Quantification of guessing probability in quantum key distribution protocols

Hong-Yi Su\textsuperscript{1,2, *}

\textsuperscript{1}College of Physics and Optoelectronic Engineering, Harbin Engineering University, Harbin 150001, People’s Republic of China
\textsuperscript{2}Graduate School of China Academy of Engineering Physics, Beijing 100193, People’s Republic of China

(Dated: May 25, 2022)

Given communication systems using quantum key distribution, the receiver can be seen as one who tries to guess the sender’s information just as eavesdroppers do. The receiver-eavesdropper similarity thus implies a simple relation in terms of guessing probability, establishing a close connection with the distance-based, information-theoretic security. The tolerable regions of error rates, determined by such a guessing-probability-based relation, are shown to be close to those determined by the entropic criteria. Thus, the role of guessing probability taken in the security proof is here advanced.

Examples of two specific protocols are illustrated. Our results contribute to evaluating an important element in communication theory, and may provide useful reference for the security analysis of quantum key distribution protocols.

I. INTRODUCTION

Guessing probability [1, 2], which is often requested by researchers alongside customers of classical cryptosystems, serves to estimate the eavesdropper’s probability of correctly guessing the key transmitted from the sender to the receiver. It has drawn particular attention [3–5] as quantum key distribution (QKD) is being implemented in recent decades. While its quantification is an important element in communication systems, it has been proved insufficient when applied in the security analysis of QKD. For instance, researchers have proved in [5] that the guessing probability, regarding the final key, is a much weaker indicator of security than the distance-based entropic criterion. They use the finite-length analysis and show that after privacy amplification with the Toeplitz matrix, the guessing probability can be made small, to such a degree, that it is in sharp disagreement with the fairly acceptable key rate implied from the entropic criterion.

That security of communication systems can be certified by using entropic criteria is attributed to Shannon, whose introduction of entropy into the communication studies led to the seminal formulation of information theory, by which an information-theoretic proof of security was for the first time attained for symmetric cryptography [6]. In modern parlance, the security proof is motivated by a similarity between the receiver (Bob) who receives signals from the sender (Alice), and the eavesdropper (Eve) who may intercept and resend the signals transmitting in between. Hence a theoretical secrecy index—i.e., the equivocation—can be estimated by means of the conditional entropy \( H(A|E) \), with \( A \) representing the original message and \( E \) the intercepted message. Much of the similarity between Bob and Eve is maintained in quantum cryptography [7, 8]. For instance, the quantum secure key rate is computed by a properly optimized difference between \( S(A|E) \) and \( S(A|B) \) [9–11], where \( S(x|y) \) denotes the quantum conditional von Neumann entropy resembling its classical counterpart. Nevertheless, quantum theory imposes a tradeoff on Bob and Eve, rendering Eve’s intercepts detectable (see [12–16] and references therein). It is noted that Eve, who presumably has an arbitrarily high-dimensional quantum memory, may be able to perform compatible measurements to discriminate Alice’s outcomes under incompatible measurements [17].

The above entropic security criterion can actually be reduced from the finite-length, distance-based criterion, i.e., the \( \varepsilon \)-security, as an asymptotic case. In general, the overall security level, \( \varepsilon \), can be divided into two parts, the correctness \( \varepsilon_{\text{cor}} \) and the secrecy \( \varepsilon_{\text{sec}} \), subject to \( \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}} \leq \varepsilon \). Here, following the notations in [18], the \( \varepsilon_{\text{cor}} \) bounds the probability that Alice and Bob fail to share identical keys of a certain length, namely, \( P(A \neq B) \leq \varepsilon_{\text{cor}} \), and the \( \varepsilon_{\text{sec}} \) bounds the trace-norm distance between a real Alice-Eve correlation and an ideal one, namely, \( \frac{1}{2} \min_{E} \| [\rho_{AE} - \tau_{A} \otimes \sigma_{E}] ] | 1 \leq \varepsilon_{\text{sec}}/(1 - \rho_{\text{abort}}) \), where \( \rho_{\text{abort}} \) denotes the probability that the protocol is aborted, \( \rho_{AE} \) is the quantum state representing the Alice-Eve correlation, \( \tau_{A} \) denotes the fully mixed state, and \( \sigma_{E} \) is an arbitrary state of Eve.

The correctness and secrecy are both essential requirements for a protocol to be secure, but \( \varepsilon_{\text{cor}} \) alone, while maybe very close to \( \varepsilon \), does not imply security. Nevertheless, focusing on \( \varepsilon_{\text{cor}} \) yields a merit that it has potential to connect the Alice-Bob correlation with the guessing probability, i.e., with the Alice-Eve correlation. One can then see Bob and Eve from a similar perspective, since both can be seen to try to guess keys from Alice. As such, a guessing-probability-based relation can be established, giving rather similar predictions as by the entropic security criterion.

Before presenting the formulation of guessing probability, we would like here to compare the guessing-probability-based relation (to be described below) with the entropic security criterion.

On the one hand, since \( \varepsilon_{\text{cor}} \) is no greater than \( \varepsilon \) in the

* hongyisu@gmail.com
II. QUANTIFYING GUESSING PROBABILITY

In this section, we will first present a rigorous definition of the maximum guessing probability and apply it to three generic QKD protocols. Then, we will explicitly derive a general key-rate formula in the information-theoretic manner. As examples, we will consider two well-known protocols and compute the maximum guessing probabilities. The determinations of the critical error rates by the guessing-probability-based relations and by the entropic criteria will be compared and discussed.

A. Definition of the maximum guessing probability

To begin with, it is convenient to consider the entanglement-based scenario [21]. The general state shared by Alice and Bob reads $\rho_{AB} = RR^T$, where $R = U \sqrt{\Lambda} V^T$, and $U$ and $V$ are $d^2 \times d^2$ matrices, $U$ denotes the unitary transform that diagonalizes $\rho_{AB}$, $\Lambda$ is a $d \times d$ matrix, with $\Lambda_k$ representing the eigenvalues of $\rho_{AB}$, and $V$ is an arbitrary $td \times td$ unitary representation of the $SU(td)$ group. The entries of $R$ can be used as coefficients of any purification of $\rho_{AB}$, namely, $|\psi\rangle_{ABE} = \sum_{ij} R_{ij} |i\rangle_{AB} |j\rangle_E$, with $|i\rangle_{AB} \in \mathcal{H}(d^2)$ and $|j\rangle_E \in \mathcal{H}(td)$ [22]. Because of the Schmidt decomposition, we define $\sum_i U |i\rangle_{AB} := |k_U\rangle_{AB}$ and $\sum_j (V^T)_{kj} |j\rangle_E := |k_V\rangle_E$, and the purification state immediately becomes $|\psi\rangle_{ABE} = \sum_k \Lambda_k |k_U\rangle_{AB} |k_V\rangle_E$, with $k = 0, 1, \cdots, \min\{d^2 - 1, td - 1\}$. Here, the basis $\{|i\rangle_{AB}\}$ can be chosen in such a way that $|k_U\rangle_{AB} = |\phi_k\rangle_{AB}$, where $|\phi_k\rangle_{AB}$ are the bases for the diagonalized $\rho_{AB} = \sum_k \Lambda_k |\phi_k\rangle_{AB}$, and the basis $|j\rangle_E$ can be chosen as the computational basis such that $|k_V\rangle_E = (V^T)^T |k\rangle_E$. The guessing probability, depending clearly on Eve’s strategy $V$, then equals

$$P_E = \text{tr}\left[ \left( \sum_{i=0}^{d-1} \sum_{a_i=0}^{d-1} |a_i\rangle_{AB} \otimes |e\rangle_E \langle e\rangle_E |\psi\rangle_{ABE} \langle \psi|_{ABE} \right) \right],$$

subject to $e = a_i + i \times d$.

One who studies security issues must take into account the worst circumstances. The quantity that indeed makes sense in evaluating Eve’s guesses must be the maximum QKD.

The justification is as follows. For a certain bit of Alice, it could be that Bob’s guess is incorrect (i.e., an error appears) but Eve’s guess is correct. This is not the worst case for key generation, however. For fixed $P_B$ and $P_E^\star$, the worst case is that for any of Alice’s bits, if Bob’s guess is incorrect, then Eve’s guess is incorrect, too. Eve can thus make the most of her correct guesses, as it is Bob’s correct guesses that are used to generate identical keys with Alice subsequently.
guessing probability,

\[ P_E^* = \max_V P_E, \]

where the optimization is accomplished by running all \( V \in SU(d) \), along with nonnegative \( \Lambda_i \)'s subject to observables of Alice and Bob.

Here, we remark on the V which corresponds to Eve’s strategy to guess Alice’s measurement results. For each \( \rho_{AB} \) shared by Alice and Bob, Eve can be presumed to hold a purification such that the complete state is described by the purification state \( |\psi\rangle_{ABE} \). The purification is not unique, and \( V \) is the unitary transformation that links these purification states which reduce to the same \( \rho_{AB} \). The importance of numerating all possible \( V \) can then be seen in an example with the BB84 protocol presented in Sec. II C, particularly the discussion around Eqs. (13) through (16).

1. Some symmetric properties

A symmetry exists in the correlations of measurements in typical QKD protocols in which qubits (i.e., \( d = 2 \)) are used and Alice and Bob share the Bell-diagonal state \([23, 24]\), namely, \(|\psi_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \), \(|\phi_1\rangle = (|00\rangle - |11\rangle)/\sqrt{2} \), \(|\phi_2\rangle = (|01\rangle + |10\rangle)/\sqrt{2} \), and \(|\phi_3\rangle = (|01\rangle - |10\rangle)/\sqrt{2} \). To see it, let us first take \( U = e^{-i\phi} \) for Alice, with \( \sigma_x = \sigma_y \cos \varphi - \sigma_z \sin \varphi \). The unitary is to transform a projector along the \( \hat{n} \) direction to one along an arbitrary \( \hat{n}' \) direction. It is simple to verify that \( U(\sigma_x)U^\dagger = \hat{n} \cdot \hat{\sigma} \), and that \( U|0\rangle = |+\rangle, U|1\rangle = -e^{i\varphi} |+\rangle - |\rangle \), where \(|\pm \rangle \) are a set of orthogonal normalized states along \( \hat{n} \), which by parametrization read \(|+\rangle := |\theta, \varphi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\varphi} |1\rangle \) and \(|-\rangle := |\theta, -\varphi\rangle = \sin \frac{\theta}{2} |0\rangle - \cos \frac{\theta}{2} e^{i\varphi} |1\rangle \).

Likewise, for Bob, a set of orthogonal normalized states along \( \hat{n}' \) can be written as \(|\pm\rangle := |\theta, -\varphi\rangle \) and \(|-\rangle := |\theta, \varphi\rangle \). Then, for the correlations

\[ P_{\pm n, \pm n'} = \text{tr} \left[ |\pm \rangle \langle \pm | \otimes |\pm \rangle \langle \pm | \right], \]

the following relations hold:

\[ P_{+n, +n'} = P_{-n, -n'}, \quad P_{+n, -n'} = P_{-n, +n'}. \]

Because Alice (Bob) has \( t \) directions to measure along, with probability \( \varphi_i \) for choosing each and subject to \( \sum_{i=0}^{t-1} \varphi_i = 1 \), the \( P_{\pm n, \pm n'} \) when computed from the data pool have to be rescaled by multiplying \( \varphi_i \). We thus for each \( i \) have specifically

\[ P_{+n, +n'} = P_{-n, -n'} = \frac{\varphi_i}{2} \times \Delta_i, \]

\[ P_{+n, -n'} = P_{-n, +n'} = \frac{\varphi_i}{2} \times (1 - \Delta_i), \]

with \( \Delta_i = \Lambda_0 + \Lambda_1 \cos^2 \theta_i + \Lambda_2 \sin^2 \theta_i \cos^2 \varphi_i + \Lambda_3 \sin^2 \theta_i \sin^2 \varphi_i \). The reason we choose \( \hat{n} \) and \( \hat{n}' \) in demonstrating the symmetry is that it is \(|\phi_0\rangle \) that we take as the maximally entangled state in the ideal quantum channel. Clearly, if we take any of other Bell states as the maximally entangled state in the ideal quantum channel, a corresponding \( \hat{n}' \) direction may be found and used for Bob to demonstrate with Alice the symmetry of \( P_{\pm n, \pm n'} \).

2. Typical types of QKD protocols

The \( \Lambda_i \)'s are not all independent of one another, since they are connected with observables, i.e., the error rates, which are known to Alice and Bob. For each \( i \), due to (4) and

\[ \varepsilon_i := \left[ P_{+n_i, -n'_i} + P_{-n_i, +n'_i} \right] / \sum_{m_i, m'_i} P_{m_i, m'_i}, \]

the sum being over \( m_i = \pm n_i \) and \( m'_i = \pm n'_i \), we find \( \varepsilon_i = 1 - \Delta_i \). Without loss of generality, let us hereafter take \( \varepsilon_0 := \varepsilon_\varphi = \Lambda_2 + \Lambda_3 \), i.e., \( \theta_0 = \varphi_0 = 0 \). Then we can list three generic protocols:

**Protocol I:** A four-state protocol with \( t = 2 \) measuring directions \( \hat{n}_0, \hat{n}_1 \). There are two error rates relating to the \( \Lambda_i \)'s, so only one parameter in \( \rho_{AB} \), say \( \Lambda_3 \), is free. That is, \( \Lambda_0 = 1 - (\cos^2 \varphi_0 - \cos^2 \varphi_1) \varepsilon_0 - (1/\sin^2 \varphi_1) \varepsilon_1 + \Lambda_1 \cos 2 \varphi_1, \Lambda_1 = 1 - \varepsilon_0 - \varphi_0, \) and \( \Lambda_2 = \varepsilon_0 - \Lambda_3 \). Hence, the \( P_{E_0}^* \) with respect to \( \varepsilon_{0,1} \) can be computed by numerating \( V \in SU(4) \) and \( \Lambda_3 \), subject to \( 0 \leq \Lambda_1 \leq 1 \) for any \( i \).

**Protocol II:** A six-state protocol with \( t = 3 \) measuring directions \( \hat{n}_{0,1,2} \). Three error rates are related to the \( \Lambda_i \)'s, so all of them are fixed. The \( P_{E_k}^* \) with respect to \( \varepsilon_{0,1,2} \) can be computed by numerating \( V \in SU(6) \).

**Protocol III:** A 2t-state protocol with \( t > 3 \) measuring directions \( \hat{n}_{0,1,...,t-1} \). The first three error rates are connected with \( \Lambda_i \)'s, and the remaining error rates are determined by the first three as

\[ \varepsilon_k = (1 + \delta_1 - \delta_2) \varepsilon_0 - \delta_1 \varepsilon_1 + \delta_2 \varepsilon_2, \]

for \( 3 \leq k < t \), with

\[ \delta_1 = \frac{\sin^2 \theta_2 \sin(\varphi_2 - \varphi_k) \sin(\varphi_2 + \varphi_k)}{\sin^2 \theta_1 \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2)} \]

\[ \delta_2 = \frac{\sin^2 \theta_2 \sin(\varphi_1 - \varphi_k) \sin(\varphi_1 + \varphi_k)}{\sin^2 \theta_1 \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2)}. \]

The \( P_{E_k}^* \) with respect to \( \varepsilon_{0,1,...,t-1} \) can be computed by numerating \( V \in SU(2t) \).

B. Derivation of a general secure key rate

We consider the information-theoretic security of QKD, for which the secure key rate is computed by
The Shannon entropy, $H(\psi_i) = -\sum \psi_i \log \psi_i$, represents the information of the choices of bases, and it is irrelevant for the key generation. Hence the mutual information we actually use is one with this quantity deducted; namely,
\[ I_{AB} = I_{AB} - H(\psi_i). \tag{9} \]

Let us next consider the eavesdropping in which Eve holds states $\rho_{E|\pm,n_i}$ conditional on Alice’s measurements with probability $\psi_i$ for each $i$. The Holevo quantity for our purpose here reads $\chi_{AE} = S(\rho_{AB}) - \sum_i \psi_i S(\rho_{E|m_i})$, where $\rho_{E|m_i}$ with $m_i = \pm n_i$ denotes the probability that Alice measures her projector $|\pm n_i\rangle\langle\pm n_i|$, and we have taken the identity $S(\rho_{E}) = S(\rho_{AB})$ as $|\psi\rangle_{ABE}$ is pure. The conditional states $\rho_{E|\pm,n_i}$ are of rank two, and have eigenvalues $\lambda_{\pm,n_i} = \lambda_{\pm,n_i} = [1 \pm \sqrt{\xi_i + \eta_i}] / 2$, where $\xi_i = (\mu_+ - \nu_+)^2 \cos^2 \theta_i$ and $\eta_i = (\mu_+^2 + \nu_+^2 + 2 \mu_- \nu_+ \cos 2 \varphi_i) \sin^2 \theta_i$, with $\mu_+ = \lambda_0 \pm \lambda_1$ and $\nu_+ = \lambda_2 \pm \lambda_3$. (These eigenvalues were computed in the $\tilde{\xi}\tilde{\zeta}$-plane in [28]; see also [22].) It is straightforward to have $S(\rho_{AB}) = H(\Lambda_i)$. The Holevo quantity is computed then
\[ \chi_{AE} = H(\Lambda_i) + \sum_{i,m,q} \psi_i \rho_{pm} \lambda_{m_i}^q \log_2 \lambda_{m_i}^q, \tag{10} \]
with the sum over $q = \pm$, $m_i = \pm n_i$, and $i = 0, ..., t - 1$. Given the symmetry of the Bell-diagonal state, it holds that $\rho_{+n_i} = \rho_{-n_i} = 1/2$ for any $n_i$.

It is remarked that for the $t = 2$ protocols, the relations between $\epsilon_i$’s and $\lambda_i$’s serve as constraints in optimizing; and for the $t \geq 3$ protocols, there is no need to optimize with $\Lambda_i$’s but the $\epsilon_i$’s must satisfy the relations in Protocol III. Obviously, under proper circumstances the general criterion reduces to some established formulas, like $R = 1 - 2h(\epsilon_2)$ and $1 - h(3\epsilon_2) - (3\epsilon_2) \log_2 3$, which have already been obtained in [25, 29] for the original BB84 and six-state protocols, respectively.

### C. Examples of guessing probability

#### 1. The BB84 protocol

The protocol belongs to the four-state protocol (i.e., Protocol I) with $\theta_0 = \varphi_0 = 0$, $\theta_1 = \pi/2$, $\varphi_1 = 0$, and $\varphi_0 = \varphi_1 = 1/2$. Let us present an optimal quantum state $\Lambda_0 = (1 + \kappa)/2$, $\Lambda_1 = \Lambda_2 = (1 - \kappa)/4$, and $\Lambda_3 = 0$, along with an optimal unitary transform $V \in SU(4)$ such that
\[
\begin{aligned}
|0\rangle_E &= \frac{1}{2} |0\rangle_E - \frac{1}{2} |1\rangle_E + \frac{1}{2} |2\rangle_E - \frac{1}{2} |3\rangle_E, \\
|1\rangle_E &= \frac{1}{\sqrt{2}} |0\rangle_E + \frac{1}{\sqrt{2}} |1\rangle_E, \\
|2\rangle_E &= \frac{1}{\sqrt{2}} |2\rangle_E + \frac{1}{\sqrt{2}} |3\rangle_E, \\
|3\rangle_E &= \frac{1}{2} |0\rangle_E - \frac{1}{2} |1\rangle_E - \frac{1}{2} |2\rangle_E + \frac{1}{2} |3\rangle_E, 
\end{aligned}
\tag{11}
\]
where $|j\rangle_E$ takes the computational basis as previously stated. The error rates equal to $\varepsilon_0 = \varepsilon_1 = (1 - \kappa)/4 := \varepsilon \in [0, 1/4]$ and the purification $|\psi\rangle_{ABE} = \sum_\kappa \sqrt{\Lambda_\kappa} |\phi_\kappa\rangle_{AB} |k\rangle_E$ are henceforth obtained. The maximum guessing probability then equals
\[
P_E = \sum_{j=0}^3 \text{tr}\left[ \left( |+n_j\rangle \langle +n_j| \otimes |2j\rangle \langle 2j|_E + |-n_j\rangle \langle -n_j| \otimes |2j\rangle \langle 2j|_E \right) |\psi\rangle\langle \psi|_{ABE} \right] 
= \frac{1}{2} + \sqrt{\frac{\Lambda_0}{2}} (\sqrt{\Lambda_1} + \sqrt{\Lambda_2}) 
= \frac{1}{2} + 2\varepsilon (1 - 2\varepsilon). \tag{12}
\]
It equals unity for $\varepsilon \in [1/4, 1/2]$. We plot the $P_E$-versus-$P_E$ figure (see Fig. 1(a)) for arbitrary Bell-diagonal states, confirming the maximum of (12).

Let us come to see in detail how $V$ relates to Eve’s strategy. (Of course, Eve’s strategy also involves the choices of $\Lambda_i$’s; namely, it is possible to take other $\Lambda_i$’s to write a different $\rho_{AB}$ that yield a same $\varepsilon$, but here we take it for simplicity and only focus on $V$.) If Eve uses an strategy that $V = \mathbb{1}$, we have $|k\rangle_E = |k\rangle_E$, and
\[
|\psi\rangle_{ABE} = \sqrt{1 - 2\varepsilon} |\phi_0\rangle_{AB} |0\rangle_E + \sqrt{\varepsilon} |\phi_1\rangle_{AB} |1\rangle_E + \\
\sqrt{1 - 2\varepsilon} |\phi_2\rangle_{AB} |2\rangle_E. \tag{13}
\]
It is obvious to see that Eve cannot discern Alice’s qubits by her projective measurements $|k\rangle\langle k|_E$, because for each component in (13) with respect to $k$, Alice’s state is fully random. Accordingly, we find
\[
P_E = \text{tr} \left[ |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_E + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_E + \\
|+\rangle\langle +|_A \otimes |2\rangle\langle 2|_E + |-\rangle\langle -|_A \otimes |3\rangle\langle 3|_E \rho_{ABE} \right] = 1/2.
\tag{14}
\]
which is smaller than (12). Hence, $V = \mathbb{1}$ is not an optimal strategy for Eve. By “optimal strategy,” we mean that the $V$, for instance the one that induces (11), can enable Eve to guess Alice’s measurement results with the largest probability, under her projective measurements $|k\rangle_E$. In other words, Eve must try to find an optimal $V$ so that with a purification $|\psi\rangle_{ABE} = \sum_{k=0}^{3} \sqrt{\Lambda_k} |\phi_k\rangle_{AB}|k\rangle_E$ she can obtain the maximum of $P_B$, i.e., the $P_B^*$, under the projection $\sum_{k} |n_k\rangle_A \otimes |k\rangle_E$, with $|n_0\rangle_A = |0\rangle_A$, $|n_1\rangle_A = |1\rangle_A$, $|n_2\rangle_A = |+\rangle_A$, and $|n_3\rangle_A = |-\rangle_A$.

In the ideal case with $\varepsilon = 0$, Eve does not have any optimal strategy $V$ because the purification state now reads

$$|\psi\rangle_{ABE} = |\phi_0\rangle_{AB}|0\rangle_E,$$

from which we always get $P_B^* = 1/2$. In the worst case with $\varepsilon = 1/4$ and letting Eve choose the optimal strategy (11), the purification state reads

$$|\psi\rangle_{ABE} = \frac{1}{\sqrt{2}} |\phi_0\rangle_{AB}|0\rangle_E + \frac{1}{\sqrt{2}} |\phi_1\rangle_{AB}|1\rangle_E \nonumber \nonumber$$

$$\quad + \frac{1}{2} |\phi_2\rangle_{AB}|2\rangle_E \nonumber \nonumber$$

$$= \frac{1}{2} \left[ |00\rangle_{AB} |0\rangle_E - |11\rangle_{AB} |1\rangle_E \right] + \frac{1}{2} \left[ |22\rangle_{AB} |2\rangle_E - |33\rangle_{AB} |3\rangle_E \right],$$

(16)

from which we find $P_B^* = 1$, as it should be.

Let $P_B > P_E^*$, and we find $\varepsilon < 10\% := \varepsilon_{cr}$. The bound is close to that determined by the entropic criterion, in the sense that the same error rate yields $R = 1 - 2h(\varepsilon_{cr}) \approx 0.062$. Note that the information of the basis is $\log_2 2 = 1$ bit, which has been deducted from the $R$ here. Meanwhile, let $R = 0$ then we find $\varepsilon_{cr} \approx 11\%$, yielding $P_B \approx 89\%$, which is slightly less than $P_E^* \approx 91\%$.

A more general comparison is presented in Table I. It is noted that the critical value of the error rate for $R = 0$ varies with the measuring directions. The critical value implied from $P_B = P_E^*$ varies with the directions, too. These variations with respect to $\phi$ are due to that it is $|\phi_0\rangle$ that we take as the maximally entangled state in the ideal case. For each $\phi_1$, if we take $|\phi'_0\rangle = e^{i\psi_1}\sigma_z \otimes e^{i\psi_2}\sigma_z |\phi_0\rangle$ as the maximally entangled state in the ideal case, i.e., the coordinate is rotated along the $\tilde{z}$ axis such that the $\tilde{z}$ direction becomes a new $\tilde{x}$ axis, then there will be no variations, and the critical value from $P_B = P_E^*$ will always be slightly smaller than that from $R = 0$, just as the $\phi_1 = 0$ case, which is in agreement with the hierarchy between $\varepsilon_{cor}$ and $\varepsilon$.

2. The six-state protocol

The protocol belongs to Protocol II with $\theta_0 = \varphi_0 = 0$, $\theta_1 = \pi/2$, $\varphi_1 = 0$, $\theta_2 = \varphi_2 = \pi/2$, and $\varphi_0 = \varphi_1 = \varphi_2 = 1/3$. Likewise, we present an optimal quantum state $\Lambda_0 = (1 + \kappa)/2$ and $\Lambda_1 = \Lambda_2 = \Lambda_3 = (1 - \kappa)/6$, along with an optimal unitary transform $V \in SU(6)$ such that

$$|0\rangle_E = \frac{1}{\sqrt{6}} |0\rangle_E - \frac{1}{\sqrt{6}} |1\rangle_E + \frac{1}{\sqrt{6}} |2\rangle_E + \frac{1}{\sqrt{6}} |3\rangle_E$$

$$+ \frac{i}{\sqrt{6}} |4\rangle_E + \frac{1}{\sqrt{6}} |5\rangle_E,$$

$$|1\rangle_E = \frac{1}{\sqrt{2}} |0\rangle_E + \frac{1}{\sqrt{2}} |1\rangle_E,$$

$$|2\rangle_E = \frac{1}{\sqrt{2}} |2\rangle_E - \frac{i}{\sqrt{2}} |3\rangle_E,$$

$$|3\rangle_E = \frac{1}{\sqrt{2}} |4\rangle_E + \frac{i}{\sqrt{2}} |5\rangle_E,$$

$$|4\rangle_E = \frac{1}{2} |0\rangle_E - \frac{1}{2} |1\rangle_E - \frac{1}{2} |2\rangle_E - \frac{1}{2} |3\rangle_E,$$

$$|5\rangle_E = - \frac{1}{2\sqrt{3}} |0\rangle_E + \frac{1}{2\sqrt{3}} |1\rangle_E - \frac{1}{2\sqrt{3}} |2\rangle_E$$

$$- \frac{1}{2\sqrt{3}} |3\rangle_E + \frac{i}{\sqrt{3}} |4\rangle_E + \frac{1}{\sqrt{3}} |5\rangle_E,$$

where $|j\rangle_E$ takes the computational basis as above. The last two vectors, $|4\rangle_E$ and $|5\rangle_E$, are irrelevant in computing $P_E^*$, as the Schmidt rank of $\rho_{AB}$ is four, despite that all $|k\rangle_E$’s here must be six-dimensional. The error rates equal to $\varepsilon_0 = \varepsilon_1 = \varepsilon_2 = (1 - \kappa)/3 := \varepsilon \in [0, 1/3]$, and the purification $|\psi\rangle_{ABE} = \sum_{k=0}^{3} \sqrt{\Lambda_k} |\phi_k\rangle_{AB}|k\rangle_E$.
It equals unity for $\varepsilon \in [1/3, 1/2]$. We, again, plot the $P_B$-versus-$P_E$ figure (see Fig. 1(b)) for arbitrary Bell-diagonal states, confirming the maximum of (18). It can be seen that (18) is lower than (12), since more observables impose more limits on Eve’s guessing capability.

Similar to the BB84 protocol, let $P_B > P_E^*$ then we find $\varepsilon < (5 - 2\sqrt{3})/13 \approx 11.8\% := \varepsilon_{cr}^*$. The bound is still slightly smaller than that in the entropic criterion, since the same error rate yields $R = 1 - h(3\varepsilon_{cr}^*/2) - (3\varepsilon_{cr}^*/2) \log_2 3 \approx 0.045$. Note again that the information of the basis are $\log_2 3 \approx 1.58$ bits, which have been deducted from $R$. Also, let $R = 0$ then we find $\varepsilon_{cr}^* \approx 12.6\%$, yielding $P_B \approx 87.4\%$, which is slightly less than $P_E^* \approx 89\%$.

### III. SUMMARY AND DISCUSSION

We have presented a general analysis of quantifying the guessing probability in QKD protocols. In particular, we have computed the maximum guessing probability and the entropy-based key rate in typical QKD protocols. Proposing a simple guessing-probability-based relation, we have compared the relation with the entropic criterion by illustrating their varied determinations on the critical error rates. This relation, which corresponds to the correctness $\varepsilon_{cor}$, has been shown to be able to impose stricter requirements than the entropic criterion, which corresponds to the overall security level $\varepsilon$, upon the key rates. Given that $\varepsilon_{cor} + \varepsilon_{sec} \leq \varepsilon$, the results are in agreement with the hierarchy within the $\varepsilon$ security. Overall, we have studied the role of guessing probability in the information-theoretic security, and our results may be useful to the QKD implementation.

In ending the paper, we would like to make a few remarks on the terminology. By far, there have also been results on evaluating the guessing probability with the Bell inequality [30]. In Ref. [31–33], for instance, researchers discuss security issues with a monogamous relation of nonlocal correlations, and there the guessing probability, or success probability, is defined in a probabilistic form of the Bell-Clauser-Horne-Shimony-Holt inequality [34]. The $P_B > P_E$ relation defined therein cannot imply $R > 0$. In Ref. [35], the device-independent QKD [8, 36–38] is investigated with various Bell inequalities. Regarding Eve’s guessing probability, their definition is similar to ours (see Eq. (18) in [35]) but bounded in terms of Bell violations. It seems further efforts are still needed on studying more efficient guessing-probability-based relations for device-independent QKD.

### ACKNOWLEDGMENTS

The study is supported by the National Natural Science Foundation of China and the NSAF.

---

**TABLE I.** The critical values of error rates $\varepsilon_{cr}$ and $\tilde{\varepsilon}_{cr}$ around which $P_B \approx P_E^*$ and $R \approx 0$, respectively, for the four-state protocol with measurements along the $n_0 = \hat{z}$ axis and an arbitrary direction $n_1$ in the $\hat{x}\hat{y}$-plane. The parameters and variables are taken as $\theta_0 = \varphi_0 = 0$, $\theta_1 = \pi/2$, $\varphi_0 = \varphi_1 = 1/2$, $\varepsilon_0 = \varepsilon_1$, $\tilde{\varepsilon}_0 = \tilde{\varepsilon}_1$, $\varepsilon = \sum_n \psi_n \varepsilon_n$, $\tilde{\varepsilon} = \sum_n \psi_n \tilde{\varepsilon}_n$, and $\delta \varepsilon := \varepsilon_{cr} - \tilde{\varepsilon}_{cr}$.

| $\varphi_1$ | 0 | $\pi/8$ | $\pi/4$ | $3\pi/8$ | $\pi/2$ |
|------------|---|--------|--------|--------|--------|
| $\varepsilon_{cr}$ (%) | 10.00 | 11.06 | 14.64 | 11.06 | 10.00 |
| $\tilde{\varepsilon}_{cr}$ (%) | 11.00 | 11.61 | 12.62 | 11.61 | 11.00 |
| $\delta \varepsilon$ (%) | -1.00 | -0.55 | +2.02 | -0.55 | -1.00 |
| $P_E^*$ | 0.9000 | 0.8894 | 0.8536 | 0.8894 | 0.9000 |

---

[1] M. Alimomeni and R. Safavi-Naini, in International Conference on Information Theoretic Security, (Springer, 2012) pp. 1-13.
[2] I. Issa and A. B. Wagner, Measuring secrecy by the probability of a successful guess, IEEE Trans. Inf. Theory 63, 3783 (2017).
[3] R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory 55, 4337-4347 (2009).
[4] H. P. Yuen, Security of quantum key distribution, IEEE Access 4, 724 (2016).
[5] X.-B. Wang, J.-T. Wang, J.-Q. Qin, C. Jiang, and Z.-W. Yu, Guessing probability in quantum key distribution, npj Quantum Information 6, 45 (2020).
[6] C. E. Shannon, Communication theory of secrecy systems, The Bell System Technical Journal 28, 656-715 (1949).
[7] C. H. Bennett and G. Brassard, in Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984 (IEEE, New York, 1984), pp. 175-179.
[8] A. K. Ekert, Quantum cryptography based on Bell’s theorem, Phys. Rev. Lett. 67, 661 (1991).
[9] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in Theory of Cryptography Conference, (Springer, 2005), pp. 386-406.
