From Classical to Semi-Quantum Secure Communication

Allison Gagliano
Departments of Mathematics & Computer Science
Eastern Connecticut State University
Willimantic, CT 06226

Walter O. Krawec and Hasan Iqbal
Computer Science & Engineering Department
University of Connecticut
Storrs, CT 06269
Email: walter.krawec@uconn.edu

***Abstract*—In this work we introduce a novel QKD protocol capable of smoothly transitioning, via a user-tuneable parameter, from classical to semi-quantum in order to help understand the effect of quantum communication resources on secure key distribution. We perform an information theoretic security analysis of this protocol to determine what level of "quantumness" is sufficient to achieve security, and we discover some rather interesting properties of this protocol along the way.**

For the full version of this paper, see arXiv:1901.01611

I. Introduction

A *semi-quantum key distribution* (SQKD) protocol's goal is similar to that of a *quantum key distribution* (QKD) protocol, namely the establishment of a secret key between two parties, Alice (A) and Bob (B), secure against an all-powerful adversary Eve (E). Semi-quantum cryptography, first introduced in 2007 by Boyer et al., in [1] with numerous protocols and results following (see our full paper [2] for additional references), imposes the restriction, however, that one of the users (typically B), is limited to being "classical" or "semi-quantum." This restriction implies B is limited to working only in the computational Z basis (spanned by states $|0\rangle$ and $|1\rangle$). He may not measure or prepare states in any other basis (we will discuss the exact capabilities of B later in this paper).

The primary interest of these protocols is to help answer the question "how quantum must a protocol be to gain an advantage over a classical one?" We know that, if both parties are classical, key distribution is impossible unless computational assumptions are made. Thus, the question semi-quantum protocols seek to help answer is: what quantum resources are required to attain unconditional security? However, besides removing certain key quantum capabilities from the two users, there has not been a semi-quantum protocol that can smoothly transition from classical to quantum allowing us to study the effects of quantum communication on secure key distribution.

In this paper, we propose such a protocol and analyze its properties. We introduce a novel SQKD protocol with a user-tuneable parameter α allowing one to, in a way, set the level of "quantumness" of the entire protocol. Indeed, when $\alpha = 0$, the protocol collapses to a classical one (which is insecure). As α increases, the protocol, in a way, becomes more quantum (in that Alice, the quantum user, is allowed to send and receive states which are less orthogonal). However, Bob's capabilities, being classical in nature, are not affected by this α parameter. In fact, as the protocol becomes "more quantum" Bob has more trouble determining A's key bit since B is always restricted to the computational $\{|0\rangle, |1\rangle\}$ basis.

Our protocol is purely of theoretical interest. We are interested in devising a way to measure the effect of quantum state generation and measurement on the security properties of a key-distribution system where one user is forced to be classical and as the other user varies in quantum capabilities. We perform an information theoretic security analysis of our protocol and look at how α affects the noise tolerance of the protocol (i.e., how does the secure communication rate change as A becomes more or less quantum, even when an all-powerful adversary is attacking). Naturally, when α is too small, the protocol is "too classical" to be secure - as α increases the protocol can attain security for some noise levels; however once α increases too much, then Alice is "too quantum" for Bob to understand completely (i.e., he is unable to correctly guess what key-bit A is trying to send to him). Of course, our protocol may also be used "unintentionally" due to hardware faults.

We make several contributions in this work. We introduce a novel SQKD protocol which is interesting theoretically as it is the first such protocol, that we are aware of, to allow researchers to gauge the effect of quantum state preparation and measurement on a key-distribution protocol where one user remains classical in nature. This protocol is also highly restrictive in nature as A and B both have severe restrictions placed on them, yet we are still able to prove security. Second, we perform an information theoretic security analysis of this protocol and our proof technique (which extends that of [3] but to the highly restricted case where fewer noise statistics may be observed) may be of independent interest and applicable to other (S)QKD protocols (note that SQKD protocols require two-way quantum channels - this, in addition to the fact that A and B cannot observe all noise statistics due to their restrictions, greatly increases the complexity of the security analysis). Finally, we evaluate our protocol, examining the effect of the α parameter for various channels and noise scenarios, discovering interesting properties along the way.

Notation and (S)QKD Security: We assume basic knowledge of quantum information; some additional background may be found in the full version online [2]. We use Z to denote the basis $\{|0\rangle, |1\rangle\}$. We use $H(X)$ to be the Shannon

978-1-5386-9291-2/19/$31.00 ©2019 IEEE

entropy of random variable X and $H(x)$, for $x \in [0, 1]$, to mean the binary entropy. We use $S(\rho)$ to mean the von Neumann entropy of density operator ρ. If ρ acts on $\mathcal{H}_A \otimes \mathcal{H}_B$ we often write ρ_{AB}. Then, ρ_B is defined as the partial trace $\rho_B = tr_A \rho_{AB}$. To simplify notation, given $|v\rangle$ in some Hilbert space, we will write $[\mathbf{v}]$ to mean $|v\rangle \langle v|$. If ρ_{AB} acts on $\mathcal{H}_A \otimes \mathcal{H}_B$, then we write $S(AB)_\rho$ to mean $S(\rho_{AB})$. We also write $S(A|B)_\rho$ to mean the conditional von Neumann entropy defined to be $S(A|B)_\rho = S(\rho_{AB}) - S(\rho_B)$. We will forgo writing the subscript "ρ" if the context is clear.

(S)QKD protocols utilize a quantum communication channel and an authenticated classical channel and operate in two stages. First, the *quantum communication stage*, produces an n-bit *raw-key* which is partially correlated and partially secret. Following this, classical error correction and privacy amplification processes are run to produce an $\ell(n)$-bit secret key. For collective attacks, where Eve attacks the channel in an i.i.d. manner, but is free to postpone the measurement of her ancilla to any future time, the Devetak-Winter key-rate equation [4] states: $r = \lim_{n\to\infty} \frac{\ell(n)}{n} = \inf[S(A|E) - H(A|B)]$, where the infimum is over all collective attacks which induce the observed statistics (e.g., the observed error rate, and also statistics from mismatched measurements which can improve the key-rate bound [5], [6]). Computing a bound on r as a function of observable statistics, is the main goal of any (S)QKD security proof [7]. As with almost all (S)QKD security proofs, we consider collective attacks in this paper. Normally security against collective attacks implies security against general attacks [8]; we suspect this result also holds for our protocol, however due to its highly restrictive nature, a rigorous proof of this is left as future work.

An SQKD protocol requires a two-way quantum channel, allowing a qubit to travel from A to B (the *forward direction*) and return from B to A (the *reverse direction*). A, the fully quantum user, is allowed to prepare any arbitrary quantum state and send it to the "classical" user B, who is allowed only to directly work with the Z basis. In more detail, on receiving a qubit, B may choose to do one of two operations:
1. `Measure and Resend`: If he chooses this option, he performs a Z basis measurement on the qubit, resulting in outcome $|r\rangle$, for $r \in \{0, 1\}$. He then resends the same state $|r\rangle$ to A. Note that he can only measure and prepare qubits in this single basis.
2. `Reflect`: In this case, B disconnects from the quantum channel and reflects all qubits back to A. If this is chosen, A is, essentially, communicating with herself.

II. Our Protocol and Security Analysis

Besides B being classical in nature, we also place additional restrictions on the quantum user A. On each iteration of the quantum communication stage, A is only allowed to send one of two possible states: either $|0\rangle$ or $|a\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha \geq 0$ is a public, user-specified, parameter and $\beta = \sqrt{1-\alpha^2}$.

When a qubit returns to A (following B's operation), she will perform a measurement using the three-outcome POVM $\Lambda = \{\Lambda_0, \Lambda_a, \Lambda_?\}$ defined: $\Lambda_0 = p|0\rangle\langle 0|$, $\Lambda_a = p|a\rangle\langle a|$, and where $\Lambda_? = I - \Lambda_0 - \Lambda_1$ where $p = \frac{1}{1+\alpha}$.

Notice that, when $\alpha = 0$, the protocol "collapses" to a purely classical communication system where A sends $|0\rangle$ and $|1\rangle$ only and where she is always measuring in the Z basis (since p approaches 1 as α decreases and so $\Lambda_0 = |0\rangle\langle 0|$, $\Lambda_a = |1\rangle\langle 1|$, and $\Lambda_? \equiv 0$). Of course, B is classical regardless of the choice of α since he is only able to measure and send in the Z basis (or disconnect from the quantum channel, thus causing A to simply "talk to herself"). For $\alpha > 0$, the protocol is inherently quantum - but the question is, how far from classical ($\alpha = 0$) must the communication be before we start attaining secure communication? The quantum communication stage of our protocol is described below:

Protocol:
1. A chooses a bit k_A uniformly at random. If $k_A = 0$, she sends $|0\rangle$ to B; otherwise she sends $|a\rangle = \alpha|0\rangle + \beta|1\rangle$.
2. B chooses a random operation: `Measure and Resend` (with probability q) or `Reflect` (with probability $1 - q$). If he chooses `Measure and Resend`, he will save his measurement result as $k_B \in \{0, 1\}$.
3. Finally, with probability q, A will simply discard the qubit; otherwise, she will measure using POVM Λ, as discussed in the text, saving the outcome (which is one of "0," "a," or "?").
4. Using the authenticated classical channel, B will disclose his choice of operation and A will disclose whether she chose to measure or not. For all iterations where A chose to measure the returning qubit, A will send to B her preparation and measurement outcomes (*these iterations will be used only to test the quantum channel and not for key distillation*). For all other iterations (where A did not measure) and if B chose `Measure and Resend`, then A and B will use their respective k_A and k_B values to contribute towards their raw key.

(Note that in the asymptotic scenario, which we consider in this work, q may be set arbitrarily close to 1 as is done for other (S)QKD protocols to improve efficiency [9], [10].)

The reader will observe that, for $\alpha > 0$, our protocol always has some noise in the raw key, *even when no adversary is present*! Indeed, unless the protocol is purely classical ($\alpha = 0$), the classical user B will be unable to determine exactly the information that A is trying to send. The issue is exacerbated when an adversary comes into play (adding additional noise). As mentioned in the introduction, *the protocol is purely a theoretical one* studied for its theoretical interest to help study the "gap" between classical and quantum communication. We do not expect this protocol to ever be implemented in practice (*unless some faulty hardware forces this protocol to be used*). Note that we are also not concerned with practical attacks such as photon loss or multi-photon states [7]; though interesting, these issues are outside the scope of this theoretical analysis.

We are interested in two questions: Given an observed noise level Q, for what α is the protocol secure? Of course when $\alpha = 0$, the protocol will never be secure. Secondly, what is an optimal choice of α? That is, how "far" from the classical case of $\alpha = 0$ must the communication be to optimize the secure transfer of information between quantum A and classical B when faced with a quantum adversary E.

Security Analysis: Our goal in this section is to compute our protocol's key-rate (specifically $S(A|E)$) as a function of α and those observable parameters that A and B may measure in the channel (which are very few). To do so, we derive a density operator description of a single "successful" iteration of the protocol (where by "successful" we mean an iteration leading to the distillation of a raw key bit). For now we assume collective attacks as discussed earlier. Using a result in [11], for any SQKD protocol, it suffices to show security against so-called *restricted* collective attacks consisting of an isometry $\mathcal{F} : \mathcal{H}_T \rightarrow \mathcal{H}_T \otimes \mathcal{H}_E$ applied in the forward channel (connecting A to B) and a unitary operator U_R applied in the reverse channel and acting on $\mathcal{H}_T \otimes \mathcal{H}_E$. Here we use $\mathcal{H}_T$ to denote the two-dimensional space modeling the qubit in transit and $\mathcal{H}_E$ is Eve's ancilla. The action of $\mathcal{F}$ is simply: $\mathcal{F}\left|0\right\rangle_T = q_0 \left|0,0\right\rangle_{TE} + q_1 \left|1,e\right\rangle_{TE}$, and $\mathcal{F}\left|1\right\rangle_T = q_2 \left|0,f\right\rangle_{TE} + q_3 \left|1,0\right\rangle_{TE}$, where $q_i \in \mathbb{R}_{\geq 0}$ subject to $q_0^2 + q_1^2 = q_2^2 + q_3^2 = 1$ and where $|e\rangle$ and $|f\rangle$ are arbitrary, normalized, vectors in $\mathcal{H}_E$. In the reverse channel, Eve applies an arbitrary unitary operator, the action of which we may write as:

$$U_R \left|0,0\right\rangle_{TE} = \left|0,e_0\right\rangle + \left|1,e_1\right\rangle \quad U_R\left|1,0\right\rangle = \left|0,e_2\right\rangle + \left|1,e_3\right\rangle$$
$$U_R \left|1,e\right\rangle_{TE} = \left|0,f_0\right\rangle + \left|1,f_1\right\rangle \quad U_R\left|0,f\right\rangle = \left|0,f_2\right\rangle + \left|1,f_3\right\rangle .$$

Above, the states $|e_i\rangle$ and $|f_i\rangle$ are arbitrary states in $\mathcal{H}_E$ (though, unitarity of U_R imposes some restrictions on them which will be important momentarily).

Tracing the execution of the protocol, we may build the desired density operator which is found to be (see full paper for details on this derivation [2]):

$$\begin{aligned}\rho_{ABE} = &\frac{1}{2}[\mathbf{0}]_A \otimes ([\mathbf{0}]_B \otimes q_0^2([\mathbf{e_0}] + [\mathbf{e_1}])) \qquad (1)\\ &+ \frac{1}{2}[\mathbf{0}]_A \otimes ([\mathbf{1}]_B \otimes q_1^2([\mathbf{f_0}] + [\mathbf{f_1}]))\\ &+ \frac{1}{2}[\mathbf{1}]_A \otimes ([\mathbf{0}]_B \otimes ([\mathbf{g_3}] + [\mathbf{g_2}]))\\ &+ \frac{1}{2}[\mathbf{1}]_A \otimes ([\mathbf{1}]_B \otimes ([\mathbf{g_1}] + [\mathbf{g_0}]))\end{aligned}$$

where $[\mathbf{v}] = |v\rangle\langle v|$ for any v, and:

$$|g_0\rangle = q_1\alpha\,|f_1\rangle + q_3\beta\,|e_3\rangle \qquad |g_1\rangle = q_1\alpha\,|f_0\rangle + q_3\beta\,|e_2\rangle$$
$$|g_2\rangle = q_0\alpha\,|e_1\rangle + q_2\beta\,|f_3\rangle \qquad |g_3\rangle = q_0\alpha\,|e_0\rangle + q_2\beta\,|f_2\rangle$$

From this, we may then use a Theorem from [3] to derive the following (see full paper for details on the use of this theorem in this work):

$$\begin{aligned}S(A|E)_\rho \geq &\frac{q_0^2\langle e_0|e_0\rangle + \langle g_0|g_0\rangle}{2} \qquad (2)\\ &\times\left(H\left[\frac{q_0^2\langle e_0|e_0\rangle}{q_0^2\langle e_0|e_0\rangle + \langle g_0|g_0\rangle}\right] - H\left[\lambda(q_0\,|e_0\rangle\,, |g_0\rangle)\right]\right).\end{aligned}$$

where

$$\lambda(|x\rangle\,, |y\rangle) = \frac{1}{2}\left(1 + \frac{\sqrt{(\langle x|x\rangle - \langle y|y\rangle)^2 + 4Re^2\langle x|y\rangle}}{\langle x|x\rangle + \langle y|y\rangle}\right).$$

To compute $S(A|E)$, needed for the key-rate, we need to compute, or bound, the inner-products appearing in the above expression, based only on statistics we may observe and α.

Note that q_0 and q_1 are both observable parameters. Indeed, let $p_{0,i}^{A\rightarrow B}$ be the probability that B measures $|i\rangle$ (for $i \in \{0,1\}$) if A initially sent $|0\rangle$. This is one of the few statistics A and B actually can estimate and is, in fact, the only observable noise statistic in the forward channel (they cannot measure, for example, $p_{1,i}^{A\rightarrow B}$ when $\alpha > 0$). It is not difficult to see, from the action of $\mathcal{F}$, that $q_0^2 = p_{0,0}^{A\rightarrow B}$ and $q_1^2 = p_{0,1}^{A\rightarrow B}$. Note that, by definition of the restricted attack, it is sufficient to consider non-negative q_i [11].

As mentioned, the users cannot directly observe q_2 and q_3. However, they can estimate it by considering $p_{a,1}^{A\rightarrow B}$, the probability that B measures $|1\rangle$ if A initially sent $|a\rangle$ (this is something that may be observed). By tracing the evolution of the qubit, we derive the following (please see the full paper for details on this process [2]):

$$p_{a,1}^{A\rightarrow B} = p_{0,1}^{A\rightarrow B}\alpha^2 + q_3^2\beta^2 + 2\sqrt{p_{0,1}^{A\rightarrow B}}\,q_3\alpha\beta Re\,\langle 0|e\rangle\,. \quad (3)$$

Of course, $|\langle 0|e\rangle| \leq 1$. We are constrained by the fact that $q_3 \geq 0$ (since, for the restricted attack, each q_i are non-negative real numbers [11]). We therefore have the following lower-bound for q_3, assuming $p_{a,1}^{A\rightarrow B} \geq \alpha^2 p_{0,1}^{A\rightarrow B}$ (which it will be in our evaluations and one would expect this if the observable noise is not too high):

$$1 \geq q_3 \geq \frac{1}{\beta}\left(\sqrt{p_{a,1}^{A\rightarrow B}} - \alpha\sqrt{p_{0,1}^{A\rightarrow B}}\right). \quad (4)$$

We therefore have values, or bounds, for all q_i (note that $q_2 = \sqrt{1-q_3^2}$). It is clear that we may observe $\langle e_0|e_0\rangle\,, \langle e_1|e_1\rangle\,, \langle f_0|f_0\rangle$, and $\langle f_1|f_1\rangle$. Indeed, let $p_{i,j,k}^{A\rightarrow A}$ denote the probability that A's measurement observes "k" conditioned on the event A initially sent $|i\rangle$ and B chose Measure and Resend and actually observed $|j\rangle$. Of course, $i \in \{0,a\}$, $j \in \{0,1\}$ and $k \in \{0,a,?\}$. It is not difficult to see, then, that $p_{0,0,0}^{A\rightarrow A} = p \cdot \langle e_0|e_0\rangle$ where $p > 0$ is the POVM parameter as described earlier. By unitarity we also have $\langle e_1|e_1\rangle = 1 - \langle e_0|e_0\rangle$. Similarly, we have $p_{0,1,0}^{A\rightarrow A} = p \cdot \langle f_0|f_0\rangle$ and $\langle f_1|f_1\rangle = 1 - \langle f_0|f_0\rangle$. To simplify notation, at this point we will assume a symmetric attack and define the following: $p_{0,0,0}^{A\rightarrow A} = p\cdot(1-Q_R) \Rightarrow \langle e_0|e_0\rangle = 1-Q_R$ and $p_{0,1,0}^{A\rightarrow A} = p \cdot Q_R \Rightarrow \langle f_0|f_0\rangle = Q_R$. (Note we use Q_R to denote the noise in the Reverse channel, from B to A.)

This assumption that the *observable* noise is symmetric in this manner (which may be enforced by A and B and is a common assumption in (S)QKD security proofs) is not necessary, and our analysis below follows without it; we only use this to simplify notation. Note that, if there is no noise in the forward channel (in which case $p_{0,1,0}^{A\rightarrow A}$ is technically undefined since we are conditioning on an event which never occurs), then $\langle f_0|f_0\rangle$ and $\langle f_1|f_1\rangle$ never show up in any of our computations and so we may define $p_{0,1,0}^{A\rightarrow A}$ arbitrarily; thus we define $p_{0,1,0}^{A\rightarrow A} = p \cdot Q_R$ in this case regardless.

It is also not difficult to see that each $\langle g_i|g_i\rangle$ may be observed. For details, see the full paper, however we may derive the following (again, assuming a symmetric attack - for the general case, the details are in the full paper): $\langle g_0|g_0\rangle = p_{a,1}^{A\to B}(1-Q_R)$; $\langle g_1|g_1\rangle = p_{a,1}^{A\to B}Q_R$; $\langle g_2|g_2\rangle = p_{a,0}^{A\to B}Q_R$; and $\langle g_3|g_3\rangle = p_{a,0}^{A\to B}(1-Q_R)$.

Finally, to compute our bound on $S(A|E)$, we will also need to compute the inner product appearing in the λ function, namely we must lower-bound $Re^2\langle e_0|g_0\rangle$ (a lower-bound on this minimizes $S(A|E)$). It is not difficult (using the Cauchy-Schwarz inequality) to derive the following bound:

$$\begin{aligned}&Re^2\langle e_0|g_0\rangle \geq\\ &\left[\max\left(0, q_3\beta\langle e_0|e_3\rangle - \alpha\sqrt{p_{0,1}^{A\to B}}(1-Q_R)\right)\right]^2,\end{aligned} \tag{5}$$

We thus reduced the problem to bounding $\langle e_0|e_3\rangle$. To attain this, we must look at several more statistics. In particular, we require bounds on the "hidden" noise (i.e., noise in the reverse channel that cannot be directly observed). By expanding $\langle g_1|g_1\rangle = p_{a,1}^{A\to B}Q_R$ and solving the resulting quadratic in terms of $\sqrt{\langle e_2|e_2\rangle}$, we find:

$$\sqrt{\langle e_2|e_2\rangle} \leq \frac{1}{q_3\beta}\left(q_1\alpha\sqrt{Q_R} + \sqrt{p_{a,1}^{A\to B}Q_R}\right) \tag{6}$$

Similarly, we can bound $\langle f_3|f_3\rangle$ by considering $\langle g_2|g_2\rangle = p_{a,0}^{A\to B}Q_R$. Solving the resulting quadratic, we find:

$$\sqrt{\langle f_3|f_3\rangle} \leq \frac{1}{q_2\beta}\left(q_0\alpha\sqrt{Q_R} + \sqrt{p_{a,0}^{A\to B}Q_R}\right). \tag{7}$$

We now have upper-bounds on the "hidden" noise of the channel. (Complete details on these important derivations are available in the full version [2].)

Next, let us consider the statistic $p_{a,R,a}^{A\to A}$ which we use to denote the probability that, conditioning on the event A sends $|a\rangle$, B chooses to Reflect, and A chooses to measure using POVM Λ (see protocol description), that the outcome of this measurement is "a". Tracing the qubit's evolution (see the full paper [2] for details on this computation) we find that:

$$\begin{aligned}p_{a,R,a}^{A\to A} &= p_{a,0}^{A\to B}p_{a,0,a}^{A\to A} + p_{a,1}^{A\to B}p_{a,1,a}^{A\to A}\\ &+ 2p\cdot Re(q_0q_1\alpha^4\langle e_0|f_0\rangle + q_0q_3\alpha^3\beta\langle e_0|e_2\rangle)\\ &+ 2p\cdot Re(q_0q_1\alpha^3\beta\langle e_0|f_1\rangle + q_0q_3\alpha^2\beta^2\langle e_0|e_3\rangle)\\ &+ 2p\cdot Re(q_1q_2\alpha^3\beta\langle f_0|f_2\rangle + q_2q_3\alpha^2\beta^2\langle e_2|f_2\rangle)\\ &+ 2p\cdot Re(q_1q_2\alpha^2\beta^2\langle f_1|f_2\rangle + q_2q_3\alpha\beta^3\langle e_3|f_2\rangle)\\ &+ 2p\cdot Re(q_0q_1\alpha^3\beta\langle e_1|f_0\rangle + q_0q_3\alpha^2\beta^2\langle e_1|e_2\rangle)\\ &+ 2p\cdot Re(q_0q_1\alpha^2\beta^2\langle e_1|f_1\rangle + q_0q_3\alpha\beta^3\langle e_1|e_3\rangle)\\ &+ 2p\cdot Re(q_1q_2\alpha^2\beta^2\langle f_0|f_3\rangle + q_2q_3\alpha\beta^3\langle e_2|f_3\rangle)\\ &+ 2p\cdot Re(q_1q_2\alpha\beta^3\langle f_1|f_3\rangle + q_2q_3\beta^4\langle e_3|f_3\rangle).\end{aligned} \tag{8}$$

(Note that, above, we used the fact that $Re\langle x|y\rangle = Re\langle y|x\rangle$.) By taking advantage of the unitarity of U_R, and also solving for the $Re\langle e_0|e_3\rangle$ term, we may simplify the above to (again, full details on this simplification are explained in the full version of this paper [2]):

$$\begin{aligned}&q_0q_3\alpha^2\beta^2 Re\langle e_0|e_3\rangle\\ &= \frac{1}{2p}(p_{a,R,a}^{A\to A} - p_{a,0}^{A\to B}p_{a,0,a}^{A\to A} - p_{a,1}^{A\to B}p_{a,1,a}^{A\to A})\\ &- (\alpha^2-\beta^2)Re\langle g_1|g_3\rangle - \chi\end{aligned} \tag{9}$$

where: $\chi = Re(q_0q_1\alpha^3\beta[\langle e_0|f_1\rangle + \langle e_1|f_0\rangle]) + Re(q_0q_3\alpha^2\beta^2\langle e_1|e_2\rangle) + Re(q_1q_2\alpha^2\beta^2[\langle f_0|f_3\rangle + \langle f_1|f_2\rangle]) + Re(q_2q_3\alpha\beta^3[\langle e_2|f_3\rangle + \langle e_3|f_2\rangle])$. A and B do not have sufficient quantum capabilities to fully compute χ; however we can bound it based on what we already know and using the Cauchy-Schwarz inequality, along with unitarity of U_R:

$$\begin{aligned}|\chi| \leq\ & q_0q_1\alpha^3\beta[(1-Q_R)+Q_R]\\ &+ q_0q_3\alpha^2\beta^2\sqrt{Q_R\langle e_2|e_2\rangle}\\ &+ q_1q_2\alpha^2\beta^2\sqrt{Q_R\langle f_3|f_3\rangle}\\ &+ q_1q_2\alpha^2\beta^2\sqrt{(1-Q_R)(1-\langle f_3|f_3\rangle)}\\ &+ q_2q_3\alpha\beta^3\sqrt{\langle e_2|e_2\rangle\langle f_3|f_3\rangle}\\ &+ q_2q_3\alpha\beta^3\sqrt{(1-\langle e_2|e_2\rangle)(1-\langle f_3|f_3\rangle)}.\end{aligned} \tag{10}$$

Finally, it can be shown (see the full paper [2]) that: $Re\langle g_1|g_3\rangle = \frac{1}{2}\left(p_{a,R,0}^{A\to A}/p - \langle g_1|g_1\rangle - \langle g_3|g_3\rangle\right)$. Since $\langle g_i|g_i\rangle$ are all observable as discussed earlier, this completes our bound. To summarize, given as input α along with those observable statistics as utilized above, one must simply minimize Equation 2 over all q_3, $\langle e_2|e_2\rangle$, and $\langle f_3|f_3\rangle$, as enforced by Equations 4, 6, and 7. For any particular choice of these values, one may compute a bound on χ from Equation 10; one may also compute a bound on $Re\langle e_0|e_3\rangle$ using Equation 9. This then allows one to bound $Re^2\langle e_0|g_0\rangle$, using Equation 5 which gives a possible value of $S(A|E)$. Minimizing over $\langle e_2|e_2\rangle$, $\langle f_3|f_3\rangle$, and q_3 gives a worst-case lower-bound on $S(A|E)$ over all attacks which induce the observed statistics. In our evaluations, we perform this simple minimization numerically.

It can be seen that if $\alpha = 0$ (i.e., the protocol is classical), Equation 9 becomes simply $0 = 0$, regardless of the choice of $\langle e_0|e_3\rangle$. Thus, Eve may set $\langle e_0|e_3\rangle = 0$ in this case $\langle e_0|g_0\rangle = 0$ and so $S(A|E) = 0$ as expected. That is, in the classical case, Eve has no uncertainty on A and B's raw key and so the protocol is insecure. The interesting question is what happens when $\alpha > 0$? To finish the key-rate computation (and answer this question), we also need $H(A|B)$, however computing this is trivial and we omit the details here; the exact expression may be found in the full version of this paper [2].

Evaluation: To evaluate our protocol, and more importantly to see the effect of α on the secure key-rate, we must put values to those observable statistics $p_{\cdot,\cdot}^{A\to B}$ and $p_{\cdot,\cdot,\cdot}^{A\to A}$. We assume the channel is modeled as a depolarization channel (i.e., $\mathcal{E}_Q(\rho) = (1-2Q)\rho + Q\cdot I$) parameterized by noise values Q_F (in the forward channel), Q_R (in the reverse), and Q_X (for the "loop" channel when B reflects). From this, we find: $p_{0,0}^{A\to B} = 1-Q_F$; $p_{0,1}^{A\to B} = Q_F$; $p_{0,0,0}^{A\to A}/p = 1-Q_R$; $p_{0,1,0}^{A\to A}/p = Q_R$; $p_{a,0,0}^{A\to A}/p = 1-Q_R$; $p_{a,1,0}^{A\to A}/p = Q_R$; $p_{a,R,a}^{A\to A}/p = 1-Q_X$.

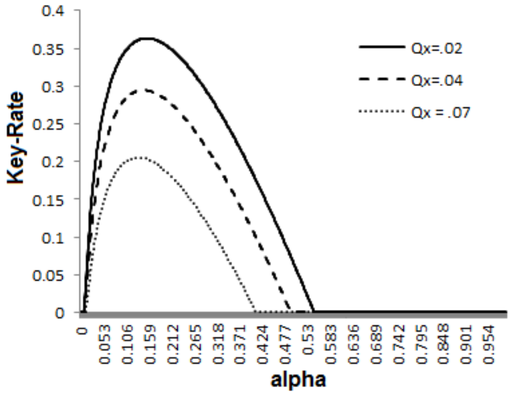

Fig. 1. Key-rate when the forward channel noise is very low (10^{-5}) and the reverse and loop noise levels are high. We see that the forward channel noise is the most critical for this protocol.

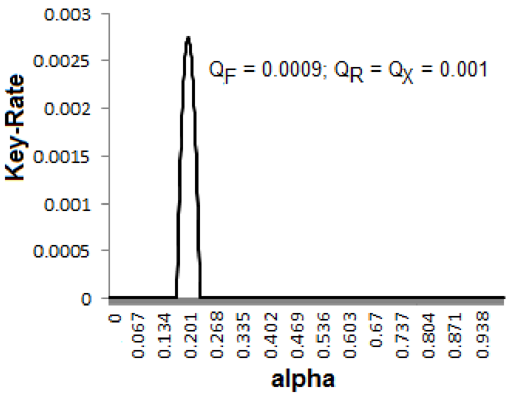

Fig. 2. Key-rate when the forward channel noise is increased - only a small window of α values exist in this case when the protocol attains a positive key-rate.

We also derive: $p^{A\to B}_{a,0} = (1-2Q_F)\alpha^2 + Q_F$; $p^{A\to B}_{a,1} = (1-2Q_F)\beta^2 + Q_F$; $p^{A\to A}_{a,0,a}/p = (1-2Q_R)\alpha^2 + Q_R$; $p^{A\to A}_{a,1,a}/p = (1-2Q_R)\beta^2 + Q_R$; and $p^{A\to A}_{a,R,0}/p = (1-2Q_X)\alpha^2 + Q_X$. *Note that the POVM parameter value $p > 0$ is not important in this asymptotic scenario;* though it would play a much larger role in a finite key analysis. Analyzing this case we leave as interesting future work.

As expected, the noise tolerance of this protocol is low, however we are able to attain positive key-rates as shown in Figures 1, and 2. Our evaluations show that our protocol is most sensitive to forward channel noise. Indeed, as shown in Figure 1, the protocol can tolerate a high level of reverse and loop noise (approaching 10%). However as the forward channel noise increases, there are only a few choices for α where a positive key-rate can be attained. Optimal values of α ranged between 0.13 and 0.2. Other comments, evaluations, and noise scenarios are available in the full paper [2].

Despite the low noise tolerance, we still consider this a positive, and interesting, result as this protocol was designed specifically to smoothly transform from classical to quantum communication and to allow research in investigating how this affects secure communication. Of course, our key-rate is a lower bound, so the actual security rate can only be higher. Further studying this would make interesting future work.

III. Closing Remarks

In this paper, we developed a new SQKD protocol with a tuneable parameter α allowing one to gauge the effect of the secure communication rate, based on "how quantum" the protocol is. When α is set to zero, the communication is purely classical and thus the protocol is insecure. As α increases, security can be attained for certain optimal choices and for certain channels. Studying the protocol further may help to shed additional light on the "gap" between quantum and classical secure communication. Furthermore, our proof approach may be applicable to other (S)QKD protocols where users are highly restricted in their quantum capabilities (either intentionally or due, perhaps, to hardware faults).

Many interesting future problems remain open. Improving our key-rate bound and performing a finite-key analysis can be very interesting. Also, studying the effect of α against different types of attacks could prove interesting (we have evidence that the optimal α is different for intercept-resend attacks). Trying to decrease the resource requirements even further could be interesting; in the full paper [2], we comment more on this.

Acknowledgments: AG would like to acknowledge the support of National Science Foundation grant number 1659764, which supported her during a summer REU at the University of Connecticut. WK and HI are partially supported by the NSF under grant number 1812070.

References

[1] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical bob," *Phys. Rev. Lett.*, vol. 99, p. 140501, Oct 2007.

[2] A. Gagliano, W. O. Krawec, and H. Iqbal, "From classical to semi-quantum secure communication (full version)," *arXiv:1901.01611*, 2019.

[3] W. O. Krawec, "Quantum key distribution with mismatched measurements over arbitrary channels," *Quantum Information and Computation*, vol. 17, no. 3 and 4, pp. 209–241, 2017.

[4] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. of the Royal Society A: Math., Physical and Engineering Science*, vol. 461, no. 2053, pp. 207–235, 2005.

[5] S. M. Barnett, B. Huttner, and S. J. Phoenix, "Eavesdropping strategies and rejected-data protocols in quantum cryptography," *Journal of Modern Optics*, vol. 40, no. 12, pp. 2501–2513, 1993.

[6] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Physical Review A*, vol. 78, no. 4, p. 042316, 2008.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[8] M. Christandl, R. Konig, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, p. 020504, Jan 2009.

[9] H.-K. Lo, H.-F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[10] W. O. Krawec, "Security proof of a semi-quantum key distribution protocol," in *Information Theory (ISIT), 2015 IEEE International Symposium on.* IEEE, 2015, pp. 686–690.

[11] ——, "Key-rate bound of a semi-quantum protocol using an entropic uncertainty relation," in *2018 IEEE International Symposium on Information Theory (ISIT)*, June 2018, pp. 2669–2673.