A simple relation of guessing probability in quantum key distribution

Hong-Yi Su

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

* Author to whom any correspondence should be addressed.
E-mail: hysu@hrbeu.edu.cn

Keywords: quantum key distribution, guessing probability, security analysis

Abstract

Given a communication system using quantum key distribution (QKD), the receiver can be seen as one who tries to guess the sender’s information just as potential eavesdroppers do. The receiver-eavesdropper similarity thus implies a simple relation in terms of guessing probability and correctness of sifted keys, related 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 security criteria. Thus, an alternative perspective on applying guessing probability in analyzing QKD issues is here provided. Examples of two specific protocols are illustrated. Our results contribute to evaluating an important element in communication study, and may provide useful reference for the security analysis of QKD protocols.

1. Introduction

Quantum key distribution (QKD) has been proved information-theoretically secure via quantum entropic arguments. For a communication (secrecy) system, however, as was stated in Claude Shannon’s seminal paper, ‘…[i]n general, the only difference between the decipherer’s knowledge and the enemy cryptanalyst’s knowledge is that the decipherer knows the particular key being used, while the cryptanalyst knows only the a priori probabilities of the various key in the set…’ [1]. Despite such a difference, the receiver and the eavesdropper are rather similar in tasks like secret key distribution. This motivates us to evaluate eavesdropping using various measures other than the Shannon entropy or many of its variants in quantum theory.

Guessing probability [2, 3], often requested by researchers alongside customers of cryptosystems, is among the candidates. It serves to estimate the eavesdropper’s probability of correctly guessing the key transmitted from the sender to the receiver. It has drawn particular attention [4–6] as QKD is being implemented in recent decades. There have been results pointing out that guessing probability of the key can provide an alternative perspective on QKD security. We for instance list a few relevant references as follows: (i) guessing probability is associated with the min-entropy, in a way that the logarithm of the probability of guessing the sender’s bits given eavesdropping provides a lower bound on the number of secret bits that can be extracted [4]. (ii) In reference [6], researchers invoke finite-length analysis to take account of fluctuation effects and show that, after privacy amplification with the Toeplitz matrix, the guessing probability can be decreased by approximately $10^{-3268}$ of a previously obtained upper bound. (iii) Guessing probability depends on the specific protocols or key distillation post-processing [7, 8]. For instance, if the eavesdropper, in order to guess the sender’s bit, takes the Helstrom strategy [9], then the eavesdropping information will be directly determined by the guessing probability (see, e.g., equation (27) in [7] for an explicit relation between mutual entropy and guessing probability). As shown in [8], some key distillation post-processing can further decrease the eavesdropper’s guessing probability. Using the classical advantage distillation [10], it is proved that (i.e., equations (71)–(73) in [8]) when security is compromised one can always have $F_N < P_{\text{success}}$ (which corresponds to $P_B < P_{\text{eq}}$ in our notation defined below). Let us
emphasize that the situation we shall consider is one without post-processing, thus differing from that in [8]. Additionally, study of guessing probability is nontrivial in itself, since it can be seen as a consequence of quantum state discrimination [11–13], a fundamental task applicable in information processing. Note that the guessing probability considered here is computed in the protocols with trusted preparation and measurement; that is, the Hilbert dimensions of quantum states will have to be assumed fixed and known. Device-independent protocols, or semi-device-independent ones, which are without the assumption on dimensionality, are beyond our scope here (see, however, the discussion in the end of the paper).

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 [1]. 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 [14, 15]. For instance, the quantum secure key rate is computed by a properly optimized difference between $S(A|E)$ and $S(A|B)$ [16–18], 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 [19–23] 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 [24].

More specifically, the secure key rate formula can be derived from the finite-length, distance-based $\varepsilon$-security [16–18], and in the asymptotic limit it reduces to several well-known expressions, like $R = 1 - 2h(Q)$ for the Bennett–Brassard 1984 (BB84) protocol [14], with $h(x) := -x \log_2 x - (1 - x) \log_2 (1 - x)$ and $Q$ the error rate. For general composable protocols, the overall security level, $\varepsilon$, can be divided into two parts, the correctness $\varepsilon_{\text{cor}}$ and the secrecy $\varepsilon_{\text{sec}}$, subject to $\varepsilon \leq \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$. Following the terminology and notations in [25], here the $\varepsilon_{\text{cor}}$ bounds the probability that Alice and Bob fail to share identical keys of a certain length, namely, $P(1 \neq B) \leq \varepsilon_{\text{cor}}$, and the $\varepsilon_{\text{sec}}$ bounds the trace-norm distance between a realistic Alice–Eve correlation and an ideal one, namely, $\frac{1}{2} \min_{\sigma_E} \| \rho_{AE} - \tau_{\text{A}} \otimes \sigma_E \|_1 \leq \varepsilon_{\text{sec}}/(1 - p_{\text{abort}})$, where $p_{\text{abort}}$ denotes the probability that the protocol is aborted, $\rho_{AE}$ is the quantum state representing the Alice–Eve correlation, $\tau_{\text{A}}$ 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, as can be seen by referring to the finite-length key rate formulas that usually involve both $\varepsilon_{\text{cor}}$ and $\varepsilon_{\text{sec}}$ (see, e.g., the formula in [25]). In applications, it is reasonable to consider correctness and secrecy separately; however, the overall security level $\varepsilon$ makes more sense than its constituents. Hence $\varepsilon_{\text{cor}}$ alone, while maybe very close to $\varepsilon$, does not imply security. Nevertheless, as we shall show in this paper, study focused on $\varepsilon_{\text{cor}}$ bears a merit that it has potential to intuitively connect the Alice–Bob correlation with the guessing probability, i.e., with the Alice–Eve correlation. The unobservable Alice–Eve correlation can thus be evaluated via the observable Alice–Bob correlation. By treating Bob and Eve from a similar perspective, i.e., both can be seen as trying to guess keys from Alice, a guessing-probability-based relation can be established, giving rather efficient predictions as by the entropic security criterion.

Before presenting the setup and formulation of guessing probability, we would like here to discuss the guessing-probability-based relation and the security criterion. On the one hand, since $\varepsilon_{\text{cor}}$ is no greater than $\varepsilon$ in magnitude, an ‘$\varepsilon_{\text{cor}}$-secure’ protocol must be considered more secure than an $\varepsilon$-secure protocol. For this reason the guessing-probability-based relation, motivated by $\varepsilon_{\text{cor}}$, is likely to impose slightly stricter requirement than the entropic criterion, motivated by $\varepsilon$, upon some essential factors, e.g., critical error rates. This is the case in our results shown in the next section, particularly in the two examples, to which we refer the readers for detail. It is stressed, however, that the gap between the different predictions should not be interpreted as some overestimate by the established security criterion, but rather as immediate consequences of the $\varepsilon$-security formalism. On the other hand, results so far in existing literature, concerning guessing probabilities that match the hierarchy between $\varepsilon_{\text{cor}}$ and $\varepsilon$, have rarely been developed. In other words, a desired $\varepsilon_{\text{cor}}$-motivated relation ought to exist in order to impose requirements stricter than—if not equivalent to—the $\varepsilon$-security criteria upon QKD protocols. Will it be done, for instance, with any carefully built relations, which could involve keys before the final phase but still remain intuitively simple? This question raises our principal motivation of quantifying the guessing probability, from which we are then able to construct meaningful relations and give an affirmative answer to the question.
2. Quantifying guessing probability

2.1. Brief description of the setup

To build such a relation, one will first have to evaluate the guessing probability via some observables (usually the error rates, known to Alice and Bob). The evaluation requires an optimization procedure, because the Alice–Bob density matrix, representing the Alice–Bob correlation, can be reduced from non-unique Alice–Bob–Eve purification states; namely, different purifications may yield different guessing probabilities for a same Alice–Bob correlation. Then, one can have a guessing-probability-based relation in terms of the Alice–Bob correlation and the Alice–Eve correlation. A desired, sufficiently efficient relation should impose some stricter requirements on the composable QKD protocols, in accord with the hierarchy between $e_{\text{cor}}$ and $e$.

Let us briefly describe the setup. We consider the QKD protocols in which Alice sends Bob keys which Eve may intercept and resend. Instead of the final key, 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 collective attacks [26, 27] so that it suffices to study a single run of preparation and measurement with the quantum state of Alice and Bob. Let $H_A(d)$, $H_B(d)$ and $H_E(2d)$ 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 $P_t = \sum_{i=0}^{d-1} P(e = a_i + i \times d)$, $a_i$ and $e$ being the outcomes of events of Alice and Eve. Motivated by $e_{\text{cor}}$, also in the light of Shannon’s idea on the similarity between Bob and Eve, we present an equally significant quantity $P_{\text{gend}}$ with $b_i$’s similarly denoting the outcomes of events of Bob, $\wp_i$ the probability that Alice chooses the $i$th basis to perform measurements, and $\sum_i \wp_i = 1$.

Given transmission 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 $P_E^*$ by listening to the publicized bases in the sifting phase and optimizing her strategies. Here $P_E^*$ represents the optimized $P_E$. The Bob-versus-Eve scenario allows us to propose the relation $P_E > P_E^*$ 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 $P_E^*$, 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.

In what follows, we will first present a 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 security criteria will be compared and discussed.

2.2. Definition of the maximum guessing probability

To begin with, it is convenient to consider the entanglement-based scenario [28, 29]. The general state shared by Alice and Bob reads $\rho_{AB} = RR^\dagger$, where $R = U\sqrt{\lambda}V^\dagger$, $R$ and $U$ are $d^2 \times d^2$ matrices, $U$ denotes the unitary transform that diagonalizes $\rho_{AB}$, $A$ is a $d^2 \times d^2$ 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, $|\psi\rangle_{ABE} = \sum_{j} U_{jA} |j\rangle_{AB} |j\rangle_E$, with $|j\rangle_E \in H_E(2d)$ and $|j\rangle_E \in H_E(2d)$ [30]. Because of the Schmidt decomposition, we define $\sum U_{jA} |j\rangle_{AB} = |k\rangle_{AB}$ and $\sum (V^\dagger)_{jB} |j\rangle_{E} = |k\rangle_{E}$, and the purification state immediately becomes $|\psi\rangle_{ABE} = \sum_1^{d^2} \sqrt{\lambda_k} |k\rangle_{AB} |k\rangle_E$, with $k = 0, 1, \ldots, \min\{d^2 - 1, td - 1\}$. Here, the basis $\{|j\rangle_{AB}\}$ can be chosen in such a way that $|k\rangle_{AB} = |\phi_k\rangle_{AB}$, where $|\phi_k\rangle_{AB}$ are the axes for the diagonalized $\rho_{AB} = \sum \lambda_k |\phi_k\rangle_{AB} \langle \phi_k|$, and the basis $\{|j\rangle_{E}\}$ can be chosen as the computational basis such that $|k\rangle_E = (V^\dagger)^{j_k} |k\rangle_E$. The guessing probability, depending clearly on Eve’s strategy $V$, then equals

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

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 guessing probability,

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

where the optimization is accomplished by running all \( V \in SU(td) \), 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 section 2.4, particularly the discussion around equation (13) through (16).

### 2.2.1. 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 \([31, 32]\), 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 \( U = e^{i\theta \sigma_z} \) for Alice, with \( \sigma_x = \sigma_y \cos \varphi - \sigma_z \sin \varphi \). The unitary is to transform a projector along the \( \hat{z} \) direction to one along an arbitrary \( \hat{n} \) direction. It is simple to verify that \( U \sigma U^{-1} = \hat{n} \cdot \sigma \), and that \( U|0\rangle = |+\rangle, U|1\rangle = -e^{-i\varphi}|-\rangle \), where \(|\pm\rangle\) are a set of orthogonal normalized states along \( n \), which by parametrization read \(|+\rangle := (\varphi) = \cos \frac{i}{2} |0\rangle + \sin \frac{i}{2} e^{i\varphi} |1\rangle \) and \(|-\rangle := (\varphi) = \sin \frac{i}{2} |0\rangle - \cos \frac{i}{2} e^{i\varphi} |1\rangle \). Likewise, for Bob, a set of orthogonal normalized states along \( n' \) can be written as \(|+\rangle' := (\varphi) \) and \(|-\rangle' := (\varphi) \). Then, for the correlations

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

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 \( \sum_{i=0}^{t} \varphi_i = 1 \), 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 \( P_{\pm n, \pm n''} \).

### 2.2.2. 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

\[ \varepsilon_i := \frac{P_{+n, +n'} + P_{-n, -n'}}{\sum_{m_i, m'_i} P_{m_i, m'_i}}, \]

(which corresponds to the correctness of the sifted key and should not be confused with the overall security level \( \varepsilon \) for the final key) 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 \( \varepsilon_i := \varepsilon_2 = \Lambda_2 + \Lambda_3 \), 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 \( \theta_0, \varphi_0 \). 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, \( \Lambda_0 = 1 - (\cos^2 \varphi_1 - \cot^2 \theta_1)\varepsilon_0 \), and \( \Lambda_2 = 1 - \delta_0 - \Lambda_0 \), and \( \Lambda_3 = \varepsilon_0 - \Lambda_0 \). Hence, the \( P_E^* \) with respect to \( \varepsilon_0, 1 \) can be 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 \( \theta_0, \varphi_0, \varphi_1 \). Three error rates are related to the \( \Lambda_i \)'s, so all of them are fixed. The \( P_E^* \) 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 $\hat{n}_{0,1,\ldots,t-1}$. The first three error rates are connected with $\Lambda_i$’s, and the remaining error rates are determined by the first three as

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

(6)

for $3 \leq k < t$, with

$$\delta_1 = \frac{\sin^2 \theta_k \sin(\varphi_1 - \varphi_k) \sin(\varphi_2 + \varphi_k)}{\sin^2 \theta_1 \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2)},$$

$$\delta_2 = \frac{\sin^2 \theta_k \sin(\varphi_1 - \varphi_k) \sin(\varphi_1 + \varphi_k)}{\sin^2 \theta_2 \sin(\varphi_1 - \varphi_2) \sin(\varphi_1 + \varphi_2)}.$$  

(7)

The $P_E$ with respect to $\varepsilon_{0,1,\ldots,t-1}$ can be computed by numerating $V \in SU(2t)$.

2.3. Derivation of a general secure key rate

We consider the information-theoretic security of QKD, for which the secure key rate is computed by $R = \max \{I_{AB} - \max_{\Lambda} \chi_{AE}, 0 \}$ [33, 34], with the optimization of the Holevo quantity $\chi_{AE}$ [35] done by running nonnegative independent $\Lambda_i$’s. Given the key is generated in all bases of the measurements, in what follows we explicitly derive the key rate. It is noted that the entropic security criterion has been well established and the derivation below is not an original contribution of this paper.

To the end, let us first derive the mutual information $I_{AB} = \sum_{ij} \sum_{m_i,m'_j} P_{m_i,m'_j} \log_2 P_{m_i,m'_j}/P_{m_i}/P_{m'_j}$, where $P_{m_i}$ and $P_{m'_j}$, with $m_i = \pm n_i$ and $m'_j = \pm n'_j$, 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 (4), we find then $I_i = \varphi_i (1 - h(\varepsilon_i)) - \varphi_i^2 \log_2 \varphi_i$, a sum of which yields

$$I_{AB} = 1 - \sum_i \varphi_i h(\varepsilon_i) + H(\varphi_i).$$  

(8)

The Shannon entropy, $H(\varphi_i) = -\sum_i \varphi \log_2 \varphi_i$, 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,

$$I_{AB} = I_{AB} - H(\varphi_i).$$  

(9)

Let us next consider the eavesdropping in which Eve holds states $\rho_{i,\pm n_i}$ conditional on Alice’s measurements with probability $\varphi_i$ for each $i$. The Holevo quantity for our purpose here reads

$$\chi_{AE} = S(\rho_{AB}) - \sum_i \varphi_i \sum_{m_i} S(\rho_{m_i}),$$

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 $S(\rho_{AB}) = S(\rho_{AB})$ as $|\psi_{AB}\rangle$ is pure. The conditional states $\rho_{i,\pm n_i}$ are of rank two, and have eigenvalues $\lambda_{\pm n_i}^\pm = \frac{1 \pm \sqrt{\xi_n + \eta_i}}{2}$, where $\xi = (\mu_+ - \mu_-)^2 \cos^2 \theta_i$ and $\eta_i = (\mu_+^2 + \mu_-^2 + 2 \mu_\pm \nu \pm \cos 2\varphi_i) \sin^2 \theta_i$, with $\mu_\pm = \Lambda_\pm \pm \Lambda_\delta$ and $\nu_\pm = \Lambda_\pm \pm \Lambda_\delta$. (These eigenvalues were computed in the $\hat{x}$-plane in [36]; see also [30].) It is straightforward to have $S(\rho_{AB}) = H(\Lambda_i)$. The Holevo quantity is computed then

$$\chi_{AE} = H(\Lambda_i) + \sum_{i,m_i,q} \varphi_i \rho_{m_i} \lambda_{m_i}^q \log_2 \lambda_{m_i}^q,$$  

(10)

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 $\rho_{+n_i} = \rho_{-n_i} = 1/2$ for any $n_i$.

It is remarked that for the $t = 2$ protocols, the relations between $\varepsilon_k$’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 $\varepsilon_k$’s must satisfy the relations in protocol III. Obviously, under proper circumstances the general criterion reduces to some established formulas, like $R = 1 - 2h(\varepsilon_2)$ and $1 - h(3\varepsilon_2/2) - (3\varepsilon_2/2)\log_2 3$, which have already been obtained in [33, 37] for the original BB84 and six-state protocols, respectively.

2.4. Examples of guessing probability

2.4.1. 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 $\Lambda_0 = (1 + \kappa)/2, \Lambda_1 = \Lambda_2 = (1 - \kappa)/2$, and
It is obvious to see that Eve cannot discern Alice’s qubits by her projective measurements on Bell-diagonal states, confirming the maximum of (12). Hence, $V$ that the optimal strategy yields an error rate $\varepsilon_0$, along with an optimal unitary transform $V \in SU(4)$ such that

\[
\begin{align*}
|0\rangle_E &= \frac{1}{2} |0\rangle_E - \frac{1}{2} |1\rangle_E + \frac{1}{2} |2\rangle_E - \frac{1}{2} |3\rangle_E, \\
|1\rangle_E &= \frac{1}{2} |0\rangle_E + \frac{1}{2} |1\rangle_E,
\end{align*}
\]

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 $|\psi\rangle_{ABE} = \sum_{k=0}^{3} \sqrt{\Lambda_k} |\phi_k\rangle_{AB}|k\rangle_E$ are henceforth obtained. The maximum guessing probability then equals

\[
P_k^E = \sum_{j=0,1} \text{tr}\left[\left(|j+\rangle_A \otimes |2j\rangle_E + |j-\rangle_A \otimes |2j+1\rangle_E\right) |\psi\rangle_{ABE} \langle \psi|_{ABE}\right] = \frac{1}{2} + \frac{\Lambda_0 + \Lambda_1}{2} = \frac{1}{2} + \sqrt{\varepsilon(1 - 2\varepsilon)}.
\]

(12)

It equals unity for $\varepsilon \in (1/4, 1/2]$. We plot the $P_b$-versus-$P_k$ figure (see figure 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 $V = \mathbb{I}$, we have $|kv\rangle_E = |k\rangle_E$, and

\[
|\psi\rangle_{ABE} = \sqrt{1 - 2\varepsilon} |\phi_0\rangle_{AB}|0\rangle_E + \sqrt{\varepsilon} |\phi_1\rangle_{AB}|1\rangle_E + \sqrt{\varepsilon} |\phi_2\rangle_{AB}|2\rangle_E.
\]

(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

\[
P_k = \text{tr}\left[\left(|0\rangle_A \otimes |0\rangle_E + |1\rangle_A \otimes |1\rangle_E + |+\rangle_A \otimes |2\rangle_E + |\rangle_\Lambda \otimes |3\rangle_E\right) \rho_{ABE}\right] = 1/2,
\]

(14)

which is smaller than (12). Hence, $V = \mathbb{I}$ is not an optimal strategy for Eve. By ‘optimal strategy’, we mean that the $V_i$ for instance the one that induces (11), can enable Eve to guess Alice’s measurement results with

Figure 1. The $P_b$-versus-$P_k$ relations for the BB84 (left) and six-state (right) protocols, where $P_b = 1 - \varepsilon$, and the upper bounds (red curves) represent the $P_k$’s in (12) and (18). The data (blue points) were collected with around 3800 (left) and 2750 (right) measurements, respectively. The dashed lines correspond to $P_b = P_k$ so the points falling in shaded regions all have the property that Eve’s maximum guessing probability is less than $P_b$. Note, however, that because Eve has less limits on Hilbert-space dimensions than Bob, $P_b$ reaches 1 well before $P_k$ decreases to 0 (see, e.g., points (3/4, 1) and (2/3, 1) on the left and right red curves, respectively).
the largest probability, under her projective measurements \(|k\rangle\langle k|_{E}\). In other words, Eve must try to find an optimal \(V\) so that with a purification \(|\psi\rangle_{ABE} = \sum_{E} \sqrt{\alpha_{E}} \phi_{A} |\psi_{E}\rangle_{E}\) she can obtain the maximum of \(P_{E}\), i.e., the \(P_{E}^{*}\) under the projection \(\sum_{E} \langle n_{E} | \langle \pi/2 | \langle k\rangle_{E}\rangle, with \(|n_{E}\rangle_{\Lambda} = |0\rangle_{\Lambda}, |n_{2}\rangle_{\Lambda} = |1\rangle_{\Lambda}, \) and \(|n_{2}\rangle_{\Lambda} = |\pi/2\rangle_{\Lambda}\).

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

\[ |\psi\rangle_{ABE} = |\phi_{0}\rangle_{AB}|0_{V}\rangle_{E}, \]

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

\[
|\psi\rangle_{ABE} = \frac{1}{\sqrt{2}} \left( |\phi_{0}\rangle_{AB} |0_{V}\rangle_{E} + \frac{1}{2} |\phi_{1}\rangle_{AB} |1_{V}\rangle_{E} + \frac{1}{2} |\phi_{2}\rangle_{AB} |2_{V}\rangle_{E} \right)
= \frac{1}{2} \left[ (|0_{V}\rangle_{AB}|0_{E}| + |1_{V}\rangle_{AB}|1_{E}| + |2_{V}\rangle_{AB}|2_{E}| - |3_{V}\rangle_{AB}|3_{E}| \right],
\]

from which we find \(P_{E}^* = 1\), 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 \(\mathcal{R} = 1 - 2h(\varepsilon_{cr}) \approx 0.062\). Note that the information of the basis is \(log_{2} 2 = 1\) bit, which has been deducted from the \(\mathcal{R}\) here. Meanwhile, let \(\mathcal{R} = 0\) 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 1. It is noted that the critical value of the error rate for \(\mathcal{R} = 0\) varies with the measuring directions. The critical value implied from \(P_{B} = P_{E}^*\) varies with the directions, too. These variations with respect to \(\varphi_{1}\) are due to that it is \(|\phi_{0}\rangle\) that we take as the maximally entangled state in the ideal case. For each \(\varphi_{1}\), if we take \(|\phi_{0}\rangle = e^{i\omega_{1}\pi/4} \otimes e^{i\omega_{1}\pi/4} |\phi_{0}\rangle\) as the maximally entangled state in the ideal case, i.e., the coordinate is rotated along the \(\hat{z}\) axis such that the \(n_{1}\) direction becomes a new \(\hat{x}\) axis, then there will be no variations, and the critical value from \(P_{B} = P_{E}^*\) will again be slightly smaller than that from \(\mathcal{R} = 0\), as in the \(\varphi_{1} = 0\) case.

2.4.2. 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 \(\varphi_{3} = \varphi_{4} = \varphi_{5} = 1/3\). 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

\[
|0_{V}\rangle_{E} = \frac{1}{\sqrt{6}} |0\rangle_{E} - \frac{1}{\sqrt{6}} |1\rangle_{E} + \frac{1}{\sqrt{6}} |2\rangle_{E} + \frac{1}{\sqrt{6}} |3\rangle_{E} + \frac{1}{\sqrt{6}} |4\rangle_{E} + \frac{1}{\sqrt{6}} |5\rangle_{E},
\]

\[
|1_{V}\rangle_{E} = \frac{1}{\sqrt{2}} |0\rangle_{E} + \frac{1}{\sqrt{2}} |1\rangle_{E},
\]

\[
|2_{V}\rangle_{E} = \frac{1}{\sqrt{2}} |2\rangle_{E} - \frac{1}{\sqrt{2}} |3\rangle_{E},
\]

\[
|3_{V}\rangle_{E} = \frac{1}{\sqrt{2}} |4\rangle_{E} + \frac{1}{\sqrt{2}} |5\rangle_{E},
\]

\[
|4_{V}\rangle_{E} = \frac{1}{2\sqrt{3}} |0\rangle_{E} - \frac{1}{2\sqrt{3}} |1\rangle_{E} - \frac{1}{2\sqrt{3}} |2\rangle_{E} - \frac{1}{2\sqrt{3}} |3\rangle_{E},
\]

\[
|5_{V}\rangle_{E} = \frac{1}{2\sqrt{3}} |0\rangle_{E} + \frac{1}{2\sqrt{3}} |1\rangle_{E} - \frac{1}{2\sqrt{3}} |2\rangle_{E} + \frac{1}{2\sqrt{3}} |3\rangle_{E} + \frac{1}{\sqrt{3}} |4\rangle_{E} + \frac{1}{\sqrt{3}} |5\rangle_{E},
\]

where \(|\rangle_{E}\) takes the computational basis as above. The last two vectors, \(|4_{V}\rangle_{E}\) and \(|5_{V}\rangle_{E}\), 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

Table 1. The critical values of error rates \(\varepsilon_{cr}\) and \(\varepsilon_{cr}\) around which \(P_{B} \approx P_{E}^*\) and \(\mathcal{R} \approx 0\), respectively, for the four-state protocol with measurements along the \(n_{0} = \hat{z}\) axis and an arbitrary direction \(\hat{n}_{2}\) in the \(\hat{x}\)-\(\hat{z}\)-plane. The parameters and variables are taken as \(\theta_{0} = \varphi_{0} = 0, \theta_{1} = \pi/2, \varphi_{1} = 1/2, \varepsilon_{0} = \varepsilon_{1}, \varepsilon_{0} = \varepsilon_{1}, \varepsilon = \sum_{E} \varepsilon_{0} \varepsilon_{1}, \delta = \sum_{E} \varepsilon_{0} \varepsilon_{1},\) and \(\varepsilon_{cr} = \varepsilon_{cr} - \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 |
| \(\varepsilon_{cr}\) (%) | 11.00 | 11.61 | 12.62 | 11.61 | 11.00 |
| \(\delta\) (%) | -1.00 | -0.35 | +2.02 | -0.35 | -1.00 |
| \(P_{E}^*\) | 0.9000 | 0.8894 | 0.8536 | 0.8894 | 0.9000 |
error rates equal to $\varepsilon_0 = \varepsilon_1 = \varepsilon_2 = (1 - \kappa)/3 := \varepsilon \in [0, 1/3]$ and the purification

$$|\psi\rangle_{\text{ABE}} = \sum_{j=0}^{2} \sqrt{\Lambda_j} |\psi\rangle_{\text{AB}} |\psi\rangle_{B}$$

are henceforth obtained. The maximum guessing probability equals

$$P_{\text{g}} = \sum_{j=0,1,2} \text{tr} \left[ (|+n_j\rangle \langle +n_j| \otimes |2j\rangle \langle 2j|) + (-|n_j\rangle \langle -n_j| \otimes |2j + 1\rangle \langle 2j + 1|) |\psi\rangle \langle \psi|_{\text{ABE}} \right]$$

$$= \frac{1}{2} + \sqrt{\frac{1}{3} \left( \sqrt{\Lambda_1} + \sqrt{\Lambda_2} + \sqrt{\Lambda_3} \right)}$$

$$= \frac{1}{2} + \sqrt{3\varepsilon(2 - 3\varepsilon)/4}. \quad (18)$$

It equals unity for $\varepsilon \in (1/3, 1/2]$. We, again, plot the $P_{\text{h}}$-versus-$P_{\text{g}}$ figure (see figure 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 $P_{\text{h}} > P_{\text{g}}$ then we find $\varepsilon < (5 - 2\sqrt{3})/13 \approx 11.8\% := \varepsilon_{\text{cr}}$. The bound is still slightly smaller than that in the entropic criterion, since the same error rate yields $R = 1 - h(3\varepsilon_{\text{cr}}/2) - (3\varepsilon_{\text{cr}}/2) \log_2 3 \approx 0.045$. Note again that the information of the basis is $\log_2 3 \approx 1.58$ bits, which have been deducted from $R$. Also, let $R = 0$ then we find $\varepsilon_{\text{cr}} \approx 12.6\%$, yielding $P_{\text{h}} \approx 87.4\%$, which is slightly less than $P_{\text{g}} \approx 89\%$.

### 3. Summary and discussion

We have presented a general analysis of quantifying the guessing probability in QKD protocols. In particular, we have proposed a simple guessing-probability-based relation, motivated by $\varepsilon$-security, and made comparison with the entropic security criteria by illustrating their varied determinations on the critical error rates in typical QKD protocols. Our results are in accord with the $\varepsilon$-security formalism according to which one must have $\varepsilon_{\text{cr}} + \varepsilon_{\text{sec}} \leq \varepsilon$. We have thus provided an alternative perspective on security issues. The results here may be useful to the QKD implementation.

The explicit relationship between the trace distance and the guessing probability, however, remains involved, because it depends on many aspects, such as eavesdropping strategies Eve takes to perform, specific QKD protocols Alice and Bob agree to use, various definitions of guessing probability, which phase of quantum cryptography the key considered is being processed in, etc. In many studies, guessing probability can be upper bounded by a function of the trace distance, as shown in [38, 39] (where the definition is different from here). Debate was raised on whether the bound is a tight one [5]. In [40], researchers have shown that the bound can actually be reached in certain eavesdropping strategies, and that different eavesdropping strategies yield ‘different numbers of guesses, sometimes even completely subversive differences, to get the final key’. Thus the level in the $\varepsilon$-security should be carefully chosen, in order to guarantee the security of the keys. In our paper, what we have attained includes two main results: to upper bound the guessing probability via observables and to build an efficient guessing-probability-based relation applicable in security analysis. In the infinite-length limit, the bound is obtained in terms of error rates, instead of the trace distance, and the guessing-probability-based relation is rather efficient in determining the maximally tolerable error rates, as already shown in the previous sections. We shall consider finite-length cases in future studies. We expect that the finite-length guessing probability may also be upper bounded by some function of parameters in the $\varepsilon$-security.

The method we have used in this paper applies to any QKD protocols in which Alice’s measuring settings are concurrent with Bob’s specified in section 2.2.1. It cannot directly apply to protocols using the Bell inequality [15], since Alice and Bob must perform Bell tests [41] and the Hilbert dimensions are usually unknown. To evaluate the guessing probability, a well received way is to redefine $P_{\text{h}}$ and $P_{\text{g}}$ as certain forms of Bell correlations. For instance, in [42–44] where researchers consider security issues with a monogamous relation of nonlocal correlations, the guessing probability, or success probability, is a probabilistic form of the Bell–Clauser–Horne–Shimony–Holt inequality [45]. The $P_{\text{h}} > P_{\text{g}}$ relation, however, cannot imply $R > 0$. In reference [46], the device-independent QKD [15, 47–49] is investigated with various Bell inequalities. Their definition of the guessing probability is similar to ours (see equation (18) in [46]) but bounded in terms of Bell violations. It is thus very worthwhile to study the guessing probability in device-independent protocols subsequently. Finally, due to noise and finite-length effects, the evaluation of probabilities may be non-ideal. One may resort to the law of large numbers to characterize the non-idealness. Suppose the ideal and actual distributions are denoted by $P^n$ and $Q^n$, respectively, where $n$ is the length of the generated key, and $P^n$ is an independent and identical distribution. Then, according to the law of large numbers, one can have $\text{Pr}[|P^n - Q^n| > \gamma] \leq 2^{-nD}$ [50], where
\[ \| P^n - Q^n \|_1 := \sum_x | P^n(x) - Q^n(x) | \] denotes the \( L_1 \) distance, and \( D = \frac{\gamma}{2 \ln 2} - d \times \frac{\ln(n+1)}{n} \). Equivalently, letting \( 2^{-nD} = \epsilon \), one gets \( \gamma = \left( \frac{2 \ln 2}{n} \left( \log_2 \frac{\gamma}{\epsilon} - d \times \log_2 \frac{1}{\epsilon} \right) \right)^{1/2} \). That is, the probability that the actual distribution deviates from the ideal one with a degree larger than \( \gamma \) is no larger than \( \epsilon \).

Acknowledgments

The author is very grateful to the referees for giving helpful comments on the results, and suggesting to note several relevant references. The study is supported by the National Natural Science Foundation of China (Grant No. 11905209). The author also acknowledges support from the National Natural Science Foundation of China (Grant Nos. 11875050 and 12088101), the NSAF (Grant No. U1930403), and the Fundamental Research Funds for the Central Universities (Grant Nos. 3072022TS2503 and 3072022CFJ2502).

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

ORCID iDs

Hong-Yi Su @ https://orcid.org/0000-0001-7233-7014

References

[1] Shannon C E 1949 Communication theory of secrecy systems “ Bell Syst. Tech. J. 28 656–715
[2] Alimomeni M and Safavi-Naini R 2012 Int. Conf. Information Theoretic Security (Springer) pp 1–13
[3] Issa I and Wagner A B 2017 Measuring securty by the probability of a successful guess IEEE Trans. Inf. Theory 63 3783
[4] König R, Renner R and Schaffner C 2009 The operational meaning of min- and max-entropy IEEE Trans. Inf. Theory 55 4337–47
[5] Yuen H P 2016 Security of quantum key distribution IEEE Access 4 724
[6] Wang X-B, Wang J-T, Qin J-Q, Jiang C and Yu Z-W 2020 Guessing probability in quantum key distribution npj Quantum Inf. 6 45
[7] Branciard C, Gisin N, Kraus B and Scarani V 2005 Security of two quantum cryptography protocols using the same four qubit states Phys. Rev. A 72 032301
[8] Bae J and Acín A 2007 Key distillation from quantum channels using two-way communication protocols Phys. Rev. A 75 012334
[9] Helstrom C W 1976 Quantum Detection and Estimation Theory (New York: Academic)
[10] Maurer U M 1993 Secret key agreement by public discussion from common information IEEE Trans. Inf. Theory 39 733–42
[11] Bae J, Hwang W-Y and Han Y-D 2011 No-signaling principle can determine optimal quantum state discrimination Phys. Rev. Lett. 107 170403
[12] Bae J and Hwang W-Y 2013 Minimum-error discrimination of qubit states: methods, solutions, and properties Phys. Rev. A 87 012334
[13] Bae J 2013 Structure of minimum-error quantum state discrimination New J. Phys. 15 073037
[14] Bennett C H and Brassard G 1984 1984 Proc. IEEE Int. Conf. Computers, Systems and Signal Processing (Bangalore, India) (New York: IEEE) pp 175–9
[15] Ekert A K 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661
[16] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 Theory of Cryptography Conf. (Berlin: Springer) pp 386–406
[17] Renner R and König R 2005 Theory of Cryptography Conf. (Springer) pp 407–25
[18] Renner R 2005 Security of quantum key distribution PhD Thesis ETH Zurich
[19] Renner R 2008 Security of quantum key distribution Int. J. Quantum Inf. 06 1
[20] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys. 74 145
[21] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution Rev. Mod. Phys. 81 1301
[22] Lo H-K, Curty M and Tamaki K 2014 Secure quantum key distribution Nat. Photon. 8 595–604
[23] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 Practical challenges in quantum key distribution npj Quantum Inf. 2 160025
[24] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 Secure quantum key distribution with realistic devices Rev. Mod. Phys. 92 025002
[25] Albert D Z 1983 On quantum-mechanical automata Phys. Lett. A 98 249–52
[26] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 Tight finite-key analysis for quantum cryptography Nat. Commun. 3 634
[27] Bihem E and Mor T 1997 Security of quantum cryptography against collective attacks Phys. Rev. Lett. 78 2256
[28] Bihem E, Boyer M, Brassard G, van de Graaf J and Mor T 2005 Security of quantum key distribution against all collective attacks Algorithmica 44 372–88
[29] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction Phys. Rev. A 54 3824–51
[30] Su H-Y 2020 Simple analysis of security of the BB84 quantum key distribution protocol Quantum Inf. Process. 19 169
[31] Kraus B, Gisin N and Renner R 2005 Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication Phys. Rev. Lett. 95 080501
[32] Renner R, Gisin N and Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols Phys. Rev. A 72 012332
[33] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol Phys. Rev. Lett. 85 441
[34] Devetak I and Winter A 2005 Distillation of secret key and entanglement from quantum states Proc. R. Soc. A 461 207–35
[35] Holevo A S 1973 Bounds for the quantity of information transmitted by a quantum communication channel Prob. Peredachi Inf. 9 3–11
[36] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 Device-independent quantum key distribution secure against collective attacks New J. Phys. 11 045021
[37] Lo H-K 2001 Proof of unconditional security of six-state quantum key distribution scheme Quantum Inf. Comput. 1 81–94
[38] Portmann C and Renner R 2014 Cryptographic security of quantum key distribution (arXiv:1409.3525)
[39] Portmann C and Renner R 2021 Security in quantum cryptography (arXiv:2102.00021)
[40] Li H-W, Shi J-H, Cai Q-Y and Sun C-P 2022 Estimating security of the quantum key distribution from the guesswork Quantum Inf. Process. 21 142
[41] Bell J S 1964 On the Einstein Podolsky Rosen paradox Phys. Phys. Fiz. 1 195–200
[42] Pawłowski M 2010 Security proof for cryptographic protocols based only on the monogamy of Bell’s inequality violations Phys. Rev. A 82 032313
[43] Hwang W-Y and Gittsovich O 2012 Comment on ‘security proof for cryptographic protocols based only on the monogamy of Bell’s inequality violations’ Phys. Rev. A 85 046301
[44] Pawłowski M 2012 Reply to comment on ‘security proof for cryptographic protocols based only on the monogamy of Bell’s inequality violations’ Phys. Rev. A 85 046302
[45] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories Phys. Rev. Lett. 23 880
[46] Masanes L, Pironio S and Acín A 2011 Secure device-independent quantum key distribution with causally independent measurement devices Nat. Commun. 2 238
[47] Mayers D and Yao A 1998 1998 Proc. 39th Annual Symp. Foundations of Computer Science (FOCS ’98) (Palo Alto, CA) (Washington, DC: IEEE Computer Society) pp 503–9
[48] Barrett J, Hardy L and Kent A 2005 No signaling and quantum key distribution Phys. Rev. Lett. 95 010503
[49] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Device-independent security of quantum cryptography against collective attack Phys. Rev. Lett. 98 230501
[50] McWilliams F J and Sloane N J A 1981 The Theory of Error-Correcting Codes (Amsterdam: North-Holland)