

Eavesdropping in Semiquantum Key Distribution Protocol

Arpita Maitra¹, Goutam Paul^{2,*}

Abstract

In semiquantum key-distribution (Boyer et al.) Alice has the same capability as in BB84 protocol, but Bob can measure and prepare qubits only in $\{|0\rangle, |1\rangle\}$ basis and reflect any other qubit. We study an eavesdropping strategy on this scheme that listens to the channel in both the directions. With the same level of disturbance induced in the channel, Eve can extract more information using our two-way strategy than what can be obtained by the direct application of one-way eavesdropping in BB84.

Keywords: BB84 Protocol, Binary Symmetric Channel, Cryptography, Optimal Eavesdropping, Quantum Cryptography, Semiquantum Key Distribution

2010 MSC: 81P94

1. Introduction

The BB84 protocol [1] is used by Alice and Bob to settle on a secret classical bit-string over an insecure quantum channel where Eve can have access. There are a number of important papers that analyze this scheme and we refer to [2, 3, 4, 5, 6] and the references therein for further reading. The BB84 protocol [1] uses the bases $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. In this case, Bob has the capability of measuring the qubits in either Z or X basis.

*Corresponding author.

¹Applied Statistics Unit, Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India. Email: arpita76b@rediffmail.com. *The work of this author was supported by the WOS-A fellowship of the Department of Science and Technology, Government of India.*

²Department of Computer Science and Engineering, Jadavpur University, Kolkata 700 032, India. Email: goutam.paul@ieee.org. *The work of this author was done in part during his visit at RWTH Aachen, Germany as an Alexander von Humboldt Fellow.*

In [7], it has been considered that Bob has limited capability and he can do the following.

(1) Whenever a qubit passes through Bob, he can let it go undisturbed, or in other words he can reflect the qubit to Alice (CTRL bits).

(2) Otherwise he can measure the qubit in the Z basis and prepare a fresh qubit in the same basis and send it to Alice (SIFT bits).

Based on this limited capability of Bob, semiquantum key distribution has been presented in [7] and later it has been analyzed in more detail in [8]. The authors call the Z basis as the classical basis, as it has one-to-one correspondence with the classical bits. Bob is called *classical* since he prepares and measures qubits in this basis only. Alice is not classical, as she needs to deal with quantum superposition of the computational basis states. Thus the protocol is called *semiquantum*. The exact protocol [7] is described in Algorithm 1.

- 1** Alice generates $N = 8n(1 + \delta)$ many qubits randomly in Z basis or X basis;
- 2** For each qubit received at Bob's end, he chooses randomly either to reflect it (CTRL) or to measure it in Z basis and resend it in the same state he measured (SIFT);
- 3** Alice measures each qubit in the basis she sent;
- 4** Alice publishes which are the Z bits she sent and Bob publishes which ones he chose to SIFT;
- 5** Alice checks the error-rate in the CTRL bits and aborts the protocol if the error-rate in either of the basis is more than some predefined threshold value;
- 6** Alice randomly chooses n SIFT bits as TEST bits and publishes them;
- 7** Bob publishes the values of these TEST bits;
- 8** Alice checks the error rate in these bits and aborts if the error-rate is more than some predefined value;
- 9** Alice and Bob select the first n remaining SIFT bits to be used as INFO bits;
- 10** Alice publishes ECC and PA data and then she and Bob use them to extract the final m -bit secret key from n -bit INFO string;

Algorithm 1: Semiquantum Key Distribution with Classical Bob [7].

In [7, 8], the authors proved that the protocol is robust. This is in the sense that for any attack inducing no error on TEST bits (a subset of the SIFT bits used for error correction [7]) and CTRL bits, Eve's final state is independent of the qubits

chosen by Bob as SIFT and the states sent by Alice. However, they did not give any quantitative estimate connecting the disturbance experienced by Alice and the information leakage at Eve's end. In [8, Section I], the authors made the following comment:

Note that our result does not imply that Eve cannot gain a large amount of information by inducing a very small but nonzero noise on qubits. It is however our belief that such a discontinuity of "information versus disturbance" does not occur, but the question is beyond the scope of this paper and is left for future research.

This gives us motivation to investigate the exact relationship between the disturbance and information leakage under certain eavesdropping model. In the semiquantum protocol [7], the qubits need to travel in two directions and thus the eavesdropper has the advantage to look into the qubits twice instead of once as in the case of BB84 [1].

In this regard, let us refer to a comment [9] on the semiquantum protocol [7] and the corresponding response [10] that are related to actual implementation issues. In [9], it has been pointed out that if the qubits are implemented by photons with some wavelength λ say, then the eavesdropper can cleverly modify the wavelength of the photons (flying from Alice to Bob) from λ to $\lambda + \delta\lambda$ without changing the polarization. For each SIFT photon, as Bob measures and recreates a fresh copy, the wavelength again becomes λ during the return path from Bob to Alice, while for each CTRL photon, as it is only reflected by Bob, and the wavelength remains $\lambda + \delta\lambda$. This is exactly the situation, where Eve can successfully tag the SIFT and CTRL photons separately before the public announcement and thus obtains all the secret key (INFO) bits without creating any disturbance in a similar line to the *mock protocol* described in [7] itself. In the response [10] to this comment [9], the authors acknowledge this attack based on implementation issues. However, it is also pointed in [10] that there may be several such attacks on various implementations of any Quantum Key Distri-

bution protocol. Naturally, there would be several countermeasures, e.g., in this case Bob may place a suitable filter to thwart this attack. To be precise, the attack of [9] considers an implementation weakness, while the attack does not work on theoretical model using perfect qubits, namely, a two- dimensional Hilbert space [10].

However, the eavesdropping strategy that we present here is not dependent on any implementation issue and should work on any perfect implementation where the standard model of eavesdropping can be implemented too. Given that, we show that our two-way eavesdropping strategy extracts more information about the secret key bits against [7] than that is possible against traditional BB84 [1] for certain range of disturbance. That is, our eavesdropping strategy works even in idealistic scenario, while the attack of [9] works only in a specific realistic scenario only that can also be thwarted with proper countermeasure.

1.1. Eavesdropping Model

In this paper, we consider the same symmetric incoherent optimal eavesdropping model of [6] that was used for the traditional BB84 protocol [1]. It is symmetric, because there will be equal error probability at Bob's end corresponding to different bases and it is incoherent as Eve works with each individual qubit.

In general, Alice sends a qubit $|\mu\rangle$ to Bob and Eve lets a four dimensional probe $|W\rangle$ of two qubits (as in [6, Section III]) that interacts unitarily with $|\mu\rangle$. Eve's measurement is delayed till Alice announces the basis that has been used (i.e., by that time Bob has already measured the state). We can model it as $U(|\mu\rangle, |W\rangle) = |\tau\rangle$, where U is the unitary operator and after its application, $|\tau\rangle$ is the entangled state of the qubit that Alice sent to Bob and the probe applied by Eve. Let D be the disturbance in the channel due to the interaction by Eve and $F = 1 - D$ be the fidelity. Without loss of generality, one can write the eavesdropping interaction for the Z basis as

$$U(|0\rangle, |W\rangle) = \sqrt{F}|E_{00}\rangle|0\rangle + \sqrt{D}|E_{01}\rangle|1\rangle, U(|1\rangle, |W\rangle) = \sqrt{D}|E_{10}\rangle|0\rangle + \sqrt{F}|E_{11}\rangle|1\rangle.$$

Following the analysis in [6, 5], it can be shown that with the optimal eavesdropping strategy, Eve's average success probability in correctly guessing a secret bit is $P_E^{(1)}(D) = \frac{1}{2} + \sqrt{D(1-D)}$. Since the *advantage* of the eavesdropper can be defined as the amount by which the success probability exceeds the probability of random guessing (which, in this case, is $\frac{1}{2}$), the advantage is given by $A_E^{(1)}(D) = \sqrt{D(1-D)}$.

Note that the strategy of [6] can directly be used towards eavesdropping against the semiquantum protocol [7]. However, we like to explore beyond this trivial application of the eavesdropping strategy of [6] and consider that the eavesdropper will try to extract information during the transmission of qubits both from Alice to Bob and Bob to Alice.

When Alice sends a qubit $|\mu\rangle$ to Bob, Eve lets a probe $|W\rangle$ that interacts unitarily with $|\mu\rangle$. Thus the interaction can be modelled as $U(|\mu\rangle, |W\rangle) = |\tau\rangle$. If Bob performs a measurement, then the 3-qubit entangled state $|\tau\rangle$ collapses to a 3-qubit post-measurement product state $|\tau_m\rangle$. When the corresponding qubit (either reflected or measured and resent) returns from Bob to Alice, then again Eve tries to interact with a probe $|W'\rangle$ and the unitary operation can be written as $U'(|\tau''\rangle, |W'\rangle) = |\tau'\rangle$, where $|\tau''\rangle$ is $|\tau\rangle$ or $|\tau_m\rangle$, according as Bob reflects or measures (respectively), and $|\tau'\rangle$ is a 5-qubit state.

2. Analysis of the Binary Symmetric Channels

One may refer to [6] to note that the analysis can be done considering the model of Binary Symmetric Channel (BSC). For the semiquantum case, we need to consider two cascaded channels, the first for the qubits moving from Alice to Bob and the second for the qubits moving from Bob to Alice, each with error probability p due to Eavesdropping. (There can be eavesdropping inducing different error probabilities p_1, p_2 in the two channels, and that can be taken care of in a similar manner.)

Following Section 1.1, we can write for the channel between Alice and Bob

$$\begin{aligned} U(|0\rangle, |W\rangle) &= \sqrt{1-p}|E_{00}\rangle|0\rangle + \sqrt{p}|E_{01}\rangle|1\rangle, \\ U(|1\rangle, |W\rangle) &= \sqrt{p}|E_{10}\rangle|0\rangle + \sqrt{1-p}|E_{11}\rangle|1\rangle, \end{aligned} \quad (1)$$

where W is the initial state of the pair of qubits at Eve's hand.

We analyze the SIFT bits and the CTRL bits separately.

Lemma 1. *For the SIFT bits, the round trip channel from Alice to Bob and back to Alice is equivalent to a binary symmetric channel with error probability $2p(1-p)$.*

Proof: Refer to Figure 1. The first BSC corresponds to the transmission from Alice to Bob and the second one corresponds to the transmission from Bob to Alice.

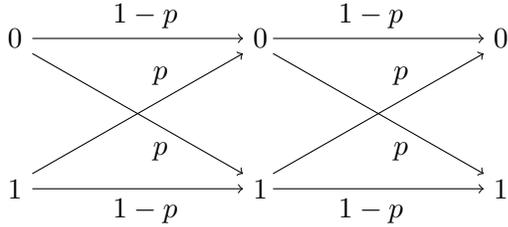


Figure 1: Cascaded BSC model for the SIFT bits

Consider one round-trip communication from Alice to Bob and then back to Alice. If Alice sends 0, the error-path is either $0 \rightarrow 0 \rightarrow 1$ or $0 \rightarrow 1 \rightarrow 1$. The path is symmetric when Alice sends 1. Thus, the error-probability would be given by $(1-p)p + p(1-p) = 2p(1-p)$. \square

Lemma 2. *For the CTRL bits, the round trip channel from Alice to Bob to Alice is equivalent to a binary symmetric channel with error probability $2p(1-p)$.*

Proof: Without loss of generality, let us consider when Alice sends 0. The case when Alice sends 1 would be symmetric.

According to Equation (1), Bob will receive a qubit entangled with the two bits of Eve, having the three-qubit entangled state $\sqrt{1-p}|E_{00}\rangle|0\rangle + \sqrt{p}|E_{01}\rangle|1\rangle$. Bob will

send the entangled qubit received as it is to Alice. Let W' be the initial state of the new pair of qubits at Eves hand with which she will interact unitarily with the qubit sent from Bob to Alice. This interaction can be written as

$$\begin{aligned} & I \otimes U(\sqrt{1-p}|E_{00}\rangle|0\rangle + \sqrt{p}|E_{01}\rangle|1\rangle, |W'\rangle) \\ &= \left((1-p)|E_{00}\rangle|E'_{00}\rangle + p|E_{01}\rangle|E'_{10}\rangle \right) |0\rangle + \sqrt{p(1-p)} \left(|E_{00}\rangle|E'_{01}\rangle + |E_{01}\rangle|E'_{11}\rangle \right) |1\rangle, \end{aligned}$$

where E'_{ij} 's are the new two-qubit probes at Eve's hand corresponding to Bob sending bit i and Alice receiving bit j . Thus, the probability that Alice measures 0 is $(1-p)^2 + p^2$ and that she measures 1 is $2p(1-p)$. \square

Note that for the SIFT case, one qubit moves from Alice to Bob and a corresponding different one moves from Bob to Alice back. In the CTRL case, it is the same qubit that is travelling in both the directions (Alice to Bob and Bob to Alice). It is important to note that the error in the channel observed by Alice is the same in both the cases. This is the reason, the eavesdropping model of [6] remains symmetric even when it is applied to the semiquantum protocol in both the directions.

Combining Lemma 1 and Lemma 2, we can write the following Theorem.

Theorem 1. *The round trip channels from Alice to Bob to Alice when Bob measures and sends a fresh qubit (SIFT) and when he just reflects the received qubit (CTRL) are equivalent, and both act as a binary symmetric channel with error probability $2p(1-p)$.*

Let $D_{one-way}$ and $D_{two-way}$ be the disturbances in the one-way BB84 protocol and the two-way semiquantum protocol respectively. We take $D_{one-way} = D$ and we have shown that $D_{two-way} = 2p(1-p)$. Both the attacks should be compared in the same footing, i.e., Eve's advantages have to be compared at the same disturbance values. For this reason, we take $D_{two-way} = D_{one-way}$, i.e., $D = 2p(1-p)$.

3. Detailed Analysis of Two-way Eavesdropping

Eve will have two guesses for the forward and backward communication. As discussed in Section 1.1, for each guess, Eve has the success probability $p_E = \frac{1}{2} +$

$\sqrt{p(1-p)} = \frac{1}{2} + \epsilon$, where $\epsilon = \sqrt{p(1-p)}$. If both the guesses give the same outcome, then the probability that the bit guessed is correct increases. Suppose during the forward communication from Alice to Bob, Eve has a success probability of $\frac{1}{2} + \epsilon_1$ and during the backward communication from Bob to Alice, Eve has a success probability of $\frac{1}{2} + \epsilon_2$. For a particular bit, let $P_E^{(2,match)}$ be Eve's posterior probability that the bit sent was b , when both her forward and the backward guesses give the same outcome $b \in \{0, 1\}$. The following result is easy to show.

Proposition 1. $P_E^{(2,match)} = \frac{1}{2} + \frac{\epsilon_1 + \epsilon_2}{1 + 4\epsilon_1\epsilon_2}$.

Since $\epsilon_i \leq \frac{1}{2}$, we have $P_E^{(2,match)} \geq \frac{1}{2} + \epsilon_i$, for $i = 1, 2$. This implies that Eve's success probability increases, when she observes the same outcome b in both directions and guesses that indeed b was sent.

Let us now substitute $\epsilon_1 = \epsilon_2 = \sqrt{p(1-p)}$, where $2p(1-p) = D$. When Eve observes the same outcome in both the directions, let her success probability as a function of the disturbance be denoted by $P_E^{(2,match)}(D)$. Thus, we have the following result.

Lemma 3. $P_E^{(2,match)}(D) = \frac{1}{2} + \frac{\sqrt{D/2}}{\frac{1}{2} + D}$.

The corresponding advantage is given by $A_E^{(2,match)}(D) = \frac{\sqrt{D/2}}{\frac{1}{2} + D}$. One may easily check that $\frac{\sqrt{D/2}}{\frac{1}{2} + D} \geq \sqrt{D(1-D)}$ for $D \in [0, \frac{1}{2}]$ and in this case, Eve's advantage for the semiquantum protocol is better than what is achieved in the eavesdropping [6] in BB84 protocol.

When both the cases do not have the same outcome, then the situation is not encouraging. In this case one has to consider one of the two outcomes as the correct guess. Without loss of generality, we accept the outcome of the first observation as the correct guess. In this case,

$$P_E^{(2,mismatch)}(D) = \frac{1}{2} + \sqrt{p(1-p)} = \frac{1}{2} + \sqrt{D/2}. \quad (2)$$

It is immediate to note that $\sqrt{D/2} \leq \sqrt{D(1-D)}$ for $D \in [0, \frac{1}{2}]$ and in this case Eve suffers with the decreased advantage.

Thus while calculating the average advantage, we consider the following strategy: “if the outcomes observed by Eve in both the directions are the same bit b , she guesses b , else she discards her guess in the backward direction and considers only the guess during the forward direction.” Let $P_E^{(2,avg)}(D)$ denote Eve’s average success probability when she follows the above strategy.

Theorem 2. $P_E^{(2,avg)}(D) = \frac{1}{2} + \frac{\sqrt{D/2(3+2D)}}{2(1+2D)}$.

Proof: It is clear that both the match and the mismatch happens with probability $\frac{1}{2}$. Hence the average success probability of Eve is given by $P_E^{(2,avg)}(D) = \frac{1}{2}P_E^{(2,match)}(D) + \frac{1}{2}P_E^{(2,mismatch)}(D)$. Substituting values of the probabilities from Lemma 3 and Equation (2), we get the result. \square

Hence, the average advantage is given by $A_E^{(2,avg)}(D) = \frac{\sqrt{D/2(3+2D)}}{2(1+2D)}$. In Figure 2, we plot the advantages for different attack strategies versus D . Note that $P_E^{(2,avg)}(D) > P_E^{(1)}(D)$, i.e., Eve has more advantage in the semiquantum protocol, if $D < 0.0877$ (up to the fourth decimal place). This region is shown magnified in the right portion of Fig. 2 for a clearer pictorial exposition.

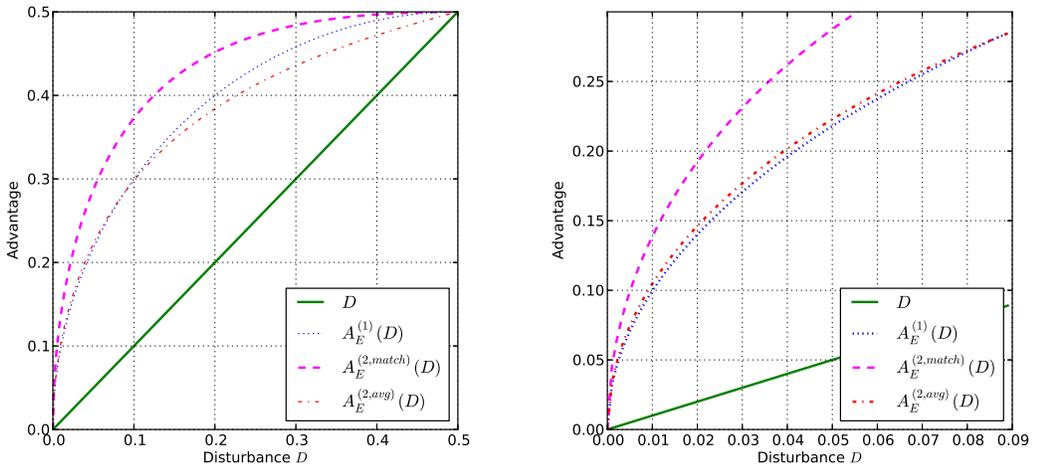


Figure 2: Advantage of the eavesdropper as a function of disturbance D under different attack models (magnified portion for $0 \leq D \leq 0.09$ is shown on the right).

The summarized strategy of eavesdropping on the semiquantum protocol would be as follows.

1. For $D \geq 0.0877$, apply unitary interaction for eavesdropping only during the communication between Alice and Bob (same as BB84).

2. For $D < 0.0877$, apply unitary interaction during both the communications (Alice to Bob and Bob to Alice) with disturbance in each channel p , where $D = 2p(1 - p)$. If the bits obtained through the two different interactions are same, then accept that as the guessed bit. If the bits obtained through the two different interactions are different, then accept the bit obtained during the communication from Alice to Bob as the guessed one.

This provides more information to the eavesdropper in certain range in the semiquantum protocol [7] than in BB84 [1] and thus our two-way eavesdropping on the the semiquantum protocol recovers more information than what can be obtained using the idea of [6] directly as it was applied against BB84.

4. Conclusion

Boyer et al. [7, 8] introduced the quantum key distribution protocol with classical Bob and showed its robustness, but left open any analysis regarding how the amount of information leakage to the eavesdropper is related to the disturbance caused by her. We analyzed an eavesdropping strategy on this scheme and explicitly derived eavesdropper's advantage as a function of the disturbance. Here our investigation exploits the model of [6] in both the directions of communication (Alice to Bob and Bob to Alice). Our two-way eavesdropping strategy against the semiquantum protocol extracts more information on the secret bits than that could be obtained by direct one-way application of the strategy in [6] that worked on BB84. Other existing eavesdropping strategies on BB84 [1] may be explored in a similar manner on the semiquantum protocol [7, 8].

References

- [1] C. H. Bennett and G. Brassard. Quantum Cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, IEEE, New York (1984).
- [2] E. Biham and T. Mor. Bounds on Information and the Security of Quantum Cryptography. *Physical Review Letters*, 79, 4034–4037 (1997).
- [3] H. E. Brandt. Quantum-cryptographic entangling probe. *Physical Review A* 71, 042312 (2005).
- [4] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81, 3018–3021 (1998) [quant-ph/9805019].
- [5] J. I. Cirac and N. Gisin. Coherent eavesdropping strategies for the 4 state quantum cryptography protocol. *Physics Letters A*, 229(1), 1–7 (1997) [quant-ph/9702002].
- [6] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. -S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Physical Review A*, 56(2), 1163–1172 (1997).
- [7] M. Boyer, D. Kenigsberg and T. Mor. Quantum key distribution with classical Bob. *Physical Review Letters*, 99, 140501 (2007).
- [8] M. Boyer, R. Gelles, D. Kenigsberg and T. Mor. Semiquantum key distribution. *Physical Review A*, 79(3), 032341 (2009).
- [9] Y. Tan, H. Lu and Q. Cai. Comment on “Quantum Key Distribution with Classical Bob”. *Physical Review Letters*, 102, 098901 (2009).
- [10] M. Boyer, D. Kenigsberg and T. Mor. Boyer, Kenigsberg, and Mor Reply. *Physical Review Letters*, 102, 098902 (2009).