entropy

MDPI

Article

Attacks against a Simplified Experimentally Feasible Semiquantum Key Distribution Protocol

Michel Boyer [1], Rotem Liss [2,*] and Tal Mor [2]

[1] Département d'Informatique et de Recherche Opérationnelle (DIRO), Université de Montréal, Montréal, QC H3C 3J7, Canada; boyer@iro.umontreal.ca

[2] Computer Science Department, Technion, Haifa 3200003, Israel; talmo@cs.technion.ac.il

* Correspondence: rotemliss@cs.technion.ac.il; Tel.: +972-4-829-3826

Received: 16 June 2018; Accepted: 16 July 2018; Published: 18 July 2018

Abstract: A semiquantum key distribution (SQKD) protocol makes it possible for a quantum party and a classical party to generate a secret shared key. However, many existing SQKD protocols are not experimentally feasible in a secure way using current technology. An experimentally feasible SQKD protocol, "classical Alice with a controllable mirror" (the "Mirror protocol"), has recently been presented and proved completely robust, but it is more complicated than other SQKD protocols. Here we prove a simpler variant of the Mirror protocol (the "simplified Mirror protocol") to be completely non-robust by presenting two possible attacks against it. Our results show that the complexity of the Mirror protocol is at least partly necessary for achieving robustness.

Keywords: quantum key distribution; semiquantum key distribution; security; attack

1. Introduction

Quantum key distribution (QKD) protocols allow two parties, Alice and Bob, to share a secret random key that is secure even against the most powerful adversaries. Semiquantum key distribution (SQKD) protocols achieve the same goal even if one of the two parties (Alice or Bob) is limited to use only classical operations: the classical party can use only the computational basis $\{|0\rangle, |1\rangle\}$, while the quantum party can use any basis—for example, both the computational basis and the Hadamard basis $\{|+\rangle \triangleq \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle \triangleq \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. As explained in [1,2], the importance of SQKD protocols is both conceptual and practical: they make it possible to investigate the amount of "quantumness" needed for QKD, and they may, in some cases, be easier to implement than standard QKD protocols.

The first SQKD protocol was "QKD with classical Bob" [1]. Later, other SQKD protocols have been suggested, including "QKD with classical Alice" [3,4] and many others (e.g., [2,5–9]). Most SQKD protocols have been proven "robust": namely [1], if the adversary Eve succeeds in getting some secret information, she must cause some errors that may be noticed by Alice and Bob. A few SQKD protocols also have a security analysis [10–13]. Proving robustness is a step towards proving security; proving the security of SQKD protocols is difficult because those protocols are usually two-way: for example, Alice sends a quantum state to Bob, and Bob performs a specific classical operation and sends the resulting quantum state back to Alice.

However, many SQKD protocols, including [1,3], are vulnerable to practical attacks and cannot be experimentally constructed in a secure way using current technology. An important classical operation of those protocols is named SIFT. The definition of a SIFT operation performed by Alice (assuming that Alice is the classical party) is as follows: Alice measures the incoming quantum state in the computational basis $\{|0\rangle, |1\rangle\}$ and then generates the state she measured and resends it towards Bob. Security of those SQKD protocols relies on the assumption that during the SIFT operation, Alice's measurement devices can measure the *precise* states $\{|0\rangle, |1\rangle\}$ and distinguish those precise

states from any imperfect similar state, and Alice's photon generation devices can generate the *precise* states $\{|0\rangle, |1\rangle\}$ and not any other (imperfect) state. In particular, the generated states $\{|0\rangle, |1\rangle\}$ must be indistinguishable from states that Alice *reflects* towards Bob. Using current photonic technology, Alice's devices are imperfect, which makes this assumption incorrect and makes possible attacks by the eavesdropper Eve: for example, Eve may send a slightly modified state towards Alice (a "tagging attack") or may distinguish between the states sent by Alice. Full details about those practical attacks are available in [14–16].

An experimentally feasible SQKD protocol named "classical Alice with a controllable mirror" (the "Mirror protocol") has recently been presented [16]. This protocol is safe against the "tagging" attack presented by [14]. Moreover, the protocol was proved by [16] to be completely robust against any attacker Eve, even if Eve is all-powerful and limited only by the laws of physics, and even if Eve can send multi-photon pulses. The robustness proof is still correct even if the detectors of Alice and Bob cannot *count* how many photons arrive in each mode: namely, when either Alice or Bob looks at a detector, which detects a specific mode, they can only notice whether it "clicks" (detects one photon or more in that mode) or not (finds the mode to be empty). This is the standard situation when using current technology.

In this paper, we present a simpler variant of the Mirror protocol (the "simplified Mirror protocol"), which is easier to implement. Our variant allows the classical party, Alice, to choose one of three operations, while the Mirror protocol allows Alice to choose one of four operations. We present two attacks against this variant, proving it to be non-robust. Our results show that the four classical operations allowed by the Mirror protocol are probably necessary for robustness.

In Section 2 we present the Mirror protocol described by [16]. In Section 3 we present the simplified Mirror protocol and its motivation. In Section 4 we prove the simplified Mirror protocol to be non-robust by presenting two attacks against it: a full attack and a weaker attack. In Section 5 we discuss potential implications of our results.

2. The Mirror Protocol

For describing the Mirror protocol (presented by [16]), we assume a photonic implementation consisting of two modes: the mode of the qubit state $|0\rangle$ and the mode of the qubit state $|1\rangle$ (below 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. We use the Fock space notations: if there is exactly one photon (and, thus, our Hilbert space is the qubit space), the Fock state $|0,1\rangle$ (equivalent to $|0\rangle$) represents one photon in the $|0\rangle$ mode, and the Fock state $|1,0\rangle$ (equivalent to $|1\rangle$) represents one photon in the $|1\rangle$ mode. 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. Most generally, the Fock state $|m_1, m_0\rangle$ represents m_1 indistinguishable photons in the $|1\rangle$ mode and m_0 indistinguishable photons in the $|0\rangle$ mode. Similarly (in the Hadamard basis), the Fock state $|m_-, m_+\rangle_X$ represents m_- indistinguishable photons in the $|-\rangle$ mode and m_+ indistinguishable photons in the $|+\rangle$ mode. More details about the Fock space notations are given in [16]; it is vital to use those mathematical notations for describing and analyzing all practical attacks on a QKD protocol (see [17] for details).

In the Mirror protocol, in each round, Bob sends to Alice the $|+\rangle_B$ state—namely, the $|0,1\rangle_{X,B} \triangleq \frac{|0,1\rangle_B + |1,0\rangle_B}{\sqrt{2}}$ state. Then, Alice prepares an ancillary state in the initial vacuum state $|0,0\rangle_A$ and chooses at random one of the following four classical operations:

- **I** (**CTRL**) Reflect all the photons towards Bob, without measuring any photon. The mathematical description is:

$$I\,|0,0\rangle_A\,|m_1, m_0\rangle_B = |0,0\rangle_A\,|m_1, m_0\rangle_B. \tag{1}$$

- **S_1 (SWAP-10)** Reflect all photons in the $|0\rangle$ mode towards Bob, and measure all photons in the $|1\rangle$ mode. The mathematical description is:

$$S_1 |0,0\rangle_A |m_1, m_0\rangle_B = |m_1, 0\rangle_A |0, m_0\rangle_B. \quad (2)$$

- **S_0 (SWAP-01)** Reflect all photons in the $|1\rangle$ mode towards Bob, and measure all photons in the $|0\rangle$ mode. The mathematical description is:

$$S_0 |0,0\rangle_A |m_1, m_0\rangle_B = |0, m_0\rangle_A |m_1, 0\rangle_B. \quad (3)$$

- **S (SWAP-ALL)** Measure all the photons, without reflecting any photon towards Bob. The mathematical description is:

$$S |0,0\rangle_A |m_1, m_0\rangle_B = |m_1, m_0\rangle_A |0,0\rangle_B. \quad (4)$$

(We note that in the above mathematical description, Alice measures her ancillary state $|\cdot\rangle_A$ in the computational basis and sends back to Bob the $|\cdot\rangle_B$ state.)

The states sent from Alice to Bob (without any error, loss, or eavesdropping) are detailed in Table 1.

Table 1. The state sent from Alice to Bob in the Mirror protocol without errors or losses, depending on Alice's classical operation and on whether Alice detected a photon or not.

Alice's Classical Operation	Did Alice Detect a Photon?	State Sent from Alice to Bob
CTRL	no (happens with certainty)	$\|0,1\rangle_{x,B} = \frac{1}{\sqrt{2}} [\, \|0,1\rangle_B + \|1,0\rangle_B]$
SWAP-10	no (happens with probability $\frac{1}{2}$)	$\|0,1\rangle_B$
SWAP-10	yes (happens with probability $\frac{1}{2}$)	$\|0,0\rangle_B$
SWAP-01	no (happens with probability $\frac{1}{2}$)	$\|1,0\rangle_B$
SWAP-01	yes (happens with probability $\frac{1}{2}$)	$\|0,0\rangle_B$
SWAP-ALL	yes (happens with certainty)	$\|0,0\rangle_B$

Then, Bob measures the incoming state in a random basis (either the computational basis $\{ |0\rangle, |1\rangle \}$ or the Hadamard basis $\{ |+\rangle, |-\rangle \}$). After completing all rounds, 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 some non-secret information on their measurement results (as elaborated in [16]). Then, Alice and Bob reveal and compute the error rate on test bits for which Alice used SWAP-10 or SWAP-01 and Bob measured in the computational basis, and the error rate on test bits for which Alice used CTRL and Bob measured in the Hadamard basis. They also check whether other errors exist (for example, they verify Bob detects no photons in case Alice uses SWAP-ALL). Alice and Bob also discard mismatched rounds, such as rounds in which Alice used SWAP-10 and Bob used the Hadamard basis. Alice and Bob share the secret bit 0 if Alice uses SWAP-10 and detects no photon while Bob measures in the computational basis and detects a photon in the $|0\rangle$ mode; similarly, they share the secret bit 1 if Alice uses SWAP-01 and detects no photon while Bob measures in the computational basis and detects a photon in the $|1\rangle$ mode.

Finally, Alice and Bob verify that the error rates are below some thresholds, and 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 protocol and a proof of its complete robustness are both available in [16].

The experimental implementation of the protocol can use two time bins (namely, two pulses), one for the $|0\rangle$ mode and one for the $|1\rangle$ mode. In this case, Alice's possible operations can be described

as possible ways for operating a controllable mirror, so that Alice can choose whether to reflect or measure the photon(s) in each time bin. The mirror can be experimentally implemented in various ways; for example:

- It can be implemented as a mechanically moved mirror. Such mirror is trivial to implement, but it is very slow.
- It can be implemented by using optical elements: an electronically-triggered Pockels cell, which changes the polarization of the photon(s) in one of the pulses, and a polarizing beam splitter, which can split the two different pulses (that now have different polarizations) into two paths. This implementation is feasible and gives much higher bit rates than the mechanical implementation.

More details about the experimental implementations are available in [16].

3. The "Simplified Mirror Protocol": A Simpler and Non-Robust Variant of the Mirror Protocol

In this paper, we discuss a simpler variant of the Mirror protocol, which we name the "simplified Mirror protocol". The simplified Mirror protocol is identical to the Mirror protocol described in Section 2, except that it does not include the SWAP-ALL operation. In other words, in the simplified protocol, Alice chooses at random one of the three classical operations CTRL, SWAP-10, and SWAP-01.

The simplified protocol is easier to implement, because the SWAP-ALL operation poses some experimental challenges to the electronic implementation discussed in Section 2: for implementing SWAP-ALL, the Pockels cell should either remain working for a long time (changing polarization for both time bins) or be operated twice (changing polarization for each time bin separately). In more details, for the two pulses representing the $|\mathrm{o}\rangle$ mode and the $|\mathrm{1}\rangle$ mode: if we assume the duration of each pulse is t and the time difference between the two pulses is T (where $t \ll T$), the first solution means keeping the Pockels cell operating during the time period $[0, T+2t]$, and the second solution means operating the Pockels cell during the two time periods $[0, t]$ and $[T+t, T+2t]$. The first solution may be problematic for some models of the Pockels cell, and the second solution may be problematic because of the recovery time needed for the Pockels cell. Therefore, at least in some implementations, the simplified Mirror protocol is much easier to implement than the standard Mirror protocol.

Moreover, analyzing the simplified protocol gives a better understanding of the properties required for an SQKD protocol to be robust. In particular, this analysis explains why the structure and complexity of the Mirror protocol are necessary for robustness.

For completeness, we provide below the full description of the simplified Mirror protocol. We note that this description is almost the same as the description of the Mirror protocol in Section 2.

In the simplified Mirror protocol, in each round, Bob sends to Alice the $|+\rangle_{\mathrm{B}}$ state—namely, the $|0{,}1\rangle_{\mathrm{x,B}} \triangleq \frac{|0,1\rangle_{\mathrm{B}}+|1,0\rangle_{\mathrm{B}}}{\sqrt{2}}$ state. Then, Alice prepares an ancillary state in the initial vacuum state $|0,0\rangle_{\mathrm{A}}$ and chooses at random one of the following three classical operations:

- **I** (**CTRL**) Reflect all the photons towards Bob, without measuring any photon. The mathematical description is:
$$I\,|0,0\rangle_{\mathrm{A}}\,|m_{\mathrm{1}},m_{\mathrm{o}}\rangle_{\mathrm{B}} = |0,0\rangle_{\mathrm{A}}\,|m_{\mathrm{1}},m_{\mathrm{o}}\rangle_{\mathrm{B}}. \tag{5}$$
- $\mathbf{S_1}$ (**SWAP-10**) Reflect all photons in the $|\mathrm{o}\rangle$ mode towards Bob, and measure all photons in the $|\mathrm{1}\rangle$ mode. The mathematical description is:
$$S_1\,|0,0\rangle_{\mathrm{A}}\,|m_{\mathrm{1}},m_{\mathrm{o}}\rangle_{\mathrm{B}} = |m_{\mathrm{1}},0\rangle_{\mathrm{A}}\,|0,m_{\mathrm{o}}\rangle_{\mathrm{B}}. \tag{6}$$
- $\mathbf{S_0}$ (**SWAP-01**) Reflect all photons in the $|\mathrm{1}\rangle$ mode towards Bob, and measure all photons in the $|\mathrm{o}\rangle$ mode. The mathematical description is:
$$S_0\,|0,0\rangle_{\mathrm{A}}\,|m_{\mathrm{1}},m_{\mathrm{o}}\rangle_{\mathrm{B}} = |0,m_{\mathrm{o}}\rangle_{\mathrm{A}}\,|m_{\mathrm{1}},0\rangle_{\mathrm{B}}. \tag{7}$$

(We note that in the above mathematical description, Alice measures her ancillary state $|\cdot\rangle_A$ in the computational basis and sends back to Bob the $|\cdot\rangle_B$ state.)

The states sent from Alice to Bob (without any error, loss, or eavesdropping) are detailed in Table 2.

Table 2. The state sent from Alice to Bob in the simplified Mirror protocol without errors or losses, depending on Alice's classical operation and on whether Alice detected a photon or not.

Alice's Classical Operation	Did Alice Detect a Photon?	State Sent from Alice to Bob
CTRL	no (happens with certainty)	$\|0,1\rangle_{x,B} = \frac{1}{\sqrt{2}}\left[\,|0,1\rangle_B + |1,0\rangle_B\right]$
SWAP-10	no (happens with probability $\frac{1}{2}$)	$\|0,1\rangle_B$
SWAP-10	yes (happens with probability $\frac{1}{2}$)	$\|0,0\rangle_B$
SWAP-01	no (happens with probability $\frac{1}{2}$)	$\|1,0\rangle_B$
SWAP-01	yes (happens with probability $\frac{1}{2}$)	$\|0,0\rangle_B$

Then, Bob measures the incoming state in a random basis (either the computational basis $\{\,|0\rangle, |1\rangle\}$ or the Hadamard basis $\{\,|+\rangle, |-\rangle\}$). After completing all rounds, Alice sends over the classical channel her operation choices (CTRL or SWAP-x; she keeps $x \in \{01, 10\}$ in secret), Bob sends over the classical channel his basis choices, and both of them reveal some non-secret information on their measurement results (as elaborated in [16]). Then, Alice and Bob reveal and compute the error rate on test bits for which Alice used SWAP-10 or SWAP-01 and Bob measured in the computational basis, and the error rate on test bits for which Alice used CTRL and Bob measured in the Hadamard basis. They also check whether other errors exist (for example, it must never happen that *both* Alice and Bob detect a photon). Alice and Bob also discard mismatched rounds, such as rounds in which Alice used SWAP-10 and Bob used the Hadamard basis. Alice and Bob share the secret bit 0 if Alice uses SWAP-10 and detects no photon while Bob measures in the computational basis and detects a photon in the $|0\rangle$ mode; similarly, they share the secret bit 1 if Alice uses SWAP-01 and detects no photon while Bob measures in the computational basis and detects a photon in the $|1\rangle$ mode.

Finally, Alice and Bob verify that the error rates are below some thresholds, and 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.

4. Attacks against the Simplified Mirror Protocol

We prove the simplified protocol to be non-robust by presenting two attacks: a "full attack" described in Section 4.1, which gives Eve full information but causes full loss of the CTRL bits, and a "weaker attack" described in Section 4.2, which gives Eve less information but causes fewer losses of CTRL bits.

4.1. A Full Attack on the Simplified Protocol that Gives Eve Full Information

In this attack, Eve gets full information of all the information bits. Namely, she gets full information on the SWAP-10 and SWAP-01 bits that were measured by Bob in the computational basis.

Eve applies her attack in two stages: the first stage is on the way from Bob to Alice, and the second stage is on the way from Alice to Bob. In both stages she uses her own probe space (namely, ancillary space) $\mathscr{H}_E = \mathscr{H}_3$ spanned by the orthonormal basis $\{\,|0\rangle_E, |1\rangle_E, |2\rangle_E\}$. We assume that Eve fully controls the environment, the errors, and the losses (this is a standard assumption when analyzing the security of QKD): namely, no losses and no errors exist between Bob and Eve or between Alice and Eve.

In the first stage of the attack (on the way from Bob to Alice), Eve intercepts the state $|+\rangle_B$ (namely, $|0,1\rangle_{x,B}$) sent by Bob, generates instead the state

$$\frac{1}{\sqrt{3}}\left[\,|0,1\rangle_B\,|1\rangle_E + |1,0\rangle_B\,|1\rangle_E + |0,0\rangle_B\,|0\rangle_E\right] = \sqrt{\frac{2}{3}}\,|0,1\rangle_{x,B}\,|1\rangle_E + \sqrt{\frac{1}{3}}\,|0,0\rangle_B\,|0\rangle_E, \tag{8}$$

and sends to Alice the B part of the state. This state causes Alice to get no photons with probability $\frac{1}{3}$ and get the expected $|+\rangle_B$ state with probability $\frac{2}{3}$. Alice then performs at random one of the three classical operations CTRL, SWAP-10, or SWAP-01. The resulting possible states of Bob+Eve are described in Table 3.

Table 3. The state of Bob+Eve after Alice's classical operation for the attacks described in Sections 4.1 and 4.2, depending on Alice's classical operation and on whether Alice detected a photon or not.

Alice's Classical Operation	Did Alice Detect a Photon?	Bob+Eve State
CTRL	no (happens with certainty)	$\frac{1}{\sqrt{3}}\left[\,|0,1\rangle_B\,|1\rangle_E + |1,0\rangle_B\,|1\rangle_E + |0,0\rangle_B\,|0\rangle_E\right]$
SWAP-10	no (happens with probability $\frac{2}{3}$)	$\frac{1}{\sqrt{2}}\left[\,|0,1\rangle_B\,|1\rangle_E + |0,0\rangle_B\,|0\rangle_E\right]$
SWAP-10	yes (happens with probability $\frac{1}{3}$)	$|0,0\rangle_B\,|1\rangle_E$
SWAP-01	no (happens with probability $\frac{2}{3}$)	$\frac{1}{\sqrt{2}}\left[\,|1,0\rangle_B\,|1\rangle_E + |0,0\rangle_B\,|0\rangle_E\right]$
SWAP-01	yes (happens with probability $\frac{1}{3}$)	$|0,0\rangle_B\,|1\rangle_E$

In the second stage of the attack (on the way from Alice to Bob), Eve applies the unitary operator V on the joint Bob+Eve state, where V is defined as follows:

$$V\,|0,1\rangle_B\,|1\rangle_E = -\sqrt{\frac{1}{3}}\,|1,0\rangle_B\,|1\rangle_E + \sqrt{\frac{2}{3}}\,|0,0\rangle_B\,|0\rangle_E, \tag{9}$$

$$V\,|1,0\rangle_B\,|1\rangle_E = -\sqrt{\frac{1}{3}}\,|0,1\rangle_B\,|0\rangle_E + \sqrt{\frac{2}{3}}\,|0,0\rangle_B\,|1\rangle_E, \tag{10}$$

$$V\,|0,0\rangle_B\,|0\rangle_E = \sqrt{\frac{1}{3}}\,|0,1\rangle_B\,|0\rangle_E + \sqrt{\frac{1}{3}}\,|1,0\rangle_B\,|1\rangle_E + \sqrt{\frac{1}{3}}\,|0,0\rangle_B\,|+\rangle_E, \tag{11}$$

$$V\,|0,0\rangle_B\,|1\rangle_E = |0,0\rangle_B\,|2\rangle_E. \tag{12}$$

V is indeed a unitary operator, because we can prove the right-hand sides to be orthonormal: all the right-hand sides are normalized vectors; the first two vectors are clearly orthogonal; the third vector is orthogonal to the first two, because $\langle 0|+\rangle_E = \langle 1|+\rangle_E = \frac{1}{\sqrt{2}}$; and the fourth vector is orthogonal to the three others. Thus, V defines (or, more precisely, can be extended to) a unitary operator on $\mathscr{H}_B \otimes \mathscr{H}_E$.

Applying the unitary operator V on Table 3 gives the states listed in Table 4. Comparing it with Table 2, we conclude that this attack never causes Alice and Bob to detect an error. Moreover, Eve detects the whole secret key: Eve measures "0" in her probe if Alice and Bob agree on the bit 0, and she measures "1" in her probe if Alice and Bob agree on the bit 1. However, Eve causes several kinds of losses; in particular, all the CTRL bits are lost.

Therefore, this attack makes it possible for Eve to get full information without inducing any error. However, Eve causes many losses, including full loss of the CTRL bits.

Table 4. The state of Bob+Eve after completing Eve's attack described in Section 4.1, depending on Alice's classical operation and on whether Alice detected a photon or not.

Alice's Classical Operation	Did Alice Detect a Photon?	Bob+Eve State
CTRL	no (happens with certainty)	$\|0,0\rangle_B \|+\rangle_E$
SWAP-10	no (happens with probability $\frac{2}{3}$)	$\frac{1}{\sqrt{6}} \|0,1\rangle_B \|0\rangle_E + \|0,0\rangle_B \frac{3\|0\rangle_E + \|1\rangle_E}{\sqrt{12}}$
SWAP-10	yes (happens with probability $\frac{1}{3}$)	$\|0,0\rangle_B \|2\rangle_E$
SWAP-01	no (happens with probability $\frac{2}{3}$)	$\frac{1}{\sqrt{6}} \|1,0\rangle_B \|1\rangle_E + \|0,0\rangle_B \frac{\|0\rangle_E + 3\|1\rangle_E}{\sqrt{12}}$
SWAP-01	yes (happens with probability $\frac{1}{3}$)	$\|0,0\rangle_B \|2\rangle_E$

4.2. A Weaker Attack on the Simplified Protocol Causing Fewer Losses of the CTRL Bits

The full attack described in Section 4.1 makes it impossible for Bob to ever detect a CTRL bit, which may look suspicious. We now present a weaker attack that lets Bob detect some CTRL bits but gives Eve less information.

The first stage of the attack (on the way from Bob to Alice) remains the same: that is, the state Eve sends to Alice is still given by Equation (8), and the resulting Bob+Eve state after Alice's classical operation is still shown in Table 3. Eve's probe space is, too, the same as before: $\mathscr{H}_E = \mathscr{H}_3 \triangleq \text{Span}\{|0\rangle_E, |1\rangle_E, |2\rangle_E\}$.

This attack is characterized by the parameter $0 \leq \epsilon \leq 1$. We will see that $\epsilon = 0$ gives the full attack described in Section 4.1, while $\epsilon = 1$ gives Eve no information at all.

Another important parameter used by the attack is

$$\kappa \triangleq \sqrt{\frac{1-\epsilon^2}{3-2\epsilon^2}}. \tag{13}$$

We notice that for small values of ϵ, the value of κ is close to $\sqrt{\frac{1}{3}}$. Moreover, for all $0 \leq \epsilon \leq 1$, it holds that $0 < \epsilon^2 + \kappa^2 \leq 1$ and $2\kappa^2 < 1$.

In the second stage of the attack (on the way from Alice to Bob), Eve applies the unitary operator V on the joint Bob+Eve state, where V is defined as follows:

$$V|0,1\rangle_B|1\rangle_E = \epsilon|0,1\rangle_B|2\rangle_E - \kappa|1,0\rangle_B|1\rangle_E + \sqrt{1-\kappa^2-\epsilon^2}|0,0\rangle_B|0\rangle_E, \tag{14}$$

$$V|1,0\rangle_B|1\rangle_E = -\kappa|0,1\rangle_B|0\rangle_E + \epsilon|1,0\rangle_B|2\rangle_E + \sqrt{1-\kappa^2-\epsilon^2}|0,0\rangle_B|1\rangle_E, \tag{15}$$

$$V|0,0\rangle_B|0\rangle_E = \kappa|0,1\rangle_B|0\rangle_E + \kappa|1,0\rangle_B|1\rangle_E + \sqrt{1-2\kappa^2}|0,0\rangle_B|+\rangle_E, \tag{16}$$

$$V|0,0\rangle_B|1\rangle_E = |0,0\rangle_B|2\rangle_E. \tag{17}$$

V is indeed a unitary operator, because we can prove the right-hand sides to be orthonormal: all the right-hand sides are clearly normalized; the first two vectors are orthogonal; the fourth vector is orthogonal to the three others; and the third vector is orthogonal to the first and to the second, because

$$1-2\kappa^2 = \frac{3-2\epsilon^2-2(1-\epsilon^2)}{3-2\epsilon^2} = \frac{1}{3-2\epsilon^2}, \tag{18}$$

$$1-\kappa^2-\epsilon^2 = \frac{(3-2\epsilon^2)-(1-\epsilon^2)-(3\epsilon^2-2\epsilon^4)}{3-2\epsilon^2} = \frac{2(1-\epsilon^2)^2}{3-2\epsilon^2}, \tag{19}$$

and thus $\frac{\sqrt{1-\kappa^2-\epsilon^2}\sqrt{1-2\kappa^2}}{\sqrt{2}} = \kappa^2$. Therefore, V extends to a unitary operator on $\mathscr{H}_B \otimes \mathscr{H}_E$.

The final global state after Eve's attack is described in Table 5 (calculated by applying the operator V on Table 3), given the following definitions:

$$a \triangleq \sqrt{1-\kappa^2-\epsilon^2}+\frac{\sqrt{1-2\kappa^2}}{\sqrt{2}}, \tag{20}$$

$$b \triangleq \frac{\sqrt{1-2\kappa^2}}{\sqrt{2}}. \tag{21}$$

Table 5. The state of Bob+Eve after completing Eve's attack described in Section 4.2, depending on Alice's classical operation and on whether Alice detected a photon or not. The parameters a and b are defined in Equations (20) and (21).

Alice's Classical Operation	Did Alice Detect a Photon?	Bob+Eve State
CTRL	no (happens with certainty)	$\sqrt{\frac{2\epsilon^2}{3}}\left\|0,1\right\rangle_{\mathrm{x,B}}\left\|2\right\rangle_{\mathrm{E}}+\sqrt{1-\frac{2\epsilon^2}{3}}\left\|0,0\right\rangle_{\mathrm{B}}\left\|+\right\rangle_{\mathrm{E}}$
SWAP-10	no (happens with probability $\frac{2}{3}$)	$\frac{1}{\sqrt{2}}\left[\left\|0,1\right\rangle_{\mathrm{B}}\left(\epsilon\left\|2\right\rangle_{\mathrm{E}}+\kappa\left\|0\right\rangle_{\mathrm{E}}\right)+\left\|0,0\right\rangle_{\mathrm{B}}\left(a\left\|0\right\rangle_{\mathrm{E}}+b\left\|1\right\rangle_{\mathrm{E}}\right)\right]$
SWAP-10	yes (happens with probability $\frac{1}{3}$)	$\left\|0,0\right\rangle_{\mathrm{B}}\left\|2\right\rangle_{\mathrm{E}}$
SWAP-01	no (happens with probability $\frac{2}{3}$)	$\frac{1}{\sqrt{2}}\left[\left\|1,0\right\rangle_{\mathrm{B}}\left(\epsilon\left\|2\right\rangle_{\mathrm{E}}+\kappa\left\|1\right\rangle_{\mathrm{E}}\right)+\left\|0,0\right\rangle_{\mathrm{B}}\left(b\left\|0\right\rangle_{\mathrm{E}}+a\left\|1\right\rangle_{\mathrm{E}}\right)\right]$
SWAP-01	yes (happens with probability $\frac{1}{3}$)	$\left\|0,0\right\rangle_{\mathrm{B}}\left\|2\right\rangle_{\mathrm{E}}$

We notice that for $\epsilon=0$, the attack is the same as in Section 4.1. If $\epsilon=1$, the loss rate of CTRL bits is $\frac{1}{3}$, and Eve gets no information at all on the information bits (because $\kappa=0$).

In general, if Alice and Bob share a "secret" bit $b\in\{0,1\}$, Eve's probe state is in the (normalized) state

$$\frac{\epsilon\left|2\right\rangle_{\mathrm{E}}+\kappa\left|b\right\rangle_{\mathrm{E}}}{\sqrt{\epsilon^2+\kappa^2}}. \tag{22}$$

When Eve measures her probe state in the computational basis $\{\left|0\right\rangle_{\mathrm{E}},\left|1\right\rangle_{\mathrm{E}},\left|2\right\rangle_{\mathrm{E}}\}$, she gets the information bit b with probability

$$p=\frac{\kappa^2}{\epsilon^2+\kappa^2}=\frac{1-\epsilon^2}{1+2\epsilon^2-2\epsilon^4}, \tag{23}$$

and the loss rates of CTRL and SWAP-x bits (where $x\in\{01,10\}$) are

$$R_{\mathrm{CTRL}} = 1-\frac{2\epsilon^2}{3}, \tag{24}$$

$$R_{\mathrm{SWAP\text{-}x}} = 1-\frac{\epsilon^2+\kappa^2}{2}, \tag{25}$$

respectively.

Table 6 shows the probabilities p and the loss rates $R_{\mathrm{CTRL}}, R_{\mathrm{SWAP\text{-}x}}$ for various values of ϵ. For example, for $\epsilon=0.5$, Eve still gets the information bit with probability $p\approx 0.55$, Bob's loss rate for the CTRL bits is $R_{\mathrm{CTRL}}\approx 0.83$, and his loss rate for the SWAP-x bits is $R_{\mathrm{SWAP\text{-}x}}\approx 0.73$.

Table 6. The probability p of Eve obtaining an information bit, and the loss rates R_{CTRL} and $R_{\mathrm{SWAP\text{-}x}}$ of CTRL and SWAP-x bits (where $x\in\{01,10\}$), respectively, for several values of the attack's parameter ϵ.

ϵ	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
p	1	0.97	0.89	0.78	0.66	0.55	0.44	0.34	0.25	0.15	0
$\mathbf{R}_{\mathrm{CTRL}}$	1	0.99	0.97	0.94	0.89	0.83	0.76	0.67	0.57	0.46	0.33
$\mathbf{R}_{\mathrm{SWAP\text{-}x}}$	0.83	0.83	0.82	0.79	0.76	0.73	0.68	0.63	0.58	0.53	0.5

For all values of ϵ, the attack causes no errors. However, in principle, it can be detected because it causes different loss rates to different types of bits: the loss rate experienced by Bob in the CTRL bits, R_{CTRL}, is usually different from the loss rate in the SWAP-x bits, $R_{\mathrm{SWAP\text{-}x}}$ (see Table 6 for details). Therefore, in principle, the attack can be detected by a statistical test for most values of ϵ.

The loss rates become equal only for the value $\epsilon = \epsilon_0 \triangleq \sqrt{\frac{3-\sqrt{3}}{2}} \approx 0.796$ (which gives $\kappa^2 = \frac{\epsilon^2}{3}$). It seems that this specific attack *cannot* be detected, even in principle: it causes no errors, and it causes the same loss rate for all qubits. For this attack, Eve gets the information bit with probability $p = \frac{1}{4}$, and the loss rates are $R_{\mathrm{CTRL}} = R_{\mathrm{SWAP\text{-}x}} = \frac{1}{\sqrt{3}} \approx 0.577$. Therefore, this attack gives Eve a reasonable amount of information, and it is not detectable by looking at errors or comparing loss rates. (We can slightly modify the attack to make the loss rate the same in both directions of the quantum channel, too.)

We conclude that this weaker attack gives Eve partial information, causes no errors, and causes several loss rates. We also conclude that since the loss rates caused by the attack are usually different for different types of bits, the attack can be detected, in principle, for any value of ϵ except ϵ_0. However, for $\epsilon = \epsilon_0$, the attack seems undetectable.

5. Discussion

We have discussed a simpler and natural variant of the Mirror protocol (the "simplified Mirror protocol") which is easier to implement. We have found the simplified Mirror protocol to be completely non-robust; therefore, this protocol is actually an "over-simplified" Mirror protocol. We have presented in Section 4.1 an attack giving Eve full information without causing any error; in addition, since this attack also causes full loss of the CTRL bits, we have presented in Section 4.2 weaker attacks giving Eve partial information, causing no errors, and causing fewer losses. In particular, we have presented a specific attack (characterized by the parameter $\epsilon = \epsilon_0 \triangleq \sqrt{\frac{3-\sqrt{3}}{2}} \approx 0.796$) that seems undetectable and gives Eve one quarter ($\frac{1}{4}$) of all information bits.

Those attacks prove that the simplified Mirror protocol, which allows Alice to use only three classical operations (CTRL, SWAP-10, and SWAP-01), is completely non-robust. On the other hand, the Mirror protocol is proved completely robust (see Section 2 and [16]). As explained in Section 3, the only difference between the simplified Mirror protocol and the Mirror protocol is that the Mirror protocol allows a fourth classical operation, SWAP-ALL; therefore, allowing the SWAP-ALL operation is necessary for robustness. More generally, the Mirror protocol probably cannot be made much simpler while remaining robust: its complexity is crucial for robustness. Therefore, we have seen that if we want to use an SQKD protocol that is experimentally feasible in a secure way, we may have to use a relatively complicated protocol.

In this paper, we have not checked the experimental feasibility of Eve's attacks, because Eve is usually assumed to be all-powerful. Nonetheless, it can be interesting to check in the future the experimental feasibility of those attacks and discover whether the simplified Mirror protocol is flawed also in practice and not "only" in theory. Other interesting directions for future research include trying to find experimentally feasible SQKD protocols that are simpler than the Mirror protocol, and trying to find similar attacks against other QKD and SQKD protocols that have no complete robustness proof.

Author Contributions: T.M. suggested to investigate the robustness of the simplified protocol. M.B. suggested and designed the two attacks. All authors performed the careful analysis of the attacks, wrote the manuscript, and reviewed and commented on the final manuscript.

Funding: The work of Tal Mor and Rotem Liss was partly supported by the Israeli MOD Research and Technology Unit.

Acknowledgments: The authors thank Natan Tamari and Pavel Gurevich for useful discussions about the experimental implementation of SWAP-ALL.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum Key Distribution
SQKD	Semiquantum Key Distribution

References

1. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum Key Distribution with Classical Bob. *Phys. Rev. Lett.* **2007**, *99*, 140501. [CrossRef] [PubMed]
2. Boyer, M.; Gelles, R.; Kenigsberg, D.; Mor, T. Semiquantum key distribution. *Phys. Rev. A* **2009**, *79*, 032341. [CrossRef]
3. Zou, X.; Qiu, D.; Li, L.; Wu, L.; Li, L. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A* **2009**, *79*, 052312. [CrossRef]
4. Boyer, M.; Mor, T. Comment on "Semiquantum-key distribution using less than four quantum states". *Phys. Rev. A* **2011**, *83*, 046301. [CrossRef]
5. Lu, H.; Cai, Q.Y. Quantum key distribution with classical Alice. *Int. J. Quantum Inf.* **2008**, *06*, 1195–1202. [CrossRef]
6. Sun, Z.W.; Du, R.G.; Long, D.Y. Quantum key distribution with limited classical Bob. *Int. J. Quantum Inf.* **2013**, *11*, 1350005. [CrossRef]
7. Yu, K.F.; Yang, C.W.; Liao, C.H.; Hwang, T. Authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process.* **2014**, *13*, 1457–1465. [CrossRef]
8. Krawec, W.O. Mediated semiquantum key distribution. *Phys. Rev. A* **2015**, *91*, 032323. [CrossRef]
9. Zou, X.; Qiu, D.; Zhang, S.; Mateus, P. Semiquantum key distribution without invoking the classical party's measurement capability. *Quantum Inf. Process.* **2015**, *14*, 2981–2996. [CrossRef]
10. Krawec, W.O. Security proof of a semi-quantum key distribution protocol. In Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, China, 14–19 June 2015, pp. 686–690. [CrossRef]
11. Krawec, W.O. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Inf. Process.* **2016**, *15*, 2067–2090. [CrossRef]
12. Zhang, W.; Qiu, D.; Mateus, P. Security of a single-state semi-quantum key distribution protocol. *Quantum Inf. Process.* **2018**, *17*, 135. [CrossRef]
13. Krawec, W.O. Practical security of semi-quantum key distribution. In *Proceedings of SPIE, Quantum Information Science, Sensing, and Computation X*; Donkor, E., Ed.; SPIE: Washington, DC, USA, 2018; Volumme 10660, p. 1066009. [CrossRef]
14. Tan, Y.G.; Lu, H.; Cai, Q.Y. Comment on "Quantum Key Distribution with Classical Bob". *Phys. Rev. Lett.* **2009**, *102*, 098901. [CrossRef] [PubMed]
15. Boyer, M.; Kenigsberg, D.; Mor, T. Boyer, Kenigsberg, and Mor Reply. *Phys. Rev. Lett.* **2009**, *102*, 098902. [CrossRef]
16. Boyer, M.; Katz, M.; Liss, R.; Mor, T. Experimentally feasible protocol for semiquantum key distribution. *Phys. Rev. A* **2017**, *96*, 062335. [CrossRef]
17. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef] [PubMed]