Mismatched Measurements and Quantum Key Distribution

Walter O. Krawec*

Introduction

When designing quantum key distribution (QKD) protocols, measurement outcomes produced by an incompatible choice of basis are usually discarded by the protocol specification. However, it has been shown that these *mismatched measurement outcomes* can actually be useful in better determining E's attack, leading potentially to an improved key-rate bound. For instance, in [1], it was shown that mismatched measurement outcomes can lead to an improved key-rate for the BB84 protocol under certain channels.

In [2, 3], the three state BB84 was considered (originally introduced in [4]). This is a protocol where Alice (A) sends only $|0\rangle, |1\rangle$, or $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ but never $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (thus, the users may not directly estimate the probability of E's attacking flipping a $|-\rangle$ to a $|+\rangle$ as may be done in the standard BB84). Despite this limitation, however, it was proven that the use of mismatched measurement outcomes allows the three-state protocol to suffer the same amount of noise as the full BB84 protocol, namely 11%. In fact, the key-rate expression for both protocols is identical. Furthermore, and rather surprisingly, the choice of the third state was largely irrelevant; i.e., A need not send $|+\rangle$ but any state $|a\rangle = \alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle$ for $\alpha \in (0,1)$ (and B measuring in the basis $\{|a\rangle, |\bar{a}\rangle\}$, where $\langle\bar{a}|a\rangle = 0$) - assuming a symmetric attack the choice of α did not matter (it may, however, affect the key rate if imprecise estimation is performed [3]). Ref. [2] went further and also studied a modified four-state BB84 where A sends $|0\rangle, |1\rangle, |+\rangle$, or $|0_Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$. It was shown that this led to the same key-rate as the full six-state BB84 protocol, again assuming a symmetric channel.

Recently, we have been developing a general framework from which to utilize mismatched measurement outcomes in the security proofs of arbitrary QKD protocols, extending the work we initially performed in [3]. We consider both one-way (where a qubit travels from A to B each iteration) and two-way protocols (where a qubit travels from A to B then back to A each iteration, thus passing through the adversary's lab twice). We show that our technique adapts to both scenarios and can lead to greatly improved key rate bounds for a variety of protocols. We also do not assume symmetric attacks and instead derive key rate expressions for various QKD protocols which may be used for asymmetric channels (for example, where E's attack flips a $|0\rangle$ with different probability than it would flip a $|1\rangle$). In fact, our key rate expressions utilize multiple noise parameters which may be estimated by the two users of the protocol.

Applications

We first consider the generalized BB84 protocol denoted $\Psi - \texttt{BB84}$, where Ψ is the set of qubit states that A may prepare randomly each iteration. We consider two cases: $\Psi_3 = \{|0\rangle, |1\rangle, |a\rangle\}$ and $\Psi_4 = \{|0\rangle, |1\rangle, |a\rangle, |b\rangle\}$, where $|a\rangle = \alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle$ and $|b\rangle = \beta|0\rangle + i\sqrt{1-\beta^2}|1\rangle$ (with $\alpha, \beta \in (0,1)$ are fixed parameters that are public knowledge). For such a protocol all states (and combinations of measurement bases) are used for parameter estimation; however, only $|0\rangle$ and $|1\rangle$ are used for key distillation. In this case, if E's attack is symmetric (in that it may be modeled as the depolarization channel $\mathcal{E}_Q(\rho) = (1-2Q)\rho + QI$, where I is the two-dimensional density operator; note this assumption is actually enforceable with mismatched measurement bases [3]), then when Ψ_3 is used, the protocol can tolerate up to 11% error while if Ψ_4 is used, it can tolerate up to 12.6% error, exactly that achieved by the full six-state BB84 (without any preprocessing) [5]. This therefore provides an alternative proof to the result of [2] (which also used mismatched measurement outcomes, though using a different proof technique, to show this same end result).

*Iona College, Computer Science Department, walter.krawec@gmail.com

α	0	0.342	0.643	0.939	0.985
Old Bound From [6]	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%

Table 1: Comparing our new key rate bound for the extended B92 protocol with the one from [6]. In particular, we compare the maximally tolerated error rates of our bound with the one from [6] for a depolarization channel and for various values of $\alpha = \langle 0|a\rangle$ (where $|0\rangle$ and $|a\rangle$ are used to encode the classical value of 0 and 1 respectively).

However, we went further and also derived a key rate expression utilizing all measurement statistics, allowing the evaluation of asymmetric channels. That is, denote by $p_{i,j}$, for $i, j \in \{0, 1, a, b\}$, the probability that, if A sends $|i\rangle$ then B measures $|j\rangle$ (conditioning on the event B chose to measure in the basis in which $|j\rangle$ exists). Our key rate expression utilizes several different combinations of i and j (e.g., $p_{0,a}$, $p_{b,1}$, $p_{0,1}$ etc.). Thus, the users need only measure these statistics, and evaluate the key-rate expression directly. Furthermore, we show the choice of $\alpha, \beta \in (0, 1)$ does not matter, assuming the asymptotic scenario and perfect parameter estimation.

Moving beyond BB84, we applied our technique to the extended B92 protocol described in [6] (which may also be considered an asymmetric SARG04 [7]). Here, A uses $|0\rangle$ and $|a\rangle$ to encode a raw key bit of 0 and 1 respectively. We derived a new key rate expression and use mismatched measurement bases to improve the channel estimation as was done for the BB84 example prior. We also considered the case where A sends states from Ψ_3 and from Ψ_4. Our results are shown in Table 1 for various choices of α assuming a symmetric attack. As before, the choice of β does not matter; the choice of α, however, does affect the key rate as it is used directly in key bit distillation (unlike the BB84 protocol). Note that the tolerated noise level becomes higher as α approaches 0 (i.e., as $|a\rangle$ approaches $|1\rangle$) which results in the BB84-style encoding.

In light of the above, we ask the question: given that our parameter estimation procedure determined particular statistics on the channel, is BB84-style encoding (i.e., using $|0\rangle$ for a raw key bit of 0 and $|1\rangle$ for a key bit of 1) optimal? For symmetric channels, BB84-style encoding was shown optimal in [8] using different techniques from ours. We consider general asymmetric channels and to answer this question, we consider a rather general (though by no means all inclusive) protocol where A encodes a raw key bit of 0 by sending a qubit $|\psi_0\rangle = \alpha_s |0\rangle + \sqrt{1 - \alpha_s^2}\, |1\rangle$ and a key bit of 1 by sending a qubit $|\psi_1\rangle = \beta_s |0\rangle + \sqrt{1 - \beta_s^2}\, |1\rangle$ for $\alpha_s, \beta_s \in [-1, 1]$. Bob will measure and if he receives outcome $|\phi_0\rangle = \alpha_r |0\rangle + \sqrt{1 - \alpha_r^2}\, |1\rangle$ he will set his raw key bit to 0; otherwise if he receives outcome $|\phi_1\rangle = \beta_r |0\rangle + \sqrt{1 - \beta_r^2}\, |1\rangle$, his key bit will be a 1 (here, $\alpha_r, \beta_r \in [-1, 1]$; we also do not assume $\langle \phi_0|\phi_1\rangle = 0$). Note the subscript "s" stands for *send*, while the "r" is for *receive*. Clearly this does not parameterize all one-way QKD protocols; it does, however, include BB84 and the extended B92 as particular sub-cases.

We derive a key-rate expression for this protocol, based on parameters $\alpha_s, \beta_s, \alpha_r, \beta_r$ and assuming states from Ψ_4 are used for parameter estimation (i.e., states in Ψ_4 will be sent by A to B and used to estimate the channel; while $|\psi_i\rangle$ and $|\phi_i\rangle$ are used for key distillation only). We evaluate this expression numerically and show that if the channel is symmetric (i.e., it is a depolarization channel), then the BB84 encoding is indeed optimal (i.e., the choice of $\alpha_s = 1, \beta_s = 0, \alpha_r = 1, \beta_r = 0$ yielded the highest key rate for the symmetric channel), confirming the result of [8]. For other, non-symmetric channels, this was not the case. We show some examples in Table 2. Note that we use $p_{i,j}$ for $i, j \in \{0, 1, a, b\}$ to denote the probability that, if A sends $|i\rangle$ then B measures $|j\rangle$ (conditioning on the event he chose to measure in the basis in which $|j\rangle$ lives). The reader will note that all statistics mentioned in the table are used in evaluating our key rate expression (both for this protocol, and all others we have considered).

Finally, we consider two-way QKD protocols: one where a qubit must travel from A to B and then return to A each iteration, thus allowing an attacker two opportunities to interact with the qubit. Furthermore, the protocol we consider is a *semi-quantum* one [9] where the user B is limited in his quantum capabilities (in particular, he can only measure in the Z basis). We use mismatched measurement bases to derive a key rate expression for the protocol of Boyer et al. [9]. Assuming a symmetric attack, and using Ψ_3 for

$\Psi_4 - \texttt{BB84}$'s key-rate	.349	0.001	0	.265	.07
Optimized key-rate	.349	0.001	.038	.307	.16
Optimized (α_s, β_s)	$(1, 0)$	$(1, 0)$	$(-1, .23)$	$(.23, -1)$	$(-.73, .65)$
Optimized (α_r, β_r)	$(1, 0)$	$(1, 0)$	$(-.94, .02)$	$(-.97, -.01)$	$(.8, -.64)$
$p_{0,1}$	.07	.126	.138	.079	.224
$p_{1,0}$	.07	.126	.191	.120	.198
$p_{a,a}$	.93	.874	.909	.966	.955
$p_{b,b}$	.93	.874	.942	.9371	.853
$p_{0,a}$	.5	.5	.523	.526	.397
$p_{1,a}$	.5	.5	.623	.544	.621
$p_{a,0}$	.5	.5	.566	.523	.619
$p_{0,b}$	.5	.5	.435	.334	.294
$p_{1,b}$	.5	.5	.505	.623	.681
$p_{b,0}$	.5	.5	.419	.396	.302

Table 2: Showing the key rate of $\Psi_4 - \texttt{BB84}$ (i.e., A sends states of the form $|0\rangle$, $|1\rangle$, $|a\rangle$, and $|b\rangle$) and the optimized one-way protocol under various attacks using our parameter estimation process (we used $\alpha = \beta = 1/\sqrt{2}$). The first two data columns are a symmetric attack with a noise level of 7% and 12.6%, respectively, in all bases. The other columns are randomly chosen, asymmetric, attacks. Note that the third data column shows an attack where BB84 would abort, yet there exists a way to distill a raw key using a different encoding. Our key rate expressions (for all protocols considered) utilize all $p_{i,j}$ statistics shown.

parameter estimation our key rate bound remains positive up to an error rate of 5.4% (assuming the two channels may be modeled as independent depolarization channels); this is an improvement over earlier work in [10] (which did not use mismatched measurement outcomes) which could only tolerate up to 4.57% (note that both results are lower bounds). If the two channels are correlated so that the error through a single channel is equal to that through both, then our new bound remains positive up to an error rate of 7.4% while the older bound in [10] only remained positive until 5.34%. Our new bound is improved if Ψ_4 is used for parameter estimation, in which case we get 6.7% for the independent channel case and 8.76% for the correlated channels.

References

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

[2] 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.

[3] Walter O Krawec. Asymptotic analysis of a three state quantum cryptographic protocol. *to appear: IEEE ISIT 2016; arXiv preprint arXiv:1601.00185*, 2016.

[4] 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.

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

[6] 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.

[7] 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.

[8] Joonwoo Bae and Antonio Acín. Key distillation from quantum channels using two-way communication protocols. *Physical Review A*, 75(1):012334, 2007.

[9] 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.

[10] 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.