Quantum Guessing Probability and Quantum Key Distribution

Hong-Yi Su$^{1,2}$,

$^1$College of Physics and Optoelectronic Engineering, Harbin Engineering University, Harbin 150001, People’s Republic of China
$^2$Graduate School of China Academy of Engineering Physics, Beijing 100193, People’s Republic of China

(Dated: December 23, 2021)

We quantify the guessing probability in quantum key distribution protocols. Given a communication system, the receiver can be seen as one who tries to guess the sender’s information just as the eavesdropper does. The receiver-eavesdropper similarity thus implies a simple relation of guessing probability by which to determine tolerable regions of the error rate in the presence of interception and resending. We also derive a general entropy-based formula for secure key rates. It is shown that the guessing-probability-based relation can impose tighter limits on eavesdropping; namely, that the threshold value of the error rate can be less than—while close to—that determined by the entropic criterion. Examples of two specific protocols are illustrated. Our results contribute to presenting an efficient and simple approach to evaluate eavesdropping in quantum key distribution, along with new insights into the entropic criterion established for security.

Shannon’s 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 [1]. In modern parlance, the 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 [2, 3]. For instance, the quantum secure key rate is computed by a properly optimized difference between $S(A|E)$ and $S(A|B)$ [4–6], 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 [7–11] 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 [12].

The guessing probability [13, 14], which is often requested by researchers alongside customers of classical cryptosystems, serves to estimate Eve’s probability of her correct guesses of the key sent from Alice to Bob. Quantum guessing probability, termed so because we consider cryptosystems governed by quantum theory, draws particular attention recently [15–17] as quantum key distribution (QKD) is being implemented. Here, we are concerned to study the sifted key—i.e., the key after the sifting phase and before the classical postprocesses such as information reconciliation and privacy amplification. We consider QKD protocols against collective attacks [18, 19] so that it suffices to study a single run of preparation and measurement with the quantum state of Alice and Bob. Let $\mathcal{H}_A(d)$, $\mathcal{H}_B(d)$ and $\mathcal{H}_E(td)$ be the Hilbert spaces of Alice, Bob and Eve, respectively. Alice has $t$ sets of $d$-dimensional bases in which to measure, hence the dimension $td$ of Eve. The guessing probability then reads

$$P_E = \sum_{i=0}^{t-1} P(e = a_i + i \times d), \quad a_i \text{ and } e \text{ being the outcomes of Alice and Eve.}$$

In the light of Shannon’s idea on the similarity between Bob and Eve, we present an equally significant quantity $P_B = \sum_{i=0}^{t-1} \varphi_i P(a_i = b_i)$, with $b_i$’s similarly denoting the outcomes of events of Bob, $\varphi_i$ the probability that Alice chooses the $i$-th basis to perform measurements, and $\sum_i \varphi_i = 1$. Bob and Eve both aim to guess Alice’s key in transmission.

To quantifying the maximum of $P_E$, denoted $P_E^\ast$ hereafter, is difficult and highly nontrivial, as it requires to numerate all possible configurations of Eve as well as all parameters in Alice and Bob’s quantum state subject to certain observables (see below for the definition). The general setup is that through a noisy quantum channel Alice prepares and sends out a sequence of qubits, which are then received and measured by Bob, and which may also be intercepted by Eve and resent to Bob. After measurements and the sifting phase, Bob gets a sequence of bits, along with a $P_B$ by comparing some of the bits in public with Alice, and Eve gets a result of Alice’s bits, along with a $P_E^\ast$ by listening to the publicized bases in the sifting phase and optimizing her configurations. The Bob-versus-Eve scenario allows us to propose the relation $P_B > P_E^\ast$ as an index that delivers nontrivial indications of the error rates in 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 $P_E^\ast$, 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.

Quantum guessing probability.—To begin with, it...
is convenient to consider the entanglement-based scenario [20]. The general state shared by Alice and Bob reads $\rho_{AB} = R R^d$, where $R = U \sqrt{A} V^d$, $R$ and $U$ are $d^2 \times d^2$ matrices, $U$ denotes the unitary transform that diagonalizes $\rho_{AB}$, $A$ is a $d^2 \times td$ matrix with $A_i$ 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, $|\psi\rangle_{AB} = \sum_{i,j} R_{ij} |i_A AB \rangle |j_E \rangle$, with $|i_A \rangle \in H(d^2)$ and $|j_E \rangle \in H(td)$ [21]. Because of the Schmidt decomposition, we define $\sum_{i} U_{ik} |i_A \rangle = |k_U \rangle_{AB}$ and $\sum_{i} (V^\dagger)_k |j_E \rangle = |k_E \rangle$, and the purification state immediately becomes $|\psi\rangle_{AB} = \sum_k \sqrt{\lambda_k} |k_U \rangle_{AB} |k_E \rangle$, with $k = 0, 1, \cdots, \min\{d^2-1, td-1\}$. Here, the basis $\{|i_A \rangle\}$ 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 $\rho_{AB} = \sum_{k} \Lambda_k |\phi_k \rangle_{AB} \langle \phi_k |$; and the basis $\{|j_E \rangle\}$ can be chosen as the computational basis such that $|k_E \rangle = (V^\dagger)^T |k \rangle$. The guessing probability, depending clearly on Eve’s configuration $V$, then equals

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

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

One who studies security issues must take into account the worst circumstances. The quantity that indeed makes sense in evaluating Eve’s guesses should be the maximum guessing probability, $P_E^\star = \max P_E$, with the optimization accomplished by running all $V \in SU(td)$ and nonnegative $\Lambda_k$’s subject to observables of Alice and Bob.

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 [22, 23], namely, $|\phi_0 \rangle = (|00\rangle + |11\rangle) / \sqrt{2}$, $|\phi_1 \rangle = (|00\rangle - |11\rangle) / \sqrt{2}$, $|\phi_2 \rangle = (|01\rangle + |10\rangle) / \sqrt{2}$, and $|\phi_3 \rangle = (|01\rangle - |10\rangle) / \sqrt{2}$. To see it, let us first take $U = e^{-i z \sigma_\varphi}$ for Alice, with $\sigma_\varphi = \sigma_y \cos \varphi - \sigma_x \sin \varphi$. The unitary is to transform a projector along the $\hat{z}$ direction to one along an arbitrary $\vec{\sigma}$ direction. It is simple to verify that $U \sigma U^\dagger = \vec{\sigma} \cdot \vec{\sigma}$, and that $U |0 \rangle = \pm |n \rangle$, $U |n \rangle = \pm e^{-i \varphi} |n \rangle$, where $| \pm n \rangle$ are a set of orthogonal normalized states along $\vec{\sigma}$, which by parametrization read $| + n \rangle := |\theta, \varphi \rangle = \cos \frac{\theta}{2} |0 \rangle + \sin \frac{\theta}{2} e^{i \varphi} |1 \rangle$ and $| - n \rangle := |\theta, -\varphi \rangle = \sin \frac{\theta}{2} |0 \rangle - \cos \frac{\theta}{2} e^{i \varphi} |1 \rangle$. Likewise, for Bob, a set of orthogonal normalized states along $\vec{n}'$ can be written as $| + n' \rangle := |\theta, -\varphi \rangle$ and $| - n' \rangle := |\theta, \varphi \rangle$. Then, for the correlations

$$P_{\pm n, \pm n'} = \text{tr} \left( |\pm n \rangle \langle \pm n | \otimes |\pm n' \rangle \langle \pm n' |_{AB} \rho_{AB} \right),$$

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 $\sum_{i=0}^{l-1} \varphi_i = 1$, 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

$$P_{+n_i, +n_i'} = P_{-n_i, -n_i'} = \frac{\varphi_i}{2} \times \Delta_i,$$

$$P_{+n_i, -n_i'} = P_{-n_i, +n_i'} = \frac{\varphi_i}{2} \times (1 - \Delta_i),$$

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 $\vec{n}$ and $\vec{n}'$ 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 $\vec{n}''$ direction may be found and used for Bob to demonstrate with Alice the symmetry of $P_{\pm n, \pm n''}$. 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 (1) and

$$\varepsilon_i := \frac{P_{+n_i, -n_i'} + P_{-n_i, +n_i'}}{\sum_{m, m'} P_{m, m'}},$$

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 $\varepsilon_0 = \varepsilon_2 = \Lambda_2 + \Lambda_3$, 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 $\hat{n}_{0,1}$. 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, $\Lambda_0 = 1 - (\cos^2 \varphi_1 - \cos^2 \theta_1) \varepsilon_0 - (1/ \sin^2 \theta_1) \varepsilon_1 + \Lambda_3 \cos 2\varphi_1$, $\Lambda_1 = 1 - \varepsilon_0 - \Lambda_0$, and $\Lambda_2 = \varepsilon_0 - \Lambda_3$. Hence, the $P_E^\star$ with respect to $\varepsilon_0$ can be computed by numerating $V \in SU(4)$ and $\Lambda_3$, subject to $0 \leq \Lambda_i \leq 1$ 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 $P_E^\star$ with respect to $\varepsilon_0, \varepsilon_1, \varepsilon_2$ can be computed by numerating $V \in SU(6)$.

**Protocol III:** A 2$t$-state protocol with $t > 3$ measuring directions $\hat{n}_{0,1,\ldots,t-1}$. The first three error rates are connected with $\Lambda_1$’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 $\delta_1 = \sin^2 \theta_1 \sin(\varphi_2 - \varphi_k) \sin(\varphi_2 + \varphi_k) \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2) \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2)$ and $\delta_2 = \sin^2 \theta_1 \sin(\varphi_1 - \varphi_k) \sin(\varphi_1 + \varphi_k) \sin(\varphi_1 - \varphi_k) \sin(\varphi_1 + \varphi_2) \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2)$ and $\delta_2 = \sin^2 \theta_1 \sin(\varphi_1 - \varphi_k) \sin(\varphi_1 + \varphi_k) \sin(\varphi_1 - \varphi_k) \sin(\varphi_1 + \varphi_2) \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2)$. The $P_E^\star$ with respect to $\varepsilon_{0,1,\ldots,t-1}$ can be computed by numerating $V \in SU(2t)$.

**Entropic criterion for the rate of secure keys generated in all bases of measurements.**—We consider the information-theoretic security of QKD, for which the secure key rate is computed as $R = \max \{I_{AB} - \max_{\lambda, \chi_{AE}} \chi_{AE} \}$, where $R$ is the entanglement quantity $\chi_{AE}$ [24, 25], with the optimization of the Holevo quantity $\chi_{AE}$ [20] done by running nonnegative
independent $\Lambda_i$'s. Obviously, as the key is generated in all bases of the measurements, a general key-rate formula is needed.

To the end, let us first derive the mutual information

$$I_{AB} = \sum_{i,j} \sum_{m_i,m_j'} P_{m_i,m_j'} \log_2 P_{m_i,m_j'}/P_{m_i',m_j},$$

where $P_{m_i}$ and $P_{m_j'}$, with $m_i = \pm n_i$ and $m_j' = \pm n_i'$, denote marginals for Alice and for Bob, respectively. We consider the protocols where cross-term data is not used; i.e., $P_{m_i,m_j'} = 0$ for $i \neq j$, such that the mutual information can be computed independently for each $i$. With the symmetry in (1), we find then $I_i = \phi_i(1 - h(\varepsilon_i)) - \phi_i \log_2 \phi_i$, with $h(x) := -x \log_2 x - (1 - x) \log_2 (1 - x)$, a sum of which yields $I_{AB} = 1 - \sum_i \phi_i h(\varepsilon_i) + H(\phi_i)$. The Shannon entropy, $H(\phi_i) = -\sum_i \phi_i \log_2 \phi_i$, 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,

$$\mathcal{I}_{AB} = I_{AB} - H(\phi_i).$$

Let us next consider the eavesdropping in which Eve holds states $\rho_E^{\pm n_i}$ conditional on Alice's measurements with probability $\phi_i$ for each $i$. The Holevo quantity for our purpose here reads $\chi_{AE} = S(\rho_{AB}) - \sum_i \phi_i S(\rho_{E|m_i})$, where $\rho_{m_i}$ with $m_i = \pm n_i$ denotes the probability that Alice measures her qubit with 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 $\rho_{E|m_i}$ are of rank two, and have eigenvalues $\lambda_{i\pm n_i} = \lambda_{i\pm n_i} = [1 \pm \sqrt{\varepsilon_i + \eta_i}]/2$, where $\varepsilon_i = (\mu_+ - \nu_+)^2 \cos^2 \theta_i$ 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 $\hat{x}\hat{z}$-plane in [27]; see also [21].) It is straightforward to have $S(\rho_{AB}) = H(\Lambda_i)$. The Holevo quantity is computed then $\chi_{AE} = H(\Lambda_i) + \sum_{m_i,q} \phi_i p_{m_i} \lambda_{q_{m_i}}^2 \log_2 \lambda_{q_{m_i}}^2$ with the sum over $q = \pm$, $m_i = \pm n_i$, and $i = 0, \ldots, t - 1$. Given the symmetry of the Bell-diagonal state, it holds that $p_{+n_i} = p_{-n_i} = 1/2$ for any $n_i$.

It is remarked that for the $t = 2$ protocols, the relations between $\varepsilon_i$'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 $\varepsilon_i$'s must satisfy the relations in Protocol III. Obviously, under proper circumstances the general criterion reduces to some established formula, like $R = 1 - 2h(\varepsilon_i)$ or $1 - h(3\varepsilon_i/2) - (3\varepsilon_i/2) \log_3 2$, for the original BB84 and six-state protocol, respectively.

Example One: 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 $|0\rangle_E = \frac{1}{2}|0\rangle_E - \frac{1}{2}|1\rangle_E - \frac{1}{2}|2\rangle_E - \frac{1}{2}|3\rangle_E$, $|1\rangle_E = \frac{1}{2}|0\rangle_E + \frac{1}{2}|1\rangle_E$, $|2\rangle_E = \frac{1}{2}|0\rangle_E + \frac{1}{2}|1\rangle_E$, and $|3\rangle_E = \frac{1}{2}|0\rangle_E - \frac{1}{2}|1\rangle_E - \frac{1}{2}|2\rangle_E + \frac{1}{2}|3\rangle_E$, where $|j\rangle_E$ takes the computational basis as previously stated. The error rates equal to $\epsilon_0 = 1 - (1 - \kappa)/4 = \epsilon \in [0, 1/4]$ and the purification $|\psi\rangle_{ABE} = \sum_{k=0}^3 \sqrt{\Lambda_k} |\phi_k\rangle_{AB} |\kappa_k\rangle_E$ are henceforth obtained. The maximum guessing probability then equals

$$P_E = \sum_{j=0}^3 \text{tr} \left[ \left( |+n_j\rangle\langle +n_j| + |2j\rangle\langle 2j| \right) |\psi\rangle_{ABE} \right] + \frac{1}{2} + \sqrt{\Lambda_0/2} \left( \sqrt{\Lambda_1} + \sqrt{\Lambda_2} \right) - 2\epsilon (1 - 2\epsilon).$$

It equals unity for $\epsilon \in [1/4, 1/2]$. We plot the $P_B$-versus-$P_E$ figure (see Fig. 1(a)) for arbitrary Bell-diagonal states, confirming the maximum of (2).

Let $P_B > P_E$, and we find $\epsilon < 10\% := \epsilon_{cr}$. The bound serves as a tighter threshold value for the BB84 error rate than with the entropic criterion, in the sense that the same error rate yields $R = 1 - 2h(\epsilon_{cr}) \simeq 0.062 \neq 0$. 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 $\epsilon_{cr} \approx 11\%$, yielding $P_B \simeq 89\%$, which is less than $P_E \approx 91\%$. In other words, a particular region exists for the error rate such that the relation $P_B > P_E$ breaks down while the entropic criterion $R > 0$ holds.

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 variation
TABLE I. The critical values of error rates impose more limits on Eve’s guessing capability. It equals unity for the protocol with measurements along the \( \hat{n} \) and \( \Lambda_0 = 2/(1 + \kappa) \) and \( \Lambda_1 = \Lambda_2 = \Lambda_3 = (1 - \kappa)/6 \), along with an optimal unitary transform \( V \in SU(6) \) such that \( |0 \rangle_E = \frac{1}{\sqrt{6}} |0 \rangle_E - \frac{1}{\sqrt{6}} |1 \rangle_E + \frac{1}{\sqrt{6}} |2 \rangle_E + \frac{1}{\sqrt{6}} |3 \rangle_E + \frac{1}{\sqrt{6}} |4 \rangle_E + \frac{1}{\sqrt{6}} |5 \rangle_E \), \( |1 \rangle_E = \frac{1}{\sqrt{2}} |0 \rangle_E + \frac{1}{\sqrt{2}} |1 \rangle_E \), \( |2 \rangle_E = \frac{1}{\sqrt{2}} |0 \rangle_E - \frac{1}{\sqrt{2}} |1 \rangle_E \), \( |3 \rangle_E = \frac{1}{\sqrt{2}} |0 \rangle_E + \frac{1}{\sqrt{2}} |1 \rangle_E \), \( |4 \rangle_E = \frac{1}{\sqrt{2}} |0 \rangle_E - \frac{1}{\sqrt{2}} |1 \rangle_E \). The maximum guessing probability equals

\[
P_E^* = \sum_{j = 0, 1, 2} \text{tr} \left[ \left( \left| n_j \rightangle \langle + n_j \right| \otimes j \right| \langle 2 j \rangle \right]_E + \left| - n_j \right\rangle \langle - n_j \right| \otimes j \right| \langle 2 j + 1 \rangle \right| \langle 2 j + 1 \rangle \rangle_E \right] = \frac{1}{2} + \frac{\sqrt{3} \kappa}{2} (\sqrt{\Lambda_1} + \sqrt{\Lambda_2} + \sqrt{\Lambda_3}) = \frac{1}{2} + \frac{3}{2} (2 - 3 \kappa) / 4. \tag{3}
\]

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 (3). It can be seen that (3) is lower than (2), since more observables impose more limits on Eve’s guessing capability.

Similar to the BB84 protocol, let \( P_B > P_E \) then we find \( \varepsilon < (5 - 2\sqrt{3}) / 13 \approx 11.8 \% = \varepsilon_{ct}^{\prime} \). The bound is still tighter than in the entropic criterion, since the same error rate yields \( R = 1 - h(3\varepsilon_{ct}^{\prime}/2) - (3\varepsilon_{ct}^{\prime}/2) \log_2 3 \approx 0.045 \neq 0 \). 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 \( \varepsilon_{ct}^{\prime} \approx 12.6 \% \), yielding \( P_B \approx 87.4 \% \), which is less than \( P_E^{\prime} \approx 89 \% \). Thus the gap, between the relation of the protocol with the BB84 and the entropic criterion \( R > 0 \), remains.

Summary and discussion.—We have presented a general analysis of quantifying the quantum guessing probability in QKD protocols. We have also derived a general formula of the entropy-based security criterion for keys generated in all relevant bases of measurements. In particular, we have computed the maximum guessing probability and the entropy-based key rate in the BB84 and six-state 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. The relation has been shown to be able to impose even tighter restrictions than the entropic criterion on the key rates. Thus, our results have validated a proper way of using guessing probability as an efficient index to estimate eavesdropping.

We would like to make a few remarks on the terminology. It should at first be noted that our results do not contradict those in [17], where the authors prove that the entropic criterion is much stricter than the guessing probability. The reason for such different statements is that the context we consider is different from [17], namely: (a) our guessing probability is about guessing the sifted key; (b) we consider a quasi-ideal scenario; (c) we propose a guessing-probability-based relation to determine critical key rates, while in [17] (a’) the guessing probability is about guessing the final key; (b’) they consider a finite-length scenario; (c’) they find an upper bound of guessing probability using the \( \varepsilon \)-security levels [6]. In our opinion, the results here and those in [17] address very different aspects of the guessing probability. Second, there have also been results on bounding Eve’s guessing probability with the Bell inequality [28]. For instance, references [29–31] 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 [32]. The \( P_B > P_E \) relation defined therein cannot imply \( R > 0 \). Reference [33] investigates the device-independent QKD with various Bell inequalities. Regarding Eve’s guessing probability, their definition is similar to ours (see Eq. (18) in [33]) but bounded in terms of Bell violations.

The study is supported by the National Natural Science Foundation of China.
1 C. E. Shannon, The Bell System Technical Journal 28, 656-715 (1949).
2 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.
3 A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
4 M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in Theory of Cryptography Conference, (Springer, 2005), pp. 386-406.
5 R. Renner and R. König, in Theory of Cryptography Conference, (Springer, 2005), pp. 407-425.
6 R. Renner, PhD Thesis (ETH Zurich, 2005); Int. J. Quant. Inf. 6, 1 (2008).
7 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
8 V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
9 H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics 8, 595-604 (2014).
10 E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Information 2, 16025 (2016).
11 F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. 92, 025002 (2020).
12 D. Z. Albert, Phys. Lett. A 98, 249-252 (1983).
13 M. Alimomeni and R. Safavi-Naini, in International Conference on Information Theoretic Security, (Springer, 2012) pp. 1-13.
14 I. Issa and A. B. Wagner, IEEE Trans. Inf. Theory 63, 3783 (2017).
15 R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory 55, 4337-4347 (2009).
16 H. P. Yuen, IEEE Access 4, 724 (2016).
17 X.-B. Wang, J.-T. Wang, J.-Q. Qin, C. Jiang, and Z.-W. Yu, npj Quantum Information 6, 45 (2020).
18 E. Biham and T. Mor, Phys. Rev. Lett. 78, 2256 (1997).
19 E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Algorithmica 34, 372-388 (2005).
20 C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. 68, 557 (1992).
21 H.-Y. Su, Quantum Info. Processing 19, 169 (2020).
22 B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. 95, 080501 (2005).
23 R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005).
24 P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
25 I. Devetak and A. Winter, Proc. R. Soc. A 461, 207-235 (2005).
26 A. S. Holevo, Probl. Peredachi Inf. 9, 3-11 (1973).
27 S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. 11, 045021 (2009).
28 J. S. Bell, Physics 1, 195-200 (1964).
29 M. Pawlowski, Phys. Rev. A 82, 032313 (2010).
30 W.-Y. Hwang and O. Gittsovich, Phys. Rev. A 85, 046301 (2012).
31 M. Pawlowski, Phys. Rev. A 85, 046302 (2012).
32 J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).
33 L. Masanes, S. Pironio, and A. Acín, Nat. Commun. 2, 238 (2011).
34 D. Mayers and A. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS ’98), Palo Alto, CA, 1998 (IEEE Computer Society, Washington, DC, 1998), pp. 503-509.
35 J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. 95, 010503 (2005).
36 A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).