Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84

Arpita Maitra[1]* and Goutam Paul[2]**

[1] Applied Statistics Unit, Indian Statistical Institute,
Kolkata 700 108, India.
arpita76b@rediffmail.com
[2] Department of Computer Science and Engineering,
Jadavpur University, Kolkata 700 032, India.
goutam.paul@ieee.org

Abstract. The BB84 protocol 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. In this paper, we revisit a well known eavesdropping technique against BB84. We claim that there exist certain gaps in understanding the existing eavesdropping strategy in terms of cryptanalytic view and we try to bridge those gaps in this paper.

First we refer to the result where it is shown that in the six-state variant of the BB84 protocol (Bruß, Phys. Rev. Lett., 1998), 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 the two-bit probe provides a stronger eavesdropping strategy. However, from cryptanalytic point of view, we show that Eve has the same success probability in guessing the bit transmitted by Alice in both the cases of the two-bit and the one-bit probe. Thus, we point out that having higher mutual information may not directly lead to obtaining higher probability in guessing the key bit.

It is also explained in the work of Bruß that the six-state variant of the BB84 protocol is more secure than the traditional four-state BB84. We look into this point in more detail and identify that this advantage is only achieved at the expense of communicating more qubits in the six-state protocol. In fact, we present different scenarios, where given the same number of qubits communicated, the security comparison of the four and six-state protocols is evaluated carefully.

Keywords: Advantage, BB84, Key Distribution, Optimal Eavesdropping, Quantum Cryptography.

---

* The work of the first author was supported by the WOS-A fellowship of the Department of Science and Technology, Government of India.

** This work was done in part while the second author was visiting RWTH Aachen, Germany as an Alexander von Humboldt Fellow.

1 Introduction

Establishing a common secret key between two parties at a distance is a pre-requisite for executing a symmetric key cryptographic protocol between them. The seminal paper by Diffie and Hellman [9] presents a nice idea in this direction using the Discrete Logarithm problem. However, the pioneering work of Shor [17] showed that the key distribution [9] as well as the public key crypto-systems like RSA [16] and ECC [11] are not secure in the quantum computing model. On the other hand, there are lattice and coding theory based public key algorithms [4] that are believed to be secure in the quantum computing model and these are the main focus in the domain of post-quantum cryptography. However, these algorithms are quite complex and considerable works are going on for efficient implementation of such schemes on low end devices. In this regard, it is notable that provably secure quantum key distribution protocols exist and amongst them BB84 [1] is the first and the most cited one. It has not only been verified experimentally [3] in laboratory, but now-a-days some companies are manufacturing devices [15] to implement this protocol. In this scenario, it is important to study various eavesdropping models for these protocols and this is the motivation for our current work.

The famous BB84 protocol [1] relies on the conjugate bases $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Alice randomly selects one of the two orthogonal bases and encodes 0 and 1 respectively by a qubit prepared in one of the two states in each base. To be specific, Alice encodes 0 to $|0\rangle$ or $|+\rangle$, and 1 to $|1\rangle$ or $|-\rangle$, depending on the chosen basis Z or X respectively. Bob 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 bit string, followed by error correction and privacy amplification [2], becomes the common secret key.

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 $\left\{\frac{|0\rangle+\imath|1\rangle}{\sqrt{2}}, \frac{|0\rangle-\imath|1\rangle}{\sqrt{2}}\right\}$ ($\imath = \sqrt{-1}$) 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.

The security of the BB84 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., [6, 7, 10], that studied the relationship between "the amount of information obtained by Eve" and "the amount of dis-

turbance 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* [10], the second one is known as the *coherent attack* [7]. 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 [7] for details on this and it has been commented in the same paper that given any asymmetric attack (coherent or incoherent), one can always get a symmetric attack that can match the results of the non-symmetric strategy.

In both [10, 6], 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 [5, 6] or may interact with one qubit at her disposal - both of these lead to identical results and therefore we refer any one of them as *one-bit probe*. In [6], it was claimed that the eavesdropping using the two-bit probe provides identical information to Eve using the one-bit probe in case of four-state protocol; however, for the six-state protocol, the two-bit probe leaks more information to Eve than the one-bit probe.

1.1 Organization of the Paper

In Section 2, we revisit the background material in detail. 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, i.e., she has to decide whether the i-th bit was 0 or 1. If her decided bit matches with what Alice has 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. The difference between the attacker's success probability and the probability of random guess (in this case, the probability of random guess is $\frac{1}{2}$) gives 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, though the mutual information is different.

In Section 4, we propose a multi-round version of the BB84 protocol. Using this strategy, Alice and Bob can decrease Eve's advantage. Though the concept is similar to privacy amplification [2], we study the multi-round communication as part of the key distribution steps from a different viewpoint as follows. Both in the traditional 4-state BB84 protocol [1] and in the six-state one [6], 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 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 critically evaluate the security parameters of both the protocols.

2 Review of Optimal Eavesdropping [6, 10]

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 [6, 10]. 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 [6, 10], we get certain constraints on a, b as given in Theorem 1 in the next section. If one takes a state $|\psi\rangle$ such that the conditions on a, b as given in Theorem 1 are not admitted, then the symmetric attack of [10] needs to be modified properly.

Following [19], 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 of bases 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 [13] and it has been shown that the original proposal of [1] using the conjugate bases provides the optimal security.

In the absence of eavesdropper or any channel noise, Bob exactly knows the state that has been sent by Alice, if measured in the 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-qubit 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

$$\sqrt{F}|E'_{00}\rangle = \sqrt{F}\left(|a|^2|E_{00}\rangle + |b|^2|E_{11}\rangle\right) + \sqrt{D}\left(ab^*|E_{01}\rangle + a^*b|E_{10}\rangle\right), \tag{5}$$

$$\sqrt{D}|E'_{01}\rangle = ab\sqrt{F}\left(|E_{00}\rangle - |E_{11}\rangle\right) - \sqrt{D}\left(a^2|E_{01}\rangle - b^2|E_{10}\rangle\right). \tag{6}$$

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

$$\sqrt{D}|E'_{10}\rangle = a^*b^*\sqrt{F}\left(|E_{00}\rangle - |E_{11}\rangle\right) + \sqrt{D}\left(b^{*2}|E_{01}\rangle - a^{*2}|E_{10}\rangle\right), \tag{7}$$

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

As explained in [10, 7], 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 the pairs $\{|E'_{00}\rangle, |E'_{11}\rangle\}$ 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

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

From (9) we get the following

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

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 $\pm\imath b$.

When $a = \pm b$ or $\pm\imath b$, 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 value of D as follows

$$D = \frac{1 - x}{2 - x + y}, \text{ when } a = \pm b \quad (11)$$

$$= \frac{1 - x}{2 - x - y}, \text{ when } a = \pm\imath b. \quad (12)$$

Now consider the case when 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, the vectors will be either orthogonal or the 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 $a = \pm rb, \pm\imath rb$, 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 $a = \pm \imath r b$ 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 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 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 [10] works that we discuss in the next section.

In [10], 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 [6], three conjugate bases $|0\rangle$, $|1\rangle$; $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle+\imath|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-\imath|1\rangle}{\sqrt{2}}$ 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 $a = \frac{1}{\sqrt{2}}$, $b = \frac{\imath}{\sqrt{2}}$ 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 $a \neq \pm b, \pm \imath b$ and in those case a, b are not as given in Theorem 1. As example, one can take, $|\psi\rangle = \frac{1+\imath}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|\psi_\perp\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1-\imath}{2}|1\rangle$. Symmetric attack in the attack model of [6, 10] 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 at Receiver End

In this part, we critically revisit the attack models of [10] and [6] in the light of success probability of Eve's guess about the qubit that 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, the bit received by Bob and the outcome observed by Eve due to her measurement. Eve performs the measurement after Alice and Bob announce their bases. 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 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 [8]. 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 $P(A \mid B)$ are identical with the conditionals $P(B \mid A)$. Thus,
$H(A \mid B = 0) = H(A \mid B = 1) = -D\log_2(D) - (1 - D)\log_2(1 - D)$ and
$H(A \mid B) = P(B = 0)H(A \mid B = 0) + P(B = 1)H(A \mid B = 1)$
$= -D\log_2(D) - (1 - D)\log_2(1 - D)$. So from Equation (14) we have

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

Recall that (one may refer to Section 2 for details) the general unitary transformation designed by Eve is as follows:

$U(|0\rangle, |W\rangle) = \sqrt{F}|0\rangle|E_{00}\rangle + \sqrt{D}|1\rangle|E_{01}\rangle$, and
$U(|1\rangle, |W\rangle) = \sqrt{D}|0\rangle|E_{10}\rangle + \sqrt{F}|1\rangle|E_{11}\rangle$, where $F = 1 - D$.
If we rewrite the interactions expressed in [10, Equations 50-51] in our notation, we obtain the following expressions for $|E_{ij}\rangle$'s.
$|E_{00}\rangle = \sqrt{1-D}\frac{|00\rangle+|11\rangle}{\sqrt{2}} + \sqrt{D}\frac{|00\rangle-|11\rangle}{\sqrt{2}}$, $|E_{01}\rangle = \sqrt{1-D}\frac{|01\rangle+|10\rangle}{\sqrt{2}} - \sqrt{D}\frac{|01\rangle-|10\rangle}{\sqrt{2}}$,
$|E_{10}\rangle = \sqrt{1-D}\frac{|01\rangle+|10\rangle}{\sqrt{2}} + \sqrt{D}\frac{|01\rangle-|10\rangle}{\sqrt{2}}$, $|E_{11}\rangle = \sqrt{1-D}\frac{|00\rangle+|11\rangle}{\sqrt{2}} - \sqrt{D}\frac{|00\rangle-|11\rangle}{\sqrt{2}}$.
For $i \in \{0, 1\}$, by Bayes' Theorem, Eve's posterior probability
$P(A = i \mid V = v)$ of what Alice sent is given by

$$\frac{P(A=i)\cdot P(V=v \mid A=i)}{P(V=v)} = \frac{P(A=i)\cdot P(V=v \mid A=i)}{\sum_{j=0,1} P(A=j)\cdot P(V=v \mid A=j)}$$
$$= \frac{P(V=v \mid A=i)}{P(V=v \mid A=0) + P(V=v \mid A=1)}. \quad (17)$$

Again, the likelihoods $P(V = v \mid A = i)$ are computed as

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

After the announcement of the bases in the BB84 protocol, Eve measures her qubit in the corresponding bases. The likelihoods for the attack in [10] when computed using Equation (18) turns out to be as shown in Table 1 below.

	$V=0$	$V=1$
$A=0$	$\frac{1}{2} + \sqrt{D(1-D)}$	$\frac{1}{2} - \sqrt{D(1-D)}$
$A=1$	$\frac{1}{2} - \sqrt{D(1-D)}$	$\frac{1}{2} + \sqrt{D(1-D)}$
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 [10].

For example, $P(V = 0 \mid A = 0)$ is given by $P(B = 0 \mid A = 0)P(V = 0 \mid E_{00}) + P(B = 1 \mid A = 0)P(V = 0 \mid E_{01}) = (1-D)\cdot\left(\frac{1}{\sqrt{2}}\left(\sqrt{1-D}+\sqrt{D}\right)\right)^2 + D\cdot\left(\frac{1}{\sqrt{2}}\left(\sqrt{1-D}+\sqrt{D}\right)\right)^2 = \frac{1}{2} + \sqrt{D(1-D)} = f(D)$, say.

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. In Equation (17), putting the value of $P(V = v \mid A = i)$ from Table 1, we find that 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 $H(A|V) = P(V = 0)H(A \mid V = 0) + P(V = 1)H(A \mid V = 1) = -f(D)\log_2 f(D) -$

$(1 - f(D)) \log_2 (1 - f(D))$. Substituting in Equation (15), we have

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

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 [10, Equation 65].

Next, the interactions of [6, Equations 9-15], when expressed in our notations, become $|E_{00}\rangle = \beta|10\rangle + \sqrt{1 - |\beta|^2}|01\rangle$, $|E_{01}\rangle = |00\rangle$, $|E_{10}\rangle = |11\rangle$, and $|E_{11}\rangle = \sqrt{1 - |\beta|^2}|10\rangle + \beta|01\rangle$. From Equation (13) (Section 2), we obtain, $D = \frac{1-x}{2-x}$, which gives, $x = \frac{1-2D}{1-D}$. Noting that, $x = \langle E_{00}|E_{11}\rangle$, we get

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

Technically, the square-root in Equation (20) should be written with a $\pm$ sign. However, for simplicity, we show all calculation with the $+$ sign here. The calculation with the $-$ sign would be similar.

	$V = 0$	$V = 1$
$A = 0$	$D + (1 - D)\|\beta\|^2$	$1 - D - (1 - D)\|\beta\|^2$
$A = 1$	$1 - D - (1 - D)\|\beta\|^2$	$D + (1 - D)\|\beta\|^2$
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 [6].

	$V = 00$	$V = 01$	$V = 10$	$V = 11$
$A = 0$	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 [6].

For one-bit probe, the likelihoods for [6] when computed using Equation (18) turns out to be as shown in Table 2.

From Equation (17), we find that in this case also, the posteriors are identical with the corresponding likelihoods.

For ease of calculation, let us denote

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

	$V=00$	$V=01$	$V=10$	$V=11$
$A=0$	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 [6].

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

Also, from Table 2, we have $P(V = 0) = P(V = 1) = \frac{1}{2}$, giving $H(A|V) = P(V = 0)H(A \mid V = 0) + P(V = 1)H(A \mid V = 1) = -f_1(D)\log_2 f_1(D) - (1 - f_1(D))\log_2(1 - f_1(D))$. 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 [6, Equation 18].

Now, consider the two-bit probe. The likelihoods for [6] when computed using Equation (18) turns out to be as shown in Table 3.

From Equation (17), the posteriors are computed as given in Table 4. Hence $H(A \mid V = 00) = H(A \mid V = 11) = 0$ and $H(A \mid V = 01) = H(A \mid V = 10) = -|\beta|^2\log_2|\beta|^2 - \left(1 - |\beta|^2\right)\log_2\left(1 - |\beta|^2\right) = h(D)$ (say). Thus, $H(A|V) = P(V = 00)H(A \mid V = 00) + P(V = 01)H(A \mid V = 01) + P(V = 10)H(A \mid V = 10) + P(V = 11)H(A \mid V = 11) = \frac{D}{2}\cdot 0 + \frac{1-D}{2}\cdot h(D) + \frac{1-D}{2}\cdot h(D) + \frac{D}{2}\cdot 0 = (1-D)\cdot h(D)$. Substituting in Equation (15), we have

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

Again, this matches with [6, 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 [6] that the six-state protocol is more secure than the four-state protocol. Moreover, within the six-state protocol, two-bit probe helps Eve in obtaining more mutual information than the one-bit probe. However, we present a different view on both of these claims.

3.2 Optimal Success Probability and Its Implications

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

Definition 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 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. *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

$$\begin{aligned} P(error) &= \sum_v P(V = v) P(error \mid V = v) \\ &= \sum_v P(V = v) P(S(v) \neq A \mid V = v). \end{aligned} \tag{24}$$

The *success probability* of Eve is given by $P(success) = 1 - P(error)$.

Definition 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 $A(D) = |P(success) - P(prior)|$.*

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 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 the optimal strategy.

Theorem 2. *The optimal strategy is given by*

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

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 $\underset{i}{\text{argmax}}$ *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 $P(error)$ must minimize $P(S(v) \neq A \mid V = v)$ for each v, as per Equation (24). 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 $i_{opt}(v)$. With this optimal strategy the *optimal error probability* turns out to be $P_{opt}(error) = \sum_v P(V = v)P\left(A \neq i_{opt}(v) \mid V = v\right) = \sum_v P\left(A \neq i_{opt}(v), V = v\right)$ and the *optimal success probability* becomes $P_{opt}(success) = 1 - P_{opt}(error) = 1 - \sum_v P\left(A \neq i_{opt}(v), V = v\right)$ $= \sum_v P\left(A = i_{opt}(v), V = v\right)$. 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 by $\frac{1}{2}$, 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 $i_{opt}(v)$) for each column v.

Thus, for the attack model of [10], the optimal success probability is computed from Table 1 as

$$\begin{aligned} P_{opt}^{4\text{-}state}(success) &= \frac{1}{2}\left(\frac{1}{2} + \sqrt{D(1-D)}\right) + \frac{1}{2}\left(\frac{1}{2} + \sqrt{D(1-D)}\right) \\ &= \frac{1}{2} + \sqrt{D(1-D)} = f(D). \end{aligned} \tag{25}$$

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 six-state protocol [6] 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 [6], the optimal success probability is computed from Table 2 as

$$\begin{aligned} P_{opt1}^{6\text{-}state}(success) &= \frac{1}{2}\left(D + (1-D)|\beta^2|\right) + \frac{1}{2}\left(D + (1-D)|\beta|^2\right) \\ &= D + (1-D)|\beta|^2 = f_1(D). \end{aligned} \tag{26}$$

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 [6], the optimal success probability is computed from Table 3 as

$$\begin{aligned} P_{opt2}^{6\text{-}state}(success) &= \frac{1}{2} \cdot D + \frac{1}{2} \cdot (1-D)|\beta|^2 + \frac{1}{2} \cdot (1-D)|\beta|^2 + \frac{1}{2} \cdot D \\ &= D + (1-D)|\beta|^2 = f_1(D). \end{aligned} \tag{27}$$

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

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

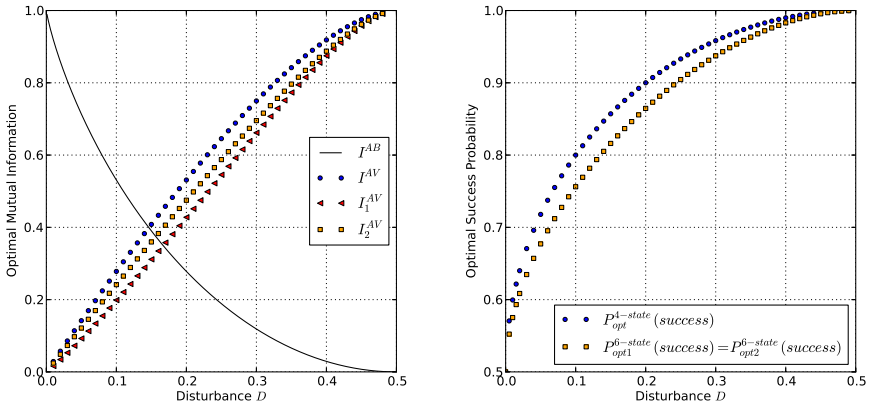

Fig. 1. Optimal mutual information and optimal success probability as a function of disturbance D.

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).

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

	One-bit Probe		Two-bit 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 [6].

$\frac{1}{2} = \frac{5}{6}$ 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 $1 + \frac{5}{6} \cdot \left(\frac{4}{5} \log_2 \frac{4}{5} + \frac{1}{5} \log_2 \frac{1}{5}\right) = 0.3984$.

According to Definition 4, the *optimal advantages* of the eavesdropper in the four-state and in the six-state protocols are respectively given by

$$A_4(D) = \sqrt{D(1-D)}. \tag{28}$$

$$A_6(D) = \frac{D + \sqrt{D(2-3D)}}{2}. \tag{29}$$

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 Comparing Four and Six-State Protocols Considering Same Number of Qubits

For BB84 with four states, on average half of the qubits communicated by Alice to Bob is discarded due to mismatch in their bases. For the six-state protocol, the expected number of discarded qubits is two-third of the total number of qubits communicated. So for a fair 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 $4n$ qubits (in the practical scenario, the exact number is little more than $4n$) and the six-state protocol must communicate around $6n$ qubits (practically little more than that). Therefore, in order to match the total number of bits communicated, the four-state protocol may be repeated $3t$ times and the six-states protocol should be repeated $2t$ times for any positive integer t.

With the above motivation, 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. The concept is in the direction to privacy amplification [2]. However, the motivation here is to compare the four-state and six-state protocol under the same footage. Any post-processing including privacy amplification can be performed on the string produced by the multi-round BB84.

The bias in K_j, the j-th bit of the final key K, depends on the biases in the j-th bits of the individual keys. We can use the Piling-up Lemma [18] stated below to compute the bias in K_j. We present the proof also for the sake of completeness.

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.

Lemma 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 $2^{m-1}\epsilon_1\epsilon_2 \ldots \epsilon_m$, considering the individual random variables as independent.*

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. *For a disturbance D in each qubit of the individual instances of BB84, the optimal advantages of the adversary in guessing a bit of the final key of m-BB84 are given by $A_4(D, m) = 2^{m-1}\left(\sqrt{D(1-D)}\right)^m$, and $A_6(D, m) = \frac{1}{2}\left(D + \sqrt{D(2-3D)}\right)^m$ corresponding to the four-state and the six-state protocols 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, $1 \leq i \leq m$. The value of this bias is given by Equation (28) for the four-state protocol and by Equation (29) for the six-state protocol. By substituting these expressions for ϵ_i in Lemma 1, the result follows. □

Note that Equations (28) and (29) can be considered as special cases of Theorem 4 with $m = 1$, i.e., they represent $A_4(D, 1)$ and $A_6(D, 1)$ respectively.

In principle, the higher the value of m, the greater is the reduction of Eve's advantage. However, one should keep in mind that with increasing m, the effective disturbance perceived by Bob also increases. We can formulate this by the following result.

Theorem 5. *For a disturbance D in the channel for each qubit of the individual instances of BB84, the effective disturbance perceived by Bob for each bit of the final key of m-BB84 is given by $\Delta(D, m) = \frac{1}{2} - 2^{m-1}\left(\frac{1}{2} - D\right)^m$.*

Proof. A disturbance D corresponds to a no-error (success) probability of $1-D = \frac{1}{2} + \left(\frac{1}{2} - D\right)$, i.e., a bias of $\left(\frac{1}{2} - D\right)$ at Bob's end. For any bit position j, the computation 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 $\epsilon_i = \left(\frac{1}{2} - D\right)$, $1 \leq i \leq m$. By Lemma 1, the equivalent bias (of no-error) for the j-th bit (and so for each bit) of the final key is given by $2^{m-1}\left(\frac{1}{2} - D\right)^m$. Thus, the equivalent no-error probability for each bit of the final key is given by $s = \frac{1}{2} + 2^{m-1}\left(\frac{1}{2} - D\right)^m$. The equivalent disturbance is given by $1 - s$. □

As discussed already, for fair comparison we should always compare four-state $3t$-BB84 with six-state $2t$-BB84 for any fixed integral value of t. Because of Theorem 5, higher t means more error for Alice and Bob. Hence, we would restrict our subsequent discussion for $t = 1$, i.e, we would compare the four-state 3-BB84 with the six-state 2-BB84, though in principle similar comparison holds for any t.

We consider three scenarios for our comparative study. Let D_4 and D_6 denote the disturbances in each qubit of the individual instances of the four and the six-state protocols respectively. For comparison in equal footing, we take $D_6 = D$ and express all the other quantities in terms of D.

4.1 Scenario 1: Equal Disturbance in Each Qubit of the Individual Instances of Four-state and Six-state BB84

Here, $D_4 = D_6 = D$. In Figure 2 (top), we plot the optimal advantages of Eve and the effective disturbances of Bob as a function of the disturbance D for $D \in [0, \frac{1}{2}]$.

As pointed out in [6], one can note that for all $D \in [0, 0.5]$, $A_4(D, 1) > A_6(D, 1)$. That is, the eavesdropper can obtain more information in the traditional 4-state BB84 [1] than the 6-state modification [6]. However, we note that $A_4(D, 3) \leq A_6(D, 2)$ for $D \leq 0.27$ (up to two decimal places). Thus, at the expense of same number of qubits, for the range of disturbance ≤ 0.27, the four-state BB84 is more secure (as eavesdropper obtains less information) than the six-state BB84 in the model we discussed above. But this greater security comes at the cost of greater effective disturbance at Bob's end, as depicted by the plot.

As a numerical example, consider $D = 0.1$. Then $A_4(D, 1) = 0.3$, which is more than $A_6(D, 1) = 0.2562$. Again, $A_4(D, 3) = 0.108$, which is less than $A_6(D, 2) = 0.1312$, implying that the four-state 3-BB84 is more secure. However,

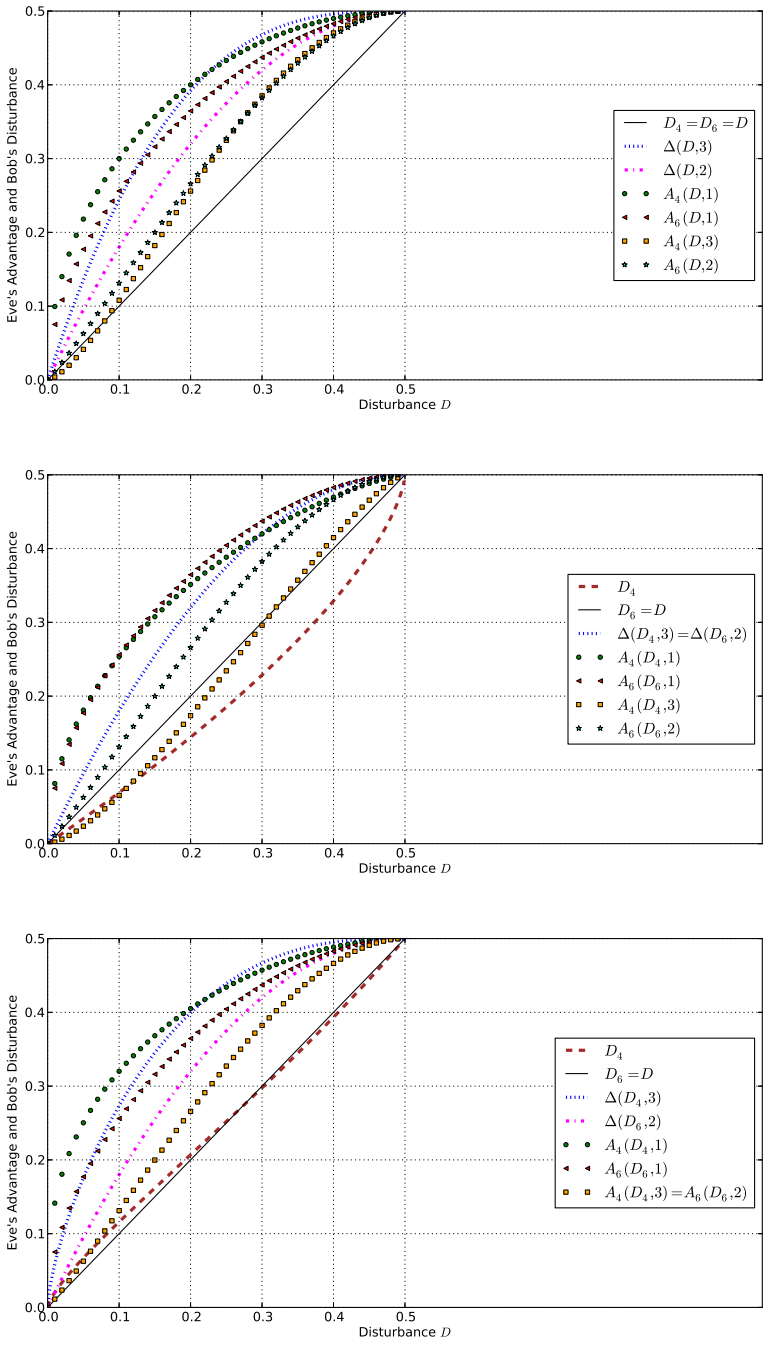

Fig. 2. Eavesdropper's advantages and Bob's disturbances against $D_6 = D$, for three cases: Scenario 1 (top), Scenario 2 (middle) and Scenario 3 (bottom).

its effective disturbance $\Delta(D_4, 3) = 0.244$ is more than that of the six-state 2-BB84 one, which is $\Delta(D_6, 2) = 0.18$.

4.2 Scenario 2: Equal Effective Disturbance in Each Bit of the Final Key of Four-state and Six-state BB84

In this scenario, we consider that Eve chooses different values of D_4 and D_6 so that the effective disturbances $\Delta(D_4, 3)$ and $\Delta(D_6, 2)$ are equal. Using Theorem 5, we can write $\Delta(D_4, 3) = \frac{1}{2} - 2^2 \left(\frac{1}{2} - D_4\right)^3$, and $\Delta(D_6, 2) = \frac{1}{2} - 2\left(\frac{1}{2} - D_6\right)^2$. Equating the right hand sides and substituting $D_6 = D$, we obtain $D_4 = \frac{1}{2} - \left(\frac{1}{2}\left(\frac{1}{2} - D\right)^2\right)^{\frac{1}{3}}$. Now we plot Eve's optimal advantages $A_4(D_4, 3)$ and $A_6(D_6, 2)$ using Theorem 4 and the quantities for Bob's disturbances in Figure 2 (middle). Note that for the entire range of D, the four-state 3-BB84 is more secure than the six-state 2-BB84.

As a numerical example, consider $D_6 = 0.1$. Then $\Delta(D_6, 2) = 0.18$. For $\Delta(D_4, 3)$ to have the same value, we must have $D_4 = 0.0691$. For the single instance, we have $A_4(D_4, 1) = 0.2536$ to be marginally less than $A_6(D_6, 1) = 0.2562$, but for multiple instances with the same number of qubits, $A_4(D_4, 3) = 0.0653$ is much less than $A_6(D_6, 2) = 0.1312$.

4.3 Scenario 3: Equal Advantages for Eve for Four-state 3-BB84 and Six-state 2-BB84

From Theorem 4, we have $A_4(D_4, 3) = 2^2 \left(\sqrt{D_4(1 - D_4)}\right)^3$, and $A_6(D_6, 2) = \frac{1}{2}\left(D_6 + \sqrt{D_6(2 - 3D_6)}\right)^2$. Equating the right hand sides and substituting $D_6 = D$, we obtain $D_4 = \frac{1}{2} - \frac{1}{2}\sqrt{1 - \left(D + \sqrt{D(2 - 3D)}\right)^{\frac{4}{3}}}$. In Figure 2 (bottom), we plot Bob's effective disturbances $\Delta(D_4, 3)$ and $\Delta(D_6, 2)$ using Theorem 5, along with Eve's advantages. Here also, the four-state protocol offers more (individual as well as effective) disturbance at Bob's end than the six-state one.

As a numerical example, consider $D_6 = 0.1$. Then $A_6(D_6, 2) = 0.1312$. For $A_4(D_4, 3)$ to have the same value, we must have $D_4 = 0.1159$. The effective disturbances are $\Delta(D_4, 3) = 0.2734 > \Delta(D_6, 2) = 0.18$. Also, for the single instances, $A_4(D_4, 1) = 0.3201 > A_6(D_6, 1) = 0.2562$.

5 Conclusion

In this paper, we revisit the symmetric incoherent eavesdropping strategy of Fuchs et al. [10] and Bruß [6] on the four and the six-state BB84 protocols respectively in the light of the success probability of Eve. We show that both the one-bit and the two-bit probes in the six-state have the same success probability for Eve. Further, we critically compare the security issues in the four and the

six-state protocols when same number of qubits are used in both the cases. Though the theoretical results of [6] as well as ours are correct, our results are placed from the cryptanalytic viewpoint of optimal eavesdropping and thus the interpretation is different from what claimed in [6].

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. C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. SIAM Journal on Computing, 17(2), 210–229 (1988).
3. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. Experimental quantum cryptography. Journal of Cryptology 5(1), pages 3–28, 1992.
4. D. J. Bernstein, J. Buchmann and E. Dahmen (Eds.). *Post-Quantum Cryptography*. Springer, 2009.
5. E. Biham and T. Mor. Bounds on Information and the Security of Quantum Cryptography. Phys. Rev. Lett. 79, 4034–4037 (1997).
6. D. Bruß. Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 81, 3018–3021 (1998) [quant-ph/9805019].
7. 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].
8. T. Cover and J. Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc., First Edition, 16–20 (1991).
9. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, pages 644–654, vol. 22, 1976.
10. 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).
11. V. Miller. Use of Elliptic Curves in Cryptography. CRYPTO 1985, pages 417–426, vol. 218, Lecture Notes in Computer Science, Springer.
12. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2002.
13. S. J. D. Phoenix. Quantum cryptography without conjugate coding. Physical Review A, 48(1), 96–102 (1993).
14. Quantum Key Distribution Equipment. ID Quantique (IDQ). `http://www.idquantique.com/`
15. Quantum Key Distribution System (Q-Box). MagiQ Technologies Inc. `http://www.magiqtech.com`
16. R. L. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, pages 120–126, vol. 21, 1978.
17. P. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science (FOCS) 1994, page 124–134, IEEE Computer Society Press.
18. D. Stinson. *Cryptography Theory and Practice*. Chapman & Hall / CRC, Third Edition, 80–81 (2005).
19. S. Wiesner. Conjugate Coding. Manuscript 1970, subsequently published in SIGACT News 15:1, 78–88, 1983.