LECTURE 8
DISTANCE MEASURES FOR QUANTUM STATES AND QUANTUM CRYPTOGRAPHY

INF587 Quantum computer science and applications

Thomas Debris-Alazard

Inria, École Polytechnique

Introduction to quantum cryptography!

Security relies on:

- No-cloning theorem
- Measuring modifies quantum states
- Incapacity to distinguish non-orthogonal quantum states

Distance between quantum states: essential tool for ensuring the security of quantum cryptography (what is possible or not, what can be done at best to distinguish, etc..)

$\longrightarrow$ As usual: we need first to understand where these concepts come from: classical world!

COURSE OUTLINE

1. Distances over distributions
2. Distance between quantum states
3. Bit commitment
4. Quantum Key Distribution

Information theory: modelize an information source as a random variable

$\longrightarrow$ Our aim: meaning of *"two information sources are similar to one another, or not"*

similar $\approx$ undistinguishable ; not-similar $\approx$ distinguishable

English and French texts

May be modelling as a sequence of random variables over the Roman alphabet:

- English: "th" most frequent pair of letters
- French: "es" most frequent pair of letters

$\longrightarrow$ To distinguish English and French: look the output distribution of letters

How to "quantify" that they are different? Are they as different as French and Hungarian?

$\longrightarrow$ Define a distance between sources of information/distributions

CONSEQUENCE

Distance between distributions/random variables:

- Quantifying the minimum amount of operations to distinguish them
- Difference of behaviours of an algorithm when changing some internal distribution

Extremely useful tool for cryptography, study of algorithms, etc...

Application case: f depends of some secret and g not but $\mathrm{distance}(f, g) = \varepsilon$

$\longrightarrow$ Owning f does not help to recover the secret...

Distance between quantum states:
enough to look at the distance between measurement outputs?

$\longrightarrow$ No! But let us see first the classical case...

DISTANCES OVER DISTRIBUTIONS

$\mathcal{X}$ be a finite set

- $f : \mathcal{X} \to \mathbb{R}$ such that $\begin{cases} f \geq 0 \\ \sum_{x \in \mathcal{X}} f(x) = 1 \end{cases}$ is called **a distribution**
- A **random variable** X taking its values in $\mathcal{X}$ is defined via $\mathbb{P}(X = x)$ for all $x \in \mathcal{X}$

Distributions $\iff$ Random variables

- From f: X be such that $\mathbb{P}(X = x) \stackrel{\text{def}}{=} f(x)$
- From X: f be such that $f(x) \stackrel{\text{def}}{=} \mathbb{P}(X = x)$

$\longrightarrow$ In what follows: we identify random variables and their associated distributions

Many "distances" (α-divergences) between distributions f and g:

- Statistical/Total-Variational/Trance distance:

$$\Delta(f,g) \stackrel{\text{def}}{=} \frac{1}{2}\sum_{x\in\mathcal{X}} |f(x)-g(x)|$$

- Hellinger distance:

$$H(f,g) \stackrel{\text{def}}{=} \sqrt{1-\sum_{x\in\mathcal{X}} \sqrt{f(x)}\sqrt{g(x)}}$$

- Kullback–Leibler divergence:

$$D_{\mathrm{KL}}(f||g) \stackrel{\text{def}}{=} -\sum_{x\in\mathcal{X}} f(x)\log_2\left(\frac{g(x)}{f(x)}\right)$$

- etc...

In what follows

Focus on statistical distance

Statistical distance

The statistical distance between two distributions f, g over a finite set $\mathcal{X}$:

$$\Delta(f, g) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{x \in \mathcal{X}} |f(x) - g(x)|$$

- The factor 1/2 ensures that $\Delta(f, g) \in [0, 1]$
- $\Delta(f, g) = 0 \iff f = g$
- $\Delta(\cdot, \cdot)$ defines a metric for distributions

Given $S \subseteq \mathcal{X}$:

$\sum_{x \in S} f(x)$ is *the probability that an event S occurs when picking x according to f*

An important property

$$\Delta(f,g) = \max_{S \text{ event}} |f(S) - g(S)| = \max_{S \text{ event}} \left| \sum_{x \in S} f(x) - \sum_{x \in S} g(x) \right|$$

Consequence

Let S_0 be the event reaching the maximum. This event S_0 is optimal to distinguish f and g

$\longrightarrow \Delta(f,g)$ is the quantity giving **how well** it is possible (using S_0) to distinguish f and g...

(in practice S_0 is hard to compute)

To take away: (proof in exercise session)

Given f or g but you don't know which one:

at least $\frac{1}{\Delta(f,g)}$ calls to the given random variable to take the good decision with probability ≈ 1.

property(ii)

One could imagine: applying a physical process, algorithm to the random variables X_f given by f and X_g given by g could help to distinguish them?

One could imagine: applying a physical process, algorithm to the random variables X_f given by f and X_g given by g could help to distinguish them?

$\longrightarrow$ No! Statistical distance can only decrease

An important property: data processing inequality

Given any function/algorithm F, then $F(X_f)$ and $F(X_g)$ are still random variables and

$$\Delta\left(F(X_f), F(X_g)\right) \leq \Delta(X_f, X_g)$$

F can be randomized, but its internal randomness has to be independent from X_f and X_g.

Concrete consequence:

$\mathcal{A}$ be an algorithm such that

$$\varepsilon \stackrel{\text{def}}{=} \mathbb{P}\left(\mathcal{A}(X) = \text{“success”}\right)$$

where “success” could mean: find the secret key from a public key output by X, factorise a number output by X, etc...

Then,

$$\varepsilon - \Delta(X, Y) \leq \mathbb{P}\left(\mathcal{A}(Y) = \text{“success”}\right) \leq \varepsilon + \Delta(X, Y)$$

$\longrightarrow$ Extremely useful in cryptography...

The statistical distance between two distributions:

- cannot increase after applying an algorithm, physical process (**data processing inequality**),
- minimum amount of resources to distinguish distributions: **at least** $\frac{1}{\Delta(f,g)}$ queries to distinguish f and g

In many scenarii this lower-bound is optimistic...

$\longrightarrow$ Sometimes necessarily: $\frac{1}{\Delta(f,g)^2} \gg \frac{1}{\Delta(f,g)}$ calls to be able to distinguish

Statistical distance: quantify how close are distributions

But how to quantify how close are quantum states?

DISTANCE BETWEEN QUANTUM STATES

Define a distance between quantum states why verify:

- Cannot increase after "quantum" operations (data processing inequality)
- Quantify the "minimum amount of resources" to distinguish

More about the distances can be found in (particularly proofs omitted here):
Nielsen and Chuang, *Quantum computation and quantum information*, Chapter 9

Trace distance

Let ρ, σ be two density operators, their trace distance is defined as

$$\Delta(\rho, \sigma) = |\rho - \sigma|_{\mathrm{tr}} \quad \text{where} \quad |M|_{\mathrm{tr}} \stackrel{\text{def}}{=} \mathrm{tr}\left(\sqrt{M^\dagger M}\right)$$

Be careful: $\Delta(\rho, \sigma) \neq \mathrm{tr}(\rho - \sigma)$

$\Delta(\cdot, \cdot)$ is a metric over density operators

- $\Delta(\rho, \sigma) = 0 \iff \rho = \sigma$
- $\Delta(\rho, \sigma) \in [0, 1]$
- $\Delta(\rho, \sigma) = \Delta(\sigma, \rho)$ (symmetry)
- $\Delta(\rho, \tau) \leq \Delta(\rho, \sigma) + \Delta(\sigma, \tau)$ (triangle inequality)

- If ρ and σ are co-diagonalizable ($\iff \rho\sigma = \sigma\rho$), in an orthonormal basis $(|e_i\rangle)_i$:

$$\rho = \sum_i p_i \, |e_i\rangle\langle e_i| \quad \text{and} \quad \sigma = \sum_i q_i \, |e_i\rangle\langle e_i|$$

where $p \overset{\text{def}}{=} (p_i)_i$ and $q \overset{\text{def}}{=} (q_i)_i$ are distributions.

$$\Delta(\rho, \sigma) = \tfrac{1}{2} \textstyle\sum_i |p_i - q_i| = \Delta(p, q)$$

$\longrightarrow$ We recover the classical statistical distance!

- If ρ and σ are pure states, $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\varphi\rangle\langle\varphi|$, then:

$$\Delta(\rho, \sigma) = \sqrt{1 - |\,\langle\psi|\varphi\rangle\,|^2}$$

$\longrightarrow$ If quantum states are orthogonal, their trace distance is maximal!

Is it intuitive?

- If ρ and σ are co-diagonalizable ($\iff \rho\sigma = \sigma\rho$), in an orthonormal basis $(|e_i\rangle)_i$:

$$\rho = \sum_i p_i |e_i\rangle\langle e_i| \quad \text{and} \quad \sigma = \sum_i q_i |e_i\rangle\langle e_i|$$

where $p \overset{\text{def}}{=} (p_i)_i$ and $q \overset{\text{def}}{=} (q_i)_i$ are distributions.

$$\Delta(\rho, \sigma) = \tfrac{1}{2} \textstyle\sum_i |p_i - q_i| = \Delta(p, q)$$

$\longrightarrow$ We recover the classical statistical distance!

- If ρ and σ are pure states, $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\varphi\rangle\langle\varphi|$, then:

$$\Delta(\rho, \sigma) = \sqrt{1 - |\langle\psi|\varphi\rangle|^2}$$

$\longrightarrow$ If quantum states are orthogonal, their trace distance is maximal!

Is it intuitive?

$\longrightarrow$ Yes! Orthogonal pure states are perfectly distinguishable...
(see Lecture 2)

Let ρ_0 and ρ_1 be two known density operators

- Alice has a bit $b \in \{0, 1\}$ unknown to Bob
- Suppose that Alice send ρ_b to Bob

What is the best probability for Bob to guess b?

Proposition (see Exercise Session)

$$\max_{\{\text{strategy}\}} \mathbb{P}\left(\text{Bob guesses } b\right) = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

$\longrightarrow$ The trace distance gives how well quantum states can be distinguished

Be careful: we know the strategy which reaches the maximum, but in most cases it is non-effective and it modifies the given state

One could imagine: applying a unitary evolution to quantum states help to distinguish?

i.e., increase $\Delta(\rho, \sigma)$

One could imagine: applying a unitary evolution to quantum states help to distinguish?

i.e., increase $\Delta(\rho, \sigma)$

$\longrightarrow$ No!

Invariance under unitary evolutions

$$\Delta(U\rho U^\dagger, U\sigma U^\dagger) = \Delta(\rho, \sigma), \quad \textit{for any unitary } U$$

Given ρ and σ: can we detect a difference when measuring? How to quantify it?

Given ρ and σ: can we detect a difference when measuring? How to quantify it?

$$\Delta(\rho, \sigma) = \max_{P \leq I \text{ projector}} \operatorname{tr}(P(\rho - \sigma))$$

Theorem (admitted)

Let $\{E_m\}$ be a POVM with $p \stackrel{\text{def}}{=} (\operatorname{tr}(E_m \rho))_m$ and $q \stackrel{\text{def}}{=} (\operatorname{tr}(E_m \sigma))_m$ be the distributions of outcomes m. Then,

$$\Delta(\rho, \sigma) = \max_{\{E_m\}} \Delta(p, q)$$

In particular, whatever is the measurement

$$\Delta(p, q) \leq \Delta(\rho, \sigma)$$

Concrete consequence

One needs at least $\geq \frac{1}{\Delta(\rho,\sigma)}$ measures to distinguish ρ and σ with probability ≈ 1.

And what about more general "quantum operations" like the depolarizing channel?

Definition

A quantum operation Φ is defined from a collection of matrices $A_1, \cdots, A_k$ such that

$$\sum_{i=1}^{k} A_i A_i^\dagger = I \quad \text{and} \quad \Phi(\rho) = \sum_{i=1}^{k} A_i \rho A_i^\dagger$$

$\longrightarrow$ Most general "quantum operation"

It captures: measurements, unitary, tracing out, noisy channel, etc...

Example: depolarizing channel

Quantum operation defined from $(1-p)I$, $\frac{p}{3}X$, $\frac{p}{3}Y$ and $\frac{p}{3}Z$.

Quantum data processing inequality

For any quantum operation Φ,

$$\Delta(\Phi(\rho), \Phi(\sigma)) \leq \Delta(\rho, \sigma)$$

Another important “distance” in the quantum world:

Fidelity

Let ρ, σ be two density operators, their fidelity is defined as

$$F(\rho, \sigma) = \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$$

Following properties

- $F(\sigma, \rho) = 1 \iff \sigma = \rho$
- $F(\sigma, \rho) \in [0, 1]$
- $F(\sigma, \rho) = F(\rho, \sigma)$ (symmetry)

Be careful: fidelity not a metric (triangular inequality not verified)

- If ρ and σ are co-diagonalizable ($\iff \rho\sigma = \sigma\rho$), in an orthonormal basis $(|e_i\rangle)_i$:

$$\rho = \sum_i p_i \,|e_i\rangle\langle e_i| \quad \text{and} \quad \sigma = \sum_i q_i \,|e_i\rangle\langle e_i|$$

where $p \stackrel{\text{def}}{=} (p_i)_i$ and $q \stackrel{\text{def}}{=} (q_i)_i$ are distributions.

$$F(\rho, \sigma) = \textstyle\sum_i \sqrt{p_i}\sqrt{q_i} = 1 - H(p, q)^2 \quad (H(\cdot, \cdot) \text{ Hellinger distance})$$

$\longrightarrow$ We recover $1 - H(p, q)^2$ known classically as the fidelity/Bhattacharyya coefficient.

- If ρ and σ are pure states, $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\varphi\rangle\langle\varphi|$, then:

$$F(\rho, \sigma) = |\langle\psi|\varphi\rangle|$$

In particular: **$F(\rho, \sigma) = 0$ when ρ, σ are orthogonal pure states**

Invariance under unitary evolutions

$$F(\mathsf{U}\rho\mathsf{U}^\dagger, \mathsf{U}\sigma\mathsf{U}^\dagger) = F(\rho, \sigma), \quad \textit{for any unitary } \mathsf{U}$$

Recall: trace distance is "invariant" by projection

$$\Delta(\rho, \sigma) = \max_{P \leq I \text{ projector}} \mathrm{tr}\left(P(\rho - \sigma)\right)$$

$\longrightarrow$ "Dual" operation for the fidelity: purification

Uhlmann's theorem (admitted)

For any two density operators ρ, σ,

$$F(\rho, \sigma) = \max_{|\psi\rangle} |\langle\psi|\varphi\rangle|$$

where the maximum is taken over purifications $|\psi\rangle$ of ρ, and a fixed purification $|\varphi\rangle$ of σ.

$\longrightarrow$ Useful characterization involved in many proofs concerning the fidelity

Example

Let $\rho \stackrel{\text{def}}{=} \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ and $\sigma \stackrel{\text{def}}{=} \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$: diagonalizable in the same basis

$$F(\rho, \sigma) = \sqrt{\frac{1}{2}}\sqrt{\frac{3}{4}} + \sqrt{\frac{1}{2}}\sqrt{\frac{1}{4}} = \sqrt{\frac{3}{8}} + \sqrt{\frac{1}{8}}$$

$|\psi\rangle \stackrel{\text{def}}{=} \frac{|00\rangle}{\sqrt{2}} + \frac{|11\rangle}{\sqrt{2}}$ and $|\varphi\rangle \stackrel{\text{def}}{=} \sqrt{\frac{3}{4}}|00\rangle + \sqrt{\frac{1}{4}}|11\rangle$ are purifications which are optimal with regards to Uhlmann's theorem.

Quantum trace distance could be related to the classical trace distance via measurements

$\longrightarrow$ The same holds for the fidelity

Theorem (admitted)

Let $\{\mathrm{E}_m\}$ be a POVM with $p \overset{\text{def}}{=} (\mathrm{tr}(\mathrm{E}_m\rho))_m$ and $q \overset{\text{def}}{=} (\mathrm{tr}(\mathrm{E}_m\sigma))_m$ be the distributions of outcomes m. Then,

$$F(\rho,\sigma) = \min_{\{\mathrm{E}_m\}} F(p,q) \quad \text{where} \quad F(p,q) = \sum_m \sqrt{p_m}\sqrt{q_m} \quad \text{(classical fidelity)}$$

In particular, whatever is the measurement

$$F(\rho,\sigma) \leq F(p,q)$$

Trace distance: cannot increase after a quantum operation

$\longrightarrow$ Fidelity cannot decrease

Quantum data processing inequality

For any quantum operation Φ,

$$F(\rho, \sigma) \leq F\left(\Phi(\rho), \Phi(\sigma)\right)$$

Uhlmann's theorem: fidelity is equal to the maximum inner product between to quantum states (purification)

It suggests: angle between states (density operators) ρ and σ as

$$A(\rho, \sigma) \stackrel{\text{def}}{=} \arccos F(\rho, \sigma)$$

Proposition (admitted, but proof uses Uhlmann's theorem)

$A(\cdot, \cdot)$ is a metric for density operators.

A priori: only quantum trace distance matters, why did we introduce the quantum fidelity?

A priori: only quantum trace distance matters, why did we introduce the quantum fidelity?

$\longrightarrow$ We can relate them

Fuchs - Van de Graaf inequalities

$1 - F(\rho,\sigma) \leq \Delta(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}$, or conversely $1 - \Delta(\rho,\sigma) \leq F(\rho,\sigma) \leq \sqrt{1 - \Delta(\rho,\sigma)^2}$

But is the fidelity useful?

A priori: only quantum trace distance matters, why did we introduce the quantum fidelity?

$\longrightarrow$ We can relate them

Fuchs - Van de Graaf inequalities

$$1 - F(\rho,\sigma) \leq \Delta(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}, \text{ or conversely } 1 - \Delta(\rho,\sigma) \leq F(\rho,\sigma) \leq \sqrt{1 - \Delta(\rho,\sigma)^2}$$

But is the fidelity useful? Yes!

Proposition (admitted)

$$\Delta(\rho^{\otimes k}, \sigma^{\otimes k}) \leq k\,\Delta(\rho,\sigma) \quad \text{and} \quad F(\rho^{\otimes k}, \sigma^{\otimes k}) = F(\rho,\sigma)^k$$

$\longrightarrow$ The strength of the fidelity comes from the above equality

Let's play the following game: if you ask, Alice gives to you

$$\rho_0 \stackrel{\text{def}}{=} \left(\frac{1}{2} - \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} + \varepsilon\right) |1\rangle\langle 1| \quad \text{or} \quad \rho_1 \stackrel{\text{def}}{=} \left(\frac{1}{2} + \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} - \varepsilon\right) |1\rangle\langle 1|$$

$\longrightarrow$ But once Alice made a first random choice, she will always make the same choice!

Your aim: find with probability ≈ 1 if Alice choose ρ_0 or ρ_1

Let's play the following game: if you ask, Alice gives to you

$$\rho_0 \stackrel{\text{def}}{=} \left(\frac{1}{2} - \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} + \varepsilon\right) |1\rangle\langle 1| \quad \text{or} \quad \rho_1 \stackrel{\text{def}}{=} \left(\frac{1}{2} + \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} - \varepsilon\right) |1\rangle\langle 1|$$

$\longrightarrow$ But once Alice made a first random choice, she will always make the same choice!

Your aim: find with probability ≈ 1 if Alice choose ρ_0 or ρ_1

How to proceed

Make k queries to Alice, measure each time in the $(|0\rangle\,, |1\rangle)$ basis

But how many queries k are needed to make the good decision (with high probability)?

- $\Delta(\rho_0, \rho_1) = \frac{\varepsilon}{2}$, therefore with k queries:

$$\Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \leq k\frac{\varepsilon}{2} \Longrightarrow \text{Necessarily: } k \geq \tfrac{2}{\varepsilon} \text{ to ensure } \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \text{ not too small}$$

Is it optimal?

USEFULNESS OF THE FIDELITY

Let's play the following game: if you ask, Alice gives to you

$$\rho_0 \overset{\text{def}}{=} \left(\frac{1}{2} - \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} + \varepsilon\right) |1\rangle\langle 1| \quad \text{or} \quad \rho_1 \overset{\text{def}}{=} \left(\frac{1}{2} + \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} - \varepsilon\right) |1\rangle\langle 1|$$

$\longrightarrow$ But once Alice made a first random choice, she will always make the same choice!

Your aim: find with probability ≈ 1 if Alice choose ρ_0 or ρ_1

How to proceed

Make k queries to Alice, measure each time in the $(|0\rangle\,, |1\rangle)$ basis

But how many queries k are needed to make the good decision (with high probability)?

- $\Delta(\rho_0, \rho_1) = \frac{\varepsilon}{2}$, therefore with k queries:

$$\Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \leq k\frac{\varepsilon}{2} \Longrightarrow \text{Necessarily: } k \geq \tfrac{2}{\varepsilon} \text{ to ensure } \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \text{ not too small}$$

Is it optimal? No! It turns out that $\Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \leq k\frac{\varepsilon}{2}$ is not-tight.

- $F(\rho_0, \rho_1) = 2\sqrt{\frac{1}{4} - \varepsilon^2} \approx 1 - 2\varepsilon^2$ and $F(\rho_1^{\otimes k}, \rho_2^{\otimes k}) = F(\rho_1, \rho_2)^k \approx 1 - 2k\varepsilon^2$

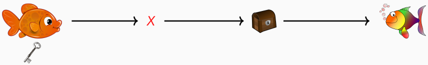
$$2k\varepsilon^2 \approx 1 - F(\rho_0^{\otimes k}, \rho_1^{\otimes k}) \leq \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \Longrightarrow \text{Choose: } k \geq \tfrac{2}{\varepsilon^2} \text{ to ensure } \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \text{ not small}$$

$\longrightarrow k \approx \frac{1}{\varepsilon^2}$ is the optimal number of queries to make the good decision (with high probability)

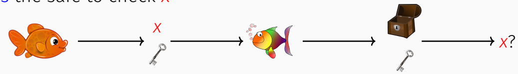
BIT COMMITMENT

COMMITMENT WITH A SAFE

- Commit phase:
  - Alice writes x on a piece of paper
  - Alice puts the paper in a safe. **She is the only one to have the key of the safe**
  - Alice sends the safe to Bob



- Reveal phase:
  - Alice reveals x and the key to unlock the safe
  - Bob opens the safe to check x



Our aim:

Use “quantum computation” to build a commitment scheme

$\longrightarrow$ Is the quantum world will offer to us an unconditionally secure commitment? (Spoiler: no...)

$$S_0 \overset{\text{def}}{=} \{|0\rangle, |1\rangle\} \quad \text{and} \quad S_1 \overset{\text{def}}{=} \{|+\rangle, |-\rangle\}$$

$\longrightarrow$ Alice wants to commit a bit $b \in \{0, 1\}$ to Bob!

Exercise

Describe a commitment protocol using S_0 and S_1 enabling Alice to commit her bit

$\Big($ **Hint:** we don't want Bob "to have any information about the commited bit" $\Big)$

$$S_0 \stackrel{\text{def}}{=} \{|0\rangle, |1\rangle\} \quad \text{and} \quad S_1 \stackrel{\text{def}}{=} \{|+\rangle, |-\rangle\}$$

Alice wants to commit b:

1. **Commit phase:** Alice chooses $|\psi\rangle \in S_b$ uniformly at random and send $|\psi\rangle$ to Bob
2. **Reveal phase:** Alice reveals $ab \in \{0,1\}^2$ to Bob where ab description of $|\psi\rangle$

$$00 \leftrightarrow |0\rangle, \quad 10 \leftrightarrow |1\rangle, \quad 01 \leftrightarrow |+\rangle \quad \text{and} \quad 11 \leftrightarrow |-\rangle$$

3. **Verification phase:** Bob measures $|\psi\rangle$ in the basis S_b (b known from ab)

Exercise

Is Bob can guess the committed bit?

Bob can only guess the committed bit with probability 1/2...

- If Alice committed 0, Bob has
$$\rho_0 = \frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}\,|1\rangle\langle 1|$$
- If Alice committed 1, Bob has
$$\rho_1 = \frac{1}{2}\,|+\rangle\langle +| + \frac{1}{2}\,|-\rangle\langle -|$$

$\longrightarrow$ But: $\rho_0 = \rho_1 = \frac{I}{2}$: they are indistinguishable (in particular, $\Delta(\rho_0, \rho_1) = 0$)

But, is the commitment scheme secure?

Exercise

Give a cheating strategy for Alice: she chooses the committed bit after the commit phase...

Alice chooses her committed value after the commit phase...

1. Alice starts with an EPR-pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
2. Alice gives the second qubit to Bob and pretends this is her commitment (up to now Alice did not make a choice)
3. If ultimately Alice wants to reveal $b = 0$: Alice measures her qubit $|x\rangle$ and gives to Bob $x0$.
4. If ultimately Alice wants to reveal $b = 1$: Alice first performs an Hadamard gate on her qubit, the state becomes
$$\frac{|+0\rangle + |-1\rangle}{\sqrt{2}} = \frac{|0+\rangle + |1-\rangle}{\sqrt{2}}$$
Alice measures her qubit and she reveals 01 if she measured $|0\rangle$, otherwise she reveals 11.

When Bob measures, everything is fine for him while **Alice has chosen her commit after the commit phase...**

One may wonder: maybe our approach with S_0 and S_1 is flawed?

$\longrightarrow$ No! But to understand this let us being more “generic”...

Remark

In what follows: a particular (but general) generic approach cannot work.

$\longrightarrow$ It turns out that any “non-interactive” bit commitment scheme can be written in the ongoing formalism

- Impossibility to build an unconditionally secure bit commitment from quantum computation:

  https://arxiv.org/pdf/quant-ph/9712023.pdf

Definition: bit commitment scheme

Protocol between two parties Alice and Bob, denoted hereafter A and B. A bit commitment scheme consists of two phases: a commit phase (Alice commits a bit b) and a reveal phase (Alice reveals to Bob her bit).

- Alice's aim: Bob cannot gain any information on her committed bit b
- Bob's aim: once Alice has made her commit, she cannot change her mind

Security requirements:

- **Completeness:** If both players are honest, the protocol should succeed with probability 1.
- **Hiding property:** If Alice is honest and Bob is dishonest, his optimal cheating probability is

$$P_{\mathrm{B}}^{\star} \stackrel{\text{def}}{=} \max_{\text{strategy}} \mathbb{P}\left(\text{Bob guesses } b \text{ after the commit phase}\right)$$

- **Binding property:** If Alice is dishonest and Bob is honest, her optimal cheating probability is

$$P_{\mathrm{A}}^{\star} = \max_{\text{strategy}} \frac{1}{2}\Big(\mathbb{P}\left(\text{Alice successfully reveals } b=0\right) + \mathbb{P}\left(\text{Alice successfully reveals } b=1\right)\Big)$$

$\longrightarrow$ Alice optimal possibility to reveal both $b=0$ and $b=1$ successfully (for a same random commit).

$\left|\psi^0_{\mathrm{AB}}\right\rangle$ and $\left|\psi^1_{\mathrm{AB}}\right\rangle$ be two (publicly known) quantum bipartite states

- **Commit phase:** Alice wants to commit b. She creates $\left|\psi^b_{\mathrm{AB}}\right\rangle$ and sends the B-part to Bob.

  $\longrightarrow$ After the commit phase, Bob has $\mathrm{tr}_{\mathrm{A}}\left(\left|\psi^b_{\mathrm{AB}}\right\rangle\right)$

- **Reveal phase:** Alice sends the A part of the quantum state $\left|\psi^b_{\mathrm{AB}}\right\rangle$ as well as b.

  $\longrightarrow$ Bob checks that he has $\left|\psi^b_{\mathrm{AB}}\right\rangle$ by projecting his (joint) state to $\left|\psi^b_{\mathrm{AB}}\right\rangle$

Sadly, this generic quantum bit commitment scheme **cannot be made secure-efficient...**

There is a strategy for Alice and Bob such that

$$P_{\mathrm{A}}^{\star} + P_{\mathrm{B}}^{\star} \geq \frac{3}{2} \quad \text{in particular, } \max\left(P_{\mathrm{A}}^{\star}, P_{\mathrm{B}}^{\star}\right) \geq \frac{3}{4}$$

In our instantiation

We have described a bit commitment scheme where $P_{\mathrm{A}}^{\star} = 1$ and $P_{\mathrm{B}}^{\star} = \frac{1}{2}$.

Bob has before the commit phase:

$$\rho_0 = \mathrm{tr}_A\left(\left|\psi_{AB}^{0}\right\rangle\right) \text{ or } \rho_1 = \mathrm{tr}_A\left(\left|\psi_{AB}^{1}\right\rangle\right)$$

Bob's optimal cheating probability

The optimal probability of Bob to guess b is

$$P_B^\star = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

$\longrightarrow$ Choose ρ_0 and ρ_1 such that $\Delta(\rho_0, \rho_1)$ is small

- Remark: the perfect secure situation is $P_B^\star = \frac{1}{2}$, Bob has nothing to do better than choosing b randomly.

But how is the optimal Alice's strategy to cheat?

Alice's optimal cheating probability

The optimal cheating probability of Alice (revealing the commit of her choice after the commit phase) is

$$P_A^\star = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2}$$

Proof

Fix a cheating strategy for Alice, σ be the state that Bob has after the commit phase.

During the reveal phase:

- $b = 0$: Alice sends qubits such that Bob has a pure state $|\varphi_0\rangle$.
- $b = 1$: Alice sends qubits such that Bob has a pure state $|\varphi_1\rangle$.

$$\mathbb{P}\left(\text{Bob accepts} \mid b = 0\right) = \left|\left\langle \varphi_0 \middle| \psi_{AB}^0 \right\rangle\right|^2 \quad \text{and} \quad \mathbb{P}\left(\text{Bob accepts} \mid b = 1\right) = \left|\left\langle \varphi_1 \middle| \psi_{AB}^1 \right\rangle\right|^2$$

By definition of the protocol: $\sigma = \mathbf{tr}_A\left(|\varphi_0\rangle\right) = \mathbf{tr}_A\left(|\varphi_1\rangle\right)$. Therefore, by Uhlmann's theorem

$$\max_{|\varphi_0\rangle} \left|\left\langle \varphi_0 \middle| \psi_{AB}^0 \right\rangle\right|^2 = F(\sigma, \rho_0)^2 \quad \text{and} \quad \max_{|\varphi_1\rangle} \left|\left\langle \varphi_1 \middle| \psi_{AB}^1 \right\rangle\right|^2 = F(\sigma, \rho_1)^2$$

Therefore, if Alice chooses correctly σ and its purifications $|\varphi_0\rangle$ and $|\varphi_1\rangle$, her probability of cheating becomes:

$$\frac{1}{2}\left(F(\sigma, \rho_0)^2 + F(\sigma, \rho_1)^1\right)$$

To conclude: see exercise session.

Bob has before the commit phase:

$$\rho_0 = \mathrm{tr}_A \left(\left| \psi_{AB}^{0} \right\rangle \right) \text{ or } \rho_1 = \mathrm{tr}_A \left(\left| \psi_{AB}^{1} \right\rangle \right)$$

$$P_A^\star = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2} \quad \text{and} \quad P_B^\star = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

Fuchs-Van de Graaf inequalities: $F(\rho_0, \rho_1) \geq 1 - \Delta(\rho_0, \rho_1)$, therefore

$$P_A^\star + P_B^\star \geq \frac{3}{2} \quad \text{in particular, } \max\left(P_A^\star, P_B^\star\right) \geq \frac{3}{4}$$

There is always a strategy for Bob or Alice to cheat with probability $\geq \frac{3}{4}$...

$\longrightarrow$ The presented bit commitment scheme cannot be unconditionally secure...

But can we build some unconditionally secure cryptography with quantum computation?

$\longrightarrow$ Yes! Quantum Key Distribution (QKD) but under some computational assumption

QUANTUM KEY DISTRIBUTION

Alice and Bob want to share privately a message. How to proceed?

One-time Pad

- Alice and Bob share a secret key $K \in \{0,1\}^n$ which has been chosen uniformly at random
- Alice wishes to send $M \in \{0,1\}^n$ to Bob. She sends:

$$C(M) = M \oplus K$$

- Bob receives $C(M)$ and computes $C(M) \oplus K = M$

Security aim: anyone that intercepts $C(M)$ without knowing K "cannot recover" M.

One-time pad: perfectly secure, even with unbounded computation impossibility to recover M

Given two possibly send messages (M_1, M_2): $\mathbb{P}_K(C(M_1) = D) = \mathbb{P}_K(C(M_2) = D)$

$\longrightarrow$ Be careful: once a key is used, don't use it again... Otherwise:

Alice and Bob want to share privately a message. How to proceed?

One-time Pad

- Alice and Bob share a secret key $K \in \{0,1\}^n$ which has been chosen uniformly at random
- Alice wishes to send $M \in \{0,1\}^n$ to Bob. She sends:

$$C(M) = M \oplus K$$

- Bob receives $C(M)$ and computes $C(M) \oplus K = M$

Security aim: anyone that intercepts $C(M)$ without knowing K "cannot recover" M.

One-time pad: perfectly secure, even with unbounded computation impossibility to recover M

Given two possibly send messages (M_1, M_2): $\mathbb{P}_K(C(M_1) = D) = \mathbb{P}_K(C(M_2) = D)$

$\longrightarrow$ Be careful: once a key is used, don't use it again... Otherwise:

From : $C(M_1)$ and $C(M_2)$, compute $C(M_1) \oplus C(M_2) = M_1 \oplus M_2$ (information about M_1 and M_2)

Drawback of the one-time pad

1. Message length $\leq$ key length and one send message per key...
2. How Alice and Bob can privately share a secret key "the snake biting its tail..."

1. Message length $\leq$ key length and one send message per key...
2. Alice and Bob need first to share a secret key

To overcome these issues:

1. Advanced Encryption Scheme (**AES**): Alice and Bob share a secret key of 128 bits (at least 2^{128} classical operations to recover the key, considered to be secure)

   $\longrightarrow$ Many other encryption scheme with short keys: field known as symmetric-key cryptography

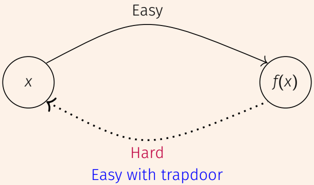
   Security: the community tries to break (cryptanalyse) proposed schemes

But the problem remains, how to share privately secret keys?

2. Key-exchange protocol: use public-key cryptography, such as trapdoor one-way functions or Diffie-Hellman protocol (1976)

Public-key cryptography relies on the use of

Trapdoor one-way function



- Alice publicly reveals f for which she knows the trapdoor
- Bob computes $f(\mathsf{K})$ and he sends it to Alice
- Alice receives $f(\mathsf{K})$ and computes $\mathsf{K} = f^{-1}(f(\mathsf{K}))$ with the trapdoor (f is supposed injective).

$\longrightarrow$ Alice and Bob shared a secret key K under the assumption that Alice is the only one to be able to invert f efficiently

How to build trapdoor one-way functions?

1. RSA: hardness to factorise an integer
2. Code and Lattice-based cryptography: hardness to decode a random code and a random lattice
3. etc...

Moral to build trapdoor one-way functions: find a mathematical hard problem **but for which there exists trapdoors**

$\longrightarrow$ Usually: difficult to find hard problems to solve such that with some quantity (the trapdoor) the problem becomes easy...

Diffie-Hellman protocol

Public data: $\mathbb{G}$ generated by g

$$\begin{array}{ccc} \text{Alice: generates } a & \xrightarrow{\quad g^a \quad} & \text{Bob: generates } b \\ \text{Alice: computes } (g^b)^a = g^{ab} & \xleftarrow[\quad g^b \quad]{} & \text{Bob: computes } (g^a)^b = g^{ab} \end{array}$$

- Alice and Bob shared g^{ab}
- Security: hard to compute g^{ab} from the knowledge of g^a and g^b (discrete logarithm problem)

Is there a key-exchange protocol using quantum computation?

$\longrightarrow$ Yes! Since the seminal work of BB84 (Bennett & Brassard, 1984)

$\big($ Quantum Key Distribution $\big)$

Key distribution

- Alice and Bob communicate over a public and authenticated channel
- At the end of the scheme, they agree on a key $\mathsf{K} \in \{0,1\}^n$.
- Any adversary eavesdropping and tampering the channel cannot gain, or vanishingly little, information about K (hard to define properly).

- Quantum Key Distribution (QKD): public channels are quantum channels

Be careful (see Exercise Session)

If the public channel is not-authenticated, there is an attack (man in the middle)

$\longrightarrow$ The channels have to be authenticated, even in the quantum setting...

But how to authenticate a channel?

Use for instance RSA-based cryptography... If you're unhappy (because broken in the quantum computing model), use post-quantum cryptography

Key distribution, quantum or not

Still need: an authenticated channel and

The only way: use a problem that is conputationally hard.

$\longrightarrow$ Sentences like: “QKD is secure because laws of physic” are false...

True sentence: “QKD is secure because laws of physic and we know problems hard even in the quantum computing model”

QKD security relies on

- Authenticated channel
- No-cloning theorem
- Measurements modify quantum states

Alice has a key string $\mathsf{K} = k_1, \cdots, k_n$ she would like to transmit to Bob

$\longrightarrow$ Alice will first perform an encoding into non-orthogonal quantum states

BB84 encoding of a bit k_i

Pick a random $b_i \in \{0, 1\}$, then

- If $b_i = 0$, build
$$|k_i\rangle^0 \stackrel{\text{def}}{=} |k_i\rangle$$
- If $b_i = 1$, build
$$|k_i\rangle^1 \stackrel{\text{def}}{=} \mathsf{H}\,|k_i\rangle = \frac{|0\rangle + (-1)^{k_i}\,|1\rangle}{\sqrt{2}}$$

k_i	b_i	$\|k_i\rangle^{b_i}$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

Why does it seems necessary to encode bits into non-orthogonal quantum states?

Alice has a key string $\mathsf{K} = k_1, \cdots, k_n$ she would like to transmit to Bob

$\longrightarrow$ Alice will first perform an encoding into non-orthogonal quantum states

BB84 encoding of a bit k_i

Pick a random $b_i \in \{0, 1\}$, then

- If $b_i = 0$, build
$$|k_i\rangle^0 \stackrel{\text{def}}{=} |k_i\rangle$$
- If $b_i = 1$, build
$$|k_i\rangle^1 \stackrel{\text{def}}{=} \mathsf{H}\,|k_i\rangle = \frac{|0\rangle + (-1)^{k_i}\,|1\rangle}{\sqrt{2}}$$

k_i	b_i	$\lvert k_i\rangle^{b_i}$
0	0	$\lvert 0\rangle$
0	1	$\lvert +\rangle$
1	0	$\lvert 1\rangle$
1	1	$\lvert -\rangle$

Why does it seems necessary to encode bits into non-orthogonal quantum states?

$\longrightarrow$ Non-orthogonal quantum states cannot be perfectly distinguished

- Alice picks a random initial raw key $\mathsf{K} = k_1, \ldots, k_n$ uniformly at random.
- For each $i \in \{1, \ldots, n\}$, Alice picks a random $b_i \in \{0, 1\}$, and sends $|k_i\rangle^{b_i}$ to Bob.
- Bob picks some random basis $b'_1, \ldots, b'_n \in \{0, 1\}$ and measures each qubit $|k_i\rangle^{b_i}$ in the basis $\{|0\rangle, |1\rangle\}$ if $b'_i = 0$, otherwise in the basis $\{|+\rangle, |-\rangle\}$. Let c_i **measurement outcome**.

THE BB84 PROTOCOL

- Alice picks a random initial raw key $\mathsf{K} = k_1, \ldots, k_n$ uniformly at random.
- For each $i \in \{1, \ldots, n\}$, Alice picks a random $b_i \in \{0, 1\}$, and sends $|k_i\rangle^{b_i}$ to Bob.
- Bob picks some random basis $b'_1, \ldots, b'_n \in \{0, 1\}$ and measures each qubit $|k_i\rangle^{b_i}$ in the basis $\{|0\rangle, |1\rangle\}$ if $b'_i = 0$, otherwise in the basis $\{|+\rangle, |-\rangle\}$. Let c_i **measurement outcome**.
- Bob sends to Alice $b'_1, \ldots, b'_n$ he used for his measurements by using a public **authenticated** channel. Alice sends back the subset $\mathcal{I} = \{i : b_i = b'_i\}$ to Bob.
- Alice picks a random $\mathcal{J} \subseteq \mathcal{I}$ of size $\frac{\sharp \mathcal{I}}{2}$ and sends $\mathcal{J}, \{k_j : j \in \mathcal{J}\}$ to Bob.
- For each $j \in \mathcal{J}$, Bob checks that $k_j = c_j$. If one of these checks fail, he aborts.
- $\mathcal{L} = \mathcal{I} \backslash \mathcal{J}$ be the subset of indices used for the final key: $\mathsf{K}_\mathsf{A} = (k_\ell)_{\ell \in \mathcal{L}}$ and $\mathsf{K}_\mathsf{B} = (c_\ell)_{\ell \in \mathcal{L}}$.
- Alice and Bob perform key reconciliation to agree on a key K_f.
- They perform privacy amplification to ensure that anyone has no information about the key: shared key $h(\mathsf{K}_f)$ for some "cryptographic" hash function h.

An eavesdropper has access to:

$$|k_i\rangle^0 \text{ or } |k_i\rangle^1 \text{ for } 1 \leq i \leq n$$

But what happens if an eavesdropper performs a measurement to guess k_i?

$\longrightarrow$ It can modify $|k_i\rangle^b$!

For instance:

Suppose that Alice sent $|\psi\rangle = |0\rangle^1 = |+\rangle$ and an eavesdropper looks at it.

1. If an attacker measures in the basis $\{|+\rangle, |-\rangle\}$ then the state is not modified
2. If an attacker measures in the basis $\{|0\rangle, |1\rangle\}$ then the state collapses to:

   $$|0\rangle \text{ with probability } 1/2 \quad \text{or} \quad |1\rangle \text{ with probability } 1/2$$

   In that case, if Bob measures the received quantum state in the basis $\{|+\rangle, |-\rangle\}$ (the same basis than Alice), he will measure $|+\rangle$ with probability 1/2

$\longrightarrow$ The eavesdropper will be detected with probability 1/4

But: $|k_i\rangle^0$ and $|k_i\rangle^1$ are non-orthogonal

$\longrightarrow$ They cannot be perfectly distinguished! At best with probability

$$\frac{1+\Delta(|+\rangle, |1\rangle)}{2} = \frac{1+\Delta(|-\rangle, |1\rangle)}{2} = \cdots = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$$

$\mathsf{K}_\mathsf{A} = (k_\ell)_{\ell \in \mathcal{L}}$ and $\mathsf{K}_\mathsf{B} = (c_\ell)_{\ell \in \mathcal{L}}$ may be different at the end of the protocol

- An eavesdropper only intercepted a small number of qubits (so is not caught with some constant probability)
- Hardware imperfection in the signal transmission or in the measurement create some inconsistency.

Key reconciliation

Alice chooses an error correcting code $\mathcal{C}$, such $\mathsf{K}_\mathsf{A} \in \mathcal{C}$, and she publicly reveals $\mathcal{C}$.

Hoping that not too much bits between K_A and K_B are different, Bob decodes K_B in $\mathcal{C}$ to recover K_A.

- Security proof of BB84 can be found here (it uses many tools of quantum information theory)
  `https://arxiv.org/pdf/1506.08458.pdf`
- Many other QKD protocols exist, see for instance

  Nielsen and Chuang, *Quantum computation and quantum information*, Chapter 12

Don't forget

The QKD's also need "classical cryptography" to be secure...

EXERCISE SESSION