Asymptotic Analysis of a Three State Quantum Cryptographic Protocol

Walter O. Krawec
Computer Science Department
Iona College
New Rochelle, NY 10801
Email: walter.krawec@gmail.com

***Abstract*—In this paper we consider a three-state variant of the BB84 quantum key distribution (QKD) protocol. We derive a new lower-bound on the key rate of this protocol in the asymptotic scenario and use mismatched measurement outcomes to improve the channel estimation. Our new key rate bound remains positive up to an error rate of 11%, exactly that achieved by the four-state BB84 protocol. This is also a substantial improvement in the tolerated noise over previous lower-bounds for this particular three-state protocol.**

***Index Terms*—Quantum Computing, Cryptography**

I. Introduction

A quantum key distribution (QKD) protocol is designed to allow two users Alice A and Bob B to establish a shared secret key that is secure against an all powerful adversary Eve E. Typically, these protocols operate by A preparing and sending qubits to B who will then measure them; both the preparation and the subsequent measurements are performed in a variety of bases as dictated by the protocol. This *quantum communication stage* results in A and B each distilling a *raw key*: a string of classical bits of size N which is partially correlated and partially secret. The users will then run an error correcting (EC) and privacy amplification (PA) protocol resulting in a secret key of size $\ell(N) \leq N$. In this paper, we are interested in the key rate in the asymptotic scenario defined $r = \lim_{N\to\infty} \frac{\ell(N)}{N}$. See [1] for more information on these standard definitions and processes.

It was shown in [2] that, assuming collective attacks (where E performs the same attack operation each iteration but is free to postpone the measurement of her ancilla to any future time), then $r = \inf(S(A|E) - H(A|B))$. Here $S(A|E)$ is the conditional von Neumann entropy; $H(A|B)$ is the conditional classical entropy, and the infimum is over the set of all collective attacks which induce the observed statistics.

In this paper, we will compute a new lower bound on the key rate of a three-state protocol first introduced in [3], [4]. Such a protocol allows A to only send $|0\rangle$, $|1\rangle$, or $|+\rangle$ (we will actually consider a generalized version where the third state is $|a\rangle = \alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle$ for any $\alpha \in (0, 1)$); thus the users cannot measure the probability of E's attack flipping a $|-\rangle$ to a $|+\rangle$ as can be done in the four-state BB84 [5] protocol. However, by using mismatched measurement outcomes [6] we can impose further restrictions on the set of possible attacks used by E thus improving the key rate bound (in particular, we will not discard, as is typically done, the measurement outcomes when A and B's choice of basis do not agree).

Our results show that, if we assume E's attack is symmetric (which could even be enforced), then the three state protocol's maximally tolerated error rate is equal to that of the four-state BB84 protocol - i.e., our key rate bound (which will be a function only of parameters that may be observed by A and B) remains positive up to an error rate of 11%. This is greatly improved over the previous best known lower-bound derived in [4] which remained positive only for an error rate less than 5.1%. We will also consider how the choice of $|a\rangle$ affects this rate.

We comment that mismatched measurement outcomes were used in [6] with the BB84 (a four-state protocol) and the six-state BB84 protocols; it was also shown to produce a superior key rate for certain quantum channels, for those two protocols. In [7] they were used to detect an attacker with greater probability for measure/resend attacks. We also used them in [8] in the proof of security for a semi-quantum QKD protocol. To our knowledge, we are the first to consider the use of mismatched outcomes to the three-state BB84 protocol.

For notation, we denote by ρ_{AB} to mean a density operator acting on the joint Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. If we write ρ_A then we mean the operator resulting from the tracing out of B's subspace (i.e., $\rho_A = tr_B\rho_{AB}$). These definitions extend to three or more subspaces. By $S(AB)_\rho$ we mean the von Neumann entropy $S(\rho_{AB})$ and $S(A|B)_\rho$ to mean $S(AB)_\rho - S(B)_\rho$. We use $H(\cdot)$ to denote the classical Shannon entropy and $h(x)$ to be the binary entropy function (i.e., $h(x) = H(x, 1-x) = -\log x - (1-x)\log(1-x)$). All logarithms in this paper are base two.

II. The Protocol

The protocol we consider in this paper is a three state one and it is a generalization of the protocol described in [3], [4]. Let $\mathcal{B} = \{|0\rangle, |1\rangle\}$ be an arbitrary orthonormal basis and let $\mathcal{A} = \{|a\rangle, |\bar{a}\rangle\}$, where $|a\rangle = \alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle$, $|\bar{a}\rangle = \sqrt{1-\alpha^2}|0\rangle - \alpha|1\rangle$, and $\alpha \in (0, 1)$. Clearly $\mathcal{A}$ is also an orthonormal basis; note that when $\alpha = 1/\sqrt{2}$, we have $|a\rangle = |+\rangle$ and $|\bar{a}\rangle = |-\rangle$ where $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$. The value of α is considered to be public knowledge.

The quantum communication stage of the protocol consists of the following process:

1) A prepares a qubit of the form $|0\rangle$, $|1\rangle$, or $|a\rangle$, choosing each with probability $p/2$, $p/2$, and $1-p$ respectively. This qubit is sent to B. Note that A cannot prepare $|\bar{a}\rangle$.
2) B chooses with probability q to measure the qubit in the $\mathcal{B} = \{|0\rangle, |1\rangle\}$ basis; otherwise, he measures in the $\mathcal{A} = \{|a\rangle, |\bar{a}\rangle\}$ basis.
3) A and B will disclose their choice of basis (using an authenticated classical channel). If their choice of basis is $\mathcal{B}$, they will use this iteration to contribute towards their raw key in the obvious way.

Note that, when $\alpha = 1/\sqrt{2}$, this protocol is exactly the three-state version of BB84 discussed in [3], [4]; that is, it is BB84 with the limitation that A can never send $|-\rangle$ and thus the users can never measure the probability of E's attack flipping a $|-\rangle$ to a $|+\rangle$ (they can only measure the probability of a $|+\rangle$ flipping to a $|-\rangle$). As discussed in [3], there are several potential practical benefits to this protocol. It is also interesting theoretically as it allows us to study the effects of decreasing A's required quantum capabilities.

III. Security Proof

To compute a lower bound on the key rate r, we must first describe the quantum system after one iteration of the protocol, conditioning on the event this iteration is used to contribute towards the raw key (in particular, A sends a state from $\mathcal{B}$ and B measures in that same basis). We will first assume collective attacks; later we will comment on general attacks.

Fix $\alpha \in (0,1)$; this parameter is public knowledge (in particular E also knows the value this is set to) and furthermore, once fixed it is constant throughout the protocol. Let U be the unitary attack operator E employs each iteration of the protocol. Since we are conditioning on the event this iteration is used to contribute to the raw key, A will prepare $|0\rangle$ or $|1\rangle$, choosing each with probability $1/2$. E will then attack with operator U. Without loss of generality, we may write U's action on basis states as follows:

$$U|0\rangle = |0, e_0\rangle + |1, e_1\rangle \ , \ U|1\rangle = |0, e_2\rangle + |1, e_3\rangle \tag{1}$$

These $|e_i\rangle$ are arbitrary states in E's ancilla and are not assumed to be normalized nor orthogonal. Unitarity of U of course imposes certain conditions on them; furthermore, parameter estimation will yield even more data on them later.

Thus, the state of the quantum system, when the qubit arrives at B's lab is: $\frac{1}{2}|0\rangle\langle 0|_A \otimes P(|0,e_0\rangle + |1,e_1\rangle) + \frac{1}{2}|1\rangle\langle 1|_A \otimes P(|0,e_2\rangle + |1,e_3\rangle)$, where $P(z) = zz^*$ and z^* is the conjugate transpose of z.

B will then measure in the $\mathcal{B}$ basis (again, we are conditioning on the event this iteration is used for the raw key) yielding the final quantum state:

$$\frac{1}{2}|00\rangle\langle 00|_{AB} \otimes |e_0\rangle\langle e_0| + \frac{1}{2}|11\rangle\langle 11|_{AB} \otimes |e_3\rangle\langle e_3|$$
$$+\frac{1}{2}|01\rangle\langle 01|_{AB} \otimes |e_1\rangle\langle e_1| + \frac{1}{2}|10\rangle\langle 10|_{AB} \otimes |e_2\rangle\langle e_2|$$

Call this state χ_{ABE}. We will make the usual assumption that the noise in the $\mathcal{B}$ basis, induced by E's attack, is symmetric: that is $\langle e_0|e_0\rangle = \langle e_3|e_3\rangle = 1-Q$ and $\langle e_1|e_1\rangle = \langle e_2|e_2\rangle = Q$. These parameters $\langle e_i|e_i\rangle$ can obviously be estimated by A and B; thus this symmetry condition can even be enforced. Note that, without this assumption, our analysis could still be carried out, though the algebra is not as amiable.

Assume, for the moment, that $Q > 0$ (we will consider the case $Q = 0$ later). Tracing out B, we may write χ_{ABE} as:

$$\chi_{AE} = (1-Q)\rho_{AE} + Q\sigma_{AE}, \tag{2}$$

where:

$$\rho_{AE} = \frac{1}{2}|0\rangle\langle 0|_A \otimes \frac{|e_0\rangle\langle e_0|}{1-Q} + \frac{1}{2}|1\rangle\langle 1|_A \otimes \frac{|e_3\rangle\langle e_3|}{1-Q} \tag{3}$$
$$\sigma_{AE} = \frac{1}{2}|0\rangle\langle 0|_A \otimes \frac{|e_1\rangle\langle e_1|}{Q} + \frac{1}{2}|1\rangle\langle 1|_A \otimes \frac{|e_2\rangle\langle e_2|}{Q}. \tag{4}$$

It is obvious that both ρ_{AE} and σ_{AE} are Hermitian semi-definite operators of unit trace. Before continuing, we require two lemmas which, though trivial to prove, we include for completeness:

Lemma 1. Given a finite dimensional Hilbert space $\mathcal{H} = \mathcal{H}_C \otimes \mathcal{H}_E$, let $\{|1\rangle_C, \cdots, |n\rangle_C\}$ be an orthonormal basis of $\mathcal{H}_C$. Consider the following density operator:

$$\rho = \sum_{i=1}^{n} p_i |i\rangle\langle i|_C \otimes \sigma_E^{(i)},$$

where $\sum p_i = 1$, $p_i \geq 0$, and each $\sigma_E^{(i)}$ is a Hermitian positive semi-definite operator of unit trace acting on $\mathcal{H}_E$. Then:

$$S(\rho) = H(p_1, \cdots, p_n) + \sum_{i=1}^{n} p_i S\left(\sigma_E^{(i)}\right).$$

Proof. See [9] for a proof. □

Lemma 2. Given a finite dimensional Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_E$ and the following density operators:

$$\rho_{AE} = p_0|0\rangle\langle 0|_A \otimes \rho_E^0 + p_1|1\rangle\langle 1|_A \otimes \rho_E^1$$
$$\sigma_{AE} = q_0|0\rangle\langle 0|_A \otimes \sigma_E^0 + q_1|1\rangle\langle 1|_A \otimes \sigma_E^1$$

$$\chi_{AE} = p_\rho \rho_{AE} + p_\sigma \sigma_{AE},$$

then the following is true:

$$S(A|E)_\chi \geq p_\rho S(A|E)_\rho + p_\sigma S(A|E)_\sigma \tag{5}$$

Proof. Let $\mathcal{H}_C$ be the two dimensional Hilbert space spanned by orthonormal basis $\{|X\rangle, |Y\rangle\}$ and let χ_{AEC} be the following density operator:

$$\chi_{AEC} = p_\rho |X\rangle\langle X| \otimes \rho_{AE} + p_\sigma |Y\rangle\langle Y| \otimes \sigma_{AE},$$

which acts on $\mathcal{H}_A \otimes \mathcal{H}_E \otimes \mathcal{H}_C$. Observe that $tr_C \chi_{AEC} = \chi_{AE}$. Due to the strong sub additivity of von Neumann entropy, it holds that: $S(A|E)_\chi \geq S(A|EC)_\chi$. We will show that:

$$S(A|EC)_\chi = p_\rho S(A|E)_\rho + p_\sigma S(A|E)_\sigma, \tag{6}$$

from which Equation 5 will follow. Of course $S(A|EC)_\chi = S(AEC)_\chi - S(EC)_\chi$. Applying Lemma 1 twice, we have:

$$\begin{aligned}S(AEC)_\chi &= h(p_\rho) + p_\rho S(AE)_\rho + p_\sigma S(AE)_\sigma\\ S(EC)_\chi &= h(p_\rho) + p_\rho S(E)_\rho + p_\sigma S(E)_\sigma.\end{aligned}$$

Thus:

$$\begin{aligned}S(A|EC)_\chi &= S(AEC)_\chi - S(EC)_\chi\\ &= p_\rho(S(AE)_\rho - S(E)_\rho)\\ &+ p_\sigma(S(AE)_\sigma - S(E)_\sigma)\\ &= p_\rho S(A|E)_\rho + p_\sigma S(A|E)_\sigma.\end{aligned}$$

□

Thus, from Lemma 2, we may compute a lower bound on $S(A|E)_\chi$ (and thus a lower bound on the key rate r). This is:

$$S(A|E)_\chi \geq (1-Q)\cdot S(A|E)_\rho + Q \cdot S(A|E)_\sigma.$$

We need now only compute the conditional entropy of the operators ρ_{AE} and σ_{AE} individually. It is clear that:

$$S(AE)_\rho = S(AE)_\sigma = h(1/2) = 1.$$

Now, tracing out A, yields:

$$\rho_E = \frac{1}{2(1-Q)}(|e_0\rangle\langle e_0| + |e_3\rangle\langle e_3|) \tag{7}$$

$$\sigma_E = \frac{1}{2Q}(|e_1\rangle\langle e_1| + |e_2\rangle\langle e_2|). \tag{8}$$

We must now compute $S(E)_\rho$ and $S(E)_\sigma$. To do so, we will need the eigenvalues of these two density operators. First consider ρ_E. Without loss of generality, we may write:

$$|e_0\rangle = z|E\rangle \ , \ \ |e_3\rangle = he^{i\theta}|E\rangle + d|I\rangle, \tag{9}$$

where $z, h, d \in \mathbb{R}$, $\langle E|E\rangle = \langle I|I\rangle = 1$, and $\langle E|I\rangle = 0$. Furthermore, we have the following:

$$z^2 = h^2 + d^2 = 1 - Q \tag{10}$$

$$hze^{i\theta} = \langle e_0|e_3\rangle \Rightarrow h^2z^2 = |\langle e_0|e_3\rangle|^2. \tag{11}$$

In this $\{|E\rangle, |I\rangle\}$ basis, we may write ρ_E as:

$$\rho_E = \frac{1}{2(1-Q)}\begin{pmatrix} z^2+h^2 & he^{i\theta}d \\ he^{-i\theta}d & d^2\end{pmatrix},$$

the eigenvalues of which are readily computed to be:

$$\lambda_\pm^\rho = \frac{1}{2} \pm \frac{\sqrt{(z^2+h^2-d^2)^2 + 4h^2d^2}}{4(1-Q)}$$

Using identities 10 and 11, we have:

$$\begin{aligned}\lambda_\pm^\rho &= \frac{1}{2} \pm \frac{\sqrt{4h^4 + 4h^2(z^2-h^2)}}{4(1-Q)}\\ &= \frac{1}{2} \pm \frac{\sqrt{h^2z^2}}{2(1-Q)} = \frac{1}{2} \pm \frac{|\langle e_0|e_3\rangle|}{2(1-Q)}.\end{aligned} \tag{12}$$

Similarly, we may compute the eigenvalues of the two-dimensional operator σ_E as:

$$\lambda_\pm^\sigma = \frac{1}{2} \pm \frac{|\langle e_1|e_2\rangle|}{2Q}. \tag{13}$$

(We are still assuming, for now, $Q > 0$.)

Thus, $S(E)_\rho = h(\lambda_+^\rho)$ and $S(E)_\sigma = h(\lambda_+^\sigma)$, and so:

$$\begin{aligned}S(A|E)_\chi &\geq (1-Q)(1-h(\lambda_+^\rho)) + Q(1-h(\lambda_+^\sigma))\\ &\geq 1 - (1-Q)\cdot h(\lambda_+^\rho) - Q\cdot h(\lambda_+^\sigma).\end{aligned}$$

It is trivial to show that $H(A|B) = h(Q)$. Thus, the key rate of this three-state protocol is lower bounded by:

$$\begin{aligned}r &= S(A|E)_\chi - H(A|B)\\ &\geq 1 - (1-Q)\cdot h(\lambda_+^\rho) - Q\cdot h(\lambda_+^\sigma) - h(Q).\end{aligned}$$

Note that, if $Q = 0$, then $|e_1\rangle \equiv |e_2\rangle \equiv 0$ and so these terms never show up in Equation 2. In this case, we may define λ_+^σ arbitrarily and the above key rate bound will still hold.

Therefore, to determine the key rate, A and B must estimate the quantities $|\langle e_0|e_3\rangle|$ and $|\langle e_1|e_2\rangle|$. These cannot be directly observed; however, by using the error rate in the $\mathcal{A}$ basis, along with mismatched measurement results, they may determine bounds on these two quantities. Before discussing how this is done, however, we mention one last critical detail. Note that λ_+^ρ and λ_+^σ are both greater than, or equal to, $1/2$. Note also that the binary entropy function $h(x)$ attains its maximum when $x = 1/2$ and on the interval $[1/2, 1]$ it is a decreasing function. Thus, if we find values λ^ρ and λ^σ, such that $1/2 \leq \lambda^\rho \leq \lambda_+^\rho$ and $1/2 \leq \lambda^\sigma \leq \lambda_+^\sigma$, then it will hold that $h(\lambda_+^\rho) \leq h(\lambda^\rho)$ (and similarly for σ). Thus, we have:

$$\begin{aligned}r &\geq 1 - (1-Q)\cdot h(\lambda_+^\rho) - Q\cdot h(\lambda_+^\sigma) - h(Q)\\ &\geq 1 - (1-Q)\cdot h(\lambda^\rho) - Q\cdot h(\lambda^\sigma) - h(Q).\end{aligned} \tag{14}$$

We will soon see that it is easier to bound the real parts of $\langle e_0|e_3\rangle$ and $\langle e_1|e_2\rangle$. Therefore, we will define:

$$\lambda^\rho = \frac{1}{2} + \frac{|Re\langle e_0|e_3\rangle|}{2(1-Q)} \geq \frac{1}{2}\ ,\ \lambda^\sigma = \frac{1}{2} + \frac{|Re\langle e_1|e_2\rangle|}{2Q} \geq \frac{1}{2}$$

(the same discussion before concerning the case when $Q = 0$ applies). It is clear that:

$$\begin{aligned}\lambda_+^\rho &= \frac{1}{2} + \frac{|\langle e_0|e_3\rangle|}{2(1-Q)} = \frac{1}{2} + \frac{\sqrt{Re^2\langle e_0|e_3\rangle + Im^2\langle e_0|e_3\rangle}}{2(1-Q)}\\ &\geq \frac{1}{2} + \frac{\sqrt{Re^2\langle e_0|e_3\rangle}}{2(1-Q)} = \lambda^\rho \geq \frac{1}{2},\end{aligned}$$

and similarly, $\lambda_+^\sigma \geq \lambda^\sigma \geq 1/2$. To evaluate our key rate bound in Equation 14, we therefore need to determine bounds on the real part only of $\langle e_0|e_3\rangle$ and $\langle e_1|e_2\rangle$.

A. Parameter Estimation

To estimate $Re\langle e_0|e_3\rangle$ and $Re\langle e_1|e_2\rangle$, we will consider, first, the noise in the $\mathcal{A}$ basis. To improve this bound, we will also consider measurement results from mismatched bases (results which are typically discarded). Before, continuing, let us introduce some notation. In particular, we will denote by

$\mathcal{R}_{i,j}$ to mean $Re\langle e_i|e_j\rangle$ (for $i,j \in \{0,1,2,3\}$. By $p_{x,y}$ we mean the probability that if A sends $|x\rangle$ (for $x \in \{0,1,a\}$), then, after E's attack, B measures $|y\rangle$ (for $y \in \{0,1,a,\bar{a}\}$). For instance, $p_{0,1} = \langle e_1|e_1\rangle = Q$. Finally, let $\beta = \sqrt{1-\alpha^2}$ (and so $|a\rangle = \alpha|0\rangle + \beta|1\rangle$).

Now, consider the quantity $p_{a,\bar{a}}$ which, to avoid confusion with $p_{a,a}$, we will also denote $Q_{\mathcal{A}}$. This represents the error in the A basis (note that, unlike in a four-state protocol, A and B cannot directly measure $p_{\bar{a},a}$). By linearity of U, we have (see Equation 1):

$$U|a\rangle = |0\rangle(\alpha|e_0\rangle + \beta|e_2\rangle) + |1\rangle(\alpha|e_1\rangle + \beta|e_3\rangle) \quad (15)$$

$$= |a\rangle(\alpha^2|e_0\rangle + \alpha\beta|e_2\rangle + \alpha\beta|e_1\rangle + \beta^2|e_3\rangle) + |\bar{a}\rangle(\beta\alpha|e_0\rangle + \beta^2|e_2\rangle - \alpha^2|e_1\rangle - \alpha\beta|e_3\rangle).$$

Thus:

$$\begin{aligned} Q_{\mathcal{A}} = {} & \alpha^2\beta^2(\langle e_0|e_0\rangle + \langle e_3|e_3\rangle) + \beta^4\langle e_2|e_2\rangle + \alpha^4\langle e_1|e_1\rangle \\ & + 2Re(\beta^3\alpha\langle e_0|e_2\rangle - \beta\alpha^3\langle e_0|e_1\rangle - \alpha^2\beta^2\langle e_0|e_3\rangle \\ & - \alpha^2\beta^2\langle e_1|e_2\rangle - \alpha\beta^3\langle e_2|e_3\rangle + \alpha^3\beta\langle e_1|e_3\rangle). \end{aligned} \quad (16)$$

Of course, α (and thus β) are public knowledge; also the quantities $\langle e_i|e_i\rangle$ can be estimated using the $\mathcal{B}$-basis noise. That leaves: $\mathcal{R}_{0,2}, \mathcal{R}_{0,1}, \mathcal{R}_{0,3}, \mathcal{R}_{1,2}, \mathcal{R}_{2,3}, \mathcal{R}_{1,3}$. Most of these, however, may be estimated using mismatched measurement results. Consider the quantity $p_{0,a}$. This is a value that would ordinarily be discarded as A and B used different bases; yet, this probability, which can be estimated by A and B, will lead to an estimate of $\mathcal{R}_{0,1}$. Indeed:

$$\begin{aligned} U|0\rangle &= |0,e_0\rangle + |1,e_1\rangle \\ &= |a\rangle(\alpha|e_0\rangle + \beta|e_1\rangle) + |\bar{a}\rangle(\beta e_0 - \alpha|e_1\rangle), \end{aligned}$$

and so:

$$\begin{aligned} p_{0,a} &= \alpha^2\langle e_0|e_0\rangle + \beta^2\langle e_1|e_1\rangle + 2\alpha\beta\mathcal{R}_{0,1} \\ \Rightarrow \mathcal{R}_{0,1} &= \frac{p_{0,a} - \alpha^2(1-Q) - \beta^2 Q}{2\alpha\beta}. \end{aligned} \quad (17)$$

On observing Q, along with $p_{0,a}$, A and B immediately may estimate $\mathcal{R}_{0,1}$. Similarly, they may use $p_{1,a}$ to estimate $\mathcal{R}_{2,3}$:

$$\mathcal{R}_{2,3} = \frac{p_{1,a} - \alpha^2 Q - \beta^2(1-Q)}{2\alpha\beta}. \quad (18)$$

When $\alpha = 1/\sqrt{2}$ (as dictated by the original three-state protocol [3], [4]), A and B need not estimate $\mathcal{R}_{0,2}$ and $\mathcal{R}_{1,3}$ due to the fact that unitarity of U (which imposes the condition $\mathcal{R}_{0,2} = -\mathcal{R}_{1,3}$) will force the terms to cancel in Equation 16. For other values of α, however, an estimate will be necessary and it may be accomplished by considering $p_{a,0}$. From Equation 15 this is:

$$\begin{aligned} p_{a,0} &= \alpha^2\langle e_0|e_0\rangle + \beta^2\langle e_2|e_2\rangle + 2\alpha\beta\mathcal{R}_{0,2} \\ \Rightarrow \mathcal{R}_{0,2} &= \frac{p_{a,0} - \alpha^2(1-Q) - \beta^2 Q}{2\alpha\beta}. \end{aligned} \quad (19)$$

Since unitarity of U forces the relation $\mathcal{R}_{1,3} = -\mathcal{R}_{0,2}$, A and B now have estimates of all quantities in Equation 16 except for $\mathcal{R}_{0,3}$ and $\mathcal{R}_{1,2}$. However, the Cauchy-Schwarz inequality forces $\mathcal{R}_{1,2} \in [-Q,Q]$. This, combined with Equation 16, allow the users to bound $\mathcal{R}_{0,3}$ and thus evaluate r (one must simply find the minimum r over all $\mathcal{R}_{1,2} \in [-Q,Q]$). For our evaluations, we performed this optimization numerically; however finding an analytic solution would be straight-forward. Finally, as the protocol is permutation invariant, the results of [10], [11] apply and thus our key rate bound holds even against the most general of attacks (not only collective).

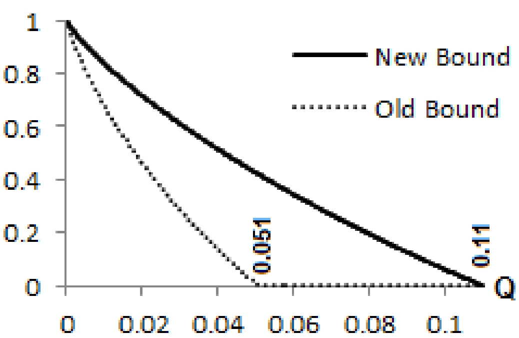


Fig. 1: Comparing our new key rate bound (for any $\alpha \in (0,1)$) with the old one from [4] assuming a symmetric attack.

B. *Evaluation*

To evaluate our key rate bound, we will first consider the case that E's attack is symmetric in that it may be modeled as a depolarization channel (this is a common assumption in QKD protocol security proofs; in fact, it could even be enforced by the users). Consider a depolarization channel with parameter Q: $\mathcal{E}_Q(\rho) = (1-2Q)\rho + QI$ where I is the two-dimensional identity operator. Then, if A sends $|i\rangle \in \mathcal{B}$, the probability of measuring $|1-i\rangle$ is Q as desired. Thus $\langle e_1|e_1\rangle = \langle e_2|e_2\rangle = Q$. Furthermore, if A sends $|0\rangle$, then the qubit's state when it arrives at B's lab is:

$$\mathcal{E}_Q(|0\rangle\langle 0|) = (1-2Q)|0\rangle\langle 0| + Q(|0\rangle\langle 0| + |1\rangle\langle 1|),$$

and so we have $p_{0,a} = (1-2Q)\alpha^2 + Q$ (note that if $\alpha = 1/\sqrt{2}$ and thus $|a\rangle = |+\rangle$, we have $p_{0,+} = 1/2$ as expected). Using this value in Equation 17 yields:

$$\begin{aligned} \mathcal{R}_{0,1} &= \frac{(1-2Q)\alpha^2 + Q - \alpha^2(1-Q) - \beta^2 Q}{2\alpha\beta} \\ &= \frac{\alpha^2 - 2\alpha^2 Q + Q - \alpha^2 + \alpha^2 Q - (1-\alpha^2)Q}{2\alpha\beta} = 0. \end{aligned}$$

Similarly, we find $\mathcal{R}_{2,3} = 0$.

If $\alpha = 1/\sqrt{2}$, we are done; otherwise, we must consider $p_{a,0}$. If A sends $|a\rangle$, then the qubit arriving at B's lab is:

$$\mathcal{E}_Q(|a\rangle\langle a|) = (1-2Q)|a\rangle\langle a| + Q(|a\rangle\langle a| + |\bar{a}\rangle\langle\bar{a}|), \quad (20)$$

from which it is clear that $p_{a,0} = (1-2Q)\alpha^2 + Q$. Substituting into Equation 19 we find that $\mathcal{R}_{0,2} = 0$. Thus also $\mathcal{R}_{1,3} = -\mathcal{R}_{0,2} = 0$.

Substituting this into Equation 16 and solving for $\mathcal{R}_{0,3}$ yields the expression:

$$\mathcal{R}_{0,3} = \frac{2\alpha^2\beta^2(1-Q) + (\beta^4+\alpha^4)Q - Q_{\mathcal{A}} - 2\alpha^2\beta^2\mathcal{R}_{1,2}}{2\alpha^2\beta^2}$$
$$= 1 - 2Q + \frac{Q - Q_{\mathcal{A}}}{2\alpha^2\beta^2} - \mathcal{R}_{1,2}, \quad (21)$$

where, above, we used the fact that: $1 = (\alpha^2+\beta^2)^2 = \alpha^4 + 2\alpha^2\beta^2 + \beta^4 \Rightarrow \alpha^4 + \beta^4 = 1 - 2\alpha^2\beta^2$.

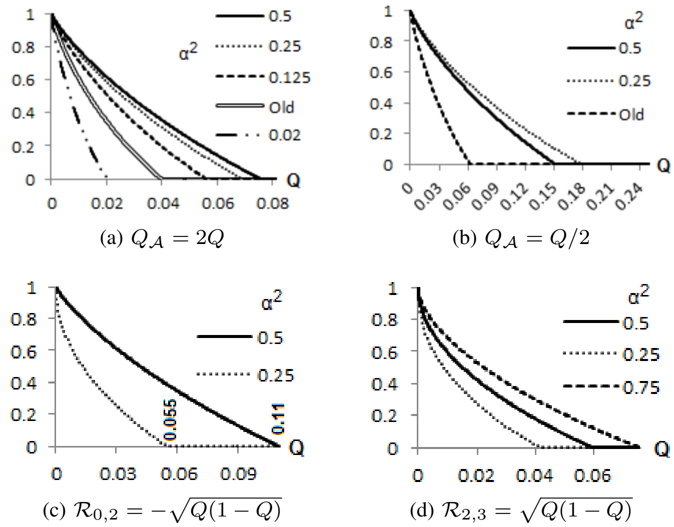
Finally, from Equation 20, we find $Q_{\mathcal{A}} = Q$ and so: $\mathcal{R}_{0,3} = 1 - 2Q - \mathcal{R}_{1,2}$. Note that, under this (entirely enforceable) assumption of a depolarization channel, the parameters α and β do not show up in the above expression; they therefore do not appear in the evaluation of r. Thus, in this symmetric case, the value of α is irrelevant (at least in the perfect qubit, asymptotic scenario - we make no claims about its relevance in more practical scenarios; it also is relevant in non-symmetric scenarios as we soon show).

To evaluate the key rate r, we must now simply minimize r over all $\mathcal{R}_{1,2} \in [-Q, Q]$. We performed this computation numerically, resulting in the key rate shown in Figure 1. Notice that the key rate is positive for all $Q \leq 11\%$; this is exactly the tolerance supported by the four state BB84 protocol. Compare this with the original lower-bound from [4] which only remained positive for $Q \leq 5.1\%$. In fact, we found that, in this symmetric case, our new key rate bound agrees exactly with that of the four-state BB84 protocol $1-h(Q)-h(Q_X) = 1-2h(Q)$ where Q_X is the error in the X ($\{|\pm\rangle\}$) basis [2]. Furthermore, this is true for any $\alpha \in (0,1)$.

While α does not appear when E's attack is symmetric; this of course is not true in other cases. We considered the effect of various settings for α when $Q_{\mathcal{A}} = 2Q$ (Figure 2 (a)) and $Q_{\mathcal{A}} = Q/2$ (Figure 2 (b)); we also plotted the old key rate bound from [4] for comparison. In Figure 2 (c) and (d) we considered the case when $p_{a,0}$ and $p_{1,a}$ are such that $\mathcal{R}_{0,2}$ and $\mathcal{R}_{2,3}$ are non-zero. As α is a parameter that must be set before the protocol runs, it seems $\alpha = 1/\sqrt{2}$ is a good compromise (other settings can do better or worse depending on the attack used).

IV. Closing Remarks

We have derived a new proof of security and key-rate bound for a three state BB84 protocol - a protocol where A sends only $|0\rangle$, $|1\rangle$, or $|a\rangle = \alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle$. Furthermore we have shown that this new key rate bound, in addition to the use of mismatched measurement outcomes, can tolerate the same maximal noise level as the four state BB84 (i.e., the key rate is positive for all $Q \leq 11\%$) in the asymptotic scenario. The technique we used in our proof - especially our use of mismatched measurement outcomes in this manner to estimate $\mathcal{R}_{i,j}$ despite the lack of the statistic $p_{\bar{a},a}$ - may hold application in the analysis of other QKD protocols where one (or both) party is limited. This is a subject we intend to investigate in the near future. Also, we restricted our attention to real α; though we suspect the result is the same for $\alpha \in \mathbb{C}$, it might be worth looking into in further detail. Finally, we only considered the asymptotic scenario; it would be useful, and important, to consider the finite key setting.



(a) $Q_{\mathcal{A}} = 2Q$ (b) $Q_{\mathcal{A}} = Q/2$
(c) $\mathcal{R}_{0,2} = -\sqrt{Q(1-Q)}$ (d) $\mathcal{R}_{2,3} = \sqrt{Q(1-Q)}$

Fig. 2: Showing how α^2 affects the key rate in various noise scenarios. Also comparing with the "Old" bound from [4] in (a) and (b). (a): when the $\mathcal{A}$ basis noise ($Q_{\mathcal{A}}$) is twice the $\mathcal{B}$ basis noise (Q). (b): when the $\mathcal{A}$ noise is half. (c): When the noise in both bases are equal, but $p_{a,0}$ is such that $\mathcal{R}_{0,2} = -\sqrt{Q(1-Q)}$ (the largest negative it could be). (d): Like (c), but now $\mathcal{R}_{2,3} = \sqrt{Q(1-Q)}$ (while $\mathcal{R}_{0,2} = 0$).

References

[1] 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.

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

[3] Chi-Hang Fred Fung and Hoi-Kwong Lo. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. *Phys. Rev. A*, 74:042342, Oct 2006.

[4] Cyril Branciard, Nicolas Gisin, Norbert Lutkenhaus, and Valerio Scarani. Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. *Quantum Information & Computation*, 7(7):639–664, 2007.

[5] 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.

[6] Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu. Tomography increases key rates of quantum-key-distribution protocols. *Physical Review A*, 78(4):042316, 2008.

[7] Stephen M Barnett, Bruno Huttner, and Simon JD Phoenix. Eavesdropping strategies and rejected-data protocols in quantum cryptography. *Journal of Modern Optics*, 40(12):2501–2513, 1993.

[8] Walter O Krawec. Security of a semi-quantum protocol where reflections contribute to the secret key. *arXiv preprint arXiv:1510.07181*, 2015.

[9] Walter O. Krawec. Security proof of a semi-quantum key distribution protocol. In *Information Theory (ISIT), 2015 IEEE International Symposium on*, pages 686–690, June 2015.

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

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