Practical Security of Semi-Quantum Key Distribution

Walter O. Krawec
walter.krawec@uconn.edu

University of Connecticut
Computer Science and Engineering Department
Storrs, CT USA

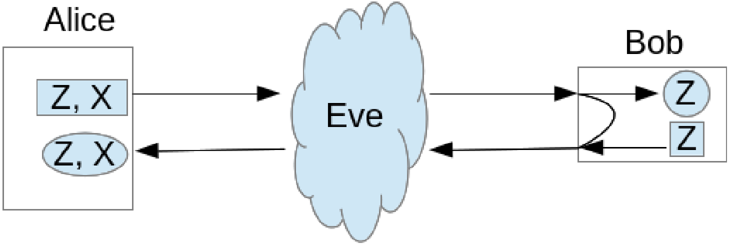
SPIE Defense April, 2018

Quantum Key Distribution

1. Quantum Key Distribution protocols allow for the establishment of a secret key, secure against an all-powerful adversary.
2. Requires both parties to be "Quantum Capable."
3. Example: If both parties communicate only in a single basis $\{|0\rangle, |1\rangle\}$ then unconditional security impossible

Semi Quantum Key Distribution (SQKD)

1. In 2007, Boyer et al., introduced the *semi-quantum* model whereby one user remains quantum capable but the other is *classical*
2. Classical user can only send and receive in a single basis ($\{|0\rangle, |1\rangle\}$) or disconnect from the line.
3. Original motivation was to study "How quantum does a protocol need to be to gain an advantage over a classical protocol?"
4. Requires a two-way channel, complicating the security analysis


Alice
Z, X
Z, X
Eve
Bob
Z
Z

B's Limitations

B, when given a qubit from A, may only:

1. `Measure and Resend`: That is, he may measure a qubit in the computational basis $|0\rangle, |1\rangle$ only. He may also send a computational basis state *normally prepared as a fresh qubit*
2. `Reflect`: He may simply disconnect from the channel and thus A is "talking to herself"

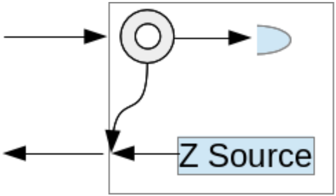
SQKD

1. Many different protocols:
   1. Original Boyer et al., protocol [1]
   2. Single-State Protocol [2]
   3. Reflection Protocol [3]
   4. Mirror Protocol [4]
   5. $\cdots$

   All (except the mirror protocol to be discussed) were studied only in the perfect qubit scenario; *only a few have information theoretic proofs of security*.

SQKD Security

1. Only recently have information theoretic security proofs become available
2. In [5], we actually show that, through careful use of *mismatched statistics*, the original SQKD protocol can withstand 11% error rate!
3. However most work thus far has remained in the theoretical "perfect-qubit" model.
4. Can the semi-quantum model operate in more practical settings? If so, how do they "behave?"


Z Source

BKLM17 Mirror Protocol

1. In [4] the first semi-quantum protocol designed for operation over practical channels was published by Boyer, Katz, Liss, and Mor.
2. It was also implemented in [6]
3. Made use of time-bin encoding and *controllable mirrors*

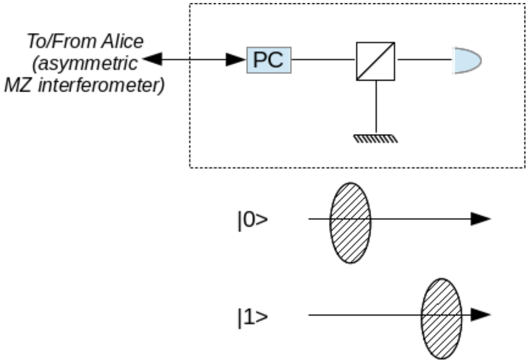


Figure : Diagram of the Mirror protocol of [4]. Based on an image in [6]

Our Work

1. In this work we present an alternative protocol also designed for operating against various photon attacks
2. We describe how to model its security and prove an upper-bound on E's information gain
3. We evaluate our bound on certain practical attacks against the system

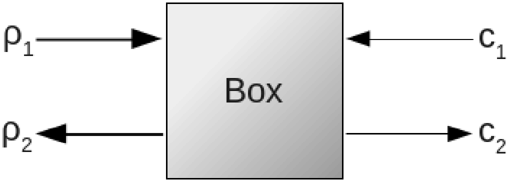
Our Work

1. In this work we present an alternative protocol for operating against various photon attacks
2. We describe how to model its security and prove an upper-bound on E's information gain
3. We evaluate our bound on certain practical attacks against the system

Our work is very preliminary and we do not claim to have solved all issues in this setting! Instead we propose a system that may eventually be extended to a practical scenario. We also consider its security against certain classes of practical attacks.

The Protocol

Our protocol makes use of the following abstract semi-quantum "box:"



The Protocol

1. If $c_1 = 0$, then $c_2 = 0$ and $\rho_2 = \rho_1$ with probability 1.
2. If $c_1 = 1$, then:

$$c_2 = 0 \text{ and } \rho_2 = \frac{1}{P_{NC}} \sum_{n \geq 0} q_n [\mathbf{1}]^{\otimes n} \qquad \text{with probability } P_{NC}$$

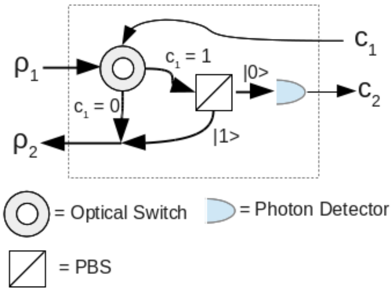
$$c_2 = 1 \text{ and } \rho_2 = \frac{1}{1 - P_{NC}} \sum_{n \geq 0} p_n [\mathbf{1}]^{\otimes n} \qquad \text{with probability } 1 - P_{NC}$$

(Note $[\mathbf{v}] = |v\rangle \langle v| = vv^*$)

Our security proof assumes q_n and p_n can be characterized if given a *known* input state ρ_1.

The Protocol

Our protocol makes use of the following abstract semi-quantum "box:"



The Protocol

Based on one in [3] (which was originally a semi-quantum version of SARG04 - however, our modification turns it into something closer to a semi-quantum B92).

1. A prepares and sends a qubit in the state $|+\rangle$
2. B picks random k_B and sets $c_1 = k_b$, recording the value of c_2
3. A measures incoming qubit in the Z or X basis. If she observes $|0\rangle$ she sets $k_A = 0$ if she observes $|-\rangle$ she sets $k_A = 1$; other results are *inconclusive*
4. If $c_2 = 1$, or if A received an inconclusive event, both parties discard the iteration.

Security Analysis: Goal

Our goal is to derive a bound on the asymptotic Devetak-Winter keyrate [7]:

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

1. We derive a bound on $S(B|E)$ for certain types of attacks.
2. We reduce the problem in the general case to a numerical optimization.

Security Analysis: Source

1. According to the protocol, the state leaving A's lab is fixed $|+\rangle$. We assume the actual state leaving her lab is:

$$\rho_A = \sum_{n\geq 0} a_n [+]^{\otimes n} \text{ (ex: } a_n = e^{-\mu}\frac{\mu^n}{n!}).$$

2. Eve captures and attacks this state via a CPTP map $\mathcal{E}$:

$$\mathcal{E}\left(\sum_{n\geq 0} a_n [+]^{\otimes n}\right) = \sum_n b_n [\mathbf{n}]_R \otimes [\mathbf{E_n}],$$

where $[\mathbf{n}]_R$ is an internal register in E's memory and $|E_n\rangle$ is a pure state modeling the qubits leaving her lab which are also potentially entangled with her quantum memory:

Security Analysis: Source

$$\mathcal{E}\left(\sum_{n\geq 0} a_n [+]^{\otimes n}\right) = \sum_n b_n [\mathbf{n}]_R \otimes [\mathbf{E_n}],$$

1. Goal is to compute $S(A|E) = S(A|ER)$; by concavity of entropy, we may as well assume E chooses an optimal $|e\rangle = |E_N\rangle$ to send:

$$|e\rangle = |E_N\rangle = \sum_{x\in\{0,1\}^N} \alpha_x \left|x\right\rangle_T \otimes \left|e_x\right\rangle_E ,$$

Anything else will cause $S(A|ER)$ to increase. Thus the state arriving at B's lab is the T portion of $[\mathbf{E_N}]$

Security Analysis: Box

$$\rho_1 = tr_E[\mathbf{E_N}]$$

1. B will set his input c_1 to be his key-bit. The box will behave as described earlier, leaving us with the system:

$$\frac{1}{2}[\mathbf{0}]_B \otimes [\mathbf{E_N}]_T + \frac{1}{2}[\mathbf{1}]_B \otimes [\mathbf{0}]_{c_2} \otimes \left(\sum_n q_n [\mathbf{1}]_T^{\otimes n} \otimes \sigma_n^E \right)$$
$$+ \frac{1}{2}[\mathbf{1}]_B \otimes [\mathbf{1}]_{c_2} \otimes \left(\sum_n p_n [\mathbf{1}]_T^{\otimes n} \otimes \sigma_n'^E \right)$$

Security Analysis: Reverse Channel

$$\frac{1}{2}[\mathbf{0}]_B \otimes [\mathbf{E_N}]_T + \frac{1}{2}[\mathbf{1}]_B \otimes [\mathbf{0}]_{c_2} \otimes \left(\sum_n q_n [\mathbf{1}]_T^{\otimes n} \otimes \sigma_n^E \right)$$
$$+ \frac{1}{2}[\mathbf{1}]_B \otimes [\mathbf{1}]_{c_2} \otimes \left(\sum_n p_n [\mathbf{1}]_T^{\otimes n} \otimes \sigma_n'^E \right)$$

1. Recall: E's goal is to "guess" at B's choice.
2. If the number of photon's leaving B's box is not equal to the number entering, then E can say for certain that $c_1 = 1$.
3. But both parties discard if $c_2 = 1$. *Thus the box must be designed so that q_n is close to P_{NC}!*

Security Analysis: Reverse Channel

1. We may assume that the σ's are pure states (this is only to E's advantage).
2. We also assume, as in [8], E will only forward to the receiver (now A) one or no photons, keeping any additional photons to herself to extract information from
3. Thus, E's second attack may be modeled (with some slight abuse of notation!) as a unitary operator:

$$U|E_N\rangle = |+, f_0\rangle + |-, f_1\rangle + |v, f_v\rangle$$
$$U|1\rangle^{\otimes N} \otimes |\sigma_N^E\rangle = |0, e_0\rangle + |1, e_1\rangle + |v, e_v\rangle$$
$$U|1\rangle^{\otimes n} \otimes |\sigma_n^E\rangle = |0, g_0^n\rangle + |1, g_1^n\rangle + |v, g_v^n\rangle, \text{ for } n < N,$$

(Note: $|v\rangle$ is the vacuum state)

Security Analysis: Back to A

1. A now measures in the Z or X basis; her outcome determines her measurement bit or whether the iteration is inconclusive. B will also, then, share his value of c_2. After some algebra, we derive:

$$\begin{aligned}\rho_{ABE} = {} & \frac{1}{M}[\mathbf{00}]_{BA} \otimes [\mathbf{F}] + \frac{1}{M}[\mathbf{01}]_{BA} \otimes [\mathbf{f_1}] \\ & + \frac{q_N}{M}[\mathbf{10}]_{BA} \otimes [\mathbf{e_0}] + \frac{q_N}{M}[\mathbf{11}]_{BA} \otimes [\mathbf{E}] \\ & + \sum_{n<N} \frac{q_n}{M}\left([\mathbf{10}]_{BA} \otimes [\mathbf{g_0^n}] + [\mathbf{11}]_{BA} \otimes [\mathbf{G^n}]\right),\end{aligned}$$

where we define:

$$|E\rangle = \frac{1}{\sqrt{2}}(|e_0\rangle - |e_1\rangle) \qquad |F\rangle = \frac{1}{\sqrt{2}}(|f_0\rangle + |f_1\rangle)$$

$$|G^n\rangle = \frac{1}{\sqrt{2}}(|g_0^n\rangle - |g_1^n\rangle),$$

Computing $S(B|E)$

$$\text{Goal: } \lim_{N\to\infty} \frac{\ell(N)}{N} = S(B|E) - H(B|A)$$

1. We break the system into a "good case" and a "bad case"

$$\rho_{ABE} = \frac{p_G}{M}\sigma_{good} + \left(1 - \frac{p_G}{M}\right)\sigma_{bad}$$

2. Here, σ_{good} contains the case where the same number of photons leave B's box that entered it.
3. While σ_{bad} contains the case where fewer qubits leave the box then enter it.
4. By taking advantage of concavity of von Neumann entropy:

$$S(B|E) \geq \frac{p_G}{M} \cdot S(B|E)_{\sigma_{good}}.$$

I.e., we may assume E has full information in the "bad" case.

After some algebra:

$$\sigma_{good} = \frac{[\mathbf{00}]_{BA} \otimes [\mathbf{F}] + [\mathbf{01}]_{BA} \otimes [\mathbf{f_1}] + q_N[\mathbf{10}]_{BA} \otimes [\mathbf{e_0}] + q_N[\mathbf{11}]_{BA} \otimes [\mathbf{E}]}{\mathtt{PKey}_{0,0} + \mathtt{PKey}_{0,1} + q_N\widetilde{\mathtt{PKey}}_{1,0} + q_N\widetilde{\mathtt{PKey}}1,1}$$

$$p_G = \mathtt{PKey}_{0,0} + \mathtt{PKey}_{0,1} + q_N\widetilde{\mathtt{PKey}}_{1,0} + q_N\widetilde{\mathtt{PKey}}1,1$$

It can be shown that, when $q_N = P_{NC}$ (i.e, the box is "perfect") then $p_G = M$ so:

$$S(B|E) = S(B|E)_{\sigma good}.$$

As q_N decreases, then so does E's uncertainty (thus, so does the key-rate).

We now condition on a new system to break the density operator into a block diagonal form. Using a method in [5] allows us to bound:

$$S(B|E)_{\sigma_{good}}$$
$$\geq \left(\frac{\mathtt{PKey}_{0,0} + q_N \widetilde{\mathtt{PKey}}_{1,1}}{p_G} \left[h\left(\frac{\mathtt{PKey}_{0,0}}{\mathtt{PKey}_{0,0} + q_N \widetilde{\mathtt{PKey}}_{1,1}} \right) - h(\lambda_1) \right] \right)$$
$$+ \left(\frac{\mathtt{PKey}_{0,1} + q_N \widetilde{\mathtt{PKey}}_{1,0}}{p_G} \left[h\left(\frac{\mathtt{PKey}_{0,1}}{\mathtt{PKey}_{0,1} + q_N \widetilde{\mathtt{PKey}}_{1,0}} \right) - h(\lambda_2) \right] \right)$$

where:

$$\lambda_1 = \frac{1}{2} \left(1 + \frac{\sqrt{(\mathtt{PKey}_{0,0} - q_N \widetilde{\mathtt{PKey}}_{1,1})^2 + 4 q_N Re^2 \langle E|F \rangle}}{\mathtt{PKey}_{0,0} + q_N \widetilde{\mathtt{PKey}}_{1,1}} \right)$$

$$\lambda_2 = \frac{1}{2} \left(1 + \frac{\sqrt{(\mathtt{PKey}_{0,1} - q_N \widetilde{\mathtt{PKey}}_{1,0})^2 + 4 q_N Re^2 \langle e_0|f_1 \rangle}}{\mathtt{PKey}_{0,1} + q_N \widetilde{\mathtt{PKey}}_{1,0}} \right)$$

We have thus reduced the problem to finding (bounds) on the real part of $\langle E|F\rangle$ and $\langle e_0|f_1\rangle$

Recall:

$|e_i\rangle$ is the state of E's memory if B's box outputs $|1\rangle^{\otimes N}$ and A measures $|i\rangle$

$|f_i\rangle$ is the state of E's memory if B's box outputs $|E_N\rangle$ and A measures $H|i\rangle$

and:

$$|E\rangle = \frac{1}{\sqrt{2}}(|e_0\rangle - |e_1\rangle)$$
$$|F\rangle = \frac{1}{\sqrt{2}}(|f_0\rangle + |f_1\rangle)$$

We have thus reduced the problem to finding (bounds) on the real part of $\langle E|F\rangle$ and $\langle e_0|f_1\rangle$

1. In general, this may be done numerically (recall U is unitary which imposes restrictions on these)
2. We work out more exact values for certain attacks, namely unambiguous state discrimination (USD) and multi-photon attack in the forward channel.

1. As this protocol (in its current form) shares many similarities to B92 [9], the USD attack applies

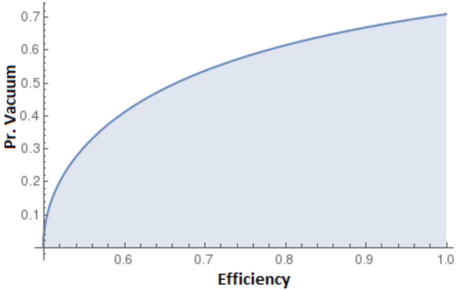
$$\begin{aligned} \nu = & \text{ dark-count probability} \\ \eta = & \text{ photon detector efficiency} \\ 1 - T = & \text{ probability of photon loss in the reverse channel} \end{aligned}$$

Then we show in the paper that our protocol is secure against against the USD attack if:

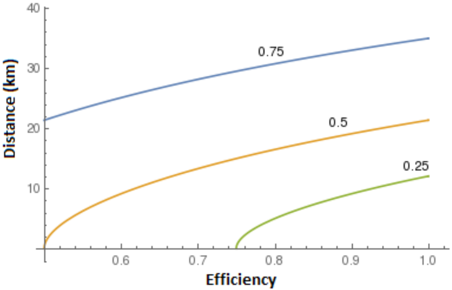
$$1 - T \leq \sqrt{\frac{P_{NC}}{\eta(1-\nu)} - \frac{1-\eta}{\eta}}.$$

If $\nu = 0$ and $\eta = 1$ (perfect detectors), then this agrees with the tolerance of B92, namely a maximal loss of 70.9%.

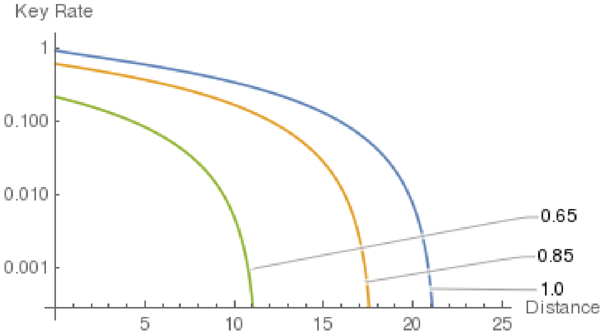
Otherwise:



If $T = 10^{-.25\ell/10}$:



More generally, we have:



Closing Remarks and Future Work

1. Obviously the distance limitation is not great! Can we do better?
2. Perhaps the Mirror protocol proposed by Mor et al., [4] can acheive higher communication distance.
3. A more thorough security analysis would be desirable (for both our protocol and the mirror one in [4]). This would also allow us to compare properties from the two.
4. Our protocol was originally based on a "semi-quantum SARG04" [3]. However, by moving to this "box" design, it "transformed" to a semi-quantum B92. Can we incorporate multiple boxes to improve security against the USD attack?

Thank you! Questions?

References I

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.

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

Walter O Krawec.
Restricted attacks on semi-quantum key distribution protocols.
Quantum Information Processing, 13(11):2417–2436, 2014.

Michel Boyer, Matty Katz, Rotem Liss, and Tal Mor.
Experimentally feasible protocol for semiquantum key distribution.
Phys. Rev. A, 96:062335, Dec 2017.

Walter O. Krawec.
Quantum key distribution with mismatched measurements over arbitrary channels.
Quantum Information and Computation, 17(3 and 4):209–241, 2017.

Natan Tamari.
Experimental Semiquantum Key Distribution: Classical Alice with Mirror.
PhD thesis, Technion Institute of Technology, May 2014.

References II

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

Cyril Branciard, Nicolas Gisin, Barbara Kraus, and Valerio Scarani.
Security of two quantum cryptography protocols using the same four qubit states.
Physical Review A, 72(3):032301, 2005.

Charles H. Bennett.
Quantum cryptography using any two nonorthogonal states.
Phys. Rev. Lett., 68:3121–3124, May 1992.