IEEE Transactions on Quantum Engineering

Received 12 May 2022; revised 4 March 2023; accepted 7 March 2023; date of publication 31 March 2023; date of current version 13 June 2023.

Digital Object Identifier 10.1109/TQE.2023.3261262

Security Proof Against Collective Attacks for an Experimentally Feasible Semiquantum Key Distribution Protocol

WALTER OLIVER KRAWEC[1], ROTEM LISS[2,3], AND TAL MOR[2]

[1]Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269 USA
[2]Department of Computer Science, Technion—Israel Institute of Technology, Haifa 3200003, Israel
[3]Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, Montréal, QC H3C 3J7, Canada

Corresponding author: Walter Oliver Krawec (e-mail: walter.krawec@uconn.edu).

The work of Walter Oliver Krawec was supported in part by the National Science Foundation under Grant 1812070. The work of Rotem Liss and Tal Mor was supported in part by the Research and Technology Unit of the Israeli Ministry of Defense and in part by the Helen Diller Quantum Center at the Technion. The work of Rotem Liss was supported in part by the Canada Research Chair Program.

ABSTRACT Semiquantum key distribution (SQKD) allows two parties (Alice and Bob) to create a shared secret key, even if one of these parties (say, Alice) is classical. However, most SQKD protocols suffer from severe practical security problems when implemented using photons. The recently developed "Mirror protocol" (Boyer, Katz, Liss, and Mor, 2017) is an experimentally feasible SQKD protocol overcoming those drawbacks. The Mirror protocol was proven robust (namely, it was proven secure against a limited class of attacks including all noiseless attacks), but its security in case some noise is allowed (natural or due to eavesdropping) has not been proved yet. Here, we prove the security of the Mirror protocol against a wide class of quantum attacks ("collective attacks"), and we evaluate the allowed noise threshold and the resulting key rate.

INDEX TERMS Quantum information, quantum key distribution (QKD), security.

I. INTRODUCTION

Quantum key distribution (QKD) protocols [1] make it possible for two parties, Alice and Bob, to generate a secret shared key. This key is information-theoretically secure against any possible attack that can be applied by an all-powerful adversary Eve limited only by the laws of physics.

Semiquantum key distribution (SQKD) [2] allows Alice and Bob to achieve the same goal even if one of them is *classical* in nature. For example, an SQKD protocol can allow a classical Alice and a quantum Bob to generate a secret shared key, where Alice is only allowed to perform operations in the computational basis $\{|0\rangle, |1\rangle\}$ and reflect qubits that go through her laboratory untouched. Previously suggested SQKD protocols include "QKD with Classical Bob" [2], [3], "QKD with Classical Alice" [4], [5], and many others (see, e.g., [6], [7], [8], [9], [10], [11], [12], [13], and [14]).

SQKD protocols use the notion of "classical operations" performed by a "classical party." However, in the 16 years since the publication of the original paper introducing SQKD protocols [2], we noticed that the term "classical party" sometimes causes confusion: in other hybrid quantum–classical protocols described in the literature (see, e.g., [15] and [16]), the term "classical operations" is kept only to operations performed on *classical* bits, and it is implicitly or explicitly assumed that all classical parties have no access to quantum states (e.g., qubits) and cannot perform any operation on them. On the other hand, classical parties in SQKD protocols *can* perform limited operations on quantum states.

To avoid this confusion, we introduce here the notion of *CloQ—Classical Operations on Quantum Data*. CloQ protocols involve at least one classical party (or CloQ party) who is restricted to using the four classical operations 1–4 described below for interacting with a quantum channel. CloQ protocols have been shown to exhibit highly interesting theoretical properties; currently, their most well-understood application is SQKD (see [17] for a recent review), but CloQ protocols have also been devised to solve other cryptographic problems, including secret sharing [18], [19], [20], secure direct communication [21], [22], [23], [24], identity verification [25], [26], and private state comparison [27]. CloQ protocols may even be devised in the future for quantum verification by defining a CloQ variant of quantum prover interactive proofs (QPIP) [28], which could allow a CloQ party to verify quantum computations performed by a fully quantum center (or prover). Possible generalizations of this idea

include verification protocols for a CloQ verifier and a computationally unbounded prover (a known concept in complexity theory), as well as blind verification protocols where the quantum prover is oblivious to the computations it performs at the CloQ verifier's request.

The classical party in a CloQ protocol is restricted to limited classical operations but is capable of performing these operations on a quantum communication channel. Such protocols rely on a two-way quantum channel, which makes security analyses difficult (similarly to other two-way QKD protocols; see, e.g., [29], [30], [31], and [32]), especially in practical and experimental settings allowing a quantum state to travel from one party to the classical party and back to the original sender. The classical party is restricted to using the following classical operations (see, e.g., [2] and [3]).

1) Preparing a qubit in one of the computational basis states: $|0\rangle$ or $|1\rangle$.
2) Measuring a qubit in the computational basis $\{|0\rangle, |1\rangle\}$.
3) Ignoring the qubit, letting it pass through their laboratory back to the sender undisturbed.
4) Permuting incoming qubits and returning them to the sender in a new order, but otherwise undisturbed.

CloQ protocols, and in particular SQKD protocols, are fascinating from a theoretical point of view because they attempt to find out "how quantum" a protocol must be to gain an advantage over a classical protocol: for example, it is impossible to perform secure key distribution using *only* classical communication (unless we make computational assumptions), but SQKD protocols show that one classical party and one quantum party *can* achieve information-theoretically secure key distribution.

While the importance of SQKD protocols is clear from a theoretical standpoint, their practical importance is more subtle. Since the practical implementation of fully quantum QKD (e.g., BB84) is a well-studied problem with numerous high-speed implementations, the reader may rightly wonder at the practical importance of studying SQKD protocols. However, there are several advantages to this study from a practical perspective. First, semiquantum communication is a practical technology, as some experimental proofs of concept have been demonstrated [33], [34], [35]. Second, while these experimental proofs of concept required hardware similar to their fully quantum counterparts, the ability to perform CloQ operations may become cheaper as technology advances, so it is important to study alternative implementation methodologies now. Third, several semiquantum protocols rely on imbalanced user capabilities—for example, the fully quantum user can invest in higher quality equipment, while the classical user can rely on cheaper devices (e.g., measurement devices with lower efficiency), leading to interesting use-case scenarios. Fourth, the security proof methodologies developed for practical SQKD protocols can be translated to other QKD protocols with potential new insights and countermeasure strategies; for example, proof techniques developed for practical SQKD can demonstrate how to compensate for imperfect or imbalanced hardware capabilities or partial device failures. Last but not least, if one wants to hide from some of the users the fact that quantum cryptography is used, the true description of the classical operations 1–4 can indeed hide any hint from such an oblivious party; after all, also when using classical data, one can either check if the bit is 0/1 or choose to avoid checking it. Taken together, not only is the study of SQKD protocols (and CloQ protocols in general) important from a theoretical standpoint, but it can also have highly interesting practical implications.

However, while the capabilities of SQKD protocols in the ideal (perfect-qubit) scenario are now fairly well understood, and while, in principle, such protocols could allow simpler devices, the security and performance of SQKD protocols under *practical* attacks are yet to be verified. In fact, as pointed out in [36] and [37], many existing SQKD protocols are experimentally infeasible: it is not known how to implement them in a secure way. Specifically, many SQKD protocols use the SIFT classical operation, which requires the classical user to first *measure* the incoming quantum state in the computational basis $\{|0\rangle, |1\rangle\}$ and then *resend* the measured state back to the quantum user; the experimental implementations of this operation are vulnerable to some "tagging attacks" described in [36], [37], and [38]. For solving this problem, an experimentally feasible SQKD protocol named the "Mirror protocol" was introduced in [38]; see also [39], which analyzed a simplified variant and attacks on it.

Most SQKD protocols have been proven robust: namely [2], if Eve obtains some secret information, she must cause some errors that may be noticed by Alice and Bob; equivalently, a protocol is "robust" if any attack that induces no errors must give Eve no information. In particular, the Mirror protocol was proven robust in [38]. Proving robustness is a step toward proving security; proving full security of SQKD protocols is difficult because these protocols are usually two-way: for example, Bob sends a quantum state to Alice, and Alice performs a specific classical operation and sends the resulting quantum state back to Bob. A few SQKD protocols also have a security analysis [40], [41], [42], [43], which is usually applicable to an ideal qubit-based description, but not to the more realistic photon-based description. So far, the Mirror protocol has not been proven secure.

In this article, we prove the security of the Mirror protocol against collective attacks. The class of the collective attacks [44], [45], [46] is an important and powerful subclass of possible attacks; the class of the general attacks (also known as the joint attacks; see, e.g., [47], [48], [49], and [50]) includes all theoretical attacks allowed by quantum physics. Security against collective attacks is conjectured (and, in some security notions, proved [51], [52], [53]) to imply security against general attacks. However, some existing security proofs of SQKD protocols against general attacks may in fact be limited to collective attacks, because they use de Finetti's theorem and similar techniques (see [51] and

[52]) that can directly be applied only to entanglement-based protocols.[1] In particular, to use these techniques, one usually requires some reduction from the two-way protocol to an entanglement-based protocol. Such reduction techniques are known for certain classes of two-way protocols [32], [54], but it is not known how to perform these reductions for all two-way protocols. In particular, the method of Beaudry et al. [32] only applies if the protocol exhibits a certain symmetry property which no semiquantum protocol can have, while the method of Guskind and Krawec [54] is currently only applicable to mediated semiquantum protocols in the ideal qubit scenario. In particular, these previous techniques do not apply to the Mirror protocol we consider in this article. Therefore, in this article, we restrict our analysis to collective attacks.

This article proves the security of the Mirror protocol under a large class of collective attacks, which include the ability of Eve to inject *multiple photons* into the classical user's laboratory, but not into the quantum user's laboratory (attacks of the later kind are left for future analysis, but we briefly discuss them in the beginning of Section III). In addition, we limit our analysis to two-mode quantum communication, leaving more complicated attacks for future research. We assume that Alice's and Bob's devices precisely implement the needed operations [most notably, Alice's classical operations described in (1)–(4)], and without loss of generality, we assume an all-powerful Eve controlling all errors and losses in the quantum channel.

We derive an information-theoretic proof of security against these attacks and simulate the performance of the protocol in a variety of realistic scenarios, including lossy quantum channels, compared to the BB84 protocol. Ultimately, our article shows that SQKD protocols hold the potential to be secure and feasible in practice, and not just "secure in ideal conditions." The methods and techniques we present in this article may also be applicable to security proofs of other SQKD protocols or even other two-way QKD protocols where users are limited in some manner in their quantum capabilities.

II. MIRROR PROTOCOL

This section is partially based on [39].

For describing the Mirror protocol, we assume a photonic implementation consisting of two modes: the mode of the qubit state $|0\rangle$ and the mode of the qubit state $|1\rangle$ (in the following, we call them "the $|0\rangle$ mode" and "the $|1\rangle$ mode," respectively). For example, the $|0\rangle$ mode and the $|1\rangle$ mode can represent two different polarizations or two different time bins. As elaborated in [38], the Mirror protocol can intuitively be described in terms of photon pulses that correspond to two distinct time bins, which means that the classical party (Alice) can only perform operations on the two distinct time bins (corresponding to the computational basis $\{|0\rangle, |1\rangle\}$) and not on their superpositions (corresponding, for example, to the Hadamard basis $\{|+\rangle, |-\rangle\}$).

A. SINGLE-PHOTON CASE

We use the Fock space notations: if there is exactly one photon, the Fock state $0, 1\rangle$ represents one photon in the $|0\rangle$ mode, and the Fock state $1, 0\rangle$ represents one photon in the $|1\rangle$ mode (and, thus, our Hilbert space is the qubit space Span$\{|0, 1\rangle, |1, 0\rangle\}$). We can extend the qubit space to a 3-dimensional Hilbert space by adding the Fock "vacuum state" $|0, 0\rangle$, which represents an absence of photons. Similarly, in the Hadamard basis, we define the Fock state $|0, 1\rangle_{\mathrm{x}} \triangleq \frac{|0,1\rangle+|1,0\rangle}{\sqrt{2}}$ (equivalent to the $|+\rangle$ state) and the Fock state $|1, 0\rangle_{\mathrm{x}} \triangleq \frac{|0,1\rangle-|1,0\rangle}{\sqrt{2}}$ (equivalent to the $|-\rangle$ state).

In the Mirror protocol (regardless of the specific implementation), in each round, Bob sends to Alice the initial state $|+\rangle_{\mathrm{B}}$, which is equivalent to $|0, 1\rangle_{\mathrm{x,B}} \triangleq \frac{|0,1\rangle_{\mathrm{B}}+|1,0\rangle_{\mathrm{B}}}{\sqrt{2}}$. Then, Alice prepares an ancillary state in the initial vacuum state $|0, 0\rangle_{\mathrm{A_{anc}}}$ and chooses *at random* one of the following four classical operations (defined on any Fock state she may possibly get, due to Eve's single-photon attacks possible in this case).

1) **I** (CTRL): Reflect all photons toward Bob, without measuring any photon. The mathematical description is
$$I|0, 0\rangle_{\mathrm{A_{anc}}}|m_1, m_0\rangle_{\mathrm{B}} = |0, 0\rangle_{\mathrm{A_{anc}}}|m_1, m_0\rangle_{\mathrm{B}}. \quad (1)$$
2) $\mathbf{S_1}$ (SWAP-10): Reflect all photons in the $|0\rangle$ mode toward Bob and measure all photons in the $|1\rangle$ mode. The mathematical description is
$$S_1|0, 0\rangle_{\mathrm{A_{anc}}}|m_1, m_0\rangle_{\mathrm{B}} = |m_1, 0\rangle_{\mathrm{A_{anc}}}|0, m_0\rangle_{\mathrm{B}}. \quad (2)$$
3) $\mathbf{S_0}$ (SWAP-01): Reflect all photons in the $|1\rangle$ mode toward Bob and measure all photons in the $|0\rangle$ mode. The mathematical description is
$$S_0|0, 0\rangle_{\mathrm{A_{anc}}}|m_1, m_0\rangle_{\mathrm{B}} = |0, m_0\rangle_{\mathrm{A_{anc}}}|m_1, 0\rangle_{\mathrm{B}}. \quad (3)$$
4) **S** (SWAP-ALL): Measure all photons, without reflecting any photon toward Bob. The mathematical description is
$$S|0, 0\rangle_{\mathrm{A_{anc}}}|m_1, m_0\rangle_{\mathrm{B}} = |m_1, m_0\rangle_{\mathrm{A_{anc}}}|0, 0\rangle_{\mathrm{B}}. \quad (4)$$

We note that in the above mathematical description, Alice measures her ancillary state $|\cdot\rangle_{\mathrm{A_{anc}}}$ in the computational basis $\{|0\rangle, |1\rangle\}$ and sends back to Bob the $|\cdot\rangle_{\mathrm{B}}$ state.

The states sent from Alice to Bob (without any error, loss, or eavesdropping) and their interpretations, depending on Alice's random choice of a classical operation and on whether Alice detected a photon or not, are detailed in Table 1.

B. MULTIPHOTON CASE

Most generally, we need to describe Alice's operation on a general state, because Eve can attack the state sent from Bob to Alice. The Fock state $|m_1, m_0\rangle$ represents m_1 indistinguishable photons in the $|1\rangle$ mode and m_0 indistinguishable

[1] Applying de Finetti's theorem and similar techniques to prepare-and-measure protocols (including SQKD protocols) is usually easy for one-way QKD protocols, but it does not necessarily work for two-way protocols.

TABLE 1. State Sent From Alice to Bob in the Mirror Protocol Without Errors or Losses, and Its Interpretation, Depending on Alice's Random Choice of a Classical Operation and on Whether Alice Detected a Photon or Not

Alice's Operation	Did Alice Detect a Photon?	State Sent to Bob	Round Type	Raw Key Bit
CTRL	no (happens with certainty)	$\|0,1\rangle_{\mathrm{x,B}}$	"test"	none
SWAP-10	no (happens with probability $\frac{1}{2}$)	$\|0,1\rangle_{\mathrm{B}}$	"raw key"	0
SWAP-10	yes (happens with probability $\frac{1}{2}$)	$\|0,0\rangle_{\mathrm{B}}$	"raw key"	none
SWAP-01	no (happens with probability $\frac{1}{2}$)	$\|1,0\rangle_{\mathrm{B}}$	"raw key"	1
SWAP-01	yes (happens with probability $\frac{1}{2}$)	$\|0,0\rangle_{\mathrm{B}}$	"raw key"	none
SWAP-ALL	yes (happens with certainty)	$\|0,0\rangle_{\mathrm{B}}$	"SWAP-ALL"	none

TABLE 2. All the Probabilities Alice and Bob Need to Estimate in Order to Compute the Key Rate in Theorem 1

Notation	Definition	Round Type This Occurs
$\langle E_0\|E_0\rangle_{\mathrm{E}}$	Probability that Alice and Bob get raw key bits 0, 0, respectively	"raw key"
$\langle E_1\|E_1\rangle_{\mathrm{E}}$	Probability that Alice and Bob get raw key bits 0, 1, respectively	"raw key"
$\langle E_2\|E_2\rangle_{\mathrm{E}}$	Probability that Alice and Bob get raw key bits 1, 0, respectively	"raw key"
$\langle E_3\|E_3\rangle_{\mathrm{E}}$	Probability that Alice and Bob get raw key bits 1, 1, respectively	"raw key"
M	Probability that both Alice and Bob get raw key bits	"raw key"
$p_{0,+}$	Probability that Alice gets raw key bit 0, and Bob observes $\|+\rangle$	"raw key" (with mismatched bases)
$p_{1,+}$	Probability that Alice gets raw key bit 1, and Bob observes $\|+\rangle$	"raw key" (with mismatched bases)
$p_{+,+}$	Probability that Bob observes $\|+\rangle$	"test"
$p_{\texttt{CTRL:0}}$	Probability that Bob observes $\|0,1\rangle$	"test" (with mismatched bases)
$p_{\texttt{CTRL:1}}$	Probability that Bob observes $\|1,0\rangle$	"test" (with mismatched bases)
$p_{\texttt{double}}$	Probability that Alice observes a "double-click" event ($\|1,1\rangle$)	"SWAP-ALL"
$p_{\texttt{create:0}}$	Probability that Alice observes $\|0,0\rangle$, and Bob observes $\|0,1\rangle$	"SWAP-ALL"
$p_{\texttt{create:1}}$	Probability that Alice observes $\|0,0\rangle$, and Bob observes $\|1,0\rangle$	"SWAP-ALL"

photons in the $|0\rangle$ mode. More details about the Fock space notations are given in [38]; using these mathematical notations is vital for describing and analyzing all practical attacks on a QKD protocol (see [55] for details and examples).

The mathematical description of the Mirror protocol in this multiphoton case remains *identical* to its description in Section II-A. However, in this case, Alice's classical operations are defined on *any* general Fock state, because Eve's attack can include any multiphoton pulse.

C. BOB'S FINAL MEASUREMENTS AND CLASSICAL POSTPROCESSING

In both cases described in Section II-A and II-B, Bob finally measures the incoming state in a random basis (either the computational basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$). We assume here, as is true in most experimental setups, that Alice and Bob use detectors and not counters: namely, their detectors cannot *count* the number of incoming photons. Therefore, when a detector clicks, Alice and Bob cannot know whether it detected a single-photon pulse (a single photon in its measured mode) or a multiphoton pulse (more than one photon in its measured mode).

After completing all rounds, Alice and Bob perform *classical postprocessing:* Alice sends over the classical channel her operation choices (CTRL, SWAP-x, or SWAP-ALL; she keeps $x \in \{01, 10\}$ in secret); Bob sends over the classical channel his basis choices; and both of them reveal all rounds where they got a loss, and all measurement results each of them got in all testing rounds (CTRL, SWAP-ALL, and a random subset of the SWAP-x rounds, for which Alice also reveals her values of $x \in \{01, 10\}$) and in all mismatched rounds (such as rounds in which Alice used SWAP-10 and Bob used the Hadamard basis).

In the nontesting rounds, as detailed in Table 1, Alice and Bob share the raw key bit 0 if Alice uses SWAP-10 and detects no photon while Bob measures in the computational basis and detects a photon (or photons) in the $|0\rangle$ mode; similarly, they share the raw key bit 1 if Alice uses SWAP-01 and detects no photon while Bob measures in the computational basis and detects a photon (or photons) in the $|1\rangle$ mode.

Now, Alice and Bob have enough information for computing all the probabilities they need for finding the key rate (that are detailed later, in Table 2), so they compute all these probabilities and deduce the final key rate according to the algorithm in Section III-G. If the final key rate is negative, they abort the protocol; otherwise, they perform error correction and privacy amplification in the standard way for QKD protocols. At the end of the protocol, Alice and Bob hold an identical final key that is completely secure against any eavesdropper.

A full description of the Mirror protocol and a proof of its robustness are both available in [38]. An illustration of the Mirror protocol is available as Fig. 1.

III. SECURITY PROOF OF THE MIRROR PROTOCOL AGAINST COLLECTIVE ATTACKS

We now prove the security of the Mirror protocol. For our security proof, we assume that the adversary Eve is restricted to collective attacks—namely, that Eve attacks each round in an independent and identical manner, but she is allowed to postpone the measurement of her private quantum ancilla until any future point in time. Beyond this, we will also

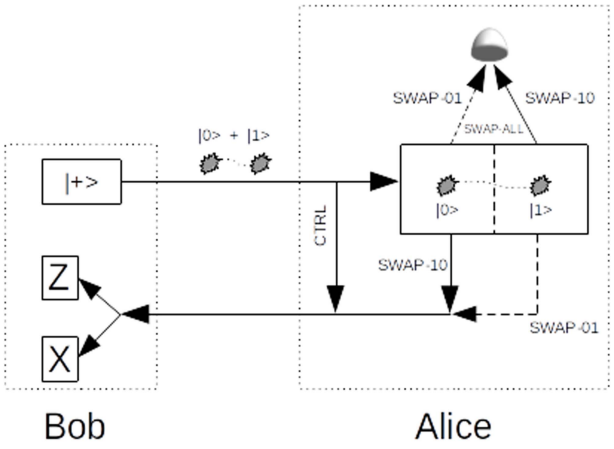

FIGURE 1. Schematic diagram of the Mirror protocol described in Section II.

assume in our security analysis that Eve is allowed to inject *any* signal into the forward channel (linking quantum Bob to classical Alice); in the reverse channel, she is free to perform any quantum unitary probe, but we will assume that the number of photons returning to Bob is at most one. That is, Eve is allowed to inject multiple photons into the channel going to Alice, but on the way back, only a single photon or no photons at all will be returned to Bob. This assumption means that Eve may need to remove photons on the way from Alice to Bob, if she sent multiple photons toward Alice; in Section III-A, we explain how Eve can perform this attack.

The above assumption (that at most one photon is sent toward Bob) is made to simplify the analysis of the return channel. We point out that according to [38], the Mirror protocol is completely *robust* even without this assumption—namely, it is proved robust against *all* multiphoton attacks and *all* kinds of losses and dark counts. However, full *security* analysis of the multiphoton case, including both losses and dark counts, is very difficult even in the simplest one-way standard QKD, and even more so in any standard two-way QKD protocol such as "Plug & Play" [29], "Ping Pong" [30], and LM05 [31] (see also [32]). Furthermore, this case has not been analyzed in security proofs of many other SQKD protocols (see, e.g., [40], [41], [42], and [43]). Therefore, we do not aim to solve this major issue here in the specific case of the Mirror protocol: extending the full security proof to this most general case is left for future research.

Our main result in this section is a lower bound on the von Neumann entropy $S(A|E)$ of the protocol. This allows us to determine a lower bound on the key rate of the protocol using the Devetak–Winter key rate equation [56]. Our main key rate result is summarized in the following theorem (which uses notations defined in Table 2).

Theorem 1: Assuming the attack model discussed above, consider the observable statistics and their respective notations listed in Table 2. Then, the key rate of the protocol is lower-bounded by

$$\begin{aligned}\mathtt{rate} \geq\ & \frac{\langle E_0|E_0\rangle_{\mathrm{E}} + \langle E_3|E_3\rangle_{\mathrm{E}}}{M} \\ & \times \left[H_2\left(\frac{\langle E_0|E_0\rangle_{\mathrm{E}}}{\langle E_0|E_0\rangle_{\mathrm{E}} + \langle E_3|E_3\rangle_{\mathrm{E}}}\right) - H_2(\lambda_1)\right] \\ & + \frac{\langle E_1|E_1\rangle_{\mathrm{E}} + \langle E_2|E_2\rangle_{\mathrm{E}}}{M} \\ & \times \left[H_2\left(\frac{\langle E_1|E_1\rangle_{\mathrm{E}}}{\langle E_1|E_1\rangle_{\mathrm{E}} + \langle E_2|E_2\rangle_{\mathrm{E}}}\right) - H_2(\lambda_2)\right] \\ & - H(A|B), \end{aligned} \tag{5}$$

where

$$\lambda_1 \triangleq \frac{1}{2} + \frac{\sqrt{(\langle E_0|E_0\rangle_{\mathrm{E}} - \langle E_3|E_3\rangle_{\mathrm{E}})^2 + 4\Re^2\langle E_0|E_3\rangle_{\mathrm{E}}}}{2\left(\langle E_0|E_0\rangle_{\mathrm{E}} + \langle E_3|E_3\rangle_{\mathrm{E}}\right)}$$

$$\lambda_2 \triangleq \frac{1}{2} + \frac{\sqrt{(\langle E_1|E_1\rangle_{\mathrm{E}} - \langle E_2|E_2\rangle_{\mathrm{E}})^2 + 4\Re^2\langle E_1|E_2\rangle_{\mathrm{E}}}}{2\left(\langle E_1|E_1\rangle_{\mathrm{E}} + \langle E_2|E_2\rangle_{\mathrm{E}}\right)}$$

$$H_2(x) \triangleq -x\log_2(x) - (1-x)\log_2(1-x)$$

and

$$\begin{aligned} & H(A|B) \\ & = H\left(\frac{\langle E_0|E_0\rangle_{\mathrm{E}}}{M}, \frac{\langle E_1|E_1\rangle_{\mathrm{E}}}{M}, \frac{\langle E_2|E_2\rangle_{\mathrm{E}}}{M}, \frac{\langle E_3|E_3\rangle_{\mathrm{E}}}{M}\right) \\ & \quad - H\left(\frac{\langle E_0|E_0\rangle_{\mathrm{E}} + \langle E_2|E_2\rangle_{\mathrm{E}}}{M}, \frac{\langle E_1|E_1\rangle_{\mathrm{E}} + \langle E_3|E_3\rangle_{\mathrm{E}}}{M}\right) \end{aligned}$$

$$H(x_1, \ldots, x_k) \triangleq -\sum_{j=1}^{k} x_j \log_2(x_j)$$

subject to the following constraint:

$$\begin{aligned} & \Re\left(\langle E_0|E_3\rangle_{\mathrm{E}} + \langle E_1|E_2\rangle_{\mathrm{E}}\right) \\ & \geq \frac{1}{2}p_{+,+} - p_{0,+} - p_{1,+} - \frac{1}{4}(p_{\mathtt{CTRL}:0} + p_{\mathtt{CTRL}:1}) + \frac{1}{2}M \\ & - \frac{1}{\sqrt{2}}\left(\sqrt{p_{\mathtt{create}:1}} + \sqrt{p_{\mathtt{double}}}\right)\left(\sqrt{\langle E_0|E_0\rangle_{\mathrm{E}}} + \sqrt{\langle E_2|E_2\rangle_{\mathrm{E}}}\right) \\ & - \frac{1}{\sqrt{2}}\left(\sqrt{p_{\mathtt{create}:0}} + \sqrt{p_{\mathtt{double}}}\right)\left(\sqrt{\langle E_1|E_1\rangle_{\mathrm{E}}} + \sqrt{\langle E_3|E_3\rangle_{\mathrm{E}}}\right) \\ & - \frac{1}{2}\left(\sqrt{p_{\mathtt{create}:0}} + \sqrt{p_{\mathtt{double}}}\right)\left(\sqrt{p_{\mathtt{create}:1}} + \sqrt{p_{\mathtt{double}}}\right). \end{aligned} \tag{6}$$

We prove Theorem 1 in several steps. First, in Section III-A, we describe Eve's most general attacks that are allowed under our attack model assumptions. Following this, in Section III-C, we present the final quantum state ρ_{ABE} shared by Alice, Bob, and Eve at the end of each round of the protocol, conditioning on a raw-key bit being generated during that round. To complete the proof, we must find a lower bound on the conditional von Neumann entropy $S(A|E)$ corresponding to ρ_{ABE}. For this, in Sections III-B–III-E, we show how Alice

TABLE 3. All Types of Rounds, According to Alice's Random Choice of a Classical Operation (CTRL, SWAP-x ($x \in \{01, 10\}$), or SWAP-ALL) and Bob's Random Choice of a Measurement Basis (Computational or Hadamard)

Round Type	Alice's Operation	Bob's Basis
"raw key"	SWAP-x	computational
mismatched "raw key"	SWAP-x	Hadamard
"test"	CTRL	Hadamard
mismatched "test"	CTRL	computational
"SWAP-ALL"	SWAP-ALL	computational
mismatched "SWAP-ALL"	SWAP-ALL	Hadamard

and Bob can use observable probabilities from all types of rounds (see Table 4) to compute inner products and norms of quantum states appearing in ρ_{ABE}. Then, in Section III-F, we use a theorem from [57] to compute the von Neumann entropy of ρ_{ABE} as a function of our computed inner products. Finally, in Section III-F, we combine all results from Sections III-B–III-E to find lower bounds on the required inner products as functions of the observable probabilities from Table 4, which completes the proof of Theorem 1.

A. EVE'S ATTACKS

1) EVE'S FIRST ATTACK

We first analyze the forward-channel attack—namely, the attack on the way from Bob to Alice. Here, we note that it is to Eve's advantage to simply discard the signal coming from Bob (which should be the same each round and carries no information at this point) and inject a signal of her own, possibly consisting of multiple photons and entangled with her private quantum ancilla.

Specifically, in each round, Bob sends to Alice the same quantum state: $|0,1\rangle_{\text{x,B}} \triangleq \frac{|0,1\rangle_{\text{B}}+|1,0\rangle_{\text{B}}}{\sqrt{2}}$. At this point, Eve performs her *first* attack: she replaces Bob's original state by her own state. Since Bob never prepares alternative initial states, Eve dropping the signal and replacing it with one of her own is the most general strategy she could perform in the collective attack scenario. Without loss of generality, Eve's state is of the form

$$|\psi_0\rangle \triangleq \sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |m_1, m_0\rangle_{\text{B}}|e_{m_1,m_0}\rangle_{\text{E}}. \tag{7}$$

Then, Eve sends subsystem B to Alice and keeps subsystem E as her own ancillary state. Note that as we are dealing with a two-way quantum communication channel, Eve has two opportunities to attack the quantum signal each round. The above equation represents the state after her first attack; however, following Alice's encoding operation, Eve will have a second opportunity to attack. Unlike many one-way protocols, we cannot reduce this to an entanglement-based protocol whereby Eve simply prepares a state and sends part to Alice and part to Bob: although some reductions for two-way (S)QKD protocols to equivalent entanglement-based protocols are known [32], [58], those results cannot be applied to this mirror-based protocol, and therefore, we cannot employ them. Thus, we must analyze Eve's attack in two stages, which makes the analysis somewhat more complicated.

2) EVE'S SECOND ATTACK

Then, Alice performs her classical operation (CTRL, SWAP-10, SWAP-01, or SWAP-ALL) and sends the resulting state back to Bob. Now, Eve performs her *second* attack, described as the unitary operator U_{R}. As explained above, for the second attack, we make the simplifying assumption that Eve always sends *at most one photon*—namely, she sends a superposition of $|0,1\rangle_{\text{B}}$, $|1,0\rangle_{\text{B}}$, and $|0,0\rangle_{\text{B}}$ with her corresponding ancillary states $|g^{0,1}_{m_1,m_0}\rangle_{\text{E}}$, $|g^{1,0}_{m_1,m_0}\rangle_{\text{E}}$, and $|g^{0,0}_{m_1,m_0}\rangle_{\text{E}}$. We emphasize that this simplifying assumption applies only to the second attack, and *not* to the first attack.

Thus, Eve's second attack is of the form

$$\begin{aligned} &U_{\text{R}}|m_1', m_0'\rangle_{\text{B}}|e_{m_1,m_0}\rangle_{\text{E}} \\ &= |0,1\rangle_{\text{B}}|f^{0,1}_{m_1',m_0',m_1,m_0}\rangle_{\text{E}} + |1,0\rangle_{\text{B}}|f^{1,0}_{m_1',m_0',m_1,m_0}\rangle_{\text{E}} \\ &\quad + |0,0\rangle_{\text{B}}|f^{0,0}_{m_1',m_0',m_1,m_0}\rangle_{\text{E}}. \end{aligned} \tag{8}$$

However, in our security proof, we use terms of the following simplified notations:

$$\begin{aligned} &U_{\text{R}}|m_1, m_0\rangle_{\text{B}}|e_{m_1,m_0}\rangle_{\text{E}} \\ &= |0,1\rangle_{\text{B}}|g^{0,1}_{m_1,m_0}\rangle_{\text{E}} + |1,0\rangle_{\text{B}}|g^{1,0}_{m_1,m_0}\rangle_{\text{E}} + |0,0\rangle_{\text{B}}|g^{0,0}_{m_1,m_0}\rangle_{\text{E}} \end{aligned} \tag{9}$$

where we denote $|g^{j,k}_{m_1,m_0}\rangle_{\text{E}} \triangleq |f^{j,k}_{m_1,m_0,m_1,m_0}\rangle_{\text{E}}$. We note that the operation of U_{R} on states $|m_1', m_0'\rangle_{\text{B}}|e_{m_1,m_0}\rangle_{\text{E}}$ where $m_1' \neq m_1$ or $m_0' \neq m_0$ will not appear in our security proof, because these states do not give us meaningful statistics[2] and thus do not contribute to the probabilities in Table 4. We also note that since Eve is all-powerful, she will have no trouble performing any unitary operation, even if it includes a complicated operation for reducing the number of photons.

In both attacks, subsystem B is sent to a legitimate user, while subsystem E is kept as Eve's ancilla.

B. ANALYZING ALL TYPES OF ROUNDS

In Table 3, we classify all rounds into six types that Alice and Bob need to analyze. The rounds are classified according to Alice's random choice of a classical operation and Bob's random choice of a measurement basis.

Notice the use of basis-mismatched rounds. Technically, we could have used only the "standard" (basis-matching) rounds for completing the security proof, by using the Cauchy–Schwarz inequality for finding worst case bounds. However, using the technique of analyzing "mismatched measurements" [59], [60], we can derive a significantly improved formula for the final key rate.

[2]States of the form $U_{\text{R}}|0, m_0\rangle_{\text{B}}|e_{m_1,m_0}\rangle_{\text{E}}$ and $U_{\text{R}}|m_1, 0\rangle_{\text{B}}|e_{m_1,m_0}\rangle_{\text{E}}$ may appear in "raw key" rounds analyzed in Section III-C, but we analyze only rounds which contribute to the raw key, where Alice detects no photon—namely, $m_1 = 0$ or $m_0 = 0$, respectively. In addition, states of the form $U_{\text{R}}|0, 0\rangle_{\text{B}}|e_{m_1,m_0}\rangle_{\text{E}}$ may appear in "SWAP-ALL" rounds analyzed in Section III-E, but we analyze only "double-clicks" of Alice (where Eve's attack U_{R} is irrelevant, although we use it algebraically to prove Lemma 2) and "creation" events (where Alice detects no photon, so $m_1 = m_0 = 0$).

TABLE 4. All the Probabilities Alice and Bob Need to Compute, and the Formulas Relating Them to Quantum States in Our Security Proof

Probability	Round	Definition	Formula
$\langle E_0\|E_0\rangle_{\mathrm{E}}$	"raw key"	Alice and Bob get raw key bits 0, 0, respectively	
$\langle E_1\|E_1\rangle_{\mathrm{E}}$	"raw key"	Alice and Bob get raw key bits 0, 1, respectively	
$\langle E_2\|E_2\rangle_{\mathrm{E}}$	"raw key"	Alice and Bob get raw key bits 1, 0, respectively	
$\langle E_3\|E_3\rangle_{\mathrm{E}}$	"raw key"	Alice and Bob get raw key bits 1, 1, respectively	
M	"raw key"	both Alice and Bob get raw key bits	$=\sum_{i=0}^{3}\langle E_i\|E_i\rangle_{\mathrm{E}}$
$p_{0,+}$	mismatched "raw key"	Alice gets raw key bit 0, and Bob observes $\|+\rangle$	$2\Re\langle E_0\|E_1\rangle_{\mathrm{E}}=2p_{0,+}$ $-\left(\langle E_0\|E_0\rangle_{\mathrm{E}}+\langle E_1\|E_1\rangle_{\mathrm{E}}\right)$
$p_{1,+}$	mismatched "raw key"	Alice gets raw key bit 1, and Bob observes $\|+\rangle$	$2\Re\langle E_2\|E_3\rangle_{\mathrm{E}}=2p_{1,+}$ $-\left(\langle E_2\|E_2\rangle_{\mathrm{E}}+\langle E_3\|E_3\rangle_{\mathrm{E}}\right)$
$p_{+,+}$	"test"	Bob observes $\|+\rangle$	$=\left\|\sum_{i=0}^{3}\|E_i\rangle_{\mathrm{E}}-\sum_{j=0}^{1}\left(\|g_j\rangle_{\mathrm{E}}-\|h_j\rangle_{\mathrm{E}}\right)\right\|^2$
$p_{\mathtt{CTRL:0}}$	mismatched "test"	Bob observes $\|0,1\rangle$	$=2\left\|\|E_0\rangle_{\mathrm{E}}+\|E_2\rangle_{\mathrm{E}}-\|g_0\rangle_{\mathrm{E}}+\|h_0\rangle_{\mathrm{E}}\right\|^2$
$p_{\mathtt{CTRL:1}}$	mismatched "test"	Bob observes $\|1,0\rangle$	$=2\left\|\|E_1\rangle_{\mathrm{E}}+\|E_3\rangle_{\mathrm{E}}-\|g_1\rangle_{\mathrm{E}}+\|h_1\rangle_{\mathrm{E}}\right\|^2$
$p_{\mathtt{double}}$	"SWAP-ALL"	Alice observes a "double-click" event ($\|1,1\rangle$)	$\langle h_0\|h_0\rangle_{\mathrm{E}}+\langle h_1\|h_1\rangle_{\mathrm{E}}\leq\frac{1}{2}p_{\mathtt{double}}$
$p_{\mathtt{create:0}}$	"SWAP-ALL"	Alice observes $\|0,0\rangle$, and Bob observes $\|0,1\rangle$	$=2\langle g_0\|g_0\rangle_{\mathrm{E}}$
$p_{\mathtt{create:1}}$	"SWAP-ALL"	Alice observes $\|0,0\rangle$, and Bob observes $\|1,0\rangle$	$=2\langle g_1\|g_1\rangle_{\mathrm{E}}$

Alice and Bob have to find relevant statistics for each type of round and compute all probabilities listed in Table 4. In Section III-C–III-E, we relate these probabilities to the quantum states appearing in our security proof, and in Section III-F, we derive the resulting final key rate formula.

In *all* types of rounds, Bob begins by sending $|0,1\rangle_{\mathrm{x,B}}\triangleq\frac{|0,1\rangle_{\mathrm{B}}+|1,0\rangle_{\mathrm{B}}}{\sqrt{2}}$, which Eve immediately replaces by her own state [see (7)]

$$|\psi_0\rangle\triangleq\sum_{\substack{m_1\geq 0\\ m_0\geq 0}}|m_1,m_0\rangle_{\mathrm{B}}|e_{m_1,m_0}\rangle_{\mathrm{E}}.$$

Then Alice chooses her classical operation, as detailed below.

C. "RAW KEY" ROUNDS: ALICE CHOOSES THE SWAP-x OPERATION

In "raw key" rounds, Alice chooses either SWAP-10 or SWAP-01 (each with probability 1/2), which are defined in (2) and (3). Then, the nonnormalized state of the joint system, conditioning on Alice detecting *no photon*,[3] is

$$\rho_{\mathrm{ABE}}^{(\text{after Alice})}=\frac{1}{2}|\mathtt{o}\rangle\langle\mathtt{o}|_{\mathrm{A}}\otimes P\left(\sum_{m_0\geq 0}|0,m_0\rangle_{\mathrm{B}}|e_{0,m_0}\rangle_{\mathrm{E}}\right)+\frac{1}{2}|\mathtt{1}\rangle\langle\mathtt{1}|_{\mathrm{A}}\otimes P\left(\sum_{m_1\geq 0}|m_1,0\rangle_{\mathrm{B}}|e_{m_1,0}\rangle_{\mathrm{E}}\right)\tag{10}$$

where we define

$$P(|\psi\rangle)\triangleq|\psi\rangle\langle\psi|.\tag{11}$$

We note that $|\mathtt{o}\rangle_{\mathrm{A}}$ and $|\mathtt{1}\rangle_{\mathrm{A}}$ denote the raw key bit of Alice: Alice deduces it from her own choice of SWAP-10 (which corresponds to $|\mathtt{o}\rangle_{\mathrm{A}}$) or SWAP-01 (which corresponds to $|\mathtt{1}\rangle_{\mathrm{A}}$), as explained in Table 1.

After Eve's second attack [namely, after Eve applies the U_{R} operator defined in (9)], the joint nonnormalized state becomes

$$\begin{aligned}U_{\mathrm{R}}\rho_{\mathrm{ABE}}^{(\text{after Alice})}U_{\mathrm{R}}^{\dagger}=&\frac{1}{2}|\mathtt{o}\rangle\langle\mathtt{o}|_{\mathrm{A}}\\&\otimes P\left(|0,1\rangle_{\mathrm{B}}\sum_{m_0\geq 0}|g_{0,m_0}^{0,1}\rangle_{\mathrm{E}}+|1,0\rangle_{\mathrm{B}}\sum_{m_0\geq 0}|g_{0,m_0}^{1,0}\rangle_{\mathrm{E}}\right.\\&\left.+|0,0\rangle_{\mathrm{B}}\sum_{m_0\geq 0}|g_{0,m_0}^{0,0}\rangle_{\mathrm{E}}\right)+\frac{1}{2}|\mathtt{1}\rangle\langle\mathtt{1}|_{\mathrm{A}}\\&\otimes P\left(|0,1\rangle_{\mathrm{B}}\sum_{m_1\geq 0}|g_{m_1,0}^{0,1}\rangle_{\mathrm{E}}+|1,0\rangle_{\mathrm{B}}\right.\\&\left.\sum_{m_1\geq 0}|g_{m_1,0}^{1,0}\rangle_{\mathrm{E}}+|0,0\rangle_{\mathrm{B}}\sum_{m_1\geq 0}|g_{m_1,0}^{0,0}\rangle_{\mathrm{E}}\right).\end{aligned}\tag{12}$$

To simplify notation, we define the following states in subsystem E:

$$\begin{aligned}|E_0\rangle_{\mathrm{E}}&\triangleq\frac{1}{\sqrt{2}}\sum_{m_0\geq 0}|g_{0,m_0}^{0,1}\rangle_{\mathrm{E}}\\|E_1\rangle_{\mathrm{E}}&\triangleq\frac{1}{\sqrt{2}}\sum_{m_0\geq 0}|g_{0,m_0}^{1,0}\rangle_{\mathrm{E}}\\|E_2\rangle_{\mathrm{E}}&\triangleq\frac{1}{\sqrt{2}}\sum_{m_1\geq 0}|g_{m_1,0}^{0,1}\rangle_{\mathrm{E}}\\|E_3\rangle_{\mathrm{E}}&\triangleq\frac{1}{\sqrt{2}}\sum_{m_1\geq 0}|g_{m_1,0}^{1,0}\rangle_{\mathrm{E}}\end{aligned}\tag{13}$$

[3]Notice that according to Table 1, raw key bits are shared by Alice and Bob only in "raw key" rounds where Alice detects *no photon* and Bob *does* detect a photon.

so (12) becomes

$$U_{\mathrm{R}}\rho_{\mathrm{ABE}}^{(\text{after Alice})}U_{\mathrm{R}}^{\dagger} = |\mathtt{0}\rangle\langle\mathtt{0}|_{\mathrm{A}} \otimes P\Bigg(|0,1\rangle_{\mathrm{B}}|E_0\rangle_{\mathrm{E}}+|1,0\rangle_{\mathrm{B}}|E_1\rangle_{\mathrm{E}} + |0,0\rangle_{\mathrm{B}}\frac{1}{\sqrt{2}}\sum_{m_0\geq 0}|g_{0,m_0}^{0,0}\rangle_{\mathrm{E}}\Bigg) + |\mathtt{1}\rangle\langle\mathtt{1}|_{\mathrm{A}} \otimes P\Bigg(|0,1\rangle_{\mathrm{B}}|E_2\rangle_{\mathrm{E}} + |1,0\rangle_{\mathrm{B}}|E_3\rangle_{\mathrm{E}} + |0,0\rangle_{\mathrm{B}}\frac{1}{\sqrt{2}}\sum_{m_1\geq 0}|g_{m_1,0}^{0,0}\rangle_{\mathrm{E}}\Bigg). \tag{14}$$

1) STANDARD "RAW KEY" ROUNDS: BOB CHOOSES THE COMPUTATIONAL BASIS

Now, Bob measures his subsystem in the computational basis $\{|\mathtt{0}\rangle, |\mathtt{1}\rangle\}$, and his raw key bit is simply his measurement result ("0" or "1"). Conditioning on Bob detecting a photon (namely, measuring $|0,1\rangle_{\mathrm{B}}$ or $|1,0\rangle_{\mathrm{B}}$), the final *normalized* state of the joint system after Bob's measurement is

$$\rho_{\mathrm{ABE}} = \frac{1}{M}(|\mathtt{00}\rangle\langle\mathtt{00}|_{\mathrm{AB}} \otimes |E_0\rangle\langle E_0|_{\mathrm{E}} + |\mathtt{01}\rangle\langle\mathtt{01}|_{\mathrm{AB}} \otimes |E_1\rangle\langle E_1|_{\mathrm{E}} + |\mathtt{10}\rangle\langle\mathtt{10}|_{\mathrm{AB}} \otimes |E_2\rangle\langle E_2|_{\mathrm{E}} + |\mathtt{11}\rangle\langle\mathtt{11}|_{\mathrm{AB}} \otimes |E_3\rangle\langle E_3|_{\mathrm{E}}) \tag{15}$$

where M is a normalization term, which is computed in the following.

Equation (15) confirms that, as written in Table 4,

$$\langle E_0|E_0\rangle_{\mathrm{E}} = \Pr(\text{Alice gets raw key bit 0, and Bob gets raw key bit 0}) \tag{16}$$

$$\langle E_1|E_1\rangle_{\mathrm{E}} = \Pr(\text{Alice gets raw key bit 0, and Bob gets raw key bit 1}) \tag{17}$$

$$\langle E_2|E_2\rangle_{\mathrm{E}} = \Pr(\text{Alice gets raw key bit 1, and Bob gets raw key bit 0}) \tag{18}$$

$$\langle E_3|E_3\rangle_{\mathrm{E}} = \Pr(\text{Alice gets raw key bit 1, and Bob gets raw key bit 1}). \tag{19}$$

In addition, we can compute the normalization term M

$$M = \sum_{i=0}^{3}\langle E_i|E_i\rangle_{\mathrm{E}} = \Pr(\text{both Alice and Bob get raw key bits}) = \Pr(\text{Alice observes no photon, and Bob observes a photon}). \tag{20}$$

Notice that all these probabilities are *observable* quantities: Alice and Bob estimate $\langle E_0|E_0\rangle_{\mathrm{E}}$, $\langle E_1|E_1\rangle_{\mathrm{E}}$, $\langle E_2|E_2\rangle_{\mathrm{E}}$, $\langle E_3|E_3\rangle_{\mathrm{E}}$, and M during the classical postprocessing stage by testing a random subset of raw key bits.

2) MISMATCHED "RAW KEY" ROUNDS: BOB CHOOSES THE HADAMARD BASIS

In this case, Bob measures his subsystem in the Hadamard basis $\{|+\rangle, |-\rangle\}$. Let us rewrite the state he measures, provided in (14), by substituting $|0,1\rangle_{\mathrm{B}} = \frac{|+\rangle_{\mathrm{B}}+|-\rangle_{\mathrm{B}}}{\sqrt{2}}$ and $|1,0\rangle_{\mathrm{B}} = \frac{|+\rangle_{\mathrm{B}}-|-\rangle_{\mathrm{B}}}{\sqrt{2}}$. We get

$$\begin{aligned} &U_{\mathrm{R}}\rho_{\mathrm{ABE}}^{(\text{after Alice})}U_{\mathrm{R}}^{\dagger} \\ &= |\mathtt{0}\rangle\langle\mathtt{0}|_{\mathrm{A}} \otimes P\Bigg(|0,1\rangle_{\mathrm{B}}|E_0\rangle_{\mathrm{E}} + |1,0\rangle_{\mathrm{B}}|E_1\rangle_{\mathrm{E}} + |0,0\rangle_{\mathrm{B}}\frac{1}{\sqrt{2}}\sum_{m_0\geq 0}|g_{0,m_0}^{0,0}\rangle_{\mathrm{E}}\Bigg) \\ &\quad + |\mathtt{1}\rangle\langle\mathtt{1}|_{\mathrm{A}} \otimes P\Bigg(|0,1\rangle_{\mathrm{B}}|E_2\rangle_{\mathrm{E}} + |1,0\rangle_{\mathrm{B}}|E_3\rangle_{\mathrm{E}} + |0,0\rangle_{\mathrm{B}}\frac{1}{\sqrt{2}}\sum_{m_1\geq 0}|g_{m_1,0}^{0,0}\rangle_{\mathrm{E}}\Bigg) \\ &= |\mathtt{0}\rangle\langle\mathtt{0}|_{\mathrm{A}} \otimes P\left(\frac{|+\rangle_{\mathrm{B}}}{\sqrt{2}}(|E_0\rangle_{\mathrm{E}} + |E_1\rangle_{\mathrm{E}}) + \cdots\right) \\ &\quad + |\mathtt{1}\rangle\langle\mathtt{1}|_{\mathrm{A}} \otimes P\left(\frac{|+\rangle_{\mathrm{B}}}{\sqrt{2}}(|E_2\rangle_{\mathrm{E}} + |E_3\rangle_{\mathrm{E}}) + \cdots\right) \end{aligned} \tag{21}$$

where the remainders of the above terms (the "$\cdots$") are irrelevant to our discussion.

We denote by $p_{0,+}$ the probability that Alice gets the raw key bit 0 and Bob observes $|+\rangle_{\mathrm{B}}$ (see Table 4). Similarly, we denote by $p_{1,+}$ the probability that Alice gets the raw key bit 1 and Bob observes $|+\rangle_{\mathrm{B}}$. These probabilities are

$$\begin{aligned} p_{0,+} &= \left|\frac{|E_0\rangle_{\mathrm{E}} + |E_1\rangle_{\mathrm{E}}}{\sqrt{2}}\right|^2 \\ &= \frac{1}{2}\left(\langle E_0|E_0\rangle_{\mathrm{E}} + \langle E_1|E_1\rangle_{\mathrm{E}} + 2\Re\langle E_0|E_1\rangle_{\mathrm{E}}\right) \\ p_{1,+} &= \left|\frac{|E_2\rangle_{\mathrm{E}} + |E_3\rangle_{\mathrm{E}}}{\sqrt{2}}\right|^2 \\ &= \frac{1}{2}\left(\langle E_2|E_2\rangle_{\mathrm{E}} + \langle E_3|E_3\rangle_{\mathrm{E}} + 2\Re\langle E_2|E_3\rangle_{\mathrm{E}}\right). \end{aligned}$$

Therefore, we find

$$2\Re\langle E_0|E_1\rangle_{\mathrm{E}} = 2p_{0,+} - (\langle E_0|E_0\rangle_{\mathrm{E}} + \langle E_1|E_1\rangle_{\mathrm{E}}) \tag{22}$$

$$2\Re\langle E_2|E_3\rangle_{\mathrm{E}} = 2p_{1,+} - (\langle E_2|E_2\rangle_{\mathrm{E}} + \langle E_3|E_3\rangle_{\mathrm{E}}). \tag{23}$$

D. "TEST" ROUNDS: ALICE CHOOSES THE CTRL OPERATION

In "test" rounds, Eve sends to Alice her state $|\psi_0\rangle \triangleq \sum_{\substack{m_1\geq 0\\ m_0\geq 0}}|m_1,m_0\rangle_{\mathrm{B}}|e_{m_1,m_0}\rangle_{\mathrm{E}}$ [see (7)], and Alice chooses the CTRL operation—namely, Alice does nothing [see (1)].

Then, Eve applies her second attack U_{R} [see (9)], and the resulting quantum state is

$$U_{\mathrm{R}}|\psi_0\rangle = |0,1\rangle_{\mathrm{B}} \sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{0,1}_{m_1,m_0}\rangle_{\mathrm{E}} + |1,0\rangle_{\mathrm{B}} \sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{1,0}_{m_1,m_0}\rangle_{\mathrm{E}} + |0,0\rangle_{\mathrm{B}} \sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{0,0}_{m_1,m_0}\rangle_{\mathrm{E}}. \tag{24}$$

1) STANDARD "TEST" ROUNDS: BOB CHOOSES THE HADAMARD BASIS

Changing basis, whereby $|0,1\rangle_{\mathrm{B}} = \frac{|+\rangle_{\mathrm{B}}+|-\rangle_{\mathrm{B}}}{\sqrt{2}}$ and $|1,0\rangle_{\mathrm{B}} = \frac{|+\rangle_{\mathrm{B}}-|-\rangle_{\mathrm{B}}}{\sqrt{2}}$, we find

$$U_{\mathrm{R}}|\psi_0\rangle = \frac{|+\rangle_{\mathrm{B}}}{\sqrt{2}}\left(\sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{0,1}_{m_1,m_0}\rangle_{\mathrm{E}} + \sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{1,0}_{m_1,m_0}\rangle_{\mathrm{E}}\right) + \cdots \tag{25}$$

where the extra $\cdots$ term is irrelevant to our discussion.

Let $p_{+,+}$ be the probability that Bob observes $|+\rangle_{\mathrm{B}}$ (see Table 4). From (25), we deduce

$$\begin{aligned} p_{+,+} &= \left|\frac{1}{\sqrt{2}}\sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{0,1}_{m_1,m_0}\rangle_{\mathrm{E}} + \frac{1}{\sqrt{2}}\sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{1,0}_{m_1,m_0}\rangle_{\mathrm{E}}\right|^2 \\ &= |(|E_0\rangle_{\mathrm{E}} + |E_2\rangle_{\mathrm{E}} - |g_0\rangle_{\mathrm{E}} + |h_0\rangle_{\mathrm{E}}) \\ &\quad + (|E_1\rangle_{\mathrm{E}} + |E_3\rangle_{\mathrm{E}} - |g_1\rangle_{\mathrm{E}} + |h_1\rangle_{\mathrm{E}})|^2 \\ &= ||E_0\rangle_{\mathrm{E}} + |E_2\rangle_{\mathrm{E}} - |g_0\rangle_{\mathrm{E}} + |h_0\rangle_{\mathrm{E}}|^2 \\ &\quad + ||E_1\rangle_{\mathrm{E}} + |E_3\rangle_{\mathrm{E}} - |g_1\rangle_{\mathrm{E}} + |h_1\rangle_{\mathrm{E}}|^2 \\ &\quad + 2\Re\left[(\langle E_0|_{\mathrm{E}} + \langle E_2|_{\mathrm{E}} - \langle g_0|_{\mathrm{E}} + \langle h_0|_{\mathrm{E}}\right) \\ &\quad \times (|E_1\rangle_{\mathrm{E}} + |E_3\rangle_{\mathrm{E}} - |g_1\rangle_{\mathrm{E}} + |h_1\rangle_{\mathrm{E}})\right] \end{aligned} \tag{26}$$

where we define

$$\begin{aligned} |g_0\rangle_{\mathrm{E}} &\triangleq \frac{1}{\sqrt{2}}|g^{0,1}_{0,0}\rangle_{\mathrm{E}} \\ |g_1\rangle_{\mathrm{E}} &\triangleq \frac{1}{\sqrt{2}}|g^{1,0}_{0,0}\rangle_{\mathrm{E}} \\ |h_0\rangle_{\mathrm{E}} &\triangleq \frac{1}{\sqrt{2}}\sum_{\substack{m_1\geq 1\\ m_0\geq 1}} |g^{0,1}_{m_1,m_0}\rangle_{\mathrm{E}} \\ |h_1\rangle_{\mathrm{E}} &\triangleq \frac{1}{\sqrt{2}}\sum_{\substack{m_1\geq 1\\ m_0\geq 1}} |g^{1,0}_{m_1,m_0}\rangle_{\mathrm{E}} \end{aligned} \tag{27}$$

and we remember from (13) that

$$|E_0\rangle_{\mathrm{E}} \triangleq \frac{1}{\sqrt{2}}\sum_{m_0\geq 0} |g^{0,1}_{0,m_0}\rangle_{\mathrm{E}}$$

$$\begin{aligned} |E_1\rangle_{\mathrm{E}} &\triangleq \frac{1}{\sqrt{2}}\sum_{m_0\geq 0} |g^{1,0}_{0,m_0}\rangle_{\mathrm{E}} \\ |E_2\rangle_{\mathrm{E}} &\triangleq \frac{1}{\sqrt{2}}\sum_{m_1\geq 0} |g^{0,1}_{m_1,0}\rangle_{\mathrm{E}} \\ |E_3\rangle_{\mathrm{E}} &\triangleq \frac{1}{\sqrt{2}}\sum_{m_1\geq 0} |g^{1,0}_{m_1,0}\rangle_{\mathrm{E}}. \end{aligned}$$

2) MISMATCHED "TEST" ROUNDS: BOB CHOOSES THE COMPUTATIONAL BASIS

In this case, we denote by $p_{\mathtt{CTRL}:0}$ the probability of Bob observing $|0,1\rangle_{\mathrm{B}}$ (see Table 4). From (24), we find (similarly to the computation of $p_{+,+}$)

$$\begin{aligned} p_{\mathtt{CTRL}:0} &= \left|\sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{0,1}_{m_1,m_0}\rangle_{\mathrm{E}}\right|^2 \\ &= 2\,||E_0\rangle_{\mathrm{E}} + |E_2\rangle_{\mathrm{E}} - |g_0\rangle_{\mathrm{E}} + |h_0\rangle_{\mathrm{E}}|^2. \end{aligned} \tag{28}$$

Similarly, denoting by $p_{\mathtt{CTRL}:1}$ the probability of Bob observing $|1,0\rangle_{\mathrm{B}}$, we find

$$\begin{aligned} p_{\mathtt{CTRL}:1} &= \left|\sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |g^{1,0}_{m_1,m_0}\rangle_{\mathrm{E}}\right|^2 \\ &= 2\,||E_1\rangle_{\mathrm{E}} + |E_3\rangle_{\mathrm{E}} - |g_1\rangle_{\mathrm{E}} + |h_1\rangle_{\mathrm{E}}|^2. \end{aligned} \tag{29}$$

E. "SWAP-ALL" ROUNDS: ALICE CHOOSES THE SWAP-ALL OPERATION, AND BOB CHOOSES THE COMPUTATIONAL BASIS

1) PROBABILITY OF A "DOUBLE-CLICK" EVENT: USED FOR UPPER-BOUNDING $\langle h_0|h_0\rangle_{\mathrm{E}}$ AND $\langle h_1|h_1\rangle_{\mathrm{E}}$

In "SWAP-ALL" rounds, Eve sends to Alice the initial state $|\psi_0\rangle \triangleq \sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |m_1,m_0\rangle_{\mathrm{B}}|e_{m_1,m_0}\rangle_{\mathrm{E}}$ described in (7), and Alice chooses the SWAP-ALL operation defined in (4), which essentially means that Alice measures subsystem B and sends a vacuum state toward Bob.

Let us denote by $p_{\mathtt{double}}$ the probability that Alice observes a "double-click" event (detecting a photon in *both* modes $|\mathtt{0}\rangle$ and $|\mathtt{1}\rangle$)—namely, that she measures a state $|m_1,m_0\rangle_{\mathrm{A_{anc}}}$ where $m_1,m_0\geq 1$ (see Table 4). This probability is easily found to be

$$p_{\mathtt{double}} = \sum_{\substack{m_1\geq 1\\ m_0\geq 1}} \langle e_{m_1,m_0}|e_{m_1,m_0}\rangle_{\mathrm{E}}.$$

We can, thus, prove the following lemma.

Lemma 2: $\langle h_0|h_0\rangle_{\mathrm{E}} \leq \frac{1}{2}p_{\mathtt{double}}$ and $\langle h_1|h_1\rangle_{\mathrm{E}} \leq \frac{1}{2}p_{\mathtt{double}}$, where $|h_0\rangle_{\mathrm{E}}$ and $|h_1\rangle_{\mathrm{E}}$ were defined in (27).

Proof: Let us define the nonnormalized state $|\zeta\rangle$ as

$$|\zeta\rangle \triangleq \frac{1}{\sqrt{2}}\sum_{\substack{m_1\geq 1\\ m_0\geq 1}} |m_1,m_0\rangle_{\mathrm{B}}|e_{m_1,m_0}\rangle_{\mathrm{E}}.$$

(We use the state $|\zeta\rangle$ only for this algebraic proof; it does not appear in the protocol.)

Clearly

$$\langle\zeta|\zeta\rangle = \frac{1}{2}\sum_{\substack{m_1\geq 1\\ m_0\geq 1}} \langle e_{m_1,m_0}|e_{m_1,m_0}\rangle_{\mathrm{E}} = \frac{1}{2}p_{\mathtt{double}}.$$

Applying U_{R} [see (9)], the state $|\zeta\rangle$ evolves to

$$\begin{aligned} U_{\mathrm{R}}|\zeta\rangle = \frac{1}{\sqrt{2}}\sum_{\substack{m_1\geq 1\\ m_0\geq 1}} \Big(&|0,1\rangle_{\mathrm{B}}|g^{0,1}_{m_1,m_0}\rangle_{\mathrm{E}}\\ &+|1,0\rangle_{\mathrm{B}}|g^{1,0}_{m_1,m_0}\rangle_{\mathrm{E}}+|0,0\rangle_{\mathrm{B}}|g^{0,0}_{m_1,m_0}\rangle_{\mathrm{E}}\Big)\\ =|0,1\rangle_{\mathrm{B}}|h_0\rangle_{\mathrm{E}}&+|1,0\rangle_{\mathrm{B}}|h_1\rangle_{\mathrm{E}}+|0,0\rangle_{\mathrm{B}}|h_{\mathrm{vac}}\rangle_{\mathrm{E}} \end{aligned}$$

(where $|h_0\rangle_{\mathrm{E}}$ and $|h_1\rangle_{\mathrm{E}}$ were defined in (27), and $|h_{\mathrm{vac}}\rangle_{\mathrm{E}} \triangleq \frac{1}{\sqrt{2}}\sum_{\substack{m_1\geq 1\\ m_0\geq 1}}|g^{0,0}_{m_1,m_0}\rangle_{\mathrm{E}}$).

By unitarity of U_{R}, we have

$$\frac{1}{2}p_{\mathtt{double}} = \langle\zeta|\zeta\rangle = \langle h_0|h_0\rangle_{\mathrm{E}}+\langle h_1|h_1\rangle_{\mathrm{E}}+\langle h_{\mathrm{vac}}|h_{\mathrm{vac}}\rangle_{\mathrm{E}}$$

which implies that $\langle h_0|h_0\rangle_{\mathrm{E}}+\langle h_1|h_1\rangle_{\mathrm{E}} \leq \frac{1}{2}p_{\mathtt{double}}$. Since both $\langle h_0|h_0\rangle_{\mathrm{E}}$ and $\langle h_1|h_1\rangle_{\mathrm{E}}$ are nonnegative, this implies $\langle h_0|h_0\rangle_{\mathrm{E}} \leq \frac{1}{2}p_{\mathtt{double}}$ and $\langle h_1|h_1\rangle_{\mathrm{E}} \leq \frac{1}{2}p_{\mathtt{double}}$, as we wanted. ■

2) PROBABILITY OF A "CREATION" EVENT: USED FOR COMPUTING $\langle g_0|g_0\rangle_{\mathrm{E}}$ AND $\langle g_1|g_1\rangle_{\mathrm{E}}$

Let $p_{\mathtt{create:0}}$ denote the probability that Alice observes $|0,0\rangle_{\mathrm{A_{anc}}}$ (namely, a vacuum state) and Bob observes $|0,1\rangle_{\mathrm{B}}$ (see Table 4). In this event, Eve "creates" (on the way from Alice to Bob) a photon in the $|\mathrm{o}\rangle$ mode that should not have existed. (See [39] for examples of such attacks.) Similarly, let $p_{\mathtt{create:1}}$ denote the probability that Alice observes $|0,0\rangle_{\mathrm{A_{anc}}}$ and Bob observes $|1,0\rangle_{\mathrm{B}}$.

After Eve sends the initial state

$$|\psi_0\rangle \triangleq \sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |m_1,m_0\rangle_{\mathrm{B}}|e_{m_1,m_0}\rangle_{\mathrm{E}}$$

described in (7), and after Alice applies the SWAP-ALL operation defined in (4), the resulting state is

$$\sum_{\substack{m_1\geq 0\\ m_0\geq 0}} |m_1,m_0\rangle_{\mathrm{A_{anc}}}|0,0\rangle_{\mathrm{B}}|e_{m_1,m_0}\rangle_{\mathrm{E}}.$$

For computing the probabilities $p_{\mathtt{create:0}}$ and $p_{\mathtt{create:1}}$, we need to analyze the term where Alice observes $|0,0\rangle_{\mathrm{A_{anc}}}$—namely, the term $|0,0\rangle_{\mathrm{A_{anc}}}|0,0\rangle_{\mathrm{B}}|e_{0,0}\rangle_{\mathrm{E}}$. Now, Eve's second attack applies the unitary operator U_{R} [described in (9)] to this nonnormalized term, which gives the following final result:

$$\begin{aligned} |0,0\rangle_{\mathrm{A_{anc}}}\otimes U_{\mathrm{R}}|0,0\rangle_{\mathrm{B}}|e_{0,0}\rangle_{\mathrm{E}} = |0,0\rangle_{\mathrm{A_{anc}}}\otimes\Big[&|0,1\rangle_{\mathrm{B}}|g^{0,1}_{0,0}\rangle_{\mathrm{E}}\\ &+|1,0\rangle_{\mathrm{B}}|g^{1,0}_{0,0}\rangle_{\mathrm{E}}+|0,0\rangle_{\mathrm{B}}|g^{0,0}_{0,0}\rangle_{\mathrm{E}}\Big]. \end{aligned}$$

Since $p_{\mathtt{create:0}}$ is the probability that Alice observes $|0,0\rangle_{\mathrm{A_{anc}}}$ and Bob observes $|0,1\rangle_{\mathrm{B}}$ (and similarly for $p_{\mathtt{create:1}}$), according to the definitions of $|g_0\rangle_{\mathrm{E}}, |g_1\rangle_{\mathrm{E}}$ in (27), we obtain

$$p_{\mathtt{create:0}} = \left\langle g^{0,1}_{0,0}|g^{0,1}_{0,0}\right\rangle_{\mathrm{E}} = 2\langle g_0|g_0\rangle_{\mathrm{E}} \tag{30}$$

$$p_{\mathtt{create:1}} = \left\langle g^{1,0}_{0,0}|g^{1,0}_{0,0}\right\rangle_{\mathrm{E}} = 2\langle g_1|g_1\rangle_{\mathrm{E}}. \tag{31}$$

F. DERIVING THE FINAL KEY RATE

We remember that the final normalized state of the joint system after Bob's measurement, in standard "raw key" rounds where raw key bits *are* generated, is, according to (15),

$$\begin{aligned} \rho_{\mathrm{ABE}} = \frac{1}{M}(&|\mathtt{00}\rangle\langle\mathtt{00}|_{\mathrm{AB}}\otimes|E_0\rangle\langle E_0|_{\mathrm{E}}\\ &+|\mathtt{01}\rangle\langle\mathtt{01}|_{\mathrm{AB}}\otimes|E_1\rangle\langle E_1|_{\mathrm{E}}\\ &+|\mathtt{10}\rangle\langle\mathtt{10}|_{\mathrm{AB}}\otimes|E_2\rangle\langle E_2|_{\mathrm{E}}\\ &+|\mathtt{11}\rangle\langle\mathtt{11}|_{\mathrm{AB}}\otimes|E_3\rangle\langle E_3|_{\mathrm{E}}). \end{aligned}$$

Theorem 1 from [57] allows us to mathematically compute a bound on the conditional von Neumann entropy $S(A|E)$ of ρ_{ABE}, as follows:

$$\begin{aligned} S(A|E) \geq &\frac{\langle E_0|E_0\rangle_{\mathrm{E}}+\langle E_3|E_3\rangle_{\mathrm{E}}}{M}\\ &\times\left[H_2\left(\frac{\langle E_0|E_0\rangle_{\mathrm{E}}}{\langle E_0|E_0\rangle_{\mathrm{E}}+\langle E_3|E_3\rangle_{\mathrm{E}}}\right)-H_2(\lambda_1)\right]\\ &+\frac{\langle E_1|E_1\rangle_{\mathrm{E}}+\langle E_2|E_2\rangle_{\mathrm{E}}}{M}\\ &\times\left[H_2\left(\frac{\langle E_1|E_1\rangle_{\mathrm{E}}}{\langle E_1|E_1\rangle_{\mathrm{E}}+\langle E_2|E_2\rangle_{\mathrm{E}}}\right)-H_2(\lambda_2)\right] \end{aligned} \tag{32}$$

where

$$\lambda_1 \triangleq \frac{1}{2}+\frac{\sqrt{(\langle E_0|E_0\rangle_{\mathrm{E}}-\langle E_3|E_3\rangle_{\mathrm{E}})^2+4\Re^2\langle E_0|E_3\rangle_{\mathrm{E}}}}{2\left(\langle E_0|E_0\rangle_{\mathrm{E}}+\langle E_3|E_3\rangle_{\mathrm{E}}\right)}$$

$$\lambda_2 \triangleq \frac{1}{2}+\frac{\sqrt{(\langle E_1|E_1\rangle_{\mathrm{E}}-\langle E_2|E_2\rangle_{\mathrm{E}})^2+4\Re^2\langle E_1|E_2\rangle_{\mathrm{E}}}}{2\left(\langle E_1|E_1\rangle_{\mathrm{E}}+\langle E_2|E_2\rangle_{\mathrm{E}}\right)}$$

$$H_2(x) \triangleq -x\log_2(x)-(1-x)\log_2(1-x).$$

Thus, to complete our proof of security, we only need bounds on the quantities $\Re\langle E_0|E_3\rangle_{\mathrm{E}}$ and $\Re\langle E_1|E_2\rangle_{\mathrm{E}}$; all the other parameters in the above expressions ($\langle E_0|E_0\rangle_{\mathrm{E}}$,

$\langle E_1|E_1\rangle_{\mathrm{E}}$, $\langle E_2|E_2\rangle_{\mathrm{E}}$, $\langle E_3|E_3\rangle_{\mathrm{E}}$, and M) are observable probabilities that appear in Table 4 and can be directly computed by Alice and Bob.

Lemma 3: The following constraint (33) on Eve's quantum states holds.

$$\begin{aligned}
&\Re\left(\langle E_0|E_3\rangle_{\mathrm{E}}+\langle E_1|E_2\rangle_{\mathrm{E}}\right)\\
&\geq \frac{1}{2}p_{+,+}-p_{0,+}-p_{1,+}-\frac{1}{4}(p_{\mathrm{CTRL}:0}+p_{\mathrm{CTRL}:1})+\frac{1}{2}M\\
&-\frac{1}{\sqrt{2}}\left(\sqrt{p_{\mathtt{create}:1}}+\sqrt{p_{\mathtt{double}}}\right)\left(\sqrt{\langle E_0|E_0\rangle_{\mathrm{E}}}+\sqrt{\langle E_2|E_2\rangle_{\mathrm{E}}}\right)\\
&-\frac{1}{\sqrt{2}}\left(\sqrt{p_{\mathtt{create}:0}}+\sqrt{p_{\mathtt{double}}}\right)\left(\sqrt{\langle E_1|E_1\rangle_{\mathrm{E}}}+\sqrt{\langle E_3|E_3\rangle_{\mathrm{E}}}\right)\\
&-\frac{1}{2}\left(\sqrt{p_{\mathtt{create}:0}}+\sqrt{p_{\mathtt{double}}}\right)\left(\sqrt{p_{\mathtt{create}:1}}+\sqrt{p_{\mathtt{double}}}\right) \qquad (33)
\end{aligned}$$

Proof: We expand (26) and substitute (22), (23) and (28), (29) (all appearing in Table 4) to find

$$\begin{aligned}
p_{+,+} =\ & \||E_0\rangle_{\mathrm{E}}+|E_2\rangle_{\mathrm{E}}-|g_0\rangle_{\mathrm{E}}+|h_0\rangle_{\mathrm{E}}\|^2\\
&+\||E_1\rangle_{\mathrm{E}}+|E_3\rangle_{\mathrm{E}}-|g_1\rangle_{\mathrm{E}}+|h_1\rangle_{\mathrm{E}}\|^2\\
&+2\Re\left[\left(\langle E_0|_{\mathrm{E}}+\langle E_2|_{\mathrm{E}}-\langle g_0|_{\mathrm{E}}+\langle h_0|_{\mathrm{E}}\right)\right.\\
&\left.\times\left(|E_1\rangle_{\mathrm{E}}+|E_3\rangle_{\mathrm{E}}-|g_1\rangle_{\mathrm{E}}+|h_1\rangle_{\mathrm{E}}\right)\right]\\
=\ & \frac{1}{2}(p_{\mathrm{CTRL}:0}+p_{\mathrm{CTRL}:1})\\
&+2\Re\left(\langle E_0|_{\mathrm{E}}+\langle E_2|_{\mathrm{E}}\right)\left(|E_1\rangle_{\mathrm{E}}+|E_3\rangle_{\mathrm{E}}\right)\\
&-2\Re\left(\langle E_0|_{\mathrm{E}}+\langle E_2|_{\mathrm{E}}\right)\left(|g_1\rangle_{\mathrm{E}}-|h_1\rangle_{\mathrm{E}}\right)\\
&-2\Re\left(\langle g_0|_{\mathrm{E}}-\langle h_0|_{\mathrm{E}}\right)\left(|E_1\rangle_{\mathrm{E}}+|E_3\rangle_{\mathrm{E}}\right)\\
&+2\Re\left(\langle g_0|_{\mathrm{E}}-\langle h_0|_{\mathrm{E}}\right)\left(|g_1\rangle_{\mathrm{E}}-|h_1\rangle_{\mathrm{E}}\right)\\
=\ & \frac{1}{2}(p_{\mathrm{CTRL}:0}+p_{\mathrm{CTRL}:1})\\
&+2p_{0,+}-\left(\langle E_0|E_0\rangle_{\mathrm{E}}+\langle E_1|E_1\rangle_{\mathrm{E}}\right)+2\Re\langle E_0|E_3\rangle_{\mathrm{E}}\\
&+2p_{1,+}-\left(\langle E_2|E_2\rangle_{\mathrm{E}}+\langle E_3|E_3\rangle_{\mathrm{E}}\right)+2\Re\langle E_1|E_2\rangle_{\mathrm{E}}\\
&-2\Re\left(\langle E_0|_{\mathrm{E}}+\langle E_2|_{\mathrm{E}}\right)\left(|g_1\rangle_{\mathrm{E}}-|h_1\rangle_{\mathrm{E}}\right)\\
&-2\Re\left(\langle g_0|_{\mathrm{E}}-\langle h_0|_{\mathrm{E}}\right)\left(|E_1\rangle_{\mathrm{E}}+|E_3\rangle_{\mathrm{E}}\right)\\
&+2\Re\left(\langle g_0|_{\mathrm{E}}-\langle h_0|_{\mathrm{E}}\right)\left(|g_1\rangle_{\mathrm{E}}-|h_1\rangle_{\mathrm{E}}\right). \qquad (34)
\end{aligned}$$

From this, we easily find (substituting (20), which appears in Table 4)

$$\begin{aligned}
&\Re\left(\langle E_0|E_3\rangle_{\mathrm{E}}+\langle E_1|E_2\rangle_{\mathrm{E}}\right)\\
&=\frac{1}{2}p_{+,+}-p_{0,+}-p_{1,+}-\frac{1}{4}(p_{\mathrm{CTRL}:0}+p_{\mathrm{CTRL}:1})+\frac{1}{2}M\\
&+\Re\left(\langle g_1|_{\mathrm{E}}-\langle h_1|_{\mathrm{E}}\right)\left(|E_0\rangle_{\mathrm{E}}+|E_2\rangle_{\mathrm{E}}\right)\\
&+\Re\left(\langle g_0|_{\mathrm{E}}-\langle h_0|_{\mathrm{E}}\right)\left(|E_1\rangle_{\mathrm{E}}+|E_3\rangle_{\mathrm{E}}\right)\\
&-\Re\left(\langle g_0|_{\mathrm{E}}-\langle h_0|_{\mathrm{E}}\right)\left(|g_1\rangle_{\mathrm{E}}-|h_1\rangle_{\mathrm{E}}\right). \qquad (35)
\end{aligned}$$

The Cauchy–Schwarz inequality, Lemma 2, and (30) and (31) (all appearing in Table 4) complete the proof. ■

Taken together, the above proof derives a lower bound on $S(A|E)$ for a raw-key generation round, and this bound is based only on observable statistics from Table 4. The Devetak–Winter key rate equation [56] (which says that the key rate of a QKD protocol under collective attacks is the difference $S(A|E)-H(A|B)$) then completes our proof of Theorem 1.

To actually evaluate our bound on $S(A|E)$, we will simply minimize (32) with respect to the condition outlined in Lemma 3 and the following conditions (resulting from the Cauchy–Schwarz inequality):

$$|\Re\langle E_0|E_3\rangle_{\mathrm{E}}|\leq\sqrt{\langle E_0|E_0\rangle_{\mathrm{E}}\cdot\langle E_3|E_3\rangle_{\mathrm{E}}} \qquad (36)$$

$$|\Re\langle E_1|E_2\rangle_{\mathrm{E}}|\leq\sqrt{\langle E_1|E_1\rangle_{\mathrm{E}}\cdot\langle E_2|E_2\rangle_{\mathrm{E}}}. \qquad (37)$$

In addition, we need to compute the expression $H(A|B)$ (needed in Theorem 1)

$$H(A|B)=H(AB)-H(B) \qquad (38)$$

where

$$\begin{aligned}
&H(AB)\\
&=H\left(\frac{\langle E_0|E_0\rangle_{\mathrm{E}}}{M},\frac{\langle E_1|E_1\rangle_{\mathrm{E}}}{M},\frac{\langle E_2|E_2\rangle_{\mathrm{E}}}{M},\frac{\langle E_3|E_3\rangle_{\mathrm{E}}}{M}\right) \qquad (39)\\
&H(B)\\
&=H\left(\frac{\langle E_0|E_0\rangle_{\mathrm{E}}+\langle E_2|E_2\rangle_{\mathrm{E}}}{M},\frac{\langle E_1|E_1\rangle_{\mathrm{E}}+\langle E_3|E_3\rangle_{\mathrm{E}}}{M}\right)\\
&H(x_1,\ldots,x_k)\triangleq-\sum_{j=1}^{k}x_j\log_2(x_j). \qquad (40)
\end{aligned}$$

G. ALGORITHM FOR COMPUTING THE KEY RATE

The following algorithm allows us to compute the key rate for any noise model and experimental data.

1) Estimate all probabilities and inner products listed in Table 4. (All these probabilities can be computed by Alice and Bob in the classical postprocessing stage.)
2) Compute the minimal value of the lower bound for $S(A|E)$ presented in (32), which is copied here

$$\begin{aligned}
S(A|E)\geq\ & \frac{\langle E_0|E_0\rangle_{\mathrm{E}}+\langle E_3|E_3\rangle_{\mathrm{E}}}{M}\\
&\times\left[H_2\left(\frac{\langle E_0|E_0\rangle_{\mathrm{E}}}{\langle E_0|E_0\rangle_{\mathrm{E}}+\langle E_3|E_3\rangle_{\mathrm{E}}}\right)-H_2(\lambda_1)\right]\\
&+\frac{\langle E_1|E_1\rangle_{\mathrm{E}}+\langle E_2|E_2\rangle_{\mathrm{E}}}{M}\\
&\times\left[H_2\left(\frac{\langle E_1|E_1\rangle_{\mathrm{E}}}{\langle E_1|E_1\rangle_{\mathrm{E}}+\langle E_2|E_2\rangle_{\mathrm{E}}}\right)-H_2(\lambda_2)\right] \qquad (41)
\end{aligned}$$

where

$$\lambda_1\triangleq\frac{1}{2}$$

$$+\frac{\sqrt{(\langle E_0|E_0\rangle_{\rm E}-\langle E_3|E_3\rangle_{\rm E})^2+4\Re^2\langle E_0|E_3\rangle_{\rm E}}}{2\left(\langle E_0|E_0\rangle_{\rm E}+\langle E_3|E_3\rangle_{\rm E}\right)}$$

$$\lambda_2 \triangleq \frac{1}{2}$$

$$+\frac{\sqrt{(\langle E_1|E_1\rangle_{\rm E}-\langle E_2|E_2\rangle_{\rm E})^2+4\Re^2\langle E_1|E_2\rangle_{\rm E}}}{2\left(\langle E_1|E_1\rangle_{\rm E}+\langle E_2|E_2\rangle_{\rm E}\right)}$$

$$H_2(x) \triangleq -x\log_2(x)-(1-x)\log_2(1-x)$$

where the minimum is taken over $\Re\langle E_0|E_3\rangle_{\rm E}$ and $\Re\langle E_1|E_2\rangle_{\rm E}$, subject to the three following constraints:

$$\begin{aligned}&\Re\left(\langle E_0|E_3\rangle_{\rm E}+\langle E_1|E_2\rangle_{\rm E}\right)\\&\geq\frac{1}{2}p_{+,+}-p_{0,+}-p_{1,+}-\frac{1}{4}(p_{\texttt{CTRL:0}}+p_{\texttt{CTRL:1}})+\frac{1}{2}M\\&-\frac{1}{\sqrt{2}}\left(\sqrt{p_{\texttt{create:1}}}+\sqrt{p_{\texttt{double}}}\right)\\&\times\left(\sqrt{\langle E_0|E_0\rangle_{\rm E}}+\sqrt{\langle E_2|E_2\rangle_{\rm E}}\right)\\&-\frac{1}{\sqrt{2}}\left(\sqrt{p_{\texttt{create:0}}}+\sqrt{p_{\texttt{double}}}\right)\\&\times\left(\sqrt{\langle E_1|E_1\rangle_{\rm E}}+\sqrt{\langle E_3|E_3\rangle_{\rm E}}\right)\\&-\frac{1}{2}\left(\sqrt{p_{\texttt{create:0}}}+\sqrt{p_{\texttt{double}}}\right)\\&\times\left(\sqrt{p_{\texttt{create:1}}}+\sqrt{p_{\texttt{double}}}\right)\end{aligned}\tag{42}$$

$$|\Re\langle E_0|E_3\rangle_{\rm E}|\leq\sqrt{\langle E_0|E_0\rangle_{\rm E}\cdot\langle E_3|E_3\rangle_{\rm E}}\tag{43}$$

$$|\Re\langle E_1|E_2\rangle_{\rm E}|\leq\sqrt{\langle E_1|E_1\rangle_{\rm E}\cdot\langle E_2|E_2\rangle_{\rm E}}.\tag{44}$$

Note that we evaluate the minimum because we assume the worst case scenario—namely, that Eve chooses her attack so as to minimize $S(A|E)$ (and, thus, minimize the key rate r).

In practice, we can minimize over a single parameter (say, $\Re\langle E_1|E_2\rangle_{\rm E}$) and take the other one ($\Re\langle E_0|E_3\rangle_{\rm E}$) as the right-hand side of (42), minus the free parameter $\Re\langle E_1|E_2\rangle_{\rm E}$ (but not less than 0). This will give us the minimum, because for any given value of $\Re\langle E_1|E_2\rangle_{\rm E}$, it is beneficial for Eve to have the smallest possible (nonnegative) value of $\Re\langle E_0|E_3\rangle_{\rm E}$.

For our evaluations, we performed this minimization by simply discretizing the search space and evaluating our bound on the entropy at all points in the space for computing the minimum. We also confirmed these results using Mathematica's `NMinimize` function.

3) Compute $H(A|B)$ using the observed parameters

$$\begin{aligned}&H(A|B)=H(AB)-H(B)\\&=H\left(\frac{\langle E_0|E_0\rangle_{\rm E}}{M},\frac{\langle E_1|E_1\rangle_{\rm E}}{M},\frac{\langle E_2|E_2\rangle_{\rm E}}{M},\frac{\langle E_3|E_3\rangle_{\rm E}}{M}\right)\\&-H\left(\frac{\langle E_0|E_0\rangle_{\rm E}+\langle E_2|E_2\rangle_{\rm E}}{M},\frac{\langle E_1|E_1\rangle_{\rm E}+\langle E_3|E_3\rangle_{\rm E}}{M}\right)\end{aligned}\tag{45}$$

where

$$H(x_1,\ldots,x_k)\triangleq-\sum_{j=1}^{k}x_j\log_2(x_j).\tag{46}$$

4) Find the final key rate expression, using the Devetak–Winter key rate formula [56]

$$r=S(A|E)-H(A|B).\tag{47}$$

This process is summarized in Algorithm 1.

Algorithm 1: Compute a Lower Bound for `rate` $= S(A|E)-H(A|B)$.

Input: All observable probabilities listed in Table 4.
Output: Lower bound on the key rate of the protocol.

```
Initialize the variable lowestAE ← ∞.
Compute all probabilities listed in Table 4 using
  the protocol's statistics observed by Alice and Bob.
/* Next, minimize S(A|E) by
   minimizing the lower bound in
   Eq. (41).                                   */
for all possible ℜ⟨E1|E2⟩E subject to Eq. (37) do
    Compute a lower bound on ℜ⟨E0|E3⟩E using
      Eq. (42) and subject to Eq. (36).
    Compute a lower bound on S(A|E) using
      Eq. (41).
    If this determined bound is lower than the existing
      value of lowestAE, save it in lowestAE.
end
Compute H(A|B) using Eq. (45), and put the result in
  variable AB.
return the difference value lowestAE − AB
```

IV. EXAMPLES

The key rate bounds we found in Section III work in a wide range of scenarios, and they can be evaluated for all the possible values of all probabilities in Table 4. We would now like to evaluate our bounds for two concrete scenarios that are easily comparable with attacks on other QKD and SQKD protocols.

A. FIRST SCENARIO: SINGLE-PHOTON ATTACKS WITHOUT LOSSES

In the first scenario, let us assume that Bob has a perfect qubit source (no multiphoton pulses), and there are no photon losses. Furthermore, let us assume that Eve does not perform a multiqubit attack at all (not even in her *first* attack). In this scenario, the only free parameters are the noises $Q_{\rm Z}$, $Q_{\rm X}$ in the channel: $Q_{\rm Z}$ is the probability that a $|0,1\rangle_{\rm B}$ state is flipped into $|1,0\rangle_{\rm B}$ (and vice versa) in "raw key" rounds, and $Q_{\rm X}$ is

TABLE 5. Computing All Probabilities in Table 4 for Both Examples (Both Scenarios)

Probability	Single-Photon without Losses	Single-Photon with Losses
$\langle E_0\|E_0\rangle_{\rm E} = \langle E_3\|E_3\rangle_{\rm E} =$	$\frac{1}{4}(1-Q_{\rm Z})$	$\frac{1}{4}(1-p_\ell^{\rm F})(1-p_\ell^{\rm R})(1-Q_{\rm Z})$
$\langle E_1\|E_1\rangle_{\rm E} = \langle E_2\|E_2\rangle_{\rm E} =$	$\frac{1}{4}Q_{\rm Z}$	$\frac{1}{4}(1-p_\ell^{\rm F})(1-p_\ell^{\rm R})Q_{\rm Z}$
$M =$	$\frac{1}{2}$	$\frac{1}{2}(1-p_\ell^{\rm F})(1-p_\ell^{\rm R})$
$p_{0,+} = p_{1,+} =$	$\frac{1}{8}$	$\frac{1}{8}(1-p_\ell^{\rm F})(1-p_\ell^{\rm R})$
$p_{+,+} =$	$1-Q_{\rm X}$	$(1-p_\ell^{\rm F})(1-p_\ell^{\rm R})(1-Q_{\rm X})$
$p_{\texttt{CTRL:0}} = p_{\texttt{CTRL:1}} =$	$\frac{1}{2}$	$\frac{1}{2}(1-p_\ell^{\rm F})(1-p_\ell^{\rm R})$
$p_{\texttt{double}} =$	0	0
$p_{\texttt{create:0}} = p_{\texttt{create:1}} =$	0	0

the probability that a $|+\rangle_{\rm B}$ state is flipped into $|-\rangle_{\rm B}$ in "test" rounds.

We consider the following noise model.

- In the "raw key" rounds, we consider that *both* the forward channel (from Bob to Alice) and the reverse channel (from Alice to Bob) are depolarizing channels with error $Q_{\rm Z}$, as follows:

$$\mathcal{E}_{Q_{\rm Z}}(\rho) = (1-2Q_{\rm Z})\rho + 2Q_{\rm Z}\cdot\frac{I_2}{2}. \tag{48}$$

- In the "test" rounds, we consider that the whole channel (from Bob to Alice and back to Bob; notice that Alice does nothing in such rounds) is a depolarizing channel with error $Q_{\rm X}$, as follows:

$$\mathcal{E}_{Q_{\rm X}}(\rho) = (1-2Q_{\rm X})\rho + 2Q_{\rm X}\cdot\frac{I_2}{2}. \tag{49}$$

Here, in the forward attack, Eve always replaces Bob's original state $|0,1\rangle_{\rm x,B} \triangleq \frac{|0,1\rangle_{\rm B}+|1,0\rangle_{\rm B}}{\sqrt{2}}$ by the following state [a special case of (7)]:

$$|\psi_0\rangle = |0,1\rangle_{\rm B}|e_{0,1}\rangle_{\rm E} + |1,0\rangle_{\rm B}|e_{1,0}\rangle_{\rm E} \tag{50}$$

with $\langle e_{0,1}|e_{0,1}\rangle_{\rm E} = \langle e_{1,0}|e_{1,0}\rangle_{\rm E} = 1/2$.

B. SECOND SCENARIO: SINGLE-PHOTON ATTACKS WITH LOSSES

In the second scenario, our noise model remains identical to the first scenario, except two modifications.

1) In the forward channel (from Bob to Alice), a loss occurs with probability $p_\ell^{\rm F}$; if it *does not* occur, the original noise model is applied.
2) In the reverse channel (from Alice to Bob), a loss occurs with probability $p_\ell^{\rm R}$; if it *does not* occur, the original noise model is applied.

We assume, in particular, that a loss is *final:* if a loss occurs in the forward channel, no photon will ever be observed in this round by either Alice or Bob.

C. EVALUATION RESULTS

In Table 5, we evaluate all probabilities in both scenarios.

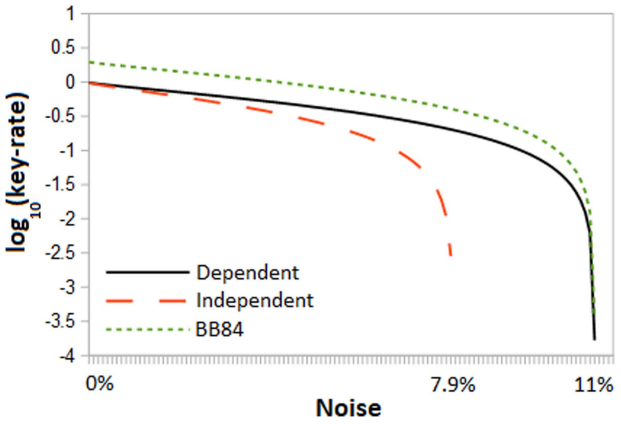

FIGURE 2. Graph of the final key rate versus the noise level of the Mirror protocol in the first scenario (single-photon attacks without losses) for dependent ($Q_{\rm X} = Q_{\rm Z}$) and independent ($Q_{\rm X} = 2Q_{\rm Z}(1-Q_{\rm Z})$) noise models, compared to two copies of BB84.

1) FIRST SCENARIO—SINGLE-PHOTON ATTACKS WITHOUT LOSSES

Substituting the probabilities from Table 5 in (42)–(44), we find the three constraints to be

$$\Re\left(\langle E_0|E_3\rangle_{\rm E} + \langle E_1|E_2\rangle_{\rm E}\right) \geq \frac{1}{4} - \frac{1}{2}Q_{\rm X} \tag{51}$$

$$|\Re\langle E_0|E_3\rangle_{\rm E}| \leq \frac{1}{4}(1-Q_{\rm Z}) \tag{52}$$

$$|\Re\langle E_1|E_2\rangle_{\rm E}| \leq \frac{1}{4}Q_{\rm Z}. \tag{53}$$

As explained in Section III-G, we numerically find the minimal value of the key rate expression $r = S(A|E) - H(A|B)$ for various values of $Q_{\rm Z,X}$ by using the lower bound on $S(A|E)$ presented in (41), which is evaluated under the three above constraints on the values of $\Re\langle E_0|E_3\rangle_{\rm E}$ and $\Re\langle E_1|E_2\rangle_{\rm E}$. This numerical optimization yields the graph shown in Fig. 2, presenting two cases.

1) In the *dependent* noise model, where the error rates $Q_{\rm X}$ and $Q_{\rm Z}$ are identical (namely, $Q_{\rm X} = Q_{\rm Z}$), we recover the asymptotic BB84 noise tolerance of 11%.
2) In the *independent* noise model, where the two-way channel is modeled as two independent depolarizing channels (namely, $Q_{\rm X} = 2Q_{\rm Z}(1-Q_{\rm Z})$), the maximal (asymptotic) noise tolerance is 7.9%.

Interestingly, both values agree with the values found in [57] for the original "QKD with Classical Bob" SQKD protocol [2].

In both scenarios, because the Mirror protocol is two-way, we compare it to *two* copies of BB84 performed from Alice to Bob; this is a common comparison for two-way protocols (see, for example, [32]). The key rate of two copies of BB84 is $2(1-2H_2(p))$—namely, twice the original key rate of BB84.

2) SECOND SCENARIO—SINGLE-PHOTON ATTACKS WITH LOSSES

Substituting the probabilities from Table 5 in (42)–(44), we find the three constraints to be

$$\Re\left(\langle E_0|E_3\rangle_{\mathrm{E}} + \langle E_1|E_2\rangle_{\mathrm{E}}\right) \geq (1-p_\ell^{\mathrm{F}})(1-p_\ell^{\mathrm{R}})\left(\frac{1}{4}-\frac{1}{2}Q_{\mathrm{X}}\right) \tag{54}$$

$$|\Re\langle E_0|E_3\rangle_{\mathrm{E}}| \leq \frac{1}{4}(1-p_\ell^{\mathrm{F}})(1-p_\ell^{\mathrm{R}})(1-Q_{\mathrm{Z}}) \tag{55}$$

$$|\Re\langle E_1|E_2\rangle_{\mathrm{E}}| \leq \frac{1}{4}(1-p_\ell^{\mathrm{F}})(1-p_\ell^{\mathrm{R}})Q_{\mathrm{Z}}. \tag{56}$$

The numerical analysis for this scenario is similar to the previous one. However, here, we must also model the loss rates, so we consider a fiber channel with loss rates $p_\ell^{\mathrm{F,R}} = 1-10^{-\alpha\ell}$ (where α is the loss coefficient, and ℓ is measured in kilometers). We consider two examples of fiber lengths: $\ell = 10\,\mathrm{km}$ and $\ell = 50\,\mathrm{km}$. Results are presented in Fig. 3.

These evaluations lead to several observations—most notably, the observation that the Mirror protocol is more sensitive to loss than BB84 even in the single photon case: increasing the fiber length from $\ell = 10$ km to $\ell = 50$ km causes a significant drop in key rate. We also note that the key rate of the Mirror protocol at only 10 km coincides with that of BB84 at 50 km. This seems to indicate, not surprisingly, that BB84 outperforms the Mirror protocol under loss. There are many reasons for this. First, note that each photon in Mirror travels twice the distance compared to BB84: while we are comparing Mirror with two copies of BB84, these copies are treated independently, and thus, for a single bit to be produced from these two copies, it is sufficient for one of the photons to survive transmission without being lost (over a fiber of length ℓ). On the other hand, in the Mirror protocol, the photon must travel through *both* channels without loss (a total fiber length of 2ℓ) for a single bit to be produced from a round. Second, in Mirror Eve has two opportunities to attack, which gives her a bigger attack strategy space for any given loss level. Finally, our security analysis against loss may not be as tight as our analysis against noise (where, as seen in Fig. 2, the Mirror protocol performs similarly to BB84 under a lossless but noisy channel). This is, to our knowledge, the first security proof for the Mirror protocol against loss, and future improvements may exist.

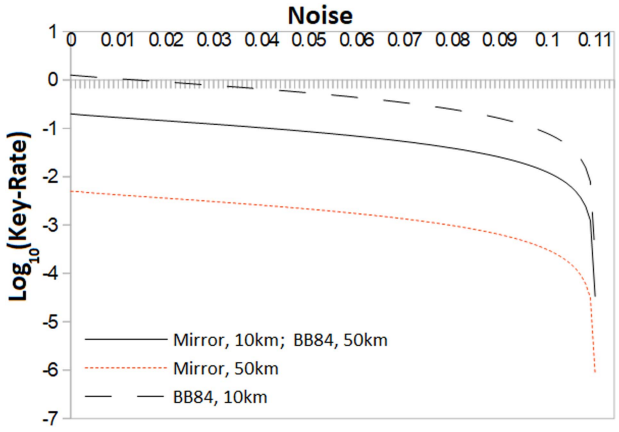

FIGURE 3. Graph of the final key rate versus the noise level of the Mirror protocol in the second scenario (single-photon attacks *with* losses), compared to two copies of BB84, for two possible lengths of fiber channels ($\ell = 10$ km and $\ell = 50$ km) and $\alpha = 0.2$ dB/km. Note that this figure presents the effective key rate computed by the expression $r = S(A|E) - H(A|B)$, which scales with the probability of a raw key bit being generated. Also note that the key rate of BB84 at 50 km coincides with that of the Mirror protocol at 10 km, so both are plotted as the same (solid) line.

V. CONCLUSION

In this article, we have proved the security of the Mirror protocol against collective attacks, including attacks where the adversary Eve sends multiple photons towards the classical user (Alice). Our analysis shows that the asymptotic noise tolerance of the Mirror protocol is comparable, in the single-photon scenario, to the "QKD with Classical Bob" protocol [2], [57] and even to the BB84 protocol. Moreover, we have suggested a general framework for analyzing multiphoton attacks; this framework may be useful for other QKD and SQKD protocols, too.

We conclude that the Mirror protocol is theoretically secure against collective attacks, and we suspect similar security results can be achieved for general attacks. Extensions of our results, such as security against general attacks, security against multiphoton attacks on both channels, and evaluation of our key rate formula in the multiphoton case, are left for future research. Our extension to multiphoton attacks also suggests the intriguing possibility of analyzing SQKD protocols employing decoy states and similar countermeasures against practical attacks.

Our results show that SQKD protocols can potentially be implemented in a secure way, overcoming the practical attacks suggested in [36] and [37]. They, therefore, hold the potential to transform the SQKD protocols, making them not only theoretically fascinating, but also practically secure.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179, doi: 10.1016/j.tcs.2014.05.025.

[2] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical Bob," *Phys. Rev. Lett.*, vol. 99, 2007, Art. no. 140501, doi: 10.1103/PhysRevLett.99.140501.

[3] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, "Semiquantum key distribution," *Phys. Rev. A*, vol. 79, 2009, Art. no. 0032341, doi: 10.1103/PhysRevA.79.032341.

[4] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, "Semiquantum-key distribution using less than four quantum states," *Phys. Rev. A*, vol. 79, 2009, Art. no. 052312, doi: 10.1103/PhysRevA.79.052312.

[5] M. Boyer and T. Mor, "Comment on "Semiquantum-key distribution using less than four quantum states"," *Phys. Rev. A*, vol. 83, 2011, Art. no. 0046301, doi: 10.1103/PhysRevA.83.046301.

[6] H. Lu and Q.-Y. Cai, "Quantum key distribution with classical Alice," *Int. J. Quantum Inf.*, vol. 6, no. 6, pp. 1195–1202, 2008, doi: 10.1142/S0219749908004353.

[7] Z.-W. Sun, R.-G. Du, and D.-Y. Long, "Quantum key distribution with limited classical Bob," *Int. J. Quantum Inf.*, vol. 11, no. 1, 2013, Art. no. 1350005, doi: 10.1142/S0219749913500056.

[8] K.-F. Yu, C.-W. Yang, C.-H. Liao, and T. Hwang, "Authenticated semi-quantum key distribution protocol using Bell states," *Quantum Inf. Process.*, vol. 13, no. 6, pp. 1457–1465, 2014, doi: 10.1007/s11128-014-0740-z.

[9] W. O. Krawec, "Mediated semiquantum key distribution," *Phys. Rev. A*, vol. 91, 2015, Art. no. 0032323, doi: 10.1103/PhysRevA.91.032323.

[10] X. Zou, D. Qiu, S. Zhang, and P. Mateus, "Semiquantum key distribution without invoking the classical party's measurement capability," *Quantum Inf. Process.*, vol. 14, no. 8, pp. 2981–2996, 2015, doi: 10.1007/s11128-015-1015-z.

[11] W. Zhang, D. Qiu, and P. Mateus, "Single-state semi-quantum key distribution protocol and its security proof," *Int. J. Quantum Inf.*, vol. 18, no. 4, 2020, Art. no. 2050013, doi: 10.1142/S0219749920500136.

[12] Z. Rong, D. Qiu, P. Mateus, and X. Zou, "Mediated semi-quantum secure direct communication," *Quantum Inf. Process.*, vol. 20, 2021, Art. no. 58, doi: 10.1007/s11128-020-02965-2.

[13] Z. Rong, D. Qiu, and X. Zou, "Two single-state semi-quantum secure direct communication protocols based on single photons," *Int. J. Modern Phys. B*, vol. 34, no. 11, 2020, Art. no. 2050106, doi: 10.1142/S0217979220501064.

[14] Z. Rong, D. Qiu, and X. Zou, "Semi-quantum secure direct communication using entanglement," *Int. J. Theor. Phys.*, vol. 59, pp. 1807–1819, 2020, doi: 10.1007/s10773-020-04447-8.

[15] U. Mahadev, "Classical verification of quantum computations," in *Proc. IEEE 59th Annu. Symp. Found. Comput. Sci.*, 2018, pp. 259–267, doi: 10.1109/FOCS.2018.00033.

[16] B. W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," *Nature*, vol. 496, no. 7446, pp. 456–460, 2013, doi: 10.1038/nature12035.

[17] H. Iqbal and W. O. Krawec, "Semi-quantum cryptography," *Quantum Inf. Process.*, vol. 19, no. 3, 2020, Art. no. 97, doi: 10.1007/s11128-020-2595-9.

[18] Q. Li, W. H. Chan, and D.-Y. Long, "Semiquantum secret sharing using entangled states," *Phys. Rev. A*, vol. 82, 2010, Art. no. 0022303, doi: 10.1103/PhysRevA.82.022303.

[19] L. Li, D. Qiu, and P. Mateus, "Quantum secret sharing with classical Bobs," *J. Phys. A*, vol. 46, no. 4, 2013, Art. no. 0045304, doi: 10.1088/1751-8113/46/4/045304.

[20] Z. Li, Q. Li, C. Liu, Y. Peng, W. H. Chan, and L. Li, "Limited resource semiquantum secret sharing," *Quantum Inf. Process.*, vol. 17, no. 10, 2018, Art. no. 285, doi: 10.1007/s11128-018-2058-8.

[21] C. Xie, L. Li, H. Situ, and J. He, "Semi-quantum secure direct communication scheme based on Bell states," *Int. J. Theor. Phys.*, vol. 57, no. 6, pp. 1881–1887, 2018, doi: 10.1007/s10773-018-3713-7.

[22] X. Zou and D. Qiu, "Three-step semiquantum secure direct communication protocol," *Sci. China Phys. Mech. Astron.*, vol. 57, no. 9, pp. 1696–1702, 2014, doi: 10.1007/s11433-014-5542-x.

[23] M.-H. Zhang, H.-F. Li, Z.-Q. Xia, X.-Y. Feng, and J.-Y. Peng, "Semiquantum secure direct communication using EPR pairs," *Quantum Inf. Process.*, vol. 16, no. 5, 2017, Art. no. 117, doi: 10.1007/s11128-017-1573-3.

[24] L. Yan, Y. Sun, Y. Chang, S. Zhang, G. Wan, and Z. Sheng, "Semi-quantum protocol for deterministic secure quantum communication using Bell states," *Quantum Inf. Process.*, vol. 17, no. 11, 2018, Art. no. 315, doi: 10.1007/s11128-018-2086-4.

[25] X.-J. Wen, X.-Q. Zhao, L.-H. Gong, and N.-R. Zhou, "A semi-quantum authentication protocol for message and identity," *Laser Phys. Lett.*, vol. 16, no. 7, 2019, Art. no. 0075206, doi: 10.1088/1612-202X/ab232c.

[26] N.-R. Zhou, K.-N. Zhu, W. Bi, and L.-H. Gong, "Semi-quantum identification," *Quantum Inf. Process.*, vol. 18, no. 6, 2019, Art. no. 197, doi: 10.1007/s11128-019-2308-4.

[27] K. Thapliyal, R. D. Sharma, and A. Pathak, "Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment," *Int. J. Quantum Inf.*, vol. 16, no. 5, 2018, Art. no. 1850047, doi: 10.1142/S0219749918500478.

[28] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, "Interactive proofs for quantum computations," Apr. 2017, *arXiv:1704.04487*, doi: 10.48550/arXiv.1704.04487.

[29] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, ""Plug and play" systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, no. 7, pp. 793–795, 1997, doi: 10.1063/1.118224.

[30] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, 2002, Art. no. 187902, doi: 10.1103/PhysRevLett.89.187902.

[31] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," *Phys. Rev. Lett.*, vol. 94, 2005, Art. no. 140501, doi: 10.1103/PhysRevLett.94.140501.

[32] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, "Security of two-way quantum key distribution," *Phys. Rev. A*, vol. 88, 2013, Art. no. 0062302, doi: 10.1103/PhysRevA.88.062302.

[33] P. Gurevich, "Experimental quantum key distribution with classical Alice," M.S. thesis, Dept. Elect. Eng. Dept. Comput. Sci., Technion—Israel Inst. Technol., Haifa, Israel, May 2013.

[34] N. Tamari, "Experimental semiquantum key distribution: Classical Alice with mirror," M.S. thesis, Dept. Elect. Eng. Dept. Comput. Sci., Technion—Israel Inst. Technol., Haifa, Israel, Nov. 2014.

[35] F. Massa et al., "Experimental semi-quantum key distribution with classical users," *Quantum*, vol. 6, p. 819, 2022, doi: 10.22331/q-2022-09-22-819.

[36] Y.-G. Tan, H. Lu, and Q.-Y. Cai, "Comment on "Quantum key distribution with classical Bob"," *Phys. Rev. Lett.*, vol. 102, 2009, Art. no. 0098901, doi: 10.1103/PhysRevLett.102.098901.

[37] M. Boyer, D. Kenigsberg, and T. Mor, "Boyer, Kenigsberg, and Mor Reply," *Phys. Rev. Lett.*, vol. 102, 2009, Art. no. 0098902, doi: 10.1103/PhysRevLett.102.098902.

[38] M. Boyer, M. Katz, R. Liss, and T. Mor, "Experimentally feasible protocol for semiquantum key distribution," *Phys. Rev. A*, vol. 96, 2017, Art. no. 0062335, doi: 10.1103/PhysRevA.96.062335.

[39] M. Boyer, R. Liss, and T. Mor, "Attacks against a simplified experimentally feasible semiquantum key distribution protocol," *Entropy*, vol. 20, no. 7, 2018, Art. no. 536, doi: 10.3390/e20070536.

[40] W. O. Krawec, "Security proof of a semi-quantum key distribution protocol," in *Proc. IEEE Int. Symp. Inf. Theory*, 2015, pp. 686–690, doi: 10.1109/ISIT.2015.7282542.

[41] W. O. Krawec, "Security of a semi-quantum protocol where reflections contribute to the secret key," *Quantum Inf. Process.*, vol. 15, no. 5, pp. 2067–2090, 2016, doi: 10.1007/s11128-016-1266-3.

[42] W. Zhang, D. Qiu, and P. Mateus, "Security of a single-state semi-quantum key distribution protocol," *Quantum Inf. Process.*, vol. 17, no. 6, 2018, Art. no. 135, doi: 10.1007/s11128-018-1904-z.

[43] W. O. Krawec, "Practical security of semi-quantum key distribution," *Proc. SPIE*, vol. 10660, 2018, Art. no. 1066009, doi: 10.1117/12.2303759.

[44] E. Biham and T. Mor, "Security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 78, pp. 2256–2259, 1997, doi: 10.1103/PhysRevLett.78.2256.

[45] E. Biham and T. Mor, "Bounds on information and the security of quantum cryptography," *Phys. Rev. Lett.*, vol. 79, pp. 4034–4037, 1997, doi: 10.1103/PhysRevLett.79.4034.

[46] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, "Security of quantum key distribution against all collective attacks," *Algorithmica*, vol. 34, no. 4, pp. 372–388, 2002, doi: 10.1007/s00453-002-0973-6.

[47] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, 2001, doi: 10.1145/382780.382781.

[48] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, 2000, doi: 10.1103/PhysRevLett.85.441.

[49] E. Biham, M. Boyer, O. P. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," *J. Cryptol.*, vol. 19, no. 4, pp. 381–439, 2006, doi: 10.1007/s00145-005-0011-3.

[50] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, 2005, Art. no. 0012332, doi: 10.1103/PhysRevA.72.012332.

[51] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no. 1, pp. 1–127, 2008, doi: 10.1142/S0219749908003256.

[52] M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, 2009, Art. no. 0020504, doi: 10.1103/PhysRevLett.102.020504.

[53] T. Metger and R. Renner, "Security of quantum key distribution from generalised entropy accumulation," Mar. 2022, *arXiv:2203.04993*, doi: 10.48550/arXiv.2203.04993.

[54] J. Guskind and W. O. Krawec, "Mediated semi-quantum key distribution with improved efficiency," *Quantum Sci. Technol.*, vol. 7, no. 3, 2022, Art. no. 0035019, doi: 10.1088/2058-9565/ac7412.

[55] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, 2000, doi: 10.1103/PhysRevLett.85.1330.

[56] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. Roy. Soc. A*, vol. 461, no. 2053, pp. 207–235, 2005, doi: 10.1098/rspa.2004.1372.

[57] W. O. Krawec, "Quantum key distribution with mismatched measurements over arbitrary channels," *Quantum Inf. Comput.*, vol. 17, no. 3/4, pp. 209–241, 2017, doi: 10.26421/QIC17.3-4-2.

[58] W. O. Krawec, "Key-rate bound of a semi-quantum protocol using an entropic uncertainty relation," in *Proc. IEEE Int. Symp. Inf. Theory*, 2018, pp. 2669–2673, doi: 10.1109/ISIT.2018.8437303.

[59] S. M. Barnett, B. Huttner, and S. J. Phoenix, "Eavesdropping strategies and rejected-data protocols in quantum cryptography," *J. Modern Opt.*, vol. 40, no. 12, pp. 2501–2513, 1993, doi: 10.1080/09500349314552491.

[60] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Phys. Rev. A*, vol. 78, 2008, Art. no. 0042316, doi: 10.1103/PhysRevA.78.042316.