Quantum Money Schemes and Attacks

Course Project

Sudhansh Peddabomma

under the supervision of Qipeng Liu
University of California San Diego

December 2023

Contents

1 Introduction

The current system for money is versatile and convenient but issues such as data leaks, counterfeits and frauds are still commonplace in many regions of the world. In the current system, we have two kinds of money

- Physical money - This form of money includes coins, notes, precious metals, etc. These media of money can easily be verified for validity, but they can be counterfeited.
- Virtual Money - The kind of money accessible through bank accounts and credit lines. These systems rely on a third-party (the bank) for transactions. The transactions are sometimes not private - when the statements are leaked.

We ideally want a form of money that cannot be counterfeited and can be spent without leaving a trace. Such a system is not possible with digital money because any information passed through classical communication channels can be copied, making it infeasible for any such kind of system.

Quantum systems, unlike their classical counterparts possess unique properties, and present a promising avenue to develop monetary schemes. Due to the laws of physics, it is impossible to clone a given quantum state as results of the **No-cloning theorem**. Wiesner [1] proposed quantum money as one of the first applications of this property. Despite numerous attempts to refine quantum money schemes, Wiesner's original proposal remains widely adopted due to its efficiency and simplicity.

Most of the schemes, including that of Wiesner's, are based on a *secret-key* architecture, wherein only the issuing authority or the bank can verify a given quantum note. As a result, every transaction has to be verified by the bank making the system inefficient. Furthermore, many of these schemes are proven not be secure. Such attacks, as discussed in later sections, leverage quantum properties to prepare counterfeit notes.

Ideally, we require a *public-key* system, where any user can use a public-key to verify a given quantum note. However, these schemes are difficult to formulate, and there is a very small number of such schemes.

Quantum Lightning, proposed by Mark Zhandry et al. [2], is a famous approach for public-key quantum money. While initially regarded as a promising public-key quantum money approach, recent research [3] has identified vulnerabilities challenging its fundamental assumptions.

In this report, we delve into the landscape of quantum money, exploring its potential and addressing the challenges faced by existing schemes. We analyze the security implications and advancements in the field, with a focus on both secret-key and public-key architectures.

2 Background

2.1 Quantum computing

Before we delve into the protocols, let us summarise some fundamentals from quantum mechanics. Quantum mechanical systems store information in a very different way as compared to classical or non-quantum systems - the act of measuring a quantum state changes the state itself.

Definition 1 (Qubit)**.** *A qubit is mathematically described as*

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$, and the states $|0\rangle, |1\rangle$ form a basis for the 2D vector space.

In such a state, the probability of obtaining 0 upon measuring the qubit is given by $|\alpha|^2$. Simply put, the coefficients associated with the basis states represents the probability of obtaining that particular basis state in the output.

Definition 2 (n-qubit system)**.** *In general, an n-qubit quantum state is of the form*

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x\,|x\rangle \tag{1}$$

where $\alpha_x \in \mathbb{C}$ *and* $\sum_{x\in\{0,1\}^n} \|\alpha_x\|^2 = 1$.

Similarly, we can generalise the notion of measurement to a general state basis using **Born's rule**.

Definition 3 (Born's Rule)**.** *A quantum state* $|\phi\rangle$ *measured under the basis* $|\phi_i\rangle$ *yields the classical output i, with probability* $\|\langle\phi_i|\phi\rangle\|^2$ *and the quantum state collapses to* $|\phi_i\rangle$

Qubits, unlike classical bits, cannot be copied. There are well-established theoretical results for approximate cloning of qubits - these allow us to design cryptographic protocols beyond classical computers. One famous example for such a result is quantum-key distribution.

Technically, we can clone qubits under certain conditions - we can always generate basis states like $|0\rangle, |1\rangle$. Therefore, we cannot use the no-cloning theorem directly for quantum money. We need a design scheme that is cryptographically secure, and such schemes are discussed below.

2.2 Mixed States

The state of the form $|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x\,|x\rangle$ is called a pure state.

Definition 4 (Mixed States)**.** *Consider an n-qubit quantum state of the form*

$$\rho = \begin{cases} |\phi_1\rangle & \text{with probability } p_1 \\ |\phi_2\rangle & \text{with probability } p_2 \\ \vdots & \\ |\phi_m\rangle & \text{with probability } p_m \end{cases} \tag{2}$$

where for $i \in [m]$, $|\phi_i\rangle$ is an n-qubit pure/mixed state, $p_i \geq 0$ and $p_1 + p_2 + \cdots + p_m = 1$

The mathematical notation for the density matrix ρ is given by

$$\rho = \sum_{i \in [m]} p_i \, |\phi_i\rangle\langle\phi_i| \tag{3}$$

The notion of measurement for mixed states is generalised by the following

Definition 5 (Projective Measurements)**.** *When ρ is measured under a projective measurement P_{ii} with $\sum_i P_i = \mathbb{I}$ and $P_i^2 = P_i$, we see the outcome i with probability $p_i = \mathrm{Tr}[P_i \rho]$ and the state collapses to $\frac{P_i \rho P_i}{\mathrm{Tr}[P_i \rho P_i]}$*

2.3 Elitzur-Vaidman bomb Testing

The goal of the Elitzur-Vaidman Bomb Testing is to test whether a "quantum bomb" system is a dud or an actual bomb. We can interact with the system using an input state $|\phi\rangle$. The output state remains $|0\rangle$ if there is no bomb. On the other hand, in presence of a bomb, if the output state flips to $|1\rangle$ (based on Born's rule) it explodes.

There is a safe algorithm to test whether the system is a dud or a bomb, without triggering it, based on the Zeno effect [4]. It is a prime example of measuring a property of a system without disturbing it. The algorithm is a probabilistic test that can certify a property of an object, by measuring another system that has not interacted with the object.

The testing procedure chooses a large N and a small angle $\delta = \frac{\pi}{2N}$. It uses two registers (probe and the system). Start with a the system state $|\phi\rangle = |0\rangle$ -

1. Prepare an augmented state with *ancillary probe qubit*, starting with $|0\rangle$.
2. Rotate the probe by a small angle δ.
3. Apply `CNOT` to couple the probe and the system qubit
4. Send the system qubit into the system, and obtain the collapsed state after measurement (if no explosion)

After N iterations, the probe qubit will output 1 with certainty when there is a bomb. It can be shown that the probability of explosion with the algorithm is of the order $O(1/N)$.

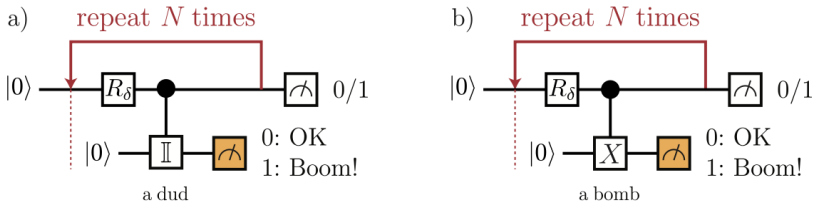

Figure 1: Visualization of the EVD Bomb Testing

2.4 Protective Measurements

The concept of protective measurement was proposed by Aharnov et al. in [5] to measure a wave-function without changing its properties appreciably when the measurement is being made.

It involves measuring the expectation value of a dichotomic observable A, to gauge the properties of the system

Definition 6 (Dichotomic Observable)**.** *A dichotomic observable A is an operator with eigenvalues ± 1 defined by*

$$A = P - P^{\perp} \tag{4}$$

where P is a projector on its $+1$ eigenspace

Given an unknown state $|\alpha\rangle \in \mathbb{C}^d$, and an access to a two outcome von Neumann measurement $\{\Pi = |\alpha\rangle\langle\alpha|, \mathbb{I} - \Pi\}$, the protocol for protective measurement has running time N, accuracy ϵ, and a failure probability f, when

- The protocol uses at most N calls to the projective measurement
- The probability that all outcomes are Π is at least $1 - f$

That is, we prepare a probe state $|\phi\rangle|\alpha\rangle$ and map it to $\left[e^{-ic\langle A\rangle\sigma_x}|\phi\rangle + \mathcal{O}(\epsilon)|\phi'\rangle\right]|\alpha\rangle$ for an appropriate constant c for an error state $|\phi'\rangle$ after N steps.

The idea is to then use the classical information $\langle A\rangle$ to measure α. For example, we can measure the expected value of the Pauli matrices on α using this procedure, and accurately reconstruct the required state.

3 Quantum Money

A quantum money scheme is characterized by two functions

- A token generation procedure $\texttt{TokenGen}(1^\lambda)$ that generates a serial number S and a quantum money state $|\$\rangle$. The serial number is kept *secret*

with the bank, and the quantum banknotes are shared with the customers.

- The verification procedure $\texttt{Ver}(S, |\$\rangle)$ outputs 0 if the banknote is valid and 1 if invalid. The bank can either choose to return the resulting state after verification (if the verification does not invalidate the note) or issue a new note to the user. The procedure should be successful with a *very high probability* for a correct input state.

We consider two categories of quantum money

- Private key quantum money
- Public key quantum money

3.1 Private-key quantum money

In such schemes, only the issuing authority can verify a quantum money state. They maintain a database of secret keys for each quantum bill issued, and verify the input quantum state with that key. Stephen Wiesner proposed one of the first frameworks in this category in 1969 [1] (but published in 1983). In these frameworks, each quantum bill is a unique random quantum state, which the issuing authority labels with a serial number.

Formally, a quantum bank note is defined as n-qubit quantum state, where each of the qubit is randomly drawn from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Each such state is associated with a serial number which the issuing authority keeps note of. During a transaction, the quantum bill is sent to the mint where the bill is matched against the corresponding serial number and verified. It can be shown that the probability of cloning these bills can be bounded by 0.85^n. However, the main bottleneck in this protocol is that every transaction must be conveyed to the bank/issuing authority.

In a follow-up paper by Bennet et al. [6], a fixed *psuedo-random* function was proposed to choose the secret keys for all the serial numbers, avoiding the growth of the secret-key table with the number of notes issued. The next scheme in this category was suggested by Tokunaga et al. in 2003. However, in this scheme, the bank has to destroy all the issued bills once it detects a counterfeit note which limits its practical applicability.

3.2 Public-key quantum money

These schemes are the desired ideal money form, where any user can verify the authenticity of a quantum money state. Bennett et al. proposed such a scheme in 1982 [6] wherein a quantum money is essentially a token which can only be used once. However, this scheme can be easily broken by a quantum computer that can run *Shor's algorithm* [7].

Mosca and Stebila [8] proposed using the same quantum states for the same denomination. They used the *complexity-theoretic no-cloning theorem* proved by Aaronson [9] (which basically limits the cloning ability through computational power), but they did not give a concrete implementation for such a scheme.

The difficulty of developing public-key quantum money lies in the designing the verification algorithm. Typically, in schemes like Weisner coding, the counterfeiter can repeatedly query the bank's verification scheme to duplicate a note with high probability of not getting caught (discussed later). However, this can be prevented if the bank returns a new note after verification and a *strict testing* regime, where no bank note is returned on failed verification.

3.3 Wiesner's Quantum Money Scheme

Consider $X \in \{0,1\}$ and $\theta \in \{0,1\}$. Then, a *single qubit Weisner state* is defined as

$$|X^\theta\rangle = \begin{cases} |0\rangle \text{ or } |1\rangle, & \theta = 0 \\ |+\rangle \text{ or } |-\rangle, & \theta = 1 \end{cases} \tag{5}$$

$$= H^\theta |X\rangle \tag{6}$$

where $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + |1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - |1\rangle$. This can easily be extended to n-qubit systems as $|X^\theta\rangle = |X_1^{\theta_1}\rangle |X_2^{\theta_2}\rangle \dots$.

Using the above framework, Wiesner Quantum Money scheme is then defined as the following

Definition 7 (Wiesner's Quantum Money Scheme)**.** *The scheme is characterized by two functions* $\texttt{TokenGen}(1^\lambda)$ *and* $\texttt{Ver}(S, |\$\rangle)$

- *The token generation procedure* $\texttt{TokenGen}(1^n)$ *generates a serial number S and and a quantum money state* $|\$\rangle$ *defined by*

$$S = f(x_1, x_2, \dots, x_n, \theta_1, \theta_2, \dots, \theta_n) \tag{7}$$

$$|\$\rangle = |x_1^{\theta_1}\rangle |x_2^{\theta_2}\rangle \dots |x_n^{\theta_n}\rangle \tag{8}$$

- *The verification procedure* $\texttt{Ver}(S, |\$'\rangle)$ *outputs* 0 *if the banknote is valid and* 1 *if invalid using the following projective measurement* $P = \{P_0 = |\$\rangle\langle\$|, \mathbb{I} - P_0\}$

We shall discuss the adaptive attacks as described in [10] on the Wiesner Quantum money scheme.

3.4 Quantum Lightning

Quantum Lightning was proposed by Zhandry [2] as a public-key quantum money scheme. The lightning bolt refers to a superposition that can be sampled efficiently, but not duplicated. Anyone can generate a random lightning

bolt, and a verifier can check that the bolt was generated honestly. The idea is to develop a sampling procedure that makes it difficult to generate same lightning bolts as seen by a verifier.

The authors use a collision-resistant hash function, f_A, and the bolt is defined as a superposition over the pre-image of some value output by f_A. That is, for some output $|y\rangle$ in the hash function range, the lightning bolt is a superposition of all states $|x\rangle$ for x in the domain of f_A such that $f_A(x) = y$.

To generate a random bolt, we use the following procedure

1. Create a superposition over the domain of f_A, and apply the unitary corresponding to f_A to the superposition
2. The output of the unitary is stored in a separate register entangled with the original superposition. We measure the output register, which collapses to a single random eigenstate $|y\rangle$. The has y constitutes as the serial number for the bank note.

   Since the two registers were entangled, the first register becomes a uniform superposition over the pre-image of y. The first register's state is the bolt or the required quantum bill.

Now, since the hash function is collision-resistant, the bolt is unclonable. If we can generate the same bolts with different serial numbers, then that would imply a collision in the hash function raising a contradiction. The formal definition of the quantum lightning scheme involves more intricate constructions by tensoring multiple *mini-bolts*. However, for our analysis we shall consider the simple scheme described above.

3.5 General Public Money Scheme

In particular, we shall consider a generic quantum money scheme described as follows - Consider a randomly chosen subspace $A \subseteq \mathbb{F}_2^n$, where $\dim(A) = n/2$.

Each quantum money state is a uniform superposition of the vectors in A. We denote this superposition by

$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_a |a\rangle .$$

Also, we know that

$$H^{\otimes n} |A\rangle = |A^\perp\rangle$$

where $\dim(|A^\perp\rangle) = n - \dim(A) = \frac{n}{2}$.

Them the quantum money scheme is constructed as follows:

1. Pick $A \subseteq \mathbb{F}^\lambda$ such that $\dim(A) = \lambda/2$.

2. TokenGen(1^λ) generates $pk, |\$\rangle$ such that

$$pk = \{P_0 = |A\rangle\langle A|, P_1 = I - |A\rangle\langle A|\}, |\$\rangle = |A\rangle.$$

3. The verification procedure can be implemented via membership oracles for A and $A^\perp$. These are implemented in the form of unitary operators U_A and $U_{A^\perp}$ that are applied on augmented qubits. We do the following:
   (a) Given a quantum state $|\phi\rangle = \sum_{v\in\mathbb{Z}_2^n} \alpha_v |v\rangle$.
   (b) Run U_A on $|\phi\rangle|0\rangle$ and measure the second qubit to obtain $|\phi'\rangle$, b'.
   (c) Run $H^{\otimes n} \cdot U_A^\perp \cdot H^{\otimes n}$ on $|\phi'\rangle|0\rangle$ and measure the second qubit to obtain $|\phi''\rangle$, b''.
   (d) When $b' = b'' = 0$, $|\phi''\rangle$ must be equal to $|A\rangle$.

The intuition behind this scheme is that the quantum money state is essentially a randomly chosen subspace of dimension $n/2$ from the complete space of dimension n. Doing so would yield us a large number of possible quantum bills of the order $\binom{n}{n/2}$. The attacker has to correctly guess the subspace in order to forge a counterfeit note.

We shall analyse the soundness of this general scheme in the later sections.

4 Bomb-testing Adaptive Attack

The bomb testing algorithm described in the previous sections can be modified, to successfully break the Wiesner Quantum Money scheme. In particular, we can successfully determine if the state is $|+\rangle$ or not. We first consider the simple case where only one Wiesner qubit is used -

The algorithm is summarized as follows -

1. Prepare $|0\rangle|\phi\rangle$.
2. Apply R_θ on the first qubit. That is, we obtain $|\phi'\rangle = R_\theta|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, where $\theta = \frac{\pi}{2N}$.
3. Apply `CNOT` to $|\phi'\rangle$ to obtain $|\phi''\rangle$. We also define $\psi_\theta = \cos\theta|0\rangle + \sin\theta|1\rangle$.
4. Verify the second qubit of $|\phi''\rangle$.
5. Repeat the procedure for N steps.

It can be shown that the bank's probability of detecting a counterfeit is at most $O(1/N)$ when the bank note is $|0\rangle, |1\rangle$. When the bank note is $|+\rangle$, the measurement of the probe qubit will yield 1 with certainty. Otherwise, the

outcome will be 0. The scheme can be extended to an n-state system wherein the quantum bill given by

$$|q\rangle = |q_1\rangle |q_2\rangle \dots |q_n\rangle$$

where each $|q_i\rangle$ is $|H^\theta X\rangle$ for $X, \theta \in \{0, 1\}$. The counterfeiter prepares the following state keeping $|q_1\rangle$ aside -

$$|q^{(1)}\rangle = |\psi\rangle |q_2\rangle \dots |q_n\rangle$$

where ψ is the modified Wiesner bit that is coupled with a probe qubit. Each of the individual Wiesner states can be determined, changing each qubit one after the other.

4.1 Further Generalization

We consider a more general Wiesner's scheme in which we use d dimensional qubits. We choose n random states from $\{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_r\rangle\}$, where each $|\beta_i\rangle \in \mathcal{C}^d$. Let $\theta_{min} = \min_{1 \le i \ne j \le r} \arccos |\langle \beta_i | \beta_j \rangle|$. For example, in the previous scheme, the set of random states is $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ with $\theta_{min} = \pi/4$.

In the previous attack, we essentially found an operator R such that $R|+\rangle = |+\rangle$ and not for the other states. In a similar way, given a generate state $|alpha\rangle$ from a set of arbitrary quantum states, we aim to find a unitary R such that $R|\alpha\rangle = |\alpha\rangle$. One such potential operator is to use the *controlled reflection* $R = 2|\alpha\rangle\langle\alpha| - \mathbb{I}$ instead of the controlled X as before.

Assuming we know the set of arbitrary states $\{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_r\rangle\}$, the idea is to select a $|\beta\rangle$ from the set, and check if the unknown state $|\alpha\rangle$ is same as our chosen state. The procedure can be repeated for all the available quantum states to identify the unknown state. The operator R behaves in the following manner

$$R|\alpha\rangle = \cos(2\theta)|\alpha\rangle + \sin(2\theta)|\alpha^\perp\rangle \tag{9}$$

where $\cos\theta = \langle\alpha|\beta\rangle$

The algorithm is summarized as

1. Prepare a probe qubit $|0\rangle$.
2. At the kth step, the state of the probe qubit is given by $|\phi_k\rangle$. We apply a rotation R_δ to the probe qubit to obtain $|\psi_{(\phi_k+\delta)}\rangle = \cos(\phi_k + \delta)|0\rangle + \sin(\phi_k + \delta)|1\rangle$ where $\delta = \frac{\pi}{2N}$.

3. The probe and the unknown qubit are coupled. The controlled R operator defined as

$$C_R = \cos(\phi_k + \delta) |0\rangle |\alpha\rangle + \sin(\phi_k + \delta) \cos(2\theta) |1\rangle |\alpha\rangle \quad (10)$$
$$+ \sin(\phi_k + \delta) \sin(2\theta) |1\rangle |\alpha^{\perp}\rangle \quad (11)$$

   The operator C_R is applied on the joint state.

4. The second register is measured and the procedure is repeated for N steps.

The probability of getting caught in the kth round can be calculated as $\sin^2(2\theta) \sin^2(\phi_k + \delta)$, and after successful verification, the (unnormalized) residual state is

$$(\cos(\phi_k + \delta) |0\rangle + \cos(2\theta) \sin(\phi_k + \delta) |1\rangle) |\alpha\rangle \quad (12)$$
$$= |\phi_{k+1}\rangle |\alpha\rangle \quad (13)$$

The transformation can be represented as

$$|\phi_{k+1}\rangle = \begin{bmatrix} 1 & 0 \\ 0 & \cos(2\theta) \end{bmatrix} R_\delta |\phi_k\rangle \quad (14)$$
$$= \begin{bmatrix} \cos\delta & -\sin\delta \\ q\sin\delta & q\cos\delta \end{bmatrix} |\phi_k\rangle = T |\phi_k\rangle \quad (15)$$

where $q = \cos(2\theta)$. At the end of N steps, we have $T^N |0\rangle$. Consider the following cases

1. Our guess is correct, i.e, $\theta = 0$. Then, $q = 0$, $T = R_\delta$, and $\langle 1|T^N|0\rangle = 1$, and the probe qubit is rotated to $|1\rangle$. We never get caught in this case.
2. Our guess is perpendicular to the unknown state, i.e, $\theta = \pi/2$. Then, $q = -1$ and $T^2 = \mathbb{I}$. Hence, after an even number of rounds $\langle 0|T^N|0\rangle = 1$, and we are never caught.
3. When our guess makes an arbitrary angle with the unknown state, i.e, $\theta_{min} \leq \theta < \pi/2$. Then, $\|q\| < 1$. For large N, we have

$$T = \begin{bmatrix} 1 & -\delta \\ q\delta & q \end{bmatrix} + \Delta T \quad (16)$$

with $\|\Delta T\| = O(\delta^2)$. Now,

$$\begin{aligned} T^N |0\rangle = T^N \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= T^{N-1} \begin{bmatrix} 1 \\ \delta q \end{bmatrix} + \underbrace{T^{N-1} \Delta T \begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{|v_1\rangle} \\ &= T^{N-2} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \underbrace{T^{N-2} \left(\begin{bmatrix} -\delta^2 q \\ 0 \end{bmatrix} + \Delta T \begin{bmatrix} 1 \\ \delta q \end{bmatrix} \right)}_{|v_2\rangle} + |v_1\rangle \\ &\vdots \\ &= \begin{bmatrix} 1 \\ \delta(q + q^2 + \cdots + q^N) \end{bmatrix} + \sum_{i \in [N]} |v_i\rangle \end{aligned}$$

The norms of the error vectors $|v_i\rangle$ can be bounded as

$$|v_k\rangle = T^{N-k} \left(\begin{bmatrix} -\delta(q + q^2 + \cdots + q^{k-1}) \\ 0 \end{bmatrix} + \Delta T \begin{bmatrix} 1 \\ \delta(q + q^2 + \cdots + q^{k-1}) \end{bmatrix} \right)$$

$$\| |v_k\rangle \| \leq \mathcal{O}\left(\delta \left(1 + q + \cdots + q^{k-1} \right) \right) \leq \mathcal{O}\left(\frac{\delta^2}{1-q} \right)$$

because $\|T\| \leq 1$ from 15. We then have,

$$\langle 0|T^N|0\rangle \geq 1 - N \| |v_N\rangle \| \geq 1 - \mathcal{O}\left(\frac{N\delta^2}{1-q} \right) \geq 1 - \mathcal{O}(N^{-1}\theta_{min}^{-2}) \quad (17)$$

using $1 - q = \Omega(\theta^2)$ for small θ

In conclusion, we can choose an N of the order $f^{-1}\theta_{min}^{-2}$ to get $\|\langle 0|T^N|0\rangle\|^2 > 1 - f$. Now, since we repeat this over all the r quantum states from the set, and we need to identify all the n qubits, the complexity of the algorithm becomes $\mathcal{O}(r^2 n^2 f^{-1}\theta_{min}^{-2})$. The square on rn appears because the failure probability for each procedure needs to be modified as $f' = f/nr$ to bound the total failure probability of the procedure.

Furthermore, we can parallelise the procedure, wherein we attach the probe qubits to all of the n states simulataneously and query the verification procedure. The failure probability does not increase because the verification in this scheme is done on each qubit independently. Therefore, the final runtime complexity of the algorithm reduces to $\mathcal{O}(r^2 n f^{-1}\theta_{min}^{-2})$

When θ_{min} is arbitrarily close to 0, i.e, the states are continuous, the attack described above fails. In this case, the attacker has to arbitrarily choose a θ_{min} to proceed with the attack. Simply put, since there is no true bound on the

value of $\theta_{\min}$, we cannot find the number of iterations. Our best bet is to guess a value, and check if that works.

Doing so, will add a new case in the above description, where $0 < \theta < \theta_{min}$. If we repeat the above procedure for an arbitrary number of steps, the *cumulative probability* of failure increases.

To understand this intuitively, θ_{min} gave us the approximate upper bound on how much the probe qubit rotates. If the θ_{min} is close to θ, then we can find an approximate N such that the probe qubit rotates by $\pi/2$ at the end of N rounds. However, if we there is no correlation between θ_{min} and θ, which is the case when the states are continuous and we take a guess, the probe qubit rotates by an arbitrary amount at the end of N steps. Moreover, if the probe qubit is very close to $|1\rangle$ during the procedure, the coupling between probe and system state becomes strong, and the operation R is applied on the system qubit with a very high probability. The state $R|\beta\rangle$ has a high chance of failing the verification protocol as we cycle through all the possible states.

In the next section, we shall see an attack based on protective measurements which is able to tackle this case.

5 Protective Measurement Attack

The idea of a protective measurement attack is similar. We define an operator A, and find its expectation value $\langle A \rangle = \langle \psi | A | \psi \rangle$ on the state $|\psi\rangle$. The classical information can then be used to reconstruct $|\phi\rangle$ accurately.

The gist of the attack is as follows - we prepare a probe with the initial state $|0\rangle$, choose $\delta = \frac{c}{N}$ for some constant c, and repeat the following procedure for N steps -

- Weakly couple the probe and the system
- Send the state to the bank for validation

We expect the following -

$$|0\rangle |\psi\rangle \xrightarrow{e^{-i\delta(\sigma_x A)}} \approx |0\rangle |\psi\rangle - i\delta |1\rangle A |\psi\rangle \tag{18}$$

$$\xrightarrow{\text{bank measures}\{|\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi|\}} \approx \left(e^{-i\delta A \sigma_x} |0\rangle\right) |\psi\rangle \tag{19}$$

$$\xrightarrow{\text{repeat } N \text{ times}} \approx \left(e^{-iN\delta A \sigma_x} |0\rangle\right) |\psi\rangle \tag{20}$$

By measuring the probe, we can approximate A and thus $|\psi\rangle$.

5.1 Construction

The building block of this attack is to ensure *weak interaction* between the probe and the system. As mentioned in Section 2.4, we use a dichotomic observable $A = P - P^{\perp}$ where P is the projection on the $+1$ eigenspace of A.

The crucial difference from the approaches in is that, instead of applying δ rotation and a controlled operator, we use the unitary coupling operation defined as

$$U = e^{-i\delta(\sigma_x \otimes A)} = e^{-i\delta(\sigma_x \otimes P - \sigma_x \otimes P^{\perp})} \tag{21}$$

$$= e^{-i\delta\sigma_x \otimes P} e^{i\delta\sigma_x \otimes P^{\perp}} = e^{-i\delta\sigma_x} \otimes P + e^{i\delta\sigma_x} \otimes P^{\perp} \tag{22}$$

As before, we assume the first part of the system is the probe followed by the unknown state to the right of the tensor product. We choose $\delta = \frac{c}{N}$ for an appropriate value of c. Here, if the probe state is close to 1, the unknown state is not affected in a significant manner unlike before.

5.2 Obtaining the expectation value of A

We have the following lemma,

Lemma 1. *For any dichotomic observable A there exists a protective measurement protocol with running time N, accuracy $\mathcal{O}(1/N)$ and failure probability $\mathcal{O}(1/N)$*

Proof. Consider an arbitrary initial state of the probe qubit $|\phi_0\rangle$. After k steps, we obtain $|\phi\rangle$ and $|\alpha\rangle$ on the second register assuming we did not fail in the k rounds.

At the $k+1$th step, on applying U, we get

$$W|\phi_k\rangle = (\mathbb{I}\otimes\langle\alpha|)U|\phi_k\rangle|\alpha\rangle = \sqrt{p_k}|\phi_{k+1}\rangle \tag{23}$$

where p_k represents the probability of success in the kth step.

The expression for W is given by

$$\begin{aligned} W &= \langle\alpha|P|\alpha\rangle e^{-i\delta\sigma_x} + \langle\alpha|P^\perp|\alpha\rangle e^{i\delta\sigma_x} \\ &= \cos\delta\langle\alpha|P+P^\perp|\alpha\rangle\mathbb{I} - i\sin\delta\langle\alpha|P-P^\perp|\alpha\rangle\sigma_x \\ &= \cos\delta\mathbb{I} - i\sin\delta\langle A\rangle\sigma_x \qquad (24) \\ & \qquad (25) \end{aligned}$$

The matrix W has the eigenvalues $\lambda_\mp = \cos\delta \mp i\langle A\rangle\sin\delta$ corresponding to eigenstates $|+\rangle, |-\rangle$. Then,

$$W^N|\phi_0\rangle = \left(\prod_{k=0}^{N-1}\sqrt{p_k}\right) = \sqrt{p}|\phi_N\rangle \tag{26}$$

where p is the probability of succeeding in all the N validation steps. For large N,

Therefore, for large N,

$$\begin{aligned} W^N &= \lambda_1^N|+\rangle\langle+| + \lambda_2^N|-\rangle\langle-| \\ &= (e^{-ic\langle A\rangle}|+\rangle\langle+|\,(e^{ic\langle A\rangle}|-\rangle\langle-| + O(1/N)(|+\rangle\langle+| + |-\rangle\langle-|) \\ &= \cos(c\langle A\rangle)(|+\rangle\langle+| + |-\rangle\langle-|) - \sin(c\langle A\rangle)(|+\rangle\langle+| - |-\rangle\langle-|) + O(1/N)\mathbb{I} \\ &= \cos(c\langle A\rangle)\mathbb{I} - \sin(c\langle A\rangle)\sigma_x + O(1/N)\mathbb{I} \\ W^N &= e^{-ic\langle A\rangle\sigma_x} + \mathcal{O}(1/N) \end{aligned}$$

At the end of N steps, the probe gets rotated by an amount proportional to $\langle A\rangle$. The final state can be written as

$$|\phi_N\rangle = e^{-ic\langle A\rangle\sigma_x}|\phi_0\rangle + \mathcal{O}(1/N)|\phi'\rangle \tag{27}$$

for some error state $|\phi'\rangle$. The value of p can then be estimated as $1-\mathcal{O}(1/N)$. □

To understand this better, consider the Wiesner states $|X^\theta\rangle$ - We choose $A = \sigma_x$, $c = \frac{\pi}{2}$, $|\phi_0\rangle = |0\rangle$. Then, we get $\langle 0|\sigma_x|0\rangle = \langle 1|\sigma_x|1\rangle = 0$ and $\langle +|\sigma_x|+\rangle = -\langle -|\sigma_x|-\rangle = 1$. The final probe state when the unknown state is initially $|+\rangle$ or $|-\rangle$ is $W^N|0\rangle = \mp i|1\rangle$. Otherwise, the probe will remain close to $|0\rangle$. Therefore, we can compute θ with certainty, which can then be used to find X as well.

In a general case, we generate many copies of $|\phi_N\rangle$ and measure it in σ_y basis to get the estimate of $\langle A\rangle$. The result is formally stated in the following lemma.

Lemma 2. *For any $\nu, \eta, f > 0$, it is possible to use a protective measurement protocol to estimate $\langle A\rangle$ with precision at least ν, confidence at least $1-\eta$, probability of failure $\mathcal{O}(f)$ and running time $\mathcal{O}(f^{-1}\nu^{-4}\ln^2(\eta^{-1}))$*

Proof. We run the above mentioned protocol for $m = 336\ln(2\eta^{-1})\nu^{-2}$ times with $N = m/f$. The total running time for this procedure is $mN = \mathcal{O}(\ln^2(\eta^{-1})\nu^{-4}f^{-1})$, and the overall failure probability is $\mathcal{O}(f)$. We set the parameter $c = \frac{\pi}{8}$ for optimality, and obtain m copies of $|\phi_N\rangle$

$$\phi_N = \cos\left(\frac{\pi}{8}\langle A\rangle\right)|0\rangle - i\sin\left(\frac{\pi}{8}\langle A\rangle\right)|1\rangle + \mathcal{O}\left(\frac{1}{N}\right)|\phi'\rangle \tag{28}$$

We measure this state in $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ basis m times. Considering $|y_+\rangle = \frac{1}{\sqrt{2}}[|0\rangle - i|1\rangle]$, let $\bar{p}$ be the probability of obtaining $+1$ as the measurement outcome and $p^{(m)}$ be the empirical frequency of $+1$. Then,

$$\begin{aligned}\bar{p} = \|\langle y_+|\phi_N\rangle\|^2 &= \frac{1}{2}\|\cos\left(\frac{\pi}{8}\langle A\rangle\right) - \sin\left(\frac{\pi}{8}\langle A\rangle\right) + \mathcal{O}\left(\frac{1}{N}\right)\|^2 \\ &= \frac{1}{2}\left(1 - \sin\left(\frac{\pi}{4}\langle A\rangle\right) + \mathcal{O}\left(\frac{1}{N}\right)\right)\end{aligned}$$

Since $\|\langle A\rangle\| \leq 1$, the expectation value $\bar{p}$ is well bounded away from 0 -

$$\bar{p} \geq \frac{1}{2} - \frac{1}{\sqrt{8}} + \mathcal{O}\left(\frac{1}{N}\right) \geq \frac{1}{7} \tag{29}$$

Let $\tilde{\nu} = \nu/4$, then

$$m = \frac{336\ln(2/\eta)}{\nu^2} \geq \frac{3\ln(2/\eta)}{\tilde{n}u^2\bar{p}} \tag{30}$$

Using Chernoff bound, the probability that $\|p^{(m)} - \bar{p}\| \geq \tilde{\nu}\bar{p}$ is at most

$$2\exp\left(-\frac{\tilde{v}^2 m\bar{p}}{3}\right) \leq \eta \tag{31}$$

The above result establishes that $p^{(m)}$ is within $\nu/4\bar{p} \leq \nu/4$ of $\bar{p}$. Using the expression from 29, we get

$$\arcsin\left(1-2p^{(m)}-\frac{\nu}{2}-\mathcal{O}\left(\frac{1}{N}\right)\right) \leq \frac{\pi}{4}\langle A\rangle \leq \arcsin\left(1-2p^{(m)}-\frac{\nu}{2}+\mathcal{O}\left(\frac{1}{N}\right)\right) \tag{32}$$

The precision of $\langle A\rangle$ can be analysed using the Taylor series expansion. We obtain the result

$$\left|\langle A\rangle - \frac{1}{\pi}\arcsin\left(1-2p^{(m)}\right)\right| \leq \nu \tag{33}$$

Therefore, the value of $\langle A\rangle$ is estimated as $\frac{4}{\pi}\arcsin\left(1-2p^{(m)}\right)$ with precision ν and confidence $1-\eta$. □

5.3 Obtaining $|\alpha\rangle$ from $\langle A\rangle$

The quantum state $|\alpha\rangle$ is obtained from $\langle A\rangle$ using Protective Tomography.

Definition 8 (Protective Tomography)**.** *A protocol achieves protective tomography with infidelity ϵ, confidence $1-\eta$, failure probability f and running time t if it outputs a classical description of a mixed state ρ such that*

- *The probability of failure (the output is $\mathbb{I}-\Pi$ for some step), is $\mathcal{O}(f)$*
- *If the algorithm does not fail, the fidelity $F(|\alpha\rangle, \rho) \geq 1-\epsilon$ with probability atleast $1-\eta$*
- *The algorithm uses at most t validations*

We have the following lemmas

Lemma 3. *There exists a protective tomography protocol for a qubit system with dimension d and running time scaling as $t = \mathcal{O}(d^{12}f^{-1}\epsilon^{-4}\ln^2(d^2\eta^{-1}))$.*

Lemma 4. *There exists a protective tomography protocol for n-qubit states of the form $|\alpha\rangle = \otimes_{i\in[n]}|\alpha_i\rangle$, with running time $t = \mathcal{O}(n^5 f^{-1}\epsilon^{-4}\ln^2(n\eta^{-1}))$.*

Proof. Using the procedure described above, we can obtain $\langle\tilde{\sigma}_j\rangle$ for $j \in \{x,y,z\}$ - the approximated values of the Pauli matrices $\langle\sigma_j\rangle = \langle\alpha|\sigma_j|\alpha\rangle$, with precision parameters $\nu = \epsilon/6, \tilde{\eta} = \eta/3, \tilde{f} = f/3$. The running time for all the algorithms would then be

$$t = 3\mathcal{O}(\tilde{f}^{-1}\tilde{\nu}^{-4}\ln^2(\tilde{\eta}^{-1})) \tag{34}$$

$$= \mathcal{O}(f^{-1}\nu^{-4}\ln^2(\eta^{-1}) \tag{35}$$

and the failure probability $f = 3\tilde{f}$ using the union bound. Similarly, the confidence bound can also be obtained as $1 - \nu$. The approximation of $|\alpha\rangle$ is given by

$$\tilde{\rho} = \mathbb{I}/2 + \sum_{j \in \{x,y,z\}} \langle \tilde{\sigma}_j \rangle \sigma_j \tag{36}$$

with fidelity at least $1 - \epsilon$ and confidence at least $1 - \eta$.

However, this matrix is not necessarily positive semi-definite with trace 1. Therefore, we choose ρ to be the closest state that is $\rho = \text{argmin}\, D(\tilde{\rho}, \tau)$, where τ runs over all single-qubit mixed states and D is the trace distance $D(\alpha, \beta) = \frac{1}{2}||\alpha - \beta||_{\text{tr}}$ and $||A||_{\text{tr}} = \text{Tr}(\sqrt{AA^\dagger})$. Using the triangle inequality and the definition of ρ, we get

$$D(\rho, |\alpha\rangle\langle\alpha|) \leq D(\rho, \tilde{\rho}) + D(\tilde{\rho}, |\alpha\rangle\langle\alpha|) \leq 2D(\tilde{\rho}, |\alpha\rangle\langle\alpha|) \tag{37}$$

Then the fidelity of the final state is ϵ with probability at least $1 - \eta$. □

6 Duplication in Public-key money

6.1 Soundness Analysis

Let us analyse what happens to the verification procedure when we use a forged state. Suppose the true state is sampled from the subspace A with dimension $n/2$. Let the unknown state be $|\alpha\rangle = \sum_{v \in A} \alpha_v |v\rangle$.

Now, we guess a vector in subspace B of dimension $n/2$. Let the forged state be $|\beta\rangle = \sum_{v \in B} \beta_v |v\rangle$ Let $S = A \cap B$ and $|A \cap B| = m$. For simplicity, let us work with subspace states.

$$U_A |B\rangle |0\rangle = |S\rangle |0\rangle + |B - S\rangle |1\rangle \tag{38}$$

$$|\phi'\rangle \propto |S\rangle \tag{39}$$

The probability of obtaining 0 on measuring the second qubit is given by $(|S|/|B|) = 2m/n$. Assuming we are successful here, we apply the Hadamard operator to obtain

$$H^{\otimes^n} |\phi'\rangle \propto |S^\perp\rangle \tag{40}$$

The applying the unitary operator $U_{A^\perp}$, we get

$$U_{A^\perp} H^{\otimes^n} |\phi'\rangle |0\rangle \propto |A^\perp \cap S^\perp\rangle |0\rangle + |A \cap S^\perp\rangle |1\rangle \tag{41}$$

Now, $S^\perp = A^\perp \cup B^\perp$. Therefore, $A \cap S^\perp = A \cap B^\perp$, and $A^\perp \cap S^\perp = A^\perp$. We then have

$$U_{A^\perp} H^{\otimes^n} |\phi'\rangle |0\rangle \propto |A^\perp\rangle |0\rangle + |A \cap B^\perp\rangle |1\rangle \tag{42}$$

The probability of obtaining 0 on the second qubit in this case is given by $\left(|A^\perp|/(|S^\perp|)\right) = \frac{n}{2(n-m)}$.

Upon successful verification, we obtain the state $|A^\perp \cap S^\perp\rangle$. The probability of success is calculated as $\frac{2m}{n} \times \frac{n}{2(n-m)} = \frac{m}{n-m}$. It can be seen that the probability of success if highest when m is close to $n/2$, i.e, we guess the subspace correctly.

Note. I tried to extend the protective measurement attack to these schemes to estimate the subspace rather than a single state. Unfortunately, I could not make any progress in that aspect. I will think about it more from other perspectives. However, I am skipping these aspects in the report for the project submission for now.

7 Conclusion

We discussed the motivation to develop secure quantum money protocols and how quantum systems have the potential to be used in these areas. Wiesner Quantum Money scheme has been widely adopted across literature, and we analysed the protocol in detail. The attacks discussed in the analysis can easily be prevented if the bank returns a new quantum bill when the detected error in the input quantum state is above a certain threshold. However, such approaches have practical limitations as generating new bills is an expensive operation.

In conclusion, the general secret-key schemes possess these security threats that make the commonly proposed systems ineffectual. The research for public-key schemes is still ongoing, and we are still at far with regards to such protocols.

Nevertheless, the attacks presented in the report also depict the interesting properties of quantum phenomena such as the Zeno effect and protective measurements. These properties have vast potential applications for general quantum systems, and the analysis will help further our understanding of the quantum computing in general.

References

[1] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78â88, jan 1983.

[2] Mark Zhandry. Quantum lightning never strikes the same state twice. *CoRR*, abs/1711.02276, 2017.

[3] Bhaskar Roberts. *Security Analysis of Quantum Lightning*, pages 562–567. 06 2021.

[4] Mikhail Lemeshko and Bretislav Friedrich. Quantum zeno effect, 2009.

[5] Y. Aharonov, J. Anandan, and L. Vaidman. Meaning of the wave function. *Phys. Rev. A*, 47:4616–4626, Jun 1993.

[6] Charles H. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Annual International Cryptology Conference*, 1982.

[7] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41:303–332, 1995.

[8] Michele Mosca and Douglas Stebila. Quantum coins, 2009.

[9] Scott Aaronson. Quantum copy-protection and quantum money. In *2009 24th Annual IEEE Conference on Computational Complexity*. IEEE, July 2009.

[10] Aharon Brodutch, Daniel Nagaj, Or Sattath, and Dominique Unruh. An adaptive attack on wiesner's quantum money, 2016.