Asymptotic Analysis of a Three State Quantum Cryptographic Protocol

Walter O. Krawec

walter.krawec@gmail.com

Iona College
Computer Science Department
New Rochelle, NY USA

IEEE ISIT July, 2016

Quantum Key Distribution (QKD)

1. Allows two users - Alice (A) and Bob (B) - to establish a shared secret key
2. Secure against an all powerful adversary
   - Does not require any computational assumptions
   - Attacker bounded only by the laws of physics
   - Something that is not possible using classical means only
3. Accomplished using a *quantum communication channel*

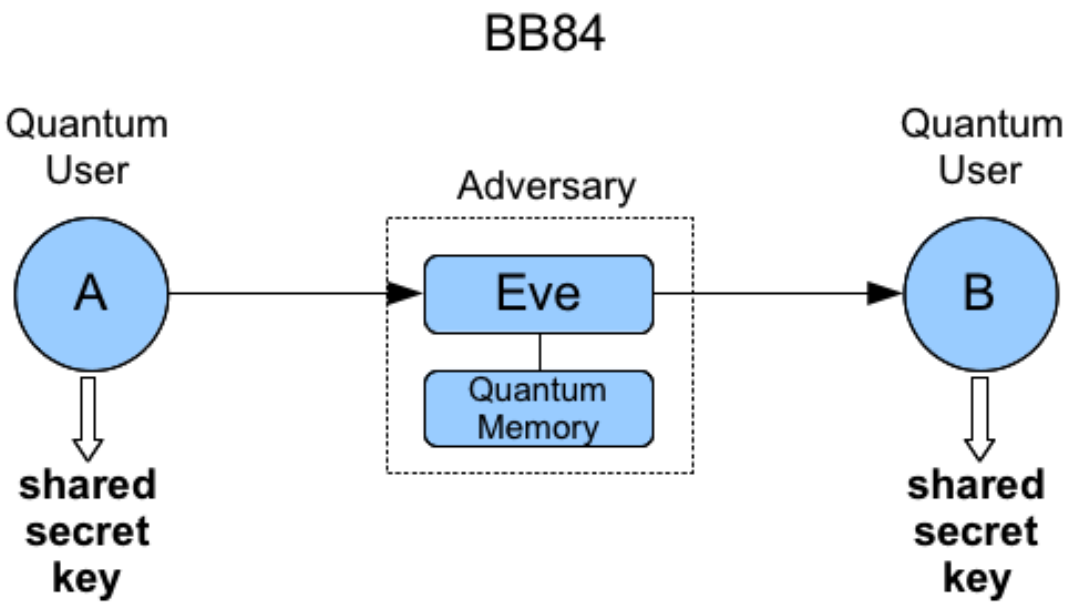

Figure: Typical QKD Setup

Three-State BB84

1. In this work, we consider a three-state variant of the BB84 protocol first introduced in [1, 2]
2. We consider a generalized version of the protocol.
3. The quantum communication stage is as follows:
   - A chooses to send a state $|0\rangle$, $|1\rangle$, or $|a\rangle = \alpha |0\rangle + \sqrt{1-\alpha^2}\,|1\rangle$, for $\alpha \in (0,1)$, with probability $p/2, p/2$, and $1-p$ respectively.
   - B chooses to measure in the $Z = \{|0\rangle, |1\rangle\}$ basis or the $\mathcal{A} = \{|a\rangle, |\bar{a}\rangle\}$ basis.
4. Notes:
   1. When $\alpha = 1/\sqrt{2}$ (thus $|a\rangle = |+\rangle$ and $|\bar{a}\rangle = |-\rangle$) this is exactly the three-state protocol considered in [1, 2]
   2. To improve efficiency, A and B may choose p close to one.

Three-State BB84

1. In this work, we consider a three-state variant of the BB84 protocol first introduced in [1, 2]
2. We consider a generalized version of the protocol.
3. The quantum communication stage is as follows:
   - A chooses to send a state $|0\rangle$, $|1\rangle$, or $|a\rangle = \alpha |0\rangle + \sqrt{1-\alpha^2}\,|1\rangle$, for $\alpha \in (0,1)$, with probability $p/2, p/2$, and $1-p$ respectively.
   - B chooses to measure in the $Z = \{|0\rangle, |1\rangle\}$ basis or the $\mathcal{A} = \{|a\rangle, |\bar{a}\rangle\}$ basis.
4. Notes:
   1. When $\alpha = 1/\sqrt{2}$ (thus $|a\rangle = |+\rangle$ and $|\bar{a}\rangle = |-\rangle$) this is exactly the three-state protocol considered in [1, 2]
   2. To improve efficiency, A and B may choose p close to one.

Mismatched Measurement Outcomes

1. Note that parties cannot measure the probability of E's attack flipping a $|\bar{a}\rangle$ to a $|a\rangle$ (unlike the "full" four-state BB84 protocol [3])
2. However, we will use *mismatched measurement outcomes* to overcome this limitation
3. Let $p_{i,j}$, for $i, j \in \{0, 1, a\}$ be the probability that, if A sends $|i\rangle$ then B measures $|j\rangle$ (after E's attack).
4. We will utilize all statistics including those of the form $p_{0,a}, p_{1,a}$, and $p_{a,j}$ to derive our key-rate expression
   - I.e., we will not discard measurement results when A and B choose different bases.
5. Doing so allows us to prove that the three-state BB84 has the same maximally tolerated error rate as the full four-state BB84 (i.e., 11%).

Related Work

We are not the first to show mismatched measurement results are useful:

1. In 1993, Barnett et al., [4] used them to detect an attacker with greater probability for measure-and-resend attacks
2. In [5] (2008) they were shown to produce superior key-rates for the four-state and six-state BB84 for certain quantum channels
3. They have been used in the analysis of certain device independent protocols [6].

Related Work (continued)

In [7] mismatched measurement results were used to analyze the generalized three-state BB84 protocol we consider in our paper, however:

1. We derive an alternative approach which can also be applied to several other protocols (as we comment on later). Thus, we also provide an alternative proof of the result in [7] that this three-state protocol can withstand up to 11% error if a symmetric attack is used.
2. Furthermore, in our work we derive a key-rate expression for any arbitrary quantum channel, parameterized by all statistics $p_{i,j}$ (only symmetric attacks were considered in [7]).

Key Rate Bound

QKD Security

1. After the quantum communication stage and parameter estimation, A and B hold an N-bit *raw key*
2. They then run an error correcting protocol and privacy amplification protocol
3. Result is an $\ell(N)$-bit secret key
4. We compute a lower-bound on the key-rate of this three-state protocol in the asymptotic scenario:

$$r = \lim_{N \to \infty} \frac{\ell(N)}{N}$$

5. We first consider *collective attacks* and so by [8, 9]:

$$r = \inf S(A|E) - H(A|B).$$

Collective Attack

1. Without loss of generality, we may model E's collective attack as a unitary U, acting on the qubit and E's private memory.
2. Furthermore, we may assume E's memory is cleared to some pure "zero" state.
3. Thus:

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

Joint Quantum State

1. To compute $r = \inf S(A|E) - H(A|B)$, we need to model the joint-quantum state, held by A, B, and E, conditioning on the event A and B use this iteration for their raw key. I.e.,:
   - A sends either $|0\rangle$ or $|1\rangle$ and B measures in the $Z = \{|0\rangle, |1\rangle\}$ basis.
2. This state is easily computed:

$$\rho_{ABE} = \frac{1}{2}(|00\rangle\langle 00|_{AB} \otimes |e_0\rangle\langle e_0| + |11\rangle\langle 11|_{AB} \otimes |e_3\rangle\langle e_3| + |01\rangle\langle 01|_{AB} \otimes |e_1\rangle\langle e_1| + |10\rangle\langle 10|_{AB} \otimes |e_2\rangle\langle e_2|).$$

$$\Rightarrow \rho_{AE} = \frac{1}{2}(|0\rangle\langle 0|_{A} \otimes [|e_0\rangle\langle e_0| + |e_1\rangle\langle e_1|] + |1\rangle\langle 1|_{A} \otimes [|e_2\rangle\langle e_2| + |e_3\rangle\langle e_3|]).$$

Joint Quantum State

1. To compute $r = \inf S(A|E) - H(A|B)$, we need to model the joint-quantum state, held by A, B, and E, conditioning on the event A and B use this iteration for their raw key. I.e.,:
   - A sends either $|0\rangle$ or $|1\rangle$ and B measures in the $Z = \{|0\rangle, |1\rangle\}$ basis.
2. This state is easily computed:

$$\rho_{ABE} = \frac{1}{2}(|00\rangle\langle 00|_{AB} \otimes |e_0\rangle\langle e_0| + |11\rangle\langle 11|_{AB} \otimes |e_3\rangle\langle e_3| + |01\rangle\langle 01|_{AB} \otimes |e_1\rangle\langle e_1| + |10\rangle\langle 10|_{AB} \otimes |e_2\rangle\langle e_2|).$$

$$\Rightarrow \rho_{AE} = \frac{1}{2}(|0\rangle\langle 0|_{A} \otimes [|e_0\rangle\langle e_0| + |e_1\rangle\langle e_1|] + |1\rangle\langle 1|_{A} \otimes [|e_2\rangle\langle e_2| + |e_3\rangle\langle e_3|]).$$

Computing $S(A|E)$

Lemma

Given a density operator:

$$\rho_{AE} = \frac{1}{N}(|0\rangle\langle 0|_A \otimes (|e_0\rangle\langle e_0|_E + |e_1\rangle\langle e_1|_E) + |1\rangle\langle 1|_A \otimes (|e_2\rangle\langle e_2|_E + |e_3\rangle\langle e_3|_E)),$$

then:

$$S(A|E) \geq \frac{N_0 + N_3}{N}\left[h\left(\frac{N_0}{N_0 + N_3}\right) - h(\lambda_{0,3})\right] + \frac{N_1 + N_2}{N}\left[h\left(\frac{N_1}{N_1 + N_2}\right) - h(\lambda_{1,2})\right],$$

where $N_i = \langle e_i|e_i\rangle$ *and:*

$$\lambda_{i,j} = \frac{1}{2} + \frac{\sqrt{(N_i - N_j)^2 + 4Re^2\langle e_i|e_j\rangle}}{2(N_i + N_j)}.$$

Parameter Estimation

$$U : |0\rangle \mapsto |0, e_0\rangle + |1, e_1\rangle \qquad |1\rangle \mapsto |0, e_2\rangle + |1, e_3\rangle$$

1. Clearly, we may measure $N_i = \langle e_i | e_i \rangle$
2. We therefore need only $Re\,\langle e_0 | e_3 \rangle$ and $Re\,\langle e_1 | e_2 \rangle$ (for $\lambda_{0,3}$ and $\lambda_{1,2}$)

Parameter Estimation (continued)

1. Linearity of E's attack operator U implies:

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

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

Let $\mathcal{R}_{i,j} = Re\langle e_i|e_j\rangle$. Then:

$$1 - p_{a,a} = Q_{\mathcal{A}} = \alpha^2\beta^2(N_0 + N_3) + \beta^4 N_2 + \alpha^4 N_1$$
$$+ 2(\beta^3\alpha\mathcal{R}_{0,2} - \beta\alpha^3\mathcal{R}_{0,1} - \alpha^2\beta^2\mathcal{R}_{0,3}$$
$$- \alpha^2\beta^2\mathcal{R}_{1,2} - \alpha\beta^3\mathcal{R}_{2,3} + \alpha^3\beta\mathcal{R}_{1,3}).$$

Parameter Estimation (continued)

1. Linearity of E's attack operator U implies:

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

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

Let $\mathcal{R}_{i,j} = Re\langle e_i|e_j\rangle$. Then:

$$1 - p_{a,a} = Q_{\mathcal{A}} = \alpha^2\beta^2(N_0 + N_3) + \beta^4 N_2 + \alpha^4 N_1$$
$$+ 2(\beta^3\alpha\mathcal{R}_{0,2} - \beta\alpha^3\mathcal{R}_{0,1} - \alpha^2\beta^2\boxed{\mathcal{R}_{0,3}}$$
$$- \alpha^2\beta^2\boxed{\mathcal{R}_{1,2}} - \alpha\beta^3\mathcal{R}_{2,3} + \alpha^3\beta\mathcal{R}_{1,3}).$$

Mismatched Measurement Outcomes

1. We may determine $\mathcal{R}_{0,1}, \mathcal{R}_{2,3}, \mathcal{R}_{0,2}, \mathcal{R}_{1,3}$ using mismatched measurement outcomes.
2. Consider $p_{0,a}$ - normally discarded due to inconsistent basis choice. But:

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

and so:

$$\begin{aligned} p_{0,a} &= \alpha^2 \langle e_0|e_0\rangle + \beta^2 \langle e_1|e_1\rangle + 2\alpha\beta\mathcal{R}_{0,1} \\ \Rightarrow \mathcal{R}_{0,1} &= \frac{p_{0,a} - \alpha^2 N_0 - \beta^2 N_1}{2\alpha\beta}. \end{aligned}$$

Mismatched Measurement Outcomes

Similarly, A and B may estimate:

$$\mathcal{R}_{0,1} = \frac{p_{0,a} - \alpha^2 N_0 - \beta^2 N_1}{2\alpha\beta}$$

$$\mathcal{R}_{2,3} = \frac{p_{1,a} - \alpha^2 N_2 - \beta^2 N_3}{2\alpha\beta}$$

$$\mathcal{R}_{0,2} = \frac{p_{a,0} - \alpha^2 N_0 - \beta^2 N_2}{2\alpha\beta}$$

$$\mathcal{R}_{1,3} = -\mathcal{R}_{0,2}$$

$$|\mathcal{R}_{1,2}| \leq \sqrt{N_1 N_2}$$

Key Rate Bound

1. Thus, mismatched measurements are used to determine $\mathcal{R}_{0,1}, \mathcal{R}_{2,3}, \mathcal{R}_{0,2}$, and $\mathcal{R}_{1,3}$.
2. From this, we optimize over all $|\mathcal{R}_{1,2}| \leq \sqrt{N_1 N_2}$ and use the expression for $Q_{\mathcal{A}}$ to determine an estimate of $\mathcal{R}_{0,3}$
3. This gives us a lower-bound on $S(A|E)$.

$$\begin{aligned} 1 - p_{a,a} = Q_{\mathcal{A}} = {} & \alpha^2\beta^2(N_0 + N_3) + \beta^4 N_2 + \alpha^4 N_1 \\ & + 2(\beta^3\alpha\mathcal{R}_{0,2} - \beta\alpha^3\mathcal{R}_{0,1} - \alpha^2\beta^2\mathcal{R}_{0,3} \\ & - \alpha^2\beta^2\mathcal{R}_{1,2} - \alpha\beta^3\mathcal{R}_{2,3} + \alpha^3\beta\mathcal{R}_{1,3}). \end{aligned}$$

Key Rate Bound (continued)

1. Computing $H(A|B)$ is easy given observed statistics $p_{i,j}$ for $i, j \in \{0, 1\}$
2. We thus computed a lower-bound on the key-rate of this protocol as a function of multiple channel statistics
3. Since we have permutation invarience, this rate holds against general attacks in the asymptotic scenario [10]

Evaluation

Evaluation

1. To evaluate our bound, we will consider a symmetric channel; i.e., E's attack may be modeled as a depolarization channel:

$$\mathcal{E}_Q(\rho) = (1 - 2Q)\rho + QI$$

2. In this case, we have:

$$p_{0,1} = p_{1,0} = Q = N_1 = N_2$$
$$p_{1,1} = p_{0,0} = 1 - Q = N_0 = N_3$$

From which our key rate bound simplifies to:

$$r \geq \underbrace{(1 - Q)[1 - h(\lambda_C)] + Q[1 - h(\lambda_W)]}_{S(A|E) \text{ from Lemma}} - \underbrace{h(Q)}_{H(A|B)}$$

where:

$$\lambda_C = \frac{1}{2} + \frac{|\mathcal{R}_{0,3}|}{2(1 - Q)} \qquad \lambda_W = \frac{1}{2} + \frac{|\mathcal{R}_{1,2}|}{2Q}$$

Evaluation (continued)

1. If A sends $|0\rangle$, the qubit arriving at B's lab is:

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

   From which we have:

$$p_{0,a} = (1-Q)\alpha^2 + Q\beta^2$$

   (Note if $\alpha = 1/\sqrt{2}$, then $p_{0,a} = 1/2$.)

2. Trivial algebra shows:

$$\mathcal{R}_{0,1} = \frac{p_{0,a} - \alpha^2 N_0 - \beta^2 N_1}{2\alpha\beta} = 0$$

Evaluation (continued)

1. Similar algebra shows:

$$\mathcal{R}_{0,1} = \frac{p_{0,a} - \alpha^2 N_0 - \beta^2 N_1}{2\alpha\beta} = 0$$

$$\mathcal{R}_{2,3} = \frac{p_{1,a} - \alpha^2 N_2 - \beta^2 N_3}{2\alpha\beta} = 0$$

$$\mathcal{R}_{0,2} = \frac{p_{a,0} - \alpha^2 N_0 - \beta^2 N_2}{2\alpha\beta} = 0$$

$$\mathcal{R}_{1,3} = -\mathcal{R}_{0,2} = 0$$

$$|\mathcal{R}_{1,2}| \leq \sqrt{N_1 N_2} = Q$$

Evaluation (continued)

1. Using this, we may conclude:

$$\begin{aligned} 1 - p_{a,a} = Q_{\mathcal{A}} = \alpha^2\beta^2(N_0 + N_3) + \beta^4 N_2 + \alpha^4 N_1 \\ + 2(\beta^3\alpha\mathcal{R}_{0,2} - \beta\alpha^3\mathcal{R}_{0,1} - \alpha^2\beta^2\mathcal{R}_{0,3} \\ - \alpha^2\beta^2\mathcal{R}_{1,2} - \alpha\beta^3\mathcal{R}_{2,3} + \alpha^3\beta\mathcal{R}_{1,3}) \end{aligned}$$

$$\Rightarrow \mathcal{R}_{0,3} = 1 - 2Q + \frac{Q - Q_{\mathcal{A}}}{2\alpha^2\beta^2} - \mathcal{R}_{1,2}$$

Evaluation (continued)

1. Using this, we may conclude:

$$\begin{aligned} 1 - p_{a,a} = Q_{\mathcal{A}} &= \alpha^2\beta^2(N_0 + N_3) + \beta^4 N_2 + \alpha^4 N_1 \\ &+ 2(\beta^3\alpha\mathcal{R}_{0,2} - \beta\alpha^3\mathcal{R}_{0,1} - \alpha^2\beta^2\mathcal{R}_{0,3} \\ &- \alpha^2\beta^2\mathcal{R}_{1,2} - \alpha\beta^3\mathcal{R}_{2,3} + \alpha^3\beta\mathcal{R}_{1,3}) \end{aligned}$$

$$\Rightarrow \mathcal{R}_{0,3} = 1 - 2Q + \frac{Q - Q_{\mathcal{A}}}{2\alpha^2\beta^2} - \mathcal{R}_{1,2}$$

$$= 1 - 2Q - \mathcal{R}_{1,2}$$

Evaluation (continued)

1. Thus, to compute the key-rate, one must optimize over $\mathcal{R}_{1,2} \in [-Q, Q]$.
2. Note also that this depolarization channel example is entirely enforceable.

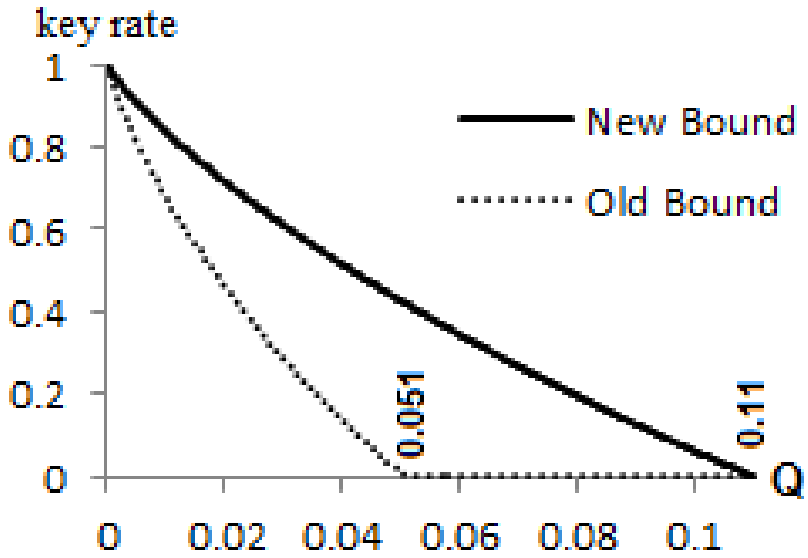

Figure: Comparing our new key rate bound (for any $\alpha \in (0, 1)$) with the one from [2] (which did not use mismatched measurement outcomes).

Evaluation (continued)

1. This shows the three-state protocol is as secure as the four-state BB84, providing an alternative proof to the one in [7]
2. However, our key-rate expression is very general and works in asymmetric channels...

Evaluation: Asymmetric Channel

key-rate	.628	.093	.008	.136	.059
$p_{0,1}$	.075	.157	.081	.159	.262
$p_{1,0}$	.009	.135	.265	.045	.050
$p_{a,\bar{a}}$	.024	.057	.081	.120	.098
$p_{0,a}$	.581	.321	.320	.403	.611
$p_{1,a}$	.419	.675	.659	.526	.343
$p_{a,0}$	.389	.649	.732	.429	.261

Table: Evaluating our key-rate bound on some randomly generated asymmetric channels.

Recent and Future Work

Recent and Future Work

1. Adding a fourth state $|b\rangle = \beta\,|0\rangle + i\sqrt{1-\beta^2}\,|1\rangle$ to the parameter estimation process allows A and B to estimate $\mathcal{R}_{1,2}$ and $\mathcal{R}_{0,3}$ directly:

$$\mathcal{R}_{0,3} = 1 - p_{a,\bar{a}} - p_{b,\bar{b}} - \frac{1}{2}\Big(\overbrace{\mathcal{R}_{0,1} + \mathcal{I}_{0,1} + \mathcal{R}_{2,3} + \mathcal{I}_{2,3}}^{\text{mismatched measurement outcomes}}\Big).$$

$$\mathcal{R}_{1,2} = p_{b,\bar{b}} - p_{a,\bar{a}} + \frac{1}{2}\Big(\underbrace{\mathcal{I}_{0,1} - \mathcal{R}_{0,1} + \mathcal{I}_{2,3} - \mathcal{R}_{2,3}}_{\text{mismatched measurement outcomes}}\Big)$$

2. By adding this extra state (and measuring in the $\mathcal{B} = \{|b\rangle, |\bar{b}\rangle\}$ basis), this four-state BB84 can tolerate the same level of noise as the full six-state BB84.

Recent and Future Work

1. Our method also extends easily to other QKD protocols, both one-way and two-way protocols

New Work: Extended B92

1. We considered the Extended B92 protocol [11]
2. Here, Alice encodes a 0 and 1 with a $|0\rangle$ and $|a\rangle$ respectively
3. Other states are used for parameter estimation

α	0	0.342	0.643	0.939	0.985
Old Bound From [11]	11%	9.3%	5.7%	1%	0.27%
New Bound Using Ψ_3	11%	9.97%	7.8%	3.8%	2.05%
New Bound using Ψ_4	12.6%	11.9%	10.2%	5.31%	2.85%

$$\Psi_3 = \{|0\rangle, |1\rangle, |a\rangle\} \qquad \Psi_4 = \{|0\rangle, |1\rangle, |a\rangle, |b\rangle\}$$

Optimized QKD

1. Alice and Bob use mismatched measurement outcomes to establish $\mathcal{R}_{i,j}$ as discussed.
2. They then choose optimal states to prepare and measure in.
3. I.e., Alice sends $|\psi_0\rangle = \alpha_s |0\rangle + \sqrt{1-\alpha_s^2}\,|1\rangle$ to encode a 0 and $|\psi_1\rangle = \beta_s |0\rangle + \sqrt{1-\beta_s^2}\,|1\rangle$ to encode a 1.
4. If Bob measures $|\phi_0\rangle = \alpha_r |0\rangle + \sqrt{1-\alpha_r^2}\,|1\rangle$ or $|\phi_1\rangle = \beta_r |0\rangle + \sqrt{1-\beta_r^2}\,|1\rangle$ his key bit is 0 or 1 respectively.

Optimized QKD

Ψ_4 – BB84's key-rate	.349	0.001	0	.265
Optimized key-rate	.349	0.001	.038	.307
Optimized (α_s, β_s)	$(1, 0)$	$(1, 0)$	$(-1, .23)$	$(.23, -1)$
Optimized (α_r, β_r)	$(1, 0)$	$(1, 0)$	$(-.94, .02)$	$(-.97, -.01)$
$p_{0,1}$	.07	.126	.138	.079
$p_{1,0}$	.07	.126	.191	.120
$p_{a,\bar{a}}$	.07	.126	.091	.034
$p_{b,\bar{b}}$	.07	.126	.058	.063
$p_{0,a}$	.5	.5	.523	.526
$p_{1,a}$	.5	.5	.623	.544
$p_{a,0}$	.5	.5	.566	.523
$p_{0,b}$	.5	.5	.435	.334
$p_{1,b}$	.5	.5	.505	.623
$p_{b,0}$	.5	.5	.419	.396

New Work: Semi-Quantum Protocol

1. We also considered the *semi-quantum* protocol of Boyer et al. [12] which uses a two-way quantum channel: $A \rightarrow B \rightarrow A$.
2. B can only measure in the $Z = \{|0\rangle, |1\rangle\}$ basis.
3. Our method provided a superior key-rate bound to prior work in [13]

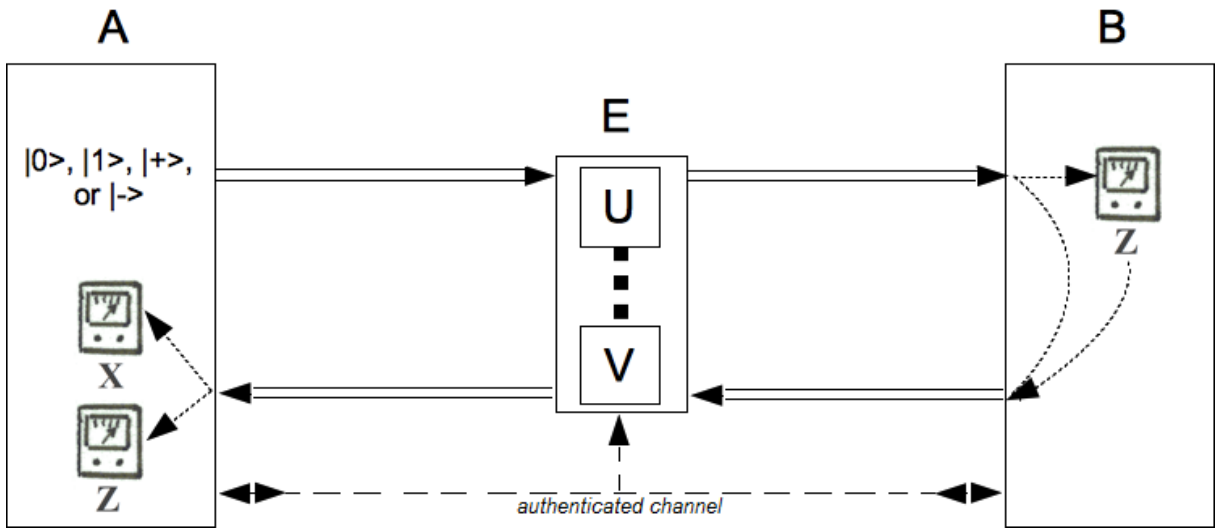

Figure: Boyer et al.'s SQKD Protocol [12]

SQKD - Evaluation

	Independent	Correlated
Old Bound From [13]	4.57%	5.34%
New Bound Using 2 Bases	5.4%	7.4%
New Bound Using 3 Bases	6.7%	8.76%

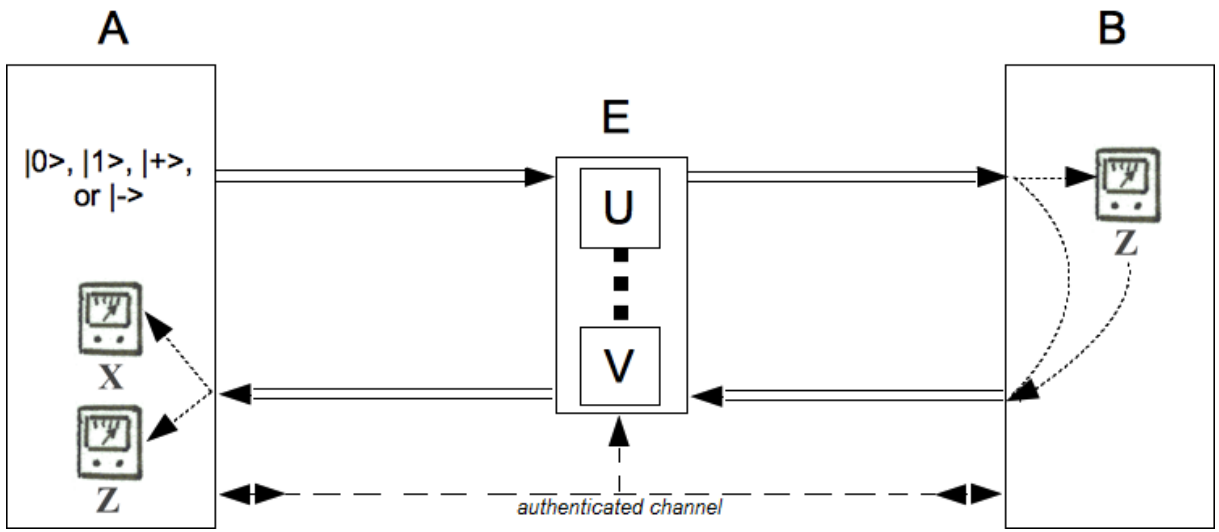

Figure: Boyer et al.'s SQKD Protocol [12]

Other Future Work

1. Consider imprecise parameter estimation more rigorously
2. We only worked in the asymptotic scenario, a finite-key analysis would be useful
3. Try to adapt this technique to other two-way protocols; also our work with the semi-quantum protocol can be improved

Thank you! Questions?

References I


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.


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.


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.


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.


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

References II


Zhen-Qiang Yin, Chi-Hang Fred Fung, Xiongfeng Ma, Chun-Mei Zhang, Hong-Wei Li, Wei Chen, Shuang Wang, Guang-Can Guo, and Zheng-Fu Han.
Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources.
Physical Review A, 90(5):052319, 2014.


Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma.
Loss-tolerant quantum cryptography with imperfect sources.
Physical Review A, 90(5):052314, 2014.


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


Igor Devetak and Andreas Winter.
Distillation of secret key and entanglement from quantum states.
Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science, 461(2053):207–235, 2005.


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

References III


Marco Lucamarini, Giovanni Di Giuseppe, and Kiyoshi Tamaki.
Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states.
Physical Review A, 80(3):032327, 2009.


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.


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