unconditional security in QKD. And, unfortunately, almost all the theory groups on QKD ignored the criticisms.

This is disagreeable in the development of science and technology. Researchers are obliged to clarify "what is going on" in the discussion of the scientific theory.

At present, there is no review on such a dispute. Our purpose is to clarify a story of the

argument on the recent theory of QKD and the criticism against them. We introduced the Shannon theory on the cryptography to confirm the basis of the concept of the unconditional security. And we compared the fundamental concept of the current security theory of QKD by R.Renner and. the outline of the Yuen's criticism. Finally, we provided evidence on which there is no theoretical proof of the unconditional security for any QKD, despite that many theoretical papers claimed the perfect proof of the unconditional security.

[1] H.P.Yuen, Key generation: Foundation and a new quantum approach, IEEE J. Selected topics in Quantum Electronics, vol-15, no-6, pp1630-1645, 2009.

[2] H.P.Yuen, Fundamental quantitative security in quantum key distribution, Physical Review A, vol-82, 062304, 2010.

[3] M.Tomamichel, C.Lim, N.Gisin, and R.Renner, Tight finite-key analysis for quantum cryptography, Nature Communication, vol-3, p639, 2012.

***Disclaimer**: Views expressed in this article do not necessarily reflect those of TechAndComputer or its staff.*