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 Computing?

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

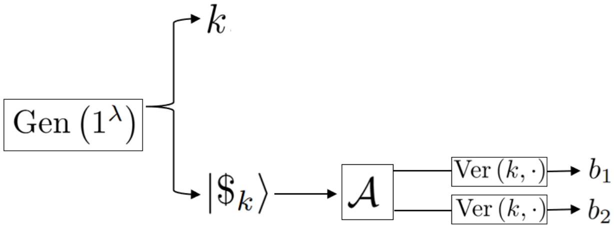
Private-key Quantum Money is a cryptographic protocol that precedes most classical cryptography. It consists of the following components:

- Gen $\left(1^\lambda\right) \longrightarrow k, |\$_k\rangle$.
- Ver $(k, |\psi\rangle) \longrightarrow$ 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:


k
$\mathrm{Gen}\left(1^{\lambda}\right)$
$|\$_k\rangle$
$\mathcal{A}$
$\mathrm{Ver}\,(k,\cdot)$
$\mathrm{Ver}\,(k,\cdot)$
b_1
b_2

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.

CS 6832: Quantum Cryptography Aug 28, 2025

Lecture 2: Quantum Money (Continued)

Instructor: Nick Spooner *Scribe: Santiago Lai*

3 Wiesner's Quantum Money Scheme

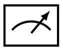
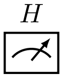
Before introducing Wisner's quantum money scheme, there are some definitions to give.

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:

$$|\psi\rangle \;—\boxed{\mathcal{M}}—\; \text{p.m. state}$$

For a state $|\psi\rangle = \sum_{i=1}^{d} \alpha_i |i\rangle$, the measurement satisfies that $\Pr[\text{outcome is } i] = |\alpha_i|^2 = |\langle i|\psi\rangle|^2$. 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.

- Gen(1^λ): Choose $\theta \leftarrow \{0,1\}^\lambda, k \leftarrow \{0,1\}^\lambda$, which together form the key. The banknote is defined as $|\$^\theta_k\rangle = |\$^{\theta_1}_{k_1}\rangle \otimes |\$^{\theta_2}_{k_2}\rangle \otimes \cdots \otimes |\$^{\theta_\lambda}_{k_\lambda}\rangle$, where $|\$^a_b\rangle = H^a|b\rangle$.
- 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 $x = y = z$.

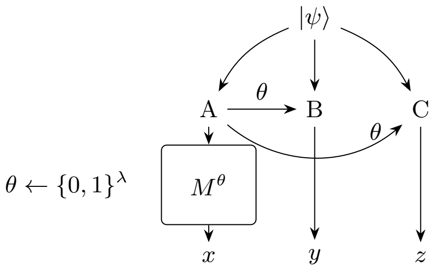


Figure 1: 3-player BB84 monogamy game

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

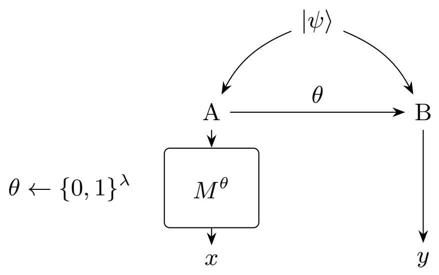


Figure 2: 2-player version

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.

CS 6832: Quantum Cryptography Sep 02, 2025

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.

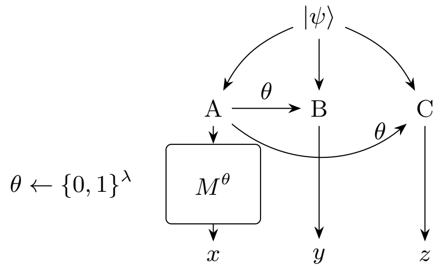


Figure 3: 3-player BB84 monogamy game

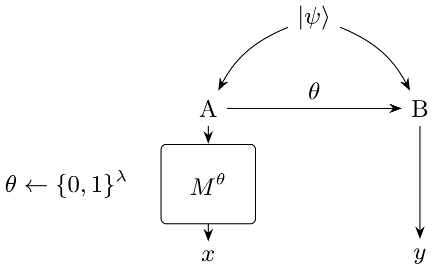


Figure 4: 2-player version

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 $\Pr[b_1 b_2 = x_1 x_2] = |\langle x_1 x_2 | \Phi^+\rangle|^2 = 0$ 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* $(\cos^2 \frac{\pi}{8})^\lambda$.

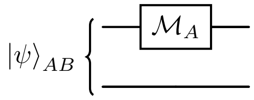
Notice that we have seen this number before; it is exactly the wining probability for the Wiesner quantum money scheme in the last lecture! Indeed, the BB84 monogamy game and the Wiesner quantum money scheme is related. To see it, we consider an alternative way to generate the keys and the banknote.

- 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$'$.*

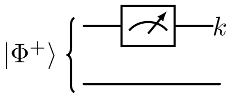
Before proving the claim, we need to define "partial" measurement.

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[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

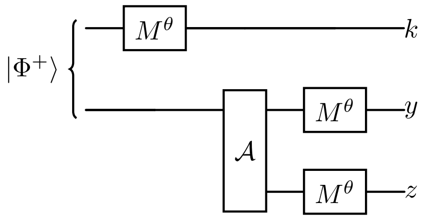


Note that $\Pr[k=0] = \Pr[k=1] = \frac{1}{2}$. When $k = 0$, the p.m. state is $|00\rangle$, and when $k = 1$ the p.m. state is $|11\rangle$. This is exactly the behavior described by Gen. The analysis for $\theta = 1$ is similar. □

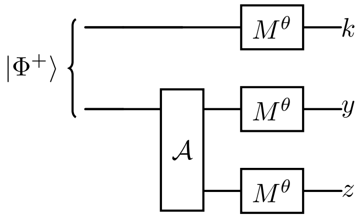
With this alternative generation algorithm Gen$'$, we have the following result.

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



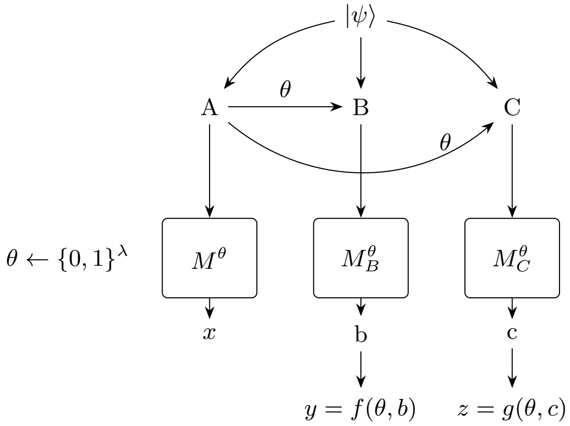
the output satisfies $k = y = z$. This is almost the BB84 monogamy game, except that we did not choose the state at start. To fix this, note that the circuit is equivalent to



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

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

□

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
  $$M_B^\theta := \{|\beta_1^\theta\rangle, \dots, |\beta_d^\theta\rangle\}$$
  and obtains outcome b.
  - Player C measures register C in basis
  $$M_C^\theta := \{|\gamma_1^\theta\rangle, \dots, |\gamma_\ell^\theta\rangle\}$$
  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 $\Big(|\ \psi\rangle_{ABC}, \big(M_B^\theta, M_C^\theta\big)_{\theta\in\{0,1\}}, f, g\Big)$. 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 $|x\rangle$, $\langle x|M|x\rangle \geq 0$ ($\iff$ 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 $\langle u|v\rangle = |u\rangle^\dagger\,|v\rangle = \langle u|\cdot|v\rangle$.

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

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

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 $B^\theta_y = \sum\limits_{b, f(\theta,b)=y} |\,\beta^\theta_b\rangle\langle\beta^\theta_b\,|$ and $C^\theta_z = \sum\limits_{c, g(\theta,c)=z} |\,\gamma^\theta_c\rangle\langle\gamma^\theta_c\,|$.
It follows that
$\Pi_\theta = \sum\limits_x |\,x^\theta\rangle\langle x^\theta\,| \otimes B^\theta_x \otimes C^\theta_x$ is an orthogonal projector.
Recall that $\mathbb{E}_\theta\Pi_\theta = \frac{1}{2}\left(\Pi_0 + \Pi_1\right)$.

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:

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

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

But note that, for permutation matrix P:

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

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

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

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

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

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

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.