Security Proofs for Private-Key Quantum Money: *From Optimal Counterfeiting Bounds to Adaptive Attack Vulnerabilities*

LU Haodong, SUN Leyuan, ZHAO Jiachen & ZHAO Xinpeng

Department of Computer Science & Engineering

The Chinese University of Hong Kong

{hdlu24, lysun0, jczhao23, xpzhao24}@cse.cuhk.edu.hk

ABSTRACT

The security of private-key quantum money, pioneered by Wiesner, relies fundamentally on quantum mechanics to prevent forgery. This review focuses on the evolution of security proofs for such schemes by examining two pivotal analyses of Wiesner's original concept. We first delve into the work establishing optimal bounds for non-adaptive counterfeiting (Molina et al., 2012). This research provides concrete security proofs by quantifying the maximum success probability for an attacker, given a single genuine private-key banknote, to produce two independently verifiable copies. For Wiesner's scheme, this probability is $(3/4)^n$, and for a classical-verification variant, it is $(3/4 + \sqrt{2}/8)^n$. Furthermore, for private-key schemes using d-dimensional quantum systems, a counterfeiting success probability of at least $2/(d+1)$ is proven. These results establish inherent exponential security against such "simple" non-interactive attacks.

In contrast, we then consider research into adaptive attacks, which explore vulnerabilities arising from the bank's interaction protocol within a "strict testing" regime (Nagaj et al., 2016). This work demonstrates a proof of insecurity under specific operational assumptions, showing that if valid money is returned post-verification, attackers can employ strategies analogous to quantum Zeno effect-based measurements (like bomb-testing or protective measurements) to progressively learn the secret quantum state associated with the private key, ultimately compromising the scheme. By juxtaposing these distinct approaches to security proofs—one proving robustness under limited attack models and the other proving vulnerability when protocol interactions are exploited—this review highlights

that comprehensive security for private-key quantum money necessitates analyzing both the quantum encoding and the surrounding operational framework.

1 INTRODUCTION

The ambition to create perfectly unforgeable currency, secure against even the most sophisticated adversaries, found a novel avenue with the advent of quantum information science. Stephen Wiesner's seminal idea of quantum money, conceived around 1970 and formally published by Wiesner (1983), introduced the concept of private-key quantum money. In this paradigm, a central authority (the bank) embeds secret information within quantum states on a physical token. Specifically, Wiesner's scheme involves the bank preparing a sequence of qubits, where each qubit is randomly chosen to be in one of four states corresponding to two non-orthogonal bases (e.g., the rectilinear $\{|0\rangle, |1\rangle\}$ and diagonal $\{|+\rangle, |-\rangle\}$ bases). The sequence of basis choices constitutes the bank's private key for that specific banknote, identified by a unique serial number. Verification requires the bank to use its private key to measure each qubit in the correct, originally chosen basis. The fundamental quantum principle underpinning its security is the no-cloning theorem (Wootters & Zurek, 1982), which asserts that an unknown quantum state cannot be perfectly duplicated. This makes illicit copying by an uninformed party inherently difficult, as any attempt to learn the state by measurement in an arbitrary basis will, with some probability, disturb it.

However, the existence of the no-cloning theorem is a starting point, not a complete security guarantee for a functional private-key quantum money system. A comprehensive understanding of security requires rigorous "security proofs" that quantify an attacker's optimal success probability under various well-defined scenarios, or, conversely, demonstrate explicit attack strategies that compromise the scheme. The nature and strength of such proofs critically depend on the assumed capabilities of the adversary and the operational protocols governing how the bank issues, verifies, and handles these quantum banknotes. This review synthesizes the insights from two key research contributions that exemplify these different facets of security proofs for Wiesner's private-key quantum money.

The first line of inquiry, exemplified by the work of Molina et al. (2012), focuses on providing rigorous proofs of security by establishing the fundamental limits of non-adaptive counterfeiting. Their central question is: given a single, authentic private-key Wiesner banknote, what is the maximum probability with which a counterfeiter can produce two banknotes that both independently pass the bank's verification procedure for that same private key, assuming the counterfeiter has no further interaction with the bank during the counterfeiting process itself? To answer this, they employed semidefinite programming (SDP), a powerful optimization technique well-suited for quantum in-

formation problems due to the positive semidefinite nature of density matrices and Choi operators representing quantum channels (Nielsen & Chuang, 2010). For Wiesner's original scheme with n qubits, their security proof culminates in an optimal success probability for the counterfeiter of exactly $(3/4)^n$. They further extended these proofs to generalizations of private-key quantum money:

- For a variant where verification involves only classical communication with the bank (the bank sends a random classical challenge specifying measurement bases), the optimal success probability is proven to be $(3/4 + \sqrt{2}/8)^n$.
- For schemes generalized to d-dimensional qudits instead of qubits, they proved that any such private-key money scheme is subject to a simple counterfeiting attack with success probability at least $2/(d+1)$, and they described a scheme for which this bound is optimally achieved.
- As an example of analyzing other private-key schemes beyond Wiesner's direct structure, they also provided a tight security bound of $(2/3)^n$ for a 6-state single-qubit variant proposed by Pastawski et al.

These results constitute crucial security proofs, demonstrating inherent exponential resistance of these private-key designs against optimal, non-interactive forging attempts, thereby establishing a fundamental security baseline.

Contrasting sharply with this model of non-interactive attacks, the second body of research, presented by Nagaj et al. (2016), explores security proofs from the perspective of vulnerability, demonstrating how specific operational protocols can render an otherwise robust private-key scheme insecure. They investigate Wiesner's scheme under an adaptive attack model within what they term a "strict testing" regime. The critical assumption here is that the bank's protocol involves returning a banknote to the user if it is deemed valid upon verification, while invalid notes are destroyed. Nagaj et al. (2016) provide a proof of insecurity by showing that this interactive feedback loop can be exploited. They propose and analyze two primary adaptive attack strategies:

1. **The Bomb-Testing (BT) Attack:** This strategy is inspired by the Elitzur-Vaidman interaction-free measurement concept. The attacker prepares an ancillary probe qubit and weakly interacts it with one of the qubits on the private-key banknote. The (potentially slightly disturbed) banknote is then submitted to the bank for verification. If the bank validates it (meaning the private key matches and the state was not overly disturbed), the note is returned. The quantum Zeno effect can play a role here: if the interaction is gentle enough,

the bank's projective measurement (part of the verification based on its private key) can "reset" the money qubit to its original state with high probability. Information about the money qubit's original state (one of the four possibilities allowed by the private-key encoding) is then inferred from the state of the attacker's probe qubit. By repeating this process for each qubit and for different potential states, the attacker can, over many interactions, deduce the bank's entire secret sequence of basis choices (the private key information encoded on that specific note). For generalized schemes with n qubits chosen from r possible states, and a minimum angular separation $\theta_{\min}$ between states, they analyze that this attack can succeed with $O(nr^2\theta_{\min}^{-2}f^{-1})$ validations with an overall failure probability f.

2. **The Protective Measurement (PM) Attack:** As an alternative, particularly for scenarios where the number of possible states per qubit might be very large or continuous (making the BT attack's reliance on $\theta_{\min}$ problematic), this attack aims to estimate the expectation value $\langle A\rangle$ of an observable A on an unknown money state $|\psi\rangle$ without significantly altering $|\psi\rangle$. Again, this involves a weak coupling between a probe system and the money qubit, followed by bank validation and return of the note. Repeated successful interactions allow the attacker to build up statistics on the probe, from which $\langle A\rangle$ can be estimated. By choosing appropriate observables (e.g., Pauli operators), the attacker can perform tomography on each qubit of the banknote, thereby reconstructing the quantum state and, implicitly, the private-key information encoded therein. Nagaj et al. (2016) provide an analysis of the resources required for this protective tomography approach.

The success of these adaptive strategies constitutes a proof that Wiesner's private-key quantum money scheme, under the assumption of a "strict testing" bank protocol, is not secure against an adversary who can repeatedly query the verification oracle.

This review aims to synthesize the insights from these two distinct approaches to providing "security proofs" for private-key quantum money. By examining the rigorous bounds against non-adaptive attacks derived by Molina et al. (2012) alongside the protocol-dependent vulnerabilities exposed by Nagaj et al. (2016), we can appreciate the multifaceted nature of security in quantum cryptographic systems. The ultimate goal is to understand what conditions and designs lead to provably secure private-key quantum money in realistic operational environments.

2 BACKGROUND

The concept of **quantum money** (Wiesner, 1983), first proposed by Stephen Wiesner in the early 1970s and later published in 1983, introduced a radical idea: using quantum states to make physical currency that is provably unforgeable. Wiesner's scheme encodes each bill with a sequence of qubits, each prepared in a randomly chosen basis—either a computational basis $\{|0\rangle, |1\rangle\}$ or a conjugate basis such as $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. These quantum bits are paired with classical metadata, such as a serial number, and their precise states and bases are recorded only at the issuing bank. To verify the authenticity of a bill, the bank performs measurements in the known correct bases and checks that the outcomes match the recorded state. A counterfeiter who attempts to duplicate the bill without knowing the correct measurement bases inevitably disturbs the original quantum states due to the uncertainty principle, rendering their copy invalid.

This intuitive security argument was later formalized by the **no-cloning theorem** (Wootters & Zurek, 1982), proven in 1982 by Wootters and Zurek. The theorem shows that no physical process can produce an exact copy of an arbitrary unknown quantum state, due to the linearity of quantum mechanics. Specifically, any attempt to clone a superposition state like $a|0\rangle + b|1\rangle$ results in a final state that deviates from two identical copies, even if cloning succeeds for certain orthogonal states like $|0\rangle$ and $|1\rangle$. This impossibility directly supports the robustness of Wiesner's quantum money scheme, as it ensures that an adversary cannot replicate the embedded qubit states without altering them and being detected during verification. Remarkably, Wiesner anticipated this cryptographic application of quantum mechanics a decade before the no-cloning theorem was rigorously established, making quantum money one of the earliest practical illustrations of how uniquely quantum properties can be harnessed for secure information processing.

3 Optimal Counterfeiting Bounds via Semidefinite Programming

This section delves into the contributions of Molina et al. (2012), who provided some of the first rigorous, quantitative analyses of the security limits of Wiesner's quantum money scheme and its generalizations. Their work moved beyond the qualitative intuition offered by the no-cloning theorem, employing powerful mathematical tools to establish tight bounds on counterfeiting capabilities.

3.1 Motivation and Problem Formulation

Wiesner's quantum money scheme (Wiesner, 1983), while conceptually groundbreaking, existed for decades without a rigorous analysis quantifying its security against optimal adversaries, particularly concerning explicit success probabilities. While the no-cloning principle (Wootters & Zurek, 1982) provides the fundamental security intuition, translating this into concrete bounds requires dedicated analysis, much like the security proofs developed for quantum key distribution protocols such as BB84 (Bennett & Brassard, 1984; Shor & Preskill, 2000). The work by Molina et al. (2012) aimed to fill this gap by providing precise mathematical formulations and solutions for counterfeiting attacks against Wiesner's scheme.

Their investigation sought answers to several key questions:

- What is the *optimal* success probability for a counterfeiter attempting a "simple counterfeiting attack" – that is, starting with a single authentic banknote associated with a specific serial number, producing two quantum states that both independently pass the bank's verification procedure for that same serial number?

- Can the security of such schemes be enhanced or modified by generalizing the underlying quantum states? This includes considering different ensembles of single-qubit states beyond Wiesner's original four, or extending the scheme to use higher-dimensional quantum systems (qudits, $d > 2$).

- Is it feasible to design variants of quantum money where the verification process relies solely on *classical* communication between the note holder and the bank, thus avoiding the need to physically send quantum states back? If so, what level of security do these classical-verification schemes offer against counterfeiting attacks?

- Can semidefinite programming (SDP) serve as a unifying mathematical framework to precisely model these counterfeiting scenarios and compute the optimal attack success probabilities?

By addressing these questions, Molina et al. (2012) aimed to place the security analysis of Wiesner's scheme on a firm quantitative footing.

3.2 Core Mathematical Tool: Semidefinite Programming (SDP)

The primary mathematical engine driving the analysis in Molina et al. (2012) is semidefinite programming (SDP). To understand its application, we first introduce some notation from the paper regarding linear operators on finite-dimensional complex Hilbert spaces. For a Hilbert space $\mathcal{X}$, $L(\mathcal{X})$ denotes the set of linear operators acting on $\mathcal{X}$, $\mathrm{Herm}(\mathcal{X})$ denotes the Hermitian operators, $\mathrm{Pos}(\mathcal{X})$ denotes the positive semidefinite operators, $\mathrm{Pd}(\mathcal{X})$ the positive definite operators, and $\mathrm{D}(\mathcal{X})$ the density operators (states, $\rho \in \mathrm{Pos}(\mathcal{X})$ with $\mathrm{Tr}(\rho) = 1$). The standard inner product between operators $A, B \in L(\mathcal{X})$ is the Hilbert-Schmidt inner product:

$$\langle A, B \rangle = \mathrm{Tr}(A^\dagger B). \tag{1}$$

For any linear map $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$, there exists a unique adjoint map $\Phi^* : L(\mathcal{Y}) \to L(\mathcal{X})$ satisfying $\langle Y, \Phi(X) \rangle = \langle \Phi^*(Y), X \rangle$ for all $X \in L(\mathcal{X})$ and $Y \in L(\mathcal{Y})$.

SDP is a subfield of convex optimization concerned with optimizing a linear objective function over the cone of positive semidefinite matrices, subject to linear equality constraints. A standard SDP formulation involves a primal and a dual problem. Given a Hermiticity-preserving linear map $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$ and Hermitian operators $A \in \mathrm{Herm}(\mathcal{X})$, $B \in \mathrm{Herm}(\mathcal{Y})$, the primal problem is typically stated as:

$$\begin{aligned} \sup \quad & \langle A, X \rangle \\ \text{s.t.} \quad & \Phi(X) = B, \\ & X \in \mathrm{Pos}(\mathcal{X}). \end{aligned} \tag{2}$$

Its corresponding dual problem is:

$$\begin{aligned} \inf \quad & \langle B, Y \rangle \\ \text{s.t.} \quad & \Phi^*(Y) \succeq A, \\ & Y \in \mathrm{Herm}(\mathcal{Y}). \end{aligned} \tag{3}$$

Here, $\Phi^*(Y) \succeq A$ means $\Phi^*(Y) - A \in \mathrm{Pos}(\mathcal{X})$.

Let α be the optimal value of the primal problem equation 2 and β be the optimal value of the dual problem equation 3. Weak duality always holds: $\alpha \leq \beta$. SDPs are particularly powerful because they can often be solved efficiently (Vandenberghe & Boyd, 1996), and under mild conditions (such as Slater's condition, which requires strict feasibility of either the primal or dual problem), strong duality holds ($\alpha = \beta$), and optimal solutions exist and are achievable.

The applicability of SDP to quantum information processing stems fundamentally from the fact that quantum states (density matrices ρ) must be positive semidefinite operators ($\rho \succeq 0$). Furthermore, quantum operations are described by quantum channels, which are linear maps that are completely positive (CP) and trace-preserving (TP). The set of CPTP maps forms a convex set, amenable to optimization techniques like SDP (Watrous, 2018).

A key mechanism bridging quantum operations and SDP is the **Choi-Jamiolkowski isomorphism** (Choi, 1975; Jamiołkowski, 1972). This establishes a one-to-one correspondence between linear maps $\Phi : L(\mathcal{H}_X) \to L(\mathcal{H}_Y)$ and linear operators $J(\Phi) \in L(\mathcal{H}_Y \otimes \mathcal{H}_X)$, where $\dim(\mathcal{H}_X) = d$. Fixing an orthonormal basis $\{|1\rangle, \ldots, |d\rangle\}$ for $\mathcal{H}_X$, the Choi operator is defined as:

$$J(\Phi) = \sum_{1 \leq i,j \leq d} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|. \tag{4}$$

This isomorphism translates properties of the map Φ into properties of the operator $J(\Phi)$:

- Φ is completely positive (CP) if and only if $J(\Phi) \in \mathrm{Pos}(\mathcal{H}_Y \otimes \mathcal{H}_X)$, i.e., $J(\Phi) \succeq 0$.
- Φ is trace-preserving (TP) if and only if $\mathrm{Tr}_Y(J(\Phi)) = I_X$, where Tr_Y denotes the partial trace over $\mathcal{H}_Y$ and I_X is the identity operator on $\mathcal{H}_X$.

The action of the channel on a pure state $|\psi\rangle \in \mathcal{H}_X$ can also be related to the Choi operator. For any vector $|\phi\rangle \in \mathcal{H}_Y$, the overlap is given by:

$$\langle\phi|\Phi(|\psi\rangle\langle\psi|)|\phi\rangle = \langle\phi \otimes \psi^T|J(\Phi)|\phi \otimes \psi^T\rangle, \tag{5}$$

where $|\psi^T\rangle$ denotes the vector obtained by taking the complex conjugate of the components of $|\psi\rangle$ in the standard basis $\{|i\rangle\}$.

This isomorphism is crucial for the work of Molina et al. (2012). Optimizing over the set of all physically realizable quantum channels (CPTP maps) Φ that perform a certain task (like counterfeiting) translates directly into optimizing over the set of Choi operators $J(\Phi)$ that satisfy $J(\Phi) \succeq 0$ and $\mathrm{Tr}_Y(J(\Phi)) = I_X$.

These conditions fit precisely into the SDP framework equation 2-equation 3, allowing for the computation of optimal strategies and success probabilities for tasks like quantum state cloning and counterfeiting.

3.3 WIESNER'S QUANTUM MONEY SCHEME: QUANTUM VERIFICATION

Wiesner's quantum money scheme [Wie83] stands as a foundational concept in quantum cryptography. It leverages the principles of quantum mechanics to create currency that is, in theory, impossible to counterfeit perfectly.

3.3.1 ORIGINAL SCHEME SETUP AND VERIFICATION

In Wiesner's original proposal, each banknote comprises n quantum bits (qubits). The bank prepares each qubit independently, choosing its state uniformly at random from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Thus, each of these four states is selected with a probability $p_k = 1/4$. The bank meticulously records this sequence of prepared states (the "key") and associates it with a unique serial number imprinted on the banknote. This record is kept secret by the bank.

Verification of a banknote's authenticity requires it to be returned to the bank. The bank, using the serial number to retrieve the secret key, performs a quantum measurement on each qubit. For a qubit prepared in $|0\rangle$ or $|1\rangle$, the bank measures in the computational basis ($\{|0\rangle, |1\rangle\}$). For a qubit prepared in $|+\rangle$ or $|-\rangle$, the measurement is performed in the Hadamard basis ($\{|+\rangle, |-\rangle\}$). The banknote is deemed authentic if and only if all measurement outcomes correspond to the originally prepared states. The security of this scheme fundamentally relies on the no-cloning theorem [WZ82], which asserts that it is impossible to create an identical copy of an unknown quantum state.

3.3.2 OPTIMAL COUNTERFEITING ATTACKS

A primary concern for any currency scheme is its resilience against counterfeiting. In the context of Wiesner's scheme, a "simple counterfeiting attack" is defined as an attempt by a counterfeiter, who is given a single genuine banknote, to produce two banknotes (associated with the same serial number) that can both independently pass the bank's verification procedure.

Let the original banknote's quantum state be in a register X, and the two alleged copies produced by the counterfeiter be in registers Y and Z. A counterfeiting attempt is described by a quantum channel (a completely positive trace-preserving map) $\Phi : L(X) \to L(Y \otimes Z)$. If the bank originally prepared the state $|\psi_k\rangle$, the probability that both counterfeit notes pass verification is

$\langle\psi_k \otimes \psi_k|\Phi(|\psi_k\rangle\langle\psi_k|)|\psi_k \otimes \psi_k\rangle$. Averaging over all possible initial states chosen by the bank (with probabilities p_k), the overall success probability of the counterfeiting attack is:

$$P_{\text{success}} = \sum_{k=1}^{N} p_k \langle\psi_k \otimes \psi_k|\Phi(|\psi_k\rangle\langle\psi_k|)|\psi_k \otimes \psi_k\rangle \quad (1)$$

The paper establishes a crucial result for Wiesner's original scheme:

Theorem 1 (Molina, Vidick, Watrous, 2012)

The optimal simple counterfeiting attack against Wiesner's quantum money scheme has a success probability of exactly $(3/4)^n$, where n is the number of qubits in each banknote.

For a single-qubit banknote ($n = 1$), the optimal success probability is $3/4$. For an n-qubit banknote, this probability decreases exponentially.

3.3.3 Semidefinite Programming (SDP) Formulation

The problem of determining the optimal success probability for a simple counterfeiting attack can be precisely formulated and solved using semidefinite programming (SDP). This mathematical framework is powerful for optimization problems involving quantum states and operations, yielding tight bounds on security.

The optimal success probability (1) can be found by solving the following primal SDP problem:

- **Primal Problem**:

$$\begin{aligned} &\sup \quad \langle Q, X\rangle \\ &\text{s.t.} \quad \text{Tr}_{Y\otimes Z}(X) = I_X \\ &X \in \text{Pos}(Y \otimes Z \otimes X) \end{aligned}$$

Here, X is the Choi-Jamiołkowski representation $J(\Phi)$ of the counterfeiting channel Φ. The operator $Q \in \text{Pos}(Y \otimes Z \otimes X)$ is defined as:

$$Q = \sum_{k=1}^{N} p_k |\psi_k \otimes \psi_k \otimes \overline{\psi_k}\rangle\langle\psi_k \otimes \psi_k \otimes \overline{\psi_k}| \quad (2)$$

where $\overline{\psi_k}$ denotes the complex conjugate of $|\psi_k\rangle$ (with respect to the standard basis in X). The inner product is $\langle A, B\rangle = \text{Tr}(A^*B)$.

The corresponding dual problem is:

- **Dual Problem**:

$$\begin{aligned} \inf \quad & \text{Tr}(Y) \\ \text{s.t.} \quad & I_{Y\otimes Z} \otimes Y \geq Q \\ & Y \in \text{Herm}(X) \end{aligned}$$

Strong duality holds for this problem, meaning the optimal values of the primal and dual problems are equal.

For Wiesner's original single-qubit scheme, $N = 4$, $p_k = 1/4$, and the states are $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The operator Q becomes:

$$Q = \frac{1}{4}(|000\rangle\langle 000| + |111\rangle\langle 111| + |++\rangle\langle +++| + |--\rangle\langle ---|).$$

The optimal value of this SDP is $3/4$. This can be shown by finding explicit feasible solutions:

- A primal feasible solution $X = J(\Phi)$ achieving $3/4$ is given by the channel below:

$$\Phi(\rho) = A_0 \rho A_0^* + A_1 \rho A_1^*,$$

  with specific Kraus operators below (mapping to a 4×1 vector space for $Y \otimes Z$):

$$A_0 = \frac{1}{\sqrt{12}} \begin{bmatrix} 3 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad A_1 = \frac{1}{\sqrt{12}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 3 \end{bmatrix},$$

- A dual feasible solution achieving $3/4$ is $Y = \frac{3}{8} I_X$.

The analysis further reveals that a counterfeiter gains no advantage by attempting to correlate attacks across multiple qubits of an n-qubit note. The optimal strategy involves attacking each qubit independently. Consequently, if the optimal success probability for a single repetition (one qubit) is α, for n repetitions (an n-qubit note), it is α^n. This confirms the $(3/4)^n$ result for Wiesner's scheme. This SDP formulation provides a rigorous confirmation of Wiesner's original intuition and quantifies the security precisely.

3.4 Generalizations and Optimizations

In this section, we extend our analysis beyond Wiesner's original quantum money scheme, exploring various generalizations and optimized schemes. Specifically, we discuss improvements

via optimized single-qubit states, the impact of parallel repetitions, threshold results, and higher-dimensional (qudit-based) quantum money schemes.

3.4.1 Single-Qubit Optimal Schemes

While Wiesner's original scheme offers a certain level of security, researchers have explored whether different ensembles of single-qubit states could provide better protection. Pastawski et al. [PYJ+11] investigated a scheme using a 6-state ensemble. In this scheme, each qubit is prepared in one of the six eigenstates of the Pauli operators ($\sigma_x, \sigma_y, \sigma_z$): $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |y+\rangle, |y-\rangle\}$, where $|y\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, each chosen with probability $1/6$. For this 6-state scheme, the optimal simple counterfeiting success probability per qubit is reduced to $2/3$.

Molina, Vidick, and Watrous (the authors of the reference paper) showed that this $2/3$ bound can also be achieved with a 4-state ensemble, specifically if the four states form a Symmetric Informationally Complete Positive Operator-Valued Measure (SIC-POVM) [RBKSC04]. For such schemes, the operator Q in the SDP (Equation 2) has a specific structure related to the transposition map, and the optimal value is $2/3$. An explicit primal solution (channel) achieving $2/3$ is

$$\Phi(\rho) = A_0 \rho A_0^* + A_1 \rho A_1^*,$$

with

$$A_0 = \frac{1}{\sqrt{6}} \begin{bmatrix} 2 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \text{and} \quad A_1 = \frac{1}{\sqrt{6}} \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

A dual solution is $Y = \frac{1}{3} I_X$.

This success probability of $2/3$ is significant because it matches the optimal success probability for the universal 1-to-2 qubit cloner (Bužek-Hillery cloner [BH96]). This cloner succeeds with probability $2/3$ for *any* input qubit state, implying that $2/3$ is a fundamental lower bound on the counterfeiting probability for any single-qubit money scheme of this type. Thus, these 6-state and 4-state SIC-POVM schemes are optimal among single-qubit schemes.

Thus, optimal single-qubit schemes outperform Wiesner's original four-state scheme, providing stronger security per qubit.

3.4.2 Parallel Repetitions and Threshold Schemes

Quantum money schemes typically use n-qubit banknotes, relying on the idea that security increases exponentially with n. As discussed for Wiesner's scheme, if the optimal counterfeiting probability

for a single instance of a scheme (e.g., one qubit) is α, then for an n-fold parallel repetition (an n-qubit note where each qubit is an independent instance of the scheme), the optimal success probability for the counterfeiter to succeed on all n instances is α^n. This multiplicative behavior holds generally for these types of schemes, meaning correlated attacks across qubits offer no advantage to the counterfeiter.

Some schemes might employ a "threshold" verification: the bank declares a banknote valid if at least t out of n qubit measurements are correct (where $t \leq n$). For such schemes, if each repetition is attacked independently and optimally with success probability α, the probability of passing the threshold test would be $\sum_{j=t}^{n} \binom{n}{j} \alpha^j (1-\alpha)^{n-j}$. The paper shows that this binomial probability is indeed the optimal counterfeiting probability for the threshold scheme, provided two conditions hold:

1. The ensemble average state is maximally mixed:

$$\sum_{k=1}^{N} p_k |\psi_k\rangle\langle\psi_k| = \frac{1}{d} I_X,$$

   where d is the dimension of the Hilbert space for a single repetition (e.g., $d = 2$ for qubits). (Equation 5 in the paper)

2. $Y = \frac{\alpha}{d} I_X$ is an optimal dual solution to the single-repetition SDP.

These conditions are met by Wiesner's original scheme and the other specific schemes discussed. This implies that even for threshold verification, independent attacks on each component are optimal.

3.4.3 Higher-Dimensional (Qudit) Schemes

An alternative way to potentially enhance security is to use quantum systems of dimension $d > 2$, known as qudits. For a d-dimensional quantum system, Werner [Wer98] showed that a universal quantum cloner can produce two copies from one original with a success probability of $2/(d+1)$ for any input state. This sets a fundamental limit: any quantum money scheme based on d-dimensional states is vulnerable to a counterfeiting attack with success probability at least $2/(d+1)$.

The paper demonstrates the existence of qudit-based quantum money schemes that achieve this optimal security bound.

Proposition 4 (Molina, Vidick, Watrous, 2012)

Let $\mathcal{E} = \{p_k, |\psi_k\rangle\}$ be an ensemble of d-dimensional states. If the operator Q (defined in Equation 2) is given by:

$$Q = \frac{1}{\text{rank}(\Pi)}(I_{L(C^d)} \otimes I_{L(C^d)} \otimes T)(\Pi)$$

where T is the transposition mapping (with respect to the standard basis of C^d) and Π is the orthogonal projector onto the symmetric subspace of $C^d \otimes C^d \otimes C^d$, then no simple counterfeiting strategy can succeed against the money scheme derived from $\mathcal{E}$ with probability more than $2/(d+1)$.

Ensembles $\mathcal{E}$ derived from quantum 3-designs satisfy the condition on Q in Equation (3) and thus lead to optimal d-dimensional money schemes. For $d = 2$ (qubits), this optimal probability is $2/(2 + 1) = 2/3$, consistent with the optimal single-qubit schemes. For $d = 3$ (qutrits), the probability drops to $2/(3+1) = 1/2$. As d increases, the security $2/(d+1)$ improves significantly, highlighting the potential of higher-dimensional systems.

3.5 Quantum Money with Classical Verification

A practical drawback of Wiesner's original scheme is the requirement for quantum communication with the bank for verification. This involves physically sending the quantum banknote to the bank, which can be cumbersome and technologically demanding.

3.5.1 Motivation and Scheme Description

To address this, variants of quantum money have been proposed that only require classical communication for verification. In such a "quantum ticket" scheme, the physical quantum state (the ticket) remains with the user during verification. The process is typically as follows:

1. The bank prepares a quantum ticket consisting of n qudits. Each qudit i is prepared in a state $|\psi_{k_i}\rangle$ based on a secret key k_i known only to the bank. The ticket has a unique serial number.

2. To verify the ticket, the user (holder) provides the serial number to the bank.

3. The bank sends the user a randomly chosen classical "challenge" $c \in \mathcal{C}$ for each qudit (or a single challenge c for the entire ticket). $\mathcal{C}$ is a fixed finite set of possible challenges.

4. The user performs a measurement $\Pi_c = \{\Pi_a^c\}_{a \in A}$ on their ticket, where the choice of measurement basis (or POVM) depends on the challenge c. The user then reports the classical outcome a to the bank.

5. The bank, knowing the original secret key k associated with the serial number and the challenge c it sent, checks if the reported outcome a is valid. The ticket is accepted if the triple (a, c, k) falls into a predefined, publicly known set S of valid triples. An honest user, knowing the state preparation, would always pass if their ticket is genuine.

A key aspect is that verification may alter or destroy the quantum state of the ticket.

3.5.2 SDP Formulation for Classical Verification

A counterfeiter in this scenario, given one genuine ticket, attempts to successfully answer two independent challenges from the bank for that same ticket. The counterfeiter's strategy can be modeled by a collection of POVMs $\{A_{a_1 a_2}^{c_1 c_2}\}_{a_1 a_2}$ for each pair of challenges (c_1, c_2). The success probability, averaged over the bank's choice of initial states $|\psi_k\rangle$ (with probability p_k) and its choice of two independent challenges c_1, c_2 (chosen uniformly from $\mathcal{C}$), is:

$$P_{\text{success}} = \sum_{k=1}^{N} p_k \frac{1}{|\mathcal{C}|^2} \sum_{c_1, c_2 \in \mathcal{C}} \sum_{\substack{(a_1,a_2):\\ (a_1,c_1,k)\in S\\ (a_2,c_2,k)\in S}} \langle \psi_k | A_{a_1 a_2}^{c_1 c_2} | \psi_k \rangle \quad (4)$$

Maximizing this probability can also be cast as an SDP. The corresponding operator Q_{cv} for this SDP is:

$$Q_{cv} = \sum_{k=1}^{N} p_k \frac{1}{|\mathcal{C}|^2} \sum_{c_1, c_2} \sum_{\substack{(a_1,a_2):\\ (a_1,c_1,k)\in S\\ (a_2,c_2,k)\in S}} |a_1\rangle|a_2\rangle|c_1, c_2, \psi_k\rangle\langle a_1|\langle a_2|\langle c_1, c_2, \psi_k|$$

This operator Q_{cv} acts on a space that includes classical registers for the outcomes a_1, a_2 and challenges c_1, c_2, in addition to the quantum state $|\psi_k\rangle$.

3.5.3 Optimality and Performance Analysis

The paper provides tight bounds for such classical verification schemes. For an n-qubit scheme analogous to Wiesner's (where qubits are prepared in one of two bases, e.g., computational or Hadamard, and the challenge selects which basis to measure), the optimal success probability for a counterfeiter to pass two independent verifications is given by: **Theorem 2 (Molina, Vidick, Watrous, 2012):** For the classical-verification analogue of Wiesner's quantum money scheme, the optimal simple counterfeiting attack has success probability exactly $(3/4 + \sqrt{2}/8)^n$.

This value is $((6 + \sqrt{2})/8)^n \approx (0.9267)^n$, which is higher than the $(3/4)^n = (0.75)^n$ for the quantum verification scheme, indicating that classical verification is inherently less secure for the same underlying state ensemble, though still offering exponential security.

The analysis can be extended to d-dimensional qudits. Consider a scheme where each qudit is prepared using one of two bases, $B_0 = \{|e_s^0\rangle\}$ and $B_1 = \{|e_t^1\rangle\}$. The challenge $c \in \{0, 1\}$ dictates which basis is measured.

Lemma 5 (Molina, Vidick, Watrous, 2012)

For such an n-qudit classical-verification scheme, the success probability of any simple counterfeiting attack is at most:

$$(3/4 + \sqrt{c_{overlap}}/4)^n,$$

where $c_{overlap} = \max_{s,t} |\langle e_s^0 | e_t^1 \rangle|^2$ is the maximum squared overlap between basis vectors from the two different bases. If $d = 2$ (qubits), this bound is achievable.
For qubits using the computational and Hadamard bases:

$$c_{overlap} = (1/\sqrt{2})^2 = 1/2,$$

leading to:

$$(3/4 + \sqrt{1/2}/4)^n = (3/4 + 1/(4\sqrt{2}))^n = (3/4 + \sqrt{2}/8)^n,$$

matching Theorem 2.

The paper further shows a matching lower bound for a specific d-dimensional scheme. This scheme uses the computational basis $\{|t\rangle\}$ and its Quantum Fourier Transform (QFT) basis $\{F|t\rangle\}$. For these bases, the overlap $c_{overlap} = 1/d$ for all pairs of basis vectors.

Lemma 6 (Molina, Vidick, Watrous, 2012)

There is a cloner for the n-qudit ticket scheme (using computational and QFT bases) which successfully answers both challenges with probability $(3/4 + 1/(4\sqrt{d}))^n$.

This result demonstrates that for these specific bases, the success probability is $(3/4 + 1/(4\sqrt{d}))^n$. As d increases, $1/(4\sqrt{d})$ decreases, and the security improves. For large d, the success probability approaches $(3/4)^n$.

These findings underscore that quantum money with classical verification can offer robust, exponentially decaying counterfeiting probabilities, making them a more practical alternative to schemes requiring quantum communication, despite a slight reduction in security compared to their quantum-verified counterparts.

4 AN ADAPTIVE ATTACK ON WIESNER'S QUANTUM MONEY

4.1 MOTIVATION

Quantum money, first introduced by Wiesner in the 1970s (Wiesner, 1983), stands as a foundational proposal for leveraging quantum mechanics to achieve unforgeable currency. At the heart of its security lies the *no-cloning theorem* (Wootters & Zurek, 1982), which prohibits perfect duplication of arbitrary quantum states. In Wiesner's scheme, each quantum banknote is associated with a *serial number* and a corresponding *quantum state*—typically a tensor product of single-qubit states, each randomly chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The pair $(s, |\$s\rangle)$, comprising the serial number and quantum state, constitutes valid money (Wiesner, 1983). Verification of a banknote is performed by measuring each qubit in its original preparation basis, information known only to the issuing bank.

A critical yet often overlooked aspect of the protocol is the *post-verification behavior*—what happens to a banknote after it passes or fails the bank's validity test. One primary model arises where successful validation leads to the *return of the same banknote*, while failed attempts result in the state being *destroyed*. This regime, termed *strict testing* (Nagaj et al., 2016), aligns with intuitive expectations: valid money remains in circulation; forgeries are confiscated. However, an important security question emerges: *Does this model inadvertently enable an attacker to extract information without being caught?*

The paper (Nagaj et al., 2016) investigates the vulnerabilities of Wiesner's scheme under *strict testing*, revealing that even without access to the post-measurement state of failed tests, a counterfeiter can still compromise the scheme. The authors demonstrate that under strict testing, the quantum Zeno effect can be exploited to perform *non-destructive, weak interactions* with the quantum money state. Such interactions enable the attacker to infer the identity of each qubit state while minimizing the risk of triggering a failed test, thus learning the full money state with high confidence and negligible disturbance. Once learned, the attacker can efficiently create counterfeit copies of the original state $|\$s\rangle$, undermining the presumed security of the scheme.

4.2 PROBLEM FORMULATION

In the paper (Nagaj et al., 2016), there are two different post-validation policies for analyzing the *security of Wiesner's quantum money*.

- **Strict Testing Regime:** The bank returns the same valid quantum banknote after a successful test, and destroys it after a failed one.
- **Token Replacement Regime:** The bank issues a *fresh new quantum banknote with a new serial number* after each successful validation, akin to a *single-use token*. The bank destroys the invalid quantum banknote after a failed test.

The adaptive attack presented in the paper (Nagaj et al., 2016) is effective *only under the strict testing regime*. The authors introduce two main techniques:

- **Zeno-assisted Elitzur-Vaidman Bomb Test**, which allows the identification of individual qubit states with low risk of detection.
- **Protective Measurement (PM) Attack**, which enables a form of tomography on the unknown state using weak measurements and repeated validation. This attack remains effective even when the number of possible states per qubit is infinite (implying $\theta_{\min} \to 0$), a setting in which the bomb-testing attack fails.

4.3 ATTACK PROCEDURE

In this section, we describe the attack procedure of both proposed techniques in (Nagaj et al., 2016).

4.3.1 THE BT(BOMB-TESTING) ATTACK

The bomb-testing attack, based on the work of (Kwiat et al., 1995), serves as a straightforward analogy for understanding quantum money. In this scenario, quantum money is likened to the bomb, while the bank's verification process parallels the bomb-checking procedure. If the money is determined to be counterfeit, it is reported, akin to the bomb's explosion leading to dire consequences. Our goal is to ascertain the state of the money without altering it. However, unlike the bomb-testing scenario, quantum money operates with four possible states per qubit, hence modification of the algorithm is required.

To understand the BT attack for quantum money, we first introduce the Elitzur-Vaidman's bomb quality tester. Here we pick a large N, then we define:

$$\delta = \frac{\pi}{2N}, \qquad R_\delta = \begin{bmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{bmatrix} \tag{6}$$

We also define a controlled interaction between probe and system qubits:

$$C_P = |0\rangle\langle 0| \otimes + |1\rangle\langle 1| \otimes P. \tag{7}$$

Typically we pick controlled-X to be P. The testing procedure starts from a probe qubit initialized to $|0\rangle$. We run the below steps for N times:

1. Prepare a system qubit initialized to $|0\rangle$
2. Rotate the probe qubit with R_δ
3. Apply C_P
4. Measure the system qubit. If we get $|1\rangle$, the bomb explodes. If we get $|0\rangle$, return to the first step.

At last, measure the probe qubit and we can know if there is a active bomb.

In the context of quantum money, we aim to apply the bomb-testing procedure to each qubit and determine its state. The primary challenge is that each qubit can exist in one of four possible states: $|a_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Here, with P is a controlled-X or controlled-$(-X)$, if the qubit $|a_i\rangle \in$

$\{|0\rangle, |1\rangle\}$, the flip will be observable by the bank, resembling the live bomb scenario in bomb-testing. Conversely, if the qubit is in the states $\{|+\rangle, |-\rangle\}$, it behaves like a dud, which will not be detected when flipped. Hence we can determine it's $|+\rangle$ or $|-\rangle$ by defining P to be controlled-X or controlled-$(-X)$. If both states not detected, we can safely measure the qubit in $\{|0\rangle, |1\rangle\}$ basis.

4.3.2 THE PM(PROTECTIVE MEASUREMENT) ATTACK

The BT attack relies on the special relationship of the 4 states. However, it doesn't work when there are infinitely many states per qubit. Hence, to solve that problem, the paper proposes a stronger attack technique named protective measure.

We first define $A = P - P^{\perp}$ where P is a projector on its +1 eigenspace and $P^{\perp} = I - P$. We treat it as the validation procedure of the bank that can be used to estimate the expectation value of any dichotomic observable. Then we can estimate $\langle A\rangle = \langle\psi| A |\psi\rangle$ without disturbing $|psi\rangle$ much. The detailed procedure would be first weakly couple the probe and system qubits by $|0\rangle |\psi\rangle \xrightarrow{e^{-i\delta(\sigma_x \otimes A)}} \approx |0\rangle |\psi\rangle - i\delta |1\rangle A |\psi\rangle$. Then we send the qubits to bank for measurement. The result would be $\left(e^{-i\delta\langle A\rangle\sigma_x} |0\rangle\right) \otimes |\psi\rangle$. Repeat the procedure for N times, and we end up with $\left(e^{-iN\delta\langle A\rangle\sigma_x} |0\rangle\right) \otimes |\psi\rangle$. Lastly, we measure the probe qubit and estimate $\langle A\rangle$ by standard parameter estimation technique.

4.4 MATHEMATICAL ANALYSIS

In this section, we provide mathematical analysis on the two attack techniques.

4.4.1 THE BT(BOMB-TESTING) ATTACK

The theoretical guarantee of the BT attack is similar to the bomb-testing. In bomb-testing, the probability of getting no explosion in N steps is:

$$\left(1 - \sin^2\delta\right)^N \geq \left(1 - \frac{\pi^2}{4N^2}\right)^N \geq 1 - N\frac{\pi^2}{4N^2} = 1 - \frac{\pi^2}{4N}. \tag{8}$$

While in the quantum money case, we need N steps for P to be controlled-X and controlled-$(-X)$ each. Suppose the quantum money obtains n qubits, then the probability that the attack works is:

$$\Pr(\text{attack succeeds}) \geq \left(1 - \frac{\pi^2}{4N}\right)^{2n} \geq 1 - \frac{\pi^2 n}{2N}, \tag{9}$$

Hence by picking a large N, typically $N = \frac{\pi^2 n}{2\epsilon}$, we obtain a success rate over $1 - \epsilon$.

4.4.2 THE PM(PROTECTIVE MEASUREMENT) ATTACK

We highlight the important theoretical guarantees established in the paper as follows. First, we present the formal definition of the algorithm.

Definition 1 (Protective Measurement) *For an unknown state $|\alpha\rangle \in \mathbb{C}^d$, two outcome von Neumann measurement $\{\Pi = \alpha, I - \Pi\}$, the validation, a protocol is a protective measurement of a dichotomic observable A with running time N, accuracy ϵ, and failure probability f when*

1. *The protocol makes at most N uses of the validation.*
2. *With probability that all the outcomes are Π is at least $1 - f$.*

In this case, the procedure maps $|\varphi\rangle |\alpha\rangle \to \left[e^{-i\frac{\pi}{8}\langle A\rangle\sigma_x} |\varphi\rangle + O(\epsilon) |\varphi'\rangle\right] |\alpha\rangle$ for all $|\varphi\rangle \in \mathbb{C}^2$.

$O(\epsilon) |\varphi'\rangle$ is relatively small and can be ignored, hence the Definition 1 aligns with the attack procedure.

With this definition, we can deduct the relationship among N, ϵ, and f.

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

The paper also provides much detailed statistics about the estimation quality.

Theorem 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 $O(f)$ and running time $O\left(f^{-1}\nu^{-4}\ln^2(\eta^{-1})\right)$.*

Unlike the BT attack, the estimation of A requires additional effort. Specifically, N is required to be $O(\nu^{-4}\ln^2(\eta^{-1}))$ as large to ensure high precision ν and high confidence $1 - \eta$.

Note that the Definition 1 and Theorem 1 only provide theoretical support for obtaining $\left(e^{-iN\delta\langle A\rangle\sigma_x} |0\rangle\right)$. Integrating the Theorem 2, we can have guarantee on the whole attack procedure, including the estimation of $\langle A\rangle$.

Definition 2 (Protective Tomography) *For an unknown state $|\alpha\rangle \in \mathbb{C}^d$, two outcome von Neumann measurement $\{\Pi = \alpha, I - \Pi\}$ the validation, 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:*

1. *The probability of failure, i.e. that at some step of the algorithm the outcome of the measurement is* $I - \Pi$*, is* $O(f)$.
2. *If the algorithm does not fail, with probability at least* $1 - \eta$*, we have* $F(|\alpha\rangle, \rho) \geq 1 - \epsilon$*,*
3. *The algorithm uses at most* t *validations.*

Now we can deduct the general theoretical guarantee for the protective tomography.

Theorem 3 *There exists a protective tomography protocol for* n*-qubit states of the form* $|\alpha\rangle = \bigotimes_{i=1}^{n} |\alpha_i\rangle$*, with running time* $t = O\left(n^5 f^{-1} \epsilon^{-4} \ln^2(n\eta^{-1})\right)$.

4.5 Security Discussion

Now, we will discuss how to protect the quantum money protocol from the two attacks.

4.5.1 Protection Through Scheme

While both of these attack techniques can counterfeit quantum money, they rely on the strict testing variant of Wiesner's scheme. A common mitigation strategy involves issuing a new quantum bill with a unique serial number to the owner after a valid test. In this case, the quantum money scheme remains secure. Consequently, these techniques serve as a cautionary reminder about the risks associated with reusing quantum money.

4.5.2 Protection Through Parameter

Another way to defend against these two attacks is to adjust the parameters in the scheme.

As discussed, increasing the number of possible states per qubit would significantly mitigate the BT attack. This is a primary reason why this paper develops the PM attack.

For protection against the PM attack, we can gain insights from the theoretical analysis. Theorem 3 indicates that the complexity of N should be $O\left(n^5 f^{-1} \epsilon^{-4} \ln^2(n\eta^{-1})\right)$ for good performance. However, note that it is proportional to n raised to the power of 5. Consequently, increasing n would be an effective protection strategy. For example, if $n = 100$, the coefficient becomes 10^{10}. In this case, while it may only take one shot to counterfeit as many quantum money bills as desired, the time cost is unacceptable. With additional measures like expiration time, we can effectively prevent the PM attack.

5 CONCLUSION

Wiesner's original private-key quantum money scheme, ingeniously leveraging the no-cloning principle, represented a foundational step towards achieving unconditionally secure cryptographic primitives. The initial promise of unforgeability was rooted in the inherent quantum difficulty of duplicating unknown states tied to the bank's secret key. However, as the comprehensive analyses provided by Molina et al. (2012) and Nagaj et al. (2016) vividly demonstrate, translating this fundamental quantum principle into a provably robust and practical security protocol for private-key money is a complex endeavor, critically dependent on the scope and nature of the security proofs considered.

The work of Molina et al. (2012) furnished crucial security proofs by delivering a quantitative understanding of the scheme's baseline resilience. Their analysis focused on non-adaptive "simple counterfeiting" attacks, where an attacker, isolated from the bank during the forgery process, attempts to duplicate a private-key banknote. By establishing optimal success probabilities—such as $(3/4)^n$ for Wiesner's original proposal and providing a lower bound of $2/(d+1)$ for counterfeiting d-dimensional private-key qudit systems—they offered concrete proof of the exponential difficulty confronting such an adversary. This line of proof underscores the inherent cryptographic strength derived from the quantum nature of the private-key encoding when the attacker operates under a restricted, non-interactive model. Their findings provide a vital security proof of the scheme's robustness against a specific, well-defined threat.

In stark contrast, the research by Nagaj et al. (2016) provided a different kind of security proof—a proof of vulnerability—by shifting the focus to the bank's operational procedures and an adaptive attacker model. Their investigation into a "strict testing" regime, a scenario where the bank's protocol involves returning valid private-key banknotes to the user, exposed critical security flaws. The adaptive attack strategies they proposed, which cleverly employ concepts like bomb-testing and protective measurements, demonstrated that an attacker could interactively query the bank's verification system. This interaction allows the attacker to progressively learn the secret quantum state corresponding to the bank's private key for that note, ultimately leading to a complete break of the scheme's unforgeability. This work powerfully proves that even private-key protocols secured by fundamental quantum laws can be compromised if the broader system implementation allows for exploitable feedback loops and information leakage through interaction.

Synthesizing these two distinct approaches to security proofs illuminates a critical lesson: the security of private-key quantum money, like Wiesner's, cannot be assessed solely on the quantum encoding or the no-cloning theorem in isolation. A comprehensive security proof must holisti-

cally consider the operational context, the precise details of the bank's interaction protocols, and the assumed capabilities of the adversary. While the no-cloning theorem provides a strong starting point for private-key systems, practical, provable unforgeability necessitates meticulous protocol design that anticipates and mitigates a wide spectrum of potential attack vectors. Specifically for Wiesner-like private-key schemes, a key implication for achieving stronger security proofs against adaptive attackers is that any secure implementation must likely preclude the return of the exact same quantum state after validation; instead, validated notes might need to be replaced with fresh, independently generated ones to break the chain of adaptive information gathering.

The insights derived from the security proofs presented by Molina et al. (2012) and the proofs of insecurity under specific protocols by Nagaj et al. (2016) chart the ongoing evolution in our understanding of quantum cryptographic security. The marked contrast between the $(3/4)^n$ proven security against simple non-adaptive attacks and the proven complete vulnerability under specific adaptive scenarios underscores the paramount importance of rigorously defining the attacker model and the full protocol specification when constructing and analyzing security proofs for private-key quantum money. Future research must continue this trajectory, exploring more sophisticated attacker models, the impact of noise, and the nuances of practical implementation to realize the full potential of provably secure quantum cryptographic primitives.

REFERENCES

Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975.

Andrzej Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

Paul Kwiat, Harald Weinfurter, Thomas Herzog, Anton Zeilinger, and Mark A. Kasevich. Interaction-free measurement. *Phys. Rev. Lett.*, 74:4763–4766, Jun 1995. doi: 10.1103/PhysRevLett.74.4763. URL `https://link.aps.org/doi/10.1103/PhysRevLett.74.4763`.

Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. *arXiv preprint arXiv:1202.4010v1 [quant-ph]*, 2012.

Daniel Nagaj, Or Sattath, Aharon Brodutch, and Dominique Unruh. An adaptive attack on Wiesner's quantum money. *arXiv preprint arXiv:1404.1507v4 [quant-ph]*, 2016.

Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.

Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299 (5886):802–803, 1982.