Quantum Lightning: Intuition, Construction, and the Limits of Public-Key Money

Author:

Juncheng Ding, Tian Ariyaratrangsee, Xiaoyang Zheng

Final Report for Phys-C191A, UC Berkeley

date: December 5, 2025

Abstract

Quantum money leverages the no-cloning theorem to provide unclonable digital currency [1]. While private-key schemes rely on trusted authorities, public-key quantum money enables anyone to verify banknotes but introduces new challenges. Zhandry's *quantum lightning* [5] strengthens public-key security by requiring that no efficient adversary can produce two valid states with the same serial number.

This report outlines the intuition behind quantum lightning—particularly the degree-2 polynomial construction based on the Non-Affine Multi-Collision Resistance (NAMCR) assumption [5]—and analyzes a fundamental limitation of all public-key quantum money: public verification inevitably enables unbounded generation, leading to unavoidable inflation. We discuss why this limitation is inherent and survey potential approaches to mitigating supply expansion.

Contents

1 Introduction

Quantum money uses quantum states as banknotes, whose security relies on the no-cloning theorem: valid notes cannot be copied without destroying the state. In *private-key* schemes, only the issuer can verify authenticity using secret information. In contrast, *public-key quantum money* allows anyone to verify a banknote, making security significantly more difficult since verification must be public while counterfeiting remains infeasible.

Quantum lightning, introduced by Zhandry, is a strong form of public-key quantum money. Each "bolt" is a quantum state that comes with a publicly verifiable serial number, and it should be computationally impossible to generate two distinct bolts sharing the same serial number. This "no double-strike" property captures a powerful notion of unforgeability and motivates new constructions based on quantum-resistant hash assumptions.

This work provides a brief introduction to these concepts and examines the core ideas underlying quantum lightning schemes.

2 Motivation for Quantum Money

The motivation for quantum money originates from the fact that quantum states cannot, in general, be cloned. Formally, the no-cloning theorem states:

Theorem 2.1 (No-Cloning Theorem [1])**.** *There exists no completely positive trace-preserving (CPTP) map $\mathcal{C}$ satisfying*

$$\mathcal{C}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| \quad \textit{for all } |\psi\rangle.$$

This physical constraint suggests that a quantum state may serve as an unclonable certificate of validity—an idea first captured in Wiesner's original conception of quantum money [1].

2.1 Wiesner's Private-Key Quantum Money

Definition 2.2 (Wiesner's Scheme [1, 2])**.** A Wiesner banknote consists of a classical serial number s and a quantum state

$$|\$_s\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle, \quad |\psi_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}.$$

The bank privately stores a classical database mapping

$$s \mapsto (\text{basis choices } b_i).$$

Verification consists of measuring each qubit in its designated basis:

$$\mathsf{Ver}_{\text{bank}}(\rho, s) = \begin{cases} 1 & \text{if measurements match } b_i, \\ 0 & \text{otherwise.} \end{cases}$$

This construction achieves information-theoretic security but is fundamentally private-key: verification requires secret information.

2.2 Public-Key vs. Private-Key Quantum Money

Public-key quantum money was introduced to eliminate the need for trusted verification [3, 4].

Definition 2.3 (Public-Key Quantum Money)**.** A public-key quantum money scheme consists of:

- a public verification circuit V,
- such that $V(\rho) = 1$ for valid notes, and
- it is computationally infeasible for any QPT adversary to prepare ρ' with $V(\rho') = 1$.

Formally, if $\mathcal{G}$ is the public generation procedure, a scheme is sound if no adversary can produce

$$\rho_1, \rho_2 \quad \text{such that} \quad \mathsf{Ver}(\rho_1) = \mathsf{Ver}(\rho_2) = 1$$

except with negligible probability.

This definition mirrors unforgeability in classical signature schemes but with quantum states as certificates.

2.3 Why Classical Public-Key Verification is Desirable

A classical verification algorithm enables verification without quantum devices [3]. The goal is:

$$\text{Quantum banknote } \rho \quad \xrightarrow{\text{measure}} \quad y \quad \xrightarrow{V(\cdot)} \quad \text{valid/invalid.}$$

This enables circulation without trusted authorities and aligns quantum money with public-key cryptographic primitives.

2.4 Problems with Earlier Approaches

Earlier constructions encountered several difficulties:

Oracle-based constructions. Schemes secure only relative to a black-box oracle [3] cannot yield concrete instantiations.

The Aaronson–Christiano subspace scheme. The candidate [4] relied on obfuscating membership in a hidden subspace $S \subseteq \mathbb{F}_2^n$. A banknote was a uniform superposition

$$|\$\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle,$$

and verification tested that

$$x \in S \quad \text{and} \quad Hx \in S^{\perp},$$

where H is the Hadamard transform.

However, follow-up work [6] showed that the "subspace-hiding obfuscation" leaked information about S, enabling forgery.

Structural leakage in general. Public verification often reveals exploitable algebraic structure. This motivates Zhandry's quantum lightning framework [5], which avoids such leakage by using hash-based assumptions.

3 Quantum Lightning: Zhandry's Contribution

Zhandry formalizes *quantum lightning* [5] as a public procedure for generating quantum states that satisfy a strong uniqueness property: it should be computationally infeasible for any efficient adversary to produce two valid states — called *bolts* — that verify to the same classical serial number. This goes beyond the ordinary no-cloning theorem, which prohibits duplicating a *given* unknown quantum state but does not preclude an adversary from generating two different states that nonetheless pass verification.

3.1 Definition: Bolts and Strong Unclonability

Definition 3.1 (Quantum Lightning Scheme [5])**.** A quantum lightning scheme consists of two public algorithms:

$$\mathsf{Storm}(1^{\lambda}) \to |\psi\rangle, \qquad \mathsf{Ver}(\rho) \to s \in \{0,1\}^* \cup \{\perp\}.$$

A state ρ is a valid bolt if

$$\Pr\left[\mathsf{Ver}(\rho) \neq \bot\right] \geq 1 - \mathrm{negl}(\lambda).$$

The security notion, called *uniqueness*, requires that no QPT adversary can produce two (possibly entangled) states (ρ_1, ρ_2) satisfying

$$\mathsf{Ver}(\rho_1) = \mathsf{Ver}(\rho_2) = s \neq \bot.$$

Formally,

$$\Pr\left[\begin{array}{c}(\rho_1, \rho_2) \leftarrow \mathcal{A} \\ \mathsf{Ver}(\rho_1) = \mathsf{Ver}(\rho_2) \neq \bot\end{array}\right] = \mathrm{negl}(\lambda).$$

3.2 Why Quantum Lightning is Stronger Than Traditional Quantum Money

Proposition 3.2 (Lightning vs. Public-Key Quantum Money [5])**.** *In public-key quantum money, unforgeability requires that no adversary can produce a new valid banknote:*

$$\mathsf{Ver}(\rho') = 1.$$

However, this does not *prevent producing two distinct states ρ_1, ρ_2 such that*

$$\mathsf{Ver}(\rho_1) = \mathsf{Ver}(\rho_2).$$

Quantum lightning strengthens this by requiring full collision resistance:

$$\textit{hard to find any } \rho_1, \rho_2 \textit{ with } \mathsf{Ver}(\rho_1) = \mathsf{Ver}(\rho_2) \neq \bot.$$

This stronger guarantee is essential for applications such as verifiable randomness or decentralized ledgers, where even one duplicated serial number constitutes a complete break.

3.3 The Win-Win Framework

Before describing the construction, it is essential to understand Zhandry's "win-win" framework. Consider a collision-resistant hash function H secure against quantum adversaries. Zhandry shows that H must fall into one of two categories [5, 7]:

Theorem 3.3 (Win–Win Dichotomy)**.** *For any hash function H:*

1. *H is* collapsing *[7]— meaning it is computationally infeasible to distinguish whether only the output register was measured or both input and output registers were measured; or*

2. *H is* not collapsing*, in which case H can be used to construct quantum lightning without additional assumptions [5].*

The degree-2 polynomial candidate is believed to fall into case (2), because the uniform superposition of all preimages $|\psi_y\rangle$ is distinguishable from a random preimage state $|x\rangle$.

3.4 Intuition: Why "Lightning Never Strikes Twice"

The phrase captures the core intuition behind uniqueness. Both Storm and Ver are public, so an adversary may attempt to engineer a specific serial number. Uniqueness requires that:

No efficient adversary can ever produce two bolts with the same serial number.

When a bolt ρ is generated, the verifier outputs a classical fingerprint

$$s = \mathsf{Ver}(\rho),$$

and reproducing another state ρ' with the same fingerprint is assumed computationally infeasible.

This requirement is strictly stronger than the no-cloning theorem:

$$|\psi\rangle \not\mapsto |\psi\rangle \otimes |\psi\rangle,$$

but quantum lightning additionally prohibits:

$$\exists\, \rho_1 \neq \rho_2 : \ \mathsf{Ver}(\rho_1) = \mathsf{Ver}(\rho_2).$$

The intuition is that each bolt contains hidden combinatorial structure—recoverable by verification but impossible to regenerate without solving a computationally hard problem such as producing a large structured multi-collision set. Hence, "lightning never strikes the same serial number twice."

4 The Degree-2 Polynomial Construction

Zhandry's concrete quantum lightning construction [5] uses degree-2 polynomial hash functions over $\mathbb{F}_2$. Crucially, these hash functions are *not* collision-resistant in the standard sense. Instead, security relies on a weaker but plausible assumption about the hardness of finding *non-affine multi-collisions* (NAMCR).

4.1 The Hash Function Family

Definition 4.1 (Degree-2 Polynomial Hash Family [5]). Let $A_i \in \{0,1\}^{m\times m}$ be random upper-triangular matrices for $i = 1, \dots, n$. Define:

$$f_{\mathcal{A}}(x) = (x^\top A_1 x, \dots, x^\top A_n x) \in \mathbb{F}_2^n.$$

Why degree-2 polynomials are NOT collision-resistant. As shown by Ding–Yang and Applebaum et al. [8,9], these functions admit efficient collision-finding attacks. Given a random offset Δ, one can find a collision pair $(x, x-\Delta)$ by solving a *linear* system of n equations in m unknowns, which has a solution when $m \geq n$. More generally:

Proposition 4.2 (Known Collision Properties [8,9]). *For $m \approx kn$:*

- *One can efficiently find $k+1$* affine *collisions.*
- *One can efficiently find $k+1$* non-affine *collisions.*

However, no known attacks can produce $2(k+1)$ non-affine collisions.

This gap is essential for Zhandry's construction.

4.2 The NAMCR Assumption

Proposition 4.3 (Non-Affine Multi-Collision Resistance (NAMCR) [5]). *Let $k = \mathrm{poly}(n)$ and $m < (k+\frac{1}{2})n$. Then $f_{\mathcal{A}}$ is $2(k+1)$-NAMCR, meaning:*

$$\Pr\left[(x_1, \dots, x_{2k+2}) \text{ collide in } f_{\mathcal{A}} \text{ and are non-affine}\right] = \mathrm{negl}(\lambda).$$

Affine collisions are easy, but generating *large, non-affine* collision sets is conjectured to be hard.

4.3 The Bolt Structure: Why Multiple Copies Are Necessary

Proposition 4.4 (Insecurity of Single Superposition Copy [5]). *A single state*

$$|\psi_y\rangle = \frac{1}{\sqrt{|S_y|}} \sum_{x:f_{\mathcal{A}}(x)=y} |x\rangle$$

is not secure. Known attacks generate $k+1$ distinct preimages of the same y, enabling $|\psi_y\rangle^{\otimes(k+1)}$.

Thus a bolt must contain multiple tensor copies:

Definition 4.5 (Bolt Structure). A bolt for serial number y is:

$$\mathbf{B}_y := |\psi_y\rangle^{\otimes(r+1)},$$

where $r \approx k$ ensures honest generation is feasible but producing $2(r+1)$ copies would violate NAMCR.

4.4 Verification: Mini-Verification and Span Membership

Verification consists of two stages:

Mini-verification. For each of the $(k+1)$ components, the verifier checks whether the state lies in the span

$$\mathrm{Span}\{|\psi_z\rangle : z \in \{0,1\}^n\}.$$

Equivalently, the verifier tests membership in the span of

$$|\phi_r\rangle = \frac{1}{2^{m/2}} \sum_x (-1)^{r \cdot f_{\mathcal{A}}(x)} |x\rangle.$$

Proposition 4.6 (Mini-Verification Soundness [5]). *The mini-verification procedure reconstructs linear constraints from the degree-2 structure and rejects any state outside the valid span with overwhelming probability.*

Consistency check. The verifier measures $f_{\mathcal{A}}(x)$ on each component to obtain $y_1, \ldots, y_{k+1}$ and accepts iff all are equal.

Proposition 4.7 (Collision Implies NAMCR Violation [5]). *If two bolts with the same serial number y pass verification, the post-measurement state equals $|\psi_y\rangle^{\otimes 2(k+1)}$, whose measurement reveals $2(k+1)$ preimages of y. Such a set is non-affine with overwhelming probability, contradicting NAMCR.*

4.5 Summary: The Security Argument

Theorem 4.8 (Security of the Degree-2 Lightning Construction [5]). *Security follows from:*

1. *$f_{\mathcal{A}}$ is not collision-resistant (affine attacks exist).*
2. *NAMCR (Assumption 4.3) forbids producing $2(k+1)$ non-affine collisions.*
3. *A single $|\psi_y\rangle$ is insecure; bolts require $(k+1)$ copies.*
4. *Verification forces any valid bolt to encode $(k+1)$ preimages of a unique y.*
5. *Any adversary producing two bolts yields $2(k+1)$ non-affine collisions, violating NAMCR.*

Thus, this is the first concrete quantum lightning scheme relying on a plausible classical cryptographic assumption.

4.6 Zhandry's Instantiation Using Multi-Collision-Resistant Hash Functions

The family of degree-2 polynomials:

$$H_A(x) = x^\top Ax$$

naturally produces multi-collisions. Zhandry's construction [5] requires only that producing *large, structured, non-affine* collision sets is hard.

Given a collision set:

$$S = \{x_1, \dots, x_k\}, \quad H_A(x_i) = y,$$

one obtains a superposition over an affine subspace whose structure cannot be succinctly encoded.

4.7 The Idea of Incompressibility

Definition 4.9 (Incompressibility [5]). Let

$$|\psi_y\rangle = \frac{1}{\sqrt{|S_y|}} \sum_{x \in S_y} |x\rangle, \qquad S_y = \{x : H_A(x) = y\}.$$

The set S_y is incompressible if no QPT algorithm outputs a poly-size description d from which a second algorithm can recover a subset $S'_y \subseteq S_y$ of superpolynomial size.

If such compression were possible, one could construct another bolt for the same y, violating uniqueness.

Proposition 4.10 (Incompressibility Prevents Duplication [5]). *Because S_y is exponentially large and highly structured, reproducing its combinatorial geometry is computationally infeasible. Hence producing two bolts with the same serial number is impossible under NAMCR.*

In summary, collision geometry induced by degree-2 polynomials is too "spread out" to be compressed. This ensures that "lightning never strikes the same serial number twice."

5 The Inflation Problem: Unlimited Generation in Public-Key Quantum Money

The previous sections established that quantum lightning prevents *cloning*—no adversary can produce two bolts with the same serial number. However, this security guarantee does not address a distinct and equally important question: *can we limit how many bolts are created in total?* As we now demonstrate, the answer is fundamentally negative for any public-key scheme.

5.1 The Core Theorem: Unbounded Generation

The central result of this section shows that unlimited generation is not a bug but an inherent feature of public-key quantum money.

Theorem 5.1 (Unbounded Generation). *Let* $(\mathsf{Gen}, \mathsf{Ver})$ *be any public-key quantum money scheme with correctness error ϵ. For any polynomial $N = N(\lambda)$, there exists a QPT algorithm producing N valid, pairwise-distinct banknotes with probability at least* $(1 - \epsilon)^N - \mathrm{negl}(\lambda)$.

Proof. The algorithm simply invokes $\mathsf{Gen}(1^\lambda)$ independently N times. By correctness, each state passes verification with probability $\geq 1 - \epsilon$.

For distinctness, we use the fact that uniqueness implies high min-entropy of serial numbers:

$$H_\infty(\mathsf{Ver}(\mathsf{Gen}(1^\lambda))) \geq n(\lambda) - O(\log \lambda).$$

The collision probability among $N = \text{poly}(\lambda)$ serial numbers is therefore:

$$\binom{N}{2} \cdot 2^{-n+O(\log \lambda)} = \text{negl}(\lambda).$$

□

5.2 Why This Is Unavoidable: Public Verification Implies Public Generation

One might hope that some clever protocol design could restrict who can generate money. The following proposition shows this is impossible in any public-key setting.

Proposition 5.2 (Public Generation is Inherent)**.** *In any public-key quantum money scheme where* Ver *is public, any party can efficiently generate valid banknotes.*

Proof. The generation algorithm Gen must be publicly specified—otherwise, how could the original issuer produce valid notes? Since Gen runs in polynomial time using only public operations (Hadamard gates, controlled unitaries, measurement), any party with a quantum computer can execute it. This contrasts fundamentally with private-key schemes, where $\mathsf{Gen}_{\text{private}}(k, s)$ requires a secret key k held only by the bank. □

5.3 The Cloning-Generation Dichotomy

Combining the above results, we see a fundamental asymmetry in quantum money security:

- **Targeted generation (Cloning) is intractable.** To clone a bolt with serial number y, an adversary is forced to solve a specific instance of the multi-collision problem. Specifically, they must produce a fresh batch of $k + 1$ tensor copies of $|\psi_y\rangle$ to pass verification. Combined with the original bolt, this would yield $2(k+1)$ colliding inputs for y. The NAMCR assumption posits that finding such a large collision set for a *fixed* output y is computationally impossible.
- **Random generation (Minting) is trivial.** The generation algorithm Storm operates without a target constraint. It samples random inputs which map to a random output y'. Because the range of the hash function is exponentially large (2^n), the probability of hitting any previously generated serial number is negligible. Thus, generating *new* money requires no collision-finding effort; it merely requires running the forward circuit, which is efficient for anyone.

The uniqueness property guarantees that for any QPT adversary:

$$\Pr\left[\mathsf{Ver}(\rho_1) = \mathsf{Ver}(\rho_2) \neq \perp\right] = \mathrm{negl}(\lambda).$$

But this says nothing about generating N *distinct* valid notes, which succeeds with overwhelming probability by Theorem 5.1.

In economic terms: quantum lightning perfectly prevents counterfeiting (copying existing money) but provides no mechanism to prevent inflation (creating new money). Any party can become a "mint" simply by running the public Storm algorithm.

6 Prospective Approaches to Supply Limitation

Several cryptographic approaches could potentially introduce supply constraints:

Hash-based difficulty. Require $H(y) < T$ for the serial number, converting generation into probabilistic search. Grover's algorithm provides $O(2^{d/2})$ speedup over classical $O(2^d)$ trials.

Verifiable Delay Functions. VDFs certify that time T has elapsed, preventing parallel mining. Quantum security of current VDF constructions remains open.

Quantum memory bounds. Exploit physical scarcity of coherent quantum storage. Verification of actual storage (vs. regeneration) is an open problem.

Entanglement-based certificates. Use monogamy of entanglement to bound supply, but this reintroduces trusted authorities.

Remark 6.1 (Open Problem)**.** Can we construct public-key quantum money where generation (not just cloning) is computationally hard? This requires making the search problem "Find ρ such that $\mathsf{Ver}(\rho) \neq \perp$" hard while keeping verification efficient.

7 Conclusion

We have analyzed the fundamental tension in public-key quantum money between *unclonability* and *unlimited generation*:

- **Cloning is hard:** The no-cloning theorem combined with NAMCR ensures duplicating valid bolts is infeasible.
- **Generation is easy:** Public verification implies public generation—any party can produce fresh bolts in polynomial time.
- **Inflation is inevitable:** Unlimited generation leads to unbounded supply, undermining scarcity-based currency applications.

This asymmetry implies that public-key quantum money, despite its strong anti-counterfeiting guarantees, cannot serve as a scarcity-based currency: any party can generate polynomially many valid coins, leading to unbounded inflation. While approaches such as hash-based difficulty or VDFs can slow generation, none fundamentally resolve this limitation.

This dichotomy is inherent to any public-key scheme. Quantum lightning shows that "lightning never strikes the same state twice," but also that lightning can strike *anywhere*. Constructing public-key quantum money where generation itself is hard remains a central open problem in quantum cryptography.

References

[1] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983. (Original manuscript circa 1970.)

[2] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology: Proceedings of Crypto '82*, pp. 267–275, 1982.

[3] S. Aaronson, "Quantum copy-protection and quantum money," in *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC)*, pp. 229–242, 2009.

[4] S. Aaronson and P. Christiano, "Quantum money from hidden subspaces," in *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 41–60, 2012.

[5] M. Zhandry, "Quantum lightning never strikes the same state twice. Or: quantum money from cryptographic assumptions," *Journal of Cryptology*, vol. 34, no. 1, article 8, 2021. (arXiv:1711.02276)

[6] A. Molina, T. Vidick, and J. Watrous, "Optimal counterfeiting attacks and generalizations for Wiesner's quantum money," in *Proceedings of the 7th Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC)*, pp. 45–64, 2012.

[7] D. Unruh, "Computationally binding quantum commitments," in *Advances in Cryptology – EUROCRYPT 2016*, pp. 497–527, 2016.

[8] Y. Ding and J. Yang, "Cryptanalysis of quadratic hash functions over $\mathbb{F}_2$," (unpublished note / known-lineage reference used in Zhandry's paper). [Note: Insert actual publication info if desired.]

[9] B. Applebaum, E. Haramaty, and Y. Ishai, "Polynomial decomposition of multivariate quadratic hash functions," *Cryptology ePrint Archive*, 2016.

[10] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, Version 0.5, 2020. Available at: `https://toc.cryptobook.us/`

[11] S. Aaronson, "Introduction to Quantum Information Science," Lecture Notes, 2023.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. Available at: `https://bitcoin.org/bitcoin.pdf`