A Note on Four-State BB84 Protocol

Arpita Maitra* and Goutam Paul#
*Applied Statistics Unit, Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India, Email: arpita76b@rediffmail.com
#Department of Computer Science and Engineering, Jadavpur University, Kolkata 700 032, India, Email: goutam.paul@ieee.org

The famous BB84 protocol relies on the conjugate bases $|0\rangle$, $|1\rangle$ and $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Fuchs et. al. (Phy. Rev. A, 1997) presented an optimal eavesdropping strategy on four-state BB84 protocol. Later Bruß (Phys. Rev. Lett., 1998) described the use of the basis $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$ along with the above two to show that the BB84 protocol with three conjugate bases (six-state protocol) provides improved security. Here we present the analysis of symmetric incoherent optimal eavesdropping strategy considering $|0\rangle$, $|1\rangle$ and a general orthogonal basis $|\psi\rangle = a|0\rangle + b|1\rangle$, $|\psi_\perp\rangle = b^*|0\rangle - a^*|1\rangle$. We could characterize the states $|\psi\rangle$, $|\psi_\perp\rangle$ based on the constraints provided by symmetric incoherent optimal eavesdropping strategy.

Keywords: BB84 Protocol, Conjugate Bases, Key Distribution, Optimal Eavesdropping, Quantum Cryptography.

INTRODUCTION

It is well known 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). This is the basic idea behind the security of the famous BB84 [1] protocol. The BB84 protocol is used by Alice and Bob to settle on a secret classical bit-string over an insecure quantum channel where Eve can have access. There are several works in the literature, e.g., [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 [4]. 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 [4] 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 [3, 5]. Alice sends a qubit $|\mu\rangle$ to Bob and Eve lets a probe $|X\rangle$ (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 $U(|\mu\rangle, |X\rangle) = |\tau\rangle$, 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 [3, 5] what optimal eavesdropping can be achieved by Eve given the disturbance at Bob's end.

The BB84 protocol [1] uses the bases $|0\rangle$, $|1\rangle$ and $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Following [8], 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. We will work with the bases $\{|0\rangle, |1\rangle\}$ and $\{|\psi\rangle, |\psi_\perp\rangle\}$. Consider $|\psi\rangle = a|0\rangle + b|1\rangle$ 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 $|a| = |b| = \frac{1}{\sqrt{2}}$. The analysis with non-conjugate bases has been presented by Phoenix [7] 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 [3] that uses three conjugate bases $|0\rangle, |1\rangle$; $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$. It is shown in the analysis of [3] that using the optimal strategy by performing certain unitary transformation on the transmit-

ted qubit, an eavesdropper can extract less information in the six-state scheme [3] than the case with four-state scheme [5] for a fixed disturbance of the qubit that Bob receives. Both in the traditional 4-state BB84 protocol [1] and in the six-state one [3], Bob measures first and then Alice publishes the bases she used. Thus, the disadvantage of the the six-state scheme [3] is that, on an average, only $\frac{1}{3}$ of qubits are kept and rest $\frac{2}{3}$ are discarded, which is worse than in the case of four-state scheme, where half of the received qubits are discarded.

In this work, we use on the bases $|0\rangle, |1\rangle$ and $|\psi\rangle$, $|\psi_\perp\rangle$. We consider $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\psi_\perp\rangle = b^*|0\rangle - a^*|1\rangle$ and then characterize the values of a, b based on the eavesdropping model presented in [3, 5]. We take each of a, b nonzero as otherwise both the base will coincide (upto rotation). It is also trivial to see that $|a|^2 + |b|^2 = 1$ from normality condition. Under the symmetric incoherent optimal eavesdropping strategy [3, 5], 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 [5] needs to be modified properly.

OUR RESULTS

In this section we present the detailed analysis of our results. 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-qubit state $|X\rangle$. 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.

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

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.

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

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

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

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

$$\begin{aligned} U(|\psi\rangle, |X\rangle) &= |0\rangle(a\sqrt{F}|E'_{00}\rangle + b^*\sqrt{D}|E'_{01}\rangle) \\ &\quad + |1\rangle(b\sqrt{F}|E'_{00}\rangle - a^*\sqrt{D}|E'_{01}\rangle). \quad (4) \end{aligned}$$

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

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

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

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

As explained in [4, 5], 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

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

The case when $0 < x, y < 1$

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 $\pm ib$.

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

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

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

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 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 [5] works that we discuss in the next section.

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 1. Thus, symmetric attack is not directly possible in these cases when y is nonzero. To have symmetric attack in these cases, Eve needs to do a so-called phase-covariant cloner that reaches the same information as in BB84.

Eavesdropping as in [5]

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 $D = \frac{1-x}{2-x+y}$.

Now, in line of [5], let us explain how Eve can optimize the information about the qubit sent by Alice. As in [5], consider $x = \cos\alpha$ and $y = \cos\beta$. Thus, the probability that Eve guesses the qubit sent by Alice correctly is $P_e = FP_\alpha + DP_\beta$, where $P_\alpha = \frac{1+\sin\alpha}{2}$ and $P_\beta = \frac{1+\sin\beta}{2}$. It has been shown in [5] that optimal eavesdropping is achieved when $\alpha = \beta$ (i.e., $x = y$) and immediately one can get $P_e = \frac{1+\sqrt{1-x^2}}{2} = \frac{1}{2} + \sqrt{D(1-D)}$, where $D = \frac{1-x}{2-x+y} = \frac{1-x}{2}$. Thus inducing a disturbance D, Eve can correctly guess the qubit sent by Alice with a probability $P_e = \frac{1}{2} + \sqrt{D(1-D)}$.

Eavesdropping as in [3]: $0 < x < 1$, $y = 0$

In [3], 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 $D = \frac{1-x}{2-x}$.

The probability that Eve guesses the qubit sent by Alice correctly is $P_e = FP_\alpha + DP_\beta$, where $P_\alpha = \frac{1+\sin\alpha}{2}$ and

$P_\beta = \frac{1+\sin\beta}{2}$. In this case, $\cos\beta = 0$, i.e., $\sin\beta = 1$ and so $P_\beta = 1$. Thus, from $P_e = (1-D)\frac{1+\sqrt{1-x^2}}{2} + D$, we obtain, $P_e = \frac{1}{2}\left(1 + D + \sqrt{D(2-3D)}\right)$.

It has been correctly pointed out in [2, 3] that the study made so far is the situation when Eve either measures only one of her two bits, or if she uses a 1-bit probe from the beginning. In order to optimize Eve's probability of correctly guessing the qubit Alice has sent, in the six-state scheme [3] another analysis has been presented where the eavesdropper requires both the qubits at her hand as resource. This is unlike the scenario for traditional BB84 protocol where 1-qubit probe is sufficient to reach optimality [2, 3]. That is, as in [3], we study the optimal eavesdropping strategy where both the qubits at Eve's end are used.

Take an orthogonal basis $\{|u\rangle, |v\rangle\}$. Consider the case when Bob measures in the same basis in the one that Alice sent, but due to Eve's interference Bob measures $|v\rangle$ though Alice did send $|u\rangle$. In such a case, Eve can deterministically distinguish two orthogonal states associated with Bob's wrong measurement. After privacy amplification and error correction, Alice and Bob actually discards such state and Eve can as well ignore it. Thus in this case, $P_e = P_\alpha$, where P_α is as above and thus, $P_e = \frac{1}{2}\left(1 + \frac{1}{1-D}\sqrt{D(2-3D)}\right)$.

Concluding notes

Let us now see how one can obtain such $|\psi\rangle$, $|\psi_\perp\rangle$ using unitary operators. We need $\mathcal{U}(|0\rangle) = |\psi\rangle$ and $\mathcal{U}(|1\rangle) = |\psi_\perp\rangle$ where $\mathcal{U}$ is the unitary operator represented in a matrix form as $\mathcal{U} = \begin{bmatrix} a & b^* \\ b & -a^* \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{i\theta_1} & e^{-i\theta_2} \\ e^{i\theta_2} & -e^{-i\theta_1} \end{bmatrix}$, where $a = \frac{1}{\sqrt{2}}e^{i\theta_1}$ and $b = \frac{1}{\sqrt{2}}e^{i\theta_2}$ with $\theta_1 - \theta_2 \not\equiv 0 \bmod \frac{\pi}{2}$. As example, one can take, $|\psi\rangle = \frac{1+i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|\psi_\perp\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1-i}{2}|1\rangle$. In this case, $\mathcal{U}$ is of the form

$$\mathcal{U} = \begin{bmatrix} \frac{1+i}{2} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1-i}{2} \end{bmatrix} = \frac{1}{2}\sigma_z + \frac{i}{2}\sigma_0 + \frac{1}{\sqrt{2}}\sigma_x, \text{ where}$$

$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ are the Pauli matrices [6, Page 65].

[1] C. H. Bennett and G. Brassard. Quantum Cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, IEEE, New York (1984).

[2] E. Biham and T. Mor. Bounds on Information and the Security of Quantum Cryptography. Physical Review Letters, 79, 4034–4037 (1997).

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

[4] 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].

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

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

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