

Mixed States in Quantum Cryptography

Ansis Rosmanis, Ilze Dzelme-Bērziņa
Institute of Mathematics and Computer Science,
University of Latvia

Abstract – Mixed states are important in quantum computation and quantum information theories. Each quantum mixed state can be described by its density matrix. We discuss how properties of mixed states and their density matrices can be used to explain fundamentals of most popular quantum computing protocols. By using density matrices we show that some of quantum protocols are safe, but some of them allow cheating.

Keywords: Quantum Cryptography, Mixed State, Protocol

1 Introduction

The roots of quantum cryptography goes back to the work of Stephen Weisner called "Conjugate Coding" from the early 1970s, which was published more then ten years latter [3]. By that time Bennet and Brassard , who were familiar with Weisner's idea, described the first quantum cryptographic communication protocol, called BB84 [1]. Quantum cryptographic systems take advantage of either the Heisenberg uncertainty principle or quantum entanglement. According to the Heisenberg uncertainty principle a measurement of the quantum system in general disturbs it and yields incomplete information about its state before the measurement. Therefore eavesdropping on a quantum communication channel causes an unavoidable disturbance, alerting the legitimate users. Ekert [2] discovered a new type of quantum key generation protocols, security of which was not based on the Heisenberg uncertainty principle, as in the case of BB84, but on the completeness of quantum mechanics.

2 Quantum Mixed States

A pure state can be described by a ket vector $|\psi\rangle$, which can be extended in the basis set of eigenstates $|\psi_i\rangle$ of an arbitrary Hermitian operator that represents an observable of the system to $|\psi\rangle = \sum_i a_i |\psi_i\rangle$ ($\sum_i a_i^2 = 1$).

Pure states are fundamental objects for quantum mechanics in the sense that evolution of any closed system can be seen as a unitary evolution of pure states. However, to deal with opened and composed quantum systems the concept of mixed state is important.

A probability distribution $\{(p_i, \psi_i) | 1 \leq i \leq n\}$ on pure states $\{\psi_i\}_{i=1}^n$ with probabilities $0 \leq p_i \leq 1$, $\sum_{i=1}^n p_i = 1$ is called a mixed state or mixture, and denoted by $[\phi] = \{(p_i, \psi_i) | 1 \leq i \leq n\}$ or $[\phi] = (p_1, \psi_1) \oplus (p_2, \psi_2) \oplus \dots \oplus (p_n, \psi_n)$, where symbol \oplus is used just to separate particular pure states and their probabilities.

Each mixed state $[\phi\rangle$ can be represented by a density operator $\rho_{[\phi\rangle}$. If $[\phi\rangle=|\psi\rangle$ for a pure state $|\psi\rangle$, then $\rho_{[\phi\rangle}=|\psi\rangle\langle\psi|$. If $[\phi\rangle=p_i, |\psi_i\rangle_{i=1}^n$, where $|\psi_i\rangle$ are pure states, then
$$\rho_{[\phi\rangle}=\sum_{i=1}^n p_i |\psi_i\rangle\langle\psi_i|.$$

The representation of pure states depends on the choice of the basis the same is true for density operators, which are uniquely represented in the matrix form through density matrices.

Theorem 1. If a mixed state $[\phi\rangle=p_i, |\psi_i\rangle_{i=1}^n$ is measured in an orthonormal basis $\{|\beta_k\rangle\}$, then the outcome is $|\beta_k\rangle$ with probability $\langle\beta_k|\rho|\beta_k\rangle$.

Corollary 1. If the measurement of the mixed state $[\phi\rangle=p_i, |\psi_i\rangle_{i=1}^n$ is performed in the standard basis, then the probability to be in the state k is equal to $Pr[k]=\rho_{k,k}$, the diagonal entry on the density matrix ρ .

Now we will list several properties of the density matrix:

1. $Tr(\rho)=1$, which follows from Corollary 1, since the sum of probabilities $Pr[k]$ is equal to 1.
2. ρ is Hermitian. It is true as $(\psi\psi^*)^*=\psi\psi^*$.
3. Eigenvalues of ρ are non-negative. As eigenvalues of a Hermitian matrix are real, the same is true for a density matrix. Suppose λ and $|e\rangle$ are an eigenvalue-eigenvector pair. And we perform a measurement in the eigenbasis, then $Pr[e]=\langle e|\rho|e\rangle=\lambda\langle e|e\rangle=\lambda$. Since the probability must be non-negative, $\lambda\geq 0$.

Theorem 2. For a density matrix $\rho : \rho=\rho^2$ iff ρ is a pure state. If ρ is a density matrix for mixed state then $\rho^2<\rho$ and $Tr(\rho^2)<1$.

Theorem 3. If ρ is a density matrix for a pure state then it has one eigenvalue equal to 1 and all other eigenvalues equal to zero.

Theorem 4. ρ is a density matrix if ρ is Hermitian, $\rho\geq 0$ and $Tr(\rho)=1$.

The trace distance between ρ_1 and ρ_2 is $\|\rho_1-\rho_2\|_{Tr}=\sum_i |\lambda_i|$, where λ_i is eigenvalue of $\rho_1-\rho_2$.

The distance of two probability distributions with respect to a basis F is defined as $|D_{\rho_1}-D_{\rho_2}|_F=\sum (Pr_{\rho_1}[i]-Pr_{\rho_2}[i])$.

Theorem 5. The maximal distance $|D_{\rho_1}-D_{\rho_2}|_F$ between two probability distributions is equal to the trace distance $\|\rho_1-\rho_2\|_{Tr}$.

3 Quantum Cryptographic Protocols

3.1 Polarization and Observables

Quantum cryptographic protocols often use non-orthogonal quantum states. We will often discuss the four following quantum states $|0\rangle, |1\rangle, |0'\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$ and $|1'\rangle=\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$. Because of the qubit physical realization the quantum cryptography uses term polarization. Let us say that the qubits $|0\rangle$ and $|1\rangle$ are rectilinearly polarized and the qubits $|0'\rangle$ and $|1'\rangle$ are diagonally polarized. We can see that $\langle 0|1\rangle=0$ and also $\langle 0'|1'\rangle=0$.

Now let us consider two observables: rectilinear observable B which consists of two linear subspaces generated by vectors $|0\rangle$ and $|1\rangle$, diagonal observable B' generated by vectors $|0'\rangle$ and $|1'\rangle$. If we have rectilinearly polarized qubit and we make a measurement in rectilinear basis, we

obtain same qubit, but if we make a measurement in diagonal basis, qubit collapses to $|0'\rangle$ with probability $\frac{1}{2}$ and to $|1'\rangle$ with probability $\frac{1}{2}$. A diagonally polarized qubit analogically collapses measured in rectilinear basis. Also we will consider observable B'' which is “between” these two. Observable B'' consists of two linear subspaces generated by vectors $\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ and $\sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle$. This is called Breidbart basis

3.2 Quantum Key Distribution

The aim of Alice and Bob is to generate secret binary key they could use to crypt their messages.

Protocol:

At first Alice is generating two random sequences of bits which determinate qubits she is sending to Bob. First sequence determinates whether she is using rectilinear or diagonal polarization. Second whether she is sending $|0\rangle$ or $|1\rangle$ if rectilinear polarization has been chosen and $|0'\rangle$ or $|1'\rangle$ otherwise. Meanwhile Bob has generated his random sequence which determinates whether to measure qubits in observable B or B' . Then Bob announces publicly which measurements he made and Alice announces whether he made the correct measurement or not. For correct measurements each bit Alice sent is the same bit Bob got at the measurement. Hence the sequence of bits gotten at correct measurements is generated key. Then they are comparing publicly some randomly chosen subset of these bits to be sure that none eavesdropping has taken place.

Eavesdropping:

Even for a single qubit eavesdropper Eve cannot know which polarization Alice is using. Let us assume Eve is using observable B for all qubits. If Alice sends rectilinearly polarized qubit, Eve always gets correct bit of information and doesn't change the qubit. If Alice sends diagonally polarized qubit, Eve gets correct bit with probability $\frac{1}{2}$ and always corrupt qubit and Bob detects this corruption with probability $\frac{1}{2}$. So for each bit the eavesdropping can be detected with probability $\frac{3}{4}$.

Let us consider the case when Eve is making her measurements in Breidbart basis. Because of symmetry let us assume that Alice sends $|1\rangle$.

$$|1\rangle = \sin\frac{\pi}{8}\left(\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle\right) - \cos\frac{\pi}{8}\left(\sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle\right)$$

Always Eve gets correct bit with probability $\cos^2\frac{\pi}{8} \approx 0.85$ but also corrupts the qubit. After Eve's measurement we can say there is a mixed state.

$$\begin{aligned} |\phi_1\rangle &= \left(\sin^2\frac{\pi}{8}, \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle\right) \oplus \left(\cos^2\frac{\pi}{8}, \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle\right) \\ \rho_{|\phi_1\rangle} &= \sin^2\frac{\pi}{8} \begin{pmatrix} \cos^2\frac{\pi}{8} & \cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ \cos\frac{\pi}{8}\sin\frac{\pi}{8} & \sin^2\frac{\pi}{8} \end{pmatrix} + \cos^2\frac{\pi}{8} \begin{pmatrix} \sin^2\frac{\pi}{8} & -\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ -\cos\frac{\pi}{8}\sin\frac{\pi}{8} & \cos^2\frac{\pi}{8} \end{pmatrix} \\ &= \begin{pmatrix} 1/4 & -1/4 \\ -1/4 & 3/4 \end{pmatrix} \end{aligned}$$

Hence, if Bob makes correct measurement (the rectilinear in this case), he gets $|1\rangle$ with probability $\frac{3}{4}$. This means that the eavesdropping can be easily detected by public comparison of bits. After that these bits have been taken out of the key.

3.3 Quantum Bit Commitment

Alice can choose bit and get committed to it in a following sense. Alice cannot change the bit and Bob cannot know Alice's bit. When Alice decides she can reveal the bit. Classically Alice could write her bit on a paper, place it in a safebox and give it to Bob. When she wanted she could tell Bob the key of the safebox.

Protocol:

If Alice's secret bit is 0, she uses rectilinear basis. Then she randomly chooses key which is one bit determining weather to send $|0\rangle$ or $|1\rangle$. If the secret bit is 1, she uses diagonal basis and sends $|0'\rangle$ or $|1'\rangle$. When Alice wants to reveal the bit she tells Bob the bit and the key. Then Bob makes measurement at corresponding observable and compares result with the key. So he can verify that Alice has not changed the bit.

Cheating:

At first, let us consider the case when the secret bit is 0. Bob doesn't know weather the key is 0 or 1. He can assume that it is 0 with probability $\frac{1}{2}$ and 1 with same probability. Hence from Bob's point of view he possesses mixed state

$$|\phi_0\rangle = \left(\frac{1}{2}, |0\rangle\right) \oplus \left(\frac{1}{2}, |1\rangle\right),$$

$$\rho_{|\phi_0\rangle} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

If the secret bit is 1, from Bob's point of view he possesses mixed state

$$|\phi_1\rangle = \left(\frac{1}{2}, |0'\rangle\right) \oplus \left(\frac{1}{2}, |1'\rangle\right),$$

$$\rho_{|\phi_1\rangle} = \frac{1}{2} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} + \frac{1}{2} \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

Density matrices corresponding to the secret bit 0 and 1 are equal. Hence trace distance between them is 0. From theorem 5 follows that states $|\phi_0\rangle$ and $|\phi_1\rangle$ cannot be distinguished in any way (if Bob measures them in arbitrary basis, he always gets same results with same probabilities). So Bob cannot cheat and get information about the secret bit before Alice tells it to him.

But there is possibility for Alice to cheat. It is known that every mixed state in system S can be expressed in extended system S_e as pure state (S is subspace of S_e). Let us consider two pure states $|\psi_0\rangle_{AB}$ and $|\psi_1\rangle_{AB}$ which are two qubit systems where Alice possesses one qubit and Bob other one. If the density matrices for Bob's qubits are equal, then there is unitary transformation U_A which uses only Alice's qubit so that $U_A |\psi_0\rangle_{AB} = |\psi_1\rangle_{AB}$. Because of this, Alice can change the secret bit at any time before telling it to Bob. It can be done by using quantum entanglement. Alice produces EPR pair $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and sends second qubit of it to Bob.

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{2}|00'\rangle + \frac{1}{2}|01'\rangle + \frac{1}{2}|10'\rangle - \frac{1}{2}|11'\rangle = \frac{1}{\sqrt{2}}|0'0'\rangle + \frac{1}{\sqrt{2}}|1'1'\rangle$$

If Alice wants the secret bit to be 0, she measures her qubit in the rectilinear basis, but in the diagonal basis for the secret bit 1. After the measurement Bob's qubit collapses to the result Alice has obtained in her measurement. Since she knows Bob's qubit, she can tell him correct key.

It is proved that there is no secure quantum bit commitment protocol.

3.4 Quantum Coin-Flipping

Alice and Bob can flip coin over a distance in such a way that neither of them can determinate the outcome of the flip but both can agree on the outcome in spite of the fact that they do not trust each other.

Protocol:

Alice randomly chooses whether she will use rectilinear or diagonal polarization. Then she is generating a random sequence of bits which determinates qubits she is sending to Bob. Meanwhile Bob has generated his random sequence which determinates whether to measure qubits in observable B or B' . (like in quantum key distribution protocol with a difference that Alice always use same polarization). Then Bob makes a guess whether Alice was using rectilinear or diagonal polarization. Alice tells whether his guess is correct (heads) or incorrect (tails). After that Bob can know which qubits was measured in correct basis and compare them to Alice's qubits.

Cheating:

The proof that Bob cannot cheat is analog to quantum bit commitment protocol. And again Alice can cheat by using quantum entanglement. When Bob has made the guess Alice can decide whether Bob's guess has to be true or not. If Alice wants it to be true, she measures her qubits at correct basis, otherwise she uses incorrect basis.

4 References

- [1] Bennett, Charles H., Brassard, G., Quantum cryptography: Public key distribution and coin tossing. International Conference on Computers, Systems & Signal Processing, Bagalore, India, (1984) 175 - 179.
- [2] Ekert, Artur K., Quantum cryptography based on Bells theorem. Phys. Rev. Lett. 67 (1991) 661663.
- [3] Wiesner, S., Conjugate coding. Sigact News, vol. 15, no. 1 (1983) 78 – 88
- [4] Gruska, J., Quantum Computing. McGraw-Hill (1999).
- [5] Nayak, A., Optimal Lower Bounds for Quantum Automata and Random Access Codes. Proc. 40th FOCS, (1999) 369-377