Quantum Walks and Application to Quantum Money

Ali Mousavi

April 2025

Contents

Abstract

This thesis explores the foundations of quantum computation, focusing on quantum walks and their application to quantum money. Quantum walks, particularly continuous-time quantum walks based on group actions, serve as a powerful computational tool with applications in search algorithms and cryptographic protocols. We examine their mathematical structure and their advantages over classical random walks, emphasizing their efficiency in state evolution and probability distribution spreading. As a part of this work, we examine efficient implementations of transforms such as the Quantum Fourier Transform (QFT) and the Quantum Hartley Transform (QHT), analyzing their role in encoding quantum states for secure cryptographic applications. In particular, we discuss a novel instantiation of a quantum money scheme based on QHT, leveraging its unique properties for improved security and efficiency. To ensure the robustness of this quantum money scheme, we develop a verification mechanism utilizing quantum walks. Unlike previous approaches, which rely on standard quantum state measurements, our method employs continuous-time quantum walks to authenticate quantum money, preventing counterfeiting while maintaining computational feasibility. Additionally, we present a detailed discussion on the efficient implementation of this scheme, including optimized circuit designs and error mitigation strategies.

Chapter 1

Introduction

Quantum money, first introduced in a seminal paper by Wiesner [29], is a form of currency represented by quantum states. Unlike classical money, an ideal quantum bill cannot be counterfeited due to the no-cloning theorem of quantum mechanics, which prohibits making an identical copy of an unknown quantum state. Wiesner's original scheme (now termed a *private-key quantum money* scheme) had significant practical drawbacks: it required the issuing bank's secret key to verify each banknote, meaning the bank had to be involved in every transaction. This reliance on the bank for verification severely limits the usability of private-key quantum money schemes.

In 2009, Aaronson [1] proposed the first *public-key quantum money* scheme, in which anyone can verify a quantum banknote while only the bank can mint (issue) new valid banknotes. Public-key quantum money removes the transactional bottleneck of involving the bank every time. Aaronson's specific scheme was later broken by Lutomirski et al. [24]. In the years since, several alternative public-key quantum money constructions have been explored [2, 17, 30, 19, 20, 23, 31]. However, each of these proposals has either been broken by further cryptanalysis [14, 26, 7, 23] or relies on unconventional cryptographic assumptions, making their security or practicality questionable.

Quantum Money from Group Actions and the Fourier Transform. A promising candidate for secure public-key quantum money based on more standard assumptions was recently proposed by Zhandry [31]. In Zhandry's scheme, the core idea is to use an abelian group action as the foundation for the quantum state. Each money state (quantum banknote) is prepared as a *group-action Fourier state*, and the corresponding serial number is an element of the underlying group (we will elaborate on these terms in later chapters). The verification algorithm in this scheme uses a group-action phase kickback routine to extract the serial number from the quantum banknote and check its validity. Doliskani [15] later proved that Zhandry's scheme is secure in the generic group action model, providing evidence for its security under well-defined assumptions.

This Work – Motivation and Contributions. In this thesis, we adapt Zhandry's group-action quantum money scheme by replacing its use of the Quantum Fourier Transform with the *Quantum Hartley Transform* (QHT) over finite abelian groups. The motivation behind this substitution is multifold. First, using the Hartley transform causes the banknotes to have *real* amplitudes instead

of complex amplitudes. We believe this shift from complex to real quantum states may offer both computational and theoretical advantages. For example, certain mathematical identities hold for any two real orthonormal bases that do not generally hold for complex bases; such differences can affect the properties of quantum states and were a barrier in prior analyses (indeed, an attempted "quantum lightning" construction in [31] failed due to properties of complex phases that do not arise with real amplitudes). Beyond this specific context, our work is a first step toward employing real-valued quantum transforms in quantum cryptography and quantum algorithms. To the best of our knowledge, this is the first significant quantum cryptographic construction that makes essential use of the quantum Hartley transform. We hope that exploring real-amplitude quantum states will inspire further research into new quantum algorithms and optimizations for real-valued transforms.

We now summarize our main contributions:

- We propose a new **public-key quantum money scheme** based on abelian group actions and the quantum Hartley transform. This scheme is an adaptation of Zhandry's group-action money scheme, modified to output real-amplitude quantum states.
- When using the Hartley transform instead of the Fourier transform, the original verification method from Zhandry's scheme is no longer straightforward and requires the use of twists to function correctly. Instead, we offer a more direct verification approach based on quantum walks.
- We show that the serial number associated with a money state (which is a hidden group element) can be efficiently computed from the quantum state. In particular, we develop a **continuous-time quantum walk algorithm** to extract the serial number of a given banknote state. This algorithm leverages the structure of the group action and the spectral properties of an associated Cayley graph. Our method demonstrates that one can recover the hidden group element (serial) with high success probability, which not only underpins the new verification technique but is also of independent interest.
- In the course of our construction, we introduce a new algorithm for efficiently implementing the **quantum Hartley transform** and related real transforms. We present a recursive technique that exploits the structure of the Hartley transform, yielding a lower gate complexity than prior approaches in the literature.

In summary, our work combines ideas from quantum cryptography (public-key quantum money), quantum walks, and quantum signal processing (Hartley and related transforms) to create a novel and potentially practical quantum money scheme.

Thesis Organization. The remainder of this thesis is organized as follows. In **Chapter 2**, we provide background on the basics of quantum computation and the theory of group actions, including the concept of cryptographic group actions which underlie our money scheme. **Chapter 3** covers quantum walks, both continuous-time and discrete-time, outlining their differences and importance in quantum algorithms. In **Chapter 4**, we apply the quantum walk framework to

group actions: we describe how a continuous-time quantum walk on a group action can be simulated efficiently, a crucial step for our serial number extraction algorithm. **Chapter 5** details the quantum money scheme itself and the role of the Hartley transform in its construction. We explain how the scheme is formulated and discuss the advantages and challenges introduced by using the Hartley transform. Finally, **Chapter 6** presents the verification algorithm for the Hartley-based quantum money. This chapter shows how we use quantum walks (as developed in Chapter 4) to reliably verify banknotes and compute their serial numbers, thereby addressing the verification issues that arose from the use of real amplitudes.

Chapter 2

Background of Quantum Computation and Group Actions

2.1 Quantum Computation Basics

Quantum computation operates on information stored in quantum states. The fundamental unit of quantum information is the *qubit*, which, unlike a classical bit, can exist in a superposition of basis states. A qubit is described by a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (in Dirac notation), where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. A system of n qubits resides in a 2^n-dimensional Hilbert space and its state can be a superposition of all 2^n basis states $|b_1 b_2 \cdots b_n\rangle$.

Computation is carried out by unitary transformations on these states. A quantum algorithm is typically a sequence of quantum gates (unitary operators) applied to an initial state (usually a simple basis state like $|00\cdots0\rangle$), followed by a measurement of some qubits to obtain a classical result. A crucial aspect of quantum computation is that certain transformations—such as the Fourier transform over an N-element group—can be implemented very efficiently on a quantum computer (in $\text{poly}(\log N)$ time), whereas their classical counterparts might require $\text{poly}(N)$ time.

2.1.1 The Quantum Fourier Transform

One example important to this work is the **quantum Fourier transform** (QFT). For an abelian group G of order N, the QFT is the unitary map

$$|g\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{h \in G} \chi_h(g)\, |h\rangle,$$

where $\{\chi_h\}$ are the characters (complex exponential homomorphisms) of G. When $G = \mathbb{Z}_N$ (the integers mod N), the QFT takes $|j\rangle$ to $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$.

Let $G \cong \mathbb{Z}_{N_1} \oplus \cdots \oplus \mathbb{Z}_{N_k}$ be a decomposition of G. The character $\chi(a, x)$ is then given by

$$\chi(a, x) = \omega_{N_1}^{a_1 x_1} \cdots \omega_{N_k}^{a_k x_k}, \quad \text{where } \omega_M = \exp(2\pi i/M).$$

The Fourier transform of a function $f : G \to \mathbb{C}$ is given by

$$\hat{f}(a) = \frac{1}{\sqrt{|G|}} \sum_{x \in G} \chi(a, x) f(x),$$

and the QFT of a quantum state $\sum_{g \in G} f(g) |g\rangle$ is $\sum_{x \in G} \hat{f}(x) |x\rangle$.

Fourier Basis and Group Actions. For a regular group action $(G, X, *)$, define

$$\left|S^{(h)} * y\right\rangle = \frac{1}{\sqrt{|S|}} \sum_{g \in S} \chi(g, h) |g * y\rangle .$$

For fixed $x \in X$, we obtain two orthonormal bases of $\mathbb{C}^X$: the standard basis $\{|x\rangle : x \in X\}$, and the Fourier basis

$$\left|G^{(h)} * x\right\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi(g, h) |g * x\rangle .$$

These states are eigenstates of the action unitary $U_k : |y\rangle \mapsto |k * y\rangle$:

$$U_k \left|G^{(h)} * x\right\rangle = \chi(-k, h) \left|G^{(h)} * x\right\rangle .$$

The cmpIndex Algorithm. Given a state $\left|G^{(h)} * x\right\rangle$, one can recover h using phase kickback. Starting from $\left|G^{(h)} * x\right\rangle |0\rangle$, apply:

- QFT to second register,
- Controlled unitary $\sum_{k \in G} U_k \otimes |k\rangle \langle k|$,
- Inverse QFT to second register.

This yields $\left|G^{(h)} * x\right\rangle |h\rangle$, extracting h efficiently.

2.1.2 The Quantum Hartley Transform

Another concept we use is the **quantum Hartley transform** (QHT), which replaces complex exponentials with real sinusoidal kernels.

Definition. For $G = \mathbb{Z}_N$, define

$$\mathrm{QHT}_N : |a\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} cas\left(\frac{2\pi a y}{N}\right) |y\rangle , \quad \text{where } cas(x) = \cos(x) + \sin(x).$$

For general abelian $G = \mathbb{Z}_{N_1} \oplus \cdots \oplus \mathbb{Z}_{N_k}$, the Hartley transform of $f : G \to \mathbb{R}$ is

$$\mathrm{QHT}_G(f)(a) = \frac{1}{\sqrt{|G|}} \sum_{y \in G} cas(2\pi\langle a, \alpha(y)\rangle) f(y), \tag{2.1}$$

where $\alpha(y) = y_1/N_1 + \cdots + y_k/N_k$.

Unitary Equivalence. Using the identity

$$cas(2\pi\langle a, \alpha(y)\rangle) = \frac{1-i}{2}\chi(a, y) + \frac{1+i}{2}\chi(-a, y),$$

we obtain:

$$\mathrm{QHT}_G = \frac{1-i}{2}\,\mathrm{QFT}_G + \frac{1+i}{2}\,\mathrm{QFT}_G^*, \tag{2.2}$$

showing that $\mathrm{QHT}_G^2 = 1$ and hence the QHT is unitary.

Quantum Formulation. The quantum Hartley transform over G maps:

$$\sum_{x \in G} f(x)\,|x\rangle \mapsto \sum_{a \in G} \mathrm{QHT}_G(f)(a)\,|a\rangle\,.$$

Because the cas function is real-valued, the resulting amplitudes remain real—a fact that plays a crucial role in real-amplitude quantum protocols.

2.2 Group Actions in Cryptography

At the heart of our quantum money scheme is the notion of a group action. A **group action** of a group G on a set X is a function $*\colon G \times X \to X$ that satisfies two properties: (1) the identity element $e \in G$ acts trivially on every $x \in X$ ($e * x = x$), and (2) the action is compatible with the group operation, meaning $g * (h * x) = (gh) * x$ for all $g, h \in G$ and $x \in X$. We will often denote the result of g acting on x by $g * x$ or simply gx when the action is clear from context.

The orbit of an element $x \in X$ under the action is the set $G * x = \{g * x : g \in G\} \subseteq X$. If there is exactly one orbit (i.e., $G * x = X$ for some x), the action is called *transitive*. If, in addition, no non-identity group element fixes any x (i.e., $g * x = x$ implies $g = e$), then the action is *free*. A group action that is both transitive and free is sometimes called a **regular action**. In a regular action, for any two elements $y, z \in X$, there is a unique group element g such that $g * y = z$. In other words, G acts like a permutation group that moves elements of X around, and knowing the starting and ending point uniquely determines the "move" g. In this case $|X| = |G|$, and we can think of X as essentially a copy of G with the group structure "hidden" by the action.

Group actions are ubiquitous in modern cryptography. A **cryptographic group action** is one where the action is easy to compute in the forward direction, but inverting the action (recovering g

from x and $g * x$) is computationally hard. This essentially functions as a one-way function: given x and g, it is easy to compute $y = g * x$, but given x and y it is infeasible to find g (except with negligible probability). One classical example is the discrete logarithm problem: consider the cyclic group $G = \mathbb{Z}_p^*$ (the multiplicative group of a prime field) acting on itself by exponentiation. Let $X = G$ and define $g * x = x^g \pmod{p}$ (treating group elements as integers). Here g is an exponent. This is a group action (in fact, just the group's own operation written differently), and computing $x^g \bmod p$ is efficient. However, given x and $y = x^g$, finding g requires solving a discrete log problem, which is believed to be hard for suitable choices of p. Thus, exponentiation can be viewed as a one-way group action.

Another prominent example comes from elliptic-curve cryptography: the action of an ideal class group on a set of elliptic curves. In schemes like CSIDH (Commutative Supersingular Isogeny Diffie–Hellman), an abelian group of ideal classes G acts on the set X of supersingular elliptic curves by isogeny (an isogeny is a structure-preserving map between curves). Starting from a curve x_0, one can efficiently compute $g * x_0$ (which is another elliptic curve) for any group element g, but given two curves x_0 and $x = g * x_0$, it is believed to be computationally hard to recover g. This hard problem is the foundation of isogeny-based cryptography. We refer to such G and X as a *cryptographic group action* pair.

Cryptographic group actions provide a natural platform for public-key quantum money schemes. In such schemes, the secret "serial number" of a quantum banknote can be an element $g \in G$, and the quantum state of the banknote can be some function of $g * x_0$ for a public base point $x_0 \in X$. The hardness of inverting the action (x_0 and $x = g * x_0$ do not easily reveal g) contributes to the security against counterfeiting, while the structure of the group action can be used to efficiently verify authenticity (as we will see with the Fourier or Hartley transform techniques).

We will assume throughout that we have a family of abelian group actions (G, X) that are cryptographically suitable: $|G|$ is large (growing with the security parameter), the action is efficiently computable, transitive and free (so $|X| = |G|$), and inverting the action is infeasible without the secret key. Such families are conjectured to exist (for example, the isogeny-based actions, and others discussed in cryptographic literature).

Finally, we note that working in the **generic group model** (or generic group *action* model) is a common theoretical approach to analyze security. In a generic model, the group elements are treated as black-box labels without exploiting any special algebraic structure beyond group axioms. Doliskani's proof of security for Zhandry's scheme [15] was in such a generic model for group actions, lending confidence that no "generic" attack can break the scheme. In this thesis, we focus on designing the scheme and algorithms at a high level and assume the underlying group action is secure; a detailed security proof is beyond our scope, though we rely on prior results for reassurance.

Chapter 3

Quantum Walks – Continuous and Discrete

Chapter 4

Simulating Group Action Quantum Walks

Chapter 5

Quantum Money and Hartley Transform

Chapter 6

Verification Algorithm Using Quantum Walks

Bibliography

[1] S. Aaronson, "Quantum Copy-Protection and Quantum Money," In Proc. of CCC, 2009.

[2] M. Zhandry, "Quantum Money from Modular Forms," In Proc. of CRYPTO, 2022.

[3] A. M. Childs, "Quantum Information Processing in Continuous Time," PhD Thesis, MIT, 2004.