METROLOGY AND MEASUREMENT SYSTEMS

Index 330930, ISSN 0860-8229

www.metrology.pg.gda.pl

FUNDAMENTAL LIMIT AND TRADE-OFF BETWEEN SECURITY AND SECURE KEY GENERATION RATE IN QUANTUM KEY DISTRIBUTION

Takehisa Iwakoshi

Quantum ICT Research Institute of Tamagawa University, 6-1-1 Tamagawa-Gakuen, Machida, Tokyo 194-8610, Japan
(✉ *t.iwakoshi@lab.tamagawa.ac.jp*, +81 42 739 8652)

Abstract

Many researchers have contributed to creating Quantum Key Distribution (QKD) since the first protocol BB84 was proposed in 1984. One of the crucial problems in QKD is to guarantee its security with finite-key lengths by Privacy Amplification (PA). However, finite-key analyses show a trade-off between the security of BB84 and the secure key rates. This study analyses two examples to show concrete trade-offs. Furthermore, even though the QKD keys have been perceived to be arbitrarily secure, this study shows a fundamental limitation in the security of the keys by connecting Leftover Hash Lemma and Guessing Secrecy on the QKD keys.

Keywords: Quantum Key Distribution, Quantum Cryptography, Privacy Amplification, Leftover Hash Lemma.

1. Introduction

Quantum Key Distribution (QKD) has been attracting attention of many scientists 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 for the ideal situation that an infinitely long key can be distributed and processed in the protocol. However, in the situation that QKD is applied to 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, [4–6] have pointed out that there must be a trade-off between the security and the key generation rate. For instance, the readers can see dependences of the key generation rate on the security parameters: $\varepsilon_{\mathrm{cor}}$ – correctness and $\varepsilon_{\mathrm{sec}}$ – security [2, 3].

This study shows that there is certainly a trade-off between the key generation rate and the security of the BB84 protocol. Therefore, one has to analyse whether the key generation rate should be in a certain region to claim its security, especially with experimental results. This study also deals with the amount of information leakage during the error-correction process given in [4–6]. The last section in this study also gives a fundamental limitation in the security of BB84 and similar QKD protocols using Privacy Amplification.

Article history: received on Sep. 03, 2018; accepted on Nov. 15, 2018; available online on Mar. 29, 2019, DOI: 10.24425/mms.2019.126333.

2. Description of BB84 protocol and Finite Analysis by M. Tomamichel *et al.* [3]

In the literature [3], the BB84 protocol is described as follows. The transmitter, Alice, prepares quantum state in X-basis or Z-basis with probabilities p_X or $1 - p_X$, then sends it to the receiver, Bob. Bob chooses his measurement basis from X-basis and Z-basis independently from Alice with probabilities p_X and $1 - p_X$. The eavesdropper, Eve, may interact with the sent quantum state in the middle of the quantum channel. They repeat the 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 the sifting processes, they announce randomly chosen l bits from their sifted keys to measure *Quantum Bit Error Rate* (QBER) denoted Q. If $Q \leq Q_{\text{tol}}$ denoting a tolerable QBER, they proceed to *Error Correction* (EC) to process the remained n bits. Finally, they also proceed to *Privacy Amplification* (PA) to process the remained bits to obtain the final key of k bits, to eliminate information on the final key Eve may have.

2.1. Security definitions

To satisfy universal composability [7, 8], ε_{sec}-security is defined as follows [3]:

$$\frac{1}{2}\text{tr}\,|\rho_{\text{SE}} - \tau_{\text{S}} \otimes \tau_{\text{E}}| \leq \frac{\varepsilon_{\text{sec}}}{1 - p_{\text{abort}}}\,. \tag{1}$$

Here, ρ_{SE} is a marginal quantum state actually distributed with Eve's state included, τ_{S} is an ideal quantum state Alice and Bob share, and τ_{E} is Eve's separated quantum state. p_{abort} is a probability of aborting QKD when the system outputs an error. Also, ε_{cor} – correctness is defined as a probability where Alice's and Bob's final keys do not agree after applying EC, while ε_{sec} – security is defined as an upper-bound of the trace distance shown in (1), which is a degree of the security of the final key in QKD processes. However, note that (1) is minimized over τ_{E} in [3], while the revised one [9] defined τ_{E} as a standardized one as in (2). Appendix B in [8] gives explanations of the differences of the trace distances.

$$\tau_{\text{E}} := \text{tr}_{\text{S}}\,\rho_{\text{SE}}\,. \tag{2}$$

2.2. Procedure of key generation rate derivation

Their steps [3] to derive the key generation rate are as follows:

1. n: a block size of the sifted key;
2. l: the number of bits for parameter estimation (The original notation is k [3]);
3. k: the number of bits of the secret key (The original notation is l [3]);
4. Q_{tol}: the tolerable QBER Q in the quantum channel;
5. r_{ex}: the expected key rate defined in (6);
6. Maximize r_{ex} over $\{n,\ l,\ Q_{\text{tol}},\ \varepsilon_{\text{cor}},\ \varepsilon_{\text{sec}}\}$;
7. Calculate the key generation rate $r := k/(l + n)$ with the parameters obtained in Step 6.

The concrete formulations are as follows:

$$k \leq n[q - h(Q_{\text{tol}} + \mu) - \text{Leak}_{\text{EC}}(\text{Q}_{\text{tol}})] + \log_2\left[\frac{1}{2}\varepsilon_{\text{sec}}^2\varepsilon_{\text{cor}}\right], \tag{3}$$

$$\text{Leak}_{\text{EC}}(Q_{\text{tol}}) := \xi h(Q_{\text{tol}}), \tag{4}$$

$$\xi := 1.1 \text{ (typically)}, \tag{5}$$

$$r_{\text{ex}} := (1 - \varepsilon_{\text{rob}})\, k/M, \tag{6}$$

$$M := n + l + 2\sqrt{nl}, \tag{7}$$

$$h(x) := -x \log_2 x - (1 - x) \log_2 (1 - x), \tag{8}$$

$$\mu := \sqrt{\frac{n+l}{nl}\frac{l+1}{l} \ln \frac{2}{\varepsilon_{\text{sec}}}}, \tag{9}$$

$$\varepsilon_{\text{rob}} := \exp\left[-n\,(Q - Q_{\text{tol}})^2\right], \tag{10}$$

$$r := k/(n + l). \tag{11}$$

In [3], the channel robustness ε_{rob} is not written. Personal e-mail exchanges had clarified it [10].

2.3. Confirmation of data reproducibility

The numerical results using (3)–(10) are shown in Fig. 1. The curves represent the derived key generation rate r, while the dots are the original data in Fig. 2 of [3]. Unfortunately, the data in [3] could not be reproduced. E-mail had been exchanged a few times with a concrete Mathematica code written by the author of this study, no replies had pointed out any errors in the code [10]. Therefore, the discussions in this section concerning the use of the Mathematica code written by the author show that the obtained curves are close enough to the original data.

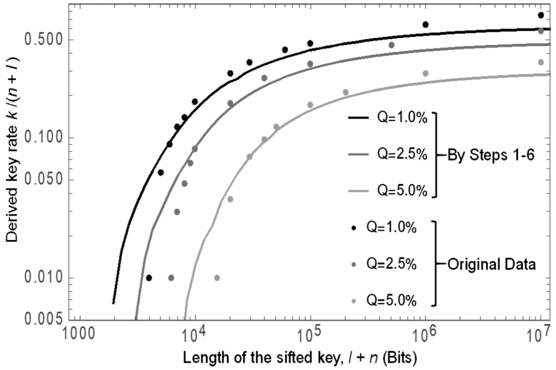

Fig. 1. Checking reproducibility of the original data. The dots show the original data, Fig. 2 in [3], while the curves are the numerical data obtained in Steps 1–7.

2.4. Trade-off between security and Key Generation Rate

The result of ε_{sec} dependence on r is shown in Fig. 2. The quality of quantum state preparation in [3] denoted q, is set to 1, and ε_{cor} is fixed to 10^{-12} so that the dependence of ε_{sec} on r can be seen. In Fig. 2a, one can see that there is a limitation in reducing ε_{sec} when $n + l$ is small. In Fig. 2b, one can see that even when $n + l = 10^6$, there is a limitation in reducing ε_{sec} when Q is large. Also, note that $r \leq k/(l + n)$ has to be satisfied for a given ε_{sec}; there are some experimental studies which claim that their systems are secure just because their experimental r

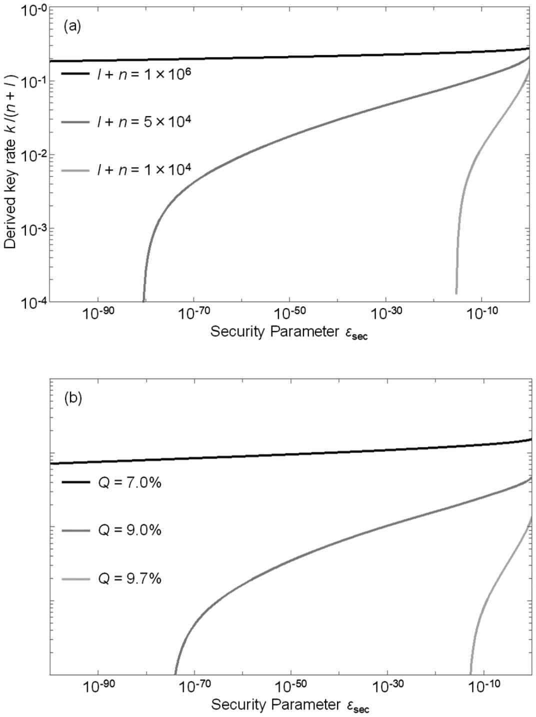

Fig. 2. a) The dependence of the sifted-key length on the secure key rate with $Q = 5.0\%$ b) the dependence of Q on the secure key rate with a sifted-key length $n + l = 10^6$ bits. One can see that there is a limitation in reducing ε_{sec} in both cases.

is positive. However, Figs. 2a and 2b show that the security cannot be claimed because the key can be generated even when $\varepsilon_{\text{sec}} \sim 1$, which means the generated key is not secure at all.

To explain the above situation, Fig. 3 is shown satisfying the condition $n = l$. The curves indicate $r = 0$ for Q and ε_{sec} represented by the axes. This means that r cannot be positive unless

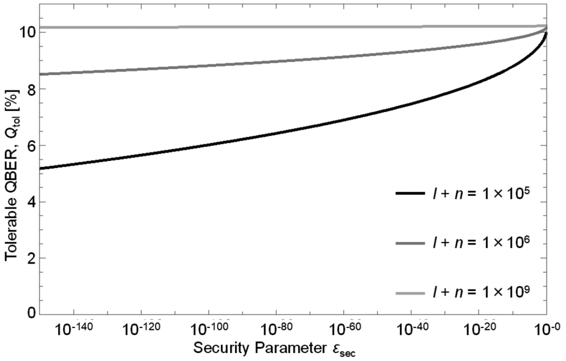

Fig. 3. The allowable Q_{tol} vs. ε_{sec}. The positive key rate is obtainable below the curves. When $n + l$ is small, the allowable Q_{tol} decreases as ε_{sec} reduces. When $n + l \geq 10^6$, such a limitation is loosened.

Q and $\varepsilon_{\mathrm{sec}}$ are situated in the region below the curves. This figure clearly shows that there is a limitation in reducing $\varepsilon_{\mathrm{sec}}$ below certain values when $n + l$ is short at a given Q. However, when $n + l$ is sufficiently large, say, more than 10^6 bits, one can reduce $\varepsilon_{\mathrm{sec}}$ as one desires.

Figure 4 shows two examples of the above situation with $\varepsilon_{\mathrm{sec}} = 10^{-24}$ and $\varepsilon_{\mathrm{sec}} = 10^{-100}$. Even when $Q \sim 10\%$, $\varepsilon_{\mathrm{sec}} = 10^{-100}$ is achievable if $n + l \geq 10^9$. However, when one needs a larger $n + l$ and a higher r, a larger PA matrix is required with its size of about $r \times (n + l)^2$, correspondingly.

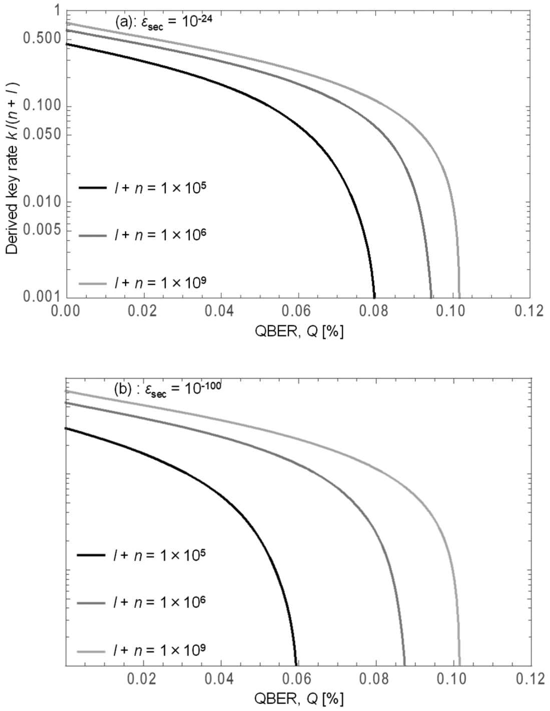

Fig. 4. a) Example of the relation between key generation rate r and Q_{tol} regarding Fig. 3. When $n + l$ is small, the allowable Q_{tol} decreases as $\varepsilon_{\mathrm{sec}}$ reduces (Compare Fig. 4a for $\varepsilon_{\mathrm{sec}} = 10^{-24}$ and 4b for $\varepsilon_{\mathrm{sec}} = 10^{-100}$)

3. Information leakage in [5]

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

$$\mathrm{Leak}_{\mathrm{EC}}(Q_{\mathrm{tol}}) := h(Q_{\mathrm{tol}})/(1 - h(Q_{\mathrm{tol}})). \tag{12}$$

Its derivation is also given in Subsection 2.3 of [6]. This section shows the effects of (12).

3.1. Numerical analyses with (12)

Figure 5 shows curves which indicate $r = 0$ under Q and $\varepsilon_{\mathrm{sec}}$ given by the axes. This result is similar to Fig. 3, but the allowable Q_{tol} becomes tighter, which is about 7.4% even for $n + l = 10^9$ bits. Fig. 6 shows examples in cases of $\varepsilon_{\mathrm{sec}} = 10^{-24}$ and $\varepsilon_{\mathrm{sec}} = 10^{-100}$, similar to Fig. 4.

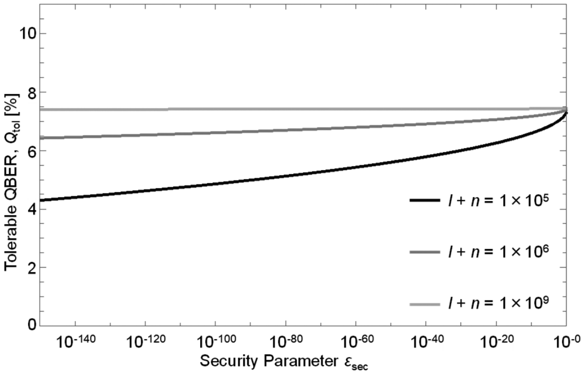

Fig. 5. The allowable Q_{tol} vs. ε_{sec} with (12) substituted for (4). The allowable Q_{tol} necessarily drops to 7.4%.

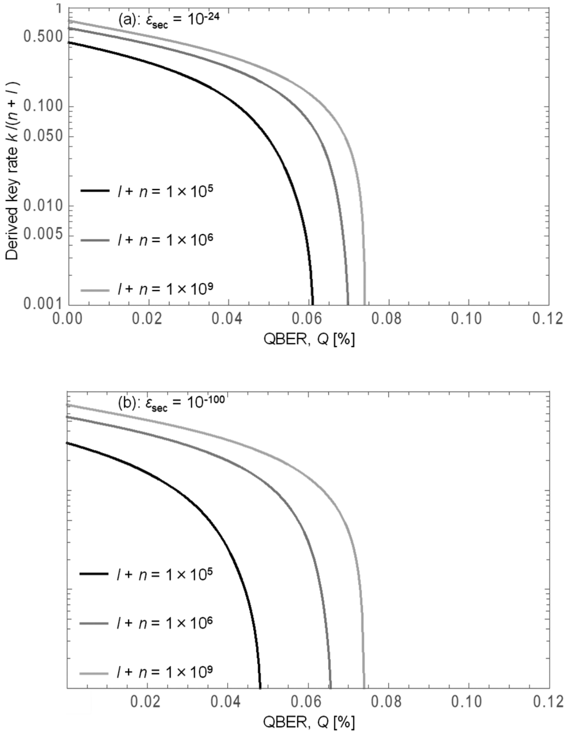

Fig. 6. The obtainable r : a) with $\varepsilon_{\text{sec}} = 10^{-24}$ and b) 10^{-100}. For the lowest curve, $n + l = 10^5$, 10^6, and 10^9 bits.

4. Effect of transmission loss

This section describes the effect of transmission loss in the quantum channel. Suppose that the transmission loss in the channel is $\eta = \eta_{\text{D}} 10^{-0.02L}$, where L is the length of quantum channel and η_{D} is the detection efficiency. To compute the optimal k, use ηn and ηl instead of n and l.

Then calculate the key generation rate $r = k/(l + n)$; use the parameters obtained in Step 6 in Subsection 2.2. Here, k and r_{ex} are defined as follows:

$$k \le n\eta \left[q - h(Q_{\text{tol}} + \mu') - \text{Leak}_{\text{EC}}(Q_{\text{tol}})\right] + \log_2 \left[\frac{1}{2}\varepsilon_{\text{sec}}^2 \varepsilon_{\text{cor}}\right], \tag{13}$$

$$r_{\text{ex}} := (1 - \varepsilon_{\text{rob}})k/M, \tag{14}$$

$$\mu' := \sqrt{\frac{n\eta + l\eta}{n\eta l\eta}\frac{l\eta + 1}{l\eta}\ln\frac{2}{\varepsilon_{\text{sec}}}}, \tag{15}$$

$$\varepsilon_{\text{rob}} := \exp\left[-n\eta\,(Q - Q_{\text{tol}})^2\right]. \tag{16}$$

Figures 7a and 7b show L the dependence of L on r for Leak_{EC} in (4) and (12), respectively. There are limitations in the achievable distance L at different $n + l$. For larger $n + l$, the achievable L also becomes longer. However, if the Leak_{EC} term described by (12) is applied, the achievable distance becomes shorter. Fig. 7 shows curves which indicate $r = 0$ for Q and ε_{sec} represented by the axes at $L = 100$ km. When $n + l = 10^5$ bits, ε_{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 a limitation in reducing ε_{sec} to around 10^{-92}. Such limitations will be more crucial when L is longer.

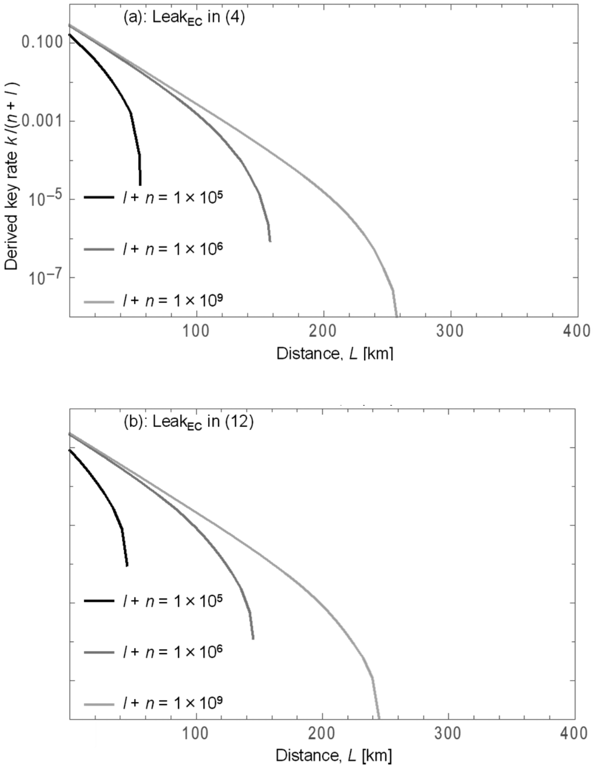

Fig. 7. The obtainable r for $\varepsilon_{\text{sec}} = 10^{-10}$ and $Q = 5\%$: a) using (4) and b) using (12). For the lowest curve, $n + l = 10^5$, 10^7, 10^9 bits.

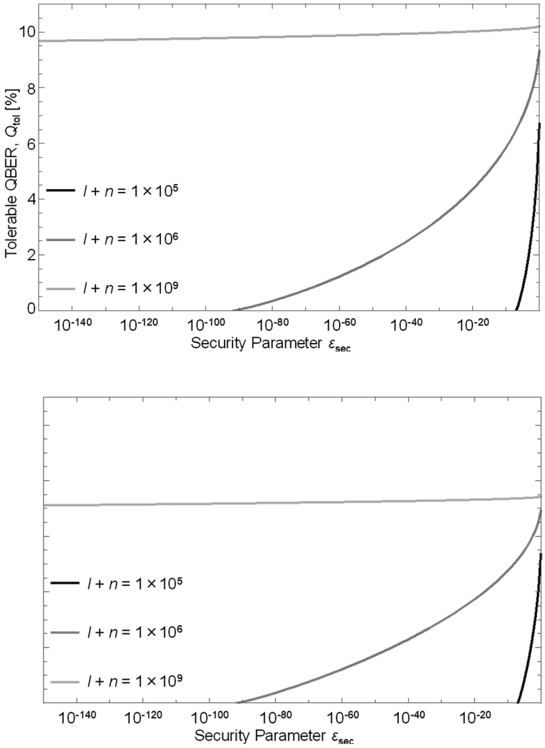

Fig. 8. The obtainable r for $\varepsilon_{\text{sec}} = 10^{-10}$ and $Q = 5\%$: a) using (4) and b) using (12). For the lowest curve, $n + l = 10^5$, 10^7, 10^9 bits.

5. Finite-key analysis in study of M. Hayashi and T. Tsurumaru [11]

5.1. Procedure of key generation rate derivation

They proposed several procedures in the literature [11], but in this paper there is employed the straightforward upper-bound procedure given in their Subsection 6.2.1.

1. n: a block size of the sifted key;
2. l: the number of bits for parameter estimation;
3. k: the number of bits of the secret key. (The original notation is G [11]);
4. Obtain the value of parameter $s(\varepsilon_{\text{sec}}^2/4)$ which satisfies (17) (The original notation is $s(\varepsilon)$, however, in this study the above notation is used to avoid confusions among ε, ε_{sec}, and ε_{cor}. Use the original equations in their Subsection 6.2.1 to derive the above notation in this study);
5. Calculate the key sacrifice amount in PA by (24);
6. By optimizing n and l, maximize the key generation rate $r = k/n$.

Then, define the following equations:

$$\varepsilon_{\text{sec}}^2/4 := \frac{1}{\sqrt{2\pi}} \int\limits_{s(\varepsilon_{\text{sec}}^2/4)}^{\infty} \exp\left[-y^2/2\right] \mathrm{d}y, \tag{17}$$

$$\gamma := ns\left(\varepsilon_{\mathrm{sec}}^2/4\right)\Big/\left[4l(n+l-1)\right], \tag{18}$$

$$Q := c/l, \tag{19}$$

$$c := 2 + \max[Ql, c_{\mathrm{min}}], \tag{20}$$

$$c_{\mathrm{min}} := 0.01l, \tag{21}$$

$$p_{\varepsilon_{\mathrm{sec}}^2/4} := (1+4\gamma)^{-1}\left(Q + 2\gamma + 2\left[\gamma\left(Q(1-Q)+\gamma\right)\right]^{1/2}\right), \tag{22}$$

$$p_{\mathrm{sft},\varepsilon_{\mathrm{sec}}^2/4} := (1+l/n)\,p_{\varepsilon_{\mathrm{sec}}^2/4} - Q \times l/n, \tag{23}$$

$$D := \mathrm{Ceil}\left[2 - \log_2 \varepsilon_{\mathrm{sec}}^2/2\right], \tag{24}$$

$$r = 1 - \mathrm{Leak}_{\mathrm{EC}}(Q) - n^{-1}\mathrm{Ceil}\left[nh\left(p_{\mathrm{sft},\varepsilon_{\mathrm{sec}}^2/4}\right)\right] - n^{-1}\left(D + \log_2 \varepsilon_{\mathrm{cor}}\right). \tag{25}$$

Here, γ is an intermediate parameter to estimate statistical fluctuation in estimating QBER in the sifted key, which appears in (23), while QBER in the sample bits Q is derived as (19). See the original descriptions in [11] to derive the optimal c in (20) and (21).

5.2. Confirmation of data reproducibility

Similarly to Subsection 2.2, the calculation procedure is confirmed by numerical simulations. The curves represent the numerical simulation results obtained in the previous section, whereas the dots – the original data from Fig. 1 of [11]. This time, the original data are well-recovered. Hence, it is confirmed that the above calculation procedure is correct (Fig. 9).

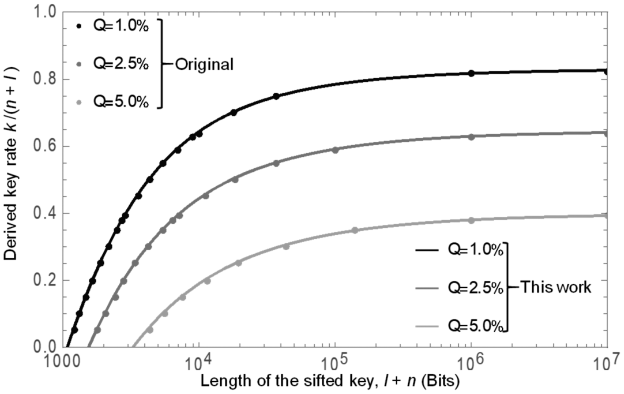

Fig. 9. Checking reproducibility of the original data using the procedure from Subsection 6.1. The obtained curves exactly trace the original data represented by dots.

5.3. Trade-off between security and key generation rate

Even with this procedure, a similar trade-off between security and key generation rate is observed in Fig. 10 and Fig. 11. From the results obtained in Subsections 2–6, it seems to be that the security and key generation have a fundamental trade-off.

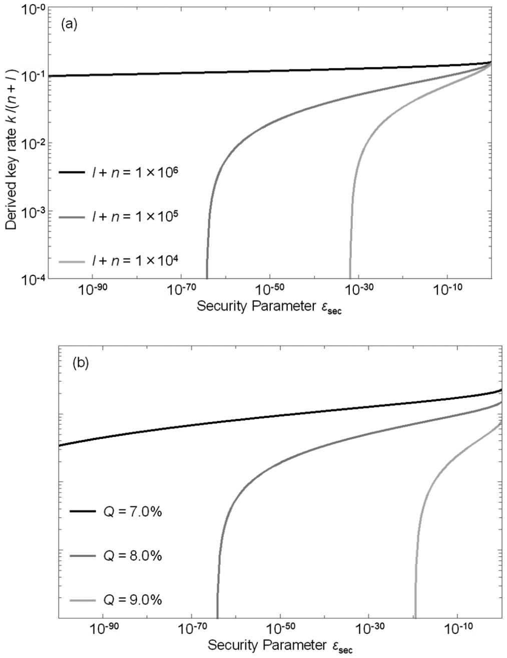

Fig. 10. The dependence of the sifted-key length on the secure key rate at $Q = 8\%$; b) the dependence of Q on the secure key rate at a shifted-key length $n + l = 10^5$ bits. One can see a similar limitation in reducing ε_{sec}.

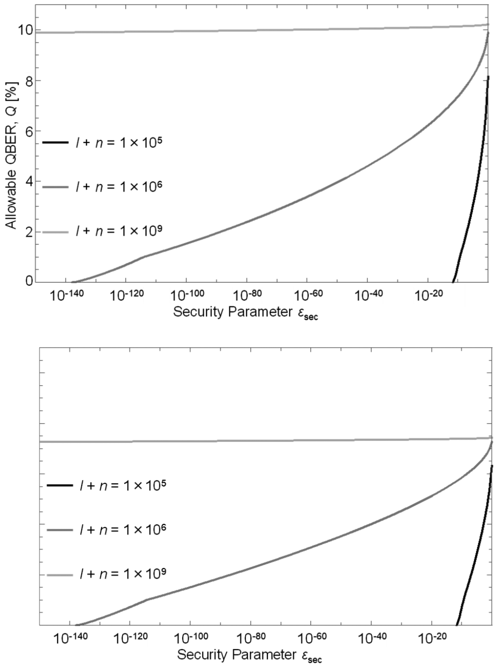

Fig. 11. The allowable Q a) using (4) b) using (12) at $L = 100$ km. From the lowest curve, $n + l = 10^5$, 10^7, 10^9 bits.

6. Fundamental security limitations in Prepare-and-Measure QKDs based on privacy amplification

Most of all prepare-and-measure QKDs use PA to make them secure. Therefore, this section revisits the characteristics of *Leftover Hash Lemma* (LHL) which guarantees the effect of PA. A clear description of LHL is presented in the literature [12] as follows:

"**Definition 2**. A strong $(\tau,\ \kappa,\ \varepsilon)$-extractor on a set $\mathcal{X}$ is a function with domain $\mathcal{X} \times \mathcal{R}$ (for a set $\mathcal{R}$) and range $\mathcal{U}$ of size of $|\mathcal{U}| = 2^{\tau}$ such that, for any random variable X on $\mathcal{X}$ satisfying $H_{\infty}(X) \geq \kappa$ and R uniformly distributed over $\mathcal{R}$, $d(f(X,\ R)|R) \leq \varepsilon$ holds."

"**Lemma 9 (*Leftover Hash Lemma*).** For any $\kappa > \tau$, there exists a strong $(\tau, \kappa, 2^{-(\kappa-\tau)/2})$-extractor."

By combining the definition 2 and the lemma 9, the following inequalities are obtained:

$$\begin{aligned} d\left(f(X,R)|R\right) &:= \frac{1}{2} \sum_{(x,r)\in(\mathcal{X},\mathcal{R})} \left|\Pr\left(f(x,r),r\right) - 2^{-f(x,r)} \Pr(r)\right| \\ &= \frac{1}{2} \sum_{(x,r)\in(\mathcal{X},\mathcal{R})} \Pr(r) \left|\Pr\left(f(x,r)|r\right) - 2^{-f(x,r)}\right| \leq \varepsilon \end{aligned} . \tag{26}$$

$$\text{with } H_{\min}\left(X|R\right) := -\log_2 \left[\sum_{r\in\mathcal{R}} \Pr(r) \max_{x\in\mathcal{X}} \Pr(x|r)\right] \geq \kappa, \tag{27}$$

$$d\left(f(X,R)|R\right) \leq \exp\left(\frac{1}{2}\left[f(x,r) - \kappa\right]\ln 2\right) \quad \text{from Lemma 9.} \tag{28}$$

More generally, Eve has a random variable Z correlated to X, and she obtains the seed S of the hash function exchanged between Alice and Bob in the authenticated public channel. Therefore, such a claim is confirmed in Subsection 2 of [13], as:

$$\begin{aligned} d\left(K(X,S)|Z,S\right) &:= \frac{1}{2} \sum_{x,z\in\mathcal{X},s\in\mathcal{R}} \left|\Pr\left(K(x,s),z,s\right) - 2^{-K(x,s)} \Pr(z,s)\right| \\ &= \frac{1}{2} \sum_{x,z\in\mathcal{X},s\in\mathcal{R}} \Pr(z,s) \left|\Pr\left(K(x,s)|z,s\right) - 2^{-K(x,s)}\right| . \\ &\leq \exp\left(\frac{1}{2}\left[K(X,S) - H_{\min}\left(X|Z,S\right)\right]\ln 2\right) \end{aligned} \tag{29}$$

It is often said that ε can be arbitrarily small in theories of QKDs, hence the QKD keys can be arbitrarily secure, by sacrificing more key-bits in LHL that eventually lowers the secure key rate. Therefore, the numerical results in this study seem to be valid. However, consider the following example: is sacrificing more keys and remaining only a 1-bit key the securest? Eve will guess the correct key with a probability of more than 1/2 by her optimal measurement. Now, let us confirm the situation in the classical case, for simplicity. Since Eve's success probability in obtaining the correct key is given in [5, 6], and [14], the final key length $|K| = K(X,\ S)$ relates to:

$$\begin{aligned} &\Pr(\text{Success}) \leq \varepsilon_{\text{sec}} + 2^{-|K|} \\ &\quad = \exp\left(\frac{1}{2}\left[K(X,S) - H_{\min}\left(X|Z,S\right)\right]\ln 2\right) + \exp\left(-K(X,S)\ln 2\right) \end{aligned} . \tag{30}$$

Therefore, there exists a lower bound of the right-hand side, because:

$$\begin{aligned}&\frac{\partial}{\partial K(X,S)}\left[\exp\left(\frac{1}{2}\left[K(X,S)-H_{\min}(X|Z,S)\right]\ln 2\right)+\exp\left(-K(X,S)\ln 2\right)\right]=0\\&\Rightarrow K(X,S)=\frac{1}{3}H_{\min}(X|Z,S)\end{aligned}. \tag{31}$$

Therefore, when the key length $K(X, S)$ is chosen so that the final key becomes the securest one:

$$\Pr(\text{Success})\leq 2\exp\left(-\frac{1}{3}H_{\min}(X|Z,S)\ln 2\right)=2\exp\left(-K(X,S)\ln 2\right). \tag{32}$$

This situation is what (36) in [5] is telling: that there exists a limitation in lowering the trace distance. The situation is illustrated in Fig. 12. Then, the corresponding key generation rate is, when n bits are sent from Alice:

$$r=(3n)^{-1}H_{\min}(X|Z,S). \tag{33}$$

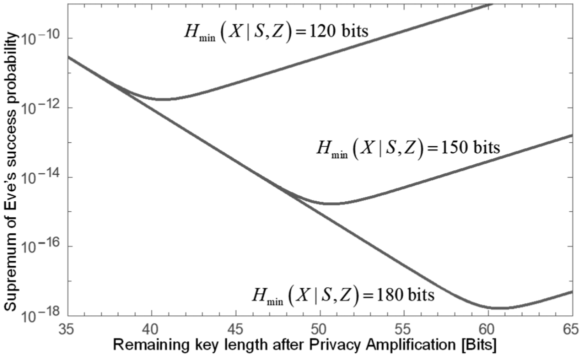

Fig. 12. Checking reproducibility of the original data using the procedure from Subsection 6.1. The obtained curves exactly trace the original data represented by dots.

If the communication channel has a loss of η, the net key generation rate should be:

$$r=(3n)^{-1}\eta H_{\min}(X|Z,S). \tag{34}$$

In the case of QKDs, the trace distance in (1) has to be upper-bounded, although the following inequality is known between the classical case and the quantum case:

$$\begin{aligned}\frac{1}{2}\mathrm{tr}\left|\rho_{\mathrm{SE}}-\tau_{\mathrm{SE}}\right|&\geq\frac{1}{2}\sum_{x,z\in\mathcal{X},s\in\mathcal{R}}\left|\mathrm{tr}\left[M\rho_{\mathrm{SE}}\right]-\mathrm{tr}\left[\tau_{\mathrm{SE}}\right]\right|\\&=\frac{1}{2}\sum_{x,z\in\mathcal{X},s\in\mathcal{R}}\Pr(z,s)\left|\Pr\left(K(x,s)|z,s\right)-2^{-K(x,s)}\right|\end{aligned}. \tag{35}$$

One may consider that the above discussion in the classical case will not hold in the case of QKDs. However, if the upper bound $\varepsilon_{\mathrm{sec}}(|K|)$ of the trace distance in (35) monotonically decreases when $|K|$ decreases [15], then:

$$\frac{\partial}{\partial|K|}\left[\varepsilon_{\mathrm{sec}}(|K|)+2^{-|K|}\right]=\frac{\partial}{\partial|K|}\varepsilon_{\mathrm{sec}}(|K|)-2^{-|K|}\ln 2. \tag{36}$$

Therefore, with a given $\partial\varepsilon_{\text{sec}}(|K|)/\partial|K| \geq 0$, a corresponding $|K|$ satisfies the left-hand side of (36) being zero. Hence, even in the case of QKDs, there exists an optimal key sacrificing amount, as well as the limitation in obtaining the securer keys.

7. Conclusions

It has been often said that the keys generated by QKDs can be arbitrarily secure. However, this study shows a trade-off between the key generation rate and its security. Moreover, from Leftover Hash Lemma and probability of Eve's optimum guessing the distributed key, it is found that there is a limitation in achieving the security. The keys generated by QKDs cannot be securer than this limit unless new protocols are found without Privacy Amplification based on Leftover Hash Lemma.

References

[1] Bennett, Ch.H., Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing Int. *Conf. on Computers, Systems and Signal Processing*, 175–179.

[2] Scarani, V., Renner, R. (2008). Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical review letters*, 100(20), 200501.

[3] Tomamichel, M., Lim, C.C. W., Gisin, N., Renner, R. (2012). Tight finite-key analysis for quantum cryptography. *Nature communications*, 3, 634.

[4] Yuen, H.P. (2012). Problems of security proofs and fundamental limit on key generation rate in quantum key distribution. *arXiv preprint arXiv:1205.3820. https://arxiv.org/abs/1205.3820.*

[5] Yuen, H.P. (2016). Security of quantum key distribution. *IEEE Access*, 4, 724–749.

[6] Iwakoshi, T. (2017). On problems in security of quantum key distribution raised by Yuen. *In Quantum Information Science and Technology III International Society for Optics and Photonics*, 10442, 1044203.

[7] Renner, R. (2008). Security of quantum key distribution. *International Journal of Quantum Information*, 6(01), 1–127.

[8] Portmann, C., Renner, R. (2014). Cryptographic security of quantum key distribution. *arXiv preprint arXiv:1409.3525*. *https://arxiv.org/abs/1409.3525.*

[9] Tomamichel, M., Lim, C.C. W., Gisin, N., Renner, R. (2011). Tight Finite-Key Analysis for Quantum Cryptography. *arXiv preprint arXiv:1103.4130v2*. *https://arxiv.org/abs/1103.4130.*

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

[11] Hayashi, M., Tsurumaru, T. (2012). Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths. *New Journal of Physics*, 14(9), 093014.

[12] Renner, R., Wolf, S. (2005). Simple and tight bounds for information reconciliation and privacy amplification. *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Berlin, Heidelberg, 199–216.

[13] Barak, B., Dodis, Y., Krawczyk, H., Pereira, O., Pietrzak, K., Standaert, F.X., Yu, Y. (2011). Leftover hash lemma, revisited. *In Annual Cryptology Conference* Springer, Berlin, Heidelberg, 1–20.

[14] Iwakoshi, T. (2018). Bit-error-rate guarantee for quantum key distribution and its characteristics compared to leftover hash lemma. *Quantum Information Science and Technology IV, International Society for Optics and Photonics*, 10803, 1080309.

[15] Tomamichel, M., Schaffner, C., Smith, A., Renner, R. (2011). Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8), 5524–5535.