RESEARCH ARTICLE | PHYSICS

Quantum key distribution with correlated sources

Margarida Pereira[1,*], Go Kato[2], Akihiro Mizutani[3], Marcos Curty[1] and Kiyoshi Tamaki[4,*]

+ See all authors and affiliations

Science Advances 09 Sep 2020:
Vol. 6, no. 37, eaaz4487
DOI: 10.1126/sciadv.aaz4487

Article Figures & Data Info & Metrics eLetters PDF

PDF

Help

Abstract

In theory, quantum key distribution (QKD) offers information-theoretic security. In practice, however, it does not due to the discrepancies between the assumptions used in the security proofs and the behavior of the real apparatuses. Recent years have witnessed a tremendous effort to fill the gap, but the treatment of correlations among pulses has remained a major elusive problem. Here, we close this gap by introducing a simple yet general method to prove the security of QKD with arbitrarily long-range pulse correlations. Our method is compatible with those security proofs that accommodate all the other typical device imperfections, thus paving the way toward achieving implementation security in QKD with arbitrary flawed devices. Moreover, we introduce a new framework for security proofs, which we call the reference

Quantum key distribution (QKD) allows two distant parties, Alice and Bob, to securely exchange cryptographic keys in the presence of an eavesdropper, Eve (*1*). Despite notable progress made in recent years, there is still a big gap between the information-theoretic security promised by the security proofs and the actual security offered by the practical implementations of QKD. The most pressing problem is the discrepancy between the idealized device models used in the security proofs and the functioning of the real devices used in the experiments. This is so because typical security proofs rely on assumptions to describe the behavior of these devices and ignore their inherent imperfections. In practice, any deviation from these theoretical models might open security loopholes that could lead to side-channel attacks, thus compromising the security of QKD. A possible solution to this problem is to construct more realistic security proofs that can take into account device flaws. Lately, there have been notable advances in this direction. This includes, e.g., the proposal of the decoy-state method (*2*–*4*), allowing the use of practical light sources while maintaining a high secret key rate. In addition, measurement device–independent QKD (MDI-QKD) (*5*) can effectively eliminate all detector side channels and is practical with the current technology (*6*–*11*). The missing step toward achieving implementation security in QKD is to better characterize and secure the parties' sources.

Security loopholes in the source could emerge from three main causes: from state preparation flaws (SPFs) due to the finite precision of the modulation devices, from information leakage either due to side channels arising from mode dependencies or due to Trojan horse attacks (THAs) (*12*–*16*), or they could be caused by undesired classical correlations between the generated pulses. Mode dependencies of the emitted signals occur when the optical mode of a pulse depends on Alice's setting choices. That is, Alice's setting choices might be encoded in various degrees of freedom of the generated signals, not only on the desired one. Moreover, Eve can perform a THA by send bright light into the source and then observing the back-reflected light to obtain partial inform about Alice's internal settings. Last, pulse correlations imply that the state of each pulse depends on the previous setting choices, such as bit and basis choices.

SPFs can be efficiently treated with the original loss-tolerant (LT) protocol (*17*). This is so because in this scheme, the resulting secret key rate is almost independent of the source's flaws. Its main drawback is the requirement that the states of the pulses are described by qubit states, which is hard to guarantee in practice because of unavoidable potential side channels. To address this limitation, a generalization of the LT protocol was put forward recently (*18*). This latter protocol encompasses SPFs, mode dependencies, and THAs without requiring detailed information about the state of the side channels, which simplifies their experimental characterization. There are also other techniques that can deal with mode dependencies and THAs, such as the Gottesman-Lo-among the emitted signals. These pulse correlations are purely classical, and they arise from the limitations of practical modulators. In general, due to memory effects of these modulation devices, the state of a pulse depends not only on the current modulation setting but also on the previous ones, meaning that the secret key information, i.e., the bit and the basis choices, is encoded not only into a single pulse but also between subsequent pulses. Theoretically, it is believed that this correlation is very hard to model because the dimensionality of the state space becomes very large. All existing security proofs circumvent this imperfection by simply neglecting it, which means that they cannot guarantee the security of practical implementations. We remark that a few recent works (25–27) have incorporated in their analysis certain pulse correlations between the emitted signals. However, all these works only consider restricted scenarios. In particular, the results in (25, 26) and in (27) only consider setting choice–independent pulse correlations and intensity correlations between neighboring pulses, respectively. Therefore, none of them can deal with pulse correlations in terms of the secret key information nor with long-range correlations. Another reason why these correlations have been ignored so far is because one expects that, in practice, they are small. However, a small imperfection does not necessarily mean a small impact on the secret key rate, as Eve could, in principle, enhance such imperfection by exploiting, say, channel loss, resulting in a poor secret key rate (19–21). Therefore, we note that pulse correlations could be a serious threat to the security of QKD.

Here, we present a general and simple framework to guarantee the security of QKD in the presence of arbitrary classical pulse correlations. The key idea is very easy yet very useful, that is, we regard the leaked information encoded into the correlations of subsequent pulses as a side channel for each of the pulses. The key features of our method include the following: (i) When combined with the generalized LT (GLT) protocol (18) or with the reference technique (RT) introduced in this can analytically guarantee the security of QKD with practical devices that suffer from typical imperfections, i.e., SPFs and side channels (including mode dependencies, THAs, and pulse correlations), even if the state of the side channels is totally unknown; (ii) due to its simplicity, our method is compatible with many other security proofs including those based on the inner product structure of the emitted pulses such as, for instance, the GLLP type security proofs (19–21) and the numerical techniques in (22–24); and (iii) our method can be applied to many QKD protocols such as, e.g., the BB84 scheme (28), the six-state protocol (29), the SARG04 protocol (30), distributed-phase-reference protocols (31–33), and MDI-QKD (5). Our results indicate the feasibility of secure QKD with arbitrary flawed devices, and therefore, they constitute an essential step toward closing the big gap between theory and practice in QKD.

PDF Help

which are close to the actual states prepared by the protocol of interest, and use them to simplify the estimation of the parameters needed to guarantee the security of the protocol. More precisely, by bounding the maximum deviation between the probabilities associated with the reference states and those associated with the actual states, one can obtain a relationship for the probabilities involving the actual states based on those of the reference states. In doing so, one can estimate the parameters needed to guarantee the security of the actual protocol from the estimation that uses the reference states. We remark that the freedom to choose the reference states is very useful when dealing with source imperfections. In particular, this freedom allows us to analytically prove the security of a QKD protocol without any information on the side-channel states. This is important for achieving implementation security since a full characterization of the side-channel states, which, in principle, could live in unknown physical modes, is certainly very challenging in practice. In this work, we consider three special cases of the RT and evaluate their secret key rate in the presence of pulse correlations and SPFs.

RESULTS

Pulse correlations occur, for instance, when the emitted signals depend on the previous values of the encoding device (e.g., a phase modulator). In other words, subsequent pulses leak information about Alice's former encoding choices. The key idea of our work to evaluate this complex scenario is to interpret these correlations as a side channel. By realistically modeling the source, we can bound this passive leakage of information and ensure secure QKD after performing enough privacy amplification. In what follows, we first outline the assumptions used in our security analysis, which is presented afterwards.

PDF
Help

Assumptions on Alice's and Bob's devices

For simplicity, we consider a three-state protocol in which modulation devices are used to encode the bit and the basis choices. We do not explicitly consider the use of the decoy-state method (*2*–*4*); however, we remark that our framework could be combined with that method and also incorporate the effect of correlated intensity modulators and other imperfections of the intensity modulators (*15*). Furthermore, we assume an asymptotic scenario where Alice sends Bob an infinite number of pulses. We note, however, that the work presented here also applies to other protocols that use more than three states, as discussed in the next section.

Additional assumptions might be required depending on the particular security proof technique that is combined with our method. For instance, if the RT based on the GLT protocol (*18*) or the RT based on the original LT protocol (*17*), which we will present below, are used, then one also needs to

$$|\psi_j\rangle_{C_kB_kE} = \sqrt{a_j}|\phi_j\rangle_{C_kB_k}|\lambda\rangle_E + \sqrt{1-a_j}|\phi_j^\perp\rangle_{C_kB_kE}$$

Here, we take a_j as a non-negative number satisfying $0 \le a_j \le 1$, which is possible by appropriately choosing the global phase of the states. The subscript C_kB_kE stands for all the systems, which include not only the k^{th} qubit (system B_k) that Alice sends to Bob over the quantum channel but also the system C_k, which is needed for purifying the state of system B_k, and E is a system that includes Eve's system. System E includes the systems sent by Alice over the quantum channel, such as the back-reflected light from a possible THA and the ancilla systems kept in Eve's laboratory. As we will discuss further later, in general, this system also includes Alice's ancilla systems used in the virtual entanglement-based protocol, which is equivalent to the actual protocol. Some of the latter systems store the setting information for all the pulses sent before the k^{th} pulse. This means, in particular, that $|\lambda\rangle_E$ could depend on the setting choices for all the previous pulses. If it is not possible to find such a state, then a_j becomes simply zero. From construction, **Eq. 1** is the most general state that can be prepared in a QKD protocol. In other words, **Eq. 1** simply decomposes a state $|\psi_j\rangle_{C_kB_kE}$ in a given Hilbert space into two states, each of which belongs to an orthogonal space. Precisely, one of them is the qubit state $|\phi_j\rangle_{C_kB_k}|\lambda\rangle_E$ (as the set of states $\{|\phi_j\rangle_{C_kB_k}|\lambda\rangle_E\}_j$ constitutes a qubit space), with $|\lambda\rangle_E$ being a state independent of the k^{th} setting choice, and the other is the setting-dependent side-channel state $|\phi_j^\perp\rangle_{C_kB_kE}$ that corresponds to unwanted and possibly unknown modes. This decomposition can always be done for an appropriate choice of a_j with $0 \le a_j \le 1$. The characterization of $|\phi_j^\perp\rangle_{C_kB_kE}$ is not required for the RT, and, in particular, no relationships between the states $|\phi_j^\perp\rangle_{C_kB_kE}$ and $|\phi_{\tilde{j}}^\perp\rangle_{C_kB_kE}$ and between $|\phi_j\rangle_{C_kB_kE}$ and $|\phi_{\tilde{j}}^\perp\rangle_{C_kB_kE}$ for $j \neq \tilde{j}$ are required, where $\widetilde{j}$ represents a different setting choice to j. To use the RT, we only need to know a lower bound on the coefficient a_j in **Eq. 1** and a full characterization of the density operator of the q The main contribution of our work is to show that one can accommodate the effect of pulse correlations through the parameter a_j in **Eq. 1**.

The assumptions on Bob's devices also depend on the security proof. For example, in the case of the RT based on the GLT protocol or based on the original LT protocol, one assumes that Bob measures the incoming pulses in the Z or the X basis. More precisely, Bob's measurements are represented by the positive operator–valued measures (POVMs) $\{\widehat{m}_{0_Z}, \widehat{m}_{1_Z}, \widehat{m}_f\}$ and $\{\widehat{m}_{0_X}, \widehat{m}_{1_X}, \widehat{m}_f\}$, respectively. Here, $\widehat{m}_{\alpha\beta}$ corresponds to Bob obtaining the bit value $\alpha \in \{0,1\}$ when selecting the basis $\beta \in \{Z, X\}$, and $\widehat{m}_f$ is associated with an inconclusive outcome. That is, we assume that these measurements satisfy the basis-independent efficiency condition, i.e., we impose that the operator $\widehat{m}_f$ is the same for both basis. Note that this condition is usually used in security proofs to remove detector side-channel attacks exploiting channel loss (*34*, *35*); however, it is not

In this section, we present the security analysis of QKD with pulse correlations. For this, we consider a security proof with the following properties. It uses an entanglement-based virtual protocol where Alice prepares pulses in an entangled state, and she (Bob) measures the local (incoming) systems to distill a secret key. In addition, it considers a particular detected pulse to estimate the phase error rate (or the phase error rate as a bound of the min-entropy). For simplicity, in what follows, we shall explicitly mention only the phase error rate, but it applies to both cases. Security against coherent attacks can then be guaranteed with the help of Azuma's inequality (*37*), Kato's inequality (*38*), or by applying the techniques in (*39*, *40*). Moreover, we assume that the security proof can be generalized such that it applies to a particular pulse with a side channel. That is, it can be used to prove the security of QKD in the presence of active and/or passive information leakage. Thanks to the reduction technique presented below, a particular pulse affected by correlations can be regarded as a pulse with a side channel, and therefore, the security of QKD with pulse correlations is guaranteed. As an example, we now demonstrate that running a three-state protocol in the presence of nearest-neighbor pulse correlations can be regarded as a three-state protocol in which each of the pulses entails side channels. We emphasize, however, that it is straightforward to generalize this reduction technique to an m-state protocol, as discussed below, and to arbitrarily long-range correlations (see Materials and Methods for more details).

Nearest-neighbor pulse correlations. Let $\{|\psi_j\rangle_{\mathrm{B}}\}_{j=0_{\mathrm{Z}},1_{\mathrm{Z}},0_{\mathrm{X}}}$ be the set of three quantum states used in the three-state protocol. We assume that Alice chooses $|\psi_j\rangle_B$ with probability p_j and sends the pulse prepared in the chosen state to Bob over the quantum channel. As for Bob's measurements, as already mentioned above, the assumptions vary according to the selected security proof. In an entanglement-based picture with nearest-neighbor pulse correlations, the transmission of n pulses by Alice can be described by first preparing n ancilla systems A and n pulses in the state

PDF
Help

$$|\Psi\rangle_{\mathrm{AB}} = \sum_{j_1} |j_1\rangle_{A_1} |\psi_{j_1}\rangle_{B_1} \sum_{j_2} |j_2\rangle_{A_2} |\psi_{j_2|j_1}\rangle_{B_2} \cdots \sum_{j_n} |j_n\rangle_{A_n} |\psi_{j_n|j_{n-1}}\rangle_{B_n} \quad (2)$$

and then by sending system B to Bob. In **Eq. 2**, $A = A_1, A_2, \ldots, A_n$ ($B = B_1, B_2, \ldots, B_n$) refers to the composite system of Alice's ancilla systems (Bob's pulses), where A_k (B_k) for $k \in \{1,2, \ldots, n\}$ denotes Alice's k^{th} ancilla system (Bob's k^{th} pulse), the index $j_k \in \{0_Z,1_Z,0_X\}$, and $\{|j_k\rangle_{A_k}\}_{j_k \in \{0_Z,1_Z,0_X\}}$ is a set of unnormalized orthogonal states in a three-dimensional Hilbert space with $\||j_k\rangle_{A_k}\| = \sqrt{p_{j_k}}$, e.g., $\||0_Z\rangle_{A_k}\| = \sqrt{p_{0_Z}}$. Importantly, $|\psi_{j_k|j_{k-1}}\rangle_{B_k}$ represents any nearest-neighbor classical pulse correlation, namely, this is the state of the k^{th} emitted pulse when Alice selects the setting j_k, given that her previous setting choice was j_{k-1}.

on the pulses received by Bob, commute with Alice's measurements. Hence, we can assume that Alice has already measured her first $k - 1$ ancillas before sending system B. Then, we have the resulting state as

$$|j_1'\rangle_{A_1}|\psi_{j_1'}\rangle_{B_1}\cdots|j_{k-1}'\rangle_{A_{k-1}}|\psi_{j_{k-1}'|j_{k-2}'}\rangle_{B_{k-1}}\sum_{j_k}|j_k\rangle_{A_k}|\psi_{j_k|j_{k-1}'}\rangle_{B_k}$$
$$\otimes\sum_{j_{k+1}}|j_{k+1}\rangle_{A_{k+1}}|\psi_{j_{k+1}|j_k}\rangle_{B_{k+1}}\cdots\sum_{j_n}|j_n\rangle_{A_n}|\psi_{j_n|j_{n-1}}\rangle_{B_n} \tag{3}$$

where j_1', ⋯, j'_{k-1} represent the outcomes of Alice's measurement on her first $k - 1$ ancillas. To simplify this state, we introduce the following definition

$$|j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n} := |j_{k+1}\rangle_{A_{k+1}}\sum_{j_{k+2}}|j_{k+2}\rangle_{A_{k+2}}|\psi_{j_{k+2}|j_{k+1}}\rangle_{B_{k+2}}\cdots\sum_{j_n}|j_n\rangle_{A_n}|\psi \tag{4}$$

which forms a set of orthogonal bases as $\{|j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n}\}_{j_{k+1}=0_Z,1_Z,0_X}$. In addition, we define the state

$$|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n} := \sum_{j_{k+1}}|j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n}|\psi_{j_{k+1}|j_k}\rangle_{B_{k+1}} \tag{5}$$

By using the above two states, we can rewrite **Eq. 3** as

$$|j_1'\rangle_{A_1}|\psi_{j_1'}\rangle_{B_1}\cdots|j_{k-1}'\rangle_{A_{k-1}}|\psi_{j_{k-1}'|j_{k-2}'}\rangle_{B_{k-1}}\sum_{j_k}|j_k\rangle_{A_k}|\psi_{j_k|j_{k-1}'}\rangle_{B_k}|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots} \tag{6}$$

As a reference, recall that if there were no pulse correlations in the three-state protocol, then the resulting state, instead of being in the form given by **Eq. 6**, would become

$$|j_1'\rangle_{A_1}|\psi_{j_1'}\rangle_{B_1}\cdots|j_{k-1}'\rangle_{A_{k-1}}|\psi_{j_{k-1}'}\rangle_{B_{k-1}}\sum_{j_k}|j_k\rangle_{A_k}|\psi_{j_k}\rangle_{B_k}|\lambda\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n} \tag{7}$$

In the security proof for the three-state protocol without pulse correlations, one typically obtains the phase error rate by considering any attack on system B_k in $\sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k}\rangle_{B_k}$ in **Eq. 7**. On the other hand, when there are nearest-neighbor pulse correlations, one can see from **Eq. 6** that Alice's information j_k is encoded not only on system B_k but also on the systems $B_{k+1}, \cdots, B_n$, and the state $|\lambda_{j_k}\rangle_{A_{k+1}, \cdots, A_n, B_{k+1}, \cdots, B_n}$, serves as side-channel information about the state $|\psi_{j_k|j'_{k-1}}\rangle_{B_k}$. This suggests that if we obtain the phase error rate for the composite systems B_k and $B_{k+1}, \cdots, B_n$ in $\sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k|j'_{k-1}}\rangle_{B_k} |\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}$, then the security follows. In other words, the three-state protocol with pulse correlations can be simply regarded as a three-state protocol where Alice prepares the states $\{|\psi_{j_k|j'_{k-1}}\rangle_{B_k} |\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}\}_{j_k \in \{0_Z, 1_Z, 0_X\}}$ for any k and sends systems B_k, $B_{k+1}, \cdots, B_n$ to Bob.

Note that our framework is also valid for the case where Alice emits mixed states instead of pure states. The emission of mixed states might happen because of imperfections in Alice's devices or when the prepared pure states are entangled with Eve's systems because of, say, a THA. To treat this latter scenario, the mixed states can be purified by introducing an ancilla system C_k, with $k \in \{1,2, \cdots, n\}$, which contains Alice's and Eve's systems. As a result, **Eq. 6** becomes

$$|j'_1\rangle_{A_1} |\psi_{j'_1}\rangle_{C_1 B_1} \cdots |\, j'_{k-1}\rangle_{A_{k-1}} |\psi_{j'_{k-1}|j'_{k-2}}\rangle_{C_{k-1}B_{k-1}} \sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k|j'_{k-1}}\rangle_{C_k B_k} |\lambda_{j_k}\rangle_{A_{k+1},\cdots,} \tag{9}$$

Again, if a security proof for the three-state protocol without pulse correlations shows that or estimate the phase error rate for $\Sigma_{jk}|j_k\rangle_{A_k}|\Psi_{j_k}\rangle_{C_k B_k}$, then it follows that $\sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k|j'_{k-1}}\rangle_{C_k B_k} |\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,C_{k+1}B_{k+1},\cdots,C_n B_n}$ is also secure if one can obtain the parameters needed for the security proof given these latter states. Furthermore, we remark that only for the purpose of estimating the phase error rate, in some cases, it may make the mathematical analysis simpler to fictitiously consider an arbitrary attack on the systems $A_{k+1}, \cdots, A_n$ (which, in reality, are inaccessible by Eve) besides the composite systems B_k and $B_{k+1}, \cdots, B_n$. Note that the number of systems that we include as side channels does not matter, but what matters is how much the state $|\lambda_{j_k}\rangle_{A_{k+1}, \cdots, A_n, B_{k+1}, \cdots, B_n}$ depends on Alice's information j_k. Therefore, this fictitious attack on $A_{k+1}, \cdots, A_n$ should not result, in general, in a lower key rate because these ancillas do not directly entail information about j_k.

PDF
Help

Having stated the framework for the security proof in the presence of pulse correlations, we now consider a particular device model with only nearest-neighbor pulse correlations. The purpose of this section is to show how to obtain the parameters needed in **Eq. 1** for a particular example of device model. Once this is achieved, one can directly apply the RT to guarantee the security of practical QKD implementations. We remark that for simplicity, below, we do not consider THAs or mode dependencies. However, they could readily be included by using the method in (*18*). In addition, we assume that a single-photon source is available, and as a concrete example for modeling pulse correlations, we select the following instance of nearest-neighbor pulse correlation

$$|\psi_{j_k|j'_{k-1}}\rangle_{B_k} = \sqrt{1-\epsilon}|\phi_{j_k}\rangle_{B_k} + e^{i\theta_{j_k|j'_{k-1}}}\sqrt{\epsilon}|\phi^{\perp}_{j_k}\rangle_{B_k} \tag{10}$$

for the three states. Here, $|\psi_{j_k|j'_{k-1}}\rangle_{B_k}$ is a single-photon state living in a qubit space with $j_k \in \{0_Z, 1_Z, 0_X\}$, $|\phi_{j_k}\rangle_{B_k}$ is a qubit state, the parameter ϵ intuitively quantifies the strength of the correlation, $\theta_{j_k \mid j'_{k-1}}$ represents how the k^{th} state depends on the previous information j'_{k-1}, and $|\phi^{\perp}_{j_k}\rangle_{B_k}$ is a state, in the same qubit space, that is orthogonal to $|\phi_{j_k}\rangle_{B_k}$. Note that, when there are no pulse correlations, i.e., $\epsilon = 0$, the state $|\psi_{j_k|j'_{k-1}}\rangle_{B_k}$ becomes the perfect state $|\phi_{j_k}\rangle_{B_k}$, which does not depend on the previous setting j'_{k-1}. However, in the presence of pulse correlations, i.e., when $\epsilon > 0$, the overall state $\left|\psi_{j_k|j'_{k-1}}\right\rangle_{B_k}$ diverges from the ideal state $|\phi_{j_k}\rangle$, since it becomes dependent on the previous setting choice. The physical intuition of this model derives from the functioning of a phase modulator. To be precise, the state of an emitted pulse is typically affected by the modulation of the previous pulses such that there is a deviation depending on its preselected phase, which is quantified in the example given in **Eq. 10** by $\theta_{j_k|j'_{k-1}}$.

Below, we show how to derive the state in the form of **Eq. 1** for this particular example starting **Eq. 10**. For this, we follow the idea introduced in the previous section and obtain the states $|\psi_{j_k|j'_{k-1}}\rangle_{B_k}|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}$ given by **Eq. 6**. By using **Eq. 10**, we have that

PDF
Help

$$\otimes \sum_{j_{k+1}} |j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n} \left(\sqrt{1-\epsilon}|\phi_{j_{k+1}}\rangle_{B_{k+1}} + e^{i\theta_{j_{k+1}|j_k}} \sqrt{\epsilon}|\phi^{\perp}_{j_{k+1}}\rangle_{B_{k+1}} \right)$$

$$=: (1-\epsilon)|\phi_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n} + \sqrt{1-(1-\epsilon)^2}|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B}$$

where

$$|\phi_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n} = |\phi_{j_k}\rangle_{B_k} \sum_{j_{k+1}} |j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n} |\phi_{j_{k+1}}\rangle_{B_{k+1}} \qquad (12)$$

is a qubit state (note that the set $\{|\phi_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}\}_{j_k\in\{0_Z,1_Z,0_X\}}$ spans a two-dimensional space) since $\sum_{jk+1}|jk+1\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n}|\phi_{jk+1}\rangle_{B_{k+1}}$ is a normalized state independent of the information j_k, and $|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}$ is a state orthogonal to this qubit state. The explicit form of $|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}$ is omitted here for simplicity, but it could be straightforwardly obtained from **Eq. 11**. We can regard our protocol as a protocol that uses the states in **Eq. 11** rather than the ideal states $|\phi_{j_k}\rangle_{B_k}$ for any k. We emphasize once again that the parameter ϵ and the state $|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}$ in **Eq. 11** represent most of the source imperfections (i.e., SPFs, mode dependencies, and THAs could be incorporated in a state of the form given by **Eq. 11**) (*18*), not only pulse correlations. This comes from the generality of **Eq. 1**.

Now, our formalism to deal with pulse correlations can be used directly with the RT since the in **Eq. 11** are in the form of **Eq. 1**. For the RT (described in the next section), we only require t a lower bound on the coefficient $1-\epsilon$ and a full characterization of the state $|\phi_{j_k}\rangle_{B_k}$. We rem however, that this framework can also be applied to the numerical techniques in (*22*–*24*) if, in addition, the form of the state $|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}$ is known or if bounds involving the inner products ${}_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}\langle\phi^{\perp}_{j_k|j'_{k-1}} \mid \phi^{\perp}_{\tilde{j}_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}$ and ${}_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}\langle\phi_{j_k|j'_{k-1}} \mid \phi^{\perp}_{\tilde{j}_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}$ for $j_k \neq \tilde{j}_k$ can be estimated, where $\tilde{j}_k$ represents a different setting choice to j_k.

PDF

Help

Here, we restricted the discussion to the case of nearest-neighbor pulse correlations, but our analysis also applies to arbitrarily long-range correlations. For instance, these correlations could be characterized by by ϵ_{k-w}, where $k-w$ is the range of the correlation, by looking at the distinguishability of the states. Here, $k-w$ can be any non-negative number, meaning that our method can incorporate arbitrary long-range correlations. One can show that from this model, it is straightforward to obtain the three states in the form given by Eq. 1 (see Materials and Methods) and consequently apply the RT.

RT based on the original LT protocol

In this section, we introduce a new framework for security proofs, the RT, which results in a high secret key rate in the presence of source imperfections. In what follows, we outline the intuition behind the key idea of the RT by applying it to the original LT protocol (17). A full description of the RT, including the detailed security proof, is presented in Materials and Methods. To simplify the discussion, here, we shall assume collective attacks; however, our analysis can be generalized to coherent attacks (see Materials and Methods for more details). Only as an example, we consider a protocol with a single-photon source in the presence of side-channel information, such as pulse correlations, in which Alice prepares the following three states for each pulse emission

$$|\psi_{j_k|j'_{k-1}}\rangle_B = (1-\epsilon)|\phi_{j_k}\rangle_B + \sqrt{1-(1-\epsilon)^2}|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_B \tag{14}$$

where B denotes the system to be sent to Bob. We remark that this subscript B could be replaced with $A_{k+1}, \cdots, A_n, B_k, B_{k+1}, \cdots, B_n$ and then we would recover Eq. 11. However, in this section, we prefer to use Eq. 14 rather than Eq. 11 for simplicity of notation. Note that, here, we analyze the case of nearest-neighbor pulse correlations, but the RT is also applicable to arbitrary long-range pulse correlations. In Eq. 14, $|\phi_{j_k}\rangle_B$ is a qubit state while $|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_B$ corresponds to the side-channel state for $j_k \in \{0_Z, 1_Z, 0_X\}$ that lives in any dimensional Hilbert space and is orthogonal to $|\phi_{j_k}\rangle_B$ for ea setting choice j_k. However, we do not assume any relationship between $|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_B$ and $|\phi^{\perp}_{\tilde{j}_k|j'_{k-1}}\rangle_B$ $j_k \neq \tilde{j}_k$. For instance, $|\phi_{j_k}\rangle_B$ can be defined as in (18) such that

PDF

Help

$$\begin{aligned}
|\phi_{0_Z}\rangle_B &= |0_Z\rangle_B, \\
|\phi_{1_Z}\rangle_B &= -\sin\left(\tfrac{\delta}{2}\right)|0_Z\rangle_B + \cos\left(\tfrac{\delta}{2}\right)|1_Z\rangle_B, \\
|\phi_{0_X}\rangle_B &= \cos\left(\tfrac{\pi}{4}+\tfrac{\delta}{4}\right)|0_Z\rangle_B + \sin\left(\tfrac{\pi}{4}+\tfrac{\delta}{4}\right)|1_Z\rangle_B
\end{aligned} \tag{15}$$

where $\{|0_Z\rangle, |1_Z\rangle\}$ is a qubit basis and $\delta(\geq 0)$ is the deviation of the phase modulation from the intended value due to SPFs (18). That is, when there is no side-channel information, the states of the single photons sent by Alice have the form given by Eq. 15, but in the presence of side-channel information, however, these states are defined by Eqs. 14 and 15.

actual states by slightly modifying the relationship for the reference states. Note that the choice of reference states is, in principle, infinite; however, for higher secret key rates, they should be linearly dependent states such that unambiguous state discrimination (*41*, *42*) is not possible. This allows us to use directly the original LT protocol (*17*) to estimate precisely some quantities associated with the reference states and their relationship as an intermediate step toward obtaining the phase error rate associated with the actual states.

As an example, we select the reference states to be $\{|\phi_{0_Z}\rangle_B, |\phi_{1_Z}\rangle_B, |\phi_{0_X}\rangle_B\}$, which are defined in **Eq. 15** and that correspond to the qubit part of the actual states in **Eq. 14**. In addition, we fictitiously consider that Alice chooses the reference states with the same probabilities as the actual states. Now, we can apply the RT in the following way. The first step is to find an expression for the probability of a phase error in terms of the reference states, which is a key parameter to be estimated in the security proof. For this, we consider an entanglement-based virtual protocol (see Materials and Methods for further details) using the reference states, where Alice prepares the virtual states

$$|\phi^{\text{vir}}_{\alpha_X}\rangle_B = \frac{|\phi_{0_Z}\rangle_B + (-1)^{\alpha}|\phi_{1_Z}\rangle_B}{\sqrt{2(1+(-1)^{\alpha}{}_B\langle\phi_{0_Z} \mid \phi_{1_Z}\rangle_B)}} \qquad (16)$$

with α ∈ {0,1} and where, for simplicity, we assumed that the selection probabilities in the *Z* basis satisfy $p_{0_Z} = p_{1_Z}$. We can then define the probability of a phase error conditional on the reference states as

$$\begin{aligned} P(\text{ph} \mid \text{Ref}) \coloneqq \;& p^{\text{vir}}_{1_X} p_{Z_B} \text{Tr}[|\,\phi^{\text{vir}}_{1_X}\rangle\langle\phi^{\text{vir}}_{1_X}|_B \widehat{M}_{0_X}] + \\ & p^{\text{vir}}_{0_X} p_{Z_B} \text{Tr}[|\,\phi^{\text{vir}}_{0_X}\rangle\langle\phi^{\text{vir}}_{0_X}|_B \widehat{M}_{1_X}] \end{aligned} \qquad (17)$$

where $p^{\text{vir}}_{\alpha_X} = \frac{1}{2} p_{Z_A}(1+(-1)^{\alpha}{}_B\langle\phi_{0_Z} \mid \phi_{1_Z}\rangle_B)$ is the probability that Alice sends the virtual states defined in **Eq. 16**, $p_{Z_A} \coloneqq p_{0_Z} + p_{1_Z}(p_{Z_B})$ is the probability that Alice (Bob) selects the *Z* basis, and $\widehat{M}_{\alpha_X}$ is Bob's POVM element after any attack by Eve in the actual protocol. That is, $\widehat{M}_{\alpha_X} \coloneqq \sum_{\widetilde{e}} \widehat{K}_{\widetilde{e}} \widehat{m}_{\alpha_X} \widehat{K}^{\dagger}_{\widetilde{e}}$, where $\widehat{K}_{\widetilde{e}}$ is the Kraus operator representing Eve's action in the actual protocol, $\widetilde{e}$ corresponds to her measurement outcome, and $\widehat{m}_{\alpha_X}$ is Bob's POVM element for detecting α$_X$ in the actual protocol. The probabilities $\text{Tr}[|\,\phi^{\text{vir}}_{1_X}\rangle\langle\phi^{\text{vir}}_{1_X}|_B \widehat{M}_{0_X}]$ and $\text{Tr}[|\,\phi^{\text{vir}}_{0_X}\rangle\langle\phi^{\text{vir}}_{0_X}|_B \widehat{M}_{1_X}]$ in **Eq. 17** cannot be directly obtained since they involve reference and virtual

$$
\begin{gathered}
|\phi^{\text{vir}}_{1_X}\rangle\langle\phi^{\text{vir}}_{1_X}|_B = a \mid \phi_{0_Z}\rangle\langle\phi_{0_Z}|_B + b \mid \phi_{1_Z}\rangle\langle\phi_{1_Z}|_B - c \mid \phi_{0_X}\rangle\langle\phi_{0_X}|_B, \\
|\phi^{\text{vir}}_{0_X}\rangle\langle\phi^{\text{vir}}_{0_X}|_B = \mid \phi_{0_X}\rangle\langle\phi_{0_X}|_B
\end{gathered}
\tag{18}
$$

where the coefficients *a*, *b*, and *c* are defined in Materials and Methods. We remark that if there are no SPFs, then the coefficients become *a* = *b* = *c* = 1. Then, by substituting **Eq. 18** into **Eq. 17**, we obtain an expression for the probability of a phase error in terms of the reference states

$$
\begin{aligned}
0 = \quad & p^{\text{vir}}_{1_X} p_{Z_B} a \text{Tr}[\mid \phi_{0_Z}\rangle\langle\phi_{0_Z}|_B \widehat{M}_{0_X}] + \\
& p^{\text{vir}}_{1_X} p_{Z_B} b \text{Tr}[\mid \phi_{1_Z}\rangle\langle\phi_{1_Z}|_B \widehat{M}_{0_X}] + \\
& p^{\text{vir}}_{0_X} p_{Z_B} \text{Tr}[\mid \phi_{0_X}\rangle\langle\phi_{0_X}|_B \widehat{M}_{1_X}] - \\
& [p^{\text{vir}}_{1_X} p_{Z_B} c \text{Tr}[\mid \phi_{0_X}\rangle\langle\phi_{0_X}|_B \widehat{M}_{0_X}] + P(\text{ph} \mid \text{Ref})]
\end{aligned}
\tag{19}
$$

In the RT, we call **Eq. 19** the reference formula since it is used as a reference to obtain a similar expression in terms of the actual states. Note that we cannot use the reference formula directly in the security proof because it entails probabilities associated with the reference states, rather than the actual states.

Fortunately, by evaluating the deviation between the reference and the actual states, we can obtain bounds on the probabilities associated with the actual states and, consequently, the phase error rate of the actual protocol. This part of the RT corresponds to the deviation evaluation part (see Materials and Methods for further details). By following the analysis in the Supplementary Materials, we have that this deviation is quantified by using

PDF
Help

$$
\begin{aligned}
& g^L\left(\text{Tr}\left[\mid A\rangle\langle A \mid \widehat{M}\right], \mid \langle A \mid R\rangle \mid\right) \le \text{Tr}\left[\mid R\rangle\langle R \mid \widehat{M}\right] \le \\
& g^U\left(\text{Tr}\left[\mid A\rangle\langle A \mid \widehat{M}\right], \mid \langle A \mid R\rangle \mid\right)
\end{aligned}
\tag{20}
$$

where $\widehat{M}$ is any non-negative bounded operator such that $0 \le \widehat{M} \le 1$ and *A* and *R* are any normalized states associated with the actual and reference states, respectively. Here, the functions $g^L(x, y)$ and $g^U(x, y)$ are defined as

$$
g^L(x, y) = \begin{cases} 0 & x < 1 - y^2 \\ x + (1 - y^2)(1 - 2x) - 2y\sqrt{(1 - y^2)x(1 - x)} & x \ge 1 - y^2 \end{cases}
\tag{21}
$$

No measurement, including any measurement performed by Eve, can induce a larger deviation between the probabilities because **Eq. 20** holds for any $\widehat{M}$. We remark that, here, one could also use the trace distance argument (*15*); however, for the problem at hand, that bound is loose, and therefore, we use a tighter bound. That is, we use the knowledge of the probability associated with the observable events in the actual protocol, i.e., $\mathrm{Tr}[| A\rangle\langle A \mid \widehat{M}]$, while the trace distance does not.

Now, we apply **Eq. 20** to the first three terms and the last line of **Eq. 19** separately, thus converting **Eq. 19** into an expression for the probability of a phase error in terms of the actual states. For instance, note that the last line can be expressed by $-p_{Z_B} S_- \mathrm{Tr}[| A_-\rangle\langle A_-|_{CB} \widehat{M}_-]$ with
$|A_-\rangle_{CB} \coloneqq \sqrt{p_{1_X}^{\mathrm{vir}} c/S_-}\,|0_{x,A}, X_B\rangle_C |\psi_{0_X|j'_{k-1}}\rangle_B + \sqrt{p_{Z_A}/2S_-}\,|0_{z,A}, Z_B\rangle_C |\psi_{0_Z|j'_{k-1}}\rangle_B + \sqrt{p_{Z_A}/2S_-}\,|1_{z,A},$
and
$\widehat{M}_- \coloneqq \widehat{P}(|0_{x,A}, X_B\rangle_C) \otimes \widehat{M}_{0_X} + \widehat{P}([|0_{z,A}, Z_B\rangle_C - |1_{z,A}, Z_B\rangle_C]/\sqrt{2}) \otimes \widehat{M}_{0_X} + \widehat{P}([|0_{z,A}, Z_B\rangle_C + |1$
where $S_- = p_{1_X}^{\mathrm{vir}} c + p_{Z_A}$, system *C* is an ancilla that stores the classical information associated with Alice's and Bob's setting choices, and $\widehat{P}(| \cdot\rangle) =| \cdot\rangle\langle\cdot|$ (see Materials and Methods). Here, we have mathematically represented the summed probabilities using the trace. By obtaining a similar expression for the first three terms of **Eq. 19**, we find that this equation becomes (see Materials and Methods)

$$
\begin{aligned}
0 \le S_+ g^U \Bigg(& \frac{p_{1_X}^{\mathrm{vir}} p_{Z_B} a}{S_+} \mathrm{Tr}[| \psi_{0_Z|j'_{k-1}}\rangle\langle\psi_{0_Z|j'_{k-1}}|_B \widehat{M}_{0_X}] + \\
& \frac{p_{1_X}^{\mathrm{vir}} p_{Z_B} b}{S_+} \mathrm{Tr}[| \psi_{1_Z|j'_{k-1}}\rangle\langle\psi_{1_Z|j'_{k-1}}|_B \widehat{M}_{0_X}] + \\
& \frac{p_{0_X}^{\mathrm{vir}} p_{Z_B}}{S_+} \mathrm{Tr}[| \psi_{0_x|j'_{k-1}}\rangle\langle\psi_{0_x|j'_{k-1}}|_B \widehat{M}_{1_X}], 1-\epsilon \Bigg) - \\
S_- g^L \Bigg(& \frac{p_{1_X}^{\mathrm{vir}} p_{Z_B} c}{S_-} \mathrm{Tr}[| \psi_{0_x|j'_{k-1}}\rangle\langle\psi_{0_x|j'_{k-1}}|_B \widehat{M}_{0_X}] + \\
& \frac{P(\mathrm{ph}|\mathrm{Act})}{S_-}, 1-\epsilon \Bigg)
\end{aligned}
$$

where $S_+ = p_{1_X}^{\mathrm{vir}} a + p_{1_X}^{\mathrm{vir}} b + p_{0_X}^{\mathrm{vir}}$ and

$$
\begin{aligned}
P(\mathrm{ph} \mid \mathrm{Act}) \coloneqq\ & \tilde{p}_{1_X}^{\mathrm{vir}} p_{Z_B} \mathrm{Tr}[| \psi_{1_X|j'_{k-1}}^{\mathrm{vir}}\rangle\langle\psi_{1_X|j'_{k-1}}^{\mathrm{vir}}|_B \widehat{M}_{0_X}] + \\
& \tilde{p}_{0_X}^{\mathrm{vir}} p_{Z_B} \mathrm{Tr}[| \psi_{0_X|j'_{k-1}}^{\mathrm{vir}}\rangle\langle\psi_{0_X|j'_{k-1}}^{\mathrm{vir}}|_B \widehat{M}_{1_X}]
\end{aligned}
\qquad (24)
$$

any Kraus operator $K_{\widetilde{e}}$, that is included in the operators M_{α_X} (see discussion just after **Eq. 17**), and it can be directly used for the phase error estimation in the actual protocol. To clearly see how **Eq. 23** is related with quantities observed in an actual experiment, we rewrite it as

$$0 \leq S_+ g^U \left(\frac{p_{1_X}^{\mathrm{vir}} p_{Z_B} a}{S_+ p_{0_Z} p_{X_B}} P(q_{0z,0x} \mid \mathrm{Act}) + \frac{p_{1_X}^{\mathrm{vir}} p_{Z_B} b}{S_+ p_{1_Z} p_{X_B}} P(q_{1z,0x} \mid \mathrm{Act}) + \frac{p_{0_X}^{\mathrm{vir}} p_{Z_B}}{S_+ p_{0_X} p_{X_B}} P(q_{0x,1x} \mid \mathrm{Act}), 1-\epsilon \right) - S_- g^L \left(\frac{p_{1_X}^{\mathrm{vir}} p_{Z_B} c}{S_- p_{0_X} p_{X_B}} P(q_{0x,0x} \mid \mathrm{Act}) + \frac{P(\mathrm{ph}|\mathrm{Act})}{S_-}, 1-\epsilon \right) \tag{25}$$

where, e.g., $P(q_{0z,0x} \mid \mathrm{Act}) \coloneqq p_{0_Z} p_{X_B} \mathrm{Tr}[| \psi_{0_Z|j'_{k-1}} \rangle \langle \psi_{0_Z|j'_{k-1}} |_B \widehat{M}_{0_X}]$ is the joint probability (i.e., the yield) that Alice selects the setting 0_Z and prepares the state $|\psi_{0_Z|j'_{k-1}}\rangle_B$ and Bob's measurement outcome is 0_X. Last, by solving **Eq. 25** with respect to *P*(ph|Act), we obtain the probability of a phase error of the actual protocol. The phase error rate is then defined as $e_X = P(\mathrm{ph}|\mathrm{Act})/Y_Z$, where $Y_Z \coloneqq P(q_{0z,0z}|\mathrm{Act}) + P(q_{0z,1z}|\mathrm{Act}) + P(q_{1z,0z}|\mathrm{Act}) + P(q_{1z,1z}|\mathrm{Act})$ is the yield in the *Z* basis, i.e., the joint probability that Alice and Bob choose the *Z* basis and Bob obtains a detection event.

Simulation of the secret key rate

To show the performance of QKD in the presence of pulse correlations, we now present the simulation results. For simplicity of discussion, here, we apply our framework to two different cases of the RT: the RT based on the GLT protocol (*18*) and the RT described in the previous section. We remark that the GLLP type security proofs (*19*–*21*) are also regarded as a special case of the where we select the actual states as the reference states and skip the reference formula part the Supplementary Materials for the proof of this claim). However, they involve four states, rather than three states, and analytical or numerical optimization is required. The comparison between the RT based on the GLLP type security proofs and the RT based on the original LT protocol is presented in the Supplementary Materials.

The main difference between the RT based on the GLT protocol and the RT based on the original LT protocol is that, in the former, a different bound is used to estimate the probabilities associated with the actual states. More precisely, the RT based on the GLT protocol essentially uses an inequality involving eigenvalues, instead of **Eq. 20**, which has the form

Here, $\lambda_{j_k}^{\min}$ and $\lambda_{j_k}^{\max}$ are the eigenvalues of a matrix in the form $\begin{bmatrix} {}_{j_k} & {}_{j_k} \\ B_{j_k} & 0 \end{bmatrix}$, where $B_{j_k} = (1-\epsilon)\sqrt{1-(1-\epsilon)^2}$ and $C_{j_k} = 1 - (1 - \epsilon)^2$. The inequality in **Eq. 26** is valid for any $\widehat{M}_{\alpha X}$ with α ∈ {0,1}, and therefore, we can use it to consider the deviation between the probabilities associated with the reference states and the ones associated with the actual states [see (*18*) for more details]. We emphasize that pulse correlations are not taken into account in (*18*); however, we can apply our method to deal with pulse correlations to this security analysis. In doing so, we simply consider a QKD protocol with the states in **Eqs. 14** and **15** and apply the RT based on the GLT protocol. That is, besides pulse correlations, we also include the effect of SPFs by assuming δ > 0 in **Eq. 15**. Furthermore, recall that system B in **Eqs. 14**, **15**, and **26** can include more systems, not only those sent to Bob. In these equations, the subscript B could be replaced by $A_{k+1}, \cdots, A_n, B_k, B_{k+1}, \cdots, B_n$, allowing us to consider pulse correlations as the side channel. Note that to simplify the mathematical analysis, we do not trace out Alice's subsequent systems $A_{k+1}, \cdots, A_n$. Since these systems are independent of the setting j_k, they do not provide any relevant information to Eve, and therefore, they do not affect our estimation of the phase error rate.

For the simulations, we assume the asymptotic regime where the secret key rate formula for a single-photon source can be expressed as

$$R \geq Y_Z(1 - h(e_X) - fh(e_Z)) \tag{27}$$

where, as defined before, Y_Z is the yield in the Z basis and e_X is the phase error rate. The term e_Z is the bit error rate, $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, and f is the error correction efficiency. Note that Y_Z and e_Z are directly observed in a practical implementat the protocol, but in the simulations, a channel model [see (*18*) for more details] is used instea experimental parameters used are as follows: dark count rate of Bob's detectors $p_d = 10^{-7}$, $f = 1.16$, and the probabilities for Alice and Bob to select the Z basis are, for simplicity, $p_{Z_A} = \frac{2}{3}$ and $p_{Z_B} = \frac{1}{2}$. Unfortunately, there are no quantitative works characterizing pulse correlations (i.e., the value of the parameter ϵ); therefore, for illustration purposes, we select the values 10^{-3} and 10^{-6} to evaluate this imperfection. In addition, to investigate how the length of the pulse correlations affects the secret key rate, we consider the nearest-neighbor correlation ϵ_1, as well as correlations among two subsequent pulses, ϵ_2, and among 10 subsequent pulses, ϵ_{10} (see **Eq. 13** for the definitions of these ϵ parameters). Regarding SPFs, we choose δ = 0 and δ = 0.063 according to the experimental results reported in (*43*–*45*). The results for the RT based on the GLT protocol and for the RT based on the original LT protocol are illustrated in **Fig. 1**.

on the original LT (RT-LT) protocol.

In all graphs, the blue and red lines are associated with the RT-GLT and the RT-LT, respectively. The solid lines correspond to the nearest-neighbor pulse correlations ϵ_1, while the dashed (dashed-dotted) lines correspond to second ϵ_2 (tenth ϵ_{10}) neighbor pulse correlations, as indicated in the legend. (**A**) When there are no SPFs and the parameter ϵ is high, the RT-GLT and the RT-LT provide similar secret key rates. (**B**) As the parameter ϵ decreases, both security proofs provide higher secret key rates, but the RT-LT clearly outperforms the RT-GLT. (**C**) In the presence of SPFs, the secret key rate is only slightly worse for all cases since the security proofs are based on the LT protocol. (**D**) For high SPFs and low ϵ, the RT-LT is still superior to the RT-GLT.

As expected, this figure shows that when the magnitude of pulse correlations characterized by ϵ_i increases, the secret key rate decreases. In addition, as the length of the correlations, taken into account, increases, the secret key rate drops. We note, however, that even when long-range correlations are considered, a secret key can still be obtained. Namely, **Fig. 1** shows that for $\epsilon = 10^{-6}$, one can generate a secret key even when there are correlations between 10 subsequent pulses. For a smaller value of the parameter ϵ_i, longer correlations can be included. If ϵ_i is small enough, then one can consider a very long range of pulse correlations while guaranteeing the security of QKD.

We emphasize that the security proof selected highly affects the results obtained, and this is also illustrated in **Fig. 1**, where we apply our technique to two different cases of the RT. To compare the RT based on the GLT protocol and the RT based on the original LT protocol as a function of pulse correlations, one can examine panels (A) and (B) or (C) and (D) of **Fig. 1**. Noticeably, as the magnitude of the pulse correlation ϵ_i increases, the secret key rate deteriorates for both of them. However, the RT based on the LT protocol outperforms the RT based on the GLT protocol in a parameter regimes investigated. In addition, by comparing panels (A) and (C) or (B) and (D) o one can see the effect of SPFs. As expected, the RT based on the GLT protocol and the RT based on the LT protocol are barely affected by this imperfection since they inherit, from the GLT protocol and the original LT protocol, respectively, high tolerance against SPFs with channel loss. The big difference observed in **Fig. 1** between these two cases of the RT arises because of the following reason. Recall that we need to evaluate the deviation between the probabilities associated with the reference states and those associated with the actual states. For this, the bound used in the RT based on the GLT protocol is obtained by calculating certain eigenvalues, and thus, they entail square root terms, which deteriorate the secret key rate. Note that in the trace distance argument (*15*), square root terms are also present, resulting in loose bounds. On the other hand, the RT based on the original LT provides a tighter estimation of the phase error rate thanks to the bound in **Eq. 20**. More precisely, the square root terms in **Eq. 20** include detection probabilities, which decrease as

PDF

Help

DISCUSSION

Security proofs of QKD have to consider source imperfections in the theoretical models. Fortunately, SPFs, THAs (12–16), and mode dependencies have been considered together very recently in (18). In this work, we have introduced a general framework to deal with pulse correlations, which are the last pieces required for securing the source. Our framework is compatible with those security proofs that incorporate other source imperfections, and therefore, it can be used to guarantee implementation security with flawed devices by combining it with MDI-QKD (5) and the results in (18). We remark that the decoy-state method (2–4) has not been considered in this work, and therefore, the imperfections of the intensity modulator have not been addressed. However, these imperfections could be straightforwardly included in our framework. The key idea for dealing with pulse correlations is interpreting the information encoded in the subsequent pulses as side-channel information. By doing so, we have shown that, as long as the magnitude of the correlations is small, a secret key can still be obtained even when there are correlations over a long range of pulses. Moreover, our framework can be directly applied in combination with existing security proofs such as the GLT protocol (18), the GLLP type security proofs involving the quantum coin idea (19–21), and the numerical techniques recently introduced in (22–24).

Furthermore, we have proposed a new framework for security proofs, which we call the RT. It uses reference states that are similar to the states sent in the actual protocol, thus allowing us to determine the parameters needed to prove the security of the latter. The RT is very general, and it can be applied to many QKD protocols. Moreover, it already includes the LT protocol, the GLT protocol, and the GLLP type security proofs as special cases. That is, we are able to reconstruct these security proofs by applying the RT, as shown in the Supplementary Materials. We have demonstrated that most of the source imperfections can be incorporated simultaneously int RT, and therefore, this technique has been proven to be very useful for guaranteeing the security of practical QKD protocols. In particular, we have shown that for the RT based on the original LT, no information about the side-channel states is required, yet it is an analytical security proof, resulting in a much simpler characterization of the source. In addition, we emphasize that the RT can be applied together with analytical or numerical optimization to estimate an upper bound on the phase error rate, which could result in a higher performance. In this work, we have rigorously proven the security of the RT, and we have provided the sufficient conditions to apply this technique to other QKD protocols (see the Supplementary Materials). We remark that, for the security proof, we have not considered the probabilities to be conditional on the detection events, which is usually important for high performance in the finite-key scenario. Fortunately, thanks to the recently developed Kato's

PDF
Help

comparison might be considered unfair because the RT based on the GLLP type security proofs requires four states and analytical or numerical optimization. Last, we note that if a better inequality to evaluate the deviation between the probabilities associated with the reference states and those associated with the actual states is available, then it could replace the inequality in **Eq. 20**, resulting in even higher secret key rates for the RT. In addition, our method could be applied to other problems in quantum information theory where one needs to estimate summed probabilities. In this sense, our work not only proves the security of practical QKD systems but also has a potential to contribute to quantum information theory in general.

MATERIALS AND METHODS

Reference technique

The RT is a new framework to prove the security of QKD protocols. It is general and can reproduce the GLLP type security proofs involving the quantum coin idea (*19*–*21*) and the original LT protocol (*17*). Moreover, it can be applied to many different protocols. To see this, we refer the reader to the Supplementary Materials where we demonstrate that the GLLP type security proofs can be reconstructed from the RT. In addition, we outline the sufficient conditions to use the RT and prove the security of an *m*-state protocol. In this section, however, we present the key idea of the RT and show that it can be seen as a generalization of the LT protocol. For concreteness of the explanation, we concentrate on a particular example, the three-state protocol considered in Results.

Usually, to prove the security of QKD protocols, a relationship among the probabilities associated with the actual states needs to be established. Quite often, it is not straightforward to construct such a relationship, and the RT could be very useful to overcome this difficulty. The key idea i

PDF
Help

consider a set of states, which we call the reference states, instead of the actual states. Thes reference states can be chosen freely, but they should be selected such that it is easy to derive a relationship among the probabilities associated with them. For this, it may be convenient to select the reference states in a structured space, such as a qubit space, and importantly, it is preferential that the resulting relationship is resilient against some imperfections in the space, such as the SPFs. Note that this relationship is associated with the reference states, and, therefore, it cannot be used directly in the security proof. However, since the reference states are chosen to be similar to the actual states, we can obtain a relationship associated with the actual states by slightly modifying the relationship for the reference states. In summary, the RT consists mainly of two parts:

1) Reference formula part: Here, we construct a relationship among the probabilities associated with the reference states.

formula, and we do not need to consider or imagine their practical implementation. Below, we show how to apply the RT in practice by presenting a rigorous security proof against coherent attacks for the three-state protocol.

Security proof of the three-state protocol with side channels. Let us assume a three-state protocol where Alice chooses a normalized state $|\psi_j\rangle_B$ from the set $\{|\psi_j\rangle_B\}_{j=0_Z,1_Z,0_X}$ with probability p_j for each pulse emission. For simplicity of discussion, we assume that $p_{0_Z} = p_{1_Z}$. The assumptions on Bob's side have been described in Results. Namely, he measures the incoming pulses in the *Z* or in the *X* basis with probabilities p_{Z_B} and p_{X_B}, respectively. More precisely, Bob's *Z*-basis (*X*-basis) measurement is represented by the POVM $\{\widehat{m}_{0_Z}, \widehat{m}_{1_Z}, \widehat{m}_f\}$ $(\{\widehat{m}_{0_X}, \widehat{m}_{1_X}, \widehat{m}_f\})$, and it satisfies the basis-independent detection efficiency condition. Note that, in this protocol, the key is generated from a subset of the states indexed by $j = 0_Z, 1_Z$, i.e., the *Z* basis and the bit values obtained by Bob's *Z*-basis measurement.

Now, we write the states sent by Alice in the form of **Eq. 1**. That is, we expand the states $|\psi_j\rangle_B$ by using an orthonormal basis, and in doing so, we select a qubit space that is common over the three states. This suggests that $|\psi_j\rangle_B$ can be, most generally, decomposed into

$$\begin{aligned}|\psi_{0_Z}\rangle_B &= (1-\epsilon_{0_Z})|\phi_{0_Z}\rangle_B + \sqrt{1-(1-\epsilon_{0_Z})^2}|\phi_{0_Z}^{\perp}\rangle_B,\\ |\psi_{1_Z}\rangle_B &= (1-\epsilon_{1_Z})|\phi_{1_Z}\rangle_B + \sqrt{1-(1-\epsilon_{1_Z})^2}|\phi_{1_Z}^{\perp}\rangle_B,\\ |\psi_{0_X}\rangle_B &= (1-\epsilon_{0_X})|\phi_{0_X}\rangle_B + \sqrt{1-(1-\epsilon_{0_X})^2}|\phi_{0_X}^{\perp}\rangle_B\end{aligned} \tag{28}$$

where the state $|\phi_j\rangle_B$ represents the qubit part of the state $|\psi_j\rangle_B$ and the state $|\phi_j^{\perp}\rangle_B$ is a (possibly) unknown side-channel state that lives in any Hilbert space and is orthogonal to $|\phi_j\rangle_B$. We stress that this orthogonality is needed only for each setting choice *j* but not between different choices of *j*. Examples of these states were presented in **Eq. 14**; however, for generality, we do not restrict ourselves only to that scenario. In the security proof, we assume that the qubit parts $\{|\phi_j\rangle_B\}_{j=0_Z,1_Z,0_X}$, which are to be adopted as the reference states, are perfectly characterized and stable in time, but we do not require any knowledge about the side-channel states $\{|\phi_j^{\perp}\rangle_B\}_{j=0_Z,1_Z,0_X}$. From an experimental viewpoint, the unnecessity of characterizing the side-channel state $|\phi_j^{\perp}\rangle_B$ in **Eq. 28** is a great advantage, as in practice, it is very challenging to perform measurements on arbitrary physical degrees of freedom. In **Eq. 28**, the coefficient ϵ_j satisfying $0 \le \epsilon_j \le 1$ quantifies the deviation of the state $|\psi_j\rangle_B (j \in \{0_Z, 1_Z, 0_X\})$ from the qubit space. That is, the states $|\psi_j\rangle_B$ are ideally qubit states; however, due to the presence of side channels, such as THA or pulse correlations, they deviate from

PDF

Help

and we know ϵ (or more generally, ϵ_j). In particular, this means that the state $|\phi_j^\perp\rangle_B$ can vary in time and can be dependent on the previous pulses, and therefore, the states $|\psi_j\rangle_B$ emitted by Alice's source do not need to be regarded as independently and identically distributed. This point will become clearer after **Eq. 55**. We remark, however, that if we select the reference states containing side-channel states, then they will no longer be perfectly known or stable in time. In this case, to make the mathematical analysis simpler, one could use analytical or numerical optimization to consider the worst-case scenario for the side-channel states, i.e., the case that maximizes the phase error rate. This maximization removes the potential dependence on the previous pulses and thus effectively provides pulses that are independent and stable in time. This is a purely mathematical step, and it does not require any extra assumptions on Alice's source, e.g., the states $|\psi_j\rangle_B$ do not need to be regarded as independently and identically distributed.

Having finished the description of the states, we move on to the security proof using the RT. We are interested in proving the security of the bit values generated from the *Z*-basis events. From Eve's perspective, this instance is equivalent to the one in which Alice selects the *Z* basis, prepares systems *A* and *B* in the state

$$\frac{1}{\sqrt{2}}(|0_Z\rangle_A|\psi_{0_Z}\rangle_B + |1_Z\rangle_A|\psi_{1_Z}\rangle_B) \tag{29}$$

and sends system *B* to Bob while keeping system *A* in her laboratory, and then both Alice and Bob perform their measurements in the *Z* basis. To prove the security of the *Z*-basis events, we need to estimate the phase errors (*17*, *46*), which are defined in the *X* basis. That is, we consider the errors that Alice and Bob would have obtained if Alice had performed the *X*-basis measurement {|0 $|1_X\rangle_A\}$ (with $|0_X\rangle_A \coloneqq (|0_Z\rangle_A + |1_Z\rangle_A)/\sqrt{2}$ and $|1_X\rangle_A \coloneqq (|0_Z\rangle_A - |1_Z\rangle_A/\sqrt{2})$ and Bob had u basis complementary to the *Z* basis (a suitable choice under the basis independent efficiency condition may be the *X* basis used in the actual protocol) for the measurement on the joint state defined in **Eq. 29**. This leads us to consider a virtual protocol in which Alice sends the virtual states $|\psi_{0_X}^{\rm vir}\rangle_B \propto |\psi_{0_Z}\rangle_B + |\psi_{1_Z}\rangle_B$ and $|\psi_{1_X}^{\rm vir}\rangle_B \propto |\psi_{0_Z}\rangle_B - |\psi_{1_Z}\rangle_B$ (*17*) to Bob with probabilities

PDF
Help

$$\tilde{p}^{\rm vir}_{\alpha_X} = \frac{1}{2}p_{Z_A}[1 + (-1)^\alpha \mathrm{Re}({}_B\langle\psi_{0_Z} \mid \psi_{1_Z}\rangle_B)] \tag{30}$$

where p_{Z_A} is the probability that Alice selects the *Z* basis. Here, $\widetilde{p}^{\,\rm vir}_{0_X}(\widetilde{p}^{\,\rm vir}_{1_X})$ is the joint probability that Alice selects the *Z* basis and prepares the normalized virtual state $|\psi_{0_X}^{\rm vir}\rangle_B$ $(|\psi_{1_X}^{\rm vir}\rangle_B)$ through the *X*-basis measurement.

$$\begin{aligned}|\psi\rangle_{CB} \coloneqq{}& \sqrt{p_{0_Z} p_{X_B}}|0_{z,A}, X_B\rangle_C|\psi_{0_Z}\rangle_B +\\ &\sqrt{p_{1_Z} p_{X_B}}|1_{z,A}, X_B\rangle_C|\psi_{1_Z}\rangle_B + \sqrt{p_{0_X} p_{X_B}}|0_{x,A}, X_B\rangle_C|\psi_{0_X}\rangle_B +\\ &\sqrt{p_{0_X} p_{Z_B}}|0_{x,A}, Z_B\rangle_C|\psi_{0_X}\rangle_B + \sqrt{\tilde{p}^{\mathrm{vir}}_{0_X} p_{Z_B}}|0^{\mathrm{vir}}_{x,A}, X_B\rangle_C|\psi^{\mathrm{vir}}_{0_X}\rangle_B +\\ &\sqrt{\tilde{p}^{\mathrm{vir}}_{1_X} p_{Z_B}}|1^{\mathrm{vir}}_{x,A}, X_B\rangle_C|\psi^{\mathrm{vir}}_{1_X}\rangle_B\end{aligned} \tag{31}$$

and then performing a measurement on system *C*, which is associated with Alice's and Bob's setting choices. In particular, $|0_{z,A}, X_B\rangle_C$ ($|1^{\mathrm{vir}}_{x,A}, X_B\rangle_C$) represents the events when Alice selects the actual state for 0_Z (the virtual state for 1_X) and Bob chooses the *X* basis. Note that there are six states of system *C* that store different classical information related with Alice's and Bob's setting choices, and they are all normalized and orthogonal to each other. After Alice prepares the entangled state in **Eq. 31**, we imagine that she performs an orthogonal measurement that projects system *C* onto one of these six states, and Bob performs the measurement according to the basis directed by the measurement outcome. We remark that the first four terms in **Eq. 31** correspond to the actual events that occur in the actual protocol, while the last two terms correspond to the virtual events. That is, the last two terms represent the events in which Alice and Bob select the *Z* basis in the actual protocol; however, their basis choice is replaced by the *X* basis for the security proof. The virtual events and the actual events are clearly defined in system *C*, and they correspond to disjoint events. The actual protocol can then be regarded as, repeatedly, say, *N* times, preparing systems *B* and *C* in the state $|\psi\rangle_{CB}$ followed by the measurements by Alice and Bob. Now, following the steps of the RT introduced above, we can estimate the phase errors associated with this protocol.

Reference formula part. As an example, we choose the reference states to be the qubit part o actual states. For the actual states defined in **Eq. 28**, this corresponds to selecting the set $\{|\phi_{0_Z}\rangle_B, |\phi_{1_Z}\rangle_B, |\phi_{0_X}\rangle_B\}$ (see **Eq. 15** for their explicit form). Now, we need to construct a relationship associated with these reference states. First, we consider the virtual entangled state

$$\frac{1}{\sqrt{2}}(|0_Z\rangle_A|\phi_{0_Z}\rangle_B + |1_Z\rangle_A|\phi_{1_Z}\rangle_B) \tag{32}$$

Note that **Eq. 32** is analogous to **Eq. 29**, but the actual states have been replaced with their respective reference states. Then, we may imagine that Alice measures system *A* in the *X* basis and sends Bob the virtual states $|\phi^{\mathrm{vir}}_{0_X}\rangle_B \propto |\phi_{0_Z}\rangle_B + |\phi_{1_Z}\rangle_B$ and $|\phi^{\mathrm{vir}}_{1_X}\rangle_B \propto |\phi_{0_Z}\rangle_B - |\phi_{1_Z}\rangle_B$ with probabilities mathematically replace all the actual and virtual states in **Eq. 31** with their respective reference states

$$\begin{aligned}&\sqrt{p_{0_Z}p_{X_B}}|0_{z,A},X_B\rangle_C|\phi_{0_Z}\rangle_B+\sqrt{p_{1_Z}p_{X_B}}|1_{z,A},X_B\rangle_C|\phi_{1_Z}\rangle_B+\\&\sqrt{p_{0_X}p_{X_B}}|0_{x,A},X_B\rangle_C|\phi_{0_X}\rangle_B+\sqrt{p_{0_X}p_{Z_B}}|0_{x,A},Z_B\rangle_C|\phi_{0_X}\rangle_B+\\&\sqrt{p^{\text{vir}}_{0_X}p_{Z_B}}|0^{\text{vir}}_{x,A},X_B\rangle_C|\phi^{\text{vir}}_{0_X}\rangle_B+\sqrt{p^{\text{vir}}_{1_X}p_{Z_B}}|1^{\text{vir}}_{x,A},X_B\rangle_C|\phi^{\text{vir}}_{1_X}\rangle_B\end{aligned}\tag{34}$$

Again, we emphasize that this entanglement-based protocol with the reference states is purely a mathematical tool for the security proof, and we do not need to consider or imagine its practical implementation. The reason why we have selected $\{|\phi_{0_Z}\rangle_B,|\phi_{1_Z}\rangle_B,|\phi_{0_X}\rangle_B\}$ as the reference states is twofold. First, these states are close to their respective actual states $\{|\psi_{0_Z}\rangle_B,|\psi_{1_Z}\rangle_B,|\psi_{0_X}\rangle_B\}$. Therefore, we expect that the probabilities associated with the reference states should be similar to those associated with the actual states. Second, by directly using the idea of the LT protocol for a qubit-based protocol (*17*), we can obtain a relationship between the reference states and the virtual states, which is expected to be LT against SPFs. More concretely, below, we consider that the reference states used are the ones defined in **Eq. 15**, and, in this case, we can express the virtual states for the reference states as in **Eq. 18**. We rewrite it here for convenience

$$\begin{aligned}&|\phi^{\text{vir}}_{1_X}\rangle\langle\phi^{\text{vir}}_{1_X}|_B=a\mid\phi_{0_Z}\rangle\langle\phi_{0_Z}|_B+b\mid\phi_{1_Z}\rangle\langle\phi_{1_Z}|_B-c\mid\phi_{0_X}\rangle\langle\phi_{0_X}|_B,\\&|\phi^{\text{vir}}_{0_X}\rangle\langle\phi^{\text{vir}}_{0_X}|_B=\mid\phi_{0_X}\rangle\langle\phi_{0_X}|_B\end{aligned}\tag{35}$$

PDF
Help

where from **Eq. 15**, the coefficients *a*, *b*, *c* ≥ 0 are given by

$$\begin{aligned}a&:=\frac{-2\ \sin\left(\frac{\pi}{4}+\frac{\delta}{4}\right)}{\cos\left(\frac{\pi}{4}+\frac{3\delta}{4}\right)-3\ \sin\left(\frac{\pi}{4}+\frac{\delta}{4}\right)},\\b&:=\frac{-2\ \sin\left(\frac{\pi}{4}+\frac{\delta}{4}\right)}{\cos\left(\frac{\pi}{4}+\frac{3\delta}{4}\right)-3\ \sin\left(\frac{\pi}{4}+\frac{\delta}{4}\right)},\\c&:=\frac{-\sin\left(\frac{\delta}{2}\right)+1}{\sin\left(\frac{\delta}{2}\right)+1}\end{aligned}\tag{36}$$

We remark that, in **Eq. 35**, we have highly exploited the properties of a qubit space, i.e., even with a negative sign in front of the coefficient *c*, $\left|\phi^{\text{vir}}_{1_X}\right\rangle\left\langle\phi^{\text{vir}}_{1_X}\right|_B$ is still a density operator, which would not be

$$p^{\mathrm{vir}}_{0_X} p_{Z_B} \mathrm{Tr}[|\,\phi^{\mathrm{vir}}_{0_X}\rangle\langle\phi^{\mathrm{vir}}_{0_X}|_B \widehat{M}^{(k)}_{1_X}] \tag{37}$$

which, as described in Results, could be interpreted as the probability of a phase error for the k^{th} pulse when using the reference states and where $\widehat{M}^{(k)}_{\alpha_X}$ with α ∈ {0,1} is Bob's POVM element for the k^{th} pulse after a coherent attack in the actual protocol, that is, $\widehat{M}^{(k)}_{\alpha X} := \sum_{\widetilde{e}} \widehat{K}^{(k)}_{\widetilde{e}} \widehat{m}_{\alpha_X} \widehat{K}^{(k)\dagger}_{\widetilde{e}}$. Here, $\widehat{K}^{(k)}_{\widetilde{e}}$ is the Kraus operator representing the action that the k^{th} pulse is subjected to. This operator is obtained by Eve's coherent attack that acts, in general, on all the pulses sent by Alice simultaneously and by considering all the $k - 1$ previous measurements by Alice and Bob. Here, $\widetilde{e}$ represents a particular outcome of the measurement conducted by Alice, Bob, and Eve. Note that, due to the entanglement caused by Eve's coherent attack, $\widehat{K}^{(k)}_{\widetilde{e}}$ depends on all the $k - 1$ previous measurement outcomes obtained by Alice and Bob. The goal now is to transform the quantities associated with the reference states in **Eq. 37** into those associated with the actual states for the k^{th} pulse

$$P^{(k)}(\mathrm{ph} \mid \mathrm{Act}) := \tilde{p}^{\mathrm{vir}}_{1_X} p_{Z_B} \mathrm{Tr}[|\,\psi^{\mathrm{vir}}_{1_X}\rangle\langle\psi^{\mathrm{vir}}_{1_X}| \widehat{M}^{(k)}_{0_X}] + \tilde{p}^{\mathrm{vir}}_{0_X} p_{Z_B} \mathrm{Tr}[|\,\psi^{\mathrm{vir}}_{0_X}\rangle\langle\psi^{\mathrm{vir}}_{0_X}|_B \widehat{M}^{(k)}_{1_X}] \tag{38}$$

Using **Eq. 35**, we can express **Eq. 37** as

$$\begin{aligned} P^{(k)}(\mathrm{ph} \mid \mathrm{Ref}) \quad &= p^{\mathrm{vir}}_{1_X} p_{Z_B} a \mathrm{Tr}[|\,\phi_{0_Z}\rangle\langle\phi_{0_Z}|_B \widehat{M}^{(k)}_{0_X}] + p^{\mathrm{vir}}_{1_X} p_{Z_B} b \mathrm{Tr}[|\,\phi_{1_Z}\rangle\langle\phi_{1_Z}|_B \widehat{M}^{(k}_{0_X} \\ & p^{\mathrm{vir}}_{1_X} p_{Z_B} c \mathrm{Tr}[|\,\phi_{0_X}\rangle\langle\phi_{0_X}|_B \widehat{M}^{(k)}_{0_X}] + p^{\mathrm{vir}}_{0_X} p_{Z_B} \mathrm{Tr}[|\,\phi_{0_X}\rangle\langle\phi_{0_X}|_B \widehat{M}^{(k)}_{1_X}] \end{aligned} \tag{39}$$

which is equivalent to

$$(p^{\mathrm{vir}}_{1_X} p_{Z_B} c\mathrm{Tr}[|\ \phi_{0_X}\rangle\langle\phi_{0_X}|_B \widehat{M}^{(k)}_{0_X}]+$$
$$p^{\mathrm{vir}}_{1_X} p_{Z_B}\mathrm{Tr}[|\ \phi^{\mathrm{vir}}_{1_X}\rangle\langle\phi^{\mathrm{vir}}_{1_X}|_B \widehat{M}^{(k)}_{0_X}]+$$
$$p^{\mathrm{vir}}_{0_X} p_{Z_B}\mathrm{Tr}[|\ \phi^{\mathrm{vir}}_{0_X}\rangle\langle\phi^{\mathrm{vir}}_{0_X}\ |\ \widehat{M}^{(k)}_{1_X}])$$

Here, we emphasize that Eq. 40 is derived on the basis of the idea of the LT protocol, and therefore, it entails the robustness against the SPFs in the qubit space. That is, if there are no side channels, i.e., ϵ = 0, then Eq. 40, which is exactly the expression that is used in the original LT protocol (*17*), results in a secret key rate that is LT against SPFs. Therefore, this shows that the RT includes the LT protocol in the reference formula part. Next, we transform the relationship for the reference states in Eq. 40 into a relationship for the actual states. That is, we enter the deviation evaluation part of the RT.

Deviation evaluation part. For the transformation of Eq. 40, we use the bound in Eq. 20. We rewrite it here for convenience

$$g^L(\mathrm{Tr}[|\ A\rangle\langle A\ |\ \widehat{M}],|\ \langle A\ |\ R\rangle\ |) \le \mathrm{Tr}[|\ R\rangle\langle R\ |\ \widehat{M}] \le g^U(\mathrm{Tr}[|\ A\rangle\langle A\ |\ \widehat{M}],|\ \langle A\ |\ R\rangle\ |) \tag{41}$$

where $|R\rangle$ ($|A\rangle$) is any normalized state associated with the reference (actual) states and

$$g^L(x,y) = \begin{cases} 0 & x < 1-y^2 \\ x+(1-y^2)(1-2x)-2y\sqrt{(1-y^2)x(1-x)} & x \ge 1-y^2 \end{cases}$$

PDF
Help

$$g^U(x,y) = \begin{cases} x+(1-y^2)(1-2x)+2y\sqrt{(1-y^2)x(1-x)} & x \le y^2 \\ 1 & x > y^2 \end{cases} \tag{43}$$

Note that $-g^L(x, y)$ and $g^U(x, y)$ are concave with respect to $0 \le x \le 1$ for any fixed $0 \le y \le 1$, and $\partial_y g^L(x, y) \ge 0$ and $\partial_y g^U(x, y) \le 0$ hold. For more details on the derivation of Eq. 41, see the Supplementary Materials. Now, we consider the first three terms in Eq. 40, which are reexpressed as where $S_+ \coloneqq p^{\text{vir}}_{1_X} a + p^{\text{vir}}_{1_X} b + p^{\text{vir}}_{0_X}$ is a normalization factor. Next, we rewrite the term Tr[·] in **Eq. 44** as

$$\begin{aligned}
&\mathrm{Tr}\left[\widehat{P}\left(\sqrt{\frac{p^{\text{vir}}_{1_X} a}{S_+}}|0_{z,A}, X_B\rangle_C|\phi_{0_Z}\rangle_B + \right.\right.\\
&\sqrt{\frac{p^{\text{vir}}_{1_X} b}{S_+}}|1_{z,A}, X_B\rangle_C|\phi_{1_Z}\rangle_B + \\
&\left.\left.\sqrt{\frac{p^{\text{vir}}_{0_X}}{S_+}}|0_{x,A}, X_B\rangle_C|\phi_{0_X}\rangle_B\right)\widehat{M}_+^{(k)}\right] \\
&\eqqcolon \mathrm{Tr}\left[\widehat{P}(|R_+\rangle_{\mathrm{CB}})\widehat{M}_+^{(k)}\right]
\end{aligned} \tag{45}$$

with

$$\begin{aligned}
|R_+\rangle_{CB} &\coloneqq \sqrt{\frac{p^{\text{vir}}_{1_X} a}{S_+}}|0_{z,A}, X_B\rangle_C|\phi_{0_Z}\rangle_B + \\
&\sqrt{\frac{p^{\text{vir}}_{1_X} b}{S_+}}|1_{z,A}, X_B\rangle_C|\phi_{1_Z}\rangle_B + \\
&\sqrt{\frac{p^{\text{vir}}_{0_X}}{S_+}}|0_{x,A}, X_B\rangle_C|\phi_{0_X}\rangle_B, \\
\widehat{M}_+^{(k)} &\coloneqq \widehat{P}(|0_{z,A}, X_B\rangle_C) \otimes \widehat{M}_{0_X}^{(k)} + \\
&\widehat{P}(|1_{z,A}, X_B\rangle_C) \otimes \widehat{M}_{0_X}^{(k)} + \\
&\widehat{P}(|0_{x,A}, X_B\rangle_C) \otimes \widehat{M}_{1_X}^{(k)}
\end{aligned}$$

where $\widehat{P}(|\cdot\rangle) = |\cdot\rangle\langle\cdot|$. Note that this is purely a mathematical reinterpretation of the summed probabilities. We are interested in mathematically replacing $|\phi_{0_Z}\rangle_B$, $|\phi_{1_Z}\rangle_B$, and $|\phi_{0_X}\rangle_B$ in **Eq. 45** with $|\psi_{0_Z}\rangle_B$, $|\psi_{1_Z}\rangle_B$, and $|\psi_{0_X}\rangle_B$, respectively, by using **Eq. 41**. For this, we may select

PDF

Help

$$\sqrt{\frac{p^{\mathrm{vir}}_{0_X}}{S_+}}|0_{x,A},X_B\rangle_C|\psi_{0_X}\rangle_B$$

and as a result, we have transformed the first three terms of **Eq. 40** into

$$\begin{aligned}&p^{\mathrm{vir}}_{1_X}p_{Z_B}a\mathrm{Tr}[|\ \phi_{0_Z}\rangle\langle\phi_{0_Z}|_B\widehat{M}^{(k)}_{0_X}]+\\&p^{\mathrm{vir}}_{1_X}p_{Z_B}b\mathrm{Tr}[|\ \phi_{1_Z}\rangle\langle\phi_{1_Z}\ |\ \widehat{M}^{(k)}_{0_X}]+\\&p^{\mathrm{vir}}_{0_X}p_{Z_B}\mathrm{Tr}[|\ \phi_{0_X}\rangle\langle\phi_{0_X}|_B\widehat{M}^{(k)}_{1_X}]\leq p_{Z_B}S_+\\&g^U\left(\mathrm{Tr}[\widehat{P}(|A_+\rangle_{CB})\widehat{M}^{(k)}_+],1-\epsilon\right)\end{aligned}\tag{47}$$

where we have selected an upper bound on $\mathrm{Tr}\ [\widehat{P}(|R_+\rangle_{CB})\widehat{M}^{(k)}_+]$ to obtain an upper bound on the phase error probability and used $|_{CB}\langle A_+|R_+\rangle_{CB}\ |$ = 1 − ϵ. Here, note that to calculate this inner product, we need to calculate the terms ${}_B\ \langle\psi_j|\phi_j\rangle\ {}_B$ rather than ${}_B\langle\psi_j\mid\phi_{\tilde{j}}\rangle_B$ with $j\neq\tilde{j}$, which shows the aforementioned simplicity of the state characterization needed in our proof. Now, to clearly see how the term $\mathrm{Tr}[\widehat{P}(|A_+\rangle_{CB})\widehat{M}^{(k)}_+]$ is related with the quantities obtained from an experimental implementation of the actual protocol, we write

$$\begin{aligned}&\mathrm{Tr}\left[\hat{P}(|A_+\rangle_{CB})\widehat{M}^{(k)}_+\right]\\&=\mathrm{Tr}\left[\frac{p^{\mathrm{vir}}_{1_X}a}{S_+}\ \middle|\ \psi_{0_Z}\middle\rangle\middle\langle\psi_{0_Z}\ \middle|\ \widehat{M}^{(k)}_{0_X}+\frac{p^{\mathrm{vir}}_{1_X}b}{S_+}\ \middle|\ \psi_{1_Z}\middle\rangle\middle\langle\psi_{1_Z}\ \middle|\ \widehat{M}^{(k)}_{0_X}\right.\\&\left.+\frac{p^{\mathrm{vir}}_{0_X}}{S_+}\ \middle|\ \psi_{0_X}\middle\rangle\middle\langle\psi_{0_X}\ \middle|\ \widehat{M}^{(k)}_{1_X}\right]\\&=\frac{p^{\mathrm{vir}}_{1_X}a}{S_+p_{0z}p_{X_B}}P^{(k)}(q_{0z,0x}\mid\mathrm{Act})+\\&\frac{p^{\mathrm{vir}}_{1_X}b}{S_+p_{1z}p_{X_B}}P^{(k)}(q_{1z,0x}\mid\mathrm{Act})+\\&\frac{p^{\mathrm{vir}}_{0_X}}{S_+p_{0x}p_{X_B}}P^{(k)}(q_{0x,1x}\mid\mathrm{Act})\end{aligned}\tag{48}$$

Next, we consider the last three terms in Eq. 40, which are reexpressed as

$$\begin{aligned}&p_{Z_B} S_- \mathrm{Tr}\Bigg[\frac{p^{\mathrm{vir}}_{1_X} c}{S_-} \mid \phi_{0_X}\Big\rangle\Big\langle \phi_{0_X}|_B \widehat{M}^{(k)}_{0_X} + \\ &\frac{p^{\mathrm{vir}}_{1_X}}{S_-} \mid \phi^{\mathrm{vir}}_{1_X}\Big\rangle\Big\langle \phi^{\mathrm{vir}}_{1_X}|_B \widehat{M}^{(k)}_{0_X} + \frac{p^{\mathrm{vir}}_{0_X}}{S_-} \mid \phi^{\mathrm{vir}}_{0_X}\Big\rangle\Big\langle \phi^{\mathrm{vir}}_{0_X}|_B \widehat{M}^{(k)}_{1_X}\Bigg]\end{aligned} \tag{49}$$

where $S_- := p^{\mathrm{vir}}_{1_X} c + p^{\mathrm{vir}}_{1_X} + p^{\mathrm{vir}}_{0_X} = p^{\mathrm{vir}}_{1_X} c + p_{Z_A}$, with $p_{Z_A} := p_{0_Z} + p_{1_Z}$ is the normalization factor. The term Tr[·] in Eq. 49 can be expressed as

$$\begin{aligned}&\mathrm{Tr}\Bigg[\widehat{P}\Bigg(\sqrt{\frac{p^{\mathrm{vir}}_{1_X} c}{S_-}} |0_{x,A}, X_B\rangle_C |\phi_{0_X}\rangle_B + \\ &\sqrt{\frac{p_{Z_A}}{2S_-}} |0_{z,A}, Z_B\rangle_C |\phi_{0_Z}\rangle_B + \\ &\sqrt{\frac{p_{Z_A}}{2S_-}} |1_{z,A}, Z_B\rangle_C |\phi_{1_Z}\rangle_B\Bigg) \widehat{M}^{(k)}_-\Bigg] \\ &=: \mathrm{Tr}[\widehat{P}(|R_-\rangle_{\mathrm{CB}}) \widehat{M}^{(k)}_-]\end{aligned} \tag{50}$$

with

$$\begin{aligned}&|R_-\rangle_{CB} := \sqrt{\frac{p^{\mathrm{vir}}_{1_X} c}{S_-}} |0_{x,A}, X_B\rangle_C |\phi_{0_X}\rangle_B + \\ &\sqrt{\frac{p_{Z_A}}{2S_-}} |0_{z,A}, Z_B\rangle_C |\phi_{0_Z}\rangle_B + \\ &\sqrt{\frac{p_{Z_A}}{2S_-}} |1_{z,A}, Z_B\rangle_C |\phi_{1_Z}\rangle_B, \\ &\hat{M}^{(k)}_- := \hat{P}(|0_{x,A}, X_B\rangle_C) \otimes \hat{M}^{(k)}_{0_X} + \\ &\hat{P}\left(\frac{|0_{z,A}, Z_B\rangle_C - |1_{z,A}, Z_B\rangle_C}{\sqrt{2}}\right) \otimes \hat{M}^{(k)}_{0_X} + \\ &\hat{P}\left(\frac{|0_{z,A}, Z_B\rangle_C + |1_{z,A}, Z_B\rangle_C}{\sqrt{2}}\right) \otimes \hat{M}^{(k)}_{1_X}\end{aligned} \tag{51}$$

PDF
Help

probability. To mathematically replace the states involving the reference states with those involving the actual states, we may select

$$
\begin{aligned}
|A_-\rangle_{CB} \coloneqq\ & \sqrt{\frac{p^{\mathrm{vir}}_{1_X} c}{S_-}} |0_{x,A}, X_B\rangle_C |\psi_{0_X}\rangle_B + \\
& \sqrt{\frac{p_{Z_A}}{2S_-}} |0_{z,A}, Z_B\rangle_C |\psi_{0_Z}\rangle_B + \\
& \sqrt{\frac{p_{Z_A}}{2S_-}} |1_{z,A}, Z_B\rangle_C |\psi_{1_Z}\rangle_B
\end{aligned}
\tag{52}
$$

As a result, we have transformed the last three terms in **Eq. 40** into

$$
\begin{aligned}
& p^{\mathrm{vir}}_{1_X} p_{Z_B} c \mathrm{Tr}[|\ \phi_{0_X}\rangle\langle\phi_{0_X}|_B \widehat{M}^{(k)}_{0_X}] + \\
& p^{\mathrm{vir}}_{1_X} p_{Z_B} \mathrm{Tr}[|\ \phi^{\mathrm{vir}}_{1_X}\rangle\langle\phi^{\mathrm{vir}}_{1_X}|_B \widehat{M}^{(k)}_{0_X}] + \\
& p^{\mathrm{vir}}_{0_X} p_{Z_B} \mathrm{Tr}[|\ \phi^{\mathrm{vir}}_{0_X}\rangle\langle\phi^{\mathrm{vir}}_{0_X}|_B \widehat{M}^{(k)}_{1_X}] \\
& \geq p_{Z_B} S_- g^L(\mathrm{Tr}[\hat{P}(|A_-\rangle_{\mathrm{CB}}) \widehat{M}^{(k)}_-], 1-\epsilon)
\end{aligned}
\tag{53}
$$

where we have selected a lower bound on $\mathrm{Tr}[\widehat{P}(|R_-\rangle_{CB}) \widehat{M}^{(k)}_-]$ to obtain an upper bound on the phase error probability and used $|{}_{CB}\langle A_- |R_-\rangle_{CB}| = 1 - \epsilon$. As before, to calculate this inner product, we need to calculate the terms ${}_B\ \langle\psi_j | \phi_j\rangle\ _B$ rather than ${}_B\langle\psi_j \mid \phi_{\tilde{j}}\rangle_B$ with $j \neq \tilde{j}$. Now, we look at $\mathrm{Tr}[\widehat{P}(|A_-\rangle_{CB}) \widehat{M}^{(k)}_-]$, which is expressed and interpreted by

$$= \mathrm{Tr}\left[\frac{p^{\mathrm{vir}}_{1_X}c}{S_-}\mid\psi_{0_X}\rangle\langle\psi_{0_X}|_B\widehat{M}^{(k)}_{0_X} + \frac{\tilde{p}^{\mathrm{vir}}_{1_X}}{S_-}\mid\psi^{\mathrm{vir}}_{1_X}\rangle\langle\psi^{\mathrm{vir}}_{1_X}|_B\widehat{M}^{(k)}_{0_X} + \right.$$

$$\left.\frac{\tilde{p}^{\mathrm{vir}}_{0_X}}{S_-}\mid\psi^{\mathrm{vir}}_{0_X}\rangle\langle\psi^{\mathrm{vir}}_{0_X}|_B\widehat{M}^{(k)}_{1_X}\right]$$

$$= \frac{p^{\mathrm{vir}}_{1_X}c}{S_-p_{0_X}p_{X_B}}P^{(k)}(q_{0x,0x}\mid\mathrm{Act}) + \frac{1}{S_-p_{Z_B}}P^{(k)}(\mathrm{ph}\mid\mathrm{Act})$$

where we have used **Eq. 38**, namely, the definition of $P^{(k)}$(ph|Act) and the fact that the states $|\psi^{\mathrm{vir}}_{\alpha_X}\rangle_B = \frac{1}{2}(|\psi_{0_Z}\rangle_B + (-1)^{\alpha}|\psi_{1_Z}\rangle_B)/\sqrt{\widetilde{p}^{\mathrm{vir}}_{\alpha_X}/p_{Z_A}}$.

Now, we combine **Eqs. 40**, **47**, **53**, and **54** to obtain a relationship for the k^{th} pulse associated with the actual states

$$0 \le p_{Z_B}S_+g^U(\mathrm{Tr}[\hat{P}(|A_+\rangle_{CB})\hat{M}^{(k)}_+],1-\epsilon)-$$
$$p_{Z_B}S_-g^L\left(\frac{p^{\mathrm{vir}}_{1_X}c}{S_-p_{0_X}p_{X_B}}P^{(k)}(q_{0x,0x}\mid\mathrm{Act})+\right. \tag{55}$$
$$\left.\frac{1}{S_-p_{Z_B}}P^{(k)}\Big(\mathrm{ph}\mid\mathrm{Act}\Big),1-\epsilon\right)$$

with $\mathrm{Tr}[\widehat{P}(|A_+\rangle_{\mathrm{CB}})\widehat{M}^{(k)}_+]$ given by **Eq. 48**. We stress that **Eq. 55** does not depend on $\widetilde{p}^{\mathrm{vir}}_{\alpha_X}$, and the inner products $|_{CB}\langle A_+|R_+\rangle_{CB}|$ and $|_{CB}\langle A_-|R_-\rangle_{CB}|$ have the value of 1 − ϵ. Therefore, **Eq. 55** does not depend on the inner products of the side-channel states or on the inner products between the channel states and the qubit states. In particular, this means that our security proof works ev do not know anything about the side-channel states, and, thus, they can vary in time and depend on the previous pulses, as discussed above. Note that **Eq. 55** is the required relationship for the actual states. This finishes the deviation evaluation part.

Last, we have to convert **Eq. 55** into a relationship in terms of numbers rather than probabilities. The procedure for this step is quite standard (*17*, *18*, *26*, *47*). For this, first, note that $g^U(x, y)$ and $-g^L(x, y)$ are concave functions with respect to $0 \le x \le 1$ for any fixed $0 \le y \le 1$. In addition, recall that the use of Azuma's inequality (*37*) or Kato's inequality (*38*) converts the summed probabilities into the corresponding number in the asymptotic limit of a large number of pulses sent. That is, for $N \to \infty$, $\sum_k^N P^{(k)}(q_{j,j_B}\mid\mathrm{Act}) \to N(q_{j,j_B}\mid\mathrm{Act})$, where $N(q_{jj_B}$ | Act) is the number of events with Alice's setting choice equal to j and Bob's outcome equal to j_B in the experiment after N runs of the

$$
\begin{aligned}
0 \le \quad & S_+ g^U \Bigg(\frac{p_{1_X}^{\mathrm{vir}} a}{S_+ p_{0_Z} p_{X_B}} \frac{N(q_{0z,0x}|\mathrm{Act})}{N} \\
& \frac{p_{1_X}^{\mathrm{vir}} b}{S_+ p_{1_Z} p_{X_B}} \frac{N(q_{1z,0x}|\mathrm{Act})}{N} + \\
& \frac{p_{0_X}^{\mathrm{vir}}}{S_+ p_{0_X} p_{X_B}} \frac{N(q_{0x,1x}|\mathrm{Act})}{N}, 1-\epsilon \Bigg) - \\
& S_- g^L \Bigg(\frac{p_{1_X}^{\mathrm{vir}} c}{S_- p_{0_X} p_{X_B}} \frac{N(q_{0x,0x}|\mathrm{Act})}{N} + \\
& \frac{1}{S_- p_{Z_B}} \frac{N(\mathrm{ph}|\mathrm{Act})}{N}, 1-\epsilon \Bigg)
\end{aligned}
\tag{56}
$$

This inequality involves only the number of events defined in the actual protocol, and by solving this with respect to *N*(ph|Act), the security proof is done. We emphasize that our proof is valid for any coherent attack because **Eqs. 55** and **56** hold for any $\widehat{K}_{\tilde{e}}^{(k)}$.

Arbitrarily long-range pulse correlations

In this section, we show how to extend our analysis to accommodate arbitrarily long-range correlations between the pulses. To simplify the discussion, we consider the three-state protocol, but this formalism can be easily extended to any number of states. Our starting point is the assumption in **Eq. 13**. We rewrite it here for convenience

$$
\left| {}_{B_k}\left\langle \psi_{j_k|j_{k-1},\cdots,j_{w+1},\tilde{j}_w,j_{w-1},\cdots,j_1} \;\middle|\; \psi_{j_k|j_{k-1},\cdots,j_{w+1},j_w,j_{w-1},\cdots,j_1} \right\rangle_{B_k} \right|^2 \ge 1-\epsilon_{k-w} \tag{57}
$$

where *k* ∈ {1,2, ⋯, *n*} and 1 ≤ *w* ≤ *k* − 1. Note that the difference between both states is in the j_w^{vir} index. Also, the right-hand side of **Eq. 57** does not depend on the indices j_k, j_{k-1}, ⋯, j_1 and ~j_w, and the term *k* − *w* is associated with the correlation under consideration. For example, when *k* − *w* = 1, it refers to the nearest-neighbor pulse correlation considered in Results. Furthermore, without loss of generality, we can assume the relation

$$
{}_{B_k}\left\langle \psi_{j_k|j_{k-1},\cdots,j_{w+1},j_w,j_{w-1},\cdots,j_1} \;\middle|\; \psi_{j_k|j_{k-1},\cdots,j_{w+1},0_X,j_{w-1},\cdots,j_1} \right\rangle_{B_k} \ge 0 \tag{58}
$$

after appropriately choosing the phase of the state $|j_w\rangle_{A_w}$. Using these assumptions, an extension of our framework is now presented. That is, we show how to obtain a lower bound on the parameter a_j

where $j_\zeta \in \{0_Z, 1_Z, 0_X\}$ and $\zeta \in \{1, 2, \cdots, n\}$. Note that j_0 represents having no condition, and the state $|\psi_{j_\zeta | j_{\zeta-1}, \cdots, j_1}\rangle_{B_\zeta}$ represents the long-range pulse correlations, that is, the state of the ζth pulse depends on all the previous setting choices. As before, we suppose that Alice measures her ancilla systems up to the kth pulse. More precisely, she measures the first $k - 1$ systems of $\{A_\zeta\}_{\zeta = \{1, 2, \cdots, n\}}$ by using the computational basis. The whole (unnormalized) state can then be expressed as

$$\begin{aligned}|\Psi_{j'_{k-1},\cdots,j'_1}\rangle_{\mathrm{AB}} &:= \left(\bigotimes_{\tilde{\zeta}=1}^{k-1} |j'_{\tilde{\zeta}}\rangle_{A_{\tilde{\zeta}}} |\psi_{j'_{\tilde{\zeta}}|j'_{\tilde{\zeta}-1},\cdots,j'_1}\rangle_{B_{\tilde{\zeta}}}\right)\\ &\otimes \sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k|j'_{k-1},\cdots,j'_1}\rangle_{B_k}\\ &\otimes \left(\sum_{j_n}\cdots\sum_{j_{k+1}} \bigotimes_{\zeta=k+1}^{n} |j_\zeta\rangle_{A_\zeta} |\psi_{j_\zeta|j_{\zeta-1},\cdots,j_{k+1},j_k,j'_{k-1},\cdots,j'_1}\rangle_{B_\zeta}\right)\end{aligned} \tag{60}$$

To clarify, after Alice's measurement, the state $|\Psi\rangle_{AB}$ in **Eq. 59** becomes the state $|\Psi_{j'_{k-1},\ldots,j'_1}\rangle_{AB}$ in **Eq. 60**, where the subscripts indicate its dependence on the previous measurement results $j'_{k-1}, \ldots, j'_1$. Note that **Eq. 60** corresponds to **Eq. 6** in Results.

Now, similar to our analysis for the nearest-neighbor pulse correlations, to see how the information j_k is encoded in the state $|\Psi_{j'_{k-1},\ldots,j'_1}\rangle_{AB}$, defined in **Eq. 60**, we rewrite it as

$$\begin{aligned}|\Psi_{j'_{k-1},\cdots,j'_1}\rangle_{\mathrm{AB}} &= \left(\bigotimes_{\tilde{\zeta}=1}^{k-1} |j'_{\tilde{\zeta}}\rangle_{A_{\tilde{\zeta}}} |\psi_{j'_{\tilde{\zeta}}|j'_{\tilde{\zeta}-1},\cdots,j'_1}\rangle_{B_{\tilde{\zeta}}}\right)\\ &\otimes \sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k|j'_{k-1},\cdots,j'_1}\rangle_{B_k}\\ &\otimes \Big(a_{j_k,j'_{k-1},\cdots,j'_1} |\Phi_{j'_{k-1},\cdots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n} +\\ &b_{j_k,j'_{k-1},\cdots,j'_1} |\Phi^{\perp}_{j_k,j'_{k-1},\cdots,j_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n}\Big)\end{aligned} \tag{61}$$

where $|\Phi_{j'_{k-1},\cdots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n}$ and $|\Phi^{\perp}_{j_k,j'_{k-1},\cdots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n}$ are normalized states, and $|\Phi_{j'_{k-1},\cdots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n}$ is orthogonal to $|\Phi^{\perp}_{j_k,j'_{k-1},\cdots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n}$. Recall that the

PDF
Help

$|\psi_{j_k|j'_{k-1},\ldots,j'_1}\rangle_{B_k} \otimes |\Phi^{\perp}_{j_k|j'_{k-1},\ldots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n}$ in **Eq. 61** corresponds to $|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{A_{k+1},\ldots,A_n,B_k,B_{k+1},\ldots,B_n}$ in **Eq. 11**.

Next, we obtain a lower bound on the coefficient $a_{j_k,j'_{k-1},\ldots,j'_1}$. For $|\Phi_{j'_{k-1},\ldots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n}$, one may choose a state such that it becomes independent of j_k. One of these choices could be

$$|\Phi_{j'_{k-1},\ldots,j'_1}\rangle_{A_{k+1},\ldots,A_n,B_{k+1},\ldots,B_n} := \sum_{j_n}\cdots\sum_{j_{k+1}}\bigotimes_{\zeta=k+1}^{n}|j_\zeta\rangle_{A_\zeta}|\psi_{j_\zeta|j_{\zeta-1},\ldots,j_{k+1},0_X,j'_{k-1},\ldots,j'_1}\rangle_{B_\zeta} \tag{62}$$

which is the state of the last (n – k) systems in **Eq. 60** with only the k^{th} index of $|\psi_{j_\zeta|j_{\zeta-1},\ldots,j_{k+1},j_k,j'_{k-1},\ldots,j'_1}\rangle_{B_\zeta}$ being fixed to 0_X. This state is independent of j_k. Since $a_{j_k,j'_{k-1},\ldots,j'_1}$ is equal to the inner product between the state given by **Eq. 62** and the vector

$$\sum_{j_n}\cdots\sum_{j_{k+1}}\bigotimes_{\zeta=k+1}^{n}|j_\zeta\rangle_{A_\zeta}|\psi_{j_\zeta|j_{\zeta-1},\ldots,j_{k+1},j_k,j'_{k-1},\ldots,j'_1}\rangle_{B_\zeta} \tag{63}$$

which is the expression in the last parenthesis of **Eq. 60**, we can evaluate a lower bound for $a_{j_k,j'_{k-1},\ldots,j'_1}$ as

$$\begin{aligned}
|a_{j_k,j'_{k-1},\ldots,j'_1}| &= |\sum_{j_n}\cdots\sum_{j_{k+1}}\prod_{\zeta=k+1}^{n}p_{j_\zeta} \\
& {}_{B_\zeta}\langle\psi_{j_\zeta|j_{\zeta-1},\ldots,j_{k+1},0_X,j'_{k-1},\ldots,j'_1} \mid \psi_{j_\zeta|j_{\zeta-1},\ldots,j_{k+1},j_k,j'_{k-1},\ldots,j'_1}\rangle_{B_\zeta}| \\
&= \sum_{j_n}\cdots\sum_{j_{k+1}}\prod_{\zeta=k+1}^{n}p_{j_\zeta} \\
& |{}_{B_\zeta}\langle\psi_{j_\zeta|j_{\zeta-1},\ldots,j_{k+1},0_X,j'_{k-1},\ldots,j'_1} \mid \psi_{j_\zeta|j_{\zeta-1},\ldots,j_{k+1},j_k,j'_{k-1},\ldots,j'_1}\rangle_{B_\zeta}| \\
&\geq \sum_{j_n}\cdots\sum_{j_{k+1}}\prod_{\zeta=k+1}^{n}p_{j_\zeta}(1-\varepsilon_{\zeta-k})^{1/2} \\
&= \prod_{\zeta=1}^{n-k}(1-\varepsilon_\zeta)^{1/2}
\end{aligned} \tag{64}$$

PDF
Help

http://advances.sciencemag.org/cgi/content/full/6/37/eaaz4487/DC1

REFERENCES AND NOTES

1. ↵ H.-K. Lo, M. Curty, K. Tamaki, Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014). CrossRef Google Scholar

2. ↵ W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003). CrossRef PubMed Google Scholar

3. H.-K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005). CrossRef PubMed Google Scholar

4. ↵ X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005). CrossRef PubMed Google Scholar

5. ↵ H.-K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012). PubMed Google Scholar

6. ↵ A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, W. Tittel, Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (201
Google Scholar

7. T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013). Google Scholar

8. Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, Q. Zhang, J.-W. Pan, Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013). Google Scholar

9. Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.-K. Lo, Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014). Google Scholar

PDF
Help

A. J. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photonics* **10**, 312–315 (2016). Google Scholar

12. ↲ N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**, 022320 (2006). Google Scholar

13. A. Vakhitov, V. Makarov, D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdroppong in quantum cryptography. *J. Mod. Opt.* **48**, 2023–2038 (2001). Google Scholar

14. M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, A. J. Shields, Practical security bounds against the trojan-horse attack in quantum key distribution. *Phys. Rev. X* **5**, 031030 (2015). Google Scholar

15. ↲ K. Tamaki, M. Curty, M. Lucamarini, Decoy-state quantum key distribution with a leaky source. *New J. Phys.* **18**, 065008 (2016). Google Scholar

16. ↲ W. Wang, K. Tamaki, M. Curty, Finite-key security analysis for quantum key distribution with leaky sources. *New J. Phys.* **20**, 083027 (2018). Google Scholar

17. ↲ K. Tamaki, M. Curty, G. Kato, H.-K. Lo, K. Azuma, Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **90**, 052314 (2014). Google Scholar

18. ↲ M. Pereira, M. Curty, K. Tamaki, Quantum key distribution with flawed and leaky sources. *npj Quantum Inf.* **5**, 62 (2019). Google Scholar

19. ↲ D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325–360 (2004). Google Scholar

20. H.-K. Lo, J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases. *Quantum Inf. Comput.* **8**, 431–458 (2007). Google Scholar

21. ↲ M. Koashi, Simple security proof of quantum key distribution based on complementarity. *New J. P*
045018 (2009). Google Scholar

22. ↲ Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, C. C. W. Lim, Characterising the correlations of prepare-and-measure quantum networks. *npj Quantum Inf.* **5**, 17 (2019). Google Scholar

23. P. J. Coles, E. M. Metodiev, N. Lütkenhaus, Numerical approach for unstructured quantum key distribution. *Nat. Commun.* **7**, 11712 (2016). Google Scholar

24. ↲ A. Winick, N. Lütkenhaus, P. J. Coles, Reliable numerical key rates for quantum key distribution. *Quantum* **2**, 77 (2018). Google Scholar

25. ↲ Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, K. Tamaki, Security of quantum key distribution with light sources that are not independently and identically distributed. *Phys. Rev. A* **93**, 042325

PDF
Help

27. ↲ K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, A. Tomita, Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Inf.* **4**, 8 (2018). Google Scholar

28. ↲ C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 9 to 12 December 1984, pp. 175–179.

29. ↲ D. Bruß, Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018–3021 (1998). CrossRef Google Scholar

30. ↲ V. Scarani, A. Acín, G. Ribordy, N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004). PubMed Google Scholar

31. ↲ K. Inoue, E. Waks, Y. Yamamoto, Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89**, 037902 (2002). CrossRef PubMed Google Scholar

32. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, Y. Yamamoto, Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nat. Photonics* **1**, 343–348 (2007). Google Scholar

33. ↲ D. Stucki, N. Brunner, N. Gisin, V. Scarani, H. Zbinden, Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87**, 194108 (2005). Google Scholar

34. ↲ L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptographic systems by tailored bright illumination. *Nat. Photonics* **4**, 686–689 (2010). CrossRef Web of Science Google Scholar

35. ↲ I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, Full-field implementation perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2**, 349 (2011). PubMed Google Scholar

36. ↲ C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, X. Ma, Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Inf. Comput.* **9**, 0131–0165 (2009). Google Scholar

37. ↲ K. Azuma, Weighted sums of certain dependent random variables. *Tohoku Math. J.* **19**, 357–367 (1967). Google Scholar

38. ↲ G. Kato, Concentration inequality using unconfirmed knowledge. arXiv:**2002.04357** (2020).

39. ↲ M. Christandl, R. König, R. Renner, Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 020504 (2009). PubMed Google Scholar

PDF
Help

weak coherent states. *Phys. Rev. A* **62**, 022306 (2000). Google Scholar

43. ↲ F. Xu, B. Qi, H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12**, 113026 (2010). Google Scholar

44. T. Honjo, K. Inoue, H. Takahashi, Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer. *Opt. Lett.* **29**, 2797–2799 (2004). PubMed Google Scholar

45. ↲ G. Li, Recent advances in coherent optical communication. *Adv. Opt. Photon.* **1**, 279–307 (2009). Google Scholar

46. ↲ P. W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000). CrossRef PubMed Web of Science Google Scholar

47. ↲ K. Tamaki, N. Lütkenhaus, M. Koashi, J. Batuwantudawe, Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse. *Phys. Rev. A* **80**, 032302 (2009). Google Scholar

Acknowledgments: We thank G. Currás Lorenzo and Á. Navarrete for very valuable discussions. We also thank an anonymous referee for finding a mistake in a previous version of this manuscript. **Funding:** This work was supported by the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through the grant TEC2017-88243-R, and the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement no. 675662 (project QCALL). K.T. acknowledges support from JSPS KAKENHI grant nos. JP18H05237 18H05237 and JST-CREST JPMJCR 1671. **Author contributions:** M.P. and K.T. conceived the initial idea of how to deal with pulse correlations. K.T. constructed the RT through discussions with all the other authors. Then, G.K., A.M., and M.C. contributed to the development and discussion of the initial idea and the RT with M.P. and K.T performed the numerical simulations. All authors contributed to writing the manuscript. **Com** **interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

PDF
Help

View Abstract

Inducing superconductivity in Weyl semimetal microstructures by selective ion sputtering
Maja D. Bachmann et al., Sci Adv, 2017

Heralded quantum steering over a high-loss channel
Morgan M. Weston et al., Sci Adv, 2018

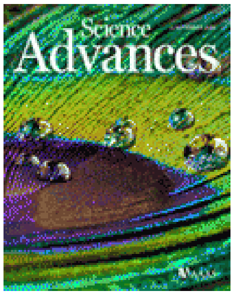
High-dimensional quantum cloning and applications to quantum hacking.
Frédéric Bouchard et al., Sci Adv, 2017

quantum key distribution based on hybrid encoding
Du Cong et al., Acta Physica Sinica, 2020

Reference-frame-independent quantum key distribution with an untrusted source*
Jia-Ji Li et al., Chinese Physics B, 2020

Experimental Point-to-Multipoint Plug-and-Play Measurement-Device-Independent Quantum Key Distribution Network
Guang-Zhao Tang et al., Chinese Physics Letters, 2019

Security Analysis of Stochastic Routing Scheme in Grid-Shaped Partially-Trusted Relay Quantum Key Distribution Network
Xingtong Liu et al., Chinese Journal of Electronics, 2018



Science Advances
Vol 6, No. 37
09 September 2020

Table of Contents

PDF
Help

View this article with *LENS*

ARTICLE TOOLS

- Email
- Print
- Request permissions
- Share
- Download Powerpoint
- Alerts
- Citation tools

MY SAVED FOLDERS

- Save to my folders

SIMILAR ARTICLES IN:

- PubMed
- Google Scholar

NAVIGATE THIS ARTICLE

- Article
  - Abstract
  - INTRODUCTION
  - RESULTS
  - DISCUSSION
  - MATERIALS AND METHODS
  - SUPPLEMENTARY MATERIALS
  - REFERENCES AND NOTES
- Figures & Data
- Info & Metrics
- eLetters
- PDF

Read the Latest Issue of *Science*

20 November 2020

Vol 370, Issue 6519

PDF

Help

FEATURE

Tomorrow's catch

BIOTECH REGULATION

Community-led governance for gene-edited crops

LINGUISTICS

Alphabets and their origins

SCI COMMUN

News at a glance

DRUG DISCOVERY

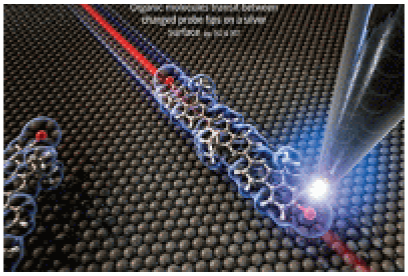


Table of Contents

About Us

Journals
News from Science
Leadership
Team Members
Work at AAAS

For Advertisers

Advertising Kit
Awards and Prizes
Custom Publishing
Webinars

For Authors

Submit
Information for Authors
Editorial Policies

PDF
Help

For Librarians

Manage Your Institutional Subscription
Information for Librarians
Request a Quote
FAQs

Related Sites

AAAS.org
EurekAlert!
Science in the Classroom
Science Magazine Japanese

Help

Science Advances ISSN 2375-2548.

Terms of Service

Privacy Policy

Contact AAAS

PDF

Help