Revisiting Symmetric Incoherent Optimal Eavesdropping in BB84 Protocol

Arpita Maitra
Applied Statistics Unit, Indian Statistical Institute,
Kolkata 700 108, India,
arpita76b@rediffmail.com

Goutam Paul
Department of Computer Science and Engineering, Jadavpur University,
Kolkata 700 032, India,
Email: goutam.paul@ieee.org

Abstract

The famous BB84 protocol relies on the conjugate bases $Z = \{|0\rangle,\ |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Fuchs et. al. (Phy. Rev. A, 1997) presented an optimal eavesdropping strategy on the four-state BB84 protocol. Later Bruß (Phys. Rev. Lett., 1998) described the use of the basis $\left\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\right\}$ along with the above two to show that the BB84 protocol with three conjugate bases (six-state protocol) provides improved security. Bruß had also shown that for the six-state protocol, the mutual information between Alice (the sender) and Eve (the eavesdropper) is higher when two-bit probe is used compared to the one-bit probe and hence provides a stronger eavesdropping strategy. In this paper, we revisit the problem towards a critical and concrete analysis in terms of Eve's success probability in guessing the qubits that Alice has sent. In this regard, we show that though Eve has more success probability in the four state BB84 than in the six state BB84, within the six state protocol she has the same success probability in guessing the qubit transmitted by Alice in both the two-bit and the one-bit probe. Finally, we propose a model of multi-round BB84 protocol, in which the advantage of Eve can be reduced arbitrarily, and with proper choice of parameters, the multi-round four state protocol can be made more secure than the multi-round six state protocol.

Keywords: Bias, Advantage, BB84 Protocol, Key Distribution, Optimal Eavesdropping, Quantum Communication, Quantum Cryptography, Sequence.

1 Introduction

The BB84 protocol [1] is used by Alice (the sender) and Bob (the receiver) to settle on a secret classical bit-string by communicating qubits over an insecure quantum channel where Eve (the Eavesdropper) can have access. Alice randomly selects one of the two orthogonal bases and encodes 1 and 0 respectively by a qubit prepared in one of the two states in each base (the one-to-one mapping between $\{0, 1\}$ and the states of the bases are known publicly). Bob also measures the qubits one by one, randomly selecting the basis from the same set of bases. After the measurement, Alice and Bob publicly announce the sequence of bases used by them and discard the bases that do not match. They identify the sequence of bits corresponding to the bases that match and the resulting bitstring, followed by error correction and privacy amplification, becomes the common secret key.

The security in the protocol is based on the fact that if one wants to distinguish two non-orthogonal quantum states, then obtaining any information is only possible at the expense of introducing disturbance in the state(s). There are several works in the literature, e.g., [2, 3, 5], that studied the relationship between "the amount of information obtained by Eve" and "the amount of disturbance created on the qubits that Bob receives from Alice". There are also several models for analysis of these problems. As example, Eve can work on each individual qubit as opposed to a set of qubits studied together. While the first one is called the *incoherent attack* [5], the second one is known as *coherent attack* [3]. In this paper we study the incoherent attack.

Another interesting issue in specifying the eavesdropping scenario is whether there will be equal error probability at Bob's end corresponding to different bases. If this is indeed equal, then we call it *symmetric* and that is what we concentrate on here. It creates certain constraint on Eve in terms of extracting information from the communicated qubits as the disturbance created on the qubits that Bob receives should be equal for all the bases. That is, as far as Alice and Bob are concerned, the interference by Eve will produce a binary symmetric channel between them, with an error probability that we will denote by D. There is also another model where this is not equal and then we call the eavesdropping model as *asymmetric*. Different error rates for different bases would be a clear indication to Alice and Bob that an eavesdropper (Eve) is interfering in the communication line. One may refer to [3] for details on this and it has been commented in the same paper that given any non-symmetric attack (coherent or non-coherent), one can always get a symmetric attack that can match the results of the non-symmetric strategy.

To explain the exact model we follow the framework of [5, 2]. Alice sends a qubit $|\mu\rangle$ to Bob and Eve lets a probe $|W\rangle$ (a four dimensional probe of two qubits as in [5, 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). That is, 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. Based on certain measurement strategy, it has been shown in [5, 2] what optimal eavesdropping can be achieved by Eve given the disturbance at Bob's end.

The original 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 $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Following [10], let $\{|\phi_i\rangle | i = 1, \ldots, N\}$ and $\{|\Phi_i\rangle | i = 1, \ldots, N\}$ be two orthonormal bases for an N dimensional Hilbert space. Such a pair will be called *conjugate*, if and only if $|\langle\phi_i|\Phi_j\rangle|^2 = \frac{1}{N}$ for any i, j. Here $\langle\phi_i|\Phi_j\rangle$ is the inner product between $|\phi_i\rangle, |\Phi_j\rangle$. The case $N = 2$ is considered here. The analysis with non-conjugate bases has been presented by Phoenix [8] and it has been shown that the original proposal of [1] using the conjugate bases provides the optimal security.

A generalization of the BB84 protocol has been studied in [2] that uses three conjugate bases $Z = \{|0\rangle, |1\rangle\}$, $X = \{|+\rangle, |-\rangle\}$ and $\left\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\right\}$. It is shown in the analysis of [2] that using the optimal strategy by performing certain unitary transformation on the transmitted qubit, an eavesdropper can extract less information in the six-state scheme [2] than the case with four-state scheme [5] for a fixed disturbance of the qubit that Bob receives. In both [5, 2], the security of BB84 is analyzed in terms of the mutual information between Alice and Eve. When measuring her probe, Eve has two choices. One option is that she measures both her qubits - this is referred as a *two-bit probe*. Alternatively she can either measure only one of her two qubits or may interact with one qubit at her disposal - both of these lead to identical results and therefore we referred any one of them as *one-bit probe*. In [2], it was claimed that the security of two-bit probe is identical to that of one-bit probe for the four state protocol, but within the six state protocol, the two-bit probe leaks more information to Eve than the four state one.

1.1 Our Contributions

We begin with a review of the analysis of the four state [5] and the six state [2] protocols in Section 2 under a general framework. We work with the bases $\{|0\rangle, |1\rangle\}$ and $\{|\psi\rangle, |\psi_\perp\rangle\}$, where $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\psi_\perp\rangle = b^*|0\rangle - a^*|1\rangle$. It is very clear that to get conjugate bases $\{|0\rangle, |1\rangle\}$ and $\{|\psi\rangle, |\psi_\perp\rangle\}$, it is necessary to have $|a| = |b| = \frac{1}{\sqrt{2}}$. In this framework, we characterize the values of a, b for the eavesdropping models of [5, 2].

Sections 3 and 4 contain our main contributions. We re-examine the security in the light of Eve's *success probability* of guessing what was sent by Alice. In practice, Eve's goal is to determine the secret key bits that Alice sends to Bob. Eve's individual probes and hence individual guesses are independent. After measurement of the i-th probe, Eve makes a guess of the i-th secret key bit. In other words, Eve has to decide whether the i-th bit was 0 or 1. If her decided bit matches with what Alice sent, then we call it a *success*, else it is an *error*. Eve's strategy would be to minimize the *error probability* in her guess, i.e., to maximize the *success probability*.

The mutual information between Alice and Eve gives a theoretical measure about the average information contained in the random variable associated with one of them about the random variable associated with the other. However, from the point of view of guessing the secret key established between Alice and Bob, Eve's success probability is a more practical parameter of cryptanalytic interest than the mutual information between Alice and Eve. Without any experiment, Eve can randomly guess any bit of the secret key with probability $\frac{1}{2}$. Any interaction by Eve and her interpretation of the subsequent measurement of that interaction can give her some extra hint about the secret bit. Thus, the success probability is a value that is always greater than or equal to $\frac{1}{2}$. In cryptography, the difference between the attacker's success probability and the probability of random guess (in this case the probability of random guess is $\frac{1}{2}$) is termed as the attacker's *advantage*.

In Section 3, we present an analysis of the success probabilities of the four state and the six state protocols and show that there is no extra advantage of the two-bit probe over the one-bit probe in the six state protocol. We show that these two probes do not differ in terms of success probability of Eve's guess about the bits sent by Alice.

In Section 4, we propose a multi-round version of the BB84 protocol. Using the Piling-up Lemma [9], we prove that a linear increase in the number of rounds causes an exponential decrease in the advantage of the Eavesdropper. Note that, the Piling-up Lemma is typically used for linear cryptanalysis [6]. To the best of our knowledge, this is the first application of the Lemma in making a cryptographic design more secure. In this scheme, independent of whether the protocol is four state or six state and irrespective of whether one-bit probe or two-bit probe is used, Alice and Bob can decrease Eve's advantage below the level of the disturbance D caused by Eve. Both in the traditional 4-state BB84 protocol [1] and in the six-state one [2], Bob measures first and then Alice publishes the bases she used. Thus, while the six state protocol is more secure than the four state one, the disadvantage of the the six-state scheme is that, on an average, only one-third of the qubits are kept and the rest two-third are discarded, which is worse than in the case of four-state scheme, where half of the received qubits are discarded. Hence, for a fair comparison between our multi-round versions of these two protocols, we must ensure that the same number of qubits communicated between Alice and Bob and in the end, the secret keys established are of the same bit length. In this setting, we prove that with proper choice of parameters, the four state protocol can be made more secure than the six state protocol.

2 Review of Optimal Eavesdropping

In this part, we study a generic version of BB84 with the bases $|0\rangle, |1\rangle$ and $|\psi\rangle$, $|\psi_{\perp}\rangle$, where $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\psi_{\perp}\rangle = b^*|0\rangle - a^*|1\rangle$. We characterize the values of a, b based on the eavesdropping model presented in [5, 2]. We take each of a, b nonzero as otherwise both the base will coincide (up to rotation). It is also trivial to see that $|a|^2 + |b|^2 = 1$ from normality condition. Under the symmetric incoherent optimal eavesdropping strategy [5, 2], we get certain constraints on a, b as given in Theorem 2.1 in the next section. If one takes a state $|\psi\rangle$ such that the conditions on a, b as given in Theorem 2.1 are not admitted, then the symmetric attack of [5] needs to be modified properly.

In the absence of eavesdropper or any channel noise, Bob exactly knows the state that has been sent by Alice if measured in correct basis. However, Eve's interaction does not allow that to happen. Consider the scenario when Alice sends one of two orthogonal states $|\psi\rangle$ and $|\psi_{\perp}\rangle$ to Bob and Eve has her own initial two-bit state $|W\rangle$. Eve's interaction with the state being sent from Alice to Bob can be modeled as the action of a unitary operator

U on three qubits as follows.

$$\begin{aligned} U(|\psi\rangle, |W\rangle) &= \sqrt{F'}|\psi\rangle|E'_{00}\rangle + \sqrt{D'}|\psi_\perp\rangle|E'_{01}\rangle, \\ U(|\psi_\perp\rangle, |W\rangle) &= \sqrt{D'}|\psi\rangle|E'_{10}\rangle + \sqrt{F'}|\psi_\perp\rangle|E'_{11}\rangle. \end{aligned} \tag{1}$$

Thus, when Alice sends $|\psi\rangle$ (respectively $|\psi_\perp\rangle$), then Bob receives $|\psi\rangle$ (respectively $|\psi_\perp\rangle$) with probability F' (this is called *fidelity*) and receives $|\psi_\perp\rangle$ (respectively $|\psi\rangle$) with probability D' (this is called *disturbance*). One may note that $F' + D' = 1$.

After Bob measures the qubit he receives, Eve tries to obtain information about Bob's qubit. As example, if Eve obtains $|E'_{00}\rangle$ after measurement, she knows that Bob has received $|\psi\rangle$. The problem with Eve is that, if she tries to extract such information with certainty, then $|E'_{00}\rangle$, $|E'_{01}\rangle$, $|E'_{10}\rangle$ and $|E'_{11}\rangle$ need to be orthogonal and in that case the error probability D' at Bob's end will be very high and Bob will abort the protocol. Thus all of $|E'_{00}\rangle$, $|E'_{01}\rangle$, $|E'_{10}\rangle$, $|E'_{11}\rangle$ cannot be orthogonal and Eve has to decide the relationship among these 2-qubit states for optimal eavesdropping strategy.

Now let us consider the case for the $|0\rangle, |1\rangle$ basis.

$$\begin{aligned} U(|0\rangle, |W\rangle) &= \sqrt{F}|0\rangle|E_{00}\rangle + \sqrt{D}|1\rangle|E_{01}\rangle, \\ U(|1\rangle, |W\rangle) &= \sqrt{D}|0\rangle|E_{10}\rangle + \sqrt{F}|1\rangle|E_{11}\rangle. \end{aligned} \tag{2}$$

The case for the generalized basis $|\psi\rangle$, $|\psi_\perp\rangle$ has already been expressed in (1). As we are studying the symmetric attack here, we consider that the fidelity F and the disturbance D are same for all the cases, i.e., $F = F'$ and $D = D'$.

We have considered $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\psi_\perp\rangle = b^*|0\rangle - a^*|1\rangle$, where a, b are nonzero. Hence, by linearity and then using Equation (2), we get

$$\begin{aligned} U(|\psi\rangle, |W\rangle) &= aU(|0\rangle, |W\rangle) + bU(|1\rangle, |W\rangle) \\ &= |0\rangle(a\sqrt{F}|E_{00}\rangle + b\sqrt{D}|E_{10}\rangle) + |1\rangle(a\sqrt{D}|E_{01}\rangle + b\sqrt{F}|E_{11}\rangle). \end{aligned} \tag{3}$$

Substituting $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\psi_\perp\rangle = b^*|0\rangle - a^*|1\rangle$ in the first one of Equation (1), we obtain

$$U(|\psi\rangle, |W\rangle) = |0\rangle(a\sqrt{F}|E'_{00}\rangle + b^*\sqrt{D}|E'_{01}\rangle) + |1\rangle(b\sqrt{F}|E'_{00}\rangle - a^*\sqrt{D}|E'_{01}\rangle). \tag{4}$$

Equating the right hand sides of Equations (3) and (4), we get

$$\begin{aligned} \sqrt{F}|E'_{00}\rangle &= \sqrt{F}\left(|a|^2|E_{00}\rangle + |b|^2|E_{11}\rangle\right) + \sqrt{D}\left(ab^*|E_{01}\rangle + a^*b|E_{10}\rangle\right), \quad (5) \\ \sqrt{D}|E'_{01}\rangle &= ab\sqrt{F}\left(|E_{00}\rangle - |E_{11}\rangle\right) - \sqrt{D}\left(a^2|E_{01}\rangle - b^2|E_{10}\rangle\right). \quad (6) \end{aligned}$$

Similarly, comparing two different expressions for $U(|\psi_\perp\rangle, |W\rangle)$, we get

$$\begin{aligned} \sqrt{D}|E'_{10}\rangle &= a^*b^*\sqrt{F}\left(|E_{00}\rangle - |E_{11}\rangle\right) + \sqrt{D}\left(b^{*2}|E_{01}\rangle - a^{*2}|E_{10}\rangle\right), \quad (7) \\ \sqrt{F}|E'_{11}\rangle &= \sqrt{F}\left(|b|^2|E_{00}\rangle + |a|^2|E_{11}\rangle\right) - \sqrt{D}\left(ab^*|E_{01}\rangle + a^*b|E_{10}\rangle\right). \quad (8) \end{aligned}$$

As explained in [5, 3], for a symmetric attack, we have the following constraints.

(i) The scalar products $\langle E_{ij}|E_{kl}\rangle$ and $\langle E'_{ij}|E'_{kl}\rangle$, are such that $\langle E_{ij}|E_{kl}\rangle = \langle E_{kl}|E_{ij}\rangle$ and $\langle E'_{ij}|E'_{kl}\rangle = \langle E'_{kl}|E'_{ij}\rangle$, for $i,j,k,l \in \{0,1\}$. This assumption implies that all the inner products must be real.

(ii) Any element of $\{|E_{00}\rangle, |E_{11}\rangle\}$ is orthogonal to any element of $\{|E_{01}\rangle, |E_{10}\rangle\}$. Similar orthogonality condition holds between $\{|E'_{00}\rangle, |E'_{11}\rangle\}$ and $\{|E'_{01}\rangle, |E'_{10}\rangle\}$.

(iii) Further, we take $\langle E_{00}|E_{11}\rangle = \langle E'_{00}|E'_{11}\rangle = x$, $\langle E_{01}|E_{10}\rangle = \langle E'_{01}|E'_{10}\rangle = y$, where x, y are real. It is evident that all the other inner products are zero due to the orthogonality conditions.

We have $\langle E'_{00}|E'_{01}\rangle = 0$ and replacing them as in (5) and (6), we get

$$ab(|a|^2 - |b|^2)(1-x) - D\left[ab\left(|a|^2 - |b|^2\right)(2-x) + \left(a^3b^* - a^*b^3\right)y\right] = 0. \tag{9}$$

From (9) we get the following

$$D = \frac{ab\left(|a|^2 - |b|^2\right)(1-x)}{ab\left(|a|^2 - |b|^2\right)(2-x) + \left(a^3b^* - a^*b^3\right)y}. \tag{10}$$

The expression of D in (10) is not defined when the denominator is zero. Given $y \neq 0$, the denominator of (10) is 0 if and only if $\left(|a| = |b| = \frac{1}{\sqrt{2}}\right)$ AND $\left(\arg(\frac{a}{b}) \equiv 0 \bmod \frac{\pi}{2}\right)$. Under this condition, we get that $a = \pm b$ or $\pm ib$.

When $a = \pm b$ or $\pm ib$, D cannot be calculated from (10) as the denominator will be zero. However, taking $\langle E'_{01}|E'_{01}\rangle = 1$ and putting there the expression of $|E'_{01}\rangle$ from (6), we get the D as follows

$$\begin{aligned} D &= \frac{1-x}{2-x+y}, \text{ when } a = \pm b & (11)\\ &= \frac{1-x}{2-x-y}, \text{ when } a = \pm ib. & (12)\end{aligned}$$

Now we look for the cases where the denominator of D in (10) is not zero. It has already been considered that $\langle E'_{00}|E'_{10}\rangle = 0$. Now replacing them as in (5) and (7) and plugging in the value of D from (10), we get $(1-x)y\left(a^2b^{*2} - a^{*2}b^2\right) = 0$.

We have considered that $\langle E_{00}|E_{11}\rangle = \langle E'_{00}|E'_{11}\rangle = x$, and $\langle E_{01}|E_{10}\rangle = \langle E'_{01}|E'_{10}\rangle = y$, where both x, y are real. Thus, it is natural to consider that $0 < x, y < 1$, otherwise either the vectors will be orthogonal or same. In such a situation, from $(1-x)y\left(a^2b^{*2} - a^{*2}b^2\right) = 0$, we get $\left(a^2b^{*2} - a^{*2}b^2\right) = 0$, i.e., $ab^* = \pm a^*b$. This holds if and only if $a = \pm rb, \pm irb$, where $r = \frac{|a|}{|b|} \neq 1$. The $r = 1$ case has already been taken care of.

For $r \neq 1$, when we put $a = \pm rb$ in (10), we get $D = \frac{1-x}{2-x+y}$, as given in (11) already. Now taking the inner product of both sides of (6) and (7) and putting $D = \frac{1-x}{2-x+y}$, we get $\langle E'_{01}|E'_{10}\rangle = \left((b^*)^2 + (a^*)^2\right)^2 y$ which has been assumed to be y. Thus, $\left((b^*)^2 + (a^*)^2\right)^2 = 1$, and given $a = \pm rb$, we obtain either both a, b are real of both a, b are imaginary.

However, for $r \neq 1$, if we put $a = \pm irb$ in (10), we get $D = \frac{1-x}{2-x-y}$ as in (12). Then following the similar manner as before, we get one of a, b is real and the other one is imaginary. Thus we have the following result.

Theorem 2.1 *Consider symmetric incoherent eavesdropping with* $0 < x, y < 1$*, on the BB84 protocol with the bases* $|0\rangle$*,* $|1\rangle$ *and* $|\psi\rangle = a|0\rangle + b|1\rangle$*,* $|\psi_\perp\rangle = b^*|0\rangle - a^*|1\rangle$*. We have (i)* $D = \frac{1-x}{2-x+y}$ *if and only if* a, b *are either both real or both imaginary and (ii)* $D = \frac{1-x}{2-x-y}$ *if and only if one of* a, b *is real and the other one is imaginary.*

Theorem 2.1 identifies that for such eavesdropping where BB84 protocol is implemented with the bases $|0\rangle$, $|1\rangle$ and $|\psi\rangle$, $|\psi_\perp\rangle$, the form of $|\psi\rangle$ is restricted given $0 < x, y < 1$. When $r \neq 1$, then the bases $|0\rangle$, $|1\rangle$ and $|\psi\rangle$, $|\psi_\perp\rangle$ cannot be conjugate. To have conjugate bases, one must take $r = 1$, i.e., $|a| = |b| = \frac{1}{\sqrt{2}}$. As the simplest example, it is natural to consider $a = b = \frac{1}{\sqrt{2}}$, which gives $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\psi_\perp\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ that has indeed been used in BB84 protocol [1]. On such conjugate bases, the eavesdropping idea of [5] works that we discuss in the next section.

In [5], the conjugate bases $|0\rangle$, $|1\rangle$ and $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ have been considered. That is in this case, $a = b = \frac{1}{\sqrt{2}}$ and $D = \frac{1-x}{2-x+y}$, as in Equation (11).

In [2], three conjugate bases $|0\rangle$, $|1\rangle$; $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$ have been exploited for the BB84 protocol. Thus, while considering $a = b = \frac{1}{\sqrt{2}}$ one gets $D = \frac{1-x}{2-x+y}$, but in case of $a = \frac{1}{\sqrt{2}}$, $b = \frac{i}{\sqrt{2}}$ we obtain $D = \frac{1-x}{2-x-y}$. To have the symmetric attack possible, we need $\frac{1-x}{2-x+y} = \frac{1-x}{2-x-y}$ and thus $y = 0$. For $y = 0$, both (11) and (12) reduce to

$$D = \frac{1-x}{2-x}. \tag{13}$$

However, there are complex numbers a, b, where $|a| = |b| = \frac{1}{\sqrt{2}}$, but $a \neq \pm b, \pm ib$ and in those case a, b are not as given in Theorem 2.1. As example, one can take, $|\psi\rangle = \frac{1+i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|\psi_\perp\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1-i}{2}|1\rangle$. Symmetric attack in the attack model of [5, 2] is not directly possible in these cases when y is nonzero. However, if Eve uses a phase-covariant cloner or orients her probes appropriately, then she can mount the same attack. Thus, by no choice of a, b, Alice and Bob can avoid the symmetric attack on the four state protocol.

3 Eavesdropper's Success Probability as a Function of Disturbance

In this part, we revisit the attack models of [5] and [2] in the light of success probability of Eve's guess about qubit was actually sent by Alice. In the analysis, we require to compute the probabilities of different related events. These probabilities form the components for the mutual information between Alice and Eve as well as the success probability for Eve's guess. First in Section 3.1, we compute these individual probabilities and for the sake of completeness show the calculation of mutual information also. Next in Section 3.2, we derive the success probabilities of Eve's guess for various cases and discuss how they give different insight from mutual information.

We introduce a few notations for the sake of our analysis. Let A, B, V be the random variables corresponding to the bit sent by Alice, bit received by Bob and the outcome observed by Eve due to her measurement. Eve performs the measurement after Alice and Bob announce their basis. After the announcement, Eve discards the probes corresponding to the qubits for which Alice and Bob's bases do not match and works with the the probes corresponding to the bases that match. For one-bit probe, Eve measures her second qubit in the bases Z or X, as used by Alice. Similarly, for two-bit probe, Eve measures in the bases $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ when Alice and Bob use the Z basis and she measures in the basis $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$ when Alice and Bob use the X basis. In this paper, we calculate all probabilities considering the Z basis only. Symmetry gives the same results when the X basis is used. Hence, without loss of generality, V can be assumed to be in $\{0, 1\}$ for one-bit probe, and it can be assumed to be in $\{00, 01, 10, 11\}$ for two-bit probe. In the subsequent discussion, we use the term Eve's *observation* to denote the observed outcome V of her measurement.

3.1 Probability Analysis and Mutual Information

We follow the standard definitions of mutual information and conditional entropy from information theory [4]. The mutual information between Alice and Bob is given by

$$I^{AB} = H(A) - H(A|B), \tag{14}$$

and the mutual information between Alice and Eve is given by

$$I^{AV} = H(A) - H(A|V), \tag{15}$$

where $H(\cdot)$ is the Shannon entropy function.

We assume that Alice randomly generates the bits to be transmitted, so that $P(A = 0) = P(A = 1) = \frac{1}{2}$. Hence $H(A) = -\frac{1}{2}\log_2(\frac{1}{2}) - \frac{1}{2}\log_2(\frac{1}{2}) = 1$.

Also, $P(B = 0 \mid A = 1) = P(B = 1 \mid A = 0) = D$ and $P(B = 0 \mid A = 0) = P(B = 1 \mid A = 1) = 1 - D$.

Hence, $P(B = 0) = P(B = 1) = \frac{1}{2}$ and the conditionals $P(A|B)$ are identical with the conditionals $P(B|A)$. Thus,

$$\begin{aligned} H(A \mid B = 0) &= H(A \mid B = 1) \\ &= -D\log_2(D) - (1 - D)\log_2(1 - D). \end{aligned}$$

Hence,

$$\begin{aligned} H(A|B) &= P(B = 0)H(A \mid B = 0) + P(B = 1)H(A \mid B = 1) \\ &= -D\log_2(D) - (1 - D)\log_2(1 - D), \end{aligned}$$

and from Equation (14) we have

$$I^{AB} = 1 + D\log_2(D) + (1 - D)\log_2(1 - D). \tag{16}$$

Recall that (refer to Equation (2)) the general unitary transformation designed by Eve is as follows.

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

For $i \in \{0, 1\}$, Eve's posterior probability of what Alice sent is given by

$$\begin{aligned} P(A = i \mid V = v) &= \frac{P(A = i) \cdot P(V = v \mid A = i)}{P(V = v)}, \quad \text{by Bayes' Theorem} \\ &= \frac{P(A = i) \cdot P(V = v \mid A = i)}{\sum\limits_{j=0,1} P(A = j) \cdot P(V = v \mid A = j)} \\ &= \frac{\frac{1}{2} \cdot P(V = v \mid A = i)}{\sum\limits_{j=0,1} \frac{1}{2} \cdot P(V = v \mid A = j)} \\ &= \frac{P(V = v \mid A = i)}{P(V = v \mid A = 0) + P(V = v \mid A = 1)}. \end{aligned} \tag{17}$$

Again, the likelihoods are computed as

$$\begin{aligned} P(V = v \mid A = i) &= P(B = 0 \mid A = i)P(V = v \mid A = i, B = 0) \\ &\quad + P(B = 1 \mid A = i)P(V = v \mid A = i, B = 1) \\ &= P(B = 0 \mid A = i)P(V = v \mid E_{i0}) \\ &\quad + P(B = 1 \mid A = i)P(V = v \mid E_{i1}). \end{aligned} \tag{18}$$

If we rewrite the interactions expressed in [5, Equations 50-51] in our notation, we obtain the following expressions for $|E_{ij}\rangle$'s.

$$\begin{aligned} |E_{00}\rangle &= \sqrt{1-D}\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \sqrt{D}\frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\ |E_{01}\rangle &= \sqrt{1-D}\frac{|01\rangle + |10\rangle}{\sqrt{2}} - \sqrt{D}\frac{|01\rangle - |10\rangle}{\sqrt{2}}, \\ |E_{10}\rangle &= \sqrt{1-D}\frac{|01\rangle + |10\rangle}{\sqrt{2}} + \sqrt{D}\frac{|01\rangle - |10\rangle}{\sqrt{2}}, \\ |E_{11}\rangle &= \sqrt{1-D}\frac{|00\rangle + |11\rangle}{\sqrt{2}} - \sqrt{D}\frac{|00\rangle - |11\rangle}{\sqrt{2}}. \end{aligned}$$

The likelihoods for the attack in [5] when computed using Equation (18) turns out to be as shown in Table 1 below. As an example, $P(V = 0 \mid A = 0)$ is given by

	$V = 0$	$V = 1$
$A = 0$	$\frac{1}{2} + \sqrt{D(1-D)}$	$\frac{1}{2} - \sqrt{D(1-D)}$
$A = 1$	$\frac{1}{2} - \sqrt{D(1-D)}$	$\frac{1}{2} + \sqrt{D(1-D)}$
Marginal of V	$\frac{1}{2}$	$\frac{1}{2}$

Table 1: Values of $P(V = v \mid A = i) = P(A = i \mid V = v)$ for the attack model of [5].

$$\begin{aligned} & P(B=0 \mid A=0)P(V=0 \mid E_{00}) + P(B=1 \mid A=0)P(V=0 \mid E_{01}) \\ = \;& (1-D) \cdot \left(\frac{1}{\sqrt{2}} \left(\sqrt{1-D} + \sqrt{D} \right) \right)^2 + D \cdot \left(\frac{1}{\sqrt{2}} \left(\sqrt{1-D} + \sqrt{D} \right) \right)^2 \\ = \;& \frac{1}{2} + \sqrt{D(1-D)} = f(D), \qquad \text{(say)}. \end{aligned}$$

Note that since $P(A = 0) = P(A = 1) = \frac{1}{2}$, the half of the sum of each column in Table 1 gives the marginal probability of V for that column. From Equation (17), we find that in this case, the posteriors are identical with the corresponding likelihoods. Hence $H(A \mid V = 0) = H(A \mid V = 1) = -f(D) \log_2 f(D) - (1 - f(D)) \log_2 (1 - f(D))$.

Also, from Table 1, we have $P(V = 0) = P(V = 1) = \frac{1}{2}$, giving

$$\begin{aligned} H(A|V) &= P(V=0)H(A \mid V=0) + P(V=1)H(A \mid V=1) \\ &= -f(D) \log_2 f(D) - (1 - f(D)) \log_2 (1 - f(D)) \,. \end{aligned}$$

Substituting in Equation (15), we have

$$I^{AV} = 1 + f(D) \log_2 f(D) + (1 - f(D)) \log_2 (1 - f(D)) \,. \qquad (19)$$

Note that the above computation is shown assuming a one-bit probe. It is easy to show that, for the four state protocol, the one-bit and the two-bit probes give identical mutual information between Alice and Eve. The expression for this mutual information is given by Equation (19) which matches with [5, Equation 65].

Next, the interactions of [2, Equations 9-15], when expressed in our notations, become

$$\begin{aligned} |E_{00}\rangle &= \beta|10\rangle + \sqrt{1-|\beta|^2}|01\rangle, \\ |E_{01}\rangle &= |00\rangle, \\ |E_{10}\rangle &= |11\rangle, \\ |E_{11}\rangle &= \sqrt{1-|\beta|^2}|10\rangle + \beta|01\rangle. \end{aligned}$$

where

$$|\beta|^2 = \frac{1}{2} \left(1 + \frac{\sqrt{D(2-3D)}}{1-D} \right). \qquad (20)$$

Note that the above expression of $|\beta|^2$ comes from Equation (13), where x is the inner-product between $|E_{00}\rangle$ and $|E_{11}\rangle$. Technically, the square-root in Equation (20) should be written with a ± sign. However, for simplicity, we show all calculation with the + sign here. The calculation with the − sign would be similar.

For one-bit probe, the likelihoods for [2] when computed using Equation (18) turns out to be as shown in Table 2 below. From Equation (17), we find that in this case also, the posteriors are identical with the corresponding likelihoods.

	$V=0$	$V=1$
$A=0$	$D+(1-D)\|\beta\|^2$	$1-D-(1-D)\|\beta\|^2$
$A=1$	$1-D-(1-D)\|\beta\|^2$	$D+(1-D)\|\beta\|^2$
Marginal of V	$\frac{1}{2}$	$\frac{1}{2}$

Table 2: Values of $P(V=v \mid A=i) = P(A=i \mid V=v)$ for one-bit probe of [2].

For ease of calculation, let us denote

$$\begin{aligned} f_1(D) &= D+(1-D)|\beta|^2 \\ &= \frac{1}{2}\left(1+D+\sqrt{D(2-3D)}\right). \end{aligned} \tag{21}$$

Hence $H(A \mid V=0) = H(A \mid V=1) = -f_1(D)\log_2 f_1(D) - (1-f_1(D))\log_2(1-f_1(D))$.

Also, from Table 2, we have $P(V=0)=P(V=1)=\frac{1}{2}$, giving

$$\begin{aligned} H(A|V) &= P(V=0)H(A \mid V=0) + P(V=1)H(A \mid V=1) \\ &= -f_1(D)\log_2 f_1(D) - (1-f_1(D))\log_2(1-f_1(D)). \end{aligned}$$

Substituting in Equation (15), we have

$$I_1^{AV} = 1 + f_1(D)\log_2 f_1(D) + (1-f_1(D))\log_2(1-f_1(D)). \tag{22}$$

This expression matches with [2, Equation 18].

Now, consider the two-bit probe. The likelihoods for [2] when computed using Equation (18) turns out to be as shown in Table 3 below.

	$V=00$	$V=01$	$V=10$	$V=11$
$A=0$	D	$1-D-(1-D)\|\beta\|^2$	$(1-D)\|\beta\|^2$	0
$A=1$	0	$(1-D)\|\beta\|^2$	$1-D-(1-D)\|\beta\|^2$	D
Marginal of V	$\frac{D}{2}$	$\frac{1-D}{2}$	$\frac{1-D}{2}$	$\frac{D}{2}$

Table 3: Values of $P(V=v \mid A=i)$ for two-bit probe of [2].

From Equation (17), the posteriors are computed as given in Table 4 below.

Hence $H(A \mid V=00) = H(A \mid V=11) = 0$ and

$$\begin{aligned} & H(A \mid V=01) = H(A \mid V=10) \\ = \; & -|\beta|^2\log_2|\beta|^2 - \left(1-|\beta|^2\right)\log_2\left(1-|\beta|^2\right) = h(D) \text{ (say)}. \end{aligned}$$

	$V=00$	$V=01$	$V=10$	$V=11$
$A=0$	1	$1-\lvert\beta\rvert^2$	$\lvert\beta\rvert^2$	0
$A=1$	0	$\lvert\beta\rvert^2$	$1-\lvert\beta\rvert^2$	1
Marginal of V	$\frac{D}{2}$	$\frac{1-D}{2}$	$\frac{1-D}{2}$	$\frac{D}{2}$

Table 4: Values of $P(A=i \mid V=v)$ for two-bit probe of [2].

Thus,

$$\begin{aligned} H(A|V) &= P(V=00)H(A \mid V=00)+P(V=01)H(A \mid V=01) \\ &\quad +P(V=10)H(A \mid V=10)+P(V=11)H(A \mid V=11) \\ &= \frac{D}{2}\cdot 0+\frac{1-D}{2}\cdot h(D)+\frac{1-D}{2}\cdot h(D)+\frac{D}{2}\cdot 0 \\ &= (1-D)\cdot h(D). \end{aligned}$$

Substituting in Equation (15), we have

$$I_2^{AV} = 1-(1-D)h(D). \tag{23}$$

Again, this matches with [2, Equation 17].

If one plots the curves of I^{AV}, I_1^{AV} and I_2^{AV} against D, one can find that for all values of $D \in (0, \frac{1}{2})$, the relation $I_1^{AV} < I_2^{AV} < I^{AV}$ holds. From this, it is concluded in [2] that the six state protocol is more secure than the four state protocol. Moreover, within the six state protocol, double qubit probe gives Eve more mutual information than the one-bit probe.

3.2 Optimal Success Probability and Its Implications

We introduce a few relevant definitions first and then proceed with the analysis.

Definition 3.1 *A* **strategy** *S of the Eavesdropper is a function of her observation v such that for each v, it produces a unique guess $S(v)$ about the bit sent by Alice to Bob.*

Definition 3.2 *For some observation v, if the Eavesdropper's guess matches with the bit sent by Alice, i.e., if $S(v)=A$, we call this event a* **success**.

Definition 3.3 *For some observation v, if the Eavesdropper's guess does not match with the bit sent by Alice, i.e., if $S(v)\neq A$, we call this event a* **failure** *or an* **error**.

Thus, the *conditional error probability* of Eve is given by

$$P(error \mid V=v) = P(S(v)\neq A \mid V=v)$$

and the *error probability* of Eve is given by

$$\begin{aligned} P(error) &= \sum_v P(V=v)P(error \mid V=v) \\ &= \sum_v P(V=v)P(S(v) \neq A \mid V=v). \end{aligned}$$

The *success probability* of Eve is given by

$$P(success) = 1 - P(error).$$

Definition 3.4 *If $P(success)$ is the success probability of the Eavesdropper in guessing the bit sent by Alice through some strategy S, and $P(prior)$ is the probability denoting the Eavesdropper's prior knowledge about the bit sent by Alice before applying any strategy, then the* **advantage** *of the Eavesdropper for the particular strategy is defined as*

$$A(D) = \left| P(success) - P(prior) \right|.$$

Since Alice chooses the bit to be sent uniformly at random over $\{0,1\}$, in our case $P(prior) = \frac{1}{2}$ and so

$$A(D) = \left| P(success) = \frac{1}{2} \right|.$$

Maximizing the success probability or the advantage is equivalent to minimizing the error probability. Note that Eve's success or error probability is a feature of the particular strategy devised by Eve. Her goal is to choose the best possible strategy in determining the secret key.

Definition 3.5 *Out of all possible strategies, the one giving the maximum success probability or the minimum error probability, is called the* **optimal strategy** *S_{opt}. The corresponding success (or error) probability is called the* **optimal success (or error) probability** *of the Eavesdropper and the corresponding advantage is called the* **optimal advantage** *of the Eavesdropper.*

In the result below, we formulate how Eve can decide up on the optimal strategy.

Theorem 3.1 *The optimal strategy is given by*

$$S_{opt}(v) = \underset{i}{\operatorname{argmax}} \; P\left(A = i \mid V = v\right),$$

and the corresponding optimal success probability is given by

$$P_{opt}(success) = \sum_v \max_i P\left(A = i, V = v\right),$$

where the notation $\underset{i}{\operatorname{argmax}}$ *denotes the particular value i_{opt} of the argument i which maximizes the above conditional probability across all values i.*

Proof: Since $P(V = v)$ is independent of the strategy S, an optimum strategy that minimizes $P(\mathit{error})$ must minimize $P(S(v) \neq A \mid V = v)$ for each v. In other words, for each v, it should maximize $P(S(v) = A \mid V = v)$. This means that $S(v)$ should produce a guess $i \in \{0,1\}$ for which $P(A = i|V = v)$ is maximum. For the particular observation v, denote this optimal value of i by $i_{\mathit{opt}}(v)$. With this optimal strategy the *optimal error probability* turns out to be

$$\begin{aligned} P_{\mathit{opt}}(\mathit{error}) &= \sum_v P(V = v) P\left(A \neq i_{\mathit{opt}}(v) \mid V = v\right) \\ &= \sum_v P\left(A \neq i_{\mathit{opt}}(v), V = v\right) \end{aligned}$$

and the *optimal success probability* becomes

$$\begin{aligned} P_{\mathit{opt}}(\mathit{success}) &= 1 - P_{\mathit{opt}}(\mathit{error}) \\ &= 1 - \sum_v P\left(A \neq i_{\mathit{opt}}(v), V = v\right) \\ &= \sum_v P\left(A = i_{\mathit{opt}}(v), V = v\right) \end{aligned}$$

Hence the result follows. ■

Since $P(A = 0) = P(A = 1) = \frac{1}{2}$, if we multiply each likelihood in Tables 1, 2 and 3, we get the corresponding joint probabilities $P(A = i, V = v)$'s and the optimal success probability is given by summing the maximum joint probability (corresponding to the row $i_{\mathit{opt}}(v)$) for each column v.

Thus, for the attack model of [5], the optimal success probability is computed from Table 1 as

$$\begin{aligned} P^{4state}_{opt}(\mathit{success}) &= \frac{1}{2}\left(\frac{1}{2} + \sqrt{D(1-D)}\right) + \frac{1}{2}\left(\frac{1}{2} + \sqrt{D(1-D)}\right) \\ &= \frac{1}{2} + \sqrt{D(1-D)} = f(D). \end{aligned} \tag{24}$$

It can be easily shown that, like the mutual information, the success probabilities are also the same in both the probes (one-bit and two-bit) for the four-state protocol.

Since the the six-state protocol [2] has different mutual information between Alice and Eve for the one-bit and the two-bit probes, one may be tempted to conclude that Eve has different success probabilities in these two probes. However, we are going to show that this is not the case. In spite of having different mutual information, both the probes lead to the same success probability for the six-state protocol.

For the one-bit probe of the six-state protocol [2], the optimal success probability is computed from Table 2 as

$$\begin{aligned} P^{6state}_{opt1}(\mathit{success}) &= \frac{1}{2}\left(D + (1-D)|\beta^2|\right) + \frac{1}{2}\left(D + (1-D)|\beta|^2\right) \\ &= D + (1-D)|\beta|^2 = f_1(D). \end{aligned} \tag{25}$$

Note that in the above derivation, we have used the fact that

$$D + (1 - D)|\beta|^2 \geq 1 - D - (1 - D)|\beta^2|,$$

which follows from $D + (1 - D)|\beta^2| \geq \frac{1}{2}$ as per Equation (21).

For the two-bit probe of [2], the optimal success probability is computed from Table 3 as

$$\begin{aligned} P_{opt2}^{6state}(success) &= \frac{1}{2} \cdot D + \frac{1}{2} \cdot (1 - D)|\beta|^2 + \frac{1}{2} \cdot (1 - D)|\beta|^2 + \frac{1}{2} \cdot D \\ &= D + (1 - D)|\beta|^2 = f_1(D). \qquad (26) \end{aligned}$$

Note that in the above derivation, we have used the fact that

$$(1 - D)|\beta|^2 \geq 1 - D - (1 - D)|\beta^2|,$$

which follows from $|\beta^2| \geq \frac{1}{2}$ as per Equation (20).

Hence, we have the following result.

Theorem 3.2 *For all $D \in (0, \frac{1}{2})$,*

$$P_{opt1}^{6state}(success) = P_{opt2}^{6state}(success) < P_{opt}^{4state}(success).$$

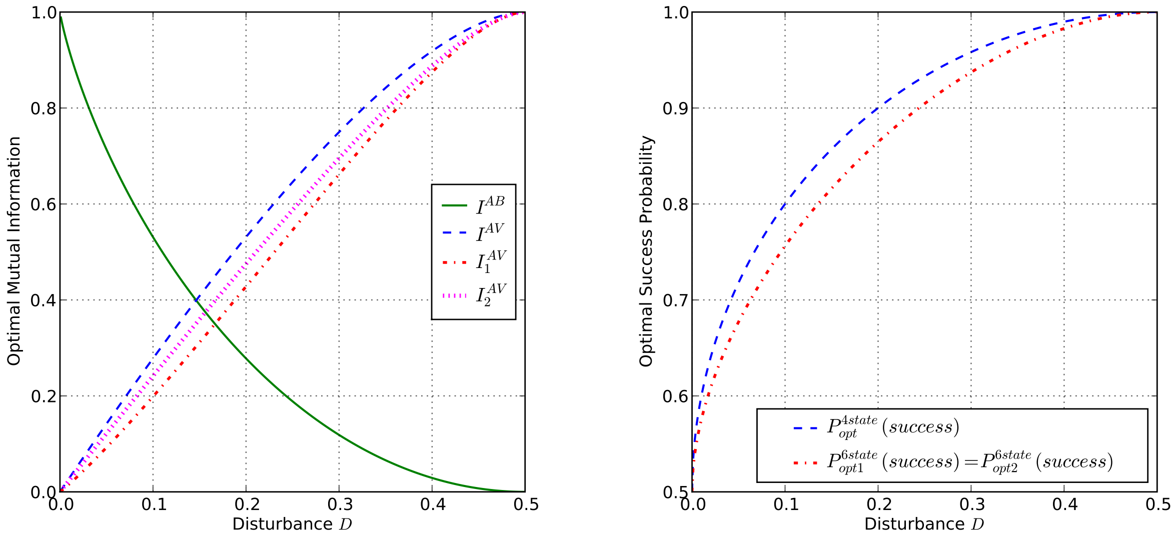

Figure 1: Optimal mutual information and optimal success probability as a function of disturbance D.

In Figure 1, we plot (as functions of the disturbance D) the optimal mutual information between Alice and Eve (on the left) and the optimal success probability of Eve's guess (on the right).

	One-Qubit Probe		Two Qubit Probe			
	$V = 0$	$V = 1$	$V = 00$	$V = 01$	$V = 10$	$V = 11$
$A = 0$	$\frac{5}{6}$	$\frac{1}{6}$	1	$\frac{1}{5}$	$\frac{4}{5}$	0
$A = 1$	$\frac{1}{6}$	$\frac{5}{6}$	0	$\frac{4}{5}$	$\frac{1}{5}$	1
Marginal of V	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{12}$	$\frac{5}{12}$	$\frac{5}{12}$	$\frac{1}{12}$

Table 5: Values of $P(A = i \mid V = v)$ for $D = \frac{1}{6}$ for both one- and two-bit probes of [2].

As an illustrative example, we show the values of the probabilities for $D = \frac{1}{6}$ in Table 5. The optimal success probability in one-bit probe is given by

$$\frac{5}{6} \cdot \frac{1}{2} + \frac{5}{6} \cdot \frac{1}{2} = \frac{5}{6}$$

and that in two-bit probe turns out to be the same:

$$1 \cdot \frac{1}{12} + \frac{4}{5} \cdot \frac{5}{12} + \frac{4}{5} \cdot \frac{5}{12} + 1 \cdot \frac{1}{12} = \frac{5}{6}.$$

But the mutual information in the first case is

$$1 + \frac{5}{6} \log_2 \frac{5}{6} + \frac{1}{6} \log_2 \frac{1}{6} = 0.3500$$

and in the second case is

$$1 + \frac{5}{6} \cdot \left(\frac{4}{5} \log_2 \frac{4}{5} + \frac{1}{5} \log_2 \frac{1}{5} \right) = 0.3984.$$

The *optimal advantages* of the eavesdropper in the four-state and in the six-state protocols are given by

$$\begin{aligned} A_{opt}^{4state}(D) &= \left| P_{opt}^{4state}(success) - \frac{1}{2} \right| \\ &= \sqrt{D(1-D)}. \end{aligned} \tag{27}$$

$$\begin{aligned} A_{opt}^{6state}(D) &= \left| P_{opt1}^{6state}(success) - \frac{1}{2} \right| \\ &= \left| P_{opt2}^{6state}(success) - \frac{1}{2} \right| \\ &= \frac{D + \sqrt{D(2-3D)}}{2}. \end{aligned} \tag{28}$$

Thus, though Eve has more mutual information in the two-bit probe, that does not give any extra cryptographic advantage in guessing the bit sent by Alice. So from the point of view of cryptanalysis, both the one-bit probe and two-bit probe are equivalent even in the six state BB84.

4 Reducing Eavesdropper's Advantage: Multi-round BB84

From Alice and Bob's point of view, the best strategy to counter-fight Eve would be to make Eve's advantage fall below the disturbance D caused by Eve. Here we are going to show that it is possible to reduce Eve's advantage by combining a number of instances of BB84.

In this direction, we define a variant of BB84, called m-BB84 in Table 6. In this protocol, Alice and Bob establish m different keys of the same length by running m independent instances of BB84 and finally establish the actual secret key by bitwise XOR-ing the individual keys together. The main idea behind this scheme is the fact that when several biased bits are XOR-ed together, the bias in the XOR output bit becomes smaller than the bias of each bit.

Protocol m-BB84

`1. Alice and Bob run` m `independent instances of BB84.`
`(The instances may either be run sequentially,`
`or they may be run in parallel through separate channels).`
`2. Suppose they establish` m `many` n`-bit secret keys, namely,`
$k_1, k_2, \ldots, k_m$`. Let` $k_{i,j}$ `be the` j`-th bit of the key` k_i `established`
`in the` i`-th instance of BB84, for` $1 \leq i \leq m$`,` $1 \leq j \leq n$`.`
`3. The` j`-th bit of the final secret key` K `is given by`
$K_j = k_{1,j} \oplus k_{2,j} \oplus \cdots \oplus k_{m,j}$`, for` $1 \leq j \leq n$`.`

Table 6: Multi-round BB84 Protocol with parameter (number of rounds) m.

The bias in K_j, the j-th bit the final key K, depends on the biases in the j-th bits of the individual keys. We can use the Piling-up Lemma [9] stated below to compute the bias in K_j. We present the proof also for the sake of completeness.

Lemma 4.1 (Piling-up Lemma) *Let ϵ_i be the bias in the binary random variable X_i, $i = 1, 2, \ldots, m$, i.e., $P(X_i = 0) = \frac{1}{2} + \epsilon_i$ and $P(X_i = 1) = \frac{1}{2} - \epsilon_i$. Then the bias in the random variable $X_1 \oplus X_2 \oplus \cdots \oplus X_m$ is given by $2^{m-1}\epsilon_1\epsilon_2 \ldots \epsilon_m$.*

Proof: The result trivially holds for $m = 1$. For $m = 2$, we have

$$\begin{aligned} & P(X_1 \oplus X_2 = 0) \\ = \; & P(X_1 = 0, X_2 = 0) + P(X_1 = 1, X_2 = 1) \\ = \; & \left(\frac{1}{2} + \epsilon_1\right)\left(\frac{1}{2} + \epsilon_2\right) + \left(\frac{1}{2} - \epsilon_1\right)\left(\frac{1}{2} - \epsilon_2\right) \\ = \; & \frac{1}{2} + 2\epsilon_1\epsilon_2 \end{aligned}$$

and hence the bias is $2^{2-1}\epsilon_1\epsilon_2$. Assume that the result holds for $m = \ell$, i.e., the bias in XOR of ℓ variables is given by $\delta = 2^{\ell-1}\epsilon_1\epsilon_2 \ldots \epsilon_l$. Now, for $k = \ell+1$, taking $Y = X_1 \oplus X_2 \oplus \cdots \oplus X_\ell$, we can apply the result for $k = 2$ to obtain the bias in $Y \oplus X_{\ell+1}$ as

$$2\delta\epsilon_{\ell+1} = 2^{\ell}\epsilon_1\epsilon_2\ldots\epsilon_{\ell+1}.$$

Hence, by induction, the result holds for any m. ■

Now, we can formulate the optimal advantage of the adversary for m-BB84 as follows.

Theorem 4.1 *For a disturbance D in each qubit, the optimal advantages of the adversary in guessing a bit of the final key of m-BB84 are given by*

$$\begin{aligned} A_{opt}^{4state}(D,m) &= 2^{m-1}\left(\sqrt{D(1-D)}\right)^m, \\ A_{opt}^{6state}(D,m) &= \frac{1}{2}\left(D + \sqrt{D(2-3D)}\right)^m, \end{aligned}$$

corresponding to four-state protocol and the six-state protocol respectively.

Proof: For any bit position j, the computation of the bias follows in the same manner. Hence, without loss of generality, fix a bit position j. Corresponding to this position, there are m key bits, each having the same bias ϵ_i, $1 \le i \le m$. The value of this bias is $A_{opt}^{4state}(D)$ or $A_{opt}^{6state}(D)$ for the four state or the six state protocol respectively. From Equations (27), (28) and Lemma 4.1, the result follows. ■

For BB84 with four states, around half of the qubits communicated by Alice to Bob is discarded due to mismatch in their bases. For the six-state protocol, the amount of discarded qubits is around two-third of the total number of qubits communicated. So for a fare comparison, we must take the same values of

1. the length of the secret key established, and

2. the total number of qubits communicated

in both the protocols. To establish a secret key of length n bits, the four state protocol must communicate around $4n$ number of qubits (in the practical scenario, the exact number is little more than $4n$) and the six state protocol must communicate around $6n$ qubits. Therefore, in order to match the total number of bits communicated, the four state protocol should be run $3t$ times and the six states protocol should be run $2t$ times for any positive integer t. In other words, we should always compare four state $3t$-BB84 with six state $2t$-BB84 for any fixed value of t. The corresponding expressions for Eve's optimal advantages can be computed by substituting $m = 3t$ and $m = 2t$ respectively in Theorem 4.1.

In Figure 2, we plot the optimal advantages of Eve as a function of the disturbance D for $D \in [0, \frac{1}{2}]$. The *blue* and *cyan* curves correspond to the four state protocol and the *red* and *magenta* curves correspond to the six state protocol. We see that for all D, $A_{opt}^{4state}(D) > A_{opt}^{6state}(D)$ (solid lines). However, with $t = 1$, we see that for a range of values of D, the curve for $A_{opt}^{4state}(D,3)$ lies below that of $A_{opt}^{6state}(D,2)$ (dashed lines). For this range, the four-state BB84 is less secure than the six-state BB84, but the four-state 3-BB84 is more secure than six-state 2-BB84.

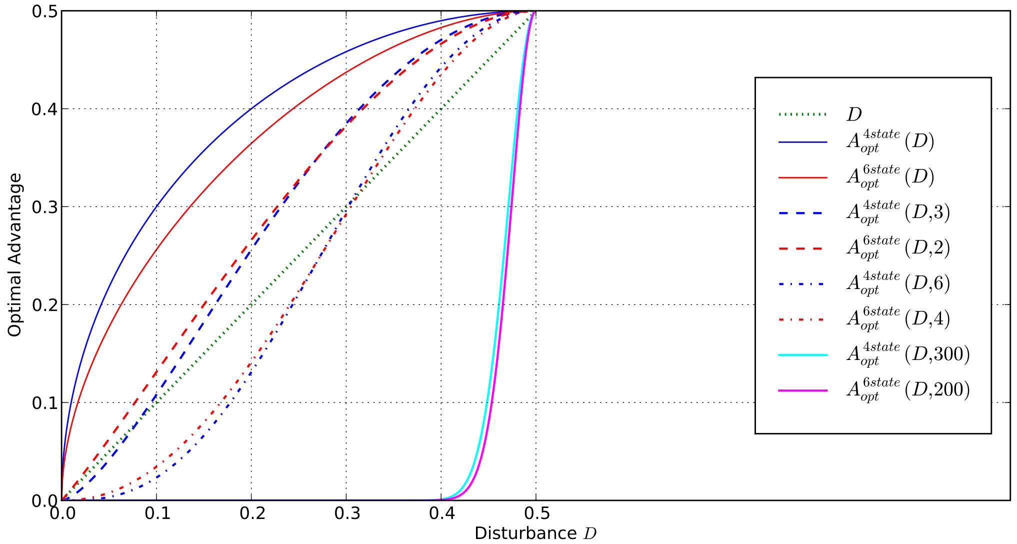

Figure 2: Optimal advantage of the eavesdropper as a function of disturbance D under different attack models.

By increasing the number of instances of BB84, Alice and Bob can reduce Eve's optimal advantage arbitrarily, even below the disturbance level D. For example, for $t = 2$, we see that both the curves for $A_{opt}^{4state}(D, 6)$ and $A_{opt}^{6state}(D, 4)$ (dash-dot lines) lie below the level D for a large portion of D's range.

In [5, Equation 76], it was shown that if $D \geq 0.146447$, then "the channel should be considered too risky for safe key generation." However, we have shown (refer to Figure 2) that by using multi-round BB84, sender and receiver can safely establish a common secret key even beyond this threshold. If the number of rounds are high enough, e.g., $t = 100$, then both $A_{opt}^{4state}(D, 300)$ and $A_{opt}^{6state}(D, 200)$ are below the level D for any value of D close to $\frac{1}{2}$ (see the *cyan* and *magenta* lines in Figure 2). In fact, for any D up to as high as 0.4, the effective advantages of the eavesdropper for both the four state 300-BB84 and the six state 200-BB84 are close to zero and Alice and Bob can safely establish a common secret key. A little beyond $D = 0.4$, there is a sharp jump in the advantage (either of $A_{opt}^{4state}(D, 300)$ or $A_{opt}^{6state}(D, 200)$) which gradually approaches the value of D, and becomes equal to $\frac{1}{2}$ when D takes the value $\frac{1}{2}$. If we keep on increasing the number of rounds, the point of the sharp jump in the advantage curve, from a value close to zero to a value close to $\frac{1}{2}$, moves further to the right, giving a broader range of security for $D \in [0, \frac{1}{2})$. This fact is formally expressed in Corollary 4.1 and 4.2.

Corollary 4.1 *At $D = \frac{1}{2}$, we have*

$$A_{opt}^{4state}(D, m) = A_{opt}^{6state}(D, m) = \frac{1}{2}$$

independent of the value of m.

Proof: Easily follows by substituting $D = \frac{1}{2}$ in the expressions for the advantages in Theorem 4.1. ∎

Corollary 4.2 *For any value of D in the interval* $0 < D < \frac{1}{2}$,

$$\lim_{m \to \infty} A_{opt}^{4state}(D, m) = 0,$$

$$\lim_{m \to \infty} A_{opt}^{6state}(D, m) = 0.$$

Proof: Take $D = \frac{1}{2} - \epsilon$, for $0 < \epsilon < \frac{1}{2}$. Then $\sqrt{D(1-D)} = \sqrt{\frac{1}{4} - \epsilon^2} < \frac{1}{2}$. Hence, this square-root is $\frac{1}{2} - \delta$, for $0 < \delta < \frac{1}{2}$. Thus,

$$\begin{aligned} A_{opt}^{4state}(D, m) &= 2^{m-1} \left(\frac{1}{2} - \delta \right)^m \\ &= \frac{1}{2}(1 - 2\delta)^m \to 0, \text{as } m \to \infty \end{aligned}$$

for any $\delta \in \left(0, \frac{1}{2}\right)$.

Again, $\sqrt{D(2-3D)} = \sqrt{\frac{1}{4} + \epsilon - 3\epsilon^2} < \frac{1}{2} + \epsilon$. Thus, $D + \sqrt{D(2-3D)} < 1$. Take this quantity to be $1 - \lambda$, for $0 < \lambda < 1$. Hence,

$$A_{opt}^{6state}(D, m) = \frac{1}{2}(1 - \lambda)^m \to 0, \text{as } m \to \infty.$$

∎

Corollary 4.1 and 4.2 together imply that at large m, there is a discontinuity at $D = \frac{1}{2}$, when the value of the advantages jump from 0 to $\frac{1}{2}$.

When BB84 is used in practice, Alice and Bob first estimate the disturbance D in the channel by sacrificing certain bits where their basis match. If the estimated D is above a threshold, then the presence of Eavesdropper may be suspected and the protocol is aborted. However, the multi-round BB84 can be executed even in the presence of very high error-rate or disturbance. In practice, Alice and Bob can first run the original BB84 scheme to estimate D. Next, using Corollary 4.3 of Theorem 4.1, they can estimate the number m of rounds to be executed to make the effective advantage of the Eavesdropper fall below the level D.

Corollary 4.3 *Given the disturbance D, the number m of rounds required for the multi-round BB84 protocol to reduce the advantage of the Eavesdropper below a threshold ϵ is given by*

$$m > \left\lceil \frac{1 + \log_2 \epsilon}{1 + \log_2 \sqrt{D(1-D)}} \right\rceil,$$

and

$$m > \left\lceil \frac{1 + \log_2 \epsilon}{\log_2 \left(D + \sqrt{D(2 - 3D)} \right)} \right\rceil ,$$

for the four-state and the six-state protocols respectively.

Proof: From Theorem 4.1, we require

$$2^{m-1} \left(\sqrt{D(1 - D)} \right)^m < \epsilon$$

for the four-state protocol and

$$\frac{1}{2} \left(D + \sqrt{D(2 - 3D)} \right)^m < \epsilon$$

for the six-state protocol. In each case, take logarithm of both sides. While dividing one logarithm by another, the inequality changes, since both the logarithms are negative. The ceiling function $\lceil \; \rceil$ is required to satisfy the condition that m has to be an integer. ■

As a concluding remark, we like to emphasize that the efficiency of multi-round BB84 comes from the fact that for a polynomial increase in the number of rounds (and hence in the number of bits communicated), Eve's optimal advantage falls exponentially.

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] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. Physcal Review Letters, 81, 3018–3021 (1998) [quant-ph/9805019].

[3] 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].

[4] T. Cover and J. Thomas. *Elements of Information Theory.* John Wiley & Sons, Inc., First Edition, 16–20 (1991).

[5] 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).

[6] M. Matsui. Linear Cryptoanalysis Method for DES Cipher. EUROCRYPT 1993, 386–397.

[7] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2002.

[8] S. J. D. Phoenix. Quantum cryptography without conjugate coding. Physical Review A, 48(1), 96–102 (1993).

[9] D. Stinson. *Cryptography Theory and Practice*. Chapman & Hall / CRC, Third Edition, 80–81 (2005).

[10] S. Wiesner. Conjugate Coding. Manuscript 1970, subsequently published in SIGACT News 15:1, 78–88, 1983.