Undergraduate Research Opportunities Programme in Science

The Utility of Phase-Covariant Quantum Cloning in Quantum Cryptography

KELVIN KOOR KAI JIE

SUPERVISOR:

VALERIO SCARANI

Abstract

In this report, we discuss how a certain class of quantum cloning, 'Phase-Covariant Quantum Cloning' could be used by a potential eavesdropper to attack the BB84 protocol. We will consider two cases, one with the help of an 'ancilla' and the other without.

Contents

1 Introduction

Quantum Cryptography is the science (some might prefer the word 'art') of exploiting quantum mechanics to perform cryptographic tasks. In general, Quantum Cryptography comprises numerous techniques and applications, such as Quantum Key Distribution (QKD), Quantum Coin Tossing, Quantum Commitment et cetera, but the one relevant to us here is QKD. Like all cryptographic protocols, quantum cryptography is without exception susceptible to attacks. One particular attack depends on 'quantum cloning'. After discussing what that is exactly, we will study its application in attacks on quantum cryptographic protocols.

Before delving into the technicalities, let us first discuss the foundations and basics of the ideas involved.

2 Preliminaries

Here we shall quickly recap the basics of the density operator formalism and important concepts in classical information theory like the Shannon entropy and mutual information. Knowledge of the tensor product and its usage in quantum mechanics is assumed.

2.1 The Density Operator Formalism

We have learned that in quantum mechanics, a quantum system is assigned a 'state' living in a Hilbert Space. But in practice, we might not even know with perfect certainty the state of the system. For example, consider a collection of atoms in a black box with only the information that a fraction of them are in state $|\psi_1\rangle$, another fraction in state $|\psi_2\rangle$ and so on, for a total of n states. How are we to characterize an atom then? We can only say that it has a probability p_i of being in state $|\psi_i\rangle$ for $i = 1, 2, ..., n$. In such a scenario, we say that our information about the system is incomplete.

John von Neumann came up with a mathematical formalism to address this, which came to be known as the density operator formalism. In the

formalism, we denote the state of the quantum system by the density operator, ρ. A system is said to be in a **pure state** if we know its state with perfect certainty, and in a **mixed state** if we do not.

2.1.1 Single and Composite Systems

Let us first consider a single system (we want to describe the state of a single system).

> Pure State, $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \sum c_i |i\rangle$, $|i\rangle$ are the eigenkets.
>
> Mixed State, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

Note the distinction between the two *different* probabilities, $|c_i|^2$ and p_i. The former is the quantum mechanical probability which we have encountered countless times, while the latter encapsulates our lack of certainty about the state of the system. $|c_i|^2$ is the probability for $|\psi\rangle$ to jump into the eigenstate $|i\rangle$ upon measurement and p_i is simply the probability of finding the system in the state $|\psi_i\rangle$ in the first place. It is obvious that a pure state is a special case of the more general mixed state, where $p_i = 0$ for all i's except one, say j, and $p_j = 1$. Also note that $\sum_i |c_i|^2 = 1$ and $\sum_i p_i = 1$.

Things get considerably more exciting when we start considering composite systems. For simplicity let us consider a bipartite system, A and B. What follows can be easily generalized to an n-partite system.

> Pure State, $\rho = |\psi^{AB}\rangle\langle\psi^{AB}|$, where $|\psi^{AB}\rangle = \sum c_{ij} |ij\rangle$, $|ij\rangle$ are the eigenkets of $\mathcal{H}_A \otimes \mathcal{H}_B$.
>
> Mixed State, $\rho = \sum_i p_i |\psi_i^{AB}\rangle\langle\psi_i^{AB}|$

For composite systems, we are further interested in another kind of state: the **separable state**.

Separable State, $\rho = \sum_i w_i \, \rho_i^A \otimes \rho_i^B$
where $\rho_i^A \in \mathcal{L}(\mathcal{H}_A)$, $\rho_i^B \in \mathcal{L}(\mathcal{H}_B)$. In general, both ρ_i^A and ρ_i^B are mixed states. Also note that $\sum_i w_i = 1$.

Entangled State: By definition, a state that is not separable.

Product State, $\rho = \rho^A \otimes \rho^B$, a special case of the separable state where where $w_i = 0$ for all i's except one, say j, and $p_j = 1$.

Remark. *A pure, separable state is always a product state.*

Properties of the Density Operator:

1. ρ is Hermitian.
2. $Tr(\rho) = 1$
3. $\langle\psi| \, \rho \, |\psi\rangle \geq 0 \; \forall \, |\psi\rangle$
4. $Tr(\rho^2) \leq 1$ with equality only for pure states.

2.1.2 The Bloch Sphere

The **Bloch Sphere** is a geometrical representation of the state of a qubit (two-level quantum system), named after Felix Bloch. We will make reference to it when we discuss phase-covariant quantum cloning later.

The general state (general in this context means the state could be either pure or mixed) of a qubit with two eigenstates, traditionally denoted as $|0\rangle$ and $|1\rangle$, could be parametrized by r, θ and ϕ in this form:

$$\rho = \frac{\mathbb{I} + \vec{n} \cdot \vec{\sigma}}{2}$$

where $\vec{\sigma}$ is the Pauli Vector encountered in quantum mechanics. $\vec{n}$ is the Bloch Vector:

$$\vec{n} = \begin{bmatrix} r \sin\theta \cos\phi \\ r \sin\theta \sin\phi \\ r \cos\theta \end{bmatrix}$$

where $r = |\vec{n}| \leq 1$, with equality only for pure states.

Illustrated below is the Bloch Sphere. We represent a qubit state by a point on/inside the sphere. The surface of the Bloch Sphere represents all the pure states of a qubit, whereas the interior represents all the mixed states. The origin corresponds to the *maximally mixed* state: $\rho = \frac{\mathbb{I}}{2}$.

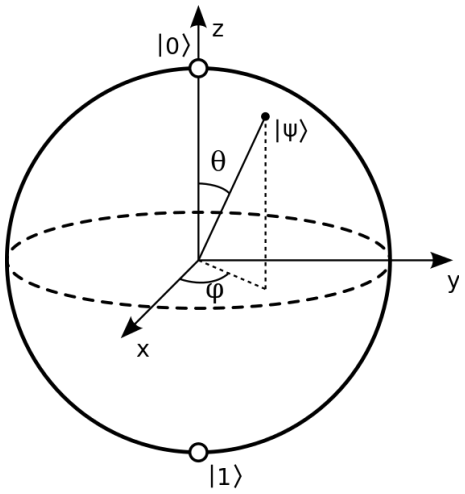

Figure 1: The Bloch Sphere

Remark. *The* $|\psi\rangle$ *in Figure 1 is given by* $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$.

2.1.3 Partial Trace and Reduced Density Operators

Consider a pure state ρ^{AB} of a bipartite system. We would like to obtain separately the individual states ρ^A and ρ^B, which in this context are called **reduced density operators**. To do so, we take the **partial trace** of ρ^{AB}. The process of partial tracing is best shown via examples.

To get ρ^A, we 'trace out' ρ^B:

$$\rho^A = Tr_B(\rho^{AB}) = \sum_i {}_B\langle i|\, \rho^{AB}\, |i\rangle_B \;\; where \;\; |i\rangle_B \in \mathcal{H}_B$$

To get ρ^B, we 'trace out' ρ^A:

$$\rho^B = Tr_A(\rho^{AB}) = \sum_i {}_A\langle i|\, \rho^{AB}\, |i\rangle_A \;\; where \;\; |i\rangle_A \in \mathcal{H}_A$$

Let us now consider two concrete examples.

Example I

Let $|\psi^{AB}\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$.

$$\begin{aligned}\rho^{AB} = |\psi^{AB}\rangle\,\langle\psi^{AB}| &= \frac{1}{2}\Big(\,|0\rangle \otimes \big(\,|0\rangle + |1\rangle\,\big)\Big)\Big(\,\langle 0| \otimes \big(\,\langle 0| + \langle 1|\,\big)\Big) \\ &= \frac{1}{2}\,|0\rangle\,\langle 0| \otimes \big(\,|0\rangle\,\langle 0| + |1\rangle\,\langle 0| + |0\rangle\,\langle 1| + |1\rangle\,\langle 1|\,\big)\end{aligned}$$

$$\rho^{A} = \sum_{i=0,1} {}_{B}\langle i|\,\rho^{AB}\,|i\rangle_{B} = |0\rangle\,\langle 0|$$

$$\rho^{B} = \sum_{i=0,1} {}_{B}\langle i|\,\rho^{AB}\,|i\rangle_{A} = \frac{1}{2}\,|0\rangle\,\langle 0| \otimes \big(\,|0\rangle\,\langle 0| + |1\rangle\,\langle 0| + |0\rangle\,\langle 1| + |1\rangle\,\langle 1|\,\big)$$

In this example, $\rho^{AB} = \rho^{A} \otimes \rho^{B}$, it is a product state.

Example II

Let $|\psi^{AB}\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$.

$$\begin{aligned}\rho^{AB} = |\psi^{AB}\rangle\,\langle\psi^{AB}| &= \frac{1}{2}\Big(\,|00\rangle\,\langle 00| + |11\rangle\,\langle 00| + |00\rangle\,\langle 11| + |11\rangle\,\langle 11|\,\Big) \\ &= \frac{1}{2}\Big(\,|0\rangle\,\langle 0| \otimes |0\rangle\,\langle 0| + |1\rangle\,\langle 0| \otimes |1\rangle\,\langle 0| + \\ &\quad |0\rangle\,\langle 1| \otimes |0\rangle\,\langle 1| + |1\rangle\,\langle 1| \otimes |1\rangle\,\langle 1|\,\Big)\end{aligned}$$

$$\rho^{A} = \rho^{B} = \sum_{i=0,1} {}_{B(A)}\langle i|\,\rho^{AB}\,|i\rangle_{B(A)} = \frac{\mathbb{I}}{2}$$

In this example, ρ^{A} and ρ^{B} are both mixed (maximally mixed, in fact). So we see even if ρ^{AB} is pure, ρ^{A} and ρ^{B} themselves need not be so. Here, ρ^{AB} is pure and entangled.

2.2 Key concepts in classical information theory

2.2.1 Shannon Entropy

Let us have a **discrete random variable** X whose probability function is $p(x) \equiv p(X = x)$. The **Shannon entropy** of X, denoted $H(X)$ is given by

$$H(X) = -\sum_x p(x) \log p(x)$$

where the logarithm is of base 2. Note that because $0 \leq p(x) \leq 1,\ H(X) \geq 0$. $H(X)$ is interpreted as the uncertainty/unknown knowledge about X, or equivalently, the amount of information we need in order to know what value X has taken on.

Joint Entropy of X and Y,

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y)$$

Conditional Entropy,

$$H(Y|X) \equiv \sum_x p(x) H(Y|X = x) = -\sum_{x,y} p(x, y) \log p(y|x)$$

Chain Rule:

- $H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
- Furthermore, if Z is a third random variable, $H(X, Y|Z) = H(X|Z) + H(Y|X, Z) = H(Y|Z) + H(X|Y, Z)$

2.2.2 Mutual Information

Let X, Y have the joint probability function $p(x, y)$ and the marginal probability functions $p(x), p(y)$.

Mutual Information of X and Y,

$$I(X; Y) \equiv \sum_{x,y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)}$$

Relation between the Shannon Entropies of X and Y and their mutual information:

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X,Y) \end{aligned}$$

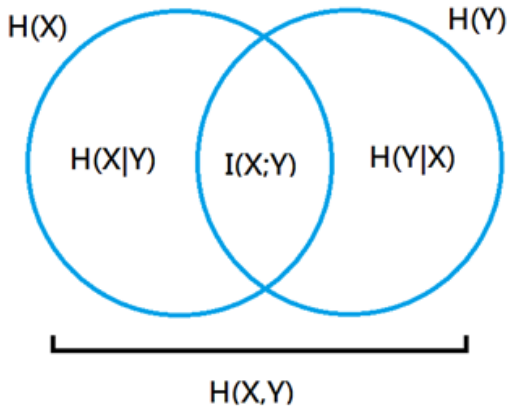

Figure 2: In a nutshell

3 Quantum Key Distribution

3.1 A recap of cryptography

Here is a quick recap of cryptography: We have a sender, traditionally called Alice, who wants to deliver a message to her counterpart, the receiver traditionally called Bob. To do so, they must first share a mutually known, but otherwise secret **key**. Alice disguises her intended message for Bob, called the **plaintext**, with the key. The disguised message is called the **ciphertext**. She then broadcasts the ciphertext (in any way she finds convenient). It is irrelevant whether any third parties get hold of this message since it would appear nonsensical; what matters is that Bob receives it. Bob then makes use of the key to retrieve the plaintext. The method of encryption and decryption with the key is called the **cipher**.

3.2 'The unbreakable cipher'

Let us consider a particular cipher. Here, the key shared between Alice and Bob possesses a few characteristics, and this together with the encryption and decryption techniques (all to be discussed shortly) form what became known as the **One-Time Pad (OTP)** (also known as the Vernam Cipher).

This is how the OTP works:

1. Long before any message transmission takes place, Alice and Bob are to agree to assign to every alphabet a corresponding unique binary number, i.e. each alphabet is written as a unique binary sequence of 0's and l's. For example, they could let $A = 0001$, $B = 0010$, $C = 0011$, $D = 0100$, $E = 0101$ etc. The word 'bad bee' would then read 001000010100001001010101. Furthermore, Alice and Bob **randomly generate** the key, also a string of 0's and 1's, which has to be reasonably long since it must be at least as long as any future message(s). The longer the key, the more messages could be encrypted and decrypted.

2. Alice creates the **ciphertext** by performing the **XOR** operation ($\oplus$, or + mod 2) bitwise between the plaintext and the key. She sends the ciphertext to Bob.

3. Bob retrieves the plaintext from the ciphertext by also performing the XOR operation bitwise between the ciphertext and the key.

Here is an example illustrating the encryption of the plaintext and decryption of the ciphertext with the key:

Creating the ciphertext using '10100101' as the plain text and '11010010' as the key:

$$\begin{aligned} & 10100101 \\ \oplus\ & 11010010 \\ \rightarrow\ & 01110111 \end{aligned}$$

Retrieving the plaintext from the ciphertext:

$$\begin{aligned} & 01110111 \\ \oplus\ & 11010010 \\ \rightarrow\ & 10100101 \end{aligned}$$

The OTP is said to be unbreakable in the sense that every possible sequence of alphabets is equally likely to be the plaintext! This was proved mathematically by the legendary Claude Shannon, although intuitively it isn't too hard to see why this is so given that the key is, we emphasize again, **completely randomly generated**.

However, it should be apparent by now that there is a serious drawback with this seemingly flawless cipher: what if Alice wants to send a really, really long message to Bob? What if Bob has to reply, thus starting a correspondence between the two that could go on and on? It would be impractical for Bob and Alice to carry the key with themselves at all times (remember, the key is supposed to be as long as the message). We see that the OTP shifts the problem from secure communication to key distribution.

One solution to the key distribution problem is public key cryptography. However, the security of public key cryptography rests on as of now still unproven computational presumptions. A well known example is the RSA cryptosystem (named after Rivest, Shamir and Adlerman). Its security is based on the difficulty of large integer factoring. Thus public key cryptography is still vulnerable to unforeseen advances in our computational capabilities.

This is where QKD comes in. Using the BB84 protocol described in the next section, we rely on the *laws of physics* to distribute the keys.

3.3 The BB84 Protocol

The Bennett and Brassard protocol (BB84) is a quantum key distribution protocol. The goal of Alice is to send the KEY (of the one-time pad) to Bob, not the message itself. Here is how it works:

1. Alice and Bob agree on using a particular qubit system, and decides on using four states, specifically the Stern-Gerlach z and x states, which we shall denote as $|+z\rangle, |-z\rangle, |+x\rangle$ and $|-x\rangle$. Note that $\langle -z| + z\rangle = \langle -x| + x\rangle = 0$, $|+z\rangle = \frac{1}{\sqrt{2}}\big(|+x\rangle + |-x\rangle\big)$ and $|-z\rangle = \frac{1}{\sqrt{2}}\big(|+x\rangle - |-x\rangle\big)$.

2. $|+z\rangle$ and $|+x\rangle$ are given the bit value '0' while $|-z\rangle$ and $|-x\rangle$ are given the bit value '1'. Note that there is still a distinction between the measurement bases.

3. Now Alice sends Bob a sequence of qubits, each independently and randomly chosen from one of the four states above.

4. For each qubit received, Bob randomly chooses one of the two measurement bases to measure the qubit, i.e. using the $z-$ basis half of the time and the $x-$ basis half of the time.

5. Alice and Bob broadcast their bases used and discard all events where they have used different bases. This process is called sifting. Insofar as there exists no Eve nor any noise, Alice and Bob should have a common string of $0's$ and $1's$ now.

Here is a table illustrating said process:

Alice's sent bits	0	1	1	0	1	0	0	1
Alice's bases	z	z	x	z	x	x	x	z
Bob's measurement bases	z	x	x	x	z	x	z	z
Bob's measured bits	0	0	1	0	1	0	1	1
Comparing bases		$\neq$		$\neq$	$\neq$		$\neq$	
Common Bit values	0		1			0		1

So the shared key between Alice and Bob is 0101. But of course, this is what we get only if we neglect Eve and noise, which we shouldn't.

Here is what could happen if Eve attacks (this is also where we should get paranoid and attribute all noise to Eve).

Alice's sent bits	0	1	1	0	1	0	0	1
Alice's bases	z	z	x	z	x	x	x	z
Eve tampers around.								
Bob's measurement bases	z	x	x	x	z	x	z	z
Bob's measured bits	0	0	0	1	1	0	1	0
Comparing bases		$\neq$		$\neq$	$\neq$		$\neq$	
Common Bit values	0		error			0		error

And we see that with unwanted interference, errors would be introduced into the sequence which should have been identical for both Alice and Bob. Alice and Bob now need to perform error correction and privacy amplification as a countermeasure. We shall not discuss these topics here.

4 Quantum Cloning

(Perfect) Quantum Cloning is a mechanism that takes an arbitrary, unknown quantum state and reproduces an exact copy (clone) without altering the original state in any way. We shall see that this is forbidden by the laws of quantum mechanics as illustrated by the No-Cloning Theorem.

Although perfect quantum cloning is not feasible, it is possible to perform imperfect quantum cloning, where the copies have non-unit fidelities. 'Fidelity' is a quantity that measures the degree of similarity between the original state and the copy made. For perfect cloning, the fidelity of the copy is unity. Another term we shall encounter is the Quantum Cloning Machine, or QCM. It is simply the device(s) with which we try to perform quantum cloning.

4.1 The No-Cloning Theorem

No-Cloning Theorem: There exists no mechanism that can perfectly replicate an arbitrary, unknown quantum state.

Proof. In this proof, we shall be generous and allow the possibility of an 'ancilla' qubit to help with the cloning. We shall show that even with ancillae, perfect cloning is not realizable.

Let $|\psi\rangle$ be the state to be cloned, $|R\rangle$ be the blank reference state (to be cloned into $|\psi\rangle$ and $|A_i\rangle$ be the initial ancilla state. Suppose that perfect cloning is realizable, i.e. there exists a unitary operator U such that for any state $|\psi\rangle$,

$$U\,|\psi\rangle\,|R\rangle\,|A_i\rangle = |\psi\rangle\,|\psi\rangle\,|A(\psi)\rangle\,^{1}$$

In particular, for two orthogonal states labelled $|0\rangle$ and $|1\rangle$, we have

$$U\,|0\rangle\,|R\rangle\,|A_i\rangle = |0\rangle\,|0\rangle\,|A(0)\rangle$$
$$U\,|1\rangle\,|R\rangle\,|A_i\rangle = |1\rangle\,|1\rangle\,|A(1)\rangle$$

Then the linearity of operators in the formalism of quantum mechanics gives us

$$U\big(\,|0\rangle + |1\rangle\,\big)\,|R\rangle\,|A_i\rangle = |00\rangle\,|A(0)\rangle + |11\rangle\,|A(1)\rangle$$

On the other hand, by definition of how this unitary operator works, we should have obtained

$$U\big(\,|0\rangle + |1\rangle\,\big)\,|R\rangle\,|A_i\rangle = \big(\,|0\rangle + |1\rangle\,\big)\big(\,|0\rangle + |1\rangle\,\big)\,|A(0+1)\rangle$$

The two expressions are clearly not the same, hence contradicting our assumption that there exists a U capable of carrying out quantum cloning. □

[1] We have for notational simplicity omitted the tensor product symbols.

4.2 Fidelity

Earlier, we mentioned that fidelity measures how close the original state and the copy made are to each other. We properly define fidelity now.

The fidelity of the i^{th} copy of the (imperfect) cloning machine is defined as

$$F_i = \langle\psi|\, \rho_i \,|\psi\rangle$$

where ρ_i is the copy's reduced density operator.

4.3 Phase-Covariant Quantum Cloning (PCQC)

We have seen that perfect quantum cloning is impossible. That however does not preclude the possibility of imperfect quantum cloning; indeed, there exists numerous such methods. For our purposes here we shall focus on the technique now known as phase-covariant quantum cloning, applied onto qubits.

First, a QCM is called **universal** if it copies all input states $|\psi\rangle$ equally well, i.e. F_i is independent of $|\psi\rangle$. Non-universal QCM are called **state-dependent**. A phase-covariant QCM is state-dependent, but *universal for qubits on the equator of the Bloch Sphere* . These qubits are of the form

$$|\psi(\varphi)\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{i\varphi}\,|1\rangle\,\big) \tag{1}$$

The term 'phase-covariant' comes from the fact that the fidelity of the copies of these states would be independent of φ, the azimuthal angle illustrated in Figure 1.

We consider first the case without an ancilla:
The unitary operator associated with this QCM is given by[2]

$$U\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle \tag{2}$$

$$U\,|1\rangle\,|0\rangle = c\,|1\rangle\,|0\rangle + s\,|0\rangle\,|1\rangle \tag{3}$$

[2]Again, we have omitted the tensor product for notational simplicity.

where c and s are real numbers satisfying $c^2 + s^2 = 1$. After evolution, the first ket of every term represents that of the first copy, and similarly for the second ket of each term. Then we have

$$U\left|\psi(\varphi)\right\rangle\left|0\right\rangle = \frac{1}{\sqrt{2}}\Big(\left|00\right\rangle + e^{i\varphi}c\left|10\right\rangle + e^{i\varphi}s\left|01\right\rangle\Big) \tag{4}$$

The evolved state (describing both copies) is entangled. Its density operator is

$$\begin{aligned}\rho = U\left|\psi(\varphi)0\right\rangle\left\langle\psi(\varphi)0\right|U^\dagger = \frac{1}{2}\Big(& s^2\left|0\right\rangle\left\langle 0\right|\otimes\left|1\right\rangle\left\langle 1\right| + e^{-i\varphi}s\left|0\right\rangle\left\langle 0\right|\otimes\left|0\right\rangle\left\langle 1\right| \\ &+ e^{i\varphi}s\left|0\right\rangle\left\langle 0\right|\otimes\left|1\right\rangle\left\langle 0\right| + sc\left|1\right\rangle\left\langle 0\right|\otimes\left|0\right\rangle\left\langle 1\right| \\ &+ sc\left|0\right\rangle\left\langle 1\right|\otimes\left|1\right\rangle\left\langle 0\right| + \left|0\right\rangle\left\langle 0\right|\otimes\left|0\right\rangle\left\langle 0\right| \\ &+ e^{i\varphi}c\left|1\right\rangle\left\langle 0\right|\otimes\left|0\right\rangle\left\langle 0\right| + e^{-i\varphi}c\left|0\right\rangle\left\langle 1\right|\otimes\left|0\right\rangle\left\langle 0\right| \\ &+ c^2\left|1\right\rangle\left\langle 1\right|\otimes\left|0\right\rangle\left\langle 0\right|\Big)\end{aligned} \tag{5}$$

The reduced density operators obtained by partial-tracing ρ are

$$\rho_I = Tr_{II}(\rho) = \frac{1}{2}\Big(\left|0\right\rangle\left\langle 0\right| + c^2\left|1\right\rangle\left\langle 1\right| + s^2\left|0\right\rangle\left\langle 0\right| + e^{i\varphi}c\left|1\right\rangle\left\langle 0\right| + e^{-i\varphi}c\left|0\right\rangle\left\langle 1\right|\Big) \tag{6}$$

$$\rho_{II} = Tr_I(\rho) = \frac{1}{2}\Big(\left|0\right\rangle\left\langle 0\right| + s^2\left|1\right\rangle\left\langle 1\right| + c^2\left|0\right\rangle\left\langle 0\right| + e^{i\varphi}s\left|1\right\rangle\left\langle 0\right| + e^{-i\varphi}s\left|0\right\rangle\left\langle 1\right|\Big) \tag{7}$$

The fidelities are

$$F_I = \left\langle\psi(\varphi)0\right|U^\dagger\rho_I U\left|\psi(\varphi)0\right\rangle = \frac{1}{2}(1+c) \tag{8}$$

$$F_{II} = \left\langle\psi(\varphi)0\right|U^\dagger\rho_{II} U\left|\psi(\varphi)0\right\rangle = \frac{1}{2}(1+s) \tag{9}$$

which are indeed independent of φ.

The version with an ancilla is constructed by symmetrizing (2) and (3):

$$U\left|000\right\rangle = \left|000\right\rangle \tag{10}$$

$$U\left|100\right\rangle = c\left|100\right\rangle + s\left|010\right\rangle \tag{11}$$

$$U\left|011\right\rangle = c\left|011\right\rangle + s\left|101\right\rangle \tag{12}$$

$$U\left|111\right\rangle = \left|111\right\rangle \tag{13}$$

where the third ket in each term represents the ket for the ancilla qubit. In the next section, we finally see how phase-covariant quantum cloning could be used in attacks on BB84.

5 Attacking BB84 with PCQC

5.1 Generalities

In section 3.3, we have seen how Eve attacking the BB84 protocol could induce errors in Bob's sequence of received bits, but we didn't explore the nature of Eve's attacks then. In this section, we investigate the scenario where Eve uses PCQC in her attack.

The attack we're about to discuss is classified as an **incoherent** attack. In this attack, Eve interacts (copies with the QCM) each qubit sent from Alice to Bob individually. After Alice and Bob reveal their measurement bases and carry out sifting, Eve measures her copies of the qubits, now that she knows which measurement basis to use for each copied qubit. After this is done, Alice's, Bob's and Eve's bits (either 0 or 1) comprise a list of *classical random variables*, with a probability distribution $P(A, B, E)$.

During error correction and privacy amplification, Alice and Bob are to reduce the rate of errors in their sequence. To do so, they extract just a fraction of bits from their original sequence, in a certain manner. This 'subsequence' of bits forms the key that should be used by Alice and Bob.

It is a well-known result in classical information theory that for the new key to be acceptable, R, the ratio of the length of the extracted subsequence to the length of the original sequence, must satisfy the Csiszár-Körner Bound:

$$R = I(A;B) - min\{I(A;E), I(B;E)\}$$

where $I(X;Y)$ is the mutual information between parties X and Y. We now consider two different kinds of QCMs Eve could use: one without ancillae and the other with an ancillary qubit.

5.2 Without Ancillae

For clarity, let us replace the unitary operator U (which represents the QCM used by Eve) by an arrow $\rightarrow$.

$$|\psi(\varphi)\rangle_A |0\rangle_{E_i} \rightarrow \frac{1}{\sqrt{2}}\Big(|0\rangle_B |0\rangle_E + e^{i\varphi} c |1\rangle_B |0\rangle_E + e^{i\varphi} s |0\rangle_B |1\rangle_E \Big)$$

This is just another way of writing (4). The subscripts A and B are clear in this context; E_i represents Eve's qubit before the cloning and E represents her qubit after cloning. We shall subsequently omit the subscripts for convenience.

Now for simplicity, consider the case where Alice has sent $|+x\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle \big)$. The entangled state describing both Bob's and Eve's qubits is $\frac{1}{\sqrt{2}}\Big(|00\rangle + c|10\rangle + s|01\rangle \Big)$, just (4) with $\varphi = 0$. Bob's qubit state is $\rho_B = \frac{1}{2}\big(\mathbb{I} + s^2\sigma_z + c\sigma_x\big)$, just (6) with $\varphi = 0$ and where we have written the state in the $\{|0\rangle, |1\rangle\}$ basis. Similarly, Eve's qubit state is $\rho_E = \frac{1}{2}\big(\mathbb{I} + s^2\sigma_z + c\sigma_x\big)$.

The fidelities of Bob's and Eve's qubits are given by (8) and (9), as expected of a phase-covariant QCM. They respectively give the probabilities of Bob's and Eve's qubits to jump into the state $|+x\rangle$ upon measurement. Therefore we see that Eve, by utilizing a phase-covariant QCM in an incoherent attack on Alice's and Bob's channel, has a $\frac{1}{2}(1+s)$ chance of guessing the state sent by Alice correctly.

5.3 With Ancillae

Consider again the case where Alice sends $|+x\rangle$. In fact, let us consider the case for $|-x\rangle$ as well. Here, Eve prepares her blank qubit state to be $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle \big)$. From (10)-(13), we see that

$$|\pm x\rangle \otimes \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle \big) \rightarrow |\Gamma^{\pm}\rangle_{BE_1E_2} = \frac{1}{2}\Big(|000\rangle + c|011\rangle + s|101\rangle \pm c|100\rangle \pm s|010\rangle \pm |111\rangle \Big) \tag{14}$$

Let us explore what Eve can do with her two qubits. To do so, we first make a few change of bases.

For Bob's qubit, we make a CoB from $\{|0\rangle, |1\rangle\}$ to $\{|+x\rangle, |-x\rangle\}$ where

$$|\pm x\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle \pm |1\rangle\,\big)$$

For Eve's two qubits, we make a CoB from the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ to the Bell Basis $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ where

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle \pm |11\rangle\,\big)$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}\big(\,|01\rangle \pm |10\rangle\,\big)$$

Applying the CoB to $|\Gamma^\pm\rangle_{BE_1E_2}$ in (14) requires us to make the following replacements:

$$|0\rangle \to \frac{1}{\sqrt{2}}\big(\,|+x\rangle + |-x\rangle\,\big)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}\big(\,|+x\rangle - |-x\rangle\,\big)$$

for the first ket term and

$$|00\rangle \to \frac{1}{\sqrt{2}}\big(\,|\Phi^+\rangle + |\Phi^-\rangle\,\big)$$
$$|11\rangle \to \frac{1}{\sqrt{2}}\big(\,|\Phi^+\rangle - |\Phi^-\rangle\,\big)$$
$$|01\rangle \to \frac{1}{\sqrt{2}}\big(\,|\Psi^+\rangle + |\Psi^-\rangle\,\big)$$
$$|10\rangle \to \frac{1}{\sqrt{2}}\big(\,|\Psi^+\rangle - |\Psi^-\rangle\,\big)$$

for the second and third kets in each term. Doing so, (14) becomes

$$
\begin{aligned}
|\Gamma^{\pm}\rangle_{BE_1E_2} = \frac{1}{4}\Big\{ &\big(|{+x}\rangle + |{-x}\rangle\big)\big(|\Phi^+\rangle + |\Phi^-\rangle\big) \\
&+c\big(|{+x}\rangle + |{-x}\rangle\big)\big(|\Phi^+\rangle - |\Phi^-\rangle\big) \\
&+s\big(|{+x}\rangle - |{-x}\rangle\big)\big(|\Psi^+\rangle + |\Psi^-\rangle\big) \\
&\pm c\big(|{+x}\rangle - |{-x}\rangle\big)\big(|\Phi^+\rangle + |\Phi^-\rangle\big) \\
&\pm s\big(|{+x}\rangle + |{-x}\rangle\big)\big(|\Psi^+\rangle - |\Psi^-\rangle\big) \\
&\pm \big(|{+x}\rangle - |{-x}\rangle\big)\big(|\Phi^+\rangle - |\Phi^-\rangle\big)\Big\}
\end{aligned}
\tag{15}
$$

Next, Eve performs a unitary transformation (NOT associated with any cloning this time) on (15) whereby

$$
\begin{aligned}
|\Phi^+\rangle &\to |00\rangle \\
|\Phi^-\rangle &\to |11\rangle \\
|\Psi^+\rangle &\to |10\rangle \\
|\Psi^-\rangle &\to |01\rangle
\end{aligned}
\tag{16}
$$

to get $|\tilde{\Gamma}^{\pm}\rangle_{BE_1E_2}$. Finally, creating the new symbols $F = \frac{1+c}{2}$, $D = 1-F = \frac{1-c}{2}$, $|\chi_{\pm}\rangle = \sqrt{F}\,|0\rangle \pm \sqrt{D}\,|1\rangle$ and reformulating $|\tilde{\Gamma}^{\pm}\rangle_{BE_1E_2}$ in terms of them,we have

$$
|\tilde{\Gamma}^{\pm}\rangle_{BE_1E_2} = \sqrt{F}\,|{\pm x}\rangle\,|\chi_{\pm}\rangle\,|0\rangle \mp \sqrt{D}\,|{\mp x}\rangle\,|\chi_{\mp}\rangle\,|1\rangle \tag{17}
$$

To summarize, the entangled state describing Bob's qubit and Eve's qubits coming out of the QCM is given by $|\Gamma^{\pm}\rangle_{BE_1E_2}$, upon which Eve applies a unitary transformation to obtain $|\tilde{\Gamma}^{\pm}\rangle_{BE_1E_2}$:

$$
(14) \xrightarrow{CoB} (15) \xrightarrow{UT\ given\ by\ (16)} (17)
$$

What Eve does now is to measure qubit E_2 in the z-basis. If she gets $|0\rangle$, she knows that Bob's bit is identical to Alice's; if she gets $|1\rangle$, she knows that Bob's bit is opposite to Alice's. This implies that Eve has as much information on Bob's bit as she has on Alice's bit: $I(A;E) = I(B;E)$.

5.4 Conclusion

Eve, by utilizing a phase-covariant QCM in an incoherent attack on Alice's and Bob's channel, has a $\frac{1}{2}(1+s)$ chance of guessing the state sent by Alice correctly. By making use of an ancillary qubit in her QCM, she is able to

'symmetrize' her information on Alice's and Bob's qubits. God forbid what she might do next. As a clarification, whatever she does, the best she can do is to make Alice and Bob decide to discard the key. *Eve does not get hold of any information Alice wants to send to Bob.*

References

[1] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin and Antonio Acín "*Quantum Cloning*" Rev. Mod. Phys. 77, 1225-1256 (2005)

[2] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus and Momtchil Peev "The Security of Practical Quantum Key Distribution" Rev. Mod. Phys. 81, 1301 (2009)

[3] Michael A. Nielsen and Isaac L. Chuang "*Quantum Computation and Quantum Information*" Cambridge University Press (2010)

[4] Giuliano Benenti, Giulio Casati and Giuliano Strini "*Principles of Quantum Computation and Information*" World Scientific Publishing (2004)