CS 6832: Quantum Cryptography August 26, 2025

Lecture 1: (Private-key) Quantum Money

Instructor: Nick Spooner *Scribe: Lucas Sandleris*

1 Intro to the class

Why do we study Quantum Cryptography?

1. Quantum information can circumvent classical impossibility.
   - Oblivious Transfer achievable from One-Way Function.
   - Quantum key distribution.
   - Quantum Money
2. Quantum Computers impact on Classical Crypto
   - Quantum Computers break some hardness assumptions (like factoring).
   - Quantum computers invalidate some security proofs.
3. It's weird
   - Quantum Crypto could be independent of classical complexity!
     - Unlike Classical Crypto, might still exist even it P=NP.

1.1 Course split into three parts

1. Unconditional Quantum Computing (no CS, just from physical phenomena).
2. Post-Quantum Cryptography
3. "Fully Quantum" (Quantum cryptography with computational assumptions)

2 Private-key Quantum Money

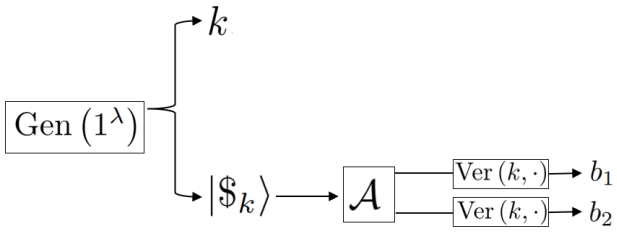
Private-key Quantum Money is a cryptographic protocol that precedes most classical cryptography. It consists of the following components:

- $\text{Gen}\left(1^\lambda\right) \longrightarrow k, |\$_k\rangle$.
- $\text{Ver}\left(k, |\psi\rangle\right) \longrightarrow$ yes/no.

We call λ the security parameter, as we will see that the security of the protocol will depend on λ (or, really, we will measure it allowing a dependence on λ).
The protocol private key is $k \in \{0,1\}^\lambda$, and its associated banknote is the quantum state $|\$_k\rangle$, which are outputs to the Generation algorithm. We call a string-state pair valid if the verifier Ver outputs yes when having the pair as input. Otherwise we say it is invalid.

We say the protocol is correct if, for all λ, $\Pr\left[\mathrm{Ver}\left(\mathrm{Gen}\left(1^\lambda\right)\right) = \mathrm{yes}\right] = 1$.

Besides the protocol being correct, we want it to satisfy some notion of security. This is, we want a (polynomial) adversary to not be able to "replicate" the banknotes without the key, as in the following diagram:



And we say that the protocol is secure if, for all polynomial-time algorithm $\mathcal{A}$ and for all λ,

$$\Pr\left[b_1 = b_2 = \mathrm{yes}\right] \leq 2^{-\Omega(\lambda)}.$$

Or, formally:

$$\Pr\left[\mathrm{Gen}(1^\lambda) \to k, |\$_k\rangle\,;\ \mathcal{A}\left(|\$_k\rangle\right) \to |\psi_1\rangle, |\psi_2\rangle\,;\ \mathrm{Ver}\left(k\,|\psi_i\rangle\right) \to b_i;\ b_1 = b_2 = \mathrm{yes}\right] \leq 2^{-\Omega(\lambda)}.$$

One important observation is that, if we aimed to do this classically by replacing $|\$_k\rangle$ with a string, then we could just have $\mathcal{A}$ return two copies of the string.
To justify why such a protocol is however possible making use of quantum states, we will look at the **No Cloning Theorem**.
Before doing so, we introduce some definitions:

Definition 2.1. An n-qubit quantum state is a unit vector $|\psi\rangle \in \mathbb{C}^{2^n}$.

Definition 2.2. If $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$ are quantum states, the combined system is represented using the (bilinear and norm-preserving) Kronecker tensor product:

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\rangle\,|\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$$

Fact 2.3. *Any quantum operation can be modeled as follows:*

$$|\psi\rangle \xrightarrow[adjoin]{} |\psi\rangle\,|e\rangle \xrightarrow[\mathcal{U}]{} \mathcal{U}\,|\psi\rangle\,|e\rangle \xrightarrow[discard]{} \rho$$

where $\mathcal{U}$ is a unitary operator (this is, $\mathcal{U}^\dagger\mathcal{U} = \mathcal{U}\mathcal{U}^\dagger = \mathcal{I}$).

Theorem 2.4 (No Cloning Theorem)**.** *There is no quantum operator Φ such that $\Phi\,|\psi\rangle = |\psi\rangle\,|\psi\rangle$ for every quantum state $|\psi\rangle$.*

Proof. Suppose that there exist $\mathcal{U}, |e\rangle$ such that, for all $|\psi\rangle$ there is $|\phi\rangle$ such that $\mathcal{U}\,|\psi\rangle\,|e\rangle = |\psi\rangle\,|\psi\rangle\,|\phi\rangle$.
Then, setting $\psi = 0$ and $\psi = 1$ yields

$$\mathcal{U}\,|0\rangle\,|e\rangle = |0\rangle\,|0\rangle\,|\phi_0\rangle \quad \text{and} \quad \mathcal{U}\,|1\rangle\,|e\rangle = |1\rangle\,|1\rangle\,|\phi_1\rangle$$

However, now set $\psi = +$, so that $|\psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. This yields

$$\mathcal{U}|+\rangle|e\rangle = |+\rangle|+\rangle|\phi_+\rangle = \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|\phi_+\rangle$$

But we also have that

$$\mathcal{U}|+\rangle|e\rangle = \frac{1}{\sqrt{2}}(\mathcal{U}|0\rangle|e\rangle + \mathcal{U}|1\rangle|e\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|\phi_0\rangle + |1\rangle|1\rangle|\phi_1\rangle)$$

This is a contradiction, as the equality

$$\frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|\phi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|\phi_0\rangle + |1\rangle|1\rangle|\phi_1\rangle)$$

does not hold for any $|\phi_0\rangle$, $|\phi_1\rangle$, $|\phi_+\rangle$, concluding the proof. □

Observation 2.5. This proof actually proves an even stronger fact, which is that no operator can clone $|0\rangle$, $|1\rangle$ and $|+\rangle$ simultaneously. This gives rise to the following idea:

Idea 2.6. Use $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ as banknotes in the Quantum Money Protocol.

Lecture 2: Quantum Money (Continued)

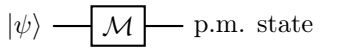
Instructor: Nick Spooner *Scribe: Santiago Lai*

3 Wiesner's Quantum Money Scheme

Before introducing Wisner's quantum money scheme, there are some definitions to give.

Definition 3.1. The Hadamard operator $H \in \mathbb{C}^{2\times 2}$ is defined such that $|+\rangle := H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $|-\rangle := H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Definition 3.2. A (simple) measurement is defined as follows. Given a Hilbert space $\mathcal{H} = \mathbb{C}^d$ and an orthonormal basis $\mathcal{M} = \{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ for $\mathcal{H}$, a measurement is given by the following process:



For a state $|\psi\rangle = \sum_{i=1}^{d} \alpha_i |i\rangle$, the measurement satisfies that $\Pr[\text{outcome is } i] = |\alpha_i|^2 = |\langle i|\psi|i|\psi\rangle|^2$. The post-measurement state, or p.m. state, collapses to the outcome $|i\rangle$ correspondingly.

Example 3.3. A measurement is often done in 2 important basis: the computational basis $\{|0\rangle, |1\rangle\}$, and the Hadamard basis $\{|+\rangle, |-\rangle\}$. In the first case we denote the measurement by  , and in the second case we denote the measurement by 

.

With the definition of measurement, we are ready to introduce Wiesner's scheme.

Definition 3.4. Wisner's quantum money scheme consists of the following Gen and Ver algorithms.

- $\text{Gen}(1^\lambda)$: Choose $\theta \leftarrow \{0,1\}^\lambda, k \leftarrow \{0,1\}^\lambda$, which together form the key. The banknote is defined as $\left|\$_k^\theta\right\rangle = \left|\$_{k_1}^{\theta_1}\right\rangle \otimes \left|\$_{k_2}^{\theta_2}\right\rangle \otimes \cdots \otimes \left|\$_{k_\lambda}^{\theta_\lambda}\right\rangle$, where $|\$_b^a\rangle = H^a|b\rangle$.
- $\text{Ver}((\theta,k),|\psi\rangle)$: For each $i \in [\lambda]$, if $\theta_i = 0$ then measure the i-th qubit in the computational basis; otherwise measure it in the Hadamard basis. Let the result be b_i. Accept if $b_i = k_i$ for all i.

Recall the definition for correctness and unclonability from last lecture. It is easy to see that the scheme is correct, since if the banknote is valid then we always measure in the correct basis. Again, the unclonability is due to the No-Cloning theorem we proved. However, it would still be useful to think of attacks on this scheme. We can immediately come up with the following attack:

Example 3.5. Consider the case where $\lambda = 1$, since the attack can easily be generalized to any λ by applying it bitwise. We measure the state in the computational basis to get $|b\rangle$, and simply send $|b\rangle |b\rangle$. If $\theta = 0$ then the attack easily successes. If $\theta = 1$, then $\Pr[b = 0] = \Pr[b = 1] = 1$, and in that case, the success probability is always $1/4$. Thus the overall success probability is $5/8$ for $\lambda = 1$, and $(5/8)^\lambda$ for any arbitrary λ.

This is far from the optimal attack one can get. In fact, we have the following result:

Theorem 3.6 (Molina, Vidick, Watrous 12')**.** *The optimal attack to Wiesner's quantum money scheme has a success probability of* $(3/4)^\lambda$.

We will show that no adversary succeeds with probability larger than $(\cos^2(\pi/8))^\lambda$ later in the lecture. Before that, we move to another important definition in quantum computing.

4 Entanglement, and the BB84 Monogamy Game

Definition 4.1. Given two Hilbert spaces $\mathcal{H}_A = \text{span}(|a_1\rangle, \ldots, |a_m\rangle)$, $\mathcal{H}_B = \text{span}(|b_1\rangle, \ldots, |b_n\rangle)$, their joint Hilbert space is $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B = \text{span}(|a_i\rangle \otimes |b_j\rangle)_{i\in[1,m]}^{j\in[1,n]}$. For a state $|\psi\rangle \in \mathcal{H}_{AB}$, it is called separable if there exists $|a\rangle \in \mathcal{H}_A, |b\rangle \in \mathcal{H}_B$ such that $|\psi\rangle = |a\rangle \otimes |b\rangle$. Otherwise, it is called an entangled state.

Example 4.2. Let $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. Then $|00\rangle, |11\rangle$ are separable states in $\mathcal{H}_{AB}$, but the EPR pair $|\Phi^+\rangle := \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is an entangled state.

In fact, entanglement is monogamous in the sense that if $\mathcal{H}_A, \mathcal{H}_B$ are very entangled, then neither $\mathcal{H}_A$ nor $\mathcal{H}_B$ can be very entangled with a third Hilbert space $\mathcal{H}_C$. The following game will be useful in showing this result, but we leave details to the next lecture.

Definition 4.3 ("BB84" monogamy game)**.** The 3-player BB84 monogamy game goes as follows. Player A, B, C are each given a part of a state $|\psi\rangle$. Player A will sample $\theta \leftarrow \{0,1\}^\lambda$, and perform measurement M^θ to get result x, where the measurement is bitwise and M^{θ_i} is in computational basis if $\theta_i = 0$, or Hadamard basis if $\theta_i = 1$. Player A then passes θ to B and C, who are allowed to perform some other operations to get y and z. They win the game if $x = y = z$.

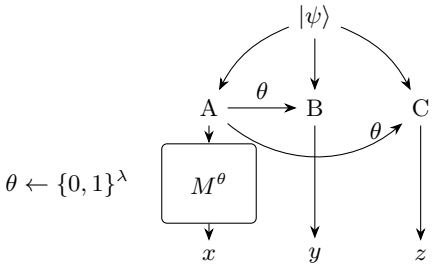


Figure 1: 3-player BB84 monogamy game

We also have a 2-player version, which is described by the following figure.

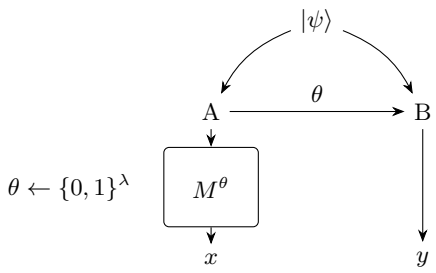


Figure 2: 2-player version

In fact, there is a winning strategy for the 2-player version. However, there is no such strategy for the 3-player BB84 monogamy game. We will see this in the next lecture.

Lecture 3: BB84 Monogamy Game

Instructor: Nick Spooner *Scribe: Santiago Lai*

5 BB84 Monogamy Game

Recall the structure of BB84 monogamy game from last lecture:

Definition 5.1. The 3-player and 2-player version of the BB84 monogamy game goes as shown in the figure below. Refer to the last lecture for more details.

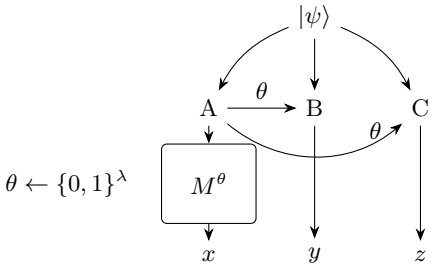


Figure 3: 3-player BB84 monogamy game

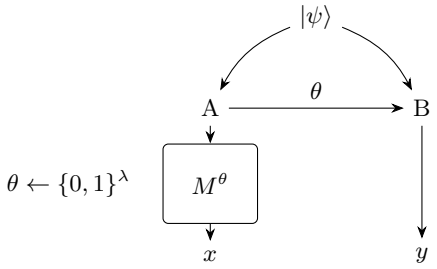


Figure 4: 2-player version

We start with an useful property of the EPR pair $|\Phi^+\rangle$, then show a winning strategy for the 2-player game.

Observation 5.2 (Ricochet property)**.** For any operator A, we have that $(A \otimes I)|\Phi^+\rangle = (I \otimes A^\top)|\Phi^+\rangle$.

Example 5.3. Let $|\psi\rangle = |\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Both players A, B will measure in the same basis M^θ where $\theta \leftarrow \{0,1\}$. Let the results of measurements be b_1, b_2, respectively. Using a case analysis:

- If $\theta = 0$, the measurement is done in the computational basis. Then $\Pr[b_1 b_2 = x_1 x_2] = |\langle x_1 x_2|\Phi^+|x_1 x_2|\Phi^+\rangle|^2 = 0$ if $x_1 \neq x_2$, or $\frac{1}{2}$ if $x_1 = x_2$. Thus we have $x_1 = x_2$.
- If $\theta = 1$, first note that $|\Phi^+\rangle = (I \otimes HH^T)|\Phi^+\rangle = (H \otimes H)|\Phi^+\rangle = \frac{|++\rangle+|--\rangle}{\sqrt{2}}$. Since the measurement is done in the Hadamard basis, by a similar analysis, we also have that $x_1 = x_2$.

Therefore, this is a wining strategy for the 2-player game.

The converse of above is also true, that is, if the strategy wins with probability 1, then $|\psi\rangle = |\Phi^+\rangle$. In particular, this implies that for the 3-player game, $\Pr[x = y] = 1$ implies that $|\psi\rangle = |\Phi^+\rangle_{AB} \otimes |c\rangle_C$, which is a separable state. Thus there is no strategy that achieves $x = z$ with probability 1.

The optimal attack for the BB84 monogamy game is described by the following theorem.

Theorem 5.4 (TFKW13)**.** *The optimal strategy for the 3-player game wins w.p. at most* $(\cos^2 \frac{\pi}{8})^\lambda$.

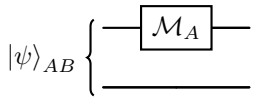
Notice that we have seen this number before; it is exactly the wining probability for the Wiesner quantum money scheme in the last lecture! Indeed, the BB84 monogamy game and the Wiesner quantum money scheme is related. To see it, we consider an alternative way to generate the keys and the banknote.

- $\mathsf{Gen}'(1^\lambda)$: Prepare $|\Phi^+\rangle = \frac{1}{\sqrt{2^\lambda}} \bigotimes_{i=1}^{\lambda} \left(|0\rangle_{A_i} |0\rangle_{B_i} + |1\rangle_{A_i} |1\rangle_{B_i}\right)$. Sample $\theta \leftarrow \{0,1\}^\lambda$, and for each $i \in [1,\lambda]$ measure A_i with M^θ. Output $((\theta, k), B)$.

Claim 5.5. *The generation algorithm Gen from last lecture is equivalent to Gen′.*

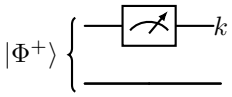
Before proving the claim, we need to define "partial" measurement.

Definition 5.6. A partial measurement is done on a joint system A, B, in the following sense:



For $|\psi\rangle = \sum_{i,j} \alpha_{i,j} |i\rangle_A |j\rangle_B$ where $\{|i\rangle\}, \{|j\rangle\}$ forms a basis for A, B, the measurement satisfies that $\Pr[\text{outcome is } i] = \sum_j |\alpha_{i,j}|^2$, and the post measurement state is $|i\rangle_A \otimes \frac{\sum_j \alpha_{i,j}|j\rangle}{\sum_j |\alpha_{i,j}|^2}$

Proof of Claim 5.5. Consider the case $\lambda = 1$, as the proof easily generalizes bitwise. For $\theta = 0$, the circuit is

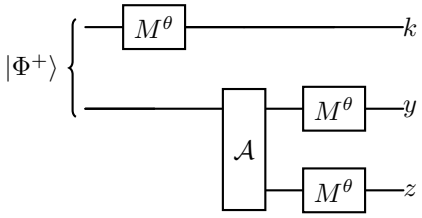


Note that $\Pr[k=0] = \Pr[k=1] = \frac{1}{2}$. When $k=0$, the p.m. state is $|00\rangle$, and when $k=1$ the p.m. state is $|11\rangle$. This is exactly the behavior described by Gen. The analysis for $\theta = 1$ is similar. □

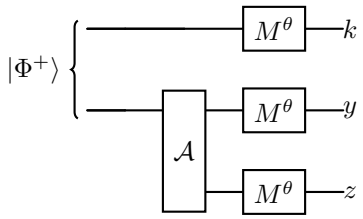
With this alternative generation algorithm Gen', we have the following result.

Proposition 5.7. The quantum money scheme reduces to the BB84 monogamy game.

Proof. With the alternative generation method, an attack on the quantum money scheme is equivalent to finding an adversary $\mathcal{A}$ such that in the following circuit



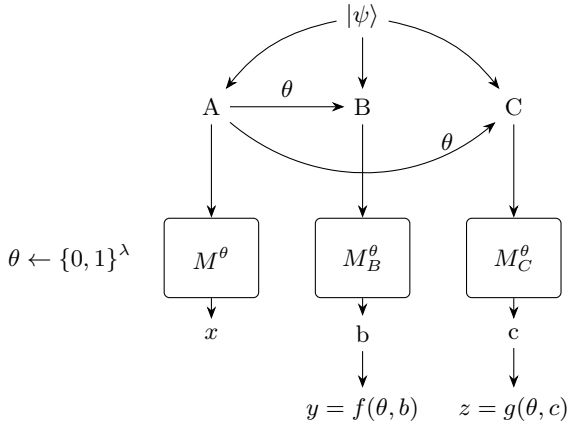
the output satisfies $k = y = z$. This is almost the BB84 monogamy game, except that we did not choose the state at start. To fix this, note that the circuit is equivalent to



Thus we can just set the initial state $|\psi\rangle$ to $(I_A \otimes \mathcal{A}_B) |\Phi^+\rangle_{AB}$. □

Finally, we prove Theorem 5.4.

Proof of Theorem 5.4. Note that the monogamy game is equivalent to finding $M^\theta = \{|x^\theta\rangle : x \in \{0,1\}^\lambda\}$ where $x^\theta = \bigotimes_{i=1}^{\theta} H^{\theta_i} |x_i\rangle$, $M_B^\theta = \{|\beta_1^\theta\rangle, \ldots, |\beta_d^\theta\rangle\}$, $M_C^\theta = \{|\gamma_1^\theta\rangle, \ldots, |\gamma_d^\theta\rangle\}$, and functions f, g such that $x = y = z$ in the figure below.



We only prove existence in this lecture, and leave optimality to the next lecture. This is easily achieved by setting $\lambda = 1$, $f = g = 0$, and $|\psi\rangle = |\frac{\pi}{8}\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C$, where $|\theta\rangle$ denotes $\cos\theta |0\rangle + \sin\theta |1\rangle$. This means that regardless of θ, player B, C will always guess 0. In this case, regardless of $\theta = 0$ or 1, we always have

$$\Pr[x = 0] = \begin{cases} |\langle 0|\frac{\pi}{8}\rangle|0|\frac{\pi}{8}\rangle|^2 = (\cos^2\frac{\pi}{8})^2 & \text{if } \theta = 0 \\ |\langle +|\frac{\pi}{8}\rangle|+|\frac{\pi}{8}\rangle|^2 = (\cos^2\frac{\pi}{8})^2 & \text{if } \theta = 1 \end{cases}$$

□

CS 6832: Quantum Cryptography September 4, 2025

Lecture 4: Monogamy of Entanglement (Optimal Adversary)

Instructor: Nick Spooner *Scribe: Lucas Sandleris*

6 Introduction

Recall the game to portray monogamy of entanglement:

- Player A prepares a tripartite state $|\psi\rangle_{ABC}$, where registers A, B, C are arbitrary finite-dimensional quantum systems. She sends register A to the referee, B to Player B, and C to Player C.
- The referee samples $\theta \in \{0, 1\}$ uniformly at random.
  - If $\theta = 0$, the referee measures A in the computational basis
  $$M^0 := \{|0\rangle, |1\rangle\}.$$
  - If $\theta = 1$, the referee measures A in the Hadamard basis
  $$M^1 := \{|+\rangle, |-\rangle\}.$$

  This yields an outcome $x \in \{0, 1\}^n$.
- Player B and Player C both receive θ.
  - Player B measures register B in basis
  $$M_B^\theta := \{|\beta_1^\theta\rangle, \ldots, |\beta_d^\theta\rangle\}$$
  and obtains outcome b.
  - Player C measures register C in basis
  $$M_C^\theta := \{|\gamma_1^\theta\rangle, \ldots, |\gamma_\ell^\theta\rangle\}$$
  and obtains outcome c.
- Player B and Player C output classical bits
$$y = f(\theta, b), \quad z = g(\theta, c),$$
- The players win if $y = z = x$.

Any strategy will be modeled as $\left(|\psi\rangle_{ABC}, \left(M_B^\theta, M_C^\theta\right)_{\theta\in\{0,1\}}, f, g\right)$. What we will prove is that, at most, the probability of winning is $\cos^2 \frac{\pi}{8}$.
First, there's some Linear Algebra background needed:

1. SVD: every matrix M can be written as $\mathcal{U}\Sigma V^T$, where $\mathcal{U}, V$ are unitary and Σ is diagonal. The entries of Σ are the **Singular Values** of M, and the eigenvalues of $M^\dagger M$. If M is Hermitian, the singular values equal the eigenvalues of M.

2. A matrix is **Positive Semi-Definite** (psd) if, for all $|x\rangle$, $\langle x|M|x|x|M|x\rangle \geq 0$ ($\iff$ all eigenvalues of M are non-negative).

   - Loewner ordering: $A \geq B$ iff $A - B$ is psd

3. Dirac's notation: $\langle\psi| = |\psi\rangle^\dagger$ and $\langle u|v|u|v\rangle = |u\rangle^\dagger |v\rangle = \langle u| \cdot |v\rangle$.

Now, with the proof:
For all $\theta \in \{0,1\}$, $|\psi\rangle = \sum_{x,b,c} \alpha^\theta_{x,b,c} \left|x^\theta\right\rangle \otimes \left|\beta^\theta_b\right\rangle \otimes \left|\gamma^\theta_c\right\rangle$.
Therefore:

$$\begin{aligned}
\Pr[\text{win}] &= \mathbb{E}_\theta \sum_{x,b,c} \Pr[x,b,c] \cdot \mathbf{1}[\, x = f(\theta,b) = g(\theta,c)\,] \\
&= \mathbb{E}_\theta \sum_{x,b,c} \left|\alpha^\theta_{x,b,c}\right|^2 \cdot \mathbf{1}[\, x = f(\theta,b) = g(\theta,c)\,] \\
&= \mathbb{E}_\theta \sum_{x,b,c} \left|\left\langle x^\theta\right| \left\langle \beta^\theta_b\right| \left\langle \gamma^\theta_c|\psi|\gamma^\theta_c|\psi\right\rangle\right|^2 \cdot \mathbf{1}[\, x = f(\theta,b) = g(\theta,c)\,] \\
&= \left\langle \psi| \left(\mathbb{E}_\theta \sum_{\substack{x,b,c \\ f(\theta,b)=g(\theta,c)=x}} \left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes \left|\beta^\theta_b\right\rangle\!\left\langle \beta^\theta_b\right| \otimes \left|\gamma^\theta_c\right\rangle\!\left\langle \gamma^\theta_c\right| \right) |\psi \right| \psi| \left(\mathbb{E}_\theta \sum_{\substack{x,b,c \\ f(\theta,b)=g(\theta,c)=x}} \left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes \left|\beta^\theta_b\right\rangle\!\left\langle \beta^\theta_b\right| \otimes \left|\gamma^\theta_c\right\rangle\!\left\langle \gamma^\theta_c\right| \right) |\psi \\
&= \Big\langle \psi| \Big(\mathbb{E}_\theta\, \Pi_\theta \Big) |\psi \Big| \psi| \Big(\mathbb{E}_\theta\, \Pi_\theta \Big) |\psi \Big\rangle
\end{aligned}$$

where $\Pi_\theta := \sum_{\substack{x,b,c \\ f(\theta,b)=g(\theta,c)=x}} |x^\theta\rangle\langle x^\theta| \otimes |\beta^\theta_b\rangle\langle\beta^\theta_b| \otimes |\gamma^\theta_c\rangle\langle\gamma^\theta_c|$.
Therefore, the maximal probability equals the largest eigenvalue of $\mathbb{E}_\theta \Pi_\theta$. But, as Π_θ is a linear combination of Hermitian matrices, it is Hermitian itself, and thus so is its expected value (as it is a linear combination of Π_0 and Π_1, so the largest eigenvalue of $\mathbb{E}_\theta \Pi_\theta$ equals its largest singular value.
For notation purposes, let $B^\theta_y = \sum_{b, f(\theta,b)=y} |\, \beta^\theta_b\rangle\langle\beta^\theta_b \,|$ and $C^\theta_z = \sum_{c, g(\theta,c)=z} |\, \gamma^\theta_c\rangle\langle\gamma^\theta_c \,|$.
It follows that
$\Pi_\theta = \sum_x |\, x^\theta\rangle\langle x^\theta \,| \otimes B^\theta_x \otimes C^\theta_x$ is an orthogonal projector.
Recall that $\mathbb{E}_\theta \Pi_\theta = \frac{1}{2}(\Pi_0 + \Pi_1)$.

Proposition 6.1. If Π_0 and Π_1 are projectors, then $||\Pi_0 + \Pi_1|| \leq 1 + ||\Pi_0 \Pi_1||$.

Proof. Note that:

$$\Pi_0 + \Pi_1 = \begin{pmatrix} \Pi_0 & \Pi_1 \end{pmatrix} \begin{pmatrix} \Pi_0 \\ \Pi_1 \end{pmatrix} = X^\dagger X \quad \text{for } X = \begin{pmatrix} \Pi_0 \\ \Pi_1 \end{pmatrix}.$$

$$\implies \quad \|\Pi_0 \Pi_1\| = \|X^\dagger X\| = \|X X^\dagger\|.$$

But note that, for permutation matrix P:

$$X X^\dagger = \begin{pmatrix} \Pi_0 & \Pi_0\Pi_1 \\ \Pi_1\Pi_0 & \Pi_1 \end{pmatrix} = \begin{pmatrix} \Pi_0 & 0 \\ 0 & \Pi_1 \end{pmatrix} + P^\dagger \begin{pmatrix} 0 & \Pi_0\Pi_1 \\ \Pi_1\Pi_0 & 0 \end{pmatrix} P.$$

Therefore we get, by triangle inequality,

$$\|XX^\dagger\| \leq 1 + \|\Pi_0\Pi_1\|.$$

□

Now, note that

$$\Pi_0 = |0\rangle\langle 0| \otimes B_0^0 \otimes C_0^0 + |1\rangle\langle 1| \otimes B_1^0 \otimes C_1^0,$$

$$\Pi_1 = |+\rangle\langle +| \otimes B_0^1 \otimes C_0^1 + |-\rangle\langle -| \otimes B_1^1 \otimes C_1^1.$$

From these, we define

$$\widetilde{\Pi}_0 := \left(|0\rangle\langle 0| \otimes B_0^0 + |1\rangle\langle 1| \otimes B_1^0\right)_{AB} \otimes I_C,$$

$$\widetilde{\Pi}_1 := \left(|+\rangle\langle +| \otimes C_0^1 + |-\rangle\langle -| \otimes C_1^1\right)_{AC} \otimes I_B.$$

And from their definitions, it follows that

$$\widetilde{\Pi}_0 \geq \Pi_0, \qquad \widetilde{\Pi}_1 \geq \Pi_1.$$

Proposition 6.2 (Left as an exercise)**.** If $\widetilde{\Pi}_0 \geq \Pi_0$ and $\widetilde{\Pi}_1 \geq \Pi_1$, then

$$\|\widetilde{\Pi}_0\widetilde{\Pi}_1\| \geq \|\Pi_0\Pi_1\|.$$

As of now, we have $\mathbb{E}_\theta\Pi_\theta = \frac{1}{2}(\Pi_0 + \Pi_1) \leq \frac{1}{2}(1 + ||\Pi_0\Pi_1||) \leq \frac{1}{2}(1 + ||\widetilde{\Pi}_0\widetilde{\Pi}_1||)$.
But note that, as Π_0 and Π_1 are projectors,

$$\|\widetilde{\Pi}_0\widetilde{\Pi}_1\| = \sqrt{\|\widetilde{\Pi}_0\widetilde{\Pi}_1\widetilde{\Pi}_0\|}.$$

And we have that

$$\widetilde{\Pi}_0\widetilde{\Pi}_1\widetilde{\Pi}_0 = \sum_{a,b,c} |a\rangle\langle a|\, H |b\rangle\langle b| H |c\rangle\langle c| \otimes B_a^0 B_c^0 \otimes C_b^1.$$

But also noting that

$$B_a^0 B_c^0 = \begin{cases} B_a^0, & a = c, \\ 0, & a \neq c. \end{cases}$$

we have that

$$\widetilde{\Pi}_0\widetilde{\Pi}_1\widetilde{\Pi}_0 = \sum_{a,b} |a\rangle\langle a|\, H |b\rangle\langle b| H |a\rangle\langle a| \otimes B_a^0 \otimes C_b^1 = \frac{1}{2}\sum_a |\, a\rangle\langle a\,| \otimes B_a^0 \otimes \sum_b C_b^1 = \frac{1}{2}\sum_a |\, a\rangle\langle a\,| \otimes B_a^0 \otimes I \leq I/2.$$

Therefore, $||\widetilde{\Pi}_0\widetilde{\Pi}_1|| = \sqrt{||\widetilde{\Pi}_0\widetilde{\Pi}_1\widetilde{\Pi}_0||} \leq \frac{1}{\sqrt{2}}$, which implies the final result that

$$\mathbb{E}_\theta\Pi_\theta \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) = \cos^2\frac{\pi}{8},$$

as desired.

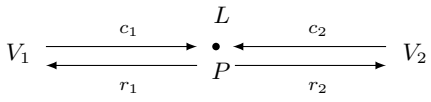
CS 6832: Quantum Cryptography September 9, 2025

Lecture 5: Position Verification and QKD (BB84 cont.)

Instructor: Nick Spooner *Scribe: Jerónimo Martín*

This lecture builds on the previous discussions about monogamy of entanglement to introduce the Position Verification game. We then make an initial attempt to construct a quantum key distribution protocol.

7 Position Verification



The Position Verification game with an honest prover.

In a Position Verification (PV) protocol, two verifiers V_1 and V_2 are separated by some distance. At the midpoint L between them is a prover P. The verifiers want to check that P is actually at L. To this end, they each send a challenge c_i ($i \in \{1, 2\}$) along this channel between them. The prover receives both, produces responses r_1, r_2 and sends one to each verifier. Verifier V_i will accept if the response r_i is adequate given c_i and if it does not take too long to accept. The goal is to only accept if both verifiers believe that the responses originated from a prover at location L. This means that responses sent by provers at other locations should be rejected. Formally, we are looking for PV protocols that satisfy the two conditions below:

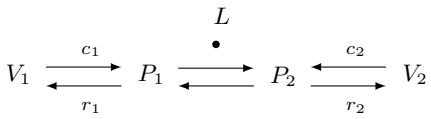
Correctness: There is a predicate Φ such that $\Phi(c_1, c_2, r_1, r_2) = 1$ and r_1, r_2 are received in time $2d(V_1, L)$, where d is a distance function[1].

Note that $d(V_1, L) = d(V_2, L)$ by our definition of L, and so $d(V_1, V_2) = 2d(V_1, L) = 2d(V_2, L)$. We can also write this distance as $d(V, L)$. Intuitively, we want to make sure that if a prover is legitimate and actually at location L (so they have no trouble receiving and sending both messages in time), then they will be able to come up with responses that the verifiers will accept in time.

Soundness: For any group of malicious provers not actually at L, it must be that $\Pr[V_1, V_2 \text{ accept}] \leq 2^{-\Omega(\lambda)}$.

It turns out that any group of provers can be reduced to just two: one between V_1 and L, and the other between V_2 and L. Although we will not prove this here, the intuitive idea is that three or more provers wouldn't be able to do much more than pass along messages to the two provers closest to the verifiers. Hence, the scenario with malicious provers looks like the diagram below.

[1] We can assume the messages travel at the speed of light and then normalize to have $c = 1$. The important part here is the distance.



The Position Verification game with malicious provers.

Theorem 7.1. *Classically, a correct and sound position verification protocol is not possible.*

Proof. Assume such a protocol exists, so it is correct. Given a classical challenge, P_1 can simply copy it and pass it along to P_2. P_2 will do the same thing, keeping c_2 and giving a copy to P_1. Thus, both P_1 and P_2 will have c_1, c_2, allowing them to produce adequate responses r_1, r_2 (they will each be able to do whatever a legitimate prover P could have done). Crucially, our time horizon of $d(V_1, V_2)$ is not intended to include time spent by provers carrying out operations on their own. Rather, it accounts for the time it takes messages to be sent from one party to another. Thus, the total time it takes for the responses to do this is exactly $d(V_1, P_1) + d(P_1, P_2) + d(P_2, V_2) = d(V_1, V_2)$. Since the protocol is correct and V_1 and V_2 receive responses satisfying Φ in time $d(V_1, V_2)$, they will accept, clearly violating soundness. □

Quantum Position Verification (QPV)

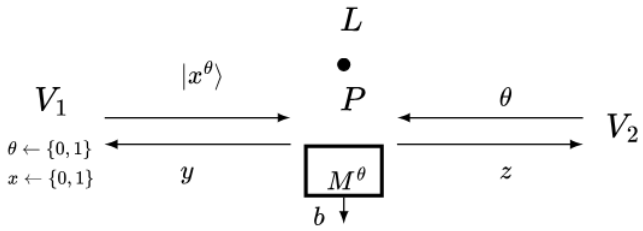
We now explore our possibilities in the quantum setting. We start with the following impossibility result, which we will not prove here. It is worth mentioning that this is not a tight lower bound on the number of EPR pairs.

Theorem 7.2. *A correct and sound position verification protocol is impossible in the quantum setting if P_1 and P_2 are sufficiently entangled, i.e. they share at least* $\exp(\exp(n))$ *EPR pairs, where n is the length of all messages in the protocol.*

Despite this, moving over to the quantum setting does offer some improvement.

Theorem 7.3. *If P_1, P_2 share $o(n)$ EPR pairs, there is a correct and secure position verification protocol.*

Instead of providing a proof, we will instead explicitly construct a protocol for $\lambda = 1$ that relies on bounding the entanglement of the provers, albeit with a much weaker security guarantee. For larger λ, the $\lambda = 1$ case we present can be done in parallel.



QPV semi-secure Protocol

V_1 will sample $\theta \sim \{0,1\}$ and $x \sim \{0,1\}$. They will then send $|x^\theta\rangle$ (as defined in previous lectures) as its challenge. V_2 sends θ as its challenge. The prover P measures in M^θ, obtaining an outcome bit b. They set

$y = z = b$ and send these as responses. V_1 receives y, V_2 receives z, and they accept iff $x = y = z$ and they received the messages in time $d(V_1, V_2)$. Correctness follows fairly straightforwardly. Since P actually has θ and $\left|x^\theta\right\rangle$, they will measure in the correct basis and obtain $b = x$, so $x = y = z$ holds. Also, if P is actually at L, the total time the protocol takes is $d(V, L)$ (V_1 and V_2's messages are sent at the same time) for P to receive the challenges plus $d(V, L)$ for them to receive the responses. This is $2d(V, L) = d(V_1, V_2)$, so the verifiers accept.

We now show that a (much) weaker form of the security condition holds in this case.

Theorem 7.4. *Instead of being able to break security with probability* 1*, any malicious provers will be limited to at most* $\cos^2(\pi/8)$*.*

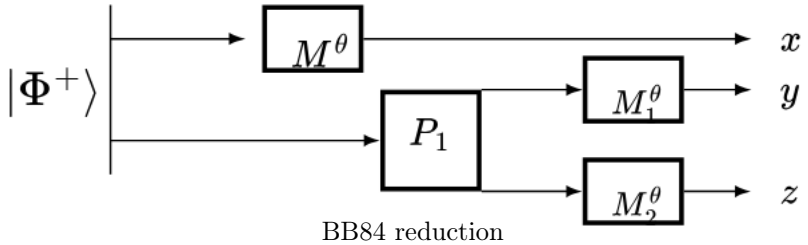
Proof.

Observation 7.5. In order to satisfy the time constraints, the two malicious provers are limited to exchanging a single message.

Given this observation, if P_1 and P_2 are not (very) entangled, e.g. they only share $o(n)$ EPR pairs, we can assume WLOG that P_2 just forwards θ to P_1. The underlying assumption here is that P_1 is able to compute anything P_2 can when given θ. Thus, P_1 performs some computation, sends part of the resulting state to P_2 and keeps the other part. They then each perform a measurement (M_1^θ and M_2^θ) and send the outcome to their respective verifier. To simplify the analysis, we will make use of the following Lemma.

Lemma 7.6. *Sampling* $\theta \sim \{0, 1\}$ *and measuring* $|\Phi^+\rangle$ *in* M^θ *is equivalent to sampling* $\theta \sim \{0, 1\}$ *and* $x \sim \{0, 1\}$ *to then prepare* $\left|x^\theta\right\rangle$*, in the sense that the distribution of* $(x, \left|x^\theta\right\rangle)$ *in the latter case is the same as the distribution of the measured qubit of the EPR pair and the other qubit pair in the former.*

This allows us to model the protocol when there are malicious provers in the diagram below.



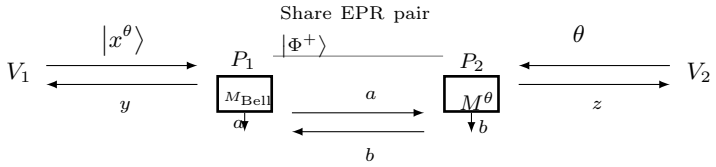
BB84 reduction

V_2 just produces θ, and P_2's role has been limited to simply giving θ to P_1, so we omit them from the diagram with the understanding that P_1 has access to θ. V_1 has been "replaced" by the Bell state and the initial measurement. We can then imagine shifting the measurement on the first register to the right of the other two measurements. After doing this, we see that the provers' endeavor to fool the verifiers is equivalent to the BB84 monogamy game (see previous scribe notes), so $\Pr[x = y = z] \leq \cos^2(\pi/8)$. This is exactly the probability that the malicious provers win, so we have shown that this protocol is slightly better in terms of security.

□

Unfortunately, this protocol falls short if the provers do share enough EPR pairs. To see this, we now present an example of an attack.

Example 7.7. To illustrate what happens if P_1 and P_2 share an EPR pair, consider the following attack.



To understand what's going on here, we introduce a basis for two-qubit states.

Definition 7.8. The Bell Basis is defined as $M_{\text{Bell}} = \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, where

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle + |{-}{+}\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle - |{-}{-}\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle - |{-}{+}\rangle)$$

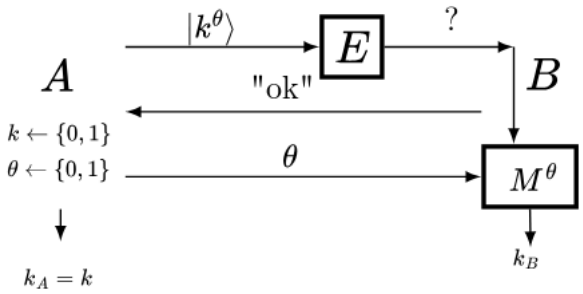
The attack works as follows: P_2 will measure their qubit of the EPR pair in M^θ, obtaining a bit b, which they send to P_1. P_1 performs a two-qubit measurement in the Bell basis on $|x^\theta\rangle$ and their qubit of the EPR pair. This will produce two classical bits, which we call a, that P_1 then sends to P_2. We can assume that they have previously agreed upon some encoding of the Bell states, so a will tell both P_1 and P_2 what the measurement was. We leave it as an exercise to observe if $\theta = 0$, then the measurement P_1 makes is $|\Phi^+\rangle$ or $|\Phi^-\rangle$ when $b = x$ and $|\Psi^+\rangle$ or $|\Phi^-\rangle$ otherwise. If $\theta = 1$, the measurement is $|\Phi^+\rangle$ or $|\Psi^+\rangle$ when $b = x$ and $|\Phi^-\rangle$ and $|\Psi^-\rangle$ otherwise. Thus, given a, P_1 and P_2 will know whether $b = x$, which will allow them to set y, z to either b or $\neg b$ in order to ensure that $x = y = z$ with probability 1. As with the other attacks, the total time it takes for the verifiers to receive the responses is simply $d(V_1, V_2)$ because P_1 and P_2 only simultaneously send each other a single message. Thus, the verifiers will accept and the attack always succeeds, violating even the weak security guarantee we found above.

Quantum Key Distribution

The goal of quantum key distribution is to achieve secret communication over public channels. In general, we model the exchange as a series of messages between A and B, where an eavesdropper E may or may not be present. After exchanging these messages, A outputs $k_A \in \{0,1\}$, and B outputs $k_B \in \{0,1\}$. If present, E outputs $k' \in \{0,1\}$. We are interested in protocols such that $\Pr[k_A = k_B] \geq 1 - 2^{-\Omega(\lambda)}$ but $\Pr[k' = k_A] \leq \frac{1}{2} + 2^{-\Omega(\lambda)}$. A and B should agree on a key, but E should not be able to do much better than trying to randomly guess what it is.

Theorem 7.9. *A protocol satisfying these requirements is clasically impossible unless E is computationally bounded. However, such a protocol is possible in the quantum setting.*

We will not prove the first half of the statement. For the second half, we will work our way up to constructing a protocol that actually works. Note that we will modify our criteria slightly given that we are now working with quantum parties. This is because it is always possible to read classical information without disrupting it, but reading quantum information will often require measurements, which can affect the quantum state under observation. Thus, for correctness, we require that if there is no eavesdropper E, $\Pr[k_A = k_B] = 1$ (this may no longer hold if there is an eavesdropper, as they might tamper with the states A and B exchange). For our first attempt, consider the exchange below.

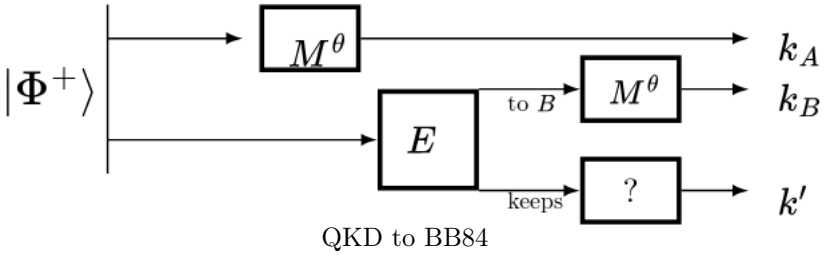


First attempt at QKD

The protocol above clearly satisfies this, since B receives $|k^\theta\rangle$ untampered with and will measure in the correct basis. However, in terms of security, it falls flat on its face. An eavesdropper E is able to send a dummy state to B while keeping $|k^\theta\rangle$. B will not know this happened, so he will send back an "ok". E will then have $|k^\theta\rangle$ and the θ that A sends when she hears from B (these are public channels), enabling E to measure $|k^\theta\rangle$ in the right basis and output the correct key with probability 1.

Observation 7.10. Despite the security flaw of the previous game, E stealing the state from B means that B's probability of getting the right key is around 1/2: since he has no access to $|k^\theta\rangle$, he can't do much better than guessing.

Idea 7.11. Based on our observation about what happens when E steals the entire state, we might conjecture that B's ability to output k_B such that k_A is affected even if E only keeps part of the state. We consider this possibility below.



QKD to BB84

In the more general case that E keeps part of the state, applying some operation to it, and then sends the rest to Bob, we can again reduce the scheme to the BB84 monogamy game. (Recall the Lemma that allows

us to substitute A's choice of k and θ for an EPR pair and a randomly sampled θ). But from a previous lecture we know that $\Pr[k_A = k_B = k']$ (we simply replace x, y, z by k_A, k_B, k') is bounded by $\cos^2(\pi/8)$, telling us that E's ability to correctly find the key decreases B's chances of doing so. We will delve further into this in the next lecture.

CS 6832: Quantum Cryptography September 11, 2025

Lecture 6: Quantum Key Distribution (BB84 cont.)

Instructor: Nick Spooner *Scribe: Jerónimo Martín*

8 Introduction

We continue our attempt to come up with a secure and correct QKD protocol, again making use of the monogamy of entanglement.

9 QKD Attempt 2

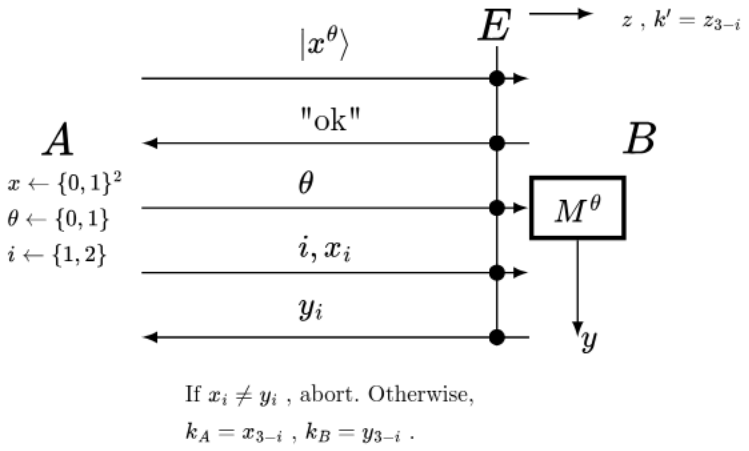
Building off of our observation from last time that if E tampers with the quantum state A sends, B is less likely to output the right key, we will broaden the possibilities for the protocol by allowing A and B to abort, which is represented by the symbol $\perp$. When A and B abort, they decide that they will not follow through with the key exchange, and therefore do not end up agreeing on a key. The exact conditions for when they decide to abort depend on the protocol, but it will generally happen when A and B detect that E has learned too much. Since we have given A and B this ability, we will adjust our requirements for correctness and security. They are now:

Correctness: If there is no eavesdropper, $\Pr[k_A = k_B, \neg\perp] = 1$. This requires that, in the absence of an eavesdropper, A and B never abort and always agree on the key.

Security: $\Pr[k_A = k' | \neg\perp] \leq \frac{1}{2} + 2^{-\Omega(\lambda)}$ when $\Pr[\neg\perp] \geq 2^{-\lambda/1000}$. Given that the protocol doesn't abort and that this happens reasonably often, we want the eavesdropper's guess to be not much better than a random guess.

Remark 9.1. *There is nothing particularly special about* 1000*. It is simply a large enough constant to ensure that the probability of not aborting is large enough. We enforce this restriction in order to avoid attacks like E always stealing the state, which would violate security, but aren't very interesting because A and B would never actually agree on a key if they always abort.*

Based on the adjusted requirements for correctness and security, the diagram below is our second attempt at a QKD protocol. We will now use two bits instead of one.



QKD attempt 2

In essence, A chooses one bit of x to compare with that bit of y. If they match, then A and B assume that their messages haven't been corrupted and output the other bit of x (A) or y (B) as the key. They abort if $x_i \neq y_i$. We one-index the bitstrings, so x_{3-i} simply refers to the other bit of x. Observe that E now tries to guess all of x, so they output a two-bit guess z.

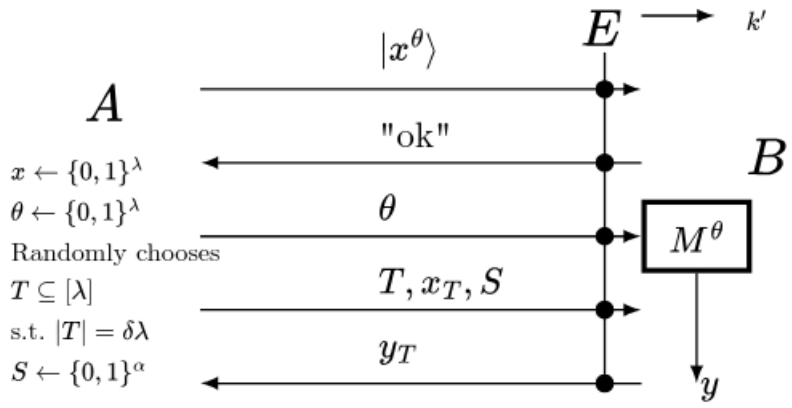
If $y \neq x$, we abort w.p. $1/2$. If they are equal, then $\Pr[z = x] \leq (\cos^2(\pi/8))^2$ by the BB84 monogamy game "theorem"[2] and the fact that we now have two bits. If $z \neq x$, then $\Pr[z_{3-i} \neq k_A] \geq 1/2$. This is progress, but the eavesdropper wins w.p. 1 when $z = x$, and our bound for that happening is $(\cos^2(\pi/8))^2 \approx 0.72$, which is not good enough.

Idea 9.2. Even though the scheme is still not as secure as we'd like, the procedure of aborting if it appears the qubits have been tampered with gives us some leverage over the eavesdropper, which we will try to exploit.

10 Actual QKD

We will use the notion of a seeded extractor, which is discussed at the end of the notes for this lecture. Further developing the ideas from our previous attempts, we present a fully secure protocol for QKD.

[2]This is simply the reduction to the monogamy of entanglement game we have been using in these lectures.



BB84 QKD Protocol

Given a set $I \subseteq [\lambda]$, the notation x_I refers to the bits i of x for which $i \in I$. This also explains the notation $x_{\hat{I}}$. Back to the protocol, A randomly chooses a subset of cardinality $\delta\lambda$ from $[\lambda]$. This is simply $\delta\lambda$ of the bits of x (as will become apparent in the proof, δ must be chosen carefully). A tells B what this set is, so B can choose the corresponding bits of y. They then compare these bits, which should always match if B received $|x^\theta\rangle$ unaltered. If $x_T \neq y_T$, A and B abort, since it means E has tampered with $|x^\theta\rangle$. Otherwise, they apply an extractor to the remaining bits of x and y, using the shared seed S, using the outputs as k_A and k_B.

Correctness follows fairly easily from the diagram above, since when there is no adversary nothing is tampered with. $x = y$ will hold because B gets $|x^\theta\rangle$ untouched and measures in the correct basis, so A and B will run the extractor on the exact same input, which will produce the same output, meaning $k_A = k_B$. As before, we are interested in proving security, which in this case means bounding $\Pr[E \to k_A | x_T = y_T] = \Pr[E \to k_A]$, since A and B do not abort only when $x_T = y_T$. Before doing so, we introduce one more tool.

Theorem 10.1. *In the BB84 monogamy game,* $\forall \gamma < 0.1, \Pr[\delta(x,y) \leq \gamma \wedge z = x] \leq 2^{-\Omega(\lambda)}$*, where* $\delta(x,y) = \frac{1}{\lambda}|\{i : x_i \neq y_i\}|$.

This theorem is a stronger version of what we had previously shown, as it simply requires that x and y be close enough to each other, not necessarily equal, in order to have $z = x$ be unlikely. Our main theorem is that

Theorem 10.2. *For the protocol described above,* $\Pr[E \to k_A | x_T = y_T] \leq 2^{-\Omega(\lambda)}$.

First notice that $x_T = y_T$ iff A and B don't abort, so this is exactly the security guarantee required of the protocol. We now prove that this holds.

Proof. Splitting into cases depending on whether or not x, y differ by less than γ,

$$\begin{aligned}\Pr[E \to k_A | x_T = y_T] &= \Pr[E \to k_A \wedge \delta(x,y) \leq \gamma | x_T = y_T] + \Pr[E \to k_A \wedge \delta(x,y) > \gamma | x_T = y_T] \\ &\leq \Pr[E \to k_A \wedge \delta(x,y) \leq \gamma | x_T = y_T] + \Pr[\delta(x,y) > \gamma | x_T = y_T]\end{aligned}$$

Call this inequality $(*)$.

We turn our attention to the second term, $\Pr[\delta(x,y) > \gamma | x_T = y_T]$. By Bayes' Theorem, this is equal to $\frac{\Pr[x_T = y_T | \delta(x,y) > \gamma]}{\Pr[x_T = y_T]}$. The denominator is the probability that we don't abort, which we can assume to be greater than $2^{-\lambda/1000}$ by our security requirement. The probability that a given bit of x and y is equal is $(1-\gamma)$, so $x_T = y_T$ has probability $(1-\gamma)^{|T|}$. This allows us to bound our expression by $\frac{(1-\gamma)^{|T|}}{2^{-\lambda/1000}} = \frac{(1-\gamma)^{\delta\lambda}}{2^{-\lambda/1000}}$. It is possible to choose constants γ, δ such that this expression is $2^{-\Omega(\lambda)}$. Putting all of this together, we have shown that $\Pr[\delta(x,y) > \gamma | x_T = y_T] \leq 2^{-\Omega(\lambda)}$.

Next, we focus on the term $\Pr[E \to k_A \wedge \delta(x,y) \leq \gamma | x_T = y_T]$. Let F be the event that $x_T = y_T \wedge \delta(x,y) \leq \gamma$. It is not too hard to show that $\Pr[F] \geq 2^{-\lambda/500}$. By the strengthened BB84 theorem above, $\Pr[E \to X \wedge F] = \Pr[k' = k_A \wedge F] \leq 2^{-\Omega(\lambda)}$. But then

$$\Pr[E \to X | F] = \Pr[E \to X \wedge F] / \Pr[F] \leq 2^{-\Omega(\lambda)} / 2^{-\lambda/500} \leq 2^{-\Omega(\lambda)}$$

This means that[3] $H_{min}(X | E\theta, F) = -\log(\max_E \Pr[E \to X | F]) \geq \Omega(\lambda)$, as $\Pr[E \to X | F] \leq 2^{-\Omega(\lambda)}$ and we have a negative log.

Fact 10.3. *A useful property of $H_{\min}$ is that if Y is supported on $\{0,1\}^t$, we have that $H_{\min}(X|Y) \geq H_{\min}(XY) - t$.*

Making use of this property in our case, with X_T being supported on $\{0,1\}^T$ and $T = \delta\lambda$, we have that $H_{\min}(X_{\overline{T}} | E\theta X_T, F) \geq H_{\min}(X | E\theta, F) - T = \Omega(\lambda) - \delta\lambda$. For the right choice of δ, we have $H_{\min}(X_{\overline{T}} | E\theta X_T, F) \geq \Omega(\lambda)$. We now use this to exploit the property of an extractor, giving us

$$D(\mathrm{Ext}(X_{\overline{T}} S) S E \Theta X_T | F,\ \mathcal{U}(\{0,1\}) S E \Theta X_T | F) \leq 2^{-\Omega(\lambda)}$$

Notice that if E were trying to guess a uniformly random bit, their probability of success would be at most $1/2$ no matter what they did. Thus, since the distributions above differ by at most $2^{-\Omega(\lambda)}$, and $\mathrm{Ext}(X_{\overline{T}}, S)$ is k_A, it must be that $\Pr[E \to k_A | F] \leq 1/2 + 2^{-\Omega(\lambda)}$. To finish up the proof, we use the following fact.

Fact 10.4. *For events A, B, C, $\Pr[A \cap B | C] = \Pr[A | B \cap C] \Pr[B | C]$. Since $\Pr[B|C] \leq 1$, $\Pr[A \cap B | C] \leq \Pr[A | B \cap C]$.*

We can now write

$$\Pr[E \to k_A \wedge \delta(x,y) \leq \gamma | x_T = y_T] \leq \Pr[E \to k_A | \delta(x,y) \leq \gamma \wedge x_T = y_T] = \Pr[E \to k_A | F] \leq 1/2 + 2^{-\Omega(\lambda)}$$

Thus, going back to (*) and using the inequalities we've derived, under the assumption that $\Pr[\neg\perp] = \Pr[x_T = y_T] \geq 2^{-\lambda/1000}$,

[3] The conditional min-entropy is defined on a joint distribution. Here, the notation $, F$ is meant to indicate that we are working with a joint distribution that is conditioned on F.

$$\begin{aligned}\Pr[E \to k_A | x_T = y_T] &\leq \Pr[E \to k_A \wedge \delta(x,y) \leq \gamma | x_T = y_T] + \Pr[\delta(x,y) > \gamma | x_T = y_T] \\ &\leq 1/2 + 2^{-\Omega(\lambda)} + 2^{-\Omega(\lambda)} \\ &= 1/2 + 2^{-\Omega(\lambda)}\end{aligned}$$

This is exactly the security guarantee we sought to prove.

□

Thus, the protocol we just examined is both correct and secure, allowing A and B to securely agree on a key using public channels.

11 Seeded Extractors

Defining seeded extractors requires us to introduce some new terminology first.

Definition 11.1. The min-entropy of a discrete RV X is $H_{\min} = -\log(\max_x \Pr[X = x])$.

Distributions that have a highly likely outcome will have lower min-entropy, while the min-entropy of those that are more "spread out" will be higher.

Definition 11.2. Let X and E be RVs supported on $(x, |\psi_x\rangle)$, i.e. they are jointly distributed. The conditional min-entropy of X given E is $H_{\min}(X|E) = -\log(\max_A \Pr[A(E) \to X])$, where A is any quantum adversary.

The max inside the log asks for the highest chance of across all quantum adversaries of guessing the corresponding value of X after being given a value of E. The better they can do, the lower the conditional min-entropy will be. Having defined these concepts, we are now ready to introduce seeded extractors.

Definition 11.3. A function $\text{Ext} : \{0,1\}^n \times \{0,1\}^\alpha \to \{0,1\}^m$ is a (k,ϵ)-extractor if $\forall X, E$ such that $H_{\min}(X|E) \geq k$, and given $S \sim \mathcal{U}(\{0,1\}^\alpha)$, we have that $D(\text{Ext}(X,S)SE, \mathcal{U}(\{0,1\}^m)SE) \leq \epsilon$, where D is the trace distance or statistical distinguishability.

Note that the concatenation of RVs is meant to indicate a joint distribution, e.g. $\mathcal{U}(\{0,1\}^m)SE$ is the joint distribution of these three RVs. Unpacking the definition slightly, the extractor is a function that attempts to extract the randomness from X by using some additional randomness S, which is the seed. The definition requires that, if we assume X is difficult enough to guess given E (the min-entropy being larger than k), the extractor produce output that looks almost (within ϵ) uniformly generated when given access to additional randomness (the seed S).

Example 11.4. Let $f_{ab}(x) = ax + b$ for $a, b, x \in \mathbb{F}_{2^n}$, a field of order 2^n. A theorem, whose proof we will not give here, tells us that $\text{Ext}(x,(a,b)) = f_{ab}(x)_1$ is a (k,ϵ)-strong seeded extractor given $k \geq 2\log(1/\epsilon)$. The notation $f_{ab}(x)_1$ refers to the first bit of x, so this extractor gives us a single bit of randomness. If we want m bits, i.e. $f_{ab}(x)_{[1,m]}$, assuming the output has enough bits, the condition is $k \geq 2m\log(1/\epsilon)$.

Lecture 7: Quantum Key Distribution cont.

Instructor: Nick Spooner *Scribe: Max Scialabba*

12 Quantum Key Distribution

12.1 Protocol

- Alice and Bob are two players trying to communicate a bit of information without it being observed by an eavesdropper Eve.
- Alice starts by generating $x, \theta \sim \mathcal{U}([0,1]^\lambda)$.
- Alice sends $\left|x^\theta\right\rangle$, where is $\theta_i = 0$, $\left|x^\theta\right\rangle_i = |x\rangle$, and if $\theta_i = 1$, $\left|x^\theta\right\rangle_i = H|x\rangle$.
- Bob verifies that he received the message, and Alice then sends over θ.
- Bob measures $|x\rangle$ using θ and the procedure outlined above, obtaining y.
- Alice generates $T \sim U(\{S \subseteq [\lambda] \mid |S| = \delta\lambda\})$, and $s \sim ([0,1]^{\delta\lambda})$.
- Alice sends T, x_T, and s, where x_T are the bits of x indexed by T.
- Bob sends back y_T.
- If $x_T \neq y_T$ they abort. Otherwise, the transmission is successful.

12.2 Proof of Security

We want to show that if $\mathbb{P}[E \to k_A \mid x_T = y_T] \leq 2^{\Omega(\lambda)}$. Here, $k_A = \texttt{Ext}(s, x_{\overline{T}})$ (i.e. the bits not needed by Bob), where $\texttt{Ext}$ is the extractor we defined in last lecture. We assume that $\mathbb{P}[x_T = y_T] \geq 2^{-\lambda/1000}$, to have some small but non zero guarantee that the protocol does not abort. This is implied by $H_{\min}(X_{\overline{T}} \mid E \circ \theta \circ X_T, F)$, where F is the condition, $x_T = y_T \wedge \delta(x,y) \leq \gamma$. We then know that $\mathcal{D}(\texttt{Ext}(X_{\overline{T}}, S) \circ S \circ E \circ \theta \circ X_T \mid F, \mathcal{U}([0,1]) \circ S \circ E \circ \theta \circ X_T \mid F) \leq 2^{-\Omega(\lambda)}$. The first part of this expression is k_A, and in the one-bit case, $\mathbb{P}[E \to k_A] = \frac{1}{2} \pm 2^{-\Omega(\lambda)}$, where as in for the second part of the expression $\mathbb{P}[E \to k_A] = \frac{1}{2}$ due to the uniform randomness.

If $H_{\min}(X \mid E) \geq k$, and $S \sim \mathcal{U}([0,1]^\delta)$, then $\mathcal{D}(\texttt{Ext}(X,S) \circ S \circ E, \mathcal{U}([0,1]) \circ S \circ E) \leq 2^{-\Omega(\lambda)}$. We know that $\mathbb{P}[E \to x \wedge F] \leq 2^{-\Omega(\lambda)} \implies \mathbb{P}[E \to x \mid F] \leq 2^{-\Omega(\lambda)}$, since $\mathbb{P}[F] \geq 2^{-\lambda/500}$. By the definition of min-entropy, $H_{\min}(X \mid E \circ \theta \circ F) = -\log\Big(\max_E(\mathbb{P}[E \to x \mid F])\Big)$. We know that since $\mathbb{P}[E \to k_1 \mid F] \leq 2^{-\Omega(\lambda)}$, $H_{\min}(X \mid E \circ \theta \circ F) \geq \Omega(\lambda)$. Finally, we know that $H_{\min}(X_{\overline{T}} \mid X_T, F) \geq H_{\min}(X \mid F) - |T|$. So, $H_{\min}(X_{\overline{T}} \mid E \circ \theta \circ F) \geq \Omega(\lambda)$, and thus $\mathbb{P}[E \to k_A \mid x_T = y_T] \leq 2^{\Omega(\lambda)}$.

13 Quantum Bit Commitment

13.1 Classical Commitment

In the bit commitment protocol, we want two parties, C and R to commit to a bit $b \in [0,1]$. To do this, we do the following procedure:

- The committer C first generates a random string $\omega \sim \mathcal{U}(\{0,1\}^\ell)$ and a random bit $b \sim \mathcal{U}([0,1])$, and computes $c_m \texttt{Com}(1^\lambda, b, \omega)$.
- C sends c_m to R, the revealer.
- C then sends b and ω to R, who accepts if $c_m = \texttt{Com}(1^\lambda, b, \omega)$.

Denote $\texttt{Com}(b) = (\texttt{Com}(1^\lambda, b, \omega) \mid \omega \sim \mathcal{U}(\{0,1\}^\ell))$. We want to have two properties:

- Hiding: $\mathcal{D}(\texttt{Com}(0), \texttt{Com}(1)) \leq 2^{-\Omega(\lambda)}$, i.e. R can't tell b given c_m.
- Binding: $\forall c_m, \nexists\, \omega_0, \omega : \forall b, \texttt{Com}(1^\lambda, b, \omega_0) = c_m$ (where c_m is defined as before), i.e. C can only reveal one choice of b.

These properties are incompatible. Given a binding bit commitment protocol, we can distinguish between $b = 0$ and $b = 1$ by going through all possible ω until either $\texttt{Com}(0) = c_m$ or $\texttt{Com}(1) = c_m$ —- by the binding property only one of $\{0,1\}$ can achieve this value, so it will determine the bit b perfectly.

13.2 Quantum Bit Commitment

For the quantum bit commitment protocol, we have an identical set up. However, instead of the computation of $c_m \to e$ and $\omega \to D$ (changing notation to match the typical quantum use) for some arbitrary classical protocol function $\texttt{Com}$, we can use the standard form theorem, which allows us to do develop a gate U_b such that $U_b \left|0^\ell\right\rangle = |\psi\rangle_b$ for arbitrary $|\psi_b\rangle$. From this, we can choose gates U_0 and U_1 that ensure that $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal.

Given e and D, we have the following new definitions for hiding and binding:

- Hiding: $\mathcal{D}(|\psi_0\rangle_{[|e|]}, |\psi_1\rangle_{[|e|]}) \leq 2^{-\Omega(\lambda)}$
- Binding: For any unitary $\mathcal{U}$ on D (of size $|D|$), $|\langle\psi_1| (I_{|e|} \otimes \mathcal{U}) |\psi_0\rangle|^2 \leq 2^{-\Omega(\lambda)}$

This binding notion is called "honest binding." It is the (subjectively) weakest binding notion, and it can be shown that all other binding notions are equivalent to it. We will show later that quantum bit commitment is impossible using this binding. We finish by proposing a sample (but invalid) quantum bit commitment scheme from Bennet and Brassard (in the same paper as the BB84 protocol):

- Commit: To commit to b, choose $x \sim \mathcal{U}([0,1])$, and send $\left|x^b\right\rangle$.

- Reveal: Send b and x, and have the user accept if $y = x$, where y is the commitment $\left|x^b\right\rangle$ measured using bit b (i.e. for $b = 0$, $\left|x^b\right\rangle = |x\rangle$, and for $b = 1$, $\left|x^b\right\rangle = H|x\rangle$).

This scheme is perfectly hiding but (not at all binding).

CS 6832: Quantum Cryptography Sep 18, 2025

Lecture 8: Impossibility of QBC

Instructor: Nick Spooner *Scribe: Yunya Zhao*

14 Last time: QBC

Last lecture, we introduced the standard form of a quantum bit commitment scheme, which we recall below:

Let $|\psi_1\rangle, |\psi_0\rangle \in \mathcal{H}_{CD}$.

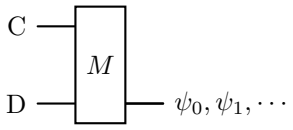
Commit Phase
$b \in \{0,1\}$, prepare $|\psi_b\rangle \in \mathcal{H}_{CD}$

$$\text{C} \xrightarrow{\quad\mathcal{C}\quad} \text{R}$$

Reveal Phase

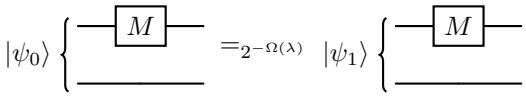
$$\text{C} \xrightarrow{\quad b, \mathcal{D}\quad} \text{R}$$

The receiver then measures with basis $M = \{|\psi_0\rangle, |\psi_1\rangle, \cdots\}$



and accepts if the outcome is ψ_b for the b received in reveal phase.

We would like a quantum bit commitment scheme to have **hiding** and **binding** properties: Hiding requires that no measurement should be able to distinguish $|\psi_0\rangle$ and $|\psi_1\rangle$, which is, $\forall M$,



And binding requres that $\forall \mathcal{U}_D$ on D

$$|\langle\psi_1| I_C \otimes \mathcal{U}_D |\psi_0\rangle| \leq 2^{-\Omega(\lambda)}$$

15 BB84 commitment scheme

The BB84 commitment scheme is the following:

- Commit: $b \in \{0,1\}$ choose $x \sim \{0,1\}$, send $\left|x^b\right\rangle$
- Reveal: send b, x, accept if measuring $\left|x^b\right\rangle$ with M^b gives outcome x

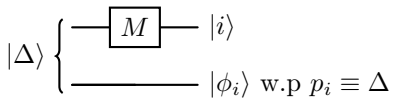
It turns out that this scheme is hiding, but not binding. To see this, we first convert the BB84 scheme into standard form.

15.1 Putting BB84 scheme in standard form

Purification First, we introduce purification of mixed states. Let $\Delta = (p_i, |\phi_i\rangle)_{i=1}^n$, $\sum_{i=1}^n p_i = 1$, $p_i > 0$. Let $\mathcal{H}_E$ be a space with basis $\{|1\rangle, \cdots, |n\rangle\}$, then

$$|\Delta\rangle = \sum_{i=1}^{p} \sqrt{p_i} \, |i\rangle_E \, |\phi_i\rangle_A$$

is a *purification* of Δ.



Note that purification are not unique, but equivalent up to a change of basis of E.

$$|\Delta\rangle = \mathcal{U}_E \otimes I_A \, |\tilde{\Delta}\rangle$$

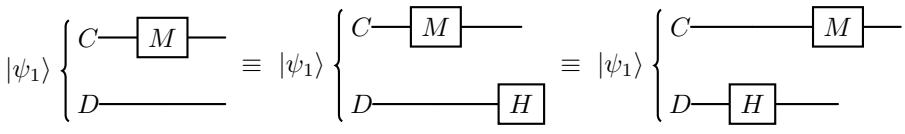
Going back to BB84 Say $b = 0$, then $\Delta = ((\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle))$,

$$|\psi_0\rangle = \frac{1}{\sqrt{2}} \, |0\rangle_D \, |0\rangle_C + \frac{1}{\sqrt{2}} \, |1\rangle_D \, |1\rangle_C = \left|\Phi^+\right\rangle$$

and if $b = 1$, then $\Delta = ((\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle))$,

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \, |0\rangle_D \, |+\rangle_C + \frac{1}{\sqrt{2}} \, |1\rangle_D \, |-\rangle_C = (I_D \otimes H_C) \left|\Phi^+\right\rangle = (H_D \otimes I_C) \left|\Phi^+\right\rangle$$

Hiding property Observe that $(H_D \otimes I) \, |\psi_1\rangle = |\psi_0\rangle$, so



NO binding property The scheme is *not* binding for the exact reason above. Alice could prepare an entangled state and delay the "commitment" to the reveal phase by apply a Hadamard matrix. In fact, it is so not binding that

$$|\langle\psi_1| \, H_D \otimes I_C \, |\psi_0\rangle|^2 = 1$$

16 Impossibility of QBC

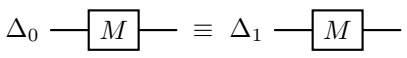
Theorem 16.1. *There is no QBC that is perfectly hiding and "nonzero" binding.*

In fact, one could prove a stronger version which states that if a scheme ε-hiding, then it must be at least $(1-\varepsilon)$-binding. So no scheme can achieve both good hiding and binding at the same time.

To prove the theorem, we need a few tools, we which we introduce now.

16.1 Distinguishability of mixed states

Two mixed states are distinguishable if $\exists M$ such that



e.g. as we saw in the BB84 scheme, $\Delta_0 = ((\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle))$ and $\Delta_1 = ((\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle))$ are indistinguishable.

Definition 16.2 (Density matrix)**.** Let $\Delta = (p_i, |\psi_i\rangle)_{i=1}^n$, the density matrix $\rho(\Delta) \in \mathbb{C}^{d\times d}$ is defined as

$$\rho(\Delta) = \sum_{i=1}^{n} p_i \, |\psi_i\rangle\langle\psi_i|$$

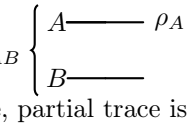
Proposition 16.3. Δ_0, Δ_1 are perfectly indistinguishable iff $\rho(\Delta_0) = \rho(\Delta_1)$.

e.g. $\rho(\Delta_0) = \frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}\,|1\rangle\langle 1| = \frac{1}{2}I$, $\rho(\Delta_1) = \frac{1}{2}\,|+\rangle\,\langle +| + \frac{1}{2}\,|-\rangle\,\langle -| = \frac{1}{2}I$, these are called maximally mixed states.

16.2 The partial trace

Let $|\psi\rangle_{AB} = \sum_{i,j} \alpha_{i,j}\,|\alpha_i\rangle_A\,|b_j\rangle_B$, then the partial trace $\mathrm{Tr}_B : \mathcal{L}(\mathcal{H}_{\mathcal{AB}}) \to \mathcal{L}(\mathcal{H}_{\mathcal{A}})$ is defined as

$$\mathrm{Tr}_B(|a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|) = |a_i\rangle\langle a_j| \cdot \langle b_k|b_l\rangle = \begin{cases} |a_i\rangle\langle a_j| & \text{if } k = l \\ 0 & \text{o/w} \end{cases}$$

$|\psi\rangle_{AB}$ 

, $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$, where $|\psi\rangle\langle\psi|$ is the density matrix of pure state $|\psi\rangle$. In some sense, partial trace is "reverse" purification.

$$\Delta \overset{\text{purify with E}}{\longrightarrow} |\Delta\rangle$$

then

$$\mathrm{Tr}_E(|\Delta\rangle\langle\Delta|) = \rho(\Delta)$$

16.3 Proof of impossibility of QBC

Now we finally prove the impossibility of QBC. We state the theorem formally.

Theorem 16.4. *If* $\mathrm{Tr}_D(|\psi_0\rangle\langle\psi_0|) = \mathrm{Tr}_D(|\psi_1\rangle\langle\psi_1|)$*, then* $\exists \mathcal{U}_D$ *on* D*, such that* $(I_C \otimes \mathcal{U}_D)|\psi_0\rangle = |\psi_1\rangle$

Proof. We will need Schmidt Decomposition, which states that for $|\psi\rangle_{AB}$, $\exists$ bases $\{|a_1\rangle, \cdots, |a_d\rangle\}$ and $\{|b_1\rangle, \cdots, |b_{d'}\rangle\}$ for A, B and $(\lambda_i)_{i=1}^r$, $\lambda_i \geq 0$ such that $|\psi\rangle = \sum_{i=1}^r \lambda_i |a_i\rangle |b_i\rangle$ and the Schmidt rank $r \leq \min(d, d')$.

$\rho = \mathrm{Tr}_D(|\psi_0\rangle\langle\psi_0|) = \mathrm{Tr}_D(|\psi_1\rangle\langle\psi_1|)$ by assumption. By Schmidt decomposition $|\psi_0\rangle = \sum_{i=1}^r \lambda_i |c_i\rangle_C |d_i\rangle_D$, and we can write $|\psi_1\rangle$ as

$$\sum_{i=1}^{d} |c_i\rangle \ |\tilde{\delta}_i\rangle$$

where $|\tilde{\delta}_i\rangle$'s may not necessarily be normalized or orthogonal.

We can calcualte $|\psi_0\rangle\langle\psi_0| = \sum_{i,j=1}^d \lambda_i\lambda_j |c_i\rangle\langle c_j| \otimes |d_i\rangle\langle d_j|$.

$$\begin{aligned}
\rho = \mathrm{Tr}_D(|\psi_0\rangle\langle\psi_0|) &= \sum_{i,j} \lambda_i\lambda_j \mathrm{Tr}_D(|c_i\rangle\langle c_j| \otimes |d_i\rangle\langle d_j|) \\
&= \sum_{i,j} \lambda_i\lambda_j |c_i\rangle\langle c_j| \cdot \langle d_i|d_j\rangle \\
&= \sum_{i} \lambda_i^2 |c_i\rangle\langle c_j| \\
&= \begin{pmatrix} \lambda_1^2 & & & & & \\ & \ddots & & & & \\ & & \lambda_r^2 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}
\end{aligned}$$

Similarly, we compute $\mathrm{Tr}_D(|\psi_1\rangle\langle\psi|)$.

$$\begin{aligned}
\mathrm{Tr}_D(|\psi_1\rangle\langle\psi|) &= \mathrm{Tr}_D(\sum_{i=1}^{d}\sum_{j=1}^{d} |c_i\rangle\langle c_j| \otimes \left|\tilde{\delta}_i\right\rangle\left\langle\tilde{\delta}_j\right|) \\
&= \sum_{i=1}^{d}\sum_{j=1}^{d} \mathrm{Tr}_D(|c_i\rangle\langle c_j| \otimes \left|\tilde{\delta}_i\right\rangle\left\langle\tilde{\delta}_j\right|) \\
&= \sum_{i=1}^{d}\sum_{j=1}^{d} (|c_i\rangle\langle c_j| \cdot \left\langle\tilde{\delta}_i\middle|\tilde{\delta}_j\right\rangle) \\
&= \begin{pmatrix} & & \\ & \mathrm{entry}(i,j) = \left\langle\tilde{\delta}_i\middle|\tilde{\delta}_j\right\rangle & \\ & & \end{pmatrix}
\end{aligned}$$

By our assumption, the two partial traces are the same, i.e. the matrices are the same. Therefore,

$$\left\langle \tilde{\delta}_i \middle| \tilde{\delta}_j \right\rangle = \begin{cases} 0 & \text{if } i \neq j \\ \lambda_i^2 & \text{if } i = j \leq r \\ 0 & \text{otherwise} \end{cases}$$

This is saying that $\| \left|\tilde{\delta}_i\right\rangle \| = \lambda_i$. Knowing this, when $i \leq r$ (otherwise it doesn't matter as it won't add to the sum) we can normalize $\left|\tilde{\delta}_i\right\rangle$ to be

$$\left|\delta_i\right\rangle = \frac{\left|\tilde{\delta}_i\right\rangle}{\lambda_i}$$

Now $\{\left|\delta_1\right\rangle, \cdots, \left|\delta_r\right\rangle\}$ form an orthonormal basis, and $\left|\psi_1\right\rangle$ can be written in basis $\left|c_i\right\rangle$ and $\left|\delta_i\right\rangle$

$$\left|\psi_1\right\rangle = \sum_{i=1}^{r} \lambda_i \left|c_i\right\rangle \left|\delta_i\right\rangle$$

To finish the proof, we define

$$\mathcal{U}_D = \sum_{i=1}^{r} \left|\delta_i\right\rangle\!\left\langle d_i\right| + \sum_{i=r+1}^{d} \left|d_i\right\rangle\!\left\langle d_i\right|$$

One can verify that $\mathcal{U}_D$ is unitary or observe that it is a valid change of basis, thus $(I \otimes \mathcal{U}_D)\left|\psi_0\right\rangle = \left|\psi_1\right\rangle$ $\square$

The above theorem is also known as the "unitary invariance of purification" which can be stated as the following: all purifications of a given mixed state are related to each other by a unitary acting only on the reference (purifying) system.

CS 6832: Quantum Cryptography Sep 23, 2025

Lecture 9: Intro to classical (post-quantum) cryptography

Instructor: Nick Spooner *Scribe: Yunya Zhao*

17 Introduction

We start a new part of the course: Post-quantum Cryptography. We will start by introducing classical (post quantum) cryptograph, namely classical algorithms/schemes that can resist quantum adversaries.

18 Classical bit commitment

The first thing we look at is still bit commitment. As before, the commitment $c \leftarrow \mathrm{Com}(b, r)$, $b \in \{0,1\}$, $r \in \{0,1\}^{p(\lambda)}$.

Hiding (statistical) define $\mathrm{Com}^\lambda(b) = (\mathrm{Com}(b,r)|r \leftarrow \{0,1\}^{p(\lambda)})$. We say the scheme is (statistically) hiding if

$$\mathrm{Com}^\lambda(0) \approx \mathrm{Com}^\lambda(1)$$

Binding (perfect) We say a scheme is binding if

$$\forall r_1, r_2, \mathrm{Com}(0, r_1) \neq \mathrm{Com}(1, r_2)$$

Bit commitment schemes are not possible with both statistical hiding and binding— not even when we have quantum information (as seen last lecture). Therefore, we consider the relaxation of the model with *computational* hiding.

To do that, we first need to define *negligible functions*.

Definition 18.1. A function $f : \mathbb{N} \to \mathbb{R}$ is negligible if for any polynomial p, $\exists \lambda_0 \in \mathbb{N}$ such that $\forall \lambda > \lambda_0$, $f(\lambda) \leq \frac{1}{p(\lambda)}$.

Examples of negligible functions include $2^{-\lambda}$, $2^{\frac{\lambda}{1000}}$, $\lambda^{-\log\log\log\lambda}$. Examples of NOT negligible functions include λ^{-1000} although it can be very small. The following propositions state useful properties of negligible functions.

Proposition 18.2.

- if f, g are both negligible, then $f + g$ is also negligible
- if f is negligible and p is a polynomial, then $p \cdot f$ is also negligible.

Now we define the notion of computational hiding

Definition 18.3 (Computational hiding)**.** A scheme is computationally hiding if $\text{Com}^\lambda(0) \approx_C \text{Com}^\lambda(1)$. This is equivalent to saying that for all polynomials t, any probabilistic classcial algorithm $\mathcal{A}(x)$ with runtime upper bounded by $t(|x|)$, the following is true

$$\left|\Pr\left[\mathcal{A}(\text{Com}^\lambda(0)) = 1\right] - \Pr\left[\mathcal{A}(\text{Com}^\lambda(1)) = 1\right]\right| \text{ is negligible}$$

With this relaxation from statistical hiding to computational hiding, we can show that bit commitment schemes conditionally exist.

Theorem 18.4. *Under reasonable conjectures (there are various such conjectures, so we won't go into the details here), computationally hiding and statistically binding commitment schemes exist.*

Proof. We will prove the above by giving a construction. This construction relies on the following objects called crytographic PRGs.

Definition 18.5 (Pseudorandom generator (PRG))**.** A PRG is a (class of) function $\{G_\lambda\}_\lambda : \{0,1\}^\lambda \to \{0,1\}^{s(\lambda)}$ efficiently computable such that for $r \leftarrow \{0,1\}^\lambda$,

$$G_\lambda(r) \approx_C \mathcal{U}(\{0,1\}^{s(\lambda)})$$

$s(\lambda) > \lambda$ is called the "stretch" of the PRG.

It is known that under reasonable conjectures, for all polynomials s, there exists PRG of stretch s. We now use these PRGs to give a commitment scheme, this result is due to Naor [1].

In the setup phase, a trusted third party will generate some string

$$\text{Setup}(1^\lambda) \to R \in \{0,1\}^{3\lambda}$$

The commitment is

$$\text{Com}_R(b, r) = G_\lambda(r) \oplus (b \cdot R)$$

where $G_\lambda : \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ is a PRG, and $b \cdot R$ is R if $b = 1$, and is 0 if $b = 0$. We now show that it is computationally hiding. By our construction,

$$\text{Com}_R(0, r) = G(r) \approx_C \mathcal{U}(\{0,1\}^{3\lambda})$$

On the other hand,

$$\text{Com}_R(1, r) = G(r) \oplus R \approx_C \mathcal{U}(\{0,1\}^{3\lambda}) \oplus R = \mathcal{U}(\{0,1\}^{3\lambda})$$

Intuitively, both distributions are computationally indistinguishable from the uniform distribution, thus the are also computationally indistinguishable. A formal proof of this will be via security reductions, where one needs to show that if you can distinguish $\text{Com}_R(1)$ from $\text{Com}_R(0)$, then you would break the PRG. We will see such proof techniques later in this course.

Now we need to show that this scheme is still statistically binding— this is not too hard.

$$\begin{aligned}
\Pr_R[\exists r_0, r_1 \text{ such that } \mathrm{Com}_R(b, r_0) = \mathrm{Com}_R(b, r_1)] &= \Pr_R[\exists r_0, r_1 \text{ such that } G(r_0) = G(r_1) \oplus R] \\
&= \Pr_R[\exists r_0, r_1 \text{ such that } G(r_0) \oplus G(r_1) = R] \\
&\leq \sum_{r_0, r_1} \Pr[G(r_0) \oplus G(r_1) = R] \\
&= \sum_{r_0, r_1} \frac{1}{2^{3\lambda}} \\
&= 2^{2\lambda} \cdot 2^{-3\lambda} \\
&= 2^{-\lambda}
\end{aligned}$$

We therefore conclude that with probability greater than $1 - 2^{-\lambda}$, $\forall r_0, r_1, \mathrm{Com}_R(b, r_0) \neq \mathrm{Com}_R(b, r_1)$, the scheme is statistically binding. □

Lecture 10: One-way Functions

Instructor: Nick Spooner *Scribe: Max Scialabba*

19 One-way functions (OWF)

Definition 19.1. A **one-way function** or **OWF** is a (polynomially) efficiently computable function of $\{0,1\}^* \to \{0,1\}^*$ that for any probabilistic polynomial time (PPT) algorithm time algorithm $\mathcal{A}$, $\mathbb{P}_{\mathbf{x}\in\{0,1\}^\lambda}[f(A(f(\mathbf{x})) = f(\mathbf{x})]$ is negligible in λ. Another way of saying this is that $\mathbb{P}_{\mathbf{x}\in\{0,1\}^\lambda}[A(f(\mathbf{x})) \in f^{-1}(x)]$ is negligible in λ.

Many things in classical cryptography imply one way functions, such as encryption, cryptographic hashing, key agreement, bit commitment, etc.. So, one-way functions are a minimal requirement towards any of these problems / tasks. However, we don't yet know whether one-way functions exist (this would imply $\mathtt{P} \neq \mathtt{NP}$). One-way functions admit the exists of pseudorandom generators, bit commitment, and secret key encryption.

Lemma 19.2. *Computationally hiding, statistically binding bit commitments imply one-way functions.*

Proof: We want to show that $\mathtt{Com}(b, \mathbf{r})$ is one-way. To do this we will show that if $\mathtt{Com}(b, \mathbf{r})$ is not one way, it is not a bit commitment.

There exists a PPT algorithm $\mathcal{A}$ such that $\mathbb{P}_{(b,\mathbf{r})\in\{0,1\}^{1+p(\lambda)}}[\mathtt{Com}(\mathcal{A}(\mathtt{Com}(b,\mathbf{r}))) = \mathtt{Com}(b,\mathbf{r})] \in \epsilon(\lambda)$, for some non-negligible factor function. ϵ.

Define an algorithm $\mathcal{A}' : \{0,1\}^* \to \{0,1\}^{1+p(x)}$ as follows: to compute $\mathcal{A}'(\mathbf{c})$ for $\mathbf{c} \in \{0,1\}^*$, run $\mathcal{A}(\mathbf{c})$ and get output $(b', \mathbf{r}')$. If $\mathtt{Com}(b', \mathbf{r}') = \mathbf{c}$, then output $(b', \mathbf{r}')$. Otherwise, obtain $b'' \sim \mathcal{U}(\{0,1\})$ and output $(b'', \mathbf{r}')$.

If $\mathtt{Com}(b, \mathbf{r}) = \mathtt{Com}(b', \mathbf{r}')$ and $\mathtt{Com}(b', \mathbf{r}') = \mathbf{c}$, then $\mathcal{A}'(\mathtt{Com}(b', \mathbf{r}')) = b$ with probability 1. Otherwise, if $\mathtt{Com}(b, \mathbf{r}) = \mathtt{Com}(b', \mathbf{r}')$ and $\mathtt{Com}(b', \mathbf{r}') \neq \mathbf{c}$, then $\mathcal{A}'(\mathtt{Com}(b', \mathbf{r}')) = b$ with probability $\frac{1}{2}$. We then get the following:

$$\mathbb{P}[\mathcal{A}'(\mathtt{Com}(1)) = 1] - \mathbb{P}[\mathcal{A}'(\mathtt{Com}(0)) = 1] = \mathbb{P}[\mathcal{A}'(\mathtt{Com}(1)) = 1] + \mathbb{P}[\mathcal{A}'(\mathtt{Com}(0)) = 1] - 1$$

Define $\epsilon_b = \mathbb{P}_{\mathbf{r}\in\{0,1\}^{p(\lambda)}}[\mathtt{Com}(\mathcal{A}(\mathtt{Com}(b,\mathbf{r}))) = \mathtt{Com}(b,\mathbf{r})]$. As such, $\epsilon(\lambda) = \frac{1}{2}(\epsilon_0 + \epsilon_1)$. We also know from the work above that $\mathbb{P}_{\mathbf{r}\in\{0,1\}^{p(x)}}[\mathcal{A}'(\mathtt{Com}(b,\mathbf{r})) = b] = \epsilon_b + \frac{1}{2}(1-\epsilon)$ (replacing b' with a generic b). Converting notation yields the following:

$$\mathbb{P}[\mathcal{A}'(\mathtt{Com}(1)) = 1] - \mathbb{P}[\mathcal{A}'(\mathtt{Com}(0)) = 1] = \epsilon_0 + \frac{1}{2}(1-\epsilon_0) + \epsilon_1 + \frac{1}{2}(1-\epsilon_1) - 1$$

$$\mathbb{P}[\mathcal{A}'(\mathtt{Com}(1)) = 1] - \mathbb{P}[\mathcal{A}'(\mathtt{Com}(0)) = 1] = \frac{1}{2}\epsilon_1 + \frac{1}{2}\epsilon_2 = \epsilon(\lambda)$$

Since $\epsilon(\lambda)$ is non-negligible, we can use $\mathcal{A}'$ to isolate $b = 1$ from $b = 0$, breaking the hiding property. As such, $\texttt{Com}(b, \mathbf{r})$ must be one-way.

20 Candidate One-way Functions

There are many candidate one-way functions, although we cannot verify any of them:

- $f_{fact}(x)$, where we use x to choose large primes p and q, and output $p \cdot q$.
- $f_{DL}(x) = g^x$ for $g \in G$, a graph of prime order.
- $f_{SIS}(A, x) = (A, Ax \pmod q)$, given $A \in \mathbb{Z}_q^{n \times m}$ and $x \in \{0,1\}^m$
- $f_{SHA}(x)$, a function designed to be as complicated as possible.

21 Post Quantum Cryptography

Definition 21.1. An algorithm is said to run in **quantum polynomial time** or **QPT** if it can be computed (polynomially) efficiently using a quantum computer.

Definition 21.2. A **post-quantum one-way function** or **PQ-OWF** is a (polynomially) efficiently computable function of $\{0,1\}^* \to \{0,1\}^*$ that for any quantum polynomial time (QPT) algorithm time algorithm $\mathcal{A}$, $\underset{\mathbf{x} \in \{0,1\}^\lambda}{\mathbb{P}}[f(A(f(\mathbf{x})) = f(\mathbf{x})]$ is negligible in λ.

Some one-way functions are not post-quantum one-way functions, as a corollary of Shor's algorithm:

Theorem 21.3. *(Shor 1994) f_{fact} and f_{DL} are not post quantum one-way functions.*

However, it is believed that f_{SIS} and f_{SHA} are likely post-quantum one-way functions.

22 Zero-knowledge Proof

Definition 22.1. A **zero knowledge proof** is a quantum protocol with the following set-up:

- A prover P.
- A verifier V which is a (classical) PPT algorithm.
- An output $(P, V)(x) = b$

Where, given P and V, for all decision problems $\texttt{L} \subseteq [0,1]^*$, we have the following:

- Completeness: $\forall x \in \mathcal{L}$, $\mathbb{P}[(P, V)(x) = 1] = 1$.

- Soundness: $\forall x \notin \mathcal{L}$, $\forall \widetilde{P}$, $\mathbb{P}[(\widetilde{P}, V)(x) = 1] \leq \frac{1}{2}$.
- Zero-knowledge: $\forall x \in \mathcal{L}$, $\forall V$ (such that V is PPT), $\exists S_{\widetilde{V}}$ called a **simulator** such that $\texttt{View}_{\widetilde{V}}((P, \widetilde{V})(x)) \approx_C S_{\widetilde{V}}(x)$ (where $\mathbf{x}_\lambda \approx_C \mathbf{y}_\lambda$ if $\mathbb{P}[\mathcal{A}(\mathbf{x}_\lambda) = 1] - \mathbb{P}[\mathcal{A}(\mathbf{y}_\lambda) = 1]$ is negligible for all PPT algorithms $\mathcal{A}$, where $\mathbf{x}_\lambda, \mathbf{y}_\lambda \sim \mathcal{U}\{0,1\}^\lambda$). $\texttt{View}_{\widetilde{V}}$ also includes a transcript of the randomness of $\widetilde{V}$.

Proposition 22.2. Every $\mathcal{L} \in \texttt{BBP}$ has a trivial zero-knowledge proof.

Proof: The prover P does nothing. V determines whether $x \in \mathcal{L}$, and such a V exists since $\mathcal{L} \in \texttt{BBP}$.

Theorem 22.3. *(Goldreich, Micali, Widgerson, 1986) If computationally hiding, statistically binding bit commitments exist, then every $L \in \texttt{NP}$ has a zero-knowledge proof.*

References

[1] Moni Naor. "Bit Commitment Using Pseudorandomness". In: *J. Cryptology* 4 (1991), pp. 151–158. DOI: 10.1007/BF00196774.