Restricted Attacks on Semi-Quantum Key Distribution Protocols*

Walter O. Krawec
Stevens Institute of Technology
Hoboken NJ 07030, USA
walter.krawec@gmail.com

Abstract

In this paper, we investigate single state, semi-quantum key distribution protocols. These are protocols whereby one party is limited to measuring only in the computational basis, while the other, though capable of measuring in both computational and Hadamard bases, is limited to preparing and sending only a single, publicly known qubit state. Such protocols rely necessarily on a two-way quantum communication channel making their security analysis difficult. However we will show that, for single state protocols, we need only consider a restricted attack operation by Eve. We will also describe a new single state protocol which permits "reflections" to carry information and use our results concerning restricted attacks to show its robustness.

1 Introduction

It is by now well known that two parties, whom we shall refer to throughout as Alice (A) and Bob (B), may agree, via the use of a quantum communication channel, on a shared secret key which is secure against even an all powerful active adversary, customarily referred to as Eve (E). The security of such quantum key distribution (QKD) protocols is based not upon computational assumptions, as is the case, for instance, with classical public key cryptology, but instead on physical assumptions (Eve being bounded in power only by the laws of physics). Protocols such as BB84 [1], SARG04 [2], and others [3] have been analyzed extensively of late and exact proofs of their unconditional security have been constructed. These QKD protocols, and others like them, assume that both A and B are permitted to perform various quantum operations. For instance, in BB84, it is assumed that both parties may prepare and measure qubits in either the computational "Z" basis ($|0\rangle, |1\rangle$) or the Hadamard "X"

[*] The final publication is available at Springer via http://dx.doi.org/10.1007/s11128-014-0802-2

basis ($|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$). Though there have been of course many various alterations to the assumptions of Alice and Bob, it is still assumed that they both may perform such "quantum" operations.

Recently however [4, 5] it has been shown possible to construct QKD protocols where A is allowed to perform quantum operations (e.g., preparing and measuring in either the Z or X basis) however B is limited to perform "classical" operations (we will define Bob's permitted operations shortly). Such a protocol, which allows quantum A and this limited B to agree on a secret key is called a *semi-quantum key distribution* (SQKD) protocol.

SQKD protocols rely on a two-way quantum communication channel (one that allows a qubit to travel from Alice to Bob, then back again to Alice) and an authenticated classical public channel. Eve may perform any operation of her choice on the quantum channel (in both directions); however she may only listen to, but not tamper with, messages on the authenticated public classical channel.

Typically, A starts the communication by sending a qubit, prepared in either the Z or X basis to Bob. Bob then, who is "classical", may perform one of the following operations:

1. Measure the qubit in the Z basis and prepare a new qubit in the same Z basis.

2. Reflect the incoming qubit (learning nothing about it) back to Alice.

A qubit returns to Alice who may then measure in either the Z or X basis. After repeating this process N times, Alice and Bob attempt to "sift" two bit strings: $\texttt{info}_A$ and $\texttt{info}_B$ respectively. It is hoped that, after performing the protocol, their two strings are not only highly correlated, but that Eve has limited knowledge of them. They may then perform error correction and privacy amplification to distill a secure secret key for future cryptographic uses.

Due to B's ability to only work directly with the "0/1" Z basis, he is termed a "classical" Bob. From this point of view then, SQKD protocols are very interesting from a theoretical standpoint for they attempt to answer the question concerning exactly how "quantum" a protocol need be in order to provide the same benefits as their fully quantum counterparts (e.g., BB84). Whether or not B is truly classical though is a subject for debate (e.g., he still requires the ability to reflect or the ability to produce truly random choices); we prefer the term "semi-quantum", though we will use the two interchangeably throughout.

Notice that, unlike BB84 which uses a one-way quantum channel, Eve has two chances to interact with the traveling qubit: once when it is first sent from Alice to Bob, then again when it is returning from Bob to Alice. This greatly increases the complexity of the protocol's analysis. In parenthesis, there have been some two-way QKD (not using a restricted, classical Bob but instead a fully quantum B) protocols recently constructed, however, progress has only recently been made in proving their unconditional security [6, 7], though only by making various assumptions [7].

To prove the security of SQKD protocols, the concept of "robustness" was introduced in [4]. There it was defined that a SQKD protocol is *completely robust* if, whenever Eve learns non-zero information on one (or both) of the `info` strings, she induces a disturbance in the quantum channel (or a certain amount of noise) which, with non-zero probability, Alice or Bob may detect. Though we will not concern ourselves with it, they also defined the notion of *partially robust* whereby Eve may learn some limited information on one of the `info` strings without inducing any detectable error. In this paper however, we only are interested in completely robust protocols and, whenever we write "robust" we mean "completely".

Various other SQKD protocols have been proposed since these first; see for instance [8, 9, 10, 11]. In [9], a protocol utilizing entangled states was described. The protocol of [10] introduced the idea of B sending any qubit $|r\rangle$ where r may or may not be based on his measurement result (this was also used in [8]); as we will show, in the single-state case, this adds some extra complexity to the security analysis. In [11] a protocol was proposed which did not require the authenticated channel. The protocols of [8, 12] design robust key distribution protocols permitting a fully quantum A and several classical parties $B, C, \ldots$ to share a key.

Moving beyond key distribution, [13] introduced a three party secret sharing protocol permitting a fully quantum A to share a secret with two semi-quantum users B and C. Their protocol required A to produce GHZ states and was shown secure against eavesdropping and adversarial B or C (quantum A was, of course, trusted since she had the secret). Alternative protocols were proposed in [14, 15, 16]. Security in all these was based on the notion of robustness.

While the first SQKD protocols [4, 5] involved Alice sending, on each iteration, a qubit randomly prepared as either $|0\rangle, |1\rangle, |+\rangle$, or $|-\rangle$, it was recently shown in [17] (see also the comment [18]) that SQKD protocols exist even if Alice only prepares a single, publicly known state $|+\rangle$ each iteration. Such protocols are called *single state SQKD protocols*. Other single state protocols were developed in [8].

In this paper we will show that, for single state protocols, and assuming that Bob always resends the same state he measures (as is the case with most SQKD protocols), the most general attack of Eve, whereby she applies a unitary operator, interacting with her own private ancilla space, on both channels (using two different unitary operators U_E between Alice and Bob and U_F between Bob and Alice) is equivalent to a restricted attack whereby she prepares a single qubit state of her choice (however not entangled with her own ancilla) and applies only a single unitary operator U'_F on the return state (this operator interacts with her private ancilla). We will show that this result holds also for protocols whereby Alice sends one of two orthogonal states (chosen probabilistically each iteration) however it does not necessarily apply when Alice may send one of three or more states.

Note that, in [8], the authors described a single state SQKD protocol where B was able to prepare a qubit in the Z basis different from what he measured (as in [10]). They also claimed, without proof, that, due to this "refresh" of the qubit, E's attack on the first channel is not needed. In our paper, we prove rigorously that, for single state protocols where B is not allowed to "refresh" the qubit (i.e., unlike in [8], he must always send $|r\rangle$ if he measures $|r\rangle$), then the first attack by E is not entirely necessary (though E may still "bias" the superposition in the first channel). We also discuss the case when B is allowed to refresh the qubit.

Our security results apply to any single state protocol and our results may be useful when deriving equations computing the quantum information E may hold on the `info` string. For instance, in [19], the author computed an equation relating the disturbance caused by E's attack to the information E may gain in an individual attack (i.e., an attack where E performs the same operation each iteration and performs a measurement before A and B's key is used for anything - unlike a *collective attack* where the measurement is performed at any later time; see [3] for more information on the various attack models commonly used). Our results could be used to not only simplify their analysis (where they considered two attack operators); but also could be used to extend their work to the case of collective attacks and, perhaps, to understand the key rate of a protocol (see [3, 20]).

In this paper, we will apply our results to the security analysis of a new single state protocol we devise. This protocol, instead of using the measurement results to sift an `info` string, as is the case with all other SQKD protocols (not only single state) that we are aware of, uses Bob's actual operation to determine the bit string. Namely, if B chooses to reflect, this will constitute an `info` bit of 0; otherwise if B chooses to measure and resend this will correspond to a 1. Thus this protocol demonstrates for the first time, the possibility of using reflections and X basis qubits to carry information, even though classical Bob cannot work directly with such qubits. Prior SQKD protocols simply use the X basis to measure the noise of the channel.

We point out that the results in this paper concern only the perfect qubit scenario. We do not consider security involving actual implementation issues. For instance we do not consider the "photon tagging attack" mentioned in [21]. However, as mentioned in [22], theoretical security proofs in quantum cryptology and their practical implementation are often very different, with theoretical security proofs generally preceding practical ones. This paper focuses only on the former leaving the latter as interesting future work. We observe that there are many open questions in the theoretical, perfect qubit setting, such as computing the key rate in the asymptotic scenario [3], to which our results may be applied.

2 Limited Attack Strategies

Let us recall the general attack strategy used by an eavesdropper (Eve) with a semi-quantum key distribution protocol. Since these are two-way protocols (that is, a qubit travels first from Alice to Bob then from Bob to Alice), Eve has two opportunities to attack the quantum communication. Thus, when proving the security of previous semi-quantum protocols, it is assumed that Eve captures the qubit from Alice (who starts the communication), applies a unitary U_E entangling the qubit with her own personal quantum system, and then forwards a qubit to Bob. Bob then performs some operation on it (reflecting or measuring then resending) and returns the result. Eve captures this return qubit and applies a second unitary operator U_F acting not only on Bob's returned qubit, but also on Eve's system (the same system which interacted originally with Alice's qubit via U_E). In this section, we show this first attack operator is not necessary for single state protocols.

To help us analyze these protocols, let us expand the underlying quantum system slightly by providing ancilla spaces for both Alice and Bob. That is, the system over which a SQKD protocol operates is: $\mathcal{H} := \mathcal{H}_A \otimes \mathcal{H}_T \otimes \mathcal{H}_E \otimes \mathcal{H}_B$. Here, $\mathcal{H}_A$ and $\mathcal{H}_B$ are Alice and Bob's private quantum registers and may be spanned by such states as $\left|0\right\rangle, \left|1\right\rangle$ or, in Bob's case, additionally $\left|\texttt{measure}\right\rangle, \left|\texttt{reflect}\right\rangle$. These states serve to model the "bookkeeping" that Alice and Bob must perform (e.g., Bob must remember whether he measured or reflected on any particular iteration). While Bob is semi-quantum and Alice does not wish to use a quantum memory, the use of these registers is equivalent to Alice and Bob storing their decisions and measurement outcomes in classical memory. It is simply, for our purposes, a convenient notational system.

$\mathcal{H}_T$ is the transit or travel space and is two dimensional (a qubit). At the start of each iteration, Alice holds $\mathcal{H}_T$ and prepares a new qubit in this space. It is then "passed" to Eve who may perform an attack of her choice. Bob is then given this space and performs one of the permitted "classical" operations (reflect or measure and resend) at which point it is passed back to Eve who, after performing a second attack, returns it to Alice who may then make a measurement.

Finally, $\mathcal{H}_E$ is Eve's personal ancilla space.

To analyze Bob's operations, let ρ be a density operator on $\mathcal{H}$ and denote by $\mathcal{B}_R(\rho)$ the operation whereby Bob reflects the qubit while recording his choice in his private quantum register. Denote by $\mathcal{B}_M(\rho)$ the result of Bob measuring in the computational basis, recording the result, and resending. Thus:

$$\begin{aligned}
\mathcal{B}_R(\rho) &= \rho \otimes \left|\texttt{reflect}\right\rangle \left\langle\texttt{reflect}\right|_B \\
\\
\mathcal{B}_M(\rho) &= M_{\left|0\right\rangle}\rho M_{\left|0\right\rangle} \otimes \left|\texttt{measure}, 0\right\rangle \left\langle\texttt{measure}, 0\right|_B \\
&+ M_{\left|1\right\rangle}\rho M_{\left|1\right\rangle} \otimes \left|\texttt{measure}, 1\right\rangle \left\langle\texttt{measure}, 1\right|_B ,
\end{aligned}$$

where $M_{\left|i\right\rangle}$ is Bob's measurement operator, projecting that transit space $\mathcal{H}_T$ to $\left|i\right\rangle$. That is to say, $M_{\left|i\right\rangle} := I_A \otimes \left|i\right\rangle \left\langle i\right|_T \otimes I_E \otimes I_B$ where I_A is the identity operator on $\mathcal{H}_A$ etc.

In the following, we will make a distinction between what we call *general collective attacks* and *restricted collective attacks*. In both cases, we assume that Eve uses a separate ancilla for each iteration and that she uses the same attack operators each iteration. That is to say, each iteration of the protocol acts on a separate copy of the system $\mathcal{H}$. The general collective attack is a

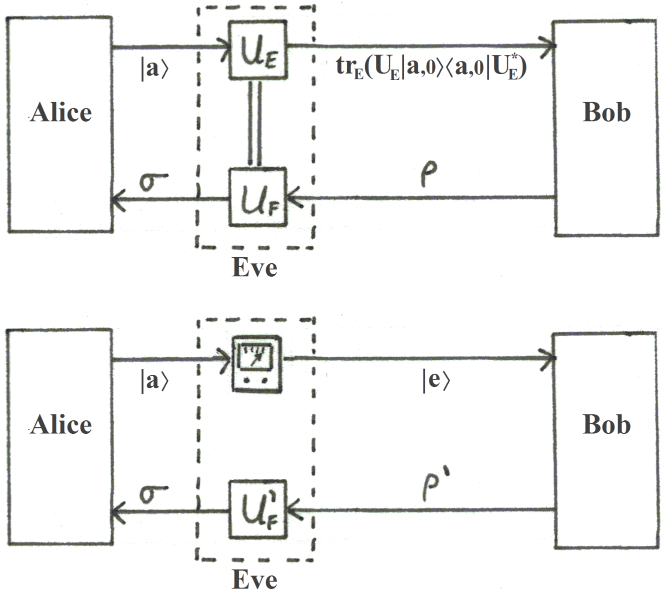

Figure 1: The top figure is the general collective attack scenario whereby Eve entangles Alice's sent qubit $|a\rangle$ with her own private ancilla (via the application of U_E) before forwarding to Bob. Afterwards, she applies U_F which interacts with the return qubit and again with her private ancilla. On the bottom is the restricted collective attack whereby Eve, depending perhaps on a measurement, prepares a new qubit (not entangled with her ancilla) and only applies a single attack operator U_F' on the return qubit. Both scenarios, under certain conditions, are equivalent.

strategy whereby Eve applies a unitary operator U_E to the qubit traveling from Alice to Bob; this operator acts on $\mathcal{H}_T \otimes \mathcal{H}_E$. U_F is a unitary operator, also acting on the joint space $\mathcal{H}_T \otimes \mathcal{H}_E$, applied by Eve on the returning qubit (from Bob to Alice).

The *restricted collective attack* however consists only of a single unitary operator U_F' and a pair of non-negative real numbers α, β such that $\alpha^2 + \beta^2 = 1$. For this attack, Eve will send the qubit $\alpha |0\rangle + \beta |1\rangle$ (observe it is not entangled with her own ancilla) to Bob. When B returns a qubit, she will then apply the operator U_F', acting on $\mathcal{H}_T \otimes \mathcal{H}_E$ and return a qubit to A.

See Fig. 1 for a pictorial representation of the two attack scenarios.

In both cases, we assume Eve may postpone measurement of her ancilla to any future time. For instance, she might wish to wait for a cipher text to travel between A and B before choosing an optimal measurement of her ancilla [3].

Lemma 2.1. If Bob is restricted to operations $\mathcal{B}_R$ and $\mathcal{B}_M$ (chosen probabilistically by Bob) and if Alice is restricted to sending either a single qubit state

$|a\rangle$ or randomly choosing from two orthogonal states $\{|a\rangle, |b\rangle\}$ (all of which is publicly known), and assuming that Eve's ancilla state is known to her (that is, it is in some state $|\chi\rangle_E$ which Eve can determine with probability one), then for every general collective attack, consisting of two unitary operators U_E applied between Alice and Bob and U_F applied between Bob and Alice there is an equivalent restricted attack whereby Eve sends a single qubit $\alpha|0\rangle + \beta|1\rangle$ and only applies a single unitary operator U'_F on the returning qubit state. Furthermore α and β are real and non-negative.

Proof. First assume that Alice only sends a single, publicly known state $|a\rangle$. Then, after interacting with Eve's first probe U_E, the state is of the form $|e\rangle = |0, e_0\rangle + |1, e_1\rangle$ where $|e_0\rangle$ and $|e_1\rangle$ are vectors (not necessarily normalized or orthogonal) in $\mathcal{H}_E$ such that $\langle e_0|e_0\rangle + \langle e_1|e_1\rangle = 1$. Eve sends to Bob the state $tr_E(|e\rangle\langle e|)$.

Bob will then, with probability p_R perform operation $\mathcal{B}_R$; otherwise with probability $p_M = 1 - p_R$, he will perform operation $\mathcal{B}_M$. After B returns the qubit to E, we find that the state of the system to be:

$$\begin{aligned}
\rho &= p_R\,|e\rangle\langle e| \otimes \sigma_B^{(R)} \\
&\quad + p_M\left(M_{|0\rangle}\,|e\rangle\langle e|\,M_{|0\rangle} \otimes \sigma_B^{(M,0)} + M_{|1\rangle}\,|e\rangle\langle e|\,M_{|1\rangle} \otimes \sigma_B^{(M,1)}\right)
\end{aligned}$$

$$\begin{aligned}
&= p_R\left(|0,e_0\rangle\langle 0,e_0| + |1,e_1\rangle\langle 1,e_1| + |0,e_0\rangle\langle 1,e_1| + |1,e_1\rangle\langle 0,e_0|\right) \otimes \sigma_B^{(R)} \\
&\quad + p_M\left(|0,e_0\rangle\langle 0,e_0| \otimes \sigma_B^{(M,0)} + |1,e_0\rangle\langle 1,e_1| \otimes \sigma_B^{(M,1)}\right),
\end{aligned}$$

where $M_{|i\rangle}$ is defined as before, $\sigma_B^{(R)}$ is the state of Bob's system $\mathcal{H}_B$ in the event he reflected, and $\sigma_B^{(M,j)}$ is the state of Bob's system in the event he measured and resent with outcome $|j\rangle$ (these σ_B's are all of unit trace).

Now assume that, instead of sending $tr_E(|e\rangle\langle e|)$ to Bob (where $|e\rangle = U_E|a\rangle$), Eve instead sends the state: $|e'\rangle = \alpha|0\rangle + \beta|1\rangle$ where $\alpha := \sqrt{\langle e_0|e_0\rangle}$ and $\beta := \sqrt{\langle e_1|e_1\rangle}$ (these are the same $|e_0\rangle, |e_1\rangle$ as before which Eve has complete information on). Note that, since $\langle x|x\rangle \in \mathbb{R}$ for any state $|x\rangle$, and in fact $\langle x|x\rangle \geq 0$, both α and β are real and non-negative as claimed. Bob applies the same process as described above resulting in the system being in the state:

$$\begin{aligned}
\rho^{\text{restricted}} &= p_R\,|e'\rangle\langle e'| \otimes \sigma_B^{(R)} \\
&\quad + p_M\left(M_{|0\rangle}\,|e'\rangle\langle e'|\,M_{|0\rangle} \otimes \sigma_B^{(M,0)} + M_{|1\rangle}\,|e'\rangle\langle e'|\,M_{|1\rangle} \otimes \sigma_B^{(M,1)}\right)
\end{aligned}$$

$$\begin{aligned}
&= p_R\left(\alpha^2|0\rangle\langle 0| + \beta^2|1\rangle\langle 1| + \alpha\beta|0\rangle\langle 1| + \beta\alpha|1\rangle\langle 0|\right) \otimes \sigma_B^{(R)} \\
&\quad + p_M\left(\alpha^2|0\rangle\langle 0| \otimes \sigma_B^{(M,0)} + \beta^2|1\rangle\langle 1| \otimes \sigma_B^{(M,1)}\right).
\end{aligned}$$

We will now construct a unitary operator V, acting only on $\mathcal{H}_T \otimes \mathcal{H}_E$, such that $V\rho^{\text{restricted}}V^* = \rho$. Note that we assume, without loss of generality, that E's system is cleared to some zero state $|0\rangle \in \mathcal{H}_E$.

Case 1: Assume that $\alpha = \sqrt{\langle e_0|e_0\rangle}$ and $\beta = \sqrt{\langle e_1|e_1\rangle}$ are both non-zero. Define V to be the unitary operator such that: $V|i,0\rangle = |i,e_i\rangle / \sqrt{\langle e_i|e_i\rangle}$. Since Eve is fully aware of how her probe U_E operates, she has full information on the state $|e_i\rangle$ and thus, may construct such a unitary V - note that it is only relevant how V operates when Eve's ancilla is in the state $|0\rangle$ and thus V may act arbitrarily for other initial states of $\mathcal{H}_E$.

Then we have:

$$\begin{aligned}
V\rho^{\text{restricted}}V^* &= p_R(\frac{\alpha^2}{\alpha^2}|0,e_0\rangle\langle 0,e_0| + \frac{\beta^2}{\beta^2}|1,e_1\rangle\langle 1,e_1| \\
&+ \frac{\alpha\beta}{\alpha\beta}|0,e_0\rangle\langle 1,e_1| + \frac{\beta\alpha}{\beta\alpha}|1,e_1\rangle\langle 0,e_0|) \otimes \sigma_B^{(R)} \\
&+ p_M(\frac{\alpha^2}{\alpha^2}|0,e_0\rangle\langle 0,e_0| \otimes \sigma_B^{(M,0)} + \frac{\beta^2}{\beta^2}|1,e_1\rangle\langle 1,e_1| \otimes \sigma_B^{(M,1)}) \\
&= \rho.
\end{aligned}$$

Note that in the above we abused notation slightly: we actually applied the operator $V \otimes I_B$ where I_B is the identity operator acting on B's space $\mathcal{H}_B$.

Case 2: One of α or β is zero. This is similar to case 1, however now either $|0,e_0\rangle \equiv 0$ or $|1,e_1\rangle \equiv 0$ (depending on which of α or β is zero). Thus, we may follow the same process as above however we need not worry about how V acts on the state $|0,0\rangle$ if $\alpha = 0$ or $|1,0\rangle$ if $\beta = 0$.

Of course α and β cannot both be zero simultaneously and thus we are finished with the single state case. If Alice chooses between two orthogonal states $|a\rangle$ or $|b\rangle$, both of which are publicly known, Eve may first perform a measurement to determine which of the two were sent. Based on this measurement, she may proceed as above in the single state case (her operator U_E may act differently on either $|a\rangle$ or $|b\rangle$ however since she knows, deterministically which state was sent, she may construct the operator V appropriately).

Therefore, any attack that can be performed before forwarding the qubit to Bob, can be done afterwards (except, perhaps, for "skewing" the superposition). By setting $U'_F = U_F \cdot V$, the proof is complete. □

In the above, we took the meaning "equivalent" to imply that there was no difference in the final quantum state of the protocol when either the general attack (U_E, U_F) was used or the restricted attack was used (up to, perhaps, an irrelevant global phase change). Obviously the actual operations E performs are not equivalent. It is, however, easier to consider the restricted attack when considering the security of a protocol; the above lemma shows we may do so without any loss of generality.

As an example of how the two attacks might be different (in terms of actions performed by E, not in terms of the final quantum state), consider a single-state protocol where A always sends $\left|a\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{i}{\sqrt{2}}\left|1\right\rangle$ (now there are complex probability amplitudes) and where E's general attack on the first channel is to ignore the qubit (i.e., $U_E = I$, the identity operator); U_F is arbitrary. Consider now the "equivalent" restricted attack. We may write $U_E\left|a\right\rangle = I\left|a\right\rangle$ as $\left|0, e_0\right\rangle + \left|1, e_1\right\rangle$ where $\left|e_0\right\rangle = \frac{1}{\sqrt{2}}\left|\chi\right\rangle$ and $\left|e_1\right\rangle = \frac{i}{\sqrt{2}}\left|\chi\right\rangle$ where $\left|\chi\right\rangle \in \mathcal{H}_E$ and $\left\langle\chi|\chi\right\rangle = 1$. The restricted attack would be for E to send the (different) qubit $\left|e'\right\rangle = \sqrt{\left\langle e_0|e_0\right\rangle}\left|0\right\rangle + \sqrt{\left\langle e_1|e_1\right\rangle}\left|1\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle$. Thus, when faced with this particular general attack, B receives a qubit with a complex probability amplitude; for the restricted attack he receives $\left|+\right\rangle$ (the reader may check that B would also receive $\left|+\right\rangle$ if A sent $\left|-\right\rangle$). However, since B can only measure in the Z basis, this change does not affect anything on his end of the protocol.

When B is finished, he returns a qubit; in this case either $\left|+\right\rangle$ or $\left|j\right\rangle$ for $j \in \{0, 1\}$ depending on whether he reflected or measured and resent respectively. The restricted attack now calls for E to apply V so that $\left|0, 0\right\rangle$ is sent to $\left|0, e_0\right\rangle / \sqrt{\left\langle e_0|e_0\right\rangle} = \left|0, \chi\right\rangle$ and, similarly, $\left|1, 0\right\rangle$ maps to $i\left|1, \chi\right\rangle$. Thus we see that, if B reflected, V will restore $\left|+\right\rangle$ to the original $\left|a\right\rangle$ (which is the state B would have sent had the general attack been used and he reflected); if B measured and sent $\left|0\right\rangle$ nothing is changed (besides, perhaps, adjusting E's ancilla to $\left|\chi\right\rangle$ as called for by the general U_E); if B measured and sent $\left|1\right\rangle$ the phase is changed to $i\left|1\right\rangle$, however global phase changes do not matter. Thus, while the operations performed by E are very different, at the end of the protocol, there is absolutely no difference between the two in terms of the final resulting quantum state, and so no advantage may be gained by E.

We observe that, in the case of single-state protocols, there is an alternative way to write Lemma 2.1. It is:

- Assuming the same conditions as in the lemma (except now A sends only a single state $\left|a\right\rangle$ each iteration), for every general attack (U_E, U_F) there is an equivalent restricted attack (b, U'_F) where $b \in [-1/2, 1/2]$ and U'_F is an operator acting on $\mathcal{H}_T \otimes \mathcal{H}_E$. For this attack E sends the state:

  $$\sqrt{\frac{1}{2} + b}\left|0\right\rangle + \sqrt{\frac{1}{2} - b}\left|1\right\rangle,$$

  and applies U'_E on the returning qubit. Note that b depends on U_E while U'_F depends on both U_E and U_F.

This is clearly equivalent to the original lemma: note that E sends the state $\left|e\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ for real, non-negative α, β. Since $\alpha^2 \in [0, 1]$, we may write it as $\alpha^2 = 1/2 + b$ for some $b \in [-1/2, 1/2]$ which forces $\beta^2 = 1 - \alpha^2 = 1/2 - b$. Since both α and β are non-negative, the claim follows.

To simplify things, when we later analyze the security of a protocol, we simply consider Eve's attack as first biasing the superposition, then applying an arbitrary U'_F operator. That is to say, there is no need to consider V's construction as it is "absorbed" into the arbitrary U'_F.

It is interesting to consider exactly how "tight" our above result is. First, let us consider what happens if Alice chooses to send from a collection of non-orthogonal states (e.g., the three or four state protocols of [4, 5, 17]); in this case there exist arbitrary general attacks for which no equivalent restricted attack exists (there are, of course, general attacks for which restricted attacks exist - take, for instance, the trivial attack where $U_E = U_F = I$, the identity operator). Again, by "equivalent" we mean that the final resulting quantum states are identical (up to a global phase change). This should come as no surprise: in [23] an attack was described against the original SQKD protocol of [4] (a protocol which dictated that A should prepare one of the four Z or X states randomly each iteration - i.e., it is not a single state protocol), involving both directions of the qubit, which leaked more information to E than a single channel attack could with the same level of disturbance.

However, in this case, we must be careful how we define the restricted attack; it may no longer make sense that E will prepare her own state disregarding the one sent from A. Instead, we will simply say it is an attack whereby E sends a qubit, unentangled with her own ancilla $\mathcal{H}_E$, to B. This may be achieved in a variety of manners: perhaps by E preparing her own fresh qubit; or perhaps E applies a unitary U'_E to the qubit sent from A to B, acting only on $\mathcal{H}_T$. We will assume the state sent by her is pure and not mixed.

Of course, the process she uses must be the same each iteration (it is a collective attack). So if she prepares a fresh qubit each time, it must be the same qubit each iteration - this is in contrast to the two-orthogonal case in Lemma 2.1 where we allow E to make a measurement and adjust her preparation and V operator based on this result; however allowing this doesn't make as much sense in the multi-state case where a measurement would be potentially destructive. Alternatively, if she uses U'_E, it must be the same U'_E each iteration. Both of these scenarios have their problems and there might be a "stronger" version of the restricted attack which allows us to claim something similar to Lemma 2.1; analyzing this further could be interesting future work.

Once again, assume Bob is restricted to operations $\mathcal{B}_R$ and $\mathcal{B}_M$ and that, on iteration t of the protocol (that is, the t'th qubit sent from Alice), Alice sends the state $|a_t\rangle$, chosen from a set of states $\mathcal{S}$ which we assume contains at least two non-orthogonal states (e.g., $\mathcal{S} = \{|0\rangle, |1\rangle, |+\rangle\}$). Let $|a_t\rangle = \alpha_t |0\rangle + \beta_t |1\rangle$, where α_t and β_t are unknown to Eve. Consider the result of Eve's general collective attack (U_E, U_F) where U_E acts on Alice's qubit and Eve's ancilla (prepared in the state $|\chi\rangle$) as follows:

$$\begin{aligned} U_E |0, \chi\rangle &= |0, e_0\rangle + |1, e_1\rangle \\ U_E |1, \chi\rangle &= |0, e_2\rangle + |1, e_3\rangle \end{aligned}$$

Such that:

$$\begin{aligned} \langle e_0|e_0\rangle + \langle e_1|e_1\rangle = \langle e_2|e_2\rangle + \langle e_3|e_3\rangle = 1 \\ \langle e_2|e_0\rangle + \langle e_3|e_1\rangle = \langle e_0|e_2\rangle + \langle e_1|e_3\rangle = 0 \end{aligned}$$

Since our claim is that not every general attack is equivalent to a restricted attack, we may consider an attack of our own choosing. Therefore, let us assume that $\langle e_j|e_j\rangle > 0$ for all j, and $\langle e_j|e_k\rangle = 0$ for all $j \neq k$.

By linearity, we have $U_E\,|a_t\rangle = \alpha_t(|0, e_0\rangle + |1, e_1\rangle) + \beta_t(|0, e_2\rangle + |1, e_3\rangle) = |0, \tilde{e}_0^t\rangle + |1, \tilde{e}_1^t\rangle$ where $|\tilde{e}_0^t\rangle = \alpha_t\,|e_0\rangle + \beta_t\,|e_2\rangle$ and $|\tilde{e}_1^t\rangle = \alpha_t\,|e_1\rangle + \beta_t\,|e_3\rangle$.

After Bob's operation, the state, when E receives a qubit, is:

$$\begin{aligned}\rho &= p_R U_E\,|a_t,\chi\rangle\,\langle a_t,\chi|\,U_E^* \otimes \sigma_B^{(R)} \\ &\quad + p_M\left(|0,\tilde{e}_0^t\rangle\,\langle 0,\tilde{e}_0^t| \otimes \sigma_B^{(M,0)} + |1,\tilde{e}_1^t\rangle\,\langle 1,\tilde{e}_1^t| \otimes \sigma_B^{(M,1)}\right).\end{aligned}$$

If, however, Eve attempts to use a restricted collective attack, she will send the state $|E_t\rangle := x_t\,|0\rangle + y_t\,|1\rangle$ for some $x_t, y_t \in \mathbb{C}$ with $|x_t|^2 + |y_t|^2 = 1$. This state may be something she prepared fresh, or it may be the result of the product $U_E'\,|a_t\rangle$ where U_E' is an operator acting only on $\mathcal{H}_T$ (thus it may also be the same state A sent if $U_E' = I$ - e.g., $x_t = \alpha_t$, $y_t = \beta_t$ - in the case E simply "ignores" the first quantum channel). She then receives, after Bob's operation, the state:

$$\begin{aligned}\rho^{restricted} &= p_R\,|E_t\rangle\,\langle E_t| \otimes \sigma_B^{(R)} \\ &\quad + p_M\left(|x_t|^2\,|0\rangle\,\langle 0| \otimes \sigma_B^{(M,0)} + |y_t|^2\,|1\rangle\,\langle 1| \otimes \sigma_B^{(M,1)}\right).\end{aligned}$$

Note that, from this, it is clear that the state sent by E must satisfy $|x_t|^2 = \langle\tilde{e}_0^t|\tilde{e}_0^t\rangle$ and $|y_t|^2 = \langle\tilde{e}_1^t|\tilde{e}_1^t\rangle$. If this is not the case, the restricted attack is not necessarily equivalent to the general collective attack (B's measurement will produce outcomes with different probabilities - whether or not this is something advantageous to E is irrelevant as we are only considering when the attacks produce equivalent final quantum states). By our assumptions on the states $|e_j\rangle$, this implies both $|x_t|^2$ and $|y_t|^2$ must be non-zero.

Eve now wishes to apply a unitary V, acting on $\mathcal{H}_T \otimes \mathcal{H}_E$, such that $V\rho^{restricted}V^* = \rho$. However, just looking at the case when B measures and receives outcome 0, which happens with non-zero probability by our assumptions on $|e_j\rangle$, in order to do so, she requires $V\,|0,\chi\rangle = e^{i\theta_0^t}\,|0,\tilde{e}_0^t\rangle\,/|x_t|$ (assuming here that E's ancilla is cleared to the state $|\chi\rangle \in \mathcal{H}_E$). The state $|\tilde{e}_0^t\rangle$ (and also $|\tilde{e}_1^t\rangle$) are functions not only of $|e_j\rangle$ (which depend only on E's first attack operator U_E), but also α_i and β_i - two values which, unlike the single state and two-orthogonal state protocols considered in Lemma 2.1, cannot, with probability one, be determined by E. As a consequence of this, E cannot, with absolute certainty, construct the necessary operation V.

For instance, on iteration $t = 0$, from the arguments above, it is forced that $V\,|0,\chi\rangle = e^{i\theta_0^0}\,|0,\tilde{e}_0^0\rangle\,/|x_0|$. On iteration $t = 1$, again, it is required that $V\,|0,\chi\rangle = e^{i\theta_0^1}\,|0,\tilde{e}_0^1\rangle\,/|x_1|$ (by our assumptions on $|e_i\rangle$, neither $|x_0|$ nor $|x_1|$ are zero). Now we have:

$$\begin{aligned}
&V\,|0,\chi\rangle = V\,|0,\chi\rangle \\
\iff &\frac{e^{i\theta_0^0}}{|x_0|}(\alpha_0\,|e_0\rangle + \beta_0\,|e_2\rangle) = \frac{e^{i\theta_0^1}}{|x_1|}(\alpha_1\,|e_0\rangle + \beta_1\,|e_2\rangle) \\
\iff &\left(\alpha_0 - \frac{|x_0|}{|x_1|}e^{i(\theta_0^1-\theta_0^1)}\alpha_1\right)|e_0\rangle = \left(\frac{|x_0|}{|x_1|}\beta_1 e^{i(\theta_0^1-\theta_0^0)} - \beta_0\right)|e_2\rangle
\end{aligned}$$

Since $\langle e_0|e_2\rangle = \langle e_2|e_0\rangle = 0$, and $\langle e_j|e_j\rangle > 0$, by our assumptions, this forces $\alpha_0 = xe^{i\theta}\alpha_1$ and $\beta_0 = xe^{i\theta}\beta_1$, where $\theta = \theta_0^1 - \theta_0^0$ and $x = |x_0|/|x_1|$. This of course implies that $|a_0\rangle$ must be equal to $xe^{i\theta}\,|a_1\rangle$. First, this forces $x = 1$ and, so, $|x_0| = |x_1|$; secondly, in the event of this equality, the state sent on the second iteration is forced to be the same state sent on the first up to a global phase change. This argument may be repeated for subsequent iterations.

Just to illustrate, let $\alpha_0 = 1$ (in case A sent $|0\rangle$). Then V must send $|0,\chi\rangle$ to $c\,|0,e_0\rangle$ (for some non-zero scalar $c \in \mathbb{C}$). If $\alpha_1 = 0$ (so $\beta_1 = 1$), then V must send $|0,\chi\rangle$ to $c'\,|0,e_2\rangle$ (again $c' \neq 0$). Since we assumed $\langle e_0|e_0\rangle, \langle e_2|e_2\rangle > 0$ and $\langle e_0|e_2\rangle = 0$ this cannot be done.

Thus, in this scenario of multi-state protocols, the restricted collective attack is not *necessarily* equivalent to the general collective attack (there may be some attacks which are equivalent of course - perhaps a large enough family of "useful" attacks are contained here - this may be interesting future work). Whether this difference is of any use to the adversary depends on the protocol and the general attack (U_E, U_F).

Returning to single-state and two-orthogonal state protocols, the SQKD protocols of [10] allow Bob to measure in the Z basis and then prepare a new qubit which may or may not depend on the measurement result. For instance, if Bob measures $|0\rangle$, he may send $|1\rangle$. In this case the restricted attack is also not necessarily equivalent to the general one.

Indeed, assume Alice is restricted to sending either a single state $|a\rangle$ or choosing, probabilistically, to prepare and send one of two orthogonal states $|a\rangle$ or $|b\rangle$. Furthermore, assume there is a non-zero probability that Bob may send $|1-r\rangle$ after measuring $|r\rangle$ (for $r \in \{0,1\}$). In the general collective attack, Eve sends to Bob the state $tr_E(|e\rangle\langle e|)$ where $|e\rangle := |0,e_0\rangle + |1,e_1\rangle$. For the restricted attack she sends only $\alpha\,|0\rangle + \beta\,|1\rangle$; as before let us assume that $\langle e_j|e_j\rangle > 0$. Observe that, after Bob has performed his encoding operation, in order to construct an operator V mapping the restricted state to the general state, it must be that V maps the state $|0\rangle \to e^{i\theta_0}\,|0,e_0\rangle/\sqrt{\langle e_0|e_0\rangle}$ (in case Bob reflected or measured and resent) and $|0\rangle \to e^{i\theta_1}\,|0,e_1\rangle/\sqrt{\langle e_1|e_1\rangle}$ (in case Bob measured 1 and prepared 0). But this forces:

$$|e_0\rangle = \left(\frac{\sqrt{\langle e_0|e_0\rangle}}{\sqrt{\langle e_1|e_1\rangle}}\right)e^{i(\theta_1-\theta_0)}\,|e_1\rangle\,,$$

which is not necessarily true for every U_E (for instance, if $\langle e_0|e_1\rangle = 0$).

Depending on the actual attack E employed, there may be an equivalent restricted version; however this is not guaranteed for any (U_E, U_F). Whether or not E can use this to gain an advantage is subject to the actual protocol and specific general attack.

The following lemma is helpful when proving robustness of a single state (or two-orthogonal state) SQKD protocol. Essentially it states that, if Eve wishes to avoid detection, she must send the same state that Alice sent. That is, she cannot attempt to bias the state slightly and then "fix" it on the return path. Thus, when proving robustness, one may simply ignore the initial channel completely and concentrate on Eve's return attack.

Lemma 2.2. Let $\{|a\rangle, |b\rangle\}$ be an orthonormal basis of $\mathcal{H}_T$. Assume that, on any iteration, Alice sends either $|a\rangle$ or $|b\rangle$, and that there is a non-zero chance that Bob will reflect, and Alice will measure in the $\{|a\rangle, |b\rangle\}$ basis to verify the security of the channel or that Bob will measure and resend and that Alice will measure in the Z basis for the same security purpose. Then, assuming Eve is limited to collective attacks:

1. In order to avoid detection, if Alice prepares and sends the state $|a\rangle$, Eve must send the state $|e\rangle = \alpha|0\rangle + \beta|1\rangle$ such that $|\alpha|^2 = |\langle 0|a\rangle|^2, |\beta|^2 = |\langle 1|a\rangle|^2$, (similarly for the case that A sent $|b\rangle$).

2. If E wishes to avoid detection, and if A prepares and sends the state $|a\rangle$, there is no advantage to E by sending any other state (i.e., she should send $|e\rangle = |a\rangle$) - similarly for $|b\rangle$.

Proof. Eve may perform a measurement in the $\{|a\rangle, |b\rangle\}$ basis to determine which state was sent by Alice (unnecessary in the single-state case). Assume, on iteration i, A sends $|a\rangle = \gamma|0\rangle + \delta|1\rangle$ for $\gamma, \delta \in \mathbb{C}$. Since Lemma 2.1 applies, Eve will then send to Bob the state $|e\rangle = \alpha|0\rangle + \beta|1\rangle$ for $\alpha, \beta \in \mathbb{C}$ (we provide her extra power here allowing her to chose probability amplitudes that are complex even though our previous lemma showed they might as well be real - we do this in case γ or δ are complex allowing part (2) of this lemma to follow naturally).

Bob will either measure and resend or reflect. Either way he will return a qubit to Eve who will then apply her unitary probe U_F acting on $\mathcal{H}_T \otimes \mathcal{H}_E$. Since we are assuming a collective attack, we may assume, without loss of generality, that Eve's ancilla space is cleared to $|0\rangle_E$. The most general attack U_F acts as follows:

$$U_F|0,0\rangle = |U_0\rangle := |0,e_0\rangle + |1,e_1\rangle$$
$$U_F|1,0\rangle = |U_1\rangle := |0,e_2\rangle + |1,e_3\rangle$$

Where $|e_i\rangle$ are states in Eve's ancilla satisfying:

$$\langle e_0|e_0\rangle + \langle e_1|e_1\rangle = \langle e_2|e_2\rangle + \langle e_3|e_3\rangle = 1$$
$$\langle e_2|e_0\rangle + \langle e_3|e_1\rangle = \langle e_0|e_2\rangle + \langle e_1|e_3\rangle = 0$$

Thus, after Bob has reflected and Eve has applied U_F, the state of the system is:

$$\begin{array}{rcl}\rho^{\text{reflect}} & = & U_F \left|e\right\rangle \left\langle e\right| U_F^* = |\alpha|^2 \left|U_0\right\rangle \left\langle U_0\right| + |\beta|^2 \left|U_1\right\rangle \left\langle U_1\right| \\ & + & \alpha\beta^* \left|U_0\right\rangle \left\langle U_1\right| + \alpha^*\beta \left|U_1\right\rangle \left\langle U_0\right|, \end{array} \tag{1}$$

where α^*, β^* represents complex conjugation (or conjugate transpose in the case of U_F^*).

If Bob had measured and resent, the system would be in the state:

$$\rho^{\text{measure}} = |\alpha|^2 \left|U_0\right\rangle \left\langle U_0\right| + |\beta|^2 \left|U_1\right\rangle \left\langle U_1\right|.$$

Observe that, if B had measured and resent, in order to avoid detection, it must be the case that $\left|e_1\right\rangle = \left|e_2\right\rangle \equiv 0$ (else, there is a possibility that Alice, measuring in the Z basis, would get a different result from Bob's measurement). This simplifies the states such that $\left|U_0\right\rangle := \left|0, e_0\right\rangle$, $\left|U_1\right\rangle := \left|1, e_3\right\rangle$ and $\left\langle e_0|e_0\right\rangle = \left\langle e_3|e_3\right\rangle = 1$.

We next consider the case that Bob reflects and Alice measures in the $\{\left|a\right\rangle, \left|b\right\rangle\}$ basis. Denote by p_a the probability that, if Alice decides to measure in this basis, she receives outcome $\left|a\right\rangle = \gamma\left|0\right\rangle + \delta\left|1\right\rangle$. To avoid detection, Eve must try to construct U_F so that $p_a = 1$. From Equation 1, we can compute this probability as follows:

$$p_a = |\alpha\gamma|^2 \left\langle e_0|e_0\right\rangle + |\beta\delta|^2 \left\langle e_3|e_3\right\rangle + \alpha\beta^*\gamma\delta^* \left\langle e_0|e_3\right\rangle + \alpha^*\beta\gamma^*\delta \left\langle e_3|e_0\right\rangle,$$

Let $\gamma = \sqrt{p}e^{i\theta_a}, \delta = \sqrt{1-p}e^{i\theta_b}$, and $\left\langle e_0|e_3\right\rangle = re^{i\theta_e}$ ($r \in [0,1]$). Also let $\alpha = \sqrt{q}e^{i\theta_n}$ and $\beta = \sqrt{1-q}e^{i\theta_m}$. We must show $p_a = 1 \Rightarrow p = q$:

$$\begin{array}{rcl} p_a & = & |\alpha\gamma|^2 \left\langle e_0|e_0\right\rangle + |\beta\delta|^2 \left\langle e_3|e_3\right\rangle + \alpha\beta^*\gamma\delta^* \left\langle e_0|e_3\right\rangle + \alpha^*\beta\gamma^*\delta \left\langle e_3|e_0\right\rangle, \\ & = & qp + (1-q)(1-p) \\ & + & r\sqrt{q(1-q)p(1-p)}\left(e^{i(\theta_n-\theta_m+\theta_a-\theta_b+\theta_e)} + e^{i(\theta_m-\theta_n+\theta_b-\theta_a-\theta_e)}\right) \\ & \leq & qp + (1-q)(1-p) + 2\sqrt{q(1-q)p(1-p)} \end{array} \tag{2}$$

With equality only if $r = 1$ and $\theta_e = \theta_m - \theta_n + \theta_b - \theta_a + 2\pi k$ ($k \in \mathbb{Z}$). Note that both these values (r and θ_e) are in Eve's control and that θ_a and θ_b are public knowledge. Since Equation 2 is bounded by one, and since it is Eve's goal for $p_a = 1$, she must require, these values to be set as described (else $p_a < 1$). Thus we have equality above and so:

$$\begin{array}{rcl} p_a = \quad qp + (1-q)(1-p) + 2\sqrt{q(1-q)p(1-p)} & = & 1 \\ \Rightarrow \qquad p^2 - 2pq + q^2 & = & 0 \\ \Rightarrow \qquad p = q & & \end{array}$$

Thus, $q = |\alpha|^2 = p = |\gamma|^2 = |\left\langle 0|a\right\rangle|^2$ and $|\beta|^2 = |\delta|^2 = |\left\langle 1|a\right\rangle|^2$ as desired.

The second statement is clear since Eve may always apply a unitary operator, rotating the phase of $\left|0\right\rangle$ and $\left|1\right\rangle$ arbitrarily, after Bob has performed his encoding operation. □

The above results in this section only apply to collective attacks. However, when proving a protocol is robust, this is sufficient assuming the probability of Alice and Bob running a security check on the first iteration occurs with non-zero probability and that A sends a qubit only after receiving one from B on the last iteration (which is an assumption used, for example, in [17]). Furthermore, when moving away from robustness and considering, for instance, the key-rate in the asymptotic scenario [3] of these SQKD protocols (which is important future work), it can be shown using the results described in [24, 25] that, if A and B permute their `info` bits (after the quantum communication stage A chooses randomly a permutation and announces it on the public channel), security against collective attacks implies security against any arbitrary, general, coherent attack. It is this line of work, which is perhaps the next step for SQKD protocols, that we suspect our security lemma would be most useful.

3 A New Single State SQKD Protocol

In this section, we present a new single state SQKD protocol and use the above results to prove its robustness. This protocol is, to our knowledge, the first such protocol which permits reflections, and thus X basis states, to contribute to the `info` string, even though Bob is unable to manipulate (i.e., measure and/or prepare) such states. This protocol operates not by using the actual measurement results to contribute to the key, but instead Bob's action. That is, if he choses to reflect Alice's qubit, this will constitute a zero `info` bit; otherwise, if he choses to measure and resend, that iteration will count as a one bit. While the protocols of [4, 5] may be considered the semi quantum version of the BB84 protocol, our protocol described here might be, in some ways, considered to be the semi-quantum version of the SARG04 protocol [2] which we took some inspiration from.

A single iteration of the protocol runs as follows:

1. Alice sends the state $|+\rangle$ to Bob.

2. Bob chooses a random bit $k_B \in \{0, 1\}$; this will be his candidate $\texttt{info}_B$ bit for this iteration (we say "candidate" as it might come to pass that this iteration is discarded in which case k_B is "thrown out").

3. Next, B executes the following process depending on his random choice k_B:

   - If $k_B = 0$, then Bob reflects the qubit. He also sets an internal, private flag denoted $\texttt{accept}_B$ to the value `TRUE` with probability $1/2$; otherwise he sets this flag $\texttt{accept}_B = \texttt{FALSE}$.
   - If $k_B = 1$, then Bob measures and resends. Furthermore, he sets his internal, private flag $\texttt{accept}_B$ to `TRUE` only if his measurement result was a $|0\rangle$; otherwise he sets this flag to `FALSE`.

Note that if $k_B = 0$, his private flag's value is completely random; otherwise its value depends on his measurement result. He keeps the value of $\texttt{accept}_B$ private for now.

4. Alice chooses randomly to measure the incoming qubit in the Z or X basis. Alice sets two internal registers $\texttt{accept}_A$ and k_A (her candidate $\texttt{info}_A$ bit for this iteration) as follows:
   - If she measures in the Z basis resulting in the outcome $|1\rangle$, she sets $\texttt{accept}_A = \texttt{TRUE}$ and $k_A = 0$
   - If she measures in the X basis and this results in outcome $|-\rangle$, she sets $\texttt{accept}_A = \texttt{TRUE}$ and $k_A = 1$.
   - All other cases, she sets $\texttt{accept}_A = \texttt{FALSE}$ and sets k_A to any arbitrary value.

5. With a certain probability (determined by the user), A sets $\texttt{accept}_A$ to `FALSE`. We will see that this forces this iteration to be used as a security check.

6. Alice and Bob broadcast their values of $\texttt{accept}_A$ and $\texttt{accept}_B$ respectively. If both are set to `TRUE`, then Alice and Bob use their values of k_A and k_B for their `info` strings.

7. Security Check: If one or both values are `FALSE`, Bob informs Alice of his value for k_B and also, in the case that $k_B = 1$, his measurement outcome. This allows Alice to verify the security of the channel as follows:
   - If Bob reflected ($k_B = 0$), and Alice measured in the X basis, she should have received $|+\rangle$.
   - If Bob measured and resent ($k_B = 1$) and Alice measured in the Z basis, she should have received the same value Bob measured.
   - If the number of errors exceeds some user-configurable threshold, both Alice and Bob abort.

This process repeats N times. As usual, following this, Alice and Bob run error correcting and privacy amplification protocols.

In a noiseless channel, one would expect $N/8$ of these iterations to contribute to the `info` string. Of the remaining $7N/8$ iterations, one would expect that one quarter of them are used to estimate the noise in the X basis and another quarter to be used to estimate the noise in the Z basis.

Theorem 3.1. The protocol described above is correct. That is, if there is no noise, both Alice and Bob will agree on the same `info` string.

Proof. Consider a single iteration of the protocol. After Alice sends to Bob $|+\rangle$, Bob will either measure and resend (representing an `info` bit of 1 and accepting only if the measurement result was a zero) or he will simply reflect (representing an `info` bit of 0 and accepting only with probability 1/2). Bob will store his decision in a private register $\mathcal{H}_B$ spanned by the basis states $|a,0\rangle, |a,1\rangle, |r\rangle$ representing respectively, whether he accepts this iteration with `info` $= 0$, accepts with `info` $= 1$, or rejects this iteration. This register's use will be equivalent to Bob storing his decisions in a classical memory. Thus, after Bob's operation, the system is in the state (we are assuming no noise):

$$\begin{aligned} \rho &= \tfrac{1}{4} |+\rangle \langle +| \otimes |a,0\rangle \langle a,0|_B + \tfrac{1}{4} |+\rangle \langle +| \otimes |r\rangle \langle r|_B \\ &+ \tfrac{1}{2} \left(\tfrac{1}{2} |0\rangle \langle 0| \otimes |a,1\rangle \langle a,1|_B + \tfrac{1}{2} |1\rangle \langle 1| \otimes |r\rangle \langle r|_B \right) \end{aligned} \tag{3}$$

When Alice receives a qubit back from Bob, she will either measure in the X or Z basis (choosing either with probability 1/2). If she chooses to measure in the X basis, she will accept with `info` $= 1$ only if she measures $|-\rangle$. If she chooses to measure in the Z basis she will accept with `info` $= 0$ only if she measures $|1\rangle$. All other cases are rejected. Assume that Alice has her own private quantum register $\mathcal{H}_A$ spanned by the same basis states as $\mathcal{H}_B$. Thus, after Alice's operation, the state of the system is:

$$\sigma = \frac{1}{2} M_X(\rho) + \frac{1}{2} M_Z(\rho), \tag{4}$$

where:

$$\begin{aligned} M_X(\rho) &= \tfrac{1}{4} |+\rangle \langle +| \otimes |r\rangle \langle r|_A \otimes |a,0\rangle \langle a,0|_B + \tfrac{1}{4} |+\rangle \langle +| \otimes |r\rangle \langle r|_A \otimes |r\rangle \langle r|_B \\ &+ \tfrac{1}{8} |+\rangle \langle +| \otimes |r\rangle \langle r|_A \otimes |a,1\rangle \langle a,1|_B \\ &+ \tfrac{1}{8} |-\rangle \langle -| \otimes |a,1\rangle \langle a,1|_A \otimes |a,1\rangle \langle a,1|_B \\ &+ \tfrac{1}{8} |+\rangle \langle +| \otimes |r\rangle \langle r|_A \otimes |r\rangle \langle r|_B \\ &+ \tfrac{1}{8} |-\rangle \langle -| \otimes |a,1\rangle \langle a,1|_A \otimes |r\rangle \langle r|_B \end{aligned} \tag{5}$$

and:

$$\begin{aligned} M_Z(\rho) &= \tfrac{1}{8} (|0\rangle \langle 0| \otimes |r\rangle \langle r|_A \otimes |a,0\rangle \langle a,0|_B \\ &+ |1\rangle \langle 1| \otimes |a,0\rangle \langle a,0|_A \otimes |a,0\rangle \langle a,0|_B) \\ &+ \tfrac{1}{8} (|0\rangle \langle 0| \otimes |r\rangle \langle r|_A \otimes |r\rangle \langle r|_B + |1\rangle \langle 1| \otimes |a,0\rangle \langle a,0|_A \otimes |r\rangle \langle r|_B) \\ &+ \tfrac{1}{4} (|0\rangle \langle 0| \otimes |r\rangle \langle r|_A \otimes |a,1\rangle \langle a,1|_B + |1\rangle \langle 1| \otimes |a,0\rangle \langle a,0|_A \otimes |r\rangle \langle r|_B) \end{aligned} \tag{6}$$

From this, it is clear that if A and B both accept, their respective `info` bits will match. □

Theorem 3.2. The protocol described above is completely robust.

Proof. In the following, we will assume, as was done with the security proofs in [17], that A sends a qubit only after receiving one from B. Also, as with [4, 5] (and all other robustness proofs for SQKD protocols), we will prove robustness before error correction (as that process by necessity leaks information to E - see [4] for more information on the definition of robustness).

Consider the first iteration of the protocol. It is possible that the very first iteration may be used to verify the security of the channel. Since this is the first iteration, Eve's ancilla space is in some known state $|\chi\rangle\langle\chi|_E$. Applying Lemma 2.1, we know Eve may simply send a state $|e\rangle = \alpha|0\rangle + \beta|1\rangle$ for real α and β. By Lemma 2.2, to avoid detection, Eve might as well send the state $|e\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Bob will then either reflect (with probability $p_R = 1/2$) or measure and resend (with probability $p_M = 1/2$). Furthermore, Bob will store his choice and, if applicable, his measurement result, in his own private register (he may also store other information such as the value of $\texttt{accept}_B$, however this information is not required for our current discussion). Thus, when Eve receives the qubit back from Bob, the system is in the state:

$$\begin{array}{rcl} \rho & = & p_R|+\rangle\langle+|_T \otimes |\chi\rangle\langle\chi|_E \otimes |\texttt{reflect}\rangle\langle\texttt{reflect}|_B \\ & + & \frac{p_M}{2}|0\rangle\langle 0|_T \otimes |\chi\rangle\langle\chi|_E \otimes |\texttt{measure},0\rangle\langle\texttt{measure},0|_B \\ & + & \frac{p_M}{2}|1\rangle\langle 1|_T \otimes |\chi\rangle\langle\chi|_E \otimes |\texttt{measure},1\rangle\langle\texttt{measure},1|_B \end{array} \tag{7}$$

Eve will now apply a unitary operator U_F acting on the transit space and her ancilla space. U_F acts as follows:

$$\begin{array}{c} U_F|0,\chi\rangle = |U_0\rangle := |0,e_0\rangle + |1,e_1\rangle \\ U_F|1,\chi\rangle = |U_1\rangle := |0,e_2\rangle + |1,e_3\rangle \end{array}$$

Where $|e_i\rangle$ are states in Eve's ancilla satisfying:

$$\begin{array}{c} \langle e_0|e_0\rangle + \langle e_1|e_1\rangle = \langle e_2|e_2\rangle + \langle e_3|e_3\rangle = 1 \\ \langle e_2|e_0\rangle + \langle e_3|e_1\rangle = \langle e_0|e_2\rangle + \langle e_1|e_3\rangle = 0 \end{array}$$

The state after Eve applies U_F is $\sigma := U_F\rho U_F^*$ defined as:

$$\begin{array}{rcl} \sigma & = & \frac{p_R}{2}(|U_0\rangle\langle U_0| + |U_1\rangle\langle U_1| + |U_0\rangle\langle U_1| + |U_1\rangle\langle U_0|) \otimes |\texttt{reflect}\rangle\langle\texttt{reflect}|_B \\ & + & \frac{p_M}{2}|U_0\rangle\langle U_0| \otimes |\texttt{measure},0\rangle\langle\texttt{measure},0|_B \\ & + & \frac{p_M}{2}|U_1\rangle\langle U_1| \otimes |\texttt{measure},1\rangle\langle\texttt{measure},1|_B \end{array} \tag{8}$$

The transit qubit is then sent back to Alice who performs a measurement. Assume that Bob chose to measure and resend and that Alice also choose to measure in the Z basis. Furthermore, assume that Alice and Bob agree to use this iteration as a security check. These events occur with non-zero probability. Then, it is clear, in order for Eve to avoid detection, it must be the case that $|e_1\rangle = |e_2\rangle = 0$ (thus $\langle e_0|e_0\rangle = \langle e_3|e_3\rangle = 1$).

Consider now the event that Bob chose to reflect, Alice to measure in the X basis, and both chose to use this iteration to check the security of the channel (again, this is an event that occurs with non-zero probability). Define $\sigma_{reflect} = \frac{1}{2}(|U_0\rangle\langle U_0| + |U_1\rangle\langle U_1| + |U_0\rangle\langle U_1| + |U_1\rangle\langle U_0|)$ (the state of the system if Bob chose to reflect; i.e., the resulting state if Bob measures $\texttt{reflect}$). It is clear that the probability of Alice measuring $|+\rangle$ then is:

$$\begin{aligned} p_+ &:= tr(\left|+\right\rangle\left\langle+\right| \sigma_{reflect} \left|+\right\rangle\left\langle+\right|) \\ &= \tfrac{1}{2}tr\left(\tfrac{1}{2}(\left|+\right\rangle(\left|e_0\right\rangle\left\langle e_0\right| + \left|e_3\right\rangle\left\langle e_3\right| + \left|e_0\right\rangle\left\langle e_3\right| + \left|e_3\right\rangle\left\langle e_0\right|)\left\langle+\right|)\right) \\ &= \tfrac{1}{4}(\langle e_0|e_0\rangle + \langle e_3|e_3\rangle + \langle e_0|e_3\rangle + \langle e_3|e_0\rangle) \end{aligned} \tag{9}$$

Eve avoids detection if and only if $p_+ = 1$. Since $\langle e_0|e_0\rangle = \langle e_3|e_3\rangle = 1$, $p_+ = 1$ if and only if $\langle e_0|e_3\rangle = \langle e_3|e_0\rangle = 1$. This however implies that $|e_0\rangle = |e_3\rangle$. Indeed, assume for contradiction that $|e_3\rangle = |e_0\rangle + |x\rangle$ for some vector $|x\rangle$. Then, $1 = \langle e_0|e_3\rangle = \langle e_0|e_0\rangle + \langle e_0|x\rangle \Rightarrow \langle e_0|x\rangle = 0$. Also, $1 = \langle e_3|e_3\rangle = \langle e_3|e_0\rangle + \langle e_3|x\rangle \Rightarrow \langle e_3|x\rangle = 0$. Finally, $0 = \langle e_3|x\rangle = \langle e_0|x\rangle + \langle x|x\rangle \Rightarrow \langle x|x\rangle = 0 \iff |x\rangle = 0 \iff |e_0\rangle = |e_3\rangle$.

Therefore, at the end of the first iteration, to avoid detection, Eve's ancilla space must be in the state $\left|e_0\right\rangle\left\langle e_0\right|$ regardless of A or B's operations. Thus, to avoid detection, Eve learns nothing on the first iteration. Furthermore, E is fully aware of the state of her ancilla.

All that remains to be shown is that the public discussion leaks no information to Eve. This however is clear. The only discussion sent is whether or not both Alice and Bob accept the iteration. Note that if one or both of them decide to reject the iteration, there is no contribution to the `info` string and, thus, no information for Eve to learn. Therefore we must only consider the case when both accept. This can occur only in the case of two events:

1. Bob choose to reflect, Bob choose to accept, Alice choose to measure in the Z basis, and her measurement outcome was $|1\rangle$. Each of these events occur with probability 1/2. In this case both Alice and Bob agree on an `info` bit of 0.

2. Bob choose to measure and resend, Bob's measurement result was $|0\rangle$, Alice choose to measure in the X basis, and her measurement outcome was $|-\rangle$. Each of these individual events occur with probability 1/2. In this case both Alice and Bob agree on an `info` bit of 1.

The probability of Event 1 occurring is 1/16; likewise for Event 2 occurring. Thus, when Eve learns that both Alice and Bob have accepted, it is equally likely that the `info` bit they agreed upon was a 0 or a 1. Furthermore, if Eve incorporates this knowledge into her ancilla space, she is still fully aware of its state and thus Lemmas 2.1 and 2.2 may be applied again on subsequent iterations repeating the above discussion. Thus, inductively, we see this protocol is robust. □

4 Closing Remarks

From a theoretical standpoint, semi quantum key distribution is a very interesting line of research helping us to better understand exactly how "quantum" two parties need to be in order to derive the same benefits from a fully quantum protocol (e.g., BB84). It is interesting to observe that, in this semi-quantum setting, X basis states may be used not only for security purposes, but to contribute to the `info` string as our new protocol demonstrates. Beyond this, a vital next step in SQKD research is to understand the effects of noise (induced by E's attack) on the protocol by considering, for instance, the key rate in the asymptotic scenario [3, 26, 20] and attempting to compute the maximal tolerated noise before this rate drops to zero. It can be shown, at least for the protocols considered in this paper, that, using the same results from [24, 25], we need only consider collective attacks and security in this setting implies security against any general attack. Usually, when considering the security of a two-way quantum channel, the complexity of this computation, even for collective attacks, increases drastically; however, when working with single state protocols, we may apply Lemma 2.1 greatly decreasing this complexity. It would be very interesting future work to apply the results in this paper in that direction to get a better idea of where these SQKD protocols stand in comparison to a fully quantum protocol.

References

[1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. New York, 1984.

[2] Antonio Acin, Nicolas Gisin, and Valerio Scarani. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A*, 69:012309, Jan 2004.

[3] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[4] Michel Boyer, D. Kenigsberg, and T. Mor. Quantum key distribution with classical bob. In *Quantum, Nano, and Micro Technologies, 2007. ICQNM '07. First International Conference on*, pages 10–10, 2007.

[5] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor. Semiquantum key distribution. *Phys. Rev. A*, 79:032341, Mar 2009.

[6] Hua Lu, Chi-Hang Fred Fung, Xiongfeng Ma, and Qing-yu Cai. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phys. Rev. A*, 84:042344, Oct 2011.

[7] Normand J Beaudry, Marco Lucamarini, Stefano Mancini, and Renato Renner. Security of two-way quantum key distribution. *arXiv preprint arXiv:1301.3138*, 2013.

[8] Hua Lu and Qing-Yu Cai. Quantum key distribution with classical alice. *International Journal of Quantum Information*, 6(06):1195–1202, 2008.

[9] Wang Jian, Zhang Sheng, Zhang Quan, and Tang Chao-Jing. Semiquantum key distribution using entangled states. *Chinese Physics Letters*, 28(10):100301, 2011.

[10] Zhi-Wei Sun, Rui-Gang Du, and Dong-Yang Long. Quantum key distribution with limited classical bob. *International Journal of Quantum Information*, 11(01), 2013.

[11] Kun-Fei Yu, Chun-Wei Yang, Ci-Hong Liao, and Tzonelih Hwang. Authenticated semi-quantum key distribution protocol using bell states. *Quantum Information Processing*, 13(6):1457–1465, 2014.

[12] Zhang Xian-Zhou, Gong Wei-Gui, Tan Yong-Gang, Ren Zhen-Zhong, and Guo Xiao-Tian. Quantum key distribution series network protocol with m-classical bobs. *Chinese Physics B*, 18(6):2143, 2009.

[13] Qin Li, W. H. Chan, and Dong-Yang Long. Semiquantum secret sharing using entangled states. *Phys. Rev. A*, 82:022303, Aug 2010.

[14] Lvzhou Li, Daowen Qiu, and Paulo Mateus. Quantum secret sharing with classical bobs. *Journal of Physics A: Mathematical and Theoretical*, 46(4):045304, 2013.

[15] Jian Wang, Sheng Zhang, Quan Zhang, and Chao-Jing Tang. Semiquantum secret sharing using two-particle entangled state. *International Journal of Quantum Information*, 10(05), 2012.

[16] Chun-Wei Yang and Tzonelih Hwang. Efficient key construction on semi-quantum secret sharing protocols. *International Journal of Quantum Information*, 11(05), 2013.

[17] Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A*, 79:052312, May 2009.

[18] Michel Boyer and Tal Mor. Comment on semiquantum-key distribution using less than four quantum states. *Physical Review A*, 83(4):046301, 2011.

[19] Takayuki Miyadera. Relation between information and disturbance in quantum key distribution protocol with classical alice. *Int. J. of Quantum Information*, 9, 2011.

[20] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95:080501, Aug 2005.

[21] Yong-gang Tan, Hua Lu, and Qing-yu Cai. Comment on quantum key distribution with classical bob. *Phys. Rev. Lett.*, 102:098901, Mar 2009.

[22] Michel Boyer, Dan Kenigsberg, and Tal Mor. Boyer, kenigsberg, and mor reply:. *Phys. Rev. Lett.*, 102:098902, Mar 2009.

[23] Arpita Maitra and Goutam Paul. Eavesdropping in semiquantum key distribution protocol. *Information Processing Letters*, 113(12):418–422, 2013.

[24] Matthias Christandl, Robert Konig, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.

[25] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[26] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.