Quantum Cryptography: On the Security of the BB84 Key-Exchange Protocol

Thomas Baignères

EPFL - LASEC
(thomas.baigneres@epfl.ch)

Contents

Basics of quantum mechanics - Superposition Principle

A two dimensional quantum system is a qubit. It can be in one of two mutually distinguishable states $|0\rangle$ and $|1\rangle$, or in both at the same time (superposition of states):

$$\alpha\,|0\rangle + \beta\,|1\rangle \quad \text{where} \quad |\alpha|^2 + |\beta|^2 = 1$$

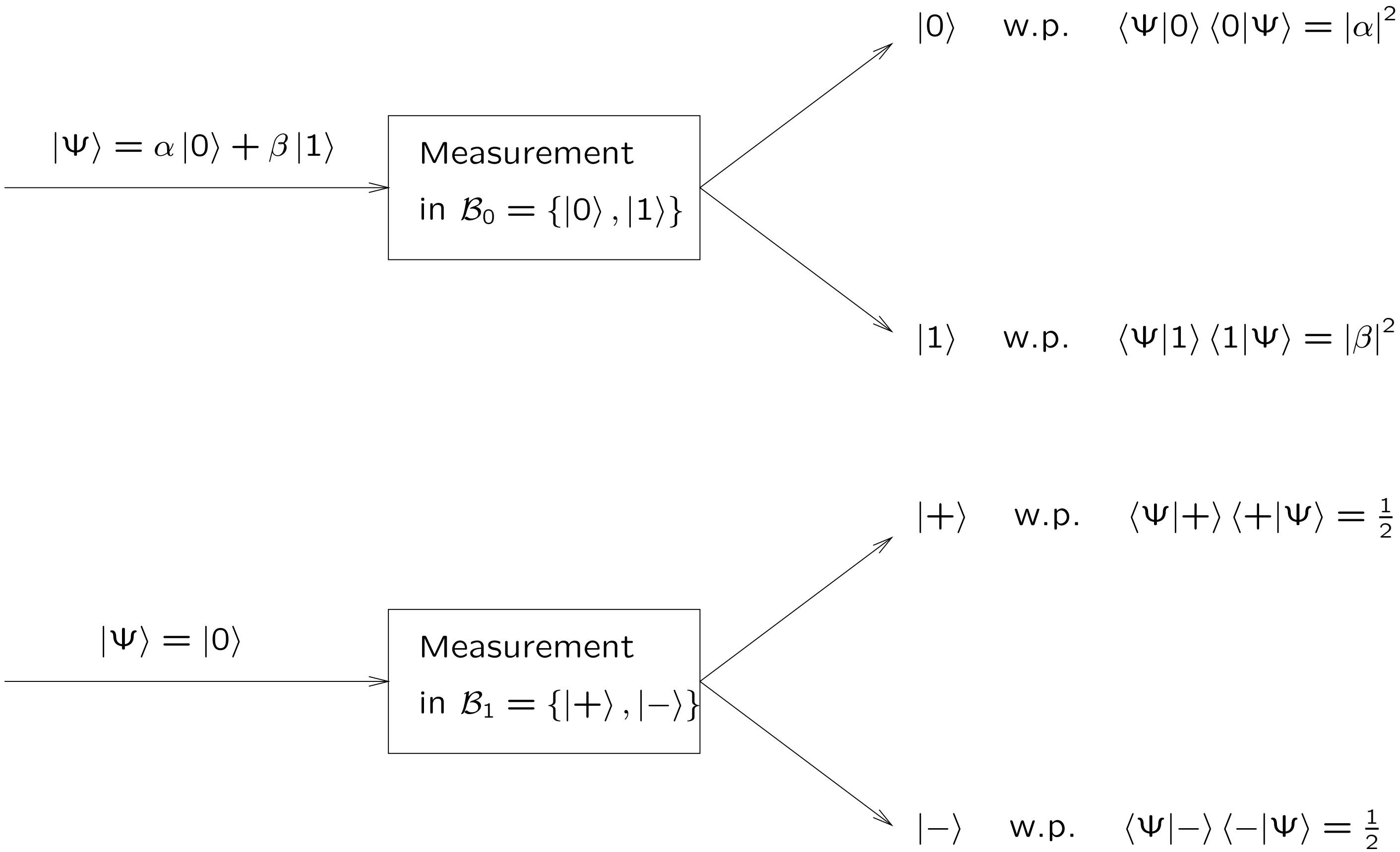
A basis for a qubit is a set of two orthonormal states. Examples:

- $\mathcal{B}_0 = \{|0\rangle\,, |1\rangle\}$ is a basis ($\langle 0|1\rangle = 0$)
- $\mathcal{B}_1 = \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\} = \{|+\rangle\,, |-\rangle\}$ is a basis as

$$\langle +|-\rangle = \frac{1}{2}(\langle 0|0\rangle + \langle 1|0\rangle - \langle 0|1\rangle - \langle 1|1\rangle) = 0$$

Basics of quantum mechanics - Measurement

A measurement of the system in the $\mathcal{B}_0$ basis projects the state of the qubit onto one of the two basis elements $\{|0\rangle, |1\rangle\}$.



Basics of quantum mechanics - Large systems

The joint state of two qubits is the tensor product of the two spaces of each individual qubit. $\mathcal{B}_0$ is an orthonormal basis for one qubit, a basis for a two qubit system is

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

This includes states such as the Bell state or EPR (Einstein,Podolsky,Rosen) pair, which are entangled states:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Neither qubit is in a defined state.

If you have n qubits, their joint state is described by a 2^n dimensional vector. The basis states of the vector are

$$\{|000\ldots00\rangle, |000\ldots01\rangle \cdots |111\ldots11\rangle\}$$

Basics of quantum mechanics - Density Operator (1)

How can we describe a qubit whose state is not completely known? Using the density operator.

If a quantum system is in state $|\Psi_i\rangle$ with probability p_i, the density operator is

$$\rho = \sum_i p_i \, |\Psi_i\rangle \, \langle\Psi_i|$$

When we can write

$$\rho = |\Psi\rangle \, \langle\Psi|$$

we say that the state in a pure state. Otherwise it is in a mixed state.

Two systems with identical density operator are indistinguishable.

Basics of quantum mechanics - Density Operator (2)

Example: Consider a qubit which is in state $|0\rangle$ or $|1\rangle$ with equal probability.

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

Consider a qubit which is in state $|+\rangle$ or $|-\rangle$ with equal probability.

$$\rho = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{1}{4}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1 & 1\end{bmatrix} + \frac{1}{4}\begin{bmatrix}1\\-1\end{bmatrix}\begin{bmatrix}1 & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

Both states are undistinguishable.

Basics of quantum mechanics - Fundamental results

No-Cloning Theorem

You cannot duplicate an unknown quantum state.

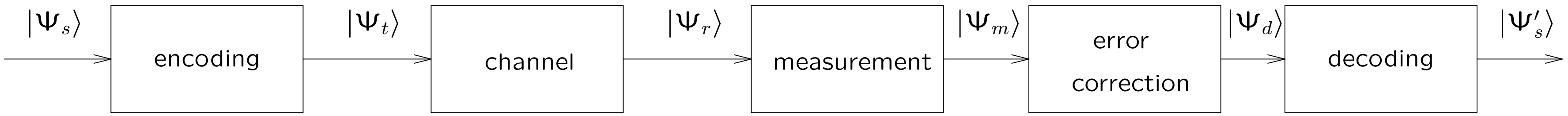
Heisenberg uncertainty principle

You cannot completely measure a quantum state.

QEC: CSS codes - Introduction

Quantum error correcting codes protect quantum information against noise.

The codes work by encoding quantum states in a special way that makes them resilient against the effects of noise, and then decoding when it is wished to recover the original state.



Objective: $|\Psi_s\rangle = |\Psi'_s\rangle$.

QEC: CSS codes - Definition (1)

CSS (Calderbank-Shor-Stean) codes use linear codes:

- $\mathcal{C}_1$ is a $[n, k_1]$ linear code, with generator matrix G_1 and parity check matrix H_1
- $\mathcal{C}_2$ is a $[n, k_2]$ linear code, with generator matrix G_2 and parity check matrix H_2

such that $\mathcal{C}_2 \subset \mathcal{C}_1$. $\mathcal{C}_1$ and $\mathcal{C}_2^{\perp}$ correct up to t errors.

Equivalence relation: $x, y \in \mathcal{C}_1$ are equivalent $\Leftrightarrow \exists w \in \mathcal{C}_2$ s.t. $x = y \oplus w$.

Set of equivalence classes is $\mathcal{C}_1/\mathcal{C}_2$, of cardinality $2^{k_1 - k_2}$.

QEC: CSS codes - Definition (2)

The CSS codeword encoding the state $|x\rangle$, where $x \in \mathcal{C}_1/\mathcal{C}_2$, is:

$$|x\rangle \rightarrow \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{w \in \mathcal{C}_2} |x \oplus w\rangle$$

If $x, y \in \mathcal{C}_1/\mathcal{C}_2$ are equivalent, they are encoded by the same codeword.

We have defined a $[n, k_1 - k_2]$ quantum correcting code.

It can correct up to t bit-flip and t phase-flip simultaneously.

QEC: CSS codes - Introducing errors

e_1 is an n-bit vector with 1s where bit-flip errors occurred and 0s elsewhere.

e_2 is an n-bit vector with 1s where phase-flip errors occurred and 0s elsewhere.

Corrupted state:

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{w \in \mathcal{C}_2} (-1)^{(x \oplus w) \cdot e_2} |x \oplus w \oplus e_1\rangle$$

QEC: CSS codes - Correcting bit-flip errors

We add enough ancillary qubits to our system and compute

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{w \in \mathcal{C}_2} (-1)^{(x \oplus w) \cdot e_2} |x \oplus w \oplus e_1\rangle |\mathsf{H}_1(x \oplus w \oplus e_1)\rangle \ .$$

As $x, w \in \mathcal{C}_1$

$$|\mathsf{H}_1(x \oplus w \oplus e_1)\rangle = |\mathsf{H}_1 e_1\rangle$$

which can be measured without perturbing the original state.

Since $\mathcal{C}_1$ can correct up to t errors, we can deduce from $\mathsf{H}_1 e_1$ where bit-flip error occurs and correct them.

QEC: CSS codes - Correcting phase-flip errors

We have recovered

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{w \in \mathcal{C}_2} (-1)^{(x \oplus w) \cdot e_2} |x \oplus w\rangle$$

Applying Hadamard transform to each qubit, we obtain (after some calculation...)

$$\frac{1}{\sqrt{2^n / |\mathcal{C}_2|}} \sum_{z' \in \mathcal{C}_2^{\perp}} (-1)^{x \cdot z'} \left| z' \oplus e_2 \right\rangle$$

From phase-flips we obtain bit-flips! We know how they can be corrected (using properties of $\mathcal{C}_2^{\perp}$). After correction, applying Hadamard transform again gives back the original state.

$$|x\rangle \rightarrow \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{w \in \mathcal{C}_2} |x \oplus w\rangle$$

QKE overview

Alice and Bob want to share a secret key, Eve wants to obtain some information about it. Alice and Bob have access to an authenticated classic channel and to a quantum channel.

- In 1984, C.H. Bennett and G. Brassard propose the first QKE protocol, but limited their security proofs to classical attacks.
- Since then, several proofs were proposed, none was easy to understand!
- In '99, H. Lo and H.F. Chau came up with a provably secure QKE protocol . . . but impossible to implement.
- In '00, P.W. Shor and J. Preskill find the first simple proof of the security of the BB84 protocol over noisy channels.

Contents

BB84 protocol over noiseless channels (1)

Alice chooses at a basis at random among

$$\mathcal{B}_0 = \{|0\rangle, |1\rangle\} \quad \text{and} \quad \mathcal{B}_1 = \left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}.$$

She chooses a bit at random. If it is 0, she sends the first state of her basis, otherwise she sends the second state of her Basis. She iterates N times.

Bob chooses a basis at random to make the measurements. At the end Alice and Bob announce their basis. When they coincide, Alice and Bob keep the corresponding bit. When they differ the bit is discarded. The both obtain an n-bit string ($n \leq N$).

BB84 protocol over noiseless channels (2)

Alice chooses some random positions for check bits that Bob will use to compute the error rate (errors are introduced by Eve). If it is too high, they abort the protocol. Otherwise, the remaining bits can be used.

Formal reason why Eve inevitably introduces errors: As Alice chooses a basis and a bit at random, the density operator of the system accessible to Eve is

$$\rho^{\mathcal{B}_0} = \rho^{\mathcal{B}_1} = \frac{1}{2^N} I^{\otimes N}.$$

Eve cannot distinguish it from the maximally random density matrix. If she learns something about the system, she will perturb it.

QKE with CSS codes - Main idea

The security of BB84 over noiseless channels can be achieved because any error in the state received by Bob must have been introduced by Eve. But what happens on a realistic channel where noise can also be the source of errors?

Idea: Make use of Quantum Error Correcting codes in order to recover on Bob side the original state sent by Alice. This state is therefore disentangled from any state from the outside world (including any state controlled by Eve).

Alice encodes the key using a CSS codeword, interspersing it with check bits. Bob will use them to find the error rate. As CSS codes correct a limited number of errors, if the rate is to high, Alice and Bob abort the protocol.

QKE with CSS codes - Shifted CSS codes

Problem: the density matrix accessible to Eve must be indistinguishable from the maximally random density matrix.

Solution: Use a set of shifted CSS codes, where

$$|k\rangle \rightarrow \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{w \in \mathcal{C}_2} (-1)^{\alpha \cdot w} |k \oplus w \oplus \beta\rangle$$

where $\alpha \in F_2^n/\mathcal{C}_2^{\perp}$ and $\beta \in F_2^n/\mathcal{C}_1$ (randomly chosen by Alice) and where $k \in \mathcal{C}_1/\mathcal{C}_2$.

This is the state she sends to Bob. It can be shown that for Eve, the state in now indistinguishable from the maximally random density matrix.

QKE with CSS codes - Recovering the key

The qubits of the code are interspersed with check qubits that will allow Bob to check the error rate. If it is too high, the CSS codes won't be able to correct errors (and therefore to disentangle the state from the outside world). In that case the protocol aborts.

Otherwise, Alice sends α and β to Bob who recovers the original codeword, corrects errors and recovers $|k\rangle$.

According to the No-cloning theorem, this protocol is secure.

To implement this protocol, Bob must have access to a quantum memory. . .

Equivalence to the BB84 protocol

We are going to see why the security of the QKE protocol with CSS codes implies the security of the BB84 protocol over noisy channels.

The latest differs slightly from the noiseless version we have studied.

In order to see the link between both protocols we can either study the BB84 protocol in details . . .

Equivalence to the BB84 protocol - Going into details...

1. Alice creates $(4+\delta)n$ random bits.
2. Alice chooses a random $(4+\delta)n$-bit string b. For each bit, she creates a state in the $\mathcal{B}_0$ basis (when the corresponding bit of b is 0) or in the $\mathcal{B}_1$ basis (when the corresponding bit of b is 1).
3. Alice sends the resulting qubits to Bob.
4. Bob receives the $(4+\delta)n$ qubits, measuring each in $\mathcal{B}_0$ or $\mathcal{B}_1$ at random.
5. Alice announces b.
6. Bob discard any result where his basis doesn't coincide with Alice's one. With high probability, there are at least $2n$ bits left (if not, abort the protocol). Alice decides randomly on a set of $2n$ bits to use for the protocol, and chooses at random n of these to be check bits.
7. Alice and Bob announce the values of their check bits. If too few of these value agree (high error rate), they abort the protocol.
8. Alice announces $u \oplus v$, where v is the string consisting of the remaining non-check bits, and u is a random codeword in $\mathcal{C}_1$.
9. Bob substract $u \oplus v$ from his own remaining non-check bits $v \oplus \epsilon$ (where ϵ represents errors), and corrects the result $u \oplus \epsilon$ in order to obtain u, a codeword in $\mathcal{C}_1$.
10. Alice and Bob use the coset of u in $\mathcal{C}_1/\mathcal{C}_2$ as the secret key.

Equivalence to the BB84 protocol - ...or not

...or try to underline the main ideas.

Bob is only interested in the bit values of the encoded key $\rightarrow$ he doesn't have to correct the phase $\rightarrow$ he doesn't need α.

We could show that when Alice announces β, Bob can recover $k \oplus w \oplus \epsilon$ where $k \oplus w \in \mathcal{C}_1$, so that Bob can correct ϵ. Alice and Bob use the equivalence class of $k \oplus w$ as a secret key.

In the BB84 protocol, Alice announces some value $u \oplus v$ where $u \in \mathcal{C}_1$. Bob knows $v \oplus \epsilon$. They will equivalently use the equivalence class of u as a key.

Both protocols are equivalent $\Rightarrow$ If one is secure, the other is as well.

Conclusion

P.W. Shor and J. Preskill presented the first simple proof of BB84 over noisy channels.

Some weaknesses. . .

This proof doesn't take into account imperfect sources, only perfect single-photon sources.

Thank You for Your Attention!