ISSN 2186-6570

Trade-off between Key Generation Rate and Security of BB84 Quantum Key Distribution

Takehisa Iwakoshi

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.5, No.1, 1-4, 2015

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.5 No.1 : 1–4 (2015)

Trade-off between Key Generation Rate and Security of BB84 Quantum Key Distribution

Takehisa Iwakoshi
Quantum Information Science Research Center,
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-Gakuen, Machida, Tokyo, 194-8610, Japan
E-mail: t.iwakoshi@lab.tamagawa.ac.jp

***Abstract*—Great many efforts have been made to realize Quantum Key Distribution (QKD) since BB84 protocol was invented in 1984. One of crucial problems in realizing BB84 protocol is that one has to guarantee its security with finite-key length. Detailed finite-key analyses have been done in the past, however, a trade-off between the security of BB84 and the secure key generation rate has not been discussed precisely. This study shows that there is surely a trade-off between the key rate and the security, which gives the limitation in obtaining stronger security. However, this limitation may be removed when the sifted-key length is taken to be more than 10^7 bits.**

I. Introduction

Quantum Key Distribution (QKD) has been attracting many attentions since C. H. Bennett and G. Brassard revealed their concept in 1984 [1], so called BB84 protocol. Since the invention, many security proofs have been proposed under an ideal situation that infinitely long key can be distributed and processed in the protocol. However, in the situation that QKD is going to be applied in the real world, one has to consider the problem that the distributed key is necessarily finite.

To overcome this problem, finite-key analyses have been started [2, 3]. On the other hand, [4] pointed out that there must be a trade-off between the security and key generation rate. For instance, readers see dependencies in the key generation rate on security parameters $\varepsilon_{\mathrm{cor}}$-correctness and $\varepsilon_{\mathrm{sec}}$-security.

This study shows that there is surely a trade-off between the key generation rate and the security of BB84 protocol, therefore one has to analyze that the key generation rate should be in a certain region to claim its security, especially with experimental results. This study also treats the amount of information leakage during error-correction process given in [5].

II. DESCRIPTION OF BB84 PROTOCOL

In the literature [3], BB84 protocol is described as follows. The transmitter, Alice, prepares the quantum state in X-basis or Z-basis with probabilities p or $1-p$, and sends it to the receiver, Bob. Bob chooses his measurement basis from X-basis and Z-basis independently from Alice with probabilities p and $1-p$. The eavesdropper, Eve, may interact with the quantum state being sent in the middle of the quantum channel. They repeat this process M times, and Alice and Bob announce their communication bases in an authenticated classical channel. Then they discard bits with unmatched communication bases, and keep the remained bits as their sifted keys. After this sifting processes, they announce randomly-picked l bits from their sifted keys to measure Quantum Bit Error Rate (QBER) denoted Q. If $Q \le Q_{\mathrm{tol}}$, a tolerable QBER, they announce Error Correcting Code (ECC) to process remained n bits. Finally, they also announce Privacy Amplification Code (PAC) to process the remained bits to obtain the final key of k bits, to eliminate information on the final key Eve may have.

A. Security definitions

To satisfy universal composability [6], $\varepsilon_{\mathrm{sec}}$-security is defined as follows [3].

$$\tfrac{1}{2}\mathrm{tr}\left|\rho_{\mathrm{SE}} - \omega_{\mathrm{S}} \otimes \sigma_{\mathrm{E}}\right| \le \varepsilon_{\mathrm{sec}} / \left(1 - p_{\mathrm{abort}}\right) \tag{1}$$

Here, ρ_{SE} is a marginal quantum state actually distributed with Eve's state included, ω_{S} is an ideal quantum state Alice and Bob share, and σ_{E} is an independent quantum state Eve possesses. p_{abort} is a probability of QKD being aborted when the system outputs an error. Also, $\varepsilon_{\mathrm{cor}}$-correctness is defined as a probability where Alice's and Bob's final keys do not agree after applying ECC.

III. Finite-key analysis given in [3]

A. Procedure of key generation rate derivation

Their procedure to derive the key generation rate is as follows:

- Define a maximum extractable key length $k_{\max}$ as a function of $\{n, l, Q_{\mathrm{tol}}, \varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}}\}$.
- Define an expected key rate r_{ex}.
- Maximize r_{ex} over $\{n, l, Q_{\mathrm{tol}}, \varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}}\}$.
- Define the key generation rate r as $k_{\max}/(n+l)$.
- Substitute $\{n, l, Q_{\mathrm{tol}}, \varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}}\}$ into r.

Here, $k_{\max}$ and r_{ex} are defined as follows.

$$k_{\max} := n\left[q - h(Q_{\mathrm{tol}} + \mu)\right] - leak_{\mathrm{EC}} - \log_2\left(2\varepsilon_{\mathrm{sec}}{}^{-2}\varepsilon_{\mathrm{cor}}{}^{-1}\right) \quad (2)$$

$$r_{\mathrm{ex}} := (1-\varepsilon_{\mathrm{rob}})k_{\max} / M \quad (3)$$

$$M := n + l + 2\sqrt{nl} \quad (4)$$

$$leak_{\mathrm{EC}} := 1.1nh(Q_{tol}) \quad (5)$$

$$h(x) := -x\log_2 x - (1-x)\log_2(1-x) \quad (6)$$

$$\mu := \sqrt{\frac{n+l}{nl}\frac{l+1}{l}\ln\frac{2}{\varepsilon_{\mathrm{sec}}}} \quad (7)$$

$$\varepsilon_{\mathrm{rob}} := \exp\left[-n\left(Q - Q_{\mathrm{tol}}\right)^2\right] \quad (8)$$

In [3], $\varepsilon_{\mathrm{rob}}$ is not clearly described, but it was clarified in [7].

B. Numerical analyses

The result of $\varepsilon_{\mathrm{sec}}$ dependency of r is shown in Fig. 1. Here, q = 1 and $\varepsilon_{\mathrm{cor}}$ is fixed to 10^{-12} so that $\varepsilon_{\mathrm{sec}}$ dependency of r can clearly be seen. In Fig. 1(a), one can see that there is limitation in reducing $\varepsilon_{\mathrm{sec}}$ when $n + l$ is small. In Fig. 1(b), one can see that even when $n + l$ is large, there is limitation in reducing $\varepsilon_{\mathrm{sec}}$ when Q is large. Also, note that $r \le k_{\max}/(l + n)$ has to be satisfied to claim r is realized under $\varepsilon_{\mathrm{sec}}$-security; there are some experimental studies which claimed their systems were secure just because their experimental r were positive, but Fig.1(a) and (b) show that the security cannot be claimed unless the experimental r is below the theoretically plotted curve.

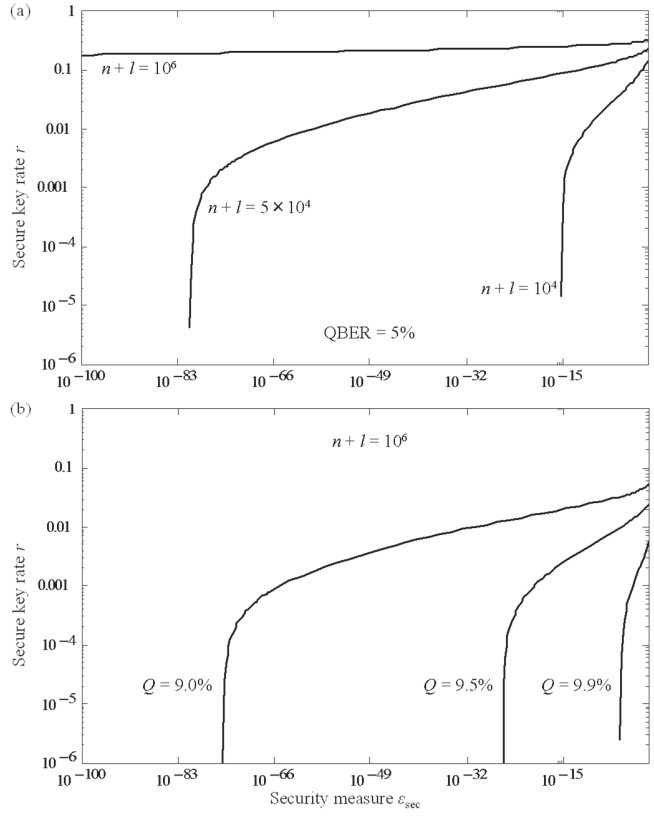

Fig. 1(a). Sifted-key length dependency and (b). QBER dependency of secure key rate. One can see there is limitation in reducing $\varepsilon_{\mathrm{sec}}$.

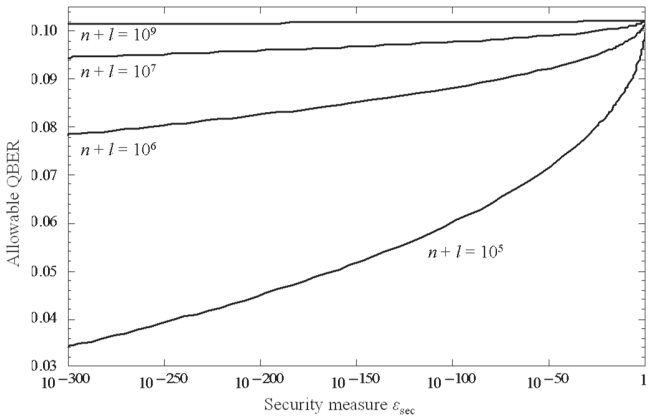

Fig. 2. Allowable Q vs $\varepsilon_{\mathrm{sec}}$. Positive r can be obtained in the region below the curves with corresponding $n + l$. When $n + l = 10^5$ bits, allowable Q decreases as $\varepsilon_{\mathrm{sec}}$ reduces. However, if $n + l \ge 10^7$ bits, there is almost no such limitation.

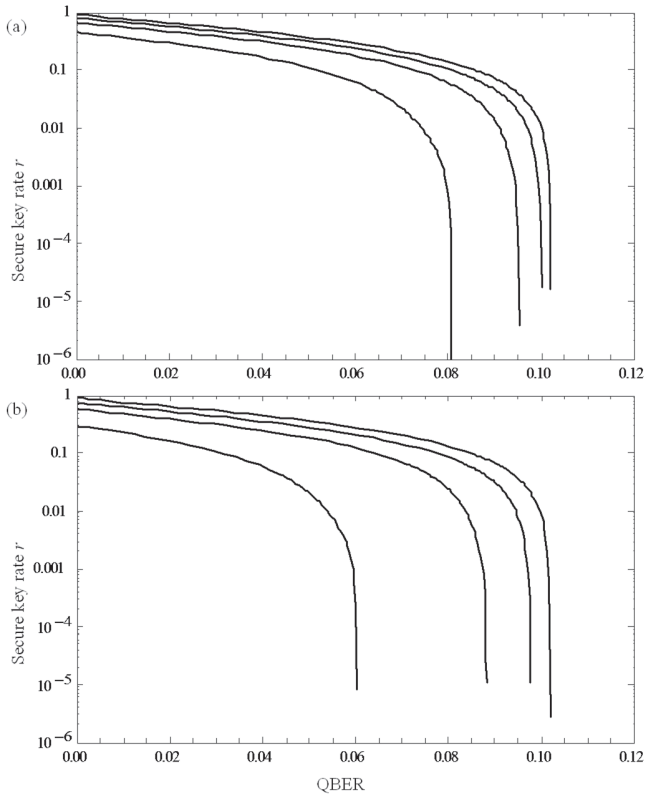

Fig. 3(a). Obtainable r with $\varepsilon_{\mathrm{sec}} = 10^{-24}$ and (b) $\varepsilon_{\mathrm{sec}} = 10^{-100}$. From the lowest curve, $n + l = 10^5$, 10^6, 10^7, 10^9 bits.

Fig. 2 shows curves which indicate r = 0 under Q and $\varepsilon_{\mathrm{sec}}$ given by the axes. This means that r cannot be positive unless Q and $\varepsilon_{\mathrm{sec}}$ are realized in the region below the curves. This figure clearly shows that there is limitation in reducing $\varepsilon_{\mathrm{sec}}$ under the certain Q when $n + l$ is short. If one wishes to realize certain $\varepsilon_{\mathrm{sec}}$, one has to discard all processes in which Q exceeds the limitation shown by the curves. However, when $n + l$ is sufficiently large, say more than 10^7 bits, one can reduce $\varepsilon_{\mathrm{sec}}$ as one desires.

Fig. 3 shows two examples in cases of $\varepsilon_{\mathrm{sec}} = 10^{-24}$ and $\varepsilon_{\mathrm{sec}} = 10^{-100}$. If the finite-key analysis in [3] is valid, even $\varepsilon_{\mathrm{sec}} = 10^{-100}$ is achievable even when $Q \sim 10\%$. However, one needs a PAC

matrix with its size about $10^5 \times 10^7$ even if $n + l = 10^7$ bits with $r = 0.01$, while [8] wrote processing even $n = 10^6$ bits may become a bottleneck of the communication speed.

IV. Information Leakage in [5]

[5] pointed out that information leakage during error-correction process should be given by

$$leak_{\mathrm{EC}} := nh(Q_{tol}) / (1 - h(Q_{tol})) \tag{9}$$

This section shows some figures replacing Eq.(5) by Eq.(9).

A. Numerical analyses with Eq.(9)

Fig. 4 shows curves which indicate $r = 0$ under Q and $\varepsilon_{\mathrm{sec}}$ given by the axes. This result is similar to Fig. 2, but allowable QBER is tighter, which is about 7.4% even for $n + l = 10^9$ bits. Fig. 5 shows examples in cases of $\varepsilon_{\mathrm{sec}} = 10^{-24}$ and $\varepsilon_{\mathrm{sec}} = 10^{-100}$. Even $\varepsilon_{\mathrm{sec}} = 10^{-100}$ is achievable even when $Q \sim 7.4\%$.

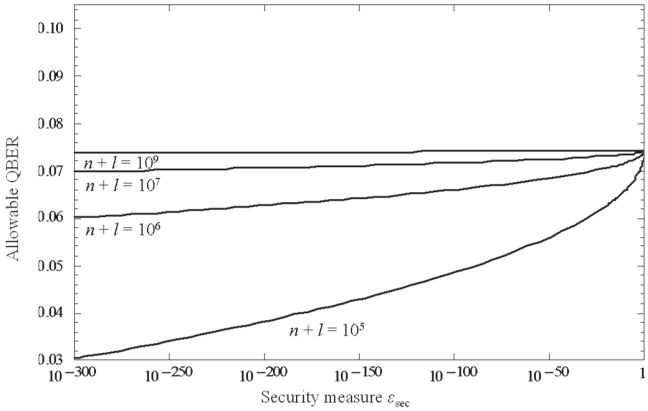

Fig. 4. Allowable Q vs $\varepsilon_{\mathrm{sec}}$. Positive r can be obtained in the region below the curves with corresponding $n + l$.

V. Effect of Transmission Loss

This section describes the effect of transmission loss of the quantum channel. To evaluate the effect, this study assumed the following situations.

- Alice transmits her M photons with probability of p for X-basis and of $1 - p$ for Z-basis.
- The transmission loss is $\eta = \eta_{\mathrm{D}} 10^{-0.02L}$, where L is the length of the quantum channel and η_{D} is the detection efficiency.
- Bob receives $M\eta$ photons. This study does not consider dark counts from the detectors.
- Alice and Bob communicate and discard bits with unmatched bases. After this process, Bob holds $(n + l)\eta$ bits.
- Bob sacrifices $l\eta$ bits to estimate Q.
- From remained $n\eta$ bits, Bob obtains $k_{\max}$ bits of the final key.

To compute the optimal $k_{\max}$, the following procedure was applied.

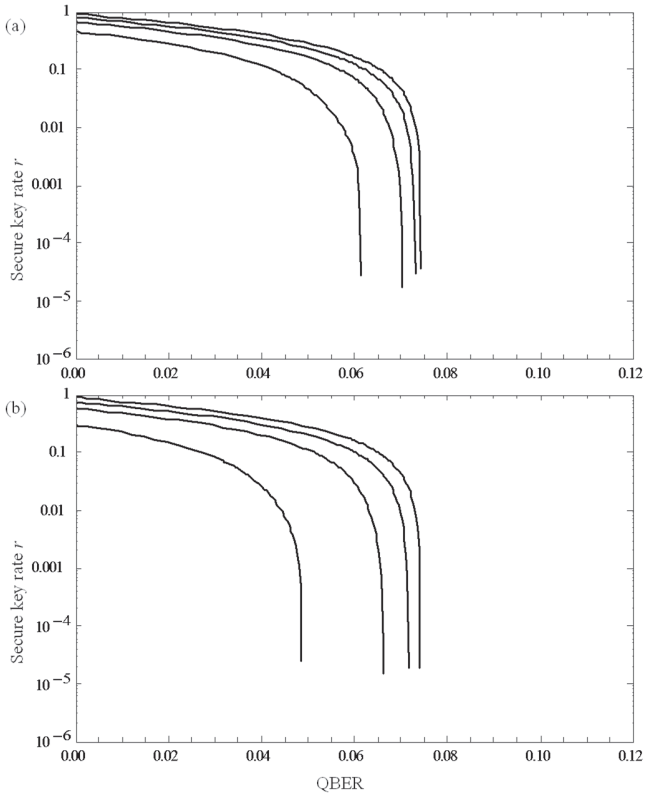

Fig. 5(a). Obtainable r with $\varepsilon_{\mathrm{sec}} = 10^{-24}$ and (b) $\varepsilon_{\mathrm{sec}} = 10^{-100}$. From the lowest curve, $n + l = 10^5$, 10^6, 10^7, 10^9 bits.

- Define a maximum extractable key length $k_{\max}$ as a function of $\{n, l, Q_{\mathrm{tol}}, \varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}}\}$.
- Define an expected key rate r_{ex}.
- Maximize r_{ex} over $\{n, l, Q_{\mathrm{tol}}, \varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}}\}$.
- Define the key generation rate r as $k_{\max} / (n + l)$.
- Substitute $\{n, l, Q_{\mathrm{tol}}, \varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}}\}$ into r.

Here, $k_{\max}$ and r_{ex} are defined as follows.

$$k_{\max} := n\eta\left[q - h(Q_{\mathrm{tol}} + \mu')\right] - leak_{\mathrm{EC}} - \log_2\left(2\varepsilon_{\mathrm{sec}}^{-2}\varepsilon_{\mathrm{cor}}^{-1}\right) \tag{10}$$

$$r_{\mathrm{ex}} := (1 - \varepsilon_{\mathrm{rob}})k_{\max} / M \tag{11}$$

$$\mu' := \sqrt{\frac{n\eta + l\eta}{n\eta l\eta}\frac{l\eta + 1}{l\eta}\ln\frac{2}{\varepsilon_{\mathrm{sec}}}} \tag{12}$$

$$\varepsilon_{\mathrm{rob}} := \exp\left[-n\eta\left(Q - Q_{\mathrm{tol}}\right)^2\right] \tag{13}$$

Fig. 6(a) and 6(b) show L dependence of r for $leak_{\mathrm{EC}}$ in Eq.(5) and Eq.(9) respectively, replacing n by $n\eta$. There are limitations in achievable distance L with different $n + l$. When $n + l$ is longer, achievable L also becomes longer. However, if the $leak_{\mathrm{EC}}$ term described by Eq.(9) is employed, the achievable distance becomes shorter.

Fig. 7 shows curves which indicate $r = 0$ under Q and $\varepsilon_{\mathrm{sec}}$ given by the axes with $L = 100$ km. When $n + l = 10^5$ bits, $\varepsilon_{\mathrm{sec}}$ cannot be smaller than about 10^{-8} even when $Q = 0$. Although it is much better when $n + l = 10^6$ bits, there is still limitation in reducing $\varepsilon_{\mathrm{sec}}$ around 10^{-92}. Such limitations will be more crucial when L is longer.

VI. Future works to be discussed

To evaluate the trade-off between the secure key rate and the transmission loss, the effect of dark counts from Bob's detectors and multi-photon statistics from Alice's device have to be taken into consideration. Further attacks also have to be taken into consideration, for instance, probabilistic re-send attacks in [9]. This attack allows Eve to send a probabilistically cloned state to Bob, which does not cause increase in QBER.

VII. Conclusion

In this study, numerical analyses based on [3] are shown to clarify the limitation in the finite-key generation in BB84 quantum key distribution. For instance, one cannot achieve sufficient allowable Quantum Bit Error Rate without sifted-key length more than 10^7 bits. Furthermore, information leakage during error-correction process in the literature [5] was taken into consideration. The given information leakage lowers the allowable Quantum Bit Error Rate further, but formulation in [3] still gives sufficient key generation rate. However, attacks such as probabilistic re-send attacks by which Eve sends a probabilistically cloned state to Bob without causing increase of Quantum-Bit-Error-Rate [9]. Also, dark counts from Bob's detectors and multi-photon statistics from Alice's device have to be taken into consideration.

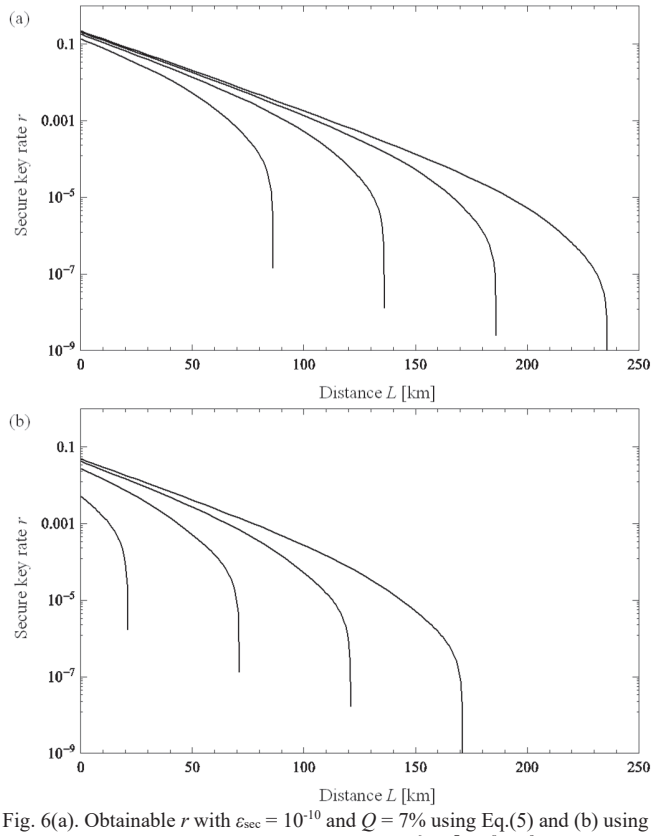

Fig. 6(a). Obtainable r with $\varepsilon_{sec} = 10^{-10}$ and $Q = 7\%$ using Eq.(5) and (b) using Eq.(9). From the lowest curve, $n + l = 10^6$, 10^7, 10^8, 10^9 bits.

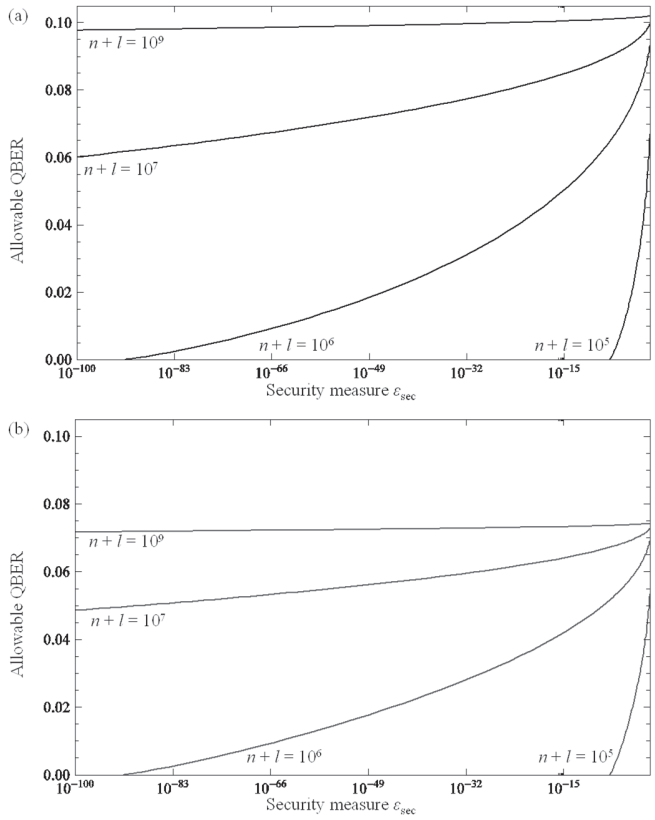

Fig. 7(a). Allowable Q with $L = 100$ km using Eq.(5) and (b) using Eq.(9). From the lowest curve, $n + l = 10^6$, 10^7, 10^8, 10^9 bits.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. 175. No. 0. (1984).

[2] V. Scarani and R. Renner. "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," Phys. Rev. Lett. Phys. Rev. Lett. **100**, 200501 (2008).

[3] M. Tomamichel, et al. "Tight finite-key analysis for quantum cryptography," Nature communications 3, 634 (2012)., arXiv.org, quant-ph:1103.4130v2, 17th Oct. (2012).

[4] H. P. Yuen, "KCQ: A New Approach to Quantum Cryptography I. General Principles and Qubit Key Generation," arXiv.org, quant-ph:0311061v2, 19st Nov. (2003).

[5] H. P. Yuen, "Problems of Security Proofs and Fundamental Limit on Key Generation Rate in Quantum Key Distribution," arXiv.org, quant-ph:1205.3820v2, 21st May (2012).

[6] R. Renner, "Security of quantum key distribution," Int. J. Quant. Inform., vol.6, no.1, pp.1-127, (2008).

[7] M. Tomamichel and C. C. W. Lim, private e-mail to T. Iwakoshi, 7th Jan.-25th May, (2015).

[8] T. Tsurumaru, Lecture note on finite-data analysis in IEICE symposium on Information Technology, 25th Sep. (2014).

[9] H. P. Yuen, "Effect of Transmission Loss on the Fundamental Security of Quantum Key Distribution," arXiv.org, quant-ph:1109.1049v1, 6th Sep. (2011).