Quantum cryptography

March 11

Plan

1. Introduction

- Quantum key distribution with a security-proof only relying on
  - authenticated channel between Alice and Bob
  - laws of quantum physics
- Information theoretically secure : no computational assumptions
- Implemented in practice
  - 2004 first bank transfer in Swiss
  - 2007 ballot results of the Swiss canton of Geneva transmitted to the capital
  - Chinese network
    - 2016: space mission $\to$ QKD channel between China and Austria (7500 km)
    - 2017: 2000-km fiber line between Beijing, Jinan, Hefei and Shanghai
  - current optic fibre networks : infrastructure is in place for a more widespread use

KQD basic principles

- private key bits created by communicating qubits over a public channel
- Eve can not gain information from the qubits without disturbing the states
- Eve can not clone the qubits
- Non-orthogonal states are sent through the channel

Exercise : distinguishing two non orthogonal quantum states

1. Show how to distinguish perfectly two orthogonal states with just one measurement
2. Show that there is no (general) measurement that distinguishes perfectly two non orthogonal states

Recall: Measurement

A (general) measurement is given by a collection of $\mathbf{M}_1, \ldots, \mathbf{M}_k$ such that

$$\sum_{m=1}^{k} \mathbf{M}_m^* \mathbf{M}_m = \mathbf{I}$$

$$\text{Measuring } |\psi\rangle \quad \to \quad \frac{\mathbf{M}_m |\psi\rangle}{\|\mathbf{M}_m |\psi\rangle\|} \text{ with prob. } \|\mathbf{M}_m |\psi\rangle\|^2$$

Solution

1. projective measurement along $V \oplus V^{\perp}$ where V contains the first state and $V^{\perp}$ the second one

2. Let the two states be $|\psi_1\rangle$ and $|\psi_2\rangle$ and the measurement be given by a collection $\mathbf{M}_1, \dots, \mathbf{M}_k$ which are such that $\sum_{m=1}^{k} \mathbf{M}_m^* \mathbf{M}_m = \mathbf{I}.s$ If it is possible to distinguish perfectly between $|\psi_1\rangle$ and $|\psi_2\rangle$ with these measurements, then if we let $f : \{1, \cdots, k\} \to \{1, 2\}$ be the decision made on $|\psi_1\rangle$ and $|\psi_2\rangle$ based on the measurement we should have

   (i) $\mathbf{I} = \mathbf{E}_1 + \mathbf{E}_2$
   (ii) $\langle\psi_i| E_i |\psi_i\rangle = 1$

   where

$$\mathbf{E}_i \stackrel{\text{def}}{=} \sum_{j:f(j)=i} \mathbf{M}_i^* \mathbf{M}_i$$

Since $\langle\psi_1|\psi_1\rangle = 1$ and $\mathbf{I} = \mathbf{E}_1 + \mathbf{E}_2$ we have

$$1 = \langle\psi_1| E_1 |\psi_1\rangle + \langle\psi_1| E_2 |\psi_1\rangle$$

Since $\langle\psi_1| E_1 |\psi_1\rangle = 1$ we deduce

$$0 = \langle\psi_1| E_2 |\psi_1\rangle = \left\| \sqrt{E_2}\, |\psi_1\rangle \right\|^2$$

Decompose $|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\psi_3\rangle$ with $|\psi_3\rangle$ orthogonal to $|\psi_1\rangle$. We have $|\beta| < 1$ since $|\alpha|^2 + |\beta|^2 = 1$ and $|\psi_1\rangle$ and $|\psi_2\rangle$ are non-orthogonal. Since $\sqrt{\mathbf{E}_2}\,|\psi_2\rangle = \beta\sqrt{\mathbf{E}_2}\,|\psi_3\rangle$ we have

$$\langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \left\| \sqrt{\mathbf{E}_2}\, |\psi_3\rangle \right\| = |\beta|^2 \langle\psi_3| E_2 |\psi_3\rangle \leq |\beta|^2 < 1$$

Exercise : information gain on non orthogonal states implies disturbance

- $|\psi\rangle$ and $|\phi\rangle$ two non-orthogonal states.
- Process of Eve : unitarily interact $|\psi\rangle$ and $|\phi\rangle$ with an ancilla $|u\rangle$ without disturbance:

$$
\begin{aligned}
|\psi\rangle\,|u\rangle &\mapsto |\psi\rangle\,|v\rangle \\
|\phi\rangle\,|u\rangle &\mapsto |\phi\rangle\,|v'\rangle
\end{aligned}
$$

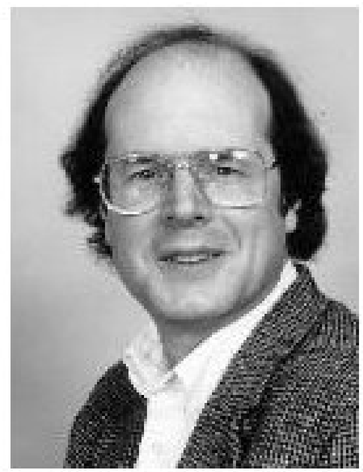
Prove that $|v\rangle = |v'\rangle$ meaning that Eve can not gain information on $|\psi\rangle$ and $|\phi\rangle$

Solution

$$
\begin{aligned}
\langle v|v'\rangle \langle \psi|\phi\rangle &= \langle u|u\rangle \langle \psi|\phi\rangle \\
&\Downarrow \\
\langle v|v'\rangle &= \langle u|u\rangle = 1 \\
&\Downarrow \\
|v\rangle &= |v'\rangle
\end{aligned}
$$

2. The BB84 protocol

- Proposed by Charles Bennett and Gilles Brassard in 1984



- Originally proposed/based on photon polarization

Phase 1: Alice side

- Binary strings of length $(4+\delta)n$ encoded with as a block of $(4+\delta)n$ qubits

$$
\begin{aligned}
\mathbf{a} &= a_1 \cdots a_{(4+\delta)n} && \text{keybit string} \\
\mathbf{b} &= b_1 \cdots b_{(4+\delta)n} && \text{basis string} \\
0 \text{ basis} &= \{|0\rangle, |1\rangle\} && 1 \text{ basis} = \{|+\rangle, |-\rangle\} \\
|+\rangle &\stackrel{\text{def}}{=} \frac{|0\rangle + |1\rangle}{\sqrt{2}} && |-\rangle \stackrel{\text{def}}{=} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
|\psi_{00}\rangle &\stackrel{\text{def}}{=} |0\rangle && |\psi_{10}\rangle \stackrel{\text{def}}{=} |1\rangle \\
|\psi_{01}\rangle &\stackrel{\text{def}}{=} |+\rangle && |\psi_{11}\rangle \stackrel{\text{def}}{=} |-\rangle
\end{aligned}
$$

- Alice sends to Bob

$$
|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} \left|\psi_{a_k b_k}\right\rangle
$$

Phase 2 : Bob's side

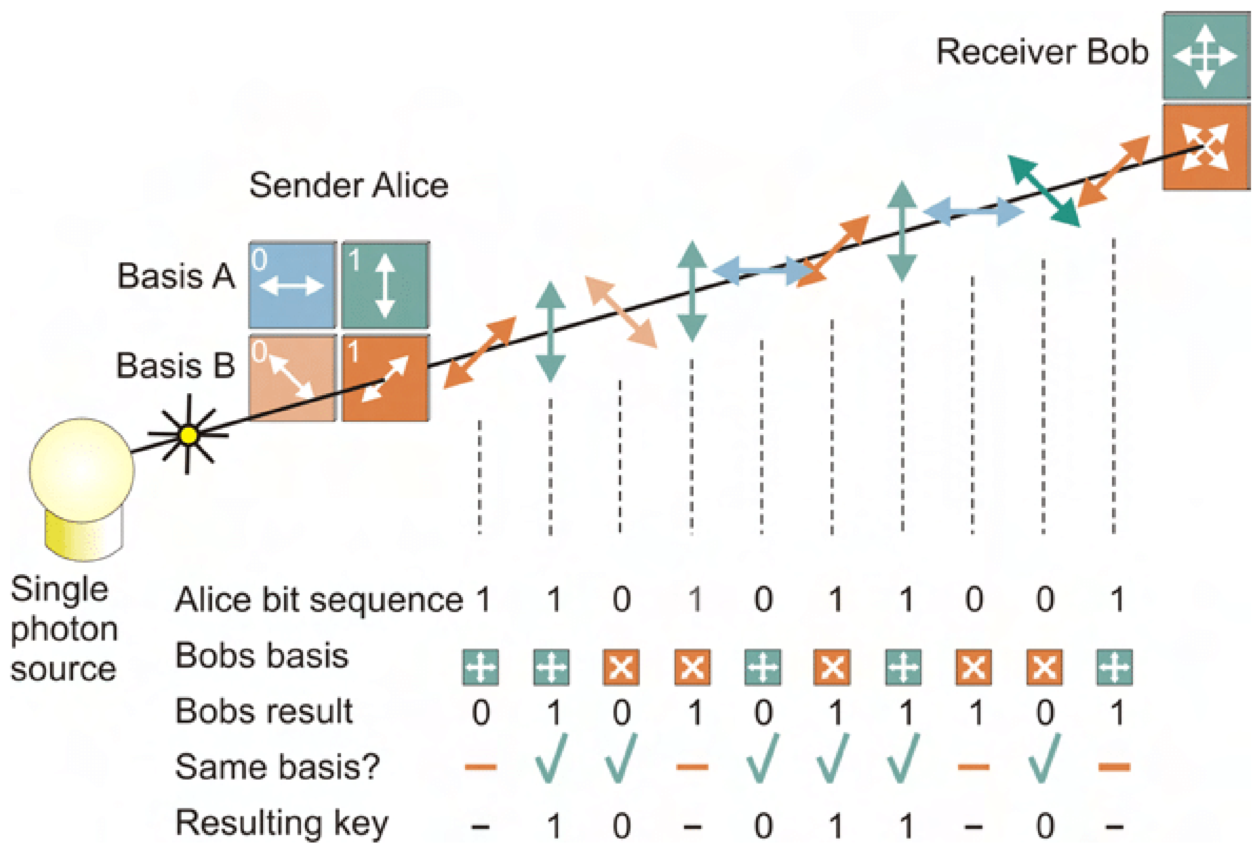
- When Bob has received the $(4+\delta)n$ qubits he announces that to Alice
- He measures each of these qubits in either the $\{|0\rangle, |1\rangle\}$ or the $\{|+\rangle, |-\rangle\}$ basis. Each basis is chosen uniformly at random

Phase 3: Verification

1. Alice announces $\mathbf{b}$, Bob announces his own choice $\mathbf{b}'$ of bases
2. They keep $2n$ bits corresponding to $b_i = b_i'$
3. Alice selects n positions among them to serve as check on Eve's interference and tells Bob which bits she selected
4. Alice and Bob compare $\mathbf{a}$ and $\mathbf{a}'$ on these n positions. Abort if too many bits disagree

Information reconciliation/privacy amplification

- Reconciliation: ending with a common string from $\mathbf{a}$ and $\mathbf{a}'$ by public communication
- Privacy amplification: ending with a common and private string by public communication


Receiver Bob
Sender Alice
Basis A
0
1
Basis B
0
1
Single photon source
Alice bit sequence 1 1 0 1 0 1 1 0 0 1
Bobs basis
Bobs result 0 1 0 1 0 1 1 1 0 1
Same basis?
Resulting key – 1 0 – 0 1 1 – 0 –

Exercise: Eve's attack

1. Find a basis choice which gives Eve the same information on a_i irrespective of the basis choice b_i

2. Let $\hat{a}_i$ be Eve's choice for a_i that maximizes $\mathbf{Prob}(\hat{a}_i = a_i)$. Give a formula for $\mathbf{Prob}(\hat{a}_i = a_i)$

3. What is in this case $\mathbf{Prob}(a'_i \neq a_i)$?

Solution

1. basis $\{\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\}$
2. $\mathbf{Prob}(\hat{a}_i = a_i) = \cos^2(\pi/8) \approx 0.85$
3. $\mathbf{Prob}(a_i' \neq a_i) = \sin^2(\pi/8) \approx 0.15$

3. The Bennett protocol

- Highlights that the impossibility of perfect distinction between non-orthogonal states lies at the heart of quantum cryptography
- Alice prepares one classical bit a and sends to Bob

$$|\psi\rangle = \begin{cases} |0\rangle & \text{if } a = 0 \\ \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{if } a = 1 \end{cases}$$

- Bob generates a random classical bit a'.
  - he measures $|\psi\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis if $a' = 0$
  - he measures $|\psi\rangle$ in the $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ basis if $a' = 1$

  $\rightarrow b \in \{0, 1\}$
- He publicly announces b
- keep only pairs for which $b = 1$. Final key $= a$ for Alice $= 1 - a'$ for Bob

4. The EPR protocol

- Based on EPR pairs
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
- Symmetric protocol
- Alice and Bob share n EPR pairs, Alice has the first qubit of the pairs, Bob the second one

1. Alice choose randomly $\mathbf{b} \in \{0,1\}^n$ and Bob $\mathbf{b}' \in \{0,1\}^n$
2. According to b_i (resp. b'_i) Alice (resp. Bob) measures her/his qubit of the i-th pair in the $\{|0\rangle, |1\rangle\}$ basis for a 0 bit and in $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$ for a 1 bit and obtain a_i and a'_i respectively
3. Communicate $\mathbf{b}$ and $\mathbf{b}'$ publicly and keep only the a_i's for which $b_i = b'_i$

Fidelity $\Rightarrow$ security

- Quantum information theory: if Alice and Bob share an entangled state $|\beta_{00}\rangle^{\otimes k}$ Eve has no information on a k-bit string they may have in common
- Random sampling can upper-bound eavesdropping

$$
\begin{aligned}
|\beta_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
|\beta_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
|\beta_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\
|\beta_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}
\end{aligned}
$$

  - bit flips detected by the projectors $|\beta_{01}\rangle\langle\beta_{01}| + |\beta_{11}\rangle\langle\beta_{11}|$ and $|\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|$
  - phase flips detected by the projectors $|\beta_{10}\rangle\langle\beta_{10}| + |\beta_{11}\rangle\langle\beta_{11}|$ and $|\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}|$

5. The Lo-Chau protocol

$$|\beta_{00}\rangle^{\otimes n} \xrightarrow{\text{noise/Eve}} \rho \xrightarrow{\text{entanglement distillation}} \rho' \approx |\beta_{00}\rangle^{\otimes k}$$

- Sacrificing half of the EPR pairs for measuring the noise
- Based on a random CSS code to correct a fraction δ of X, Y and Z errors in ρ

The Lo-Chau protocol

1. Alice creates $2n$ EPR pairs
2. Alice chooses randomly $\mathbf{b} \in \{0,1\}^{2n}$, performs Hadamard $\mathbf{H}$ on the 2nd qubit for which $\mathbf{b}$ is 1, sends these qubits to Bob
3. After receiving the announcement that Bob received its qubits, Alice announces $\mathbf{b}$ and the n pairs that serve as check qubits, Bob performs $\mathbf{H}$ when $b = 1$
4. Alice and Bob measure their n check qubits in the $\{|0\rangle, |1\rangle\}$ basis and publicly share their results, abort if $\#$ disagreements $> t$
5. Alice and Bob measure their remaining qubits according to the check matrix of an $[[n,k,t]]$-CSS code, share the results and correct the quantum state $\to |\beta_{00}\rangle^{\otimes k}$: entanglement distillation
6. Alice and Bob measure the k EPR pairs in the $\{|0\rangle, |1\rangle\}$ basis to obtain a shared secret key

Entanglement distillation

1. Alices prepares $|\beta_{00}\rangle^{\otimes n}$ and sends the second qubit of each EPR pair to Bob
2. There is channel noise which results in $(\mathbf{I} \otimes \mathbf{E}) |\beta_{00}\rangle^{\otimes n}$ where $\mathbf{I}$ is the identity acting on Alice's side and $\mathbf{E}$ is a Pauli error of weight t acting on Bob's side

Goal: generate $|\beta_{00}\rangle^{\otimes k}$
Means: $[[n, k, t]]$ stabilizer code $\mathcal{C}$

Exercise : stabilizer code

Consider an $[[n, k]]$ stabilizer code with generators $g_1, \cdots, g_{n-k}$. What happens if

(i) we start from an arbitrary n-qubit quantum state $|\psi\rangle$

(ii) perform the measurement according to $g_1, \cdots, g_{n-k}$

(iii) find a Pauli error $\mathbf{E}$ whose syndrome corresponds to the measurement

(iv) and finally apply $\mathbf{E}^*$ to the measured state ?

Exercise : properties of Bell states

1. For any matrix $\mathbf{M} \in \mathbb{C}^{2^n \times 2^n}$, show that there exists $\mathbf{M}'$ such that

$$(\mathbf{M} \otimes \mathbf{I}) |\beta_{00}\rangle^{\otimes n} = (\mathbf{I} \otimes \mathbf{M}') |\beta_{00}\rangle^{\otimes n}$$

   where $\mathbf{M}$ acts on Alice's side whereas $\mathbf{M}'$ acts on Bob's side

2. Let $\mathbf{P}_1, \cdots, \mathbf{P}_{2^{n-k}}$ be the projectors corresponding to ± 1 eigenspaces of the generators $g_1, \cdots, g_{n-k}$. Show that for all i

$$(\mathbf{P}_i \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{E}) |\beta_{00}\rangle^{\otimes n} = (\mathbf{I} \otimes \mathbf{E})(\mathbf{P}_i \otimes \mathbf{P}_i^{\intercal}) |\beta_{00}\rangle^{\otimes n}$$

Solution

1. First we notice that

$$|\beta_{00}\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,|x\rangle$$

From this we deduce

$$\begin{aligned}
(\mathbf{M} \otimes \mathbf{I})\,|\beta_{00}\rangle^{\otimes n} &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} M_{yx}\,|y\rangle\,|x\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle \sum_{x \in \{0,1\}^n} M_{yx}\,|x\rangle \\
&= (\mathbf{I} \otimes \mathbf{M}^{\mathsf{T}})\,|\beta_{00}\rangle^{\otimes n}
\end{aligned}$$

2.

$$
\begin{aligned}
(\mathbf{P}_i \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{E}) \left|\beta_{00}\right\rangle^{\otimes n} &= (\mathbf{I} \otimes \mathbf{E})(\mathbf{P}_i \otimes \mathbf{I}) \left|\beta_{00}\right\rangle^{\otimes n} \\
&= (\mathbf{I} \otimes \mathbf{E})(\mathbf{P}_i \otimes \mathbf{I})(\mathbf{P}_i \otimes \mathbf{I}) \left|\beta_{00}\right\rangle^{\otimes n} \\
&= (\mathbf{I} \otimes \mathbf{E})(\mathbf{P}_i \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{P}_i^{\intercal}) \left|\beta_{00}\right\rangle^{\otimes n} \\
&= (\mathbf{I} \otimes \mathbf{E})(\mathbf{P}_i \otimes \mathbf{P}_i^{\intercal}) \left|\beta_{00}\right\rangle^{\otimes n}
\end{aligned}
$$

Exercise : entanglement distillation protocol

The entanglement distillation protocol consists in

1. Alices measures the $n-k$ generators of $\mathcal{C}$ on her side
2. she performs the inverse of a unitary Pauli error that has the measured syndrome σ_A
3. she tells Bob her syndrome
4. Bob computes his syndrome and performs the unitary transform of weight $\leq t$ that would give him the same syndrome as Alice
5. they both perform the decoding unitary corresponding to $\mathcal{C}$

6. Another modification of the Lo-Chau protocol : the CSS protocol

- Problem of the Lo-Chau protocol : needs full power of quantum computing to perform entanglement distillation + entanglement
- This protocol can be simplified without compromising security
- We begin to simplify it by removing the need to distribute EPR pairs
- Idea: Alice's measurements collapse the pairs into n single qubits

Modified Lo-Chau protocol (II)

1. Alice creates random bits $a_1, \dots, a_n$, qubits $|a_1\rangle, \cdots, |a_n\rangle$ and $|\beta_{00}\rangle^{\otimes n}$
2. Alice chooses randomly n positions (out of $2n$) puts the $|a_i\rangle$'s in them and half of each EPR pair in the remaining positions
3. Alice chooses randomly $\mathbf{b} \in \{0,1\}^{2n}$ and performs Hadamard $\mathbf{H}$ on the qubit for which $\mathbf{b}$ is 1 then sends each of those qubits to Bob
4. Bob ack. the rec. of the qubits, Alice announces $\mathbf{b}$ and the n check qubits, Bob performs $\mathbf{H}$ when $b = 1$
5. Bob measures check qubits in $|0\rangle, |1\rangle$, shares results, aborts if $\#$ disagree. $> t$
6. Alice and Bob measure their remaining qubits accord. to the check matrix of an $[[n,k,t]]$-CSS code, share results and correct the quantum state $\rightarrow |\beta_{00}\rangle^{\otimes k}$
7. Alice and Bob measure the k EPR pairs in the $\{|0\rangle, |1\rangle\}$ basis to obtain a shared secret key

CSS Codes

- Based on two binary linear codes $\mathcal{C}_X$ and $\mathcal{C}_Z$ such that

$$\boxed{\mathcal{C}_Z^\perp \subset \mathcal{C}_X}$$

- Quantum code $\mathcal{Q}$ defined by

$$\begin{aligned}
\mathcal{Q} &\stackrel{\text{def}}{=} \mathbf{Vect}\left\{|\xi_{\mathbf{u}}\rangle : \mathbf{u} \in \mathcal{C}_X/\mathcal{C}_Z^\perp\right\} \\
|\xi_{\mathbf{u}}\rangle &= \frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v}\in\mathcal{C}_Z^\perp} |\mathbf{u}+\mathbf{v}\rangle \\
k_Z^\perp &= \dim \mathcal{C}_Z^\perp
\end{aligned}$$

- Encodes k qubits where

$$\begin{aligned}
k_X &= \dim \mathcal{C}_X \\
k &= k_X - k_Z^\perp
\end{aligned}$$

- Corrects t errors if $\mathcal{C}_X$ and $\mathcal{C}_Z$ correct t errors

Quantum measurement

- Error $\mathbf{e} \in \{\mathbf{I}, X, Y, Z\}^n$ decomposes as

$$\mathbf{e} = e_X X + e_Z Z$$

- Syndrome measurement yields

$$\begin{aligned} \sigma_X &= \mathbf{H}_X \mathbf{e}_X^\intercal \\ \sigma_Z &= \mathbf{H}_Z \mathbf{e}_Z^\intercal \end{aligned}$$

- After error + measurement, the code state $|\xi_U\rangle$ becomes

$$\left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v}\in\mathcal{C}_Z^\perp} (-1)^{\mathbf{e}_Z\cdot\mathbf{v}} \left|\mathbf{u}+\mathbf{v}+\mathbf{e}_X\right\rangle$$

- The code state gets projected to one of the (orthogonal) spaces

$$\mathsf{CSS}_{\mathbf{z},\mathbf{x}}(\mathcal{C}_X, \mathcal{C}_Z) \stackrel{\text{def}}{=} \mathbf{Vect}\left\{\left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle, \mathbf{u} \in \mathcal{C}_X/\mathcal{C}_Z^\perp\right\}$$

Exercise : $\left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle$

1. Prove that all the states $\left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle$ are orthogonal when $\mathbf{u}$ ranges over $\mathcal{C}_X/\mathcal{C}_Z^{\perp}$, $\mathbf{e}_X$ and $\mathbf{e}_Z$ are vectors that are a particular solution of $\mathbf{H}_X\mathbf{e}_X^{\mathsf{T}} = \sigma_X$, $\mathbf{H}_Z\mathbf{e}_Z^{\mathsf{T}} = \sigma_Z$ and σ_X, σ_Z range respectively over $\mathbb{F}_2^{n-k_X}$ and $\mathbb{F}_2^{k_Z^{\perp}}$

2. Prove that

$$\left|\beta_{00}\right\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} |j\rangle\,|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z} \left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle \left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle$$

3. Give an interpretation of Steps 6 and 7 in terms of $\left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle$

Solution

- When Alice measures the stabilizer generators corresponding to $\mathbf{H}_X$ and $\mathbf{H}_Z$ she obtains random values $\mathbf{x}$ and $\mathbf{z}$
- her final measurement yields $\mathbf{u}$
- the remaining qubits are thus left in $\left|\xi_{\mathbf{u},\mathbf{e}_X,\mathbf{e}_Z}\right\rangle$ which is the codeword for $\mathbf{u}$ in $\mathsf{CSS}_{\mathbf{z},\mathbf{x}}(\mathcal{C}_X,\mathcal{C}_Z)$
- Alice measurements yield random qubits encoded in a random code

Modification III

1. Alice creates random bits $a_1, \ldots, a_n$, qubits $|a_1\rangle, \cdots, |a_n\rangle$ and $|\beta_{00}\rangle^{\otimes n}$

2. Alice chooses randomly n positions (out of $2n$) puts the $|a_i\rangle$'s in them and half of each EPR pair in the remaining positions

$\Rightarrow 1'$. Alice creates random bits $a_1, \ldots, a_n$, qubits $|a_1\rangle, \cdots, |a_n\rangle$, random $\mathbf{x}$, $\mathbf{z}$, random k bits $\tilde{\mathbf{u}}$ and encodes $\tilde{\mathbf{u}}$ in $\mathrm{CSS}_{\mathbf{z},\mathbf{x}}(\mathcal{C}_X, \mathcal{C}_Z)$

$\Rightarrow 2'$. Alice chooses randomly n positions (out of $2n$) puts the $|a_i\rangle$'s in them and encoded qubits in the remaining positions

4. Bob ack. the rec. of the qubits, Alice announces $\mathbf{b}$ and the n check qubits, Bob performs $\mathbf{H}$ when $b = 1$

$\Rightarrow 4$. Bob ack. the rec. of the qubits, Alice announces $\mathbf{b}$, $\mathbf{x}$, $\mathbf{z}$ and the n check qubits, Bob performs $\mathbf{H}$ when $b = 1$

The CSS protocol

1. Alice creates random check bits $\mathbf{a} \in \mathbb{F}_2^n$, key bits $\tilde{\mathbf{u}} \in \mathbb{F}_2^k \sim \mathbf{u} \in \mathcal{C}_X/\mathcal{C}_Z^\perp$, random $\mathbf{z}, \mathbf{x} \in \mathbb{F}_2^n$ and encodes $|\mathbf{u}\rangle$ in $\text{CSS}_{\mathbf{z},\mathbf{x}}(\mathcal{C}_X, \mathcal{C}_Z)$
2. Alice chooses randomly n positions (out of $2n$) puts the check qubits $|a_i\rangle$ in them and the encoded qubits in the remaining positions.
3. Alice chooses randomly $\mathbf{b} \in \{0,1\}^{2n}$ and performs a Hadamard transform on the qubit for which $\mathbf{b}$ is 1 then sends all the qubits to Bob
4. Bob ack. the rec. of the qubits, Alice announces $\mathbf{b}$, $\mathbf{x}$, $\mathbf{z}$ and the positions of the check qubits, Bob performs $\mathbf{H}$ when $b = 1$
5. Bob performs Hadamards on the qubits where $\mathbf{b}$ is 1, measures the check qubits in $|0\rangle, |1\rangle$, shares results, aborts if $\#$ disagree. $> t$
6. Bob decodes the remaining n qubits in $\text{CSS}_{\mathbf{z},\mathbf{x}}(\mathcal{C}_X, \mathcal{C}_Z)$
7. Bob measures his qubits to obtain the shared secret key $\tilde{\mathbf{u}}$

7. Secure BB84 protocol

- The CSS QKD protocol is secure by reduction from the modified Lo-Chau protocol
- Much simpler protocol : does not use EPR pairs
- Drawbacks
  - requires quantum computations
  - Bob needs a quantum memory

Exercise

1. Explain how we can obtain $\mathbf{u}+\mathbf{v}+\mathbf{x}+\mathbf{e}$ for some error $\mathbf{e}$ added by the channel or Eve and some $\mathbf{v} \in \mathcal{C}_X/\mathcal{C}_Z^{\perp}$
2. how can you recover $\mathbf{e}$ and then $\mathbf{u}+\mathbf{v}$?
3. how can you recover $\mathbf{u}$?

Modification I

6. Bob decodes the remaining n qubits in $\mathsf{CSS}_{\mathbf{z},\mathbf{x}}(\mathcal{C}_X, \mathcal{C}_Z)$

$\Rightarrow 6'$. Bob measures the qubits to get $\mathbf{u}+\mathbf{v}+\mathbf{x}+\mathbf{e}$, subtracts $\mathbf{x}$ from the result, correct it with the code $\mathcal{C}_X$ to get $\mathbf{u}+\mathbf{v}$

7. Bob measures his qubits to obtain the shared secret key $\tilde{\mathbf{u}}$

$\Rightarrow 7'$. Bob obtain $\mathbf{u}$ and then $\tilde{\mathbf{u}}$ by determining in which coset of $\mathcal{C}_Z^{\perp}$ in $\mathcal{C}_Z$ $\mathbf{u}+\mathbf{v}$ lies.

Exercise

1. Notice that in the modified protocol Alice does not need to reveal $\mathbf{z}$. Show that she can effectively send a mixed state $\rho_{\mathbf{u},\mathbf{x}}$. Give an expression for this mixed state.

2. Show that

$$\frac{1}{2^n}\sum_{\mathbf{z}} |\xi_{\mathbf{u},\mathbf{z},\mathbf{x}}\rangle \langle\xi_{\mathbf{u},\mathbf{z},\mathbf{x}}| = \frac{1}{2^n}\sum_{\mathbf{v}\in\mathcal{C}_Z^{\perp}} |\mathbf{u}+\mathbf{v}+\mathbf{x}\rangle \langle\mathbf{u}+\mathbf{v}+\mathbf{x}|$$

3. How can you create $\rho_{\mathbf{u},\mathbf{v}}$?

Solution

1. mixed state averaged over the values of $\mathbf{z}$: $|\xi_{\mathbf{u},\mathbf{z},\mathbf{x}}\rangle$ is created with probability $\frac{1}{2^n} \Rightarrow$ mixed state $\rho_{\mathbf{u},\mathbf{v}} = \frac{1}{2^n}\sum_{\mathbf{z}} |\xi_{\mathbf{u},\mathbf{z},\mathbf{x}}\rangle \langle \xi_{\mathbf{u},\mathbf{z},\mathbf{x}}|$
2.

$$\begin{aligned}
\rho_{\mathbf{u},\mathbf{v}} &= \frac{1}{2^n}\sum_{\mathbf{z}} |\xi_{\mathbf{u},\mathbf{z},\mathbf{x}}\rangle \langle \xi_{\mathbf{u},\mathbf{z},\mathbf{x}}| \\
&= \frac{1}{2^{n+k_Z^\perp}}\sum_{\mathbf{z}} \sum_{\mathbf{v}_1,\mathbf{v}_2\in\mathcal{C}_Z^\perp} (-1)^{\mathbf{z}\cdot(\mathbf{v}_1+\mathbf{v}_2)} |\mathbf{u}+\mathbf{v}_1+\mathbf{x}\rangle \langle \mathbf{u}+\mathbf{v}_2+\mathbf{x}| \\
&= \frac{1}{2^{k_Z^\perp}} \sum_{\mathbf{v}\in\mathcal{C}_Z^\perp} |\mathbf{u}+\mathbf{v}+\mathbf{x}\rangle \langle \mathbf{u}+\mathbf{v}+\mathbf{x}|
\end{aligned}$$

3. Alice classically chooses $\mathbf{v} \in \mathcal{C}_Z$ at random, constructs $|\mathbf{u}+\mathbf{v}+\mathbf{x}\rangle$ using her randomly determined $\mathbf{x}$ and $\mathbf{u}$

Modification II

1. Alice creates random check bits $\mathbf{a} \in \mathbb{F}_2^n$, key bits $\tilde{\mathbf{u}} \in \mathbb{F}_2^k \sim \mathbf{u} \in \mathcal{C}_X/\mathcal{C}_Z^{\perp}$, random $\mathbf{z}, \mathbf{x} \in \mathbb{F}_2^n$ and encodes $|\mathbf{u}\rangle$ in $\mathsf{CSS}_{\mathbf{z},\mathbf{x}}(\mathcal{C}_X, \mathcal{C}_Z)$

$\Rightarrow 1.'$ Alice creates random check bits $\mathbf{a} \in \mathbb{F}_2^n$, key bits $\tilde{\mathbf{u}} \in \mathbb{F}_2^k \sim \mathbf{u} \in \mathcal{C}_X/\mathcal{C}_Z^{\perp}$, random $\mathbf{x} \in \mathbb{F}_2^n$, random $\mathbf{v} \in \mathcal{C}_Z^{\perp}$ and encodes n qubits in $|0\rangle$ and $|1\rangle$ according to the state $|\mathbf{u} + \mathbf{v} + \mathbf{x}\rangle$

Modification III

- Currently
  - Alice sends $|\mathbf{u}+\mathbf{v}+\mathbf{x}\rangle$
  - Bob receives and measures to obtain $\mathbf{u}+\mathbf{v}+\mathbf{x}+\mathbf{e}$
  - Alice sends $\mathbf{x}$
  - Bob subtracts to obtain $\mathbf{u}+\mathbf{v}+\mathbf{e}$
- If Alice chooses $\mathbf{u} \in \mathcal{C}_X$ (as opposed to $\mathcal{C}_X/\mathcal{C}_Z^{\perp}$) then $\mathbf{v}$ is unnecessary
- $\mathbf{v}+\mathbf{x}$ is completely random $\Leftrightarrow$
  - Alice chooses x sends $|\mathbf{x}\rangle$
  - Bob receives and measures to obtain $\mathbf{x}+\mathbf{e}$
  - Alice sends $\mathbf{x}-\mathbf{u}$
  - Bob subtracts to obtain $\mathbf{u}+\mathbf{e}$

$\Rightarrow$ between check and code bits

Modification IV

- Removing the Hadamard operations by encoding either in the $\{|0\rangle, |1\rangle\}$ basis or in the $\{|+\rangle, |-\rangle\}$ basis
- Removing quantum memory : Bob measures directly choosing either to measure in the $\{|0\rangle, |1\rangle\}$ basis or in the $\{|+\rangle, |-\rangle\}$ basis

Secure BB84

1. Alice creates $(4+\delta)n$ random bits
2. for each bit she creates a qubit in either the $\mathbf{Z}$ or $\mathbf{X}$ basis according to random $\mathbf{b}$ and sends them to Bob
3. she chooses a random $\mathbf{u} \in \mathcal{C}_X/\mathcal{C}_Z^{\perp}$
4. Bob receives the qubits, announces it, measure them in the $\mathbf{Z}$ or $\mathbf{X}$ basis
5. Alice announces $\mathbf{b}$ and they discard those bits Bob measure in a basis other than b
6. Alice and Bob publicly compare their check bits. Abort if #disag. $> t$. Alice is left with $\mathbf{x}$, Bob with $\mathbf{x}+\mathbf{e}$
7. Alice announces $\mathbf{x}-\mathbf{u}$. Bob subtracts this from his result and correct it in $\mathcal{C}_X$ to get $\mathbf{u}$
8. They compute the coset $\mathbf{u}+\mathcal{C}_Z^{\perp}$ in $\mathcal{C}_X$ to get the key $\tilde{\mathbf{u}}$

Information reconciliation and privacy amplification

- $\mathcal{C}_Z$ used for information reconciliation
- $\mathcal{C}_Z^\perp$ used for privacy amplification