Quantum Information Processing (2022) 21:142
https://doi.org/10.1007/s11128-022-03487-9

# Estimating security of the quantum key distribution from the guesswork

**Hong-Wei Li[1] · Jian-Hong Shi[1] · Qing-Yu Cai[2] · Chang-Pu Sun[3]**

Received: 17 September 2021 / Accepted: 10 March 2022 / Published online: 4 April 2022


**Abstract**
Quantum key distribution can provide information-theoretic security keys. In practice, the eavesdropper may attack the transmitted quantum state, which makes some information leakage to the generated key. The security of the final key depends on how difficult it is for the eavesdropper to guess the key. The guessing probability is bounded by the trace distance between the practical generated quantum state and the ideal quantum state and hence can be applied to estimate security of quantum key distribution. With the trace distance $\varepsilon$ and the secret key length $n$, we prove that the guessing probability can reach the upper bound $\varepsilon+2^{-n}$ in some special cases. We show that different attacking strategies will give different numbers of guesses, sometimes even completely subversive differences, to get the final key. Our results demonstrate that the appropriate security parameter $\varepsilon$ should be carefully selected to guarantee the security of the generated key.

**Keywords** Quantum key distribution · Security · Guesswork · Trace distance

## 1 Introduction

Quantum key distribution (QKD) [1] is the art of sharing the information-theoretical security key between two distant parties Alice and Bob, while the eavesdropper Eve cannot get the secret key even if she has unlimited computation power [2–4]. From the

✉ Hong-Wei Li
h.w.lee.roy@gmail.com

Qing-Yu Cai
qycai@wipm.ac.cn

1 Henan Key Laboratory of Quantum Information and Cryptography, SSF, IEU, Zhengzhou 450001, Henan, China

2 School of Information and Communication Engineering, Hainan University, Haikou 570228, China

3 Graduate School of Chinese Academy of Engineering Physics, Beijing 100084, China

adversary's point of view, the perfect secret key should have the uniform probability distribution. However, the practically generated key is usually imperfect, which may leak some information to Eve. More precisely, part of the secret key bit information may be leaked to Eve during the quantum state preparation and measurement step or the classical postprocessing step [5–7]. To prove security of a QKD protocol, the trace distance between the practical quantum state and the ideal quantum state has been proposed [4, 8–11]. Based on the trace distance method, a QKD protocol has the security intensity $\varepsilon$ if the generated classical-quantum state $\rho_{AE}$ between Alice and Eve has the following condition

$$D(\rho_{\mathrm{AE}}, \rho_{\mathrm{UE}}) = \tfrac{1}{2}\mathrm{tr}|\rho_{\mathrm{AE}} - \rho_U \otimes \rho_E| \leq \varepsilon, \tag{1}$$

where $\rho_{\mathrm{AE}}$ is the practical classical-quantum state generated between Alice and Eve, $\rho_{\mathrm{UE}} = \rho_U \otimes \rho_E$ is the ideal classical-quantum state shared between Alice and Eve. Under the secret key length $n$, $\rho_U$ is the maximum mixed state $\frac{I}{2^n}$, which can be illustrated by the uniform probability distribution. $\varepsilon$ is the security intensity of the QKD protocol, which can be estimated by combining the privacy amplification security parameter with the min-entropy security parameter [12–14]. For any two quantum states $\rho_{\mathrm{AE}}$ and $\rho_{\mathrm{UE}}$, Eve can apply arbitrary positive operator valued measure (POVM) to get classical measurement outcomes, which have the probability distribution $P_{\mathrm{AE}}$ and $Q_{\mathrm{UE}}$, respectively. Correspondingly, the trace distance between $P_{\mathrm{AE}}$ and $Q_{\mathrm{UE}}$ can be bounded by the trace distance $D(\rho_{\mathrm{AE}}, \rho_{\mathrm{UE}})$ with the following inequality

$$D(P_{AE}, Q_{\mathrm{UE}}) \leq D(\rho_{\mathrm{AE}}, \rho_{\mathrm{UE}}) \leq \varepsilon. \tag{2}$$

From Eve's viewpoint, the perfect quantum state $\rho_{\mathrm{UE}}$ can be illustrated as $\rho_{\mathrm{UE}} = \rho_U \otimes \rho_E$, where the measurement outcome about $\rho_U$ has the uniform probability distribution $P_U$. Correspondingly, the joint probability distribution about Alice and Eve's measurement outcomes can be given by $Q_{\mathrm{UE}} = P_U P_E$, where Eve's measurement outcome $e$ has the probability distribution $P_E(e)$. Note that the two quantum states $\rho_U$ and $\rho_E$ are independent, thus Alice's measurement outcomes have the uniform probability distribution under Eve's arbitrary measurement outcome $e$.

Based on the classical-quantum state $\rho_{\mathrm{AE}}$ and the trace distance $\varepsilon$, Eve can apply appropriate POVM to get the probability distribution $P_{\mathrm{AE}}$. Since all of the quantum states $\rho_{\mathrm{AE}}$ have the restriction $D(\rho_{\mathrm{AE}}, \rho_{\mathrm{UE}}) \leq \varepsilon$ can be utilized by Eve, she can choose different attacking strategies to get the probability distribution $P_{\mathrm{AE}}$. Based on Eve's attacking strategies, the guesswork is defined as the number of guesses required in order to correctly guess the secret key. From Eve's viewpoint, she can guess the secret key with the maximal guessing probability by utilizing the probability distribution $P_{\mathrm{AE}}$. Accordingly, how to analyze the maximal guessing probability is an important question [15] to prove security of a QKD protocol.

Based on the trace distance $\varepsilon$ and the secret key length $n$, it has been proved that the maximal guessing probability of the generated key can be bounded by $p \leq \varepsilon + 2^{-n}$ [10, 11]. However, there are still two important questions about the guessing probability and guesswork to be solved, the first question is if the maximal guessing probability $\varepsilon + 2^{-n}$ is tight in the general case, and the second question is how to understand the

operational meaning of the guesswork [16]. To answer the first question, we propose a special state preparation between Alice and Eve, and the result accurately proves that the upper bound value of the guessing probability can be reached to $\varepsilon + 2^{-n}$. But we should emphasize that the maximal guessing probability $\varepsilon + 2^{-n}$ do not demonstrate that the QKD protocol is not secure, this is because only some special quantum states can reach this upper bound value, but Eve has no explicit attacking strategy to reach this bound generally. To answer the second question, we propose two attacking strategies to analyze the guesswork with different trace distance values $\varepsilon$. In the first attacking strategy, by utilizing the probability distribution $P_{\mathrm{AE}}$, Eve will guess the generated key from the high probability to the low probability, and we prove that this attacking strategy has the guesswork $\frac{2^n+1}{2} - 2^n\varepsilon$. In the second attacking strategy, by utilizing the probability distribution $P_{\mathrm{AE}}$, Eve will only guess the generated key with the maximal guessing probability value, and we prove that this strategy has the guesswork $\log_{1-\varepsilon}(1-q)$ with the success probability at least $q$. Based on the two attacking strategies, we prove the lower bound of the guesswork, which can be applied to estimate the minimum number of guesses required to correctly guess the secret key. Our results demonstrate that the trace distance is an efficient method to estimate security of the QKD protocol, but the appropriate trace distance $\varepsilon$ should be carefully selected to guarantee the guesswork value is large enough in both of the two attacking strategies.

The rest of this paper is arranged as follows: in Sect. 2, we propose the precise quantum state preparation and measurement protocol to reach the guessing probability $p = 2^{-n} + \varepsilon$. In Sect. 3, we analyze the relationship between the average guesswork and the trace distance $\varepsilon$ with the secret key length $n$. In Sect. 4, we propose two detailed attacking strategies to estimate Eve's attacking probability, and the lower bound of the guesswork will be discussed correspondingly.

## 2 The tight bound of the guessing probability

Based on the security definition given by the trace distance method [4, 17], a QKD protocol has the security intensity $\varepsilon$ if the practical generated quantum state $\rho_{\mathrm{Ext}(X,Y)YE'}$ has the following restriction

$$D(\rho_{\mathrm{Ext}(X,Y)YE'}, \rho_{UYE'}) = \tfrac{1}{2}\mathrm{tr}|\rho_{\mathrm{Ext}(X,Y)YE'} - \rho_{UYE'}| \leq \varepsilon, \tag{3}$$

where $\rho_{\mathrm{Ext}(X,Y)YE'}$ is the practical quantum state shared between Alice, Eve and the uniform seed $Y$, and $\rho_{UYE'} = \rho_U \otimes \rho_Y \otimes \rho_{E'}$ is the perfect quantum state. $\rho_Y$ is the uniform seed, which is used for the privacy amplification. In a practical QKD system, the uniform seed $\rho_Y$ will be prepared by Alice or Bob, and it will be transmitted to the other party by utilizing an authenticated classical channel. $\rho_U$ is the maximum mixed state, which can be illustrated by the uniform classical probability distribution, and it demonstrates that Eve has no information about the generated key. Since the random seed $\rho_Y$ is known by Eve, we can simply assume that $\rho_Y$ is part of Eve's system. Correspondingly, the classical-quantum state shared between Alice and Eve can be

rewritten as $\rho_{AE} \equiv \rho_{\mathrm{Ext}(X,Y)YE'}$, where $\rho_A = \mathrm{tr}_{Y,E'}\rho_{\mathrm{Ext}(X,Y)YE'}$ and $\rho_E = \rho_Y \otimes \rho_{E'}$, and we can get the trace distance condition $D(\rho_{AE}, \rho_U \otimes \rho_E) \leq \varepsilon$.

To prove security of the QKD protocol with the trace distance method, the security parameter $\varepsilon$ can be divided into the min-entropy security parameter $\varepsilon_{\min}$ and the privacy amplification security parameter $\varepsilon_{\mathrm{pa}}$. More generally, if Ext: $\{0,1\}^m \times \{0,1\}^d \to \{0,1\}^n$ is a quantum-proof $(k, \varepsilon_{\mathrm{pa}})$ strong extractor, then for any quantum state $\rho_{XE'}$ and any $\varepsilon_{\min} > 0$ with $H_{\min}^{\varepsilon_{\min}}(X|E')_{\rho_{XE'}} \geq k$, the trace distance $D(\rho_{AE}, \rho_U \otimes \rho_E)$ can be restricted by [17]

$$D(\rho_{AE}, \rho_U \otimes \rho_E) \leq \varepsilon \equiv \varepsilon_{\mathrm{pa}} + 2\varepsilon_{\min}. \tag{4}$$

This equation implies that the strong extractor can extract the same number of bits from sources which only satisfy $H_{\min}^{\varepsilon_{\min}}(X|E')_{\rho_{XE'}} \geq k$, but the generated key has a slightly larger error $\varepsilon_{\mathrm{pa}} + 2\varepsilon_{\min}$. Note that both of the two security parameters $\varepsilon_{\mathrm{pa}}$ and $\varepsilon_{\min}$ will affect the secret key rate $R$. By applying the leftover hash lemma [4, 18], the secret key rate can be given by

$$R \geq H_{\min}^{\varepsilon_{\min}}(X|E') - 2\log\frac{1}{\varepsilon_{\mathrm{pa}}}, \tag{5}$$

where $H_{\min}^{\varepsilon_{\min}}(X|E') = \max_{\sigma_{XE'} \in \mathcal{B}^{\varepsilon_{\min}}(\rho_{XE'})} H_{\min}(X|E')$, and $\mathcal{B}^{\varepsilon_{\min}}(\rho_{XE'})$ is the set of sub-normalized states $\sigma_{XE'}$ with $D(\sigma_{XE'}, \rho_{XE'}) \leq \varepsilon_{\min}$. To estimate the min-entropy function $H_{\min}(X|E')$, the guessing probability $p_{\mathrm{guess}}(X|E')$ should be calculated. More generally, by considering Alice and Eve share the classical-quantum state $\rho_{XE'} = \sum_x p_x |x\rangle\langle x| \otimes \rho_{E'}^x$, the guessing probability $p_{\mathrm{guess}}(X|E')$ can be given by

$$p_{\mathrm{guess}}(X|E') = \max_{M_x} \sum_x p_x \mathrm{tr}(M_x \rho_{E'}^x). \tag{6}$$

Based on this guessing probability calculation result, the conditional min-entropy function $H_{\min}(X|E')$ can be directly calculated as $H_{\min}(X|E') = -\log p_{\mathrm{guess}}(X|E')$ . Based on the quantum asymptotic equipartition property, the smooth min-entropy function $H_{\min}^{\varepsilon_{\min}}(X|E')$ can be restricted by [19–21]

$$H_{\min}^{\varepsilon_{\min}}(X|E') \geq H(X|E') - 4\sqrt{n}\log(2\sqrt{2^{H_{\max}(X|E')}} + 1)\sqrt{\log\frac{2}{\varepsilon_{\min}^2}}. \tag{7}$$

where $H_{\max}(X|E')$ is the conditional max-entropy function [4]. More generally, the uncertainty principle [22], entropy accumulation theorem [23] and quantum probability estimation [24] methods also have been proposed to estimate $H_{\min}^{\varepsilon_{\min}}(X|E')$. Thus, the final secret key rate can be given by

$$R \geq H(X|E') - 4\sqrt{n}\log(2\sqrt{2^{H_{\max}(X|E')}} + 1)\sqrt{\log\frac{2}{\varepsilon_{\min}^2}} - 2\log\frac{1}{\varepsilon_{\mathrm{pa}}}. \tag{8}$$

Note that Eve can also gain information from the error correction step, and this information can be analyzed by applying the chain rule of the min-entropy function. To calculate this secret key rate, the security parameters $\varepsilon_{\mathrm{pa}}$ and $\varepsilon_{\min}$ should

be previously defined, and the corresponding trace distance can be restricted by $D(\rho_{AE}, \rho_U \otimes \rho_E) \leq \varepsilon$.

After the privacy amplification step, Alice and Eve can generate the quantum state $\rho_{AE} = \sum_k p_k |k\rangle\langle k| \otimes \rho_E^k$. From Eve's viewpoint, she can get the trace distance $D(\rho_{AE}, \rho_U \otimes \rho_E) \leq \varepsilon$, thus the maximal guessing probability $p_{\text{guess}}(A|E) = \max_{M_k} \sum_k p_k \text{tr}(M_k \rho_E^k)$ can be applied to estimate security of a QKD protocol. If Alice and Eve share the ideal quantum state $\rho_U \otimes \rho_E$, the maximal guessing probability is $p_{\text{guess}}(A|E) = 2^{-n}$, where $n$ is the length of the secret key. However, a practical QKD system may leak some information in the classical post-processing step, and the maximal guessing probability should be larger than $2^{-n}$. Thus it will be interesting to discuss the relationship between the trace distance $\varepsilon$ and the maximal guessing probability $p_{\text{guess}}(A|E)$. Recently, it has been proved that the upper bound of the maximal guessing probability $p_{\text{guess}}(A|E)$ can be estimated by the following inequality [10, 11]

$$p_{\text{guess}}(A|E) \leq \varepsilon + 2^{-n}, \tag{9}$$

where the perfect state preparation means that $\varepsilon = 0$, and the maximal guessing probability will be reduced to $2^{-n}$. But, it is not clear if this maximal guessing probability is tight in the general case. In the following subsection, we propose a detailed example to demonstrate that the maximal guessing probability can be reached to $\varepsilon + 2^{-n}$ under the trace distance $\varepsilon$ and the secret key length $n$. More precisely, the detailed density matrix $\rho_{XE'}$ shared between Alice and Eve can be given by

$$\begin{aligned}\rho_{XE'} = &\tfrac{1-p}{N} I_N \otimes |N\rangle\langle N| + \tfrac{p}{N}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| \\ &+ \cdots + |N-1\rangle\langle N-1| \otimes |N-1\rangle\langle N-1|),\end{aligned} \tag{10}$$

where $N = 2^n$, and the density matrix $\rho_{E'}$ can be given by

$$\rho_{E'} = \text{tr}_X \rho_{XE'} = (1-p)|N\rangle\langle N| + \tfrac{p}{N}(|0\rangle\langle 0| + \cdots + |N-1\rangle\langle N-1|). \tag{11}$$

Correspondingly, the ideal quantum state preparation $\rho_U \otimes \rho_{E'}$ can be given by

$$\rho_U \otimes \rho_{E'} = \frac{1}{N} I_N \otimes \rho_{E'} = \frac{1-p}{N} I_N \otimes |N\rangle\langle N| + \frac{p}{N^2} I_N \otimes I_N, \tag{12}$$

where the ideal quantum state demonstrates that Eve has no information about the final secret key, thus she can only randomly guess the generated key with the guessing probability $\frac{1}{N}$. Based on this state of preparation, the trace distance between $\rho_{XE'}$ and $\rho_U \otimes \rho_{E'}$ can be calculated with the following equation

$$D(\rho_{XE'}, \rho_U \otimes \rho_{E'}) = \frac{1}{2}\text{tr}|\rho_{XE'} - \rho_U \otimes \rho_{E'}| = \frac{(N-1)p}{N} \equiv \varepsilon. \tag{13}$$

By considering all of the quantum states in the state space $\mathcal{B}^{\varepsilon_{\min}}(\rho_{XE'})$ with $\varepsilon_{\min} = \varepsilon$, the smooth min-entropy function $H_{\min}^{\varepsilon}(X|E')$ can be calculated as $H_{\min}^{\varepsilon}(X|E') = n$. By applying the left over hash lemma, Alice and Bob do not need to apply the

privacy amplification protocol with this state preparation, thus we can get $\varepsilon_{\text{pa}} = 0$. Correspondingly, the quantum states $\rho_{AE}$ and $\rho_E$ can be, respectively, given by $\rho_{AE} = \rho_{XE'}$ and $\rho_E = \rho_{E'}$. Thus, it can easily proves that the trace distance between $\rho_{AE}$ and $\rho_U \otimes \rho_E$ is

$$D(\rho_{AE}, \rho_U \otimes \rho_E) = \varepsilon. \tag{14}$$

Based on this quantum state $\rho_{AE}$ preparation, Eve can apply the projective measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|, \cdots, |N\rangle\langle N|\}$ to get the measurement outcomes. If she can get the measurement outcomes $\{|0\rangle\langle 0|, |1\rangle\langle 1|, \cdots, |N-1\rangle\langle N-1|\}$, Eve will gain the generated key with probability 1. However, if she gets the measurement outcome $\{|N\rangle\langle N|\}$, Eve can only randomly guess the generated key with probability $\frac{1}{N}$. Finally, the total guessing probability can be given by

$$p_{\text{guess}}(A|E) = p + \tfrac{1-p}{N} = \tfrac{1}{N} + \varepsilon. \tag{15}$$

Since the trace distance between $\rho_{AE}$ and $\rho_U \otimes \rho_E$ is $\varepsilon$, this result exactly demonstrates that the maximal guessing probability can be reached to $\varepsilon + 2^{-n}$. Note that this imperfect quantum state $\rho_{AE}$ can be realized if the practical QKD devices have some imperfections, such as Eve can apply the probabilistic blinding attack [25] with the attacking probability $p$.

We should stress that this result does not demonstrate that QKD is not secure. In a practical QKD system, only some special quantum states in the space $\mathcal{B}^{\varepsilon}(\rho_{AE})$ can reach the maximal guessing probability $\varepsilon + 2^{-n}$. However, how to find a unitary operation to realize the corresponding quantum states should be studied further. Thus, the trace distance is also an efficient method to estimate security of the QKD protocol, but the trace distance $\varepsilon$ should be carefully selected to satisfy different practical applications.

## 3 Estimating security of QKD from the guesswork

In probability theory, we can assume that two different secret key variables $X$ and $X'$ have the probability distributions $P_X$ and $P_{X'}$, respectively, and the trace distance $D(P_X, P_{X'})$ between $P_X$ and $P_{X'}$ can be given by

$$D(P_X, P_{X'}) = \tfrac{1}{2} \sum_{x \in X} |P_X(x) - P_{X'}(x)|. \tag{16}$$

From Eve's point of view, the generated key $U$ has the perfect security if it has the uniform probability distribution $P_U(x) = \frac{1}{N}$. However, practically generated key $X$ has $\varepsilon$-perfect security if the trace distance $D(P_X, P_U)$ can be restricted by $D(P_X, P_U) \leq \varepsilon$. If $X$ has the perfect security, we can get $P_X(x) = \frac{1}{N}$, and the corresponding trace distance can be given by $\varepsilon = 0$. By considering the generated key bit string $X = x_0 x_1 \cdots x_{n-2} x_{n-1}$ has the probability distribution $P_X$, we can rearrange the probability distribution $P_X$ from the high probability to the low probability. Without loss of generality, we assume that the detailed probability distribution

$P_X(x_0x_1\cdots x_{n-2}x_{n-1})$ can be given by

$$\begin{aligned} &p(x_0x_1\cdots x_{n-2}x_{n-1}=00\cdots00)\\ &\geq p(x_0x_1\cdots x_{n-2}x_{n-1}=00\cdots01)\\ &\geq\cdots\\ &\geq p(x_0x_1\cdots x_{n-2}x_{n-1}=11\cdots11). \end{aligned} \tag{17}$$

Based on this probability distribution, Eve can guess the secret key from the high probability to the low probability sequently, and the required guesswork $W(X)$ to correctly guess the generated key can be given by [26]

$$\begin{aligned} W(X)=\ &p(x_0x_1\cdots x_{n-2}x_{n-1}=00\cdots00)\\ &+2p(x_0x_1\cdots x_{n-2}x_{n-1}=00\cdots01)\\ &+\cdots\\ &+Np(x_0x_1\cdots x_{n-2}x_{n-1}=11\cdots11), \end{aligned} \tag{18}$$

where the guesswork $W(X)$ is the average number of guesses needed in order to correctly guess the secret key. Based on this guesswork method, we firstly analyze the guesswork with some special examples.

In the first example, the perfect key $U=u_0u_1\cdots u_{n-2}u_{n-1}$ has the uniform probability distribution as the following

$$\begin{aligned} &p(u_0u_1\cdots u_{n-2}u_{n-1}=00\cdots00)=\tfrac{1}{N}\\ &p(u_0u_1\cdots u_{n-2}u_{n-1}=00\cdots01)=\tfrac{1}{N}\\ &\cdots\\ &p(u_0u_1\cdots u_{n-2}u_{n-1}=11\cdots11)=\tfrac{1}{N}. \end{aligned} \tag{19}$$

Based on this probability distribution, the trace distance can be given by $\varepsilon=0$, and the corresponding guesswork of $U$ is

$$W(U)=\tfrac{1}{N}(1+2+\cdots+N)=\tfrac{N+1}{2}. \tag{20}$$

In the second example, all of the key bit strings $Y=y_0y_1\cdots y_{n-2}y_{n-1}$ are known by Eve, which has the following probability distribution

$$\begin{aligned} &p(y_0y_1\cdots y_{n-2}y_{n-1}=00\cdots00)=1\\ &p(y_0y_1\cdots y_{n-2}y_{n-1}=00\cdots01)=0\\ &\cdots\\ &p(y_0y_1\cdots y_{n-2}y_{n-1}=11\cdots11)=0. \end{aligned} \tag{21}$$

Based on this probability distribution, the trace distance can be given by $\varepsilon=1-\frac{1}{N}$, and the corresponding guesswork of $Y$ is 1.

In the third example, only the first bit $z_0$ of the key bit string $Z = z_0 z_1 \cdots z_{n-2} z_{n-1}$ is known by Eve, which has the following probability distribution

$$\begin{aligned} &p(z_0 z_1 \cdots z_{n-2} z_{n-1} = 00 \cdots 00) = \tfrac{2}{N} \\ &\cdots \\ &p(z_0 z_1 \cdots z_{n-2} z_{n-1} = 01 \cdots 11) = \tfrac{2}{N} \\ &p(z_0 z_1 \cdots z_{n-2} z_{n-1} = 10 \cdots 00) = 0 \\ &\cdots \\ &p(z_0 z_1 \cdots z_{n-2} z_{n-1} = 11 \cdots 11) = 0. \end{aligned} \tag{22}$$

Based on this probability distribution, the trace distance can be given by $\varepsilon = \frac{1}{2}$, and the corresponding guesswork of $Z$ is $\frac{N+2}{4}$.

In the general case, we can only bound the trace distance $D(P_X, P_U) \leq \varepsilon$, but the precise probability distribution $P_X(x_0 x_1 \cdots x_{n-2} x_{n-1})$ can't be observed, thus the guesswork of $W(X)$ can't be directly calculated. Fortunately, in the classical cryptography theory, it has been proved that the guesswork of $W(X)$ can be restricted by [27]

$$W(X) \geq \tfrac{N+1}{2} - N\varepsilon. \tag{23}$$

In the special case with $\varepsilon = 0$, the guesswork of $X$ can be given by $W(X) = \frac{N+1}{2}$. However, the guesswork of $X$ is restricted by $W(X) \geq \frac{1}{2}$ when $\varepsilon = \frac{1}{2}$. Obviously, by considering the lower bound value of $W(X)$, the security of $X$ can't be guaranteed when $\varepsilon = \frac{1}{2}$.

By comparing with the classical cryptography theory, Eve has the auxiliary quantum system in the QKD protocol. Thus, she can apply arbitrary POVM to get the classical measurement outcomes. By applying different POVMs with the quantum state $\rho_{AE}$, Alice and Eve can get different classical probability distributions $P_{AE}$. But the trace distance between $P_{AE}$ and $Q_{UE}$ can be efficiently restricted by $D(P_{AE}, Q_{UE}) \leq D(\rho_{AE}, \rho_U \otimes \rho_E) \leq \varepsilon$. More generally, for any two quantum states $\rho_{AE}$ and $\rho_{UE}$, Alice and Eve can apply arbitrary POVM $\{\Gamma_{xe} = |x\rangle\langle x| \otimes M_e, \sum_{xe} \Gamma_{xe} = 1\}_{xe}$ to get the probability distribution $P_{AE}$ and $Q_{UE}$. Since Eve has the same marginal probability distribution $P_E(e)$ in both of the two quantum states $\rho_{AE}$ and $\rho_{UE}$, the trace distance $D(P_{AE}, Q_{UE})$ can be restricted by

$$\begin{aligned} D(P_{AE}, Q_{UE}) &= \tfrac{1}{2} \sum_{e \in E} \sum_{x \in X} |P_{AE}(xe) - P_U P_E(e)| \\ &= \tfrac{1}{2} \sum_{e \in E} \sum_{x \in X} |P_A(x|e) P_E(e) - P_U P_E(e)| \\ &= \tfrac{1}{2} \sum_{e \in E} P_E(e) \sum_{x \in X} |P_A(x|e) - P_U| \\ &= \sum_{e \in E} P_E(e) \varepsilon_e \\ &\leq \varepsilon, \end{aligned} \tag{24}$$

where $\varepsilon_e$ is the trace distance between $P_{AE}(xe)$ and $P_U P_E(e)$ when Eve gets the measurement outcome $e$. From Eve's point of view, the trace distance $\varepsilon$ can be bounded by different trace distance values $\varepsilon_e$ with the corresponding probability $P_E(e)$. Note

that the trace distance $\varepsilon_e$ may be larger than $\varepsilon$, but the corresponding probability value $P_E(e)$ should be strictly restricted by $P_E(e) \leq \frac{\varepsilon}{\varepsilon_e}$ . We give two special cases to analyze the relationship between $\varepsilon$ and $\varepsilon_e$, the first case is considering $\varepsilon_e = \varepsilon$ for the arbitrary measurement outcome $e \in E$, where Eve can get the same guesswork with different measurement outcomes. The second case is considering there is a special measurement outcome $e'$ has the trace distance $\varepsilon_{e'} = 1-2^{-n} \approx 1$, thus the upper bound value of $P_E(e')$ is $\frac{\varepsilon}{1-2^{-n}} \approx \varepsilon$. This case demonstrates that Eve may get all of the key bit string when the measurement outcome $e'$ is detected, but the corresponding probability value $P_E(e')$ should be very small. On the other side, Eve can only randomly guess the generated key when the other measurement outcomes are detected.

In the general case, by considering the measurement result $e$ obtained by Eve, she can guess the generated key from the high probability to the low probability sequently, and the corresponding guesswork $W(X|e)$ can be estimated. However, Eve should also consider the probability $P_E(e)$ to estimate the average guesswork $W(X) = \sum_{e\in E} P_E(e)W(X|e)$. To analyze the average guesswork, we consider all of the measurement outcomes in Eve's side. Considering the measurement result $e$ obtained by Eve, the corresponding guesswork can be restricted by

$$W(X|e) \geq \tfrac{N+1}{2} - N\varepsilon_e. \tag{25}$$

Note that the trace distance $\varepsilon$ can be restricted by $\sum_{e\in E} P_E(e)\varepsilon_e \leq \varepsilon$, the average guesswork $W(X)$ can be given by

$$\begin{aligned} W(X) &= \sum_{e\in E} P_E(e)W(X|e) \\ &\geq \sum_{e\in E} P_E(e)(\tfrac{N+1}{2} - N\varepsilon_e) \\ &= \tfrac{N+1}{2} - N\sum_{e\in E} P_E(e)\varepsilon_e \\ &\geq \tfrac{N+1}{2} - N\varepsilon. \end{aligned} \tag{26}$$

This inequality implies that the lower bound of the average guesswork $W(X)$ is $\frac{N+1}{2} - N\varepsilon$. Guesswork $W(X)$ is approximate to $\frac{N+1}{2}$ when $\varepsilon$ is small enough, and it will be more difficult for Eve to guess the key.

## 4 Discussion

The previous results have many applications in estimating security of the QKD protocol, which demonstrates that Eve's guesswork will be similar to the perfect case $\frac{N+1}{2}$ when $\varepsilon$ is small enough. However, this guesswork maybe not a good method to estimate Eve's attacking strategy when $\varepsilon$ is not small enough. For example, the average guesswork is $W(X) \geq \frac{N+1}{2} - 10^{-4}N$ when $\varepsilon = 10^{-4}$, but this security intensity is not enough for some practical applications. From Eve's viewpoint, she may only guess the key bit string with the special measurement outcome $e_\triangle$, which has the

trace distance $\varepsilon_{e_\triangle} = 1 - \frac{1}{N}$. However, the maximum probability of this happening is $P_E(e_\triangle) \leq \frac{10^{-4}}{1-\frac{1}{N}} \approx 10^{-4}$, and this probability maybe too large for some practical applications.

Combining the trace distance with the auxiliary quantum system, Eve can get the probability distribution of the generated key, thus she can guess the key bit string with some attacking strategies. By considering the trace distance $\varepsilon$, two different attacking strategies are proposed in this work. In the first attacking strategy, Eve will guess the security key bit string from the high probability to the low probability sequently, and the required guesswork can be given by $\frac{N+1}{2} - \frac{N}{2}\varepsilon$. In the second attacking strategy, Eve will measure the auxiliary quantum system to observe if she can get the special measurement outcome $e_\triangle$ with the trace distance $\varepsilon_{e_\triangle} = 1 - \frac{1}{N}$. By applying the inequality $\sum_{e\in E} P_E(e)\varepsilon_e \leq \varepsilon$, the corresponding maximal probability to get the full key bit string can be bounded by $P_E(e_\triangle) \leq \frac{\varepsilon}{1-\frac{1}{N}} \approx \varepsilon$. By comparing with the first attacking strategy, the second attacking strategy has the advantage if $\varepsilon$ is small, but the second attacking strategy requires the keys generated in each round of QKD have the same probability distribution. More interestingly, if Eve wants to get only one secret key bit from the generated keys, the trace distance can be given by $\varepsilon_{e_\Lambda} = \frac{1}{2}$, and the corresponding maximal probability can be given by $P_E(e_\Lambda) \leq 2\varepsilon$. In the second attacking strategy, if Eve wants to successfully guess the full key bit string with the probability at least $q$, the required guesswork $g$ has the following condition

$$1 - (1-\varepsilon)^g \geq q. \tag{27}$$

By calculating this inequality, we can bound the required guesswork is $g \geq \log_{1-\varepsilon}(1-q)$, where $q \geq \varepsilon$.

To explain the two attacking strategies more clearly, we consider an example to analyze the two different attacking strategies with the trace distance $10^{-4}$. By applying this trace distance value and the secret key length $n$, the guesswork in the first attacking strategy can be given by $\frac{2^n+1}{2} - 10^{-4} \times 2^n \approx 2^{n-1}$. However, in the second attacking strategy, the guesswork can be given by $g \geq \log_{1-10^{-4}}(1-0.99) \approx 4.6 \times 10^4$ with the success probability 99%. If each round of QKD process takes 1 second, the required time resource in the second strategy is about 0.53 day. Obviously, the trace distance $10^{-4}$ is too large compared with the perfect case, and the generated key cannot be directly applied in some practical applications. Note that this result requires the keys generated in each round of QKD have the same probability distribution, but Eve has no explicit strategy to meet this condition in the ideal QKD protocol. In the worst case, even if Eve can get the same probability distribution, she can only get one round of the key in this situation, and the other rounds of the key generated by the QKD system are also secure.

## 5 Relation with previous works

After the work has been finished, an anonymous reviewer introduce the work [28] to us, where the guesswork is used as the security criterion to analyze the imperfect

key. Note that we get the similar result by considering the average guesswork in the first attacking strategy, but two different attacking strategies have been, respectively, analyzed in our work, and our analysis method is different.

## 6 Conclusion

The trace distance between the practical quantum state and the ideal quantum state can be applied to estimate security of the QKD protocol. From Eve's viewpoint, she can get a probability distribution by applying an arbitrary POVM to measure the auxiliary quantum system, and the guesswork can be utilized to estimate security of keys generated by the QKD protocol. We analyze the relationship between the trace distance and the guesswork by considering two attacking strategies. We also prove that the upper bound value of the guessing probability can be achieved with the given trace distance value, and the result demonstrates that the guesswork can be utilized to estimate security of the practical QKD system. More generally, we prove that if we have a bound on the trace distance method, then we can get bounds on the guesswork method with different attacking strategies. We should emphasize that our results demonstrate that the trace distance is an efficient method to prove security of the practical QKD system, but the appropriate trace distance should be carefully selected to guarantee the security of the generated keys.

**Acknowledgements** The author would like to thank Yan-Bao Zhang, Christopher Portmann, Marcin Pawlowski, Rong Wang and Zhen-Qiang Yin for their helpful discussions. This work is supported by the National Natural Science Foundation of China (Grant No. U2130205), the National Key Research and Development Program of China (Grant No. 2020YFA0309702) and the Natural Science Foundation of Henan (Grant No. 202300410532).

**Data Availability** The data that support the findings of this study are available from the corresponding authors on request.

## References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: roceedings of IEEE international conference on computers, systems and signal processing, Bangalore, India. New York: IEEE, 175–179 (1984)
2. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**, 2050 (1999)
3. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441 (2000)
4. Renner, R.: Security of quantum key distribution. Int. J. Quantum Inf. **6**(01), 1–127 (2008)
5. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., et al.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**(3), 1301 (2009)
6. Li, H.W., Wang, S., Huang, J.Z., et al.: Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. Phys. Rev. A **84**(6), 062308 (2011)
7. Li, H.W., Xu, Z.M., Cai, Q.Y.: Small imperfect randomness restricts security of quantum key distribution. Phys. Rev. A **98**, 062325 (2018)
8. Kraus, B., Gisin, N., Renner, R.: Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. Phys. Rev. Lett. **95**, 080501 (2005)

9. Renner, R., Gisin, N., Kraus, B.: Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A **72**, 012332 (2005)
10. Portmann, C., Renner, R.: Cryptographic security of quantum key distribution. Preprint at: arxiv.org/abs/1409.3525 (2014)
11. Portmann, C., Renner, R.: Security in quantum cryptography. Preprint at: arxiv.org/abs/2102.00021 (2021)
12. Tomamichel, M., Schaffner, C., Smith, A., et al.: Leftover hashing against quantum side information. IEEE Trans. Inf. Theory **57**, 5524 (2011)
13. Holenstein, T., Renner, R.: On the randomness of independent experiments. IEEE Trans. Inf. Theory **57**, 1865 (2011)
14. Tomamichel, M., Colbeck, R., Renner, R.: A fully quantum asymptotic equipartition property. IEEE Trans. Inf. Theory **55**, 5840 (2009)
15. Wang, X.B., Wang, J.T., Qin, J.Q., et al.: Guessing probability in quantum key distribution. NPJ Quantum Inf. **6**, 45 (2020)
16. Yuen, H.P.: Security of quantum key distribution. IEEE Access **4**, 724 (2016)
17. De, A., Portmann, C., Vidick, T., et al.: Trevisan's extractor in the presence of quantum side information. SIAM J. Comput. **41**, 915 (2009)
18. Radhakrishnan, J., Ta-Shma, A.: Bounds for dispersers, extractors, and depth-two superconcentrators. SIAM J. Discret. Math. **13**(1), 2–24 (2000)
19. Konig, R., Renner, R., Schaffner, C.: The operational meaning of min and max-entropy. IEEE Trans. Inf. Theory **55**, 4337 (2009)
20. Arnon-Friedman, R.: Reductions to IID in device-independent quantum information processing. PhD thesis, arXiv:1812.10922, (2018)
21. Tomamichel, M.: A framework for non-asymptotic quantum information theory. PhD thesis, arXiv:1203.2142, (2012)
22. Tomamichel, M., Lim, C., Gisin, N., et al.: Tight finite-key analysis for quantum cryptography. Nat. Commun. **3**, 634 (2012)
23. Dupuis, F., Fawzi, O., Renner, R.: Entropy accumulation. Commun. Math. Phys. **379**, 867–913 (2020)
24. Zhang, Y., Knill, E., Bierhorst, P.: Certifying quantum randomness by probability estimation. Phys. Rev. A **98**(4), 040304 (2018)
25. Qian, Y.J., Li, H.W., He, D.Y., et al.: Countermeasure against probabilistic blinding attack in practical quantum key distribution systems. Chin. Phys. B **24**, 090305 (2015)
26. Massey, J.L.: Guessing and entropy. In: proceedings of the IEEE international symposium on information theory. 204 (1994)
27. Pliam, J.: The disparity between work and entropy in cryptology. Cryptology ePrint Archive, Report 1998/024, (1998)
28. Hanson, E.P., Katariya, V., Datta, N., et al.: Guesswork with quantum side information. arXiv:2001.03598, (2020)