On problems in security of quantum key distribution raised by Yuen

T. Iwakoshi*[a1]
[a]Quantum ICT Research Institute of Tamagawa University,
6-1-1 Tamagawa-Gakuen, Machida, Tokyo 194-8610, Japan

ABSTRACT

In 2007, it was found that Known-Plaintext-Attack would reveal whole the string of the distributed key by Quantum Key Distribution (QKD) when the part of the plaintext was known to the eavesdropper, Eve, under the mutual information security criterion between Eve and legitimate users, Alice and Bob. To overcome, the trace distance criterion was introduced in the paper that the distance between the distributed quantum state and the ideal quantum state with Eve's quantum system decoupled from the quantum systems shared by Alice and Bob. On the other hand, Shor and Preskill proved in 2000 that entanglement-based QKDs are equivalent to prepare-and-measure QKDs, such as the first QKD, BB84. Their proof employed the mutual information criterion, therefore M. Koashi applied Shor-Preskill approach to the trace distance criterion in 2009. However, H. P. Yuen started criticisms on the security of QKDs from 2009, then completed his criticisms in 2016. He warned the security of QKDs are not sufficient. Furthermore, the trace distance would not provide "universal composability", which is supposed to guarantee Independent and Identically Distributed (IID) keys. He also proposed a new security criterion "Bit-Error-Rate (BER) guarantee," to evaluate the BER in the decoded message by Eve with her key close to the correct key. In this work, the author explains Yuen's criticisms and shows an example of the BER guarantee on BB84. Furthermore, the study revisits whether Shor-Preskill security proof approach really worked.

Keywords: Quantum Key Distribution, Quantum Cryptography, Security Proof, Quantum Network, Quantum Internet

1. INTRODUCTION

A lot of amount of investments have been done to the quantum technologies and science, especially in the field of quantum computing, recently. On the other hand, it has been often said that such developments of quantum computers would threat the security of the internet, breaking classical cryptography easily and would leak private information to malicious adversaries. Therefore, quantum cryptography and quantum secure communication technologies are also the center of the interests among the investors. Especially, Quantum Key Distribution (QKD) has been said to be unconditionally secure, or provably secure communication technique under the presence of the eavesdropper, Eve, who has unlimited power, except limitations by laws of physics, to break the cryptogram, since the invention of the first QKD protocol BB84 in 1984 [1, 2]. Many researchers have been involved in this field to realize this exciting concept.

However, recall the first successful hacking on commercial QKD systems in 2010 [3]. After the study of quantum hacking, Measurement-Device-Independent (MDI) QKD was developed[4]. However, imagine that commercial QKD systems had been widely used among the world before the discovery of the hacking technique. If it happened, we had to reform physically all quantum communication infrastructures although we saw the result before miserable security breaches happened. National Cyber Security Centre in Britain disclosed a document in 2016 about security risks of QKD and its inefficient cost performance, and possible future threats yet unknown[5].

On the other hand, numerous works have been made to remove real device imperfections from theoretical security proofs, such as MDI-QKD mentioned above, and Reference[6] to remove attacks on device imperfections. However, since 2009, H. P. Yuen, who theoretically discovered the squeezed state of coherent light[7] as well as the theories of *M*-ary quantum detection and parameter estimation[8, 9], has been warning that even the real devices work perfectly along the standardized theories, there are problems even in theories[10, 11].

At first, the security of QKDs had been proven based on the negligible amount of the mutual information between Eve and the legitimate users, Alice and Bob[12, 13]. However, it was found in 2007 that Known-Plaintext-Attacks would reveal whole the string of the distributed key by QKDs when Eve possesses quantum memory[14]. Therefore, in the same paper, it was

[1]*t.iwakoshi@lab.tamagawa.ac.jp

Quantum Information Science and Technology III, edited by Mark T. Gruneisen, Miloslav Dusek, John G. Rarity, Proc. of SPIE Vol. 10442, 1044203 · © 2017 SPIE
CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2278625

proposed as a new security criterion to upper-bound the trace distance between the distributed quantum state and the ideal quantum state with Eve's quantum system decoupled from the shared quantum system between Alice and Bob with a negligibly small parameter. In the same paper and some other literatures[14 – 18], it is often said that the trace distance itself gives the maximum failure probability in distributing the perfect key. Yuen pointed out this statement was incorrect in 2009 [10]. Honestly, even the author of this article had been wondering why Yuen's has been claiming so. However, C. Portmann and R. Renner described the proof in details in their Appendix A.4.1 in 2014 [18]. Since this finding, the author of this article fully understood what Yuen has been warning. Yuen completed his criticisms on the security of QKDs in 2016, and wrote some counterexamples to the perception that the trace distance is the maximum failure probability of QKDs[19]. His work was written in terms of classical probability theories so that conventional cryptologists can understand. This study tries explanation what Yuen has been warning, in terms of quantum information. Then, the article will give an example of Bit-Error-Rate (BER) Guarantee proposed by Yuen[19, 20] as a new security criterion, in case of BB84 protocol. Furthermore, the author will revisit whether Shor and Preskill really proved that entanglement-based QKDs would be equivalent to prepare-and-measure QKDs, such as BB84 protocol, which was not described even in Yuen's work[19].

2. TRACE DISTANCE SECURITY CRITERION IN QKD AND YUEN'S WARNINGS

This section briefly describes the overview of the trace distance security criterion of QKDs to discuss what the main points of Yuen's claims against the security of QKDs.

2.1 Overview of Trace Distance Security Criterion

Firstly, consider the quantum state ρ_{ABE} actually distributed between Alice and Bob under Eve's interactions, and the ideal quantum state τ_{ABE}, in which the shared key between Alice and Bob is IID with Eve's quantum system decoupled.

$$\tfrac{1}{2}\mathrm{tr}\left|\rho_{\mathrm{ABE}}-\tau_{\mathrm{ABE}}\right|\le\varepsilon\,. \tag{1}$$

$$\rho_{\mathrm{ABE}}:=\sum_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}}\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left|\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}\right\rangle\left\langle\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}\right|\otimes\rho_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\,. \tag{2}$$

$$\tau_{\mathrm{ABE}}:=\sum_{\boldsymbol{k}}2^{-|K|}\left|\boldsymbol{k},\boldsymbol{k}\right\rangle\left\langle\boldsymbol{k},\boldsymbol{k}\right|\otimes\tau_{\mathrm{E}}\,. \tag{3}$$

Then, consider an intermediate state σ_{ABE} in (4) where Alice and Bob share the same key. Then apply a triangle inequality (5) to divide the security problems into two parts, as shown in (5-8).

$$\begin{aligned}\sigma_{\mathrm{ABE}}&:=\sum_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}}\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left|\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{A}}\right\rangle\left\langle\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{A}}\right|\otimes\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\\ \sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})&:=\rho_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\end{aligned}\,. \tag{4}$$

$$\tfrac{1}{2}\mathrm{tr}\left|\rho_{\mathrm{ABE}}-\tau_{\mathrm{ABE}}\right|\le\tfrac{1}{2}\mathrm{tr}\left|\rho_{\mathrm{ABE}}-\sigma_{\mathrm{ABE}}\right|+\tfrac{1}{2}\mathrm{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{ABE}}\right|\,. \tag{5}$$

$$\tfrac{1}{2}\mathrm{tr}\left|\rho_{\mathrm{ABE}}-\sigma_{\mathrm{ABE}}\right|\le\varepsilon_{\mathrm{cor}}\,. \tag{6}$$

$$\tfrac{1}{2}\mathrm{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{ABE}}\right|\le\varepsilon_{\mathrm{sec}}\,. \tag{7}$$

$$\varepsilon_{\mathrm{cor}}+\varepsilon_{\mathrm{sec}}\le\varepsilon\,. \tag{8}$$

The inequality (6) is named as "ε-correctness," which indicates the probability of failure in the key agreement between Alice and Bob. The inequality (7) is named as "ε-security," which is to be said that the probability of failure in distributing an IID key string, like as seen in the following quotes.

"ε security has an intuitive interpretation: with probability at least $1-\varepsilon$, the key S can be considered identical to a perfectly secure key U, i.e., U is uniformly distributed and independent of the adversary's information. In other words, Definition 1 guarantees that the key S is perfectly secure except with probability ε."[14]

"In this definition, the parameter ε has a clear interpretation as the maximum failure probability of the process of key extraction."[16]

"The above definition of security (Definition 2) has the intuitive interpretation that except with probability ε, the key pair (S_A, S_B) behaves as a perfect key, as described by (41)."[17]

2.2 Yuen's warning to the security level of QKDs

However, Yuen warned this would be incorrect in 2009 [10], and showed a counter example in 2010 [11] and 2016 [19]. This article avoid the detailed explanations but gives simple explanations given by Yuen, as follows. As Appendix A.4.1 in the literature by C. Portmann and R. Renner[18], the expected probability for Eve successfully guessing the correct key is

$$\begin{aligned} \mathrm{tr}\left[\Gamma\left(\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\tau_{\mathrm{E}}\right)\right] &= \sum_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}}\left[\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\Pr\left(\boldsymbol{k}_{\mathrm{A}}\mid\boldsymbol{k}_{\mathrm{E}}=\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}\right)\right]-2^{-|K|} \\ &= \mathrm{Ex}\left[\Pr\left(\boldsymbol{k}_{\mathrm{A}}\mid\boldsymbol{k}_{\mathrm{E}}=\boldsymbol{k}_{\mathrm{A}}\right)\right]-2^{-|K|} \end{aligned}. \tag{9}$$

Because an arbitral operator Γ satisfies the following inequality as Eq. (9.22) in the literature[21],

$$\mathrm{tr}\left[\Gamma\left(\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\sigma_{\mathrm{E}}\right)\right]\le\tfrac{1}{2}\mathrm{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\tau_{\mathrm{E}}\right|. \tag{10}$$

$$\Gamma\coloneqq\sum_{\boldsymbol{k}_{\mathrm{A}}}\left|\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{A}}\right\rangle\left\langle\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{A}}\right|\otimes M_{\boldsymbol{k}_{\mathrm{E}}=\boldsymbol{k}_{\mathrm{A}}}\ . \tag{11}$$

Therefore,

$$\mathrm{Ex}\left[\Pr\left(\boldsymbol{k}_{\mathrm{A}}\mid\boldsymbol{k}_{\mathrm{E}}=\boldsymbol{k}_{\mathrm{A}}\right)\right]\le 2^{-|K|}+\tfrac{1}{2}\mathrm{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\tau_{\mathrm{E}}\right|\le 2^{-|K|}+\varepsilon_{\mathrm{sec}}\,. \tag{12}$$

As we see, the failure probability for QKDs that Eve guesses the correct key Alice and Bob share, is, larger than the trace distance itself. This gives a clear-cut answer to the perceived explanations that the trace distance itself is "the maximum failure probability in distributing a perfectly secure key," is not true, because of the existence of the constant factor $2^{-|K|}$. Furthermore, (12) shows the meaning of "the failure of QKDs" very clearly, because it is an expected probability where Eve successfully obtains the correct key.

Yuen also explained the importance of the numerical analysis of (12). In today's QKDs, the key length $|K|$ is set to 10^6 bits, while the best experimental value obtained in the past was $\varepsilon_{\mathrm{sec}} = 2^{-50}$ [22], archived by Round-Robin DPS QKD, which has been claimed it is almost impossible to eavesdrop, far different from conventional QKDs[23, 24]. Then from (12), this means

$$\mathrm{Ex}\left[\Pr\left(\boldsymbol{k}_{\mathrm{A}}\mid\boldsymbol{k}_{\mathrm{E}}=\boldsymbol{k}_{\mathrm{A}}\right)\right]\le 2^{-1,000,000}+2^{-50}\,. \tag{13}$$

On the other hand, the definition of "perfect secrecy" given by C. E. Shannon was[25],

$$\Pr(\boldsymbol{X}\mid\boldsymbol{C})=\Pr(\boldsymbol{X})\,. \tag{14}$$

This means, even Eve obtains the chipertext $\boldsymbol{C}$, she cannot gain any chances to obtain the plaintext $\boldsymbol{X}$ exchanged. Therefore, Eve has to do simple guessing to obtain the plaintext, therefore the probability is

$$\Pr(\boldsymbol{X}\mid\boldsymbol{C})=\Pr(\boldsymbol{X})=2^{-|\boldsymbol{X}|}\,. \tag{15}$$

Now, in case of (13), the knowledge Eve obtained from eavesdropping is $\boldsymbol{k}_{\mathrm{E}} = \boldsymbol{k}_{\mathrm{A}}$, therefore lets rewrite (13) as

$$\Pr\left(\boldsymbol{K}\mid\boldsymbol{E}\right)\coloneqq\mathrm{Ex}\left[\Pr\left(\boldsymbol{k}_{\mathrm{A}}\mid\boldsymbol{k}_{\mathrm{E}}=\boldsymbol{k}_{\mathrm{A}}\right)\right]\le 2^{-1,000,000}+2^{-50}\,. \tag{16}$$

This result clearly shows that the obtained key is not IID at all. Consider the simplest example as follows. For Eve, it is like there are 2^{50} patterns of key candidates equally possible, and no other key candidates, which satisfies $\Pr(\boldsymbol{K}|\boldsymbol{E}) \sim 2^{-50}$. On the other hand, if the distributed key is IID, there are $2^{1,000,000}$ patterns of equally possible keys for Eve. This is what

Yuen has been warning. Moreover, this means we can never satisfy the concept called "Universal Composability" because Eve has only 2^{50} possible keys, not $2^{1,000,000}$ keys. The Universal Composability[15] is a concept that any parts of the key are usable to other cryptosystems without threats when one of the systems is under attacks. This is because any parts of the keys are statistically independent from other parts. The above situation explains us that the Universal Composability will never be satisfied unless $\varepsilon_{\text{sec}} = 0$.

Then, change our mind. Now, it is shown that QKD keys are not perfect at all. However, of course, if ε_{sec} is small enough, we can say the QKD key is information-theoretically secure enough for practical uses. However, consider the following estimations. Assume that a QKD system is running for 24 hours 365 days, at the communication speed of 10^9 bits/sec with the final key length 10^6 bits. Then, 3×10^{10} keys will be exchanged in a year. Since $2^{-|K|} \ll \varepsilon_{\text{sec}}$, the expected number of keys leaked to Eve is 3×10^{-5}. This number looks sufficient for the security. However, 7.5×10^3 traffic fatal accidents had been reported in 2008 in Japan[26], while there were 7.9×10^7 cars in the same year[27]. Therefore, one car caused 9.5×10^{-5} traffic fatal accidents in average in 2008. The above values show that the number of potential eavesdropping on one QKD system in a year is about the same order of magnitude of traffic fatal accidents one car may causes in a year. If QKD systems spread over the world as explained in the introduction, the number of potential eavesdropping is close to the number of traffic fatal accidents, if $\varepsilon_{\text{sec}} = 2^{-50} = 8.9\times10^{-16}$. See also the past works by the author[28, 29]. Theoretically, it is often said that ε_{sec} could be arbitrarily small, so we could enhance the security of QKDs as high as we would wish. The author will discuss this point in the next subsection.

2.3 Criticisms on Derivation of Secure Key Rate

Yuen also questioned on the derivation of the secure key rate. The general procedures of QKDs are well known, but here the author describes as follows[30].

1. The transmitter Alice chooses the bit to send and the encoding quantum basis randomly, then she sends a corresponding quantum state to the receiver, Bob.
2. Bob also chooses the measurement basis randomly, and obtain the classical bit from the measurement.
3. They repeat the above procedures, then they discuss on the classical authenticated channel to discard the bits they chose different communication bases and holds the bits with the same communication bases.
4. Alice and Bob announces the part of their measurement results to estimate Quantum-Bit-Error-Rate, Q. If Q is greater than the certain threshold, they abort the communication regarding they cannot yield secure key strings. When they can, they proceed to error-corrections in the key strings for key agreement.
5. Alice announces the parity check matrix for the error correction, and she calculates her syndrome with it. Then she sends her syndrome to Bob hiding it by One-Time Pad (OTP) using the part of the pre-shared key.
6. Bob also calculates his syndrome using the parity check matrix Alice announced. Then he operates error-correction comparing his syndrome with Alice's one.
7. Finally, they proceed to Privacy Amplification to eliminate Eve's knowledge on the shared key, by announcing a hash function in public classical channel.

In the above process, the key consumption for OTP to hide Alice's syndrome is often given by

$$\text{leak}_{\text{EC}} = \xi \left| K_{\text{S}} \right| h_2(Q) . \tag{17}$$

Here, ξ is a factor chosen from 1 to 2, depending on the strength of the error correction code. Typically, it is set to $\xi = 1.1$ [30, 31]. To prove (17) for the case $\xi = 1$, see the following calculation. Now, let $|K_{\text{S}}|$ be the sifted key length and $|M|$ be the length of information digits. Consider $(|K_{\text{S}}|, |M|)$ linear codes, which can correct up to $Q|K_{\text{S}}|$ errors. From Hamming bound,

$$2^{|M|} \le 2^{|K_{\text{S}}|} / \sum_{e=0}^{Q|K_{\text{S}}|} {}_{|K_{\text{S}}|}C_e . \tag{18}$$

Therefore, the following inequality has to be satisfied.

$$\sum_{e=0}^{Q|K_{\text{S}}|} {}_{|K_{\text{S}}|}C_e \le 2^{|K_{\text{S}}| h_2(Q)} \le 2^{|K_{\text{S}}| - |M|} . \tag{19}$$

Thus, the key consumption by OTP to hide Alice's syndrome is $|K_S|h_2(Q)$ bits, where $h_2(Q)$ is Shannon binary entropy.

However, Yuen explains as follows. If we use ($|K_S|$, $|M|$) linear codes, the number of key candidates would shrink down to $2^{|M|}$ while we had $2^{|K_S|}$ possible candidates before the error correction. This problem would not be solved even if they hide the syndrome by OTP. One may say that there could be $2^{|K_S|-|M|}$ patterns of syndromes, and Eve would not know whether Alice and Bob reconcile their keys with which one, therefore the possible patterns of the key still remains $2^{|M|} \times 2^{|K_S|-|M|} = 2^{|K_S|}$. However, recall that Eve knows the shared key in the previous QKD round with a probability of ε_{sec}. Thus, there are only $\varepsilon_{sec}^{-1} 2^{|K_S|-|M|}$ patterns of possible keys, not $2^{|K_S|} \gg \varepsilon_{sec}^{-1} 2^{|K_S|-|M|}$, even when Eve does only pure guessing. In reality, Eve would guess the most likely key Alice and Bob shared from her measurement results when she needs, therefore the number of possible key patterns is unknown but may be narrowed down further. Therefore, using ($|K_S|$, $|M|$) linear error correction codes narrows down the possible patterns of the key for Eve in practice. There are no related studies about this issue as far as the author knows. Therefore, we cannot discuss this problem numerically furthermore.

To solve this problem, Yuen proposed an idea as follows. Consider ($|N|$, $|K_S|$) linear codes adding $|N| - |K_S|$ bits of parity check digits to the original sifted key before error correction. Then, even after the error correction, there still may be $2^{|K_S|}$ patterns of possible keys for Eve. Instead, we have to consume $|N|h_2(Q)$ bits of the pre-shared key to hide the added parity check digit by OTP to tell Bob. The amount of $|N|$ is given by Hamming bound again as seen in (18, 19). Therefore,

$$\sum_{e=0}^{Q|N|} {}_{|N|}C_e \le 2^{|N|h_2(Q)} \le 2^{|N|-|K_S|}. \tag{20}$$

Thus the key consumption by OTP for error correction is

$$\mathrm{leak}_{EC} = |K_S| h_2(Q) \left[1 - |K_S| h_2(Q)\right]^{-1} \ge |K_S| h_2(Q). \tag{21}$$

In addition, Yuen pointed out that choosing $\xi = 1.1$ habitually is not a "proven analysis" against QKD's original concept.

Here, the author gives some numerical analysis with $\varepsilon_{sec} = 10^{-24} \sim 2^{-80}$ in Fig. 1 done in the study in the literature[32]. When we use (21) derived by Yuen gives lower secure key rate especially in case of larger Q. Moreover, if the quantum channel is lossy, there are lower-limit that ε_{sec} cannot be smaller than certain values[32].

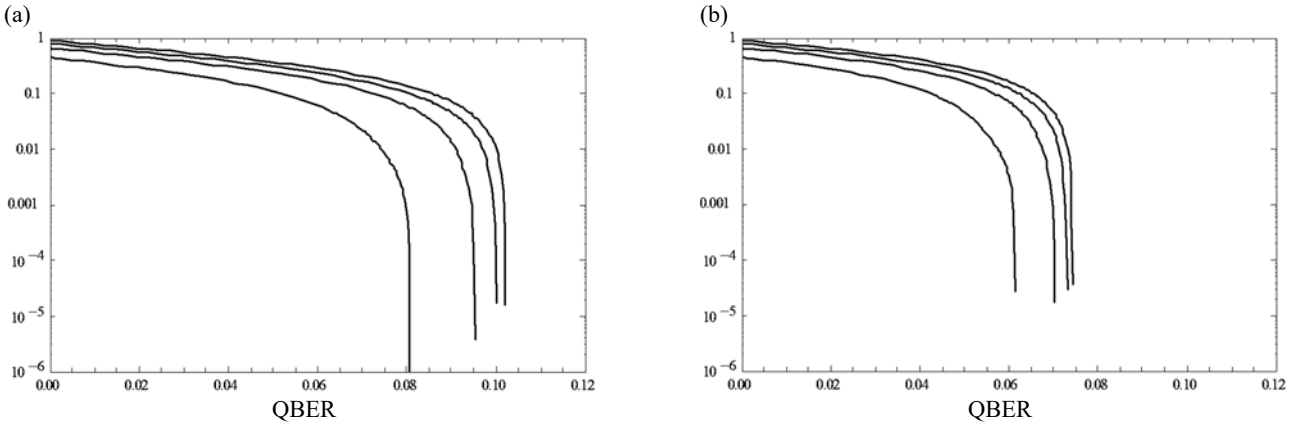

Fig. 1. (a) Key rates with leak_{EC} in (17), and (b) in (22). From the lowest curve, the sifted key length = 10^5, 10^6, 10^7, 10^9 bits. In case of Yuen's Leak_{EC}, the allowable QBER will be stricter.

2.4 Criticisms on Use of Privacy Amplification

Yuen also pointed out that Privacy Amplification may be rather harmful for the security of QKDs. His description[19] is not easy to understand, therefore, the author tries a different explanation. Consider Eve eavesdropped the quantum channel and store the quantum states correlated to the legitimate users' key in her quantum memory. Assume that, after Alice and Bob finished error correction, Eve measures her quantum memory and obtained the key string $\boldsymbol{k}_{ER}$, while Alice and Bob share the key $\boldsymbol{k}_R$. Now, let Alice choose and announce a hash function f from a set of δ-Almost Two-Universal hash function family F, then

$$\Pr_{f\in F}[f(\boldsymbol{k}_{\mathrm{ER}}) = f(\boldsymbol{k}_{\mathrm{R}})] \le \delta\,. \tag{22}$$

There are two possible cases that Eve obtains the correct key $\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}}$, and $\boldsymbol{k}_{\mathrm{ER}} \neq \boldsymbol{k}_{\mathrm{R}}$ but collision occurs because of the property of hash functions. Therefore, Eve's success probability in obtaining the correct key in the end is,

$$\begin{aligned}\Pr\left(\boldsymbol{K} \mid \boldsymbol{E}\right) &= \Pr(\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}}) + \Pr(\boldsymbol{k}_{\mathrm{ER}} \neq \boldsymbol{k}_{\mathrm{R}})\Pr(f(\boldsymbol{k}_{\mathrm{ER}}) = f(\boldsymbol{k}_{\mathrm{R}})) \\ &\le \Pr(\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}}) + \left(1 - \Pr(\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}})\right)\delta\end{aligned}\,. \tag{23}$$

The max $\Pr(\boldsymbol{K}|\boldsymbol{E})$ in (23) is larger than Eve's guessing probability before the Privacy Amplification, that is, $\Pr(\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}})$ in (23). This is understandable as follows. Even if Eve obtains the wrong key after the error correction, she may obtain the correct key by chance because of the collision probability of the hash function. Therefore, the following question arises: is Privacy Amplification really useful to gain the security of the distributed key? Consider the following example. Let $|K_{\mathrm{R}}|$ be the length of a reconciled key before Privacy Amplification, let $|K|$ be the key length after Privacy Amplification. Because of the characteristics of hash functions, trivially $|K_{\mathrm{R}}| > |K|$. If Eve does not even eavesdropping on the quantum channel but she guesses the correct key by pure guessing, it is trivial that she has more chance in guessing the correct key after hashing than she had before hashing. Yuen explained that the reason why Privacy Amplification has given misconception that it would enhance the key security was, that the averaging the hashing performance over the hashing family F in Leftover Hash Lemma. However, in reality, Alice announces publically which hash function they use. Therefore, Eve knows exactly which function is used. Therefore, to evaluate the performance of Privacy Amplification, we need to evaluate the performance of a chosen hash function without averaging. Here, the author of this article adds the other reason. Leftover hash lemma surely gives more uniform key probability distribution. However, key-shortening by hashing would raise the average of the probability distribution, giving Eve more chance to guess the correct key.

A more complicating problem is related to the previous topic of error correction. If we regard the sifted key as $(|K_{\mathrm{S}}|, |M|)$ linear codes, then there should be correlations among key bits, because we regard $|K_{\mathrm{S}}|$-bit key as $(|K_{\mathrm{S}}|, |M|)$ code, there are only $2^{|M|}$ patterns of key candidates instead of $2^{|K_{\mathrm{S}}|}$ patterns of key candidates. Evaluating the effect of Privacy Amplification is not easy when there are correlations between key bits. Therefore, again, we need to add parity check digits to the sifted key to make it $(|N|, |K_{\mathrm{S}}|)$ code, to have less correlation among key bits, so we have to take the previous problem seriously.

2.5 Authenticity of Communication Channels

There seem to be many people misunderstanding outside of the QKD researcher community because it is a common sense among QKD researchers, thus it is rarely explained. Therefore, the author explicitly writes here. Before starting QKD, Alice and Bob need to have pre-shared authentication key to recognize each other[33]. Otherwise, Eve can launch Man-in-the-Middle Attacks by pretending to be Bob to Alice, and same to Bob to be Alice, relaying both classical and quantum signals coming from Alice to Bob, which allows not only perfect eavesdropping but also falsifying the messages. Moreover, some QKD procedures need a pre-shared key for OTP for Error-Correction as explained in Sec. 2.3. In this sense, QKD is not a public key distribution technology to replace conventional public key encryptions like RSA, say, the public key of RSA is known to even Eve, but the authentication key and the pre-shared OTP key in QKDs should not be disclosed to Eve. Therefore, Alice and Bob need to share the pre-shared key secretly in some way before they start QKDs. In this sense, QKDs are similar to symmetric key cryptographies like AES, unlike public key encryptions such as RSA.

Yuen pointed out the importance of the security level of this authentication key. We may be able to share an authentication key with IID at first, but what will happen if we renew the authentication key by the part of the distributed key? As it was explained in Sec. 2.2, Eve guesses the correct key with a probability of about $\varepsilon_{\mathrm{sec}}$. Yuen regards the security of authentication is far more important than the security level of message encryption, therefore he claims $\varepsilon_{\mathrm{sec}}$ has to be far smaller than we currently can obtain. Even if $\varepsilon_{\mathrm{sec}}$ is small enough, the renewed authentication key is a part of the distributed key known to Eve with a probability of about $\varepsilon_{\mathrm{sec}}$, resulting in security degradation compared to the initial authentication key with IID, and this continues as long as QKD operation is being continued. Furthermore, the part of the distributed key known to Eve with a probability of about $\varepsilon_{\mathrm{sec}}$ has to be used in OTP for Error-Correction in Sec. 2.3. Therefore, the influence of the security degradation has to be included in security proofs for the concept of "provable security."

2.6 Importance of Bit-Error-Rate for Eavesdropper

Yuen raised a question as follows: even if Eve could not obtain the correct key, but she obtained a key close to the key Alice and Bob share, then what will happen? Cannot Eve read the message at all even if her key has just 1-bit error? How about 2 bits? Then 3 bits? Yuen emphasized the importance of Bit-Error-Rate (BER) for Eve, because it corresponds to the BER on the encrypted message by OTP, therefore he named it "BER Guarantee" [19, 20]. Clearly, a perfect key for OTP has the IID key so BER is always 1/2 for Eve, therefore she can never read the encrypted message. However, if she knows her BER is far smaller than 1/2, then she may be able to read some part of the encrypted message. Here is an example. Suppose you got a message "Tahnks" from your friend. You usually think it was a typo of "Thanks." We have no difficulties to recover the original message even there were some typos.

Now going back to the topic of QKDs, here the author writes a rough estimation. Suppose Eve can read the message if her key has BER less than the certain BER, B_E. The number of such a situation is expressed by

$$\sum_{e=0}^{|K|B_E} {}_{|K|}C_e \le 2^{|K|h_2(B_E)}. \tag{24}$$

Therefore, the rough estimation of Eve's success probability in obtaining a nearly correct message is

$$\Pr(\boldsymbol{K} \mid \boldsymbol{E}) 2^{|K|h_2(B_E)} \le 2^{-|K|(1-h_2(B_E))} + \varepsilon_{sec} 2^{|K|h_2(B_E)}. \tag{25}$$

As shown in (25), the chance Eve can read a nearly correct message would raise exponentially to the length of the secret key $|K|$. So, if $\varepsilon_{sec} = 2^{-50}$ and $|K| = 10^6$ bits, Eve's probability in obtaining a nearly correct message is almost $\Pr(\boldsymbol{K}|\boldsymbol{E}) = 1$ up to $|K|B_E = 2.5$ errors, which means Eve has no struggling in reading the encrypted message. Surely, even the author thinks the estimation by (25) is too rough, and Yuen himself wrote that it is an open question how we evaluate the security of QKDs under BER guarantee. We need further studies, and this is the main topic of this article. See an example in Sec. 3.

2.7 Security level of the cryptosystems and impossibility of experimental guarantee for general attacks

There are many experimental reports, thus the author does not list them here that their QKD systems were stably working over months or more. However, can we really confirm that Eve could not steal the key even with unlimited power except the limitations by laws of nature? One may say that the noisy environment itself is the Eve who can freely interacts with flying qubits. Then how we confirm the noisy environment could not steal the key?

Furthermore, these experimental reports said their systems were secure because the generated key rates were positive. On the other hand, we have seen that the security level is evaluated by ε_{sec} in Sec. 2.2. How much were their ε_{sec} actually in their experiments? There have been several theories to calculate the key generation rate for the finite key length with corresponding ε_{cor} and ε_{sec}. From these theories, we can derive positive key rates even with $\varepsilon_{sec} = 1$ [31, 32]. This means, the key is surely generated, but Eve can steal the key with the probability of 1, as we have seen in Sec 2.2. Therefore, the positive key generation rate never means the key is secure. The problem is always "how much secure the key is."

National Cyber Security Centre (NCSC), a part of Government Communications Headquarters (GCHQ) in UK uploaded a white paper to suggest not to use QKDs for important communication infrastructures at this phase. Here are some quotes[5].

"Consequently, QKD seems to be introducing a whole new set of potential avenues for attack that are not yet well understood." "Do not endorse QKD for any government or military applications." "Advise against replacing any existing public key solutions with QKD for commercial applications."

Yuen also described as follows[19].

"Security cannot be proved experimentally, if only because there are an infinite variety of possible attacks, which cannot all be described. There were many surprises in the history of cryptography; thus, whether there is a valid proof in an important issue, especially in QKD, where provable security appears to be the only real advantage compared to conventional cryptography."

He also quoted from the literature[34].

“Don't blindly trust anything, even if it is in print. You'll soon see that having this critical mind is an essential ingredient of what we call “professional paranoia.””

The biggest advantage of QKDs is its concept that “the security is proven against general attacks,” regardless how expensive the cryptosystems are and how slow the communication is compared to the current communication technologies. Then, if we cannot experimentally test the security of QKDs against at least variety types of potential attacks, there is a big question why we have to develop them.

2.8 Alternative security measure: quantum min-entropy

There is another possibly meaningful security measure, called min-entropy. However, it is closely connected to Eve’s probability of guessing the correct key[35]. Therefore, the author thinks there is not so big differences from using the trace distance criterion. Any other abstract security measures should be avoided because your customer would not be convinced by such an abstract security terms; they should be eager to know how much secure your system is.

3. EXAMPLE OF BIT-ERROR-RATE SECURITY GUARANTEE PROPOSED BY YUEN

This section describes an example of the BER Guarantee for BB84 protocol under Entangling-Probe Attacks (EPA) studied in the literatures[36-40]. However, their security criterion was the mutual information, which has been abandoned after the literature[14]. Therefore, this study tries adjustment of the attack for BER Guarantee. Here, we assume distribution of a sufficiently long key.

3.1 Entangling Probe Attack on BB84 protocol

Consider the following four quantum states to operate BB84 protocol for $(x_A, b_A) = \{0, 1\}^2$, where x_A is a key bit to be shared, and b_A indicates the communication basis Alice uses.

$$\left|(x_A, b_A)\right\rangle := \delta_{0,b_A}\left|x_A\right\rangle + \tfrac{1}{\sqrt{2}}\delta_{1,b_A}\left[\left|0\right\rangle + (-1)^{x_A}\left|1\right\rangle\right]. \tag{26}$$

Alice chooses one of the four quantum states in (26) with her prior probability of 1/4. On the other hand, Bob sets a measurement operator defined in (27) to yield a received bit x_B choosing his basis b_B randomly.

$$M(x_B, b_B) := \left|(x_B, b_B)\right\rangle\left\langle(x_B, b_B)\right|. \tag{27}$$

We omit the sifting process, therefore we regard Alice and Bob already have announced their basis $b_A = b_B$.

While Alice is transmitting her quantum state described in (26) to Bob, Eve attaches her quantum system and performs unitary operation U with the transmitted quantum system. Therefore,

$$\left|\psi\right\rangle := U\left|(x_A, b_A)\right\rangle_B\left|0\right\rangle_E = \sum_{k_B,k_E}\left[\delta_{0,b_A}u_{k_B,k_E,x_A} + \delta_{1,b_A}\tfrac{1}{\sqrt{2}}\left[u_{k_B,k_E,0} + (-1)^{x_A}u_{k_B,k_E,1}\right]\right]\left|k_B, k_E\right\rangle. \tag{28}$$

The U is defined as

$$\begin{aligned} U &= \sum_{k_B,k_E,k_A} u_{k_B,k_E,k_A}\left|k_B, k_E\right\rangle\left\langle k_A, 0\right| \\ UU^\dagger &= \sum_{k_B,k_E,k_A,k'_B,k'_E} u_{k_B,k_E,k_A}u^\dagger_{k'_B,k'_E,k_A}\left|k_B, k_E\right\rangle\left\langle k'_B, k'_E\right| = I \end{aligned}. \tag{29}$$

Bob receives the following quantum system.

$$\mathrm{tr}_{\mathrm{E}}\left|\psi\right\rangle\left\langle\psi\right| = \sum_{k_{\mathrm{E}},k_{\mathrm{B}},k'_{\mathrm{B}}}\left[\delta_{0,b_{\mathrm{A}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},x_{\mathrm{A}}}u^{\dagger}_{k'_{\mathrm{B}},k_{\mathrm{E}},x_{\mathrm{A}}} + \delta_{1,b_{\mathrm{A}}}\tfrac{1}{2}\left[u_{k_{\mathrm{B}},k_{\mathrm{E}},0} + (-1)^{x_{\mathrm{A}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},1}\right]\left[u_{k'_{\mathrm{B}},k_{\mathrm{E}},0} + (-1)^{x_{\mathrm{A}}}u_{k'_{\mathrm{B}},k_{\mathrm{E}},1}\right]^{\dagger}\right]\left|k_{\mathrm{B}}\right\rangle\left\langle k'_{\mathrm{B}}\right| . \quad (30)$$

Therefore, Bob's Quantum-Bit-Error-Rate (QBER) Q is

$$Q = \tfrac{1}{4}\sum_{x_{\mathrm{A}}}\left[\left|\sum_{k_{\mathrm{E}}}u_{1-x_{\mathrm{A}},k_{\mathrm{E}},x_{\mathrm{A}}}\right|^2 + \tfrac{1}{4}\left|\sum_{k_{\mathrm{E}}}\left(u_{0,k_{\mathrm{E}},0} - u_{1,k_{\mathrm{E}},1}\right) + (-1)^{x_{\mathrm{A}}}\left(u_{0,k_{\mathrm{E}},1} - u_{1,k_{\mathrm{E}},0}\right)\right|^2\right]. \quad (31)$$

On the other hand, Eve receives the following quantum state.

$$\mathrm{tr}_{\mathrm{B}}\left|\psi\right\rangle\left\langle\psi\right| \coloneqq \sum_{k_{\mathrm{B}},k_{\mathrm{E}},k'_{\mathrm{E}}}\left[\delta_{0,b_{\mathrm{A}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},x_{\mathrm{A}}}u^{\dagger}_{k_{\mathrm{B}},k'_{\mathrm{E}},x_{\mathrm{A}}} + \delta_{1,b_{\mathrm{A}}}\tfrac{1}{2}\left(u_{k_{\mathrm{B}},k_{\mathrm{E}},0} + (-1)^{x_{\mathrm{A}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},1}\right)\left(u_{k_{\mathrm{B}},k'_{\mathrm{E}},0} + (-1)^{x_{\mathrm{A}}}u_{k_{\mathrm{B}},k'_{\mathrm{E}},1}\right)^{\dagger}\right]\left|k_{\mathrm{E}}\right\rangle\left\langle k'_{\mathrm{E}}\right| . \quad (32)$$

Before Eve measures her system, she listens to the classical public channel to know how Alice and Bob reconcile their sifted keys. For example, when Bob corrects errors in his sifted key to obtain Alice's key, Eve's BER in her key is, from Helstrom's quantum binary decision theory[41],

$$\begin{aligned}\Pr(x_{\mathrm{E}} \neq x_{\mathrm{A}}) \geq \frac{1}{2} - \frac{1}{8}\sum_{k_{\mathrm{E}}}\left|\left|\sum_{k_{\mathrm{B}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},0}\right|^2 - \left|\sum_{k_{\mathrm{B}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},1}\right|^2\right| \\ - \frac{1}{8}\sum_{k_{\mathrm{E}}}\frac{1}{2}\left|\left|\sum_{k_{\mathrm{B}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},0} + u_{k_{\mathrm{B}},k_{\mathrm{E}},1}\right|^2 - \left|\sum_{k_{\mathrm{B}}}u_{k_{\mathrm{B}},k_{\mathrm{E}},0} - u_{k_{\mathrm{B}},k_{\mathrm{E}},1}\right|^2\right|\end{aligned} . \quad (33)$$

When Aice reconciles her sifted key with Bob's key, Eve's BER in her key is,

$$\begin{aligned}\Pr(x_{\mathrm{E}} \neq x_{\mathrm{B}}) &= \Pr(x_{\mathrm{E}} \neq x_{\mathrm{A}})\Pr(x_{\mathrm{A}} = x_{\mathrm{B}}) + \Pr(x_{\mathrm{E}} = x_{\mathrm{A}})\Pr(x_{\mathrm{A}} \neq x_{\mathrm{B}}) \\ &= \Pr(x_{\mathrm{E}} \neq x_{\mathrm{A}})(1-Q) + [1 - \Pr(x_{\mathrm{E}} \neq x_{\mathrm{A}})]Q \\ &= \Pr(x_{\mathrm{E}} \neq x_{\mathrm{A}})(1-2Q) + Q \coloneqq \mathrm{B}(Q) \\ &> \Pr(x_{\mathrm{E}} \neq x_{\mathrm{A}})\end{aligned} . \quad (34)$$

Therefore, in this case, it is harder for Eve to guess Bob's key. Thus, assume Alice reconciles her sifted key with Bob's key. Note, furthermore, that Eve optimizes her unitary operation U to minimize (33). However, this optimization is not the main topic of this paper, and conclusion will remain unchanged. Eve's success probability in obtaining the correct key is,

$$\Pr(\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}}) = \left[1 - \mathrm{B}(Q)\right]^{-|K_{\mathrm{R}}|}. \quad (35)$$

If Eve could successfully guessed the correct key after the Error-Correction, she can obtain the correct key even after the Privacy Amplification because she knows the hashing function used from the broadcasting Alice and Bob made. Then the success probability in eavesdropping is,

$$\begin{aligned}\Pr\left(\boldsymbol{K} \mid \boldsymbol{E}\right) &= \Pr(\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}}) + \Pr(\boldsymbol{k}_{\mathrm{ER}} \neq \boldsymbol{k}_{\mathrm{R}})\Pr(f(\boldsymbol{k}_{\mathrm{ER}}) = f(\boldsymbol{k}_{\mathrm{R}})) \\ &\leq \left[1 - \mathrm{B}(Q)\right]^{-|K_{\mathrm{R}}|} + \left(1 - \left[1 - \mathrm{B}(Q)\right]^{-|K_{\mathrm{R}}|}\right)\delta \\ &= (1-\delta)\left[1 - \mathrm{B}(Q)\right]^{-|K_{\mathrm{R}}|} + \delta\end{aligned} . \quad (36)$$

Now, we are going to evaluate the security of BB84 in BER guarantee. Eve knows her BER before the step of Privacy Amplification. For an announced hashing matrix f, Eve knows which key strings will be projected onto which hashed strings. For instance, suppose Eve chose a key $\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}} + \boldsymbol{e}_{\mathrm{R}}$ (mod 2) with error string $\boldsymbol{e}_{\mathrm{R}}$, it will be projected onto the certain final key with errors, $f(\boldsymbol{k}_{\mathrm{R}} + \boldsymbol{e}_{\mathrm{R}}) = \boldsymbol{k} + \boldsymbol{e}$ (mod 2). Then, the same manner in (36) can be applied to

$$\begin{aligned}&\Pr(\boldsymbol{k}_{\mathrm{ER}} = \boldsymbol{k}_{\mathrm{R}} + \boldsymbol{e}_{\mathrm{R}}) + \Pr(\boldsymbol{k}_{\mathrm{ER}} \neq \boldsymbol{k}_{\mathrm{R}} + \boldsymbol{e}_{\mathrm{R}})\Pr(f(\boldsymbol{k}_{\mathrm{ER}}) = f(\boldsymbol{k}_{\mathrm{R}} + \boldsymbol{e}_{\mathrm{R}})) \\ &\leq (1-\delta)\,\mathrm{B}(Q)^{-\mathrm{wt}(\boldsymbol{e}_{\mathrm{R}})}\left[1 - \mathrm{B}(Q)\right]^{-|K_{\mathrm{R}}|+\mathrm{wt}(\boldsymbol{e}_{\mathrm{R}})} + \delta\end{aligned} . \quad (37)$$

Here, $\mathrm{wt}(\boldsymbol{e}_{\mathrm{R}})$ denotes the number of errors in the error string $\boldsymbol{e}_{\mathrm{R}}$. Therefore,

$$\begin{aligned}\Pr\left(\mathrm{wt}(\boldsymbol{K}-\boldsymbol{K}_{\mathrm{E}})\le|K_{\mathrm{R}}|B_{\mathrm{E}}\right)&=\sum_{\mathrm{wt}(\boldsymbol{e}_{\mathrm{R}})=0}^{|K_{\mathrm{R}}|B_{\mathrm{E}}}{}_{|K_{\mathrm{R}}|}C_{\mathrm{wt}(\boldsymbol{e}_{\mathrm{R}})}\left[(1-\delta)\,\mathrm{B}(Q)^{\mathrm{wt}(\boldsymbol{e}_{\mathrm{R}})}\left[1-\mathrm{B}(Q)\right]^{-|K_{\mathrm{R}}|+\mathrm{wt}(\boldsymbol{e}_{\mathrm{R}})}+\delta\right]\\&\le 2^{|K_{\mathrm{R}}|h_2(B_{\mathrm{E}})}\left[\delta+(1-\delta)2^{|K_{\mathrm{R}}|h_2(\mathrm{B}(Q))}\left[1-\mathrm{B}(Q)\right]^{-|K_{\mathrm{R}}|\mathrm{B}(Q)}\right]\\&\le 2^{|K_{\mathrm{R}}|h_2(B_{\mathrm{E}})}\left[\delta+2^{|K_{\mathrm{R}}|h_2(\mathrm{B}(Q))}\left(\max\Pr\left(\boldsymbol{K}\,|\,\boldsymbol{E}\right)-\delta\right)\left[1-\mathrm{B}(Q)\right]^{|K_{\mathrm{R}}|(1-\mathrm{B}(Q))}\right]\\&\sim 2^{|K_{\mathrm{R}}|h_2(B_{\mathrm{E}})}2^{|K_{\mathrm{R}}|h_2(\mathrm{B}(Q))}\left[1-\mathrm{B}(Q)\right]^{|K_{\mathrm{R}}|(1-\mathrm{B}(Q))}\max\Pr\left(\boldsymbol{K}\,|\,\boldsymbol{E}\right)\end{aligned}. \tag{38}$$

Therefore, we see that Eve has an exponentially more chance to obtain the near-perfect plaintext as we have seen in Sec.2.6.

At this phase, B_{E}, the acceptable BER in the plaintext for Eve, is unknown. However, she may add noise from the outside of the classical authenticated channel without breaking the authentication. Then, Alice and Bob need to utilize error-correcting codes and its parity check matrix for classical communications. This may allow Eve to remove all errors in her near-perfect key up to $|K_{\mathrm{R}}|B_{\mathrm{E}}$ errors utilizing the announced parity check matrix and subtracting noise she added by herself. To prevent this kind of attacks, we may need to monitor the BER in the classical authenticated channel, and abort the protocol when the BER is too high, like the high QBER case in the quantum channel.

Moreover, note that this discussion is under assumptions that Eve perform individual attacks on each qubits, and she performs measurements after the Error-Correction. We are not sure how much secure BB84 is by means of BER guarantee under general attacks, such as collective attacks or coherent attacks.

4. POSSIBLE PROBLEMS IN SECURITY PROOFS BASED ON TRACE DISTANCE

As we have seen in Sec. 2.2., the trace distance criterion gives the maximum value of the expected probability in guessing the correct key by Eve. Even though, there are two standardized definitions in the trace distance criterion. In (3),

Case 1: $\tau_{\mathrm{E}}=\sigma_{\mathrm{E}}\coloneqq \mathrm{tr}_{\mathrm{AB}}\,\sigma_{\mathrm{ABE}}$, which is the widely used definition.

Case 2: $\tau_{\mathrm{E}}=\kappa_{\mathrm{E}}$ to hold the equality of $F(\zeta_{\mathrm{ABE}},|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})\le F(\mathrm{tr}_{\mathrm{E}}\,\zeta_{\mathrm{ABE}},|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}})$, where ζ_{ABE} is a distributed state by a entanglement-based QKD with a maximally entangled state $|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}}$[30].

There is one more possibility, the author thinks.

Case 3: τ_{E} is chosen by Eve to maximize her guessing probability of the correct key, $\Pr(\boldsymbol{K}|\boldsymbol{E})$.

Note that, in Case 3, Eve may define a different trace distance from the one Alice and Bob defined as in Case 1 and 2.

4.1 Case 1: the standardized definition of the trace distance security criterion

From the definition, consider the following spectral decomposition to calculate the trace distance:

$$\begin{aligned}\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\sigma_{\mathrm{E}}&=\sum_{\boldsymbol{k}}|\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k},\boldsymbol{k}|\otimes\sum_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}}\left[\delta_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}}-2^{-|K|}\right]\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\\&\coloneqq\sum_{\boldsymbol{k},\boldsymbol{k}_{\mathrm{E}}}|\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k},\boldsymbol{k}|\otimes\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}(\boldsymbol{k})\left|\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}(\boldsymbol{k})\right\rangle\left\langle\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}(\boldsymbol{k})\right|\end{aligned}. \tag{39}$$

The operator set $\left\{\left|\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}\right\rangle\left\langle\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}\right|\right\}$ could be POVM on Eve's system to obtain $\boldsymbol{k}_{\mathrm{E}}$. From (39). Furthermore,

$$\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}(\boldsymbol{k})=\sum_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}}\left[\delta_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}}-2^{-|K|}\right]\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left\langle\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}\left|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right|\lambda^{(\sigma)}_{\boldsymbol{k}_{\mathrm{E}}}\right\rangle. \tag{40}$$

Therefore,

$$\begin{aligned}\tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\sigma_{\mathrm{E}}\right| &= \sum\nolimits_{\boldsymbol{k},\boldsymbol{k}_{\mathrm{E}}:\lambda\geq 0}\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\sigma)}(\boldsymbol{k})=\sum\nolimits_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{B}}}\left[1-2^{-|K|}\right]\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left\langle\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\sigma)}\middle|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\middle|\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\sigma)}\right\rangle \\ &\geq \sum\nolimits_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}}\left[1-2^{-|K|}\right]\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left\langle\lambda_{\boldsymbol{k}_{\mathrm{A}}}^{(\sigma)}\middle|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\middle|\lambda_{\boldsymbol{k}_{\mathrm{A}}}^{(\sigma)}\right\rangle=\left[1-2^{-|K|}\right]\Pr\left(\boldsymbol{K}\mid\boldsymbol{E}\right)\end{aligned}. \tag{41}$$

Thus the conclusion is, with the result already has been given in Sec. 2.2,

$$\begin{aligned}\Pr\left(\boldsymbol{K}\mid\boldsymbol{E}\right) &\leq \left[1-2^{-|K|}\right]^{-1}\tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\sigma_{\mathrm{E}}\right| \\ &\leq 2^{-|K|}+\tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\sigma_{\mathrm{E}}\right|\leq 2^{-|K|}+\varepsilon_{\mathrm{sec}}^{(\sigma)}\end{aligned}. \tag{42}$$

4.2 Case 2: Koashi's security proof based on Shor-Preskill approach

Case 2 [30] has to satisfy the equality of

$$\sqrt{1-F(\zeta_{\mathrm{AB}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}})^2}\leq\sqrt{1-F(\zeta_{\mathrm{ABE}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})^2}\,. \tag{43}$$

Otherwise, the trace distance cannot be upper-bounded because

$$\begin{aligned}\varepsilon_{\mathrm{sec}}^{(\kappa)} &\geq \sqrt{1-F(\zeta_{\mathrm{AB}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}})^2}\leq\sqrt{1-F(\zeta_{\mathrm{ABE}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})^2} \\ &\geq \sqrt{1-F(\sigma_{\mathrm{ABE}},\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})^2}\geq\tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right|\end{aligned}. \tag{44}$$

Here, the Fidelity is defined as

$$F(\zeta,\kappa):=\operatorname{tr}\sqrt{\kappa^{1/2}\zeta\kappa^{1/2}}\,. \tag{45}$$

Now, consider the following spectral decomposition

$$\kappa_{\mathrm{E}}:=\sum\nolimits_{\boldsymbol{l}}\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\left|\kappa_{\mathrm{E}}(\boldsymbol{l})\right\rangle\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\right|. \tag{46}$$

Then, by Cauchy-Schwarz inequality,

$$\begin{aligned}F(\zeta_{\mathrm{ABE}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}) &= \operatorname{tr}\sqrt{\left(\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right)^{1/2}\zeta_{\mathrm{ABE}}\left(\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right)^{1/2}} \\ &= \sum\nolimits_{\boldsymbol{l}}\sqrt{\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\middle|\left\langle\mathrm{MES}\middle|\zeta_{\mathrm{ABE}}\middle|\mathrm{MES}\right\rangle\middle|\kappa_{\mathrm{E}}(\boldsymbol{l})\right\rangle} \\ &\leq \left[\sum\nolimits_{\boldsymbol{l}}\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\right]^{1/2}\left[\sum\nolimits_{\boldsymbol{l}}\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\middle|\left\langle\mathrm{MES}\middle|\zeta_{\mathrm{ABE}}\middle|\mathrm{MES}\right\rangle\middle|\kappa_{\mathrm{E}}(\boldsymbol{l})\right\rangle\right]^{1/2} \\ &= 1\times\left[\left\langle\mathrm{MES}\middle|\operatorname{tr}_{\mathrm{E}}\left(\zeta_{\mathrm{ABE}}\right)\middle|\mathrm{MES}\right\rangle\right]^{1/2}=F(\zeta_{\mathrm{AB}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}})\end{aligned}. \tag{47}$$

Therefore, the equality of (47) is satisfied by choosing in (46) as,

$$\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))=\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\middle|\left\langle\mathrm{MES}\middle|\zeta_{\mathrm{ABE}}\middle|\mathrm{MES}\right\rangle\middle|\kappa_{\mathrm{E}}(\boldsymbol{l})\right\rangle F(\zeta_{\mathrm{AB}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}})^{-2}. \tag{48}$$

As a result, using an inequality between trace distance and fidelity,

$$\begin{aligned}\varepsilon_{\mathrm{sec}}^{(\kappa)} &\geq \sqrt{1-F(\zeta_{\mathrm{AB}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}})^2}=\sqrt{1-F(\zeta_{\mathrm{ABE}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})^2} \\ &\geq \sqrt{1-F\left(\Lambda(\zeta_{\mathrm{ABE}}),\Lambda(\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})\right)^2}:=\sqrt{1-F(\sigma_{\mathrm{ABE}},\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})^2}\geq\tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right|\end{aligned}. \tag{49}$$

This is the necessary condition for Koashi's security proof. After this part, we further investigate the condition to make the trace distance equal to the upper-bound of (49).

By monotonicity of Fidelity under a CPTP map Λ, and such Λ is as follows by the definition of quantum states in (3, 4).

$$\begin{aligned} \Lambda(|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}}) &:= \tau_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}} = \sum\nolimits_{\boldsymbol{k}} 2^{-|K|} |\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k},\boldsymbol{k}|_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}} \\ \therefore \Lambda(|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}}) &= \sum\nolimits_{\boldsymbol{k}} |\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k},\boldsymbol{k}|_{\mathrm{AB}} \left(|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}}\right) |\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k},\boldsymbol{k}|_{\mathrm{AB}} \end{aligned} . \tag{50}$$

Therefore,

$$\begin{aligned} \sqrt{1-F(\zeta_{\mathrm{AB}},|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}})^2} &= \sqrt{1-F(\zeta_{\mathrm{ABE}},|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}})^2} \\ &= \sqrt{1-F(\sigma_{\mathrm{ABE}},\tau_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}})^2} \geq \tfrac{1}{2}\mathrm{tr}\left|\sigma_{\mathrm{ABE}} - \tau_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}}\right| \end{aligned} . \tag{51}$$

Because

$$\begin{aligned} F(\sigma_{\mathrm{ABE}},\tau_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}}) &= \mathrm{tr}\left[\sum\nolimits_{\boldsymbol{k},\boldsymbol{k}'} 2^{-|K|} |\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k}',\boldsymbol{k}'| \otimes \kappa_{\mathrm{E}}{}^{1/2} \langle\boldsymbol{k},\boldsymbol{k}|\sigma_{\mathrm{ABE}}|\boldsymbol{k}',\boldsymbol{k}'\rangle \kappa_{\mathrm{E}}{}^{1/2}\right]^{1/2} \\ &= \mathrm{tr}\left[\sum\nolimits_{\boldsymbol{k},\boldsymbol{k}'} 2^{-|K|} |\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k}',\boldsymbol{k}'| \otimes \kappa_{\mathrm{E}}{}^{1/2} \langle\boldsymbol{k},\boldsymbol{k}|\Lambda(\zeta_{\mathrm{ABE}})|\boldsymbol{k}',\boldsymbol{k}'\rangle \kappa_{\mathrm{E}}{}^{1/2}\right]^{1/2} \\ &= \mathrm{tr}\left[\sum\nolimits_{\boldsymbol{k}} 2^{-|K|} |\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k},\boldsymbol{k}| \otimes \kappa_{\mathrm{E}}{}^{1/2} \langle\boldsymbol{k},\boldsymbol{k}|\zeta_{\mathrm{ABE}}|\boldsymbol{k},\boldsymbol{k}\rangle \kappa_{\mathrm{E}}{}^{1/2}\right]^{1/2} \\ &= \mathrm{tr}\left[\sum\nolimits_{\boldsymbol{k}} \left|\langle\boldsymbol{k},\boldsymbol{k}|\mathrm{MES}\rangle\right|^2 |\boldsymbol{k},\boldsymbol{k}\rangle\langle\boldsymbol{k},\boldsymbol{k}| \otimes \kappa_{\mathrm{E}}{}^{1/2} \langle\boldsymbol{k},\boldsymbol{k}|\zeta_{\mathrm{ABE}}|\boldsymbol{k},\boldsymbol{k}\rangle \kappa_{\mathrm{E}}{}^{1/2}\right]^{1/2} \\ &= F(\zeta_{\mathrm{ABE}},|\mathrm{MES}\rangle\langle\mathrm{MES}|_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}}) \end{aligned} . \tag{52}$$

To satisfy equality in (51), define the purified quantum systems by adding a virtual system R as

$$\begin{aligned} |\sigma\rangle &:= \sum\nolimits_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}}} \Pr_{\sigma}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})^{1/2} |\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{A}}\rangle |\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\rangle |\sigma_{\mathrm{R}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\rangle \\ |\tau\rangle &:= \sum\nolimits_{\boldsymbol{k},\boldsymbol{l}} 2^{-|K|/2} \Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))^{1/2} |\boldsymbol{k},\boldsymbol{k}\rangle |\kappa_{\mathrm{E}}(\boldsymbol{l})\rangle |\kappa_{\mathrm{R}}(\boldsymbol{l})\rangle \end{aligned} . \tag{53}$$

(53) satisfies Uhlmann's inequalities,

$$\begin{aligned} \sqrt{1-F(|\sigma\rangle\langle\sigma|,|\tau\rangle\langle\tau|)^2} &\geq \sqrt{1-F(\sigma_{\mathrm{ABE}},\tau_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}})^2} \\ \tfrac{1}{2}\mathrm{tr}\left|\sigma_{\mathrm{ABE}} - \tau_{\mathrm{AB}} \otimes \kappa_{\mathrm{E}}\right| = \tfrac{1}{2}\mathrm{tr}\left|\mathrm{tr}_{\mathrm{R}}\left(|\sigma\rangle\langle\sigma| - |\tau\rangle\langle\tau|\right)\right| &\leq \tfrac{1}{2}\mathrm{tr}\left\||\sigma\rangle\langle\sigma| - |\tau\rangle\langle\tau|\right\| \end{aligned} . \tag{54}$$

And, for pure quantum states,

$$\begin{aligned} \tfrac{1}{2}\mathrm{tr}\left\||\sigma\rangle\langle\sigma| - |\tau\rangle\langle\tau|\right\| &= \tfrac{1}{2}\mathrm{tr}\,|\sigma\rangle\langle\sigma| \left[1 + |\langle\sigma|\tau\rangle|^2 - |\langle\sigma|\tau\rangle|^2 - |\langle\sigma|\tau\rangle|^2\right]^{1/2} + \tfrac{1}{2}\mathrm{tr}\left|\sigma^{\perp}\right\rangle\left\langle\sigma^{\perp}\right| \left[0 + \left|\langle\sigma^{\perp}|\tau\rangle\right|^2\right]^{1/2} \\ &= \tfrac{1}{2}\left[1 - |\langle\sigma|\tau\rangle|^2\right]^{1/2} + \tfrac{1}{2}\left[1 - |\langle\sigma|\tau\rangle|^2\right]^{1/2} = \left[1 - |\langle\sigma|\tau\rangle|^2\right]^{1/2} \\ &= \sqrt{1-F\left(|\sigma\rangle\langle\sigma|,|\tau\rangle\langle\tau|\right)^2} \end{aligned} . \tag{55}$$

Then, to satisfy the equalities in (54),

$$\begin{aligned}\tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right| &= \tfrac{1}{2}\operatorname{tr}\sum\nolimits_{\boldsymbol{k},\boldsymbol{k}_{\mathrm{E}}}\left|\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}(\boldsymbol{k})\right|\left|\boldsymbol{k},\boldsymbol{k}\right\rangle\left\langle\boldsymbol{k},\boldsymbol{k}\right|\otimes\left|\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right\rangle\left\langle\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right| \\ &= \tfrac{1}{2}\sum\nolimits_{\boldsymbol{k},\boldsymbol{k}_{\mathrm{E}}}\left|\left\langle\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right|\left[2^{-|K|}\kappa_{\mathrm{E}}-\sum\nolimits_{\boldsymbol{k}_{\mathrm{B}}}\Pr(\boldsymbol{k},\boldsymbol{k}_{\mathrm{B}})\sigma_{\mathrm{E}}(\boldsymbol{k},\boldsymbol{k}_{\mathrm{B}})\right]\left|\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right\rangle\right|\end{aligned}. \tag{56}$$

$$\begin{aligned}&\because \tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right| = \tfrac{1}{2}\operatorname{tr}\left|\operatorname{tr}_{\mathrm{R}}\left(\left|\sigma\right\rangle\left\langle\sigma\right|-\left|\tau\right\rangle\left\langle\tau\right|\right)\right| \\ &\therefore \sum\nolimits_{\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{B}}}\Pr_{\sigma}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right\rangle\left\langle\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right| \coloneqq \sum\nolimits_{\boldsymbol{k}_{\mathrm{B}}}\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}). \\ &\therefore \sum\nolimits_{\boldsymbol{l}}2^{-|K|}\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\left|\kappa_{\mathrm{E}}(\boldsymbol{l})\right\rangle\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\right| \coloneqq 2^{-|K|}\kappa_{\mathrm{E}}\end{aligned} \tag{57}$$

$$\begin{aligned}&F(\left|\sigma\right\rangle\left\langle\sigma\right|,\left|\tau\right\rangle\left\langle\tau\right|) \\ &= \sum\nolimits_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}},\boldsymbol{l}}\sqrt{2^{-|K|}\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\Pr_{\sigma}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})}\left|\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l}),\kappa_{\mathrm{R}}(\boldsymbol{l})\right|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}}),\sigma_{\mathrm{R}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right\rangle\right|\end{aligned}. \tag{58}$$

Again, by Cauchy-Schwarz inequality,

$$\begin{aligned}&F(\sigma_{\mathrm{ABE}},\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}) \\ &= \sum\nolimits_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{l}}\left[\sum\nolimits_{\boldsymbol{k}_{\mathrm{B}}}2^{-|K|}\Pr(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\right|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left|\kappa_{\mathrm{E}}(\boldsymbol{l})\right\rangle\right]^{1/2} \\ &= \sum\nolimits_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{l}}\sqrt{\sum\nolimits_{\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}}}\Pr(\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}}\mid\boldsymbol{k}_{\mathrm{A}},\kappa_{\mathrm{E}}(\boldsymbol{l}))}\sqrt{\sum\nolimits_{\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}}}2^{-|K|}\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\Pr_{\sigma}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left|\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\right|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right\rangle\right|^{2}}. \\ &\geq \sum\nolimits_{\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}},\boldsymbol{l}}\sqrt{2^{-|K|}\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\Pr_{\sigma}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\Pr(\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}}\mid\boldsymbol{k}_{\mathrm{A}},\kappa_{\mathrm{E}}(\boldsymbol{l}))}\left|\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\right|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right\rangle\right|\end{aligned} \tag{59}$$

$$\begin{aligned}&\therefore \Pr(\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}}\mid\boldsymbol{k}_{\mathrm{A}},\kappa_{\mathrm{E}}(\boldsymbol{l})) \coloneqq \left|\left\langle\kappa_{\mathrm{R}}(\boldsymbol{l})\right|\sigma_{\mathrm{R}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right\rangle\right|^{2} \\ &= \frac{\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\Pr_{\sigma}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left|\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\right|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right\rangle\right|^{2}}{\sum\nolimits_{\boldsymbol{k}_{\mathrm{B}},\boldsymbol{k}_{\mathrm{E}}}\Pr(\kappa_{\mathrm{E}}(\boldsymbol{l}))\Pr_{\sigma}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\left|\left\langle\kappa_{\mathrm{E}}(\boldsymbol{l})\right|\sigma_{\mathrm{E}}(\boldsymbol{k}_{\mathrm{E}},\boldsymbol{k}_{\mathrm{A}},\boldsymbol{k}_{\mathrm{B}})\right\rangle\right|^{2}}.\end{aligned} \tag{60}$$

Under the conditions derived in (48), (53), and (60),

$$\begin{aligned}\varepsilon_{\mathrm{sec}}^{(\kappa)} &\geq \sqrt{1-F(\zeta_{\mathrm{AB}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}})^{2}} = \sqrt{1-F(\zeta_{\mathrm{ABE}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})^{2}} \\ &= \sqrt{1-F(\sigma_{\mathrm{ABE}},\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}})^{2}} = \tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right|\end{aligned}. \tag{61}$$

Furthermore, choose the POVM for Eve on the given quantum state as $\left\{\left|\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right\rangle\left\langle\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right|\right\}$ with the corresponding condition chosen by Eve with restrictions in (48), (53), and (60)

$$\Pr\left(\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right) = \left\langle\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right|\left\langle\mathrm{MES}\right|\zeta_{\mathrm{ABE}}\left|\mathrm{MES}\right\rangle\left|\lambda_{\boldsymbol{k}_{\mathrm{E}}}^{(\kappa)}\right\rangle F(\zeta_{\mathrm{AB}},\left|\mathrm{MES}\right\rangle\left\langle\mathrm{MES}\right|_{\mathrm{AB}})^{-2}. \tag{62}$$

Then, the expected probability for Eve successfully guessing the correct key is, with the same way in (42),

$$\Pr\left(\boldsymbol{K}\mid\boldsymbol{E}\right) \leq 2^{-|K|}+\tfrac{1}{2}\operatorname{tr}\left|\sigma_{\mathrm{ABE}}-\tau_{\mathrm{AB}}\otimes\kappa_{\mathrm{E}}\right| \leq 2^{-|K|}+\varepsilon_{\mathrm{sec}}^{(\kappa)}. \tag{63}$$

Note, however, that the necessary condition (48) cannot be satisfied by Alice nor Bob, because it contains the unknown quantum state ζ_{ABE}. This state is what only Eve knows. Furthermore, conditions in (48), (53), and (60) are not necessary for Alice and Bob, although Eve wishes to satisfy to maximize her guessing probability. This situation tells us that the definition of τ_E can be chosen by Eve. Further generalization as Case 3 is what the author has been questioning.

4.3 Case 3: letting Eve define the trace distance independently from Alice and Bob

Note that, in the second case Eve could choose the independent quantum state $\tau_E = \kappa_E$ to satisfy the equalities in the inequalities to bound the trace distance. This would give her more advantages. Then, here is a question; what if Eve could choose τ_E freely to maximize the trace distance itself independent from the definition by Alice and Bob? This section seeks the possibility. To do so, Eve attaches an imaginary quantum system R, constructing the total system σ_{ABER}. Then, Eve chooses τ_{ER} so that its support is not on the support of $\mathrm{tr}_{AB}\,\sigma_{ABER}$. Furthermore, Eve could choose quantum systems σ_{ABER} and τ_{ABER}, to purify like (53) showed. To put these purified quantum systems σ_{ABER} and τ_{ABER} on different supports, Eve has to satisfy

$$\begin{aligned} F\left(|\sigma\rangle\langle\sigma|,|\tau\rangle\langle\tau|\right) &= \left|\langle\tau|\sigma\rangle\right| \\ &= \sum_{\boldsymbol{k}_A,\boldsymbol{k}_B,\boldsymbol{k}_E,\boldsymbol{l}} \sqrt{2^{-|K|}\Pr(\kappa_E(\boldsymbol{l}))\Pr_\sigma(\boldsymbol{k}_E,\boldsymbol{k}_A,\boldsymbol{k}_B)}\left|\langle\kappa_E(\boldsymbol{l}),\kappa_R(\boldsymbol{l})|\sigma_E(\boldsymbol{k}_E,\boldsymbol{k}_A,\boldsymbol{k}_B),\sigma_R(\boldsymbol{k}_E,\boldsymbol{k}_A,\boldsymbol{k}_B)\rangle\right| \\ &= 0 \end{aligned} \quad (64)$$

Eve could define as

$$\left|\langle\kappa_E(\boldsymbol{l}),\kappa_R(\boldsymbol{l})|\sigma_E(\boldsymbol{k}_E,\boldsymbol{k}_A,\boldsymbol{k}_B),\sigma_R(\boldsymbol{k}_E,\boldsymbol{k}_A,\boldsymbol{k}_B)\rangle\right| = 0\,. \quad (65)$$

Then, apparently

$$\tfrac{1}{2}\mathrm{tr}\left\|\sigma\rangle\langle\sigma| - |\tau\rangle\langle\tau|\right\| = 1\,. \quad (66)$$

Now Eve can discard the virtual quantum system R, and measure her system E to guess the correct key most likely. This process is described as follows, using Γ in (11).

$$\begin{aligned} \tfrac{1}{2}\mathrm{tr}\left\|\sigma\rangle\langle\sigma| - |\tau\rangle\langle\tau|\right\| = 1 &= \mathrm{tr}_{ABE}\mathrm{tr}_R\,|\sigma\rangle\langle\sigma| = \mathrm{tr}_{ABE}\,\sigma_{ABE} \\ &\geq \mathrm{tr}_{ABE}\left[\Gamma\sigma_{ABE}\right] = \Pr\left(\boldsymbol{K}\,|\,\boldsymbol{E}\right) \end{aligned}\,. \quad (67)$$

Therefore, (67) violates the upper-bound of the trace distance in existing security proofs. More simply, we may consider

$$\begin{aligned} \sigma_{ABER} &\coloneqq \sigma_{ABE}\otimes|0\rangle\langle 0|_R \\ \tau_{ABER} &\coloneqq \tau_{ABE}\otimes\left(I-|0\rangle\langle 0|\right)_R \end{aligned}\,. \quad (68)$$

Note that the conditions in (67) and (68) are totally different from the condition (60). Thus, actually, as long as Eve can choose her own quantum system τ_E independently from the choice Alice and Bob make, the upper-bound for the trace distance cannot be given from the frameworks of standardized trace distance criterions. Shor and Preskill proved the equivalence of entanglement-based QKDs to the prepare-and-measure QKDs such as BB84 using the Fiderity between the maximally entangled state and entangled-based distributed state, however, it seems their security proof cannot be connected to the trace distance criterion, which has been useful to show the security of prepare-and-measure QKDs. The author throw a question as follows. The modified Lo-Chau protocol and the CSS protocol in Shor-Preskill proof would be perfectly secure with a probability of $1-\varepsilon_{sec}^2$, because quantum error corrections, especially phase-error-corrections would decouple Eve's system. However, a classical privacy amplification process would not correct quantum phase errors, even though the complementary analysis approach allows us to estimate the phase-error-rate from the bit-error-rate[42, 43]. Thus, Eve's system would not be decoupled in case of prepare-and-measure QKDs. This would explain why Privacy Amplification is actually harmful for QKDs as explained in Sec. 2.4, by contrast with perceived understanding that classical Privacy Amplification is equivalent to phase-error-corrections since Shor-Preskill proof back in 2000. Furthermore, this may explain why Round Robin DPS QKD protocol does not need to monitor quantum signal disturbances to estimate the

amount of key sacrifice in Privacy Amplification[23]. This may be simply because Privacy Amplification would not be required for prepare-and-measure protocols including the above protocol, as well as the secure key rate derivation based on the phase-error-rate estimation may also be invalid.

4.4 Misconception of "distinguishability advantage" interpretation of trace distance

There is an interpretation that the trace distance is "indistinguishability" of the ideal quantum state and the real quantum state[18]. Such an interpretation is justified by citing quantum binary decision theory by C. W. Helstrom[41]. The following is the overview.

In Helstrom's theory, Alice prepare ρ_0 or ρ_1 with prior probabilities of p_0 and p_1. Bob discriminates the quantum states with an optimum measurement basis. The maximum guessing probability for Bob is

$$P_{\text{guess}} = \tfrac{1}{2} + \tfrac{1}{2}\,\text{tr}\left|p_0\rho_0 - p_1\rho_1\right|. \tag{69}$$

If we assume $p_0 = p_1 = 1/2$, then we see trace distance.

$$P_{\text{guess}} = \tfrac{1}{2} + \tfrac{1}{2}\times\tfrac{1}{2}\,\text{tr}\left|\rho_0 - \rho_1\right|. \tag{70}$$

The interpretation is justified as follows. Alice prepares a QKD system which Eve can interact with, or a QKD system with an interface which gives Eve measurement results as if she is interacting with the former system but actually she cannot interact at all. Alice randomly prepares such systems with a prior probability of 1/2, and Eve judges which system is used from her measurement results. If we regard $\rho_0 = \sigma_{\text{ABE}}$ in (4) and $\rho_1 = \underline{\tau}_{\text{ABE}}$ in (3), then the maximum guessing probability for Eve is given by (70), therefore the trace distance is as advantage for Eve to distinguish the two situations.

The problems with the interpretation are as follows. It is said that Eve's success probability in guessing the correct system is given by (70), however, this would not give any idea how high the probability is for Eve to guess the correct key. Furthermore, it gives the following problems.

Now let us think the original situation of QKD. Firstly, $\underline{\tau}_{\text{ABE}}$ is a desirable quantum state but it cannot be distributed, and σ_{ABE} is the quantum state always distributed. However, in the context of this interpretation, Alice and Bob have to prepare such quantum states with a prior probability of 1/2. Such a situation does not meet the actual situation of QKD. Furthermore, if they could prepare the system with which Eve cannot interact with a probability of 1/2, then we are not sure why they do not use the perfect device every time, while we are sure that the system is always the one which Eve can interact. This means, the prior probability is very contrived. One more thing, in the quantum binary decision theory, Bob receives the whole system of the quantum state, but in the context of QKD, Eve receives only the partial system of the quantum state, such as $\text{tr}_{\text{AB}}\,\sigma_{\text{ABE}}$. Thus, the situation of the quantum binary decision problem is far different from the situation of QKDs.

Therefore, the indistinguishability interpretation cannot be useful to evaluate the security of QKD.

5. RECENT TRENDS OF QUANTUM CRYPTOGRAPHY

Defense Advanced Research Projects Agency (DARPA) in USA announced the requirement to quantum cryptography in 2012 as follows[44].

- Communication speed: 1-10 Gbps
- Communication range: 1,000-10,000 km

These are seriously challenging goals for QKDs.

Meanwhile, National Cyber Security Centre (NCSC), a part of Government Communications Headquarters (GCHQ) in UK uploaded a white paper to suggest not to use QKDs for important communication infrastructures[5].

On the other hand, there are other quantum cryptographies than QKDs. Firstly, Yuen himself proposed a protocol named Keyed Communication in Quantum-noise (KCQ)[45] (which is called Y-00 because Yuen proposed the protocol in 2000 [46], or Quantum Noise Stream Cipher, especially customized one in Tamagawa Univ. is named "Quantum Enigma Cipher"[47]).

S. Lloyd proposed Quantum Enigma Machine[48], J. H. Shapiro proposed a quantum cryptography protocol using quantum illumination technology[49]. These protocols do not use weak signals like single photons, but use macroscopic quantum nature with intensity of current optical communication, therefore they would satisfy DARPA's requirements. Other known quantum encryption protocol is Quantum Homomorphic Encryption[50]. There may be more protocols for practical uses.

Now, limiting the topic on KCQ, it is often misunderstood that it is a technology to encrypt messages directly using the initial key, not a technology to distribute secret keys. However, it is possible like QKDs to distribute secret keys by replacing the message by the secret key to be shared. Furthermore, it has often been proposed to combine QKDs and KCQ to distribute the secret key for KCQ by QKDs. However, it may not be so meaningful for KCQ if the security of QKDs still remain in $\varepsilon_{sec} = 2^{-50}$; because it means the distributed key by QKDs is like 50-bit key expanded into 10^6 bits, while KCQ basically uses 128-bits or 256-bit keys expanded by AES or any other key-expansion processes hiding it under quantum noise to enhance the security. Moreover, KCQ uses lasers with its intensity compatible to the conventional optical communications, while QKDs have limitations in the communication distance because of their weak signals. Furthermore, currently, most vulnerable parts of QKDs are the communication nodes not protected by laws of physics, as NCSC documents also mentions[5]. Moreover, consider the situation that Nation A wants to communicate with Nation B, passing through a communication node set by Nation E less trustworthy. How can we trust the communication channel when the communication node is under control of Nation E? The literature[51] may give some answers to the author's question, though the author is not fully sure yet for general cases. For instance, the literature wrote in its Sec 4.1 as follows.

"Of course, this works only if both sides share measurement results securely. If the eavesdropper can modify or control both the quantum and classical connections between the two parties, she can send false measurement results and fake a Bell inequality violation. To avoid such a man in the middle attack, we assume all classical communications are authenticated and unmodified."

This assumption may not be satisfied when Eve is pre-installed in the repeaters Nation E possesses. If we are going to build the unconditionally secure quantum internet, we have to take such worst cases into our consideration. Otherwise, the quantum internet would have the same problems as the conventional internet has. Recall that QKDs are expected to be secure against ultimately powerful Eve. In the literature[52], the optimum communication rate is derived in terms of the trace distance criterion, however, as the author described, QKDs have been estimating the best performance under the worst scenarios, therefore the next direction of researches of the quantum network should be the derivations of the best performance under the worst scenarios.

It is sure that the QKD researchers those who have pioneered highly secure communication using quantum mechanics are worthy of being honored even if unconditionally secure network based on QKDs would not be realized. Adding to it, the problems in QKD have shown important challenges that what is required for quantum encryption systems. The author of this article is unsure whether unconditionally secure communication is possible based on QKDs or not. However, in practical use, there would be choices of other quantum cryptographies than QKDs. Even in such a case, knowledge obtained in QKD studies will be greatly useful, in the author's opinion. It is also sure that developments of QKDs can be continued, however, we should take Yuen's warnings into consideration seriously.

6. CONCLUSIONS

In this article, the author made detailed explanations what H. P. Yuen has been warning on the security of QKDs since 2009. Furthermore, the article showed an example of the Bit-Error-Rate guarantee in BB84, which was suggested by Yuen for a stronger security criterion than the trace distance criterion currently standardized. According to the Bit-Error-Rate guarantee, it seems Eve may have exponentially larger chance of success in nearly perfect eavesdropping compared to the conventional security criterion, the trace distance. Furthermore, the author threw several questions on the definition of the trace distance criterion, by letting the eavesdropper define the trace distance to maximize her success probability in obtaining the correct key. Even more, it might have given us misunderstanding that prepare-and-measure QKDs are equivalent to entanglement-based QKDs using quantum error corrections, since Shor-Preskill's security proof back in 2000. Therefore, for further security analyses, we may need to abandon the trace distance security criterion.

REFERENCES

[1] Bennett, C. H. and Brassard, G., "Quantum cryptography: public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, **175**(0), (1984).

[2] Bennett, C. H. and Brassard, G., "Quantum cryptography: public key distribution and coin tossing," (rewritten version,) Theoretical Computer Science 560 7-11 (2014).

[3] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V., "Hacking commercial quantum cryptography systems by tailored bright illumination." Nature photonics **4**(10), 686-689 (2010).

[4] Lo, H.-K., Curty, M., and Qi, B., "Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. 108, 130503 (2012).

[5] The British governmental white paper, "Quantum Key Distribution," National Cyber Security Centre, a part of GCHQ in Britain, 4th Oct. (2016). https://www.ncsc.gov.uk/information/quantum-key-distribution

[6] Tamaki, K., Curty, M., and Lucamarini, M., "Decoy-state quantum key distribution with a leaky source," New Journal of Physics, **18**(6), 065008 (2016).

[7] Yuen, H. P., "Two-photon coherent states of the radiation field," Physical Review A, **13**(6), 2226, (1976).

[8] Yuen, H., Kennedy, R., and Lax, M., "Optimum testing of multiple hypotheses in quantum detection theory," IEEE Transactions on Information Theory, **21**(2), 125-134, (1975).

[9] Yuen, H., and Lax, M., "Multiple-parameter quantum estimation and measurement of nonselfadjoint observables. IEEE Transactions on Information Theory," **19**(6), 740-750, (1973).

[10] Yuen, H. P., "Universality and The Criterion 'd' in Quantum Key Generation," arXiv:0907.4694v1, quant-ph (2009).

[11] Yuen, H. P., "Fundamental Quantitative Security In Quantum Key Generation," arXiv:1008.0623v3, quant-ph, (2010), or Physical Review A, **82**(6), 062304, (2010).

[12] Bennett, C. H., Brassard, G., Crépeau, C., and Maurer, U. M., "Generalized privacy amplification," IEEE Transactions on Information Theory, **41**(6), 1915-1923, (1995).

[13] Shor, P. W., and Preskill, J., "Simple proof of security of the BB84 quantum key distribution protocol," Physical review letters, **85**(2), 441, (2000).

[14] König, R., Renner, R., Bariska, A., and Maurer, U., "Small accessible quantum information does not imply security," Physical Review Letters, **98**(14), 140502, (2007).

[15] Renner, R., and König, R., "Universally composable privacy amplification against quantum adversaries," In Theory of Cryptography Conference (pp. 407-425), Springer, Berlin, Heidelberg, (2005, February).

[16] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," Reviews of modern physics, **81**(3), 1301, (2009).

[17] Benatti, F., Fannes, M., Floreanini, R., and Petritis, D. (Eds.), "Quantum information, computation and cryptography: an introductory survey of theory, technology and experiments," (Vol. 808). Springer, (2010).

[18] Portmann, C., and Renner, R., "Cryptographic security of quantum key distribution," arXiv preprint arXiv:1409.3525v1, (2014).

[19] Yuen, H. P., "Security of quantum key distribution," IEEE Access, 4, 724-749, (2016).

[20] Yuen, H., "What The Trace Distance Security Criterion in Quantum Key Distribution Does And Does Not Guarantee," arXiv:1410.6945v1 [quant-ph], (2014).

[21] Nielsen, M., and Chuang, I., "Quantum information and computation. Quantum Information and Computation," Cambridge University Press, (2000).

[22] Takesue, H., Sasaki, T., Tamaki, K. and Koashi, M., "Experimental quantum key distribution without monitoring signal disturbance," Nature Photonics 9, 827–831, (2015).

[23] Sasaki, T., Yamamoto, Y., and Koashi, M., "Practical quantum key distribution protocol without monitoring signal disturbance," Nature, 509(7501), 475-478 (2014).

[24] Curty, M., "Quantum cryptography: Know your enemy," Nature Physics, 10(7), 479. (2014).

[25] Stinson, D. R., "Cryptography: Theory and Practice, Third Edition, Edition 3," CRC Press, (2005).

[26] Ministry of Health, Labour and Welfare Japan, http://www.mhlw.go.jp/toukei/saikin/hw/jinkou/tokusyu/furyo10/01.html

[27] Automobile Inspection and Registration Information Association Japan https://www.airia.or.jp/publish/file/e49tph00000004sb-att/e49tph00000004si.pdf

[28] Iwakoshi, T., "Security of Quantum Key Distribution from Attacker's View," The 33rd Quantum Information Technology Symposium, IEICE QIT2015-16 (2015). https://doi.org/10.13140/RG.2.2.12625.74081

[29] Iwakoshi, T., “Yuen’s Criticisms on Security of Quantum Key Distribution and Onward,” SCIS2017, 2017 Symposium on Cryptography and Information Security, Naha, Japan, 24-27th, Jan. (2017). https://doi.org/10.13140/RG.2.2.18173.77282
[30] Koashi, M., “Simple security proof of quantum key distribution based on complementarity,” New Journal of Physics, **11**(4), 045018, (2009).
[31] Tomamichel, M., Lim, C. C. W., Gisin, N., and Renner, R. “Tight finite-key analysis for quantum cryptography,” Nature communications, 3, 634, (2012).
[32] Iwakoshi, T., "Trade-off between Key Generation Rate and Security of BB84 Quantum Key Distribution," Tamagawa University Quantum ICT Research Institute Bulletin, vol.5, no.1, pp.1-4, (2015), or http://www.tamagawa.jp/research/quantum/bulletin/2015.html https://www.researchgate.net/publication/314363534
[33] Abidin, A., and Larsson, J. Å., “Direct proof of security of Wegman–Carter authentication with partially known key,” Quantum information processing, **13**(10), 2155-2170, (2014).
[34] Ferguson, N., Schneier, B., and Kohno, T., “Cryptography engineering: design principles and practical applications,” John Wiley and Sons. (2011).
[35] Konig, R., Renner, R., and Schaffner, C., “The operational meaning of min-and max-entropy,” IEEE Transactions on Information theory, 55(9), 4337-4347, (2009).
[36] Fuchs, C. A., Gisin, N., Griffiths, R. B., Niu, C. S., and Peres, A., “Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy,” Physical Review A, **56**(2), 1163, (1997).
[37] Brandt, H. E., “Topical Review: Optimum Probe Parameters for Entangling Probe in Quantum Key Distribution,“ Quantum Information Processing, **2**(1), 37-79, (2003).
[38] Brandt, H. E., “Quantum-cryptographic entangling probe,” Physical Review A, **71**(4), 04231, (2005).
[39] Kim, T., genannt Wersborg, I. S., Wong, F. N., and Shapiro, J. H., “Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol,” Physical Review A, **75**(4), 042327, (2007).
[40] Acharyya, A., and Paul, G. “Revisiting optimal eavesdropping in quantum cryptography: Optimal interaction is unique up to rotation of the underlying basis,” Physical Review A, **95**(2), 022326, (2017).
[41] Helstrom, C. W., “Quantum Detection and Estimation Theory,” Journal of Statistical Physics 1.2 231-252 (1969) or Academic press (1976).
[42] Sasaki, T., and Koashi, M., “A security proof of the round-robin differential phase shift quantum key distribution protocol based on the signal disturbance,” Quantum Science and Technology, Vol 2, Number 2, (2017).
[43] Mizutani, A., Sasaki, T., Kato, G., Takeuchi, Y., & Tamaki, K., “Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity,” Quantum Sci. Technol. 3, 014003 (2018), https://doi.org/10.1088/2058-9565/aa8705 or arXiv preprint arXiv:1705.00171. (2017).
[44] "Broad Agency Announcement Quiness: Macroscopic Quantum Communications," DSO DARPA-BAA-12-42, May 15, (2012).
[45] Barbosa, G. A., Corndorf, E., Kumar, P., and Yuen, H. P., “Secure communication using mesoscopic coherent states,” Physical Review Letters, **90**(22), 227901, (2003).
[46] Hirota, O., Kato, K., Sohma, M., Usuda, T. S., and Harasawa, K., “Quantum stream cipher based on optical communications,” Proceedings Volume 5551, Quantum Communications and Quantum Imaging II; (2004); doi: 10.1117/12.561778
[47] Futami, F., and Hirota, O., “100 Gbit/s (10× 10 Gbit/s) Y-00 cipher transmission over 120 km for secure optical fiber communication between data centers,” In Optical Fibre Technology, 2014 OptoElectronics and Communication Conference and Australian Conference on (pp. 4-6). IEEE, (2014, July).
[48] Lloyd, S., "Quantum enigma machines," arXiv preprint arXiv:1307.0380 (2013).
[49] Shapiro, J. H., Zhang, Z., and Wong, F. N., “Secure communication via quantum illumination,” Quantum information processing, **13**(10), 2171-2193, (2014).
[50] Liang, M., “Symmetric quantum fully homomorphic encryption with perfect security,” Quantum information processing, 12(12), 3675-3687. (2013).
[51] Satoh, T., Nagayama, S., and Van Meter, R., “The Network Impact of Hijacking a Quantum Repeater,” arXiv preprint arXiv:1701.04587, (2017).
[52] Azuma, K., Mizutani, A., and Lo, H. K., “Fundamental rate-loss trade-off for the quantum internet,” Nature communications, 7, 13523, (2016).