A General Quantum Duality for Representations of Groups

with Applications to Quantum Money, Lightning, and Fire

John Bostanci[1], Barak Nehoran[2], and Mark Zhandry[3]

[1]Columbia University, New York, NY, USA
[2]Princeton University, Princeton, NJ, USA
[3]NTT Research, Sunnyvale, CA, USA

Abstract

Aaronson, Atia, and Susskind (2020) established that efficiently mapping between quantum states $|\psi\rangle$ and $|\phi\rangle$ is computationally equivalent to distinguishing their superpositions $\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$ and $\frac{1}{\sqrt{2}}(|\psi\rangle - |\phi\rangle)$. We generalize this insight into a broader duality principle in quantum computation, wherein manipulating quantum states in one basis is equivalent to extracting their value in a complementary basis. In its most general form, this duality principle states that for a given group, the ability to implement a unitary representation of the group is computationally equivalent to the ability to perform a Fourier extraction from the invariant subspaces corresponding to its irreducible representations.

Building on our duality principle, we present the following applications:

- Quantum money, which captures quantum states that are verifiable but unclonable, and its stronger variant, quantum lightning, have long resisted constructions based on concrete cryptographic assumptions. While (public-key) quantum money has been constructed from indistinguishability obfuscation (iO)—an assumption widely considered too strong—quantum lightning has not been constructed from any such assumptions, with previous attempts based on assumptions that were later broken. We present the first construction of quantum lightning with a rigorous security proof, grounded in a plausible and well-founded cryptographic assumption. We extend the construction of Zhandry (2024) from Abelian group actions to non-Abelian group actions, and eliminate Zhandry's reliance on a black-box model for justifying security. Instead, we prove a direct reduction to a computational assumption – the pre-action security of cryptographic group actions. We show how these group actions can be realized with various instantiations, including with the group actions of the symmetric group implicit in the McEliece cryptosystem.
- We provide an alternative quantum money and lightning construction from one-way homomorphisms, showing that security holds under specific conditions on the homomorphism. Notably, our scheme exhibits the remarkable property that four distinct security notions—quantum lightning security, security against both worst-case cloning and average-case cloning, and security against preparing a specific canonical state—are all equivalent.
- Quantum fire captures the notion of a samplable distribution on quantum states that are efficiently clonable, but not efficiently telegraphable, meaning they cannot be efficiently encoded as classical information. These states can be spread like fire, provided they are kept alive quantumly and do not decohere. The only previously known construction relied on a unitary quantum oracle, whereas we present the first candidate construction of quantum fire using a classical oracle.

Contents

1 Introduction

Let $|\psi_0\rangle, |\psi_1\rangle$ be two orthogonal quantum states, and let $|\phi_+\rangle$ be proportional to $|\psi_0\rangle + |\psi_1\rangle$ and $|\phi_-\rangle$ be proportional to $|\psi_0\rangle - |\psi_1\rangle$. The *Swap Complexity* of $|\psi_0\rangle$ and $|\psi_1\rangle$ is the size of the smallest circuit that maps $|\psi_0\rangle$ to $|\psi_1\rangle$ and vice versa. Meanwhile, the *Distinguishing Complexity* of $|\phi_+\rangle$ and $|\phi_-\rangle$ is the size of the smallest circuit that accepts $|\phi_+\rangle$ and rejects $|\phi_-\rangle$. A fundamental result of Aaronson, Atia, and Susskind [AAS20] establishes that the swap complexity of $|\psi_0\rangle$ and $|\psi_1\rangle$ is essentially equivalent to the distinguishing complexity of $|\phi_+\rangle$ and $|\phi_-\rangle$. This duality principle, known as the "AAS duality", has emerged as a simple yet powerful tool in quantum complexity theory and cryptography.

In this work, we ask: *Can the AAS equivalence be extended to the more general context of many quantum states and multidimensional subspaces?* We give an affirmative answer to this question. First, we extend the notion of the swap complexity to a notion of "representation complexity": given a subspace, V, spanned by states $|\psi_1\rangle, \ldots, |\psi_k\rangle$, and a (potentially non-Abelian) group G, a *representation* of G on the subspace V is a homomorphism from G to the unitaries acting on the subspace (or, roughly, it is a collection of unitaries $\{\mathcal{R}(g)\}_{g\in G}$ acting on V which respects the structure of G).[1] We can call the *Representation Complexity* of $\mathcal{R}$ the size of the smallest circuit that implements the representation, that is, by mapping

$$|g\rangle \otimes |\psi_i\rangle \mapsto |g\rangle \otimes \mathcal{R}(g)\,|\psi_i\rangle \ .$$

When restricting to groups that have an efficient quantum Fourier transform (including all Abelian groups, all constant-sized or polynomial-sized groups, and several important exponential-sized non-Abelian groups), we show that the representation complexity is essentially equivalent to the complexity of implementing a *Fourier extraction*, or in other words, performing a partial measurement of the invariant subspaces preserved by the representation (i.e., its irreducible representation subspaces) and extracting the quantum state encoded in each such subspace (see Sections 1.2 and 2.2 for more discussion on Fourier extraction). For Abelian groups, this simplifies to a full projective measurement, and in particular, for the swapping representation of AAS, this is a measurement between $|\phi_+\rangle$ and $|\phi_-\rangle$. Thus the AAS duality is recovered by setting $G = \mathbb{Z}_2$. We additionally prove an *approximate* notion of this duality, where the circuit only has to approximately map between states.[2]

1.1 Applications to Cryptography

In cryptography, the AAS duality has proven quite fruitful. Cryptographic security properties come in two types: "search" type properties which stipulate the hardness of computing a specific unknown quantity, and "decision" type properties which stipulate the hardness of distinguishing between two distributions. The AAS duality has played a crucial role in establishing the equivalence between certain search-type and decision-type properties, leading to a number of significant results [Yan22, HMY23, KMNY24, MW24, HKNY24, MYY25].

We show that our new duality theorem is useful for cryptography beyond the AAS setting, by giving novel results for quantum money.

[1] For instance, in [AAS20], the representation of $G = \mathbb{Z}_2$ on the subspace spanned by $|\psi_0\rangle$ and $|\psi_1\rangle$ maps the sole non-identity element of $\mathbb{Z}_2$ to the unitary swapping $|\psi_0\rangle$ for $|\psi_1\rangle$ and vice versa.

[2] While our approximate duality theorem works for all groups, it achieves weaker error bounds than the duality of [AAS20] for $\mathbb{Z}_2$.

Quantum Money from Group Actions. Quantum money [Wie83] uses the no-cloning principle to generate unforgeable banknotes. These banknotes are quantum states that can be verified but cannot be cloned. A central problem has been to construct quantum money that can be *publicly verified* by anyone, and yet only the mint can create new banknotes. This is called public-key quantum money [Aar09].[3] Quantum *lightning* posits a stronger security notion for public-key quantum money, with a collision-resistance property that ensures that even the mint can only ever create one copy of each banknote [Zha21].

A long-standing challenge for public-key quantum money is to derive security from concrete computational assumptions (and in particular, assumptions that do not bake the unclonability of the banknotes directly into the assumption). The only prior scheme with such a proof is an instantiation of [AC12] using indistinguishability obfuscation (iO), as suggested by [BDS23] and proved in [Zha21]. However, iO is a powerful cryptographic tool whose quantum security is still uncertain. Moreover, no existing unbroken scheme has been shown to have such a security proof for the stronger security notion of quantum lightning.

Recently, [Zha24] gave a plausible construction of quantum money and quantum lightning from Abelian group actions. A group action consists of a group G, a set X, and a binary operation $* : G \times X \to X$, denoted $g * x = y$. This operation respects the group structure: $g*(h*x) = (gh)*x$. An Abelian group action is a group action where G is Abelian.[4] Unfortunately, the security of the scheme of [Zha24] requires both a computational assumption *and* an idealized modeling of group actions as a black box.

Using our duality principle, we show how to generalize this construction to work with *non-Abelian* group actions. This shift is not merely a superficial adjustment—it significantly improves on the framework in two critical ways:

1. It allows us to prove the hardness of our quantum money and lightning scheme in the *plain model*, using only a concrete assumption on the group action. This assumption also identifies an interesting potential source of hardness for non-Abelian group actions. Very roughly, for non-Abelian groups, in addition to a group action $g * (h * x) = (gh) * x$, we can also define a "pre-action" $g \circ (h * x) = (hg^{-1}) * x$, or more generally a "bi-action" $(g_0, g_1) \circledast (h * x) = (g_0 h g_1^{-1}) * x$. Our assumption states that it is hard via a quantum query to distinguish a random action from a random bi-action. Importantly, this problem only makes sense for non-Abelian group actions, as actions and pre-actions are identical in the Abelian case. Thus, the quantum money result requires us to use the full power of our non-Abelian generalization of the duality.

2. The shift to non-Abelian groups opens up the possibility for potentially more varied instantiations of the group actions. In particular, we explain how to instantiate our quantum money scheme on (a significant generalization of) the symmetric group action implicit in the McEliece cryptosystem [McE78].

Theorem 1.1 (informal)**.** *There is a public-key quantum money and quantum lightning scheme for any (non-Abelian) cryptographic group action, such that the money/lightning scheme is secure if the group action is preaction-secure.*

To the best of our knowledge, this represents the first (unbroken) quantum lightning scheme with a plain-model security proof based on a computational assumption that does inherently include unclonability.

[3] When it is otherwise clear from context, we will refer to public key quantum money as simply "quantum money".
[4] Abelian groups are those for which all the elements commute: $gh = hg \ \ \forall g, h \in G$.

Quantum Money from One-way Homomorphisms. A one-way (group) homomorphism is a function, $f(h)$, that is group homomorphic[5] and efficiently computable, but computationally intractable to invert.[6] A one-way homomorphism can be seen as an instance of a group action, with the domain group acting on the codomain as $g * f(h) = f(gh)$. However, unlike in the previous case above, the preactions for this action (i.e., $g \circ f(h) = f(hg^{-1})$) are as efficiently computable as the action itself, so security cannot be shown as before. Nevertheless, we give sufficient conditions on the one-way homomorphism such that the resulting quantum lightning scheme is secure.

We note that unlike our construction above from group actions that are pre-action secure—for which we give concrete instantiations that can be implemented in practice—we do not know if any instantiations of homomorphic functions satisfy these security conditions. But we observe that a one-way group homomorphism is essentially a group action where the computational Diffie-Hellman (CDH) problem is *easy* but yet discrete logarithms are still *hard*. While CDH is quantumly equivalent to discrete logarithms for Abelian groups [MZ22], this equivalence does not seem to follow for non-Abelian groups. Strangely, it is a hypothetical security *failure* for group actions which gives rise to plausible instantiations for quantum lightning and quantum fire (see more on the construction of quantum fire below).

We concede the disadvantage of this construction as compared to the concrete one above from preaction security, but we note that it has some unique properties that the other does not. Specifically, by leveraging our duality principle we are able to prove the remarkable fact that four distinct quantum money security notions—namely, the collision-resistance of quantum lightning security, the hardness of both worst-case cloning and average-case cloning, and the hardness of preparing the uniform superposition over the image of the homomorphism—are all identical. Thus for any particular instantiation of the one-way homomorphism, it is sufficient to prove any one of these security notions in order to get the other three.

Quantum Fire. Quantum fire refers to a collection of efficiently samplable quantum states that can be efficiently cloned, but cannot be efficiently telegraphed.[7] That is, despite the ability to make an unbounded number of copies of a quantum fire state, there is no way to efficiently encode it as classical information from which it can later be recovered. Much like a flame can be easily spread from a single source as long as it is kept alive, quantum fire can be cloned from a single quantum state as long as it is kept coherently in quantum storage.

The concept of quantum fire was first introduced in the work of Nehoran and Zhandry [NZ24], where it was shown to be essential for solving the key exfiltration problem. However, it was not formally defined or named in that work. [NZ24] provided a secure construction of quantum fire relative to a unitary quantum oracle, but this oracle construction relied on an inherently inefficient computation and baked clonability into the oracle itself. Consequently, it does not provide a pathway for instantiation in the standard model. It has not even been clear if any

[5] That is, it is a homomorphism between two groups G and H, such that $f(gh) = f(g) \cdot f(h)$ for all $g, h \in G$.

[6] Note that Shor's algorithm [Sho94] allows efficiently inverting group homomorphosms when the domain and codomain groups are Abelian. Thus, these results inherently require non-Abelian groups, and hence our generalized duality.

[7] Note that while the no-cloning theorem prohibits cloning *general* quantum states, this prohibition does not apply to quantum states chosen from an orthogonal set. The same applies to the no-telegraphing theorem, which prohibits sending *general* quantum states through a classical channel without pre-shared entanglement. States from an orthogonal set can clearly be telegraphed by measuring them in this basis and later recreating them accordingly. Such states can be cloned in a similar fashion. In other words, any states chosen from an orthogonal set can be both cloned and telegraphed *information-theoretically*, but these tasks are not necessarily both efficient. In fact, it was shown in [NZ24] that there are likely to be state families where cloning is efficient and yet telegraphing is not. Quantum fire is the cryptographic primitive that samples such states efficiently.

classical oracle could allow efficient cloning of quantum states that are inherently quantum (and thus not telegraphable).

Inspired by the duality principle, we give a plausible candidate construction of quantum fire relative to a one-way group homomorphism. Remarkably, despite the similarity to the construction of quantum lightning from group homomorphisms, where the states are *unclonable*, the states in this scheme are inherently *clonable*, and efficiently so. Nevertheless, there is no apparent way to telegraph the states efficiently. Moreover, it is straightforward to define a classical oracle that gives a candidate one-way group homomorphism. Thus, we obtain a candidate construction of quantum fire with conjectured security relative to a classical oracle, improving upon the unitary oracle construction of [NZ24].[8]

1.2 A Generalized Duality

Fourier extraction. A major stepping stone towards our duality theorem is the idea of a Fourier extraction. Every group representation preserves some set of invariant subspaces $\{\mathsf{W}_\lambda\}_{\lambda\in[n]}$.[9] A *course* Fourier measurement[10] of the representation is, roughly, a projection onto these subspaces. We get a classical label λ indicating the subspace we have projected onto, as well as a collapsed state, $|\psi\rangle$, within the subspace W_λ. A *fine* Fourier measurement[11] further measures within each of those subspaces, in a basis that depends on the algorithm. For instance, if $\{|\psi_j^\lambda\rangle\}_{j\in\dim(\mathsf{W}_\lambda)}$ is a basis for W_λ, we get outcomes λ and j, and collapse our state to $|\psi_j^\lambda\rangle$.[12] In either case, the state after the measurement is still within the subspace.

In some applications, we care about the *coherent* information encoded within each subspace. That is, it is not enough to know which collapsed state $|\psi_j^\lambda\rangle$ we received. We want to have, in our hands, the coherent superposition that appeared in the subspace. That is, if the original state was $\sum_{j\in[\dim(\mathsf{W}_\lambda)]}\alpha_j|\psi_j^\lambda\rangle$, we want to *extract* the full superposition $\sum_j\alpha_j|j\rangle$. This transformation, which we call a *Fourier extraction*, extracts the full state coherently from the subspace.[13]

If implemented naïvely, Fourier measurements do not suffice for this task. They either do not recover the information about where the state was *within* each subspace (in the case of course Fourier measurement), or they recover it in a collapsed form (in the fine case). In our work, we consider the stronger notion of a "*Fourier extraction*", an operation that measures the subspace and *coherently recovers* the encoded state.

[8] Note that, as observed in [NZ24], an unconditional security proof relative to such a classical oracle would likely require proving a classical oracle separation between the complexity classes QMA and QCMA, a major open problem of Aharonov and Naveh [AN02], which, despite recent progress, has evaded resolution.

[9] That is, these subspaces are invariant under all of the unitaries U_g corresponding to each group element $g\in G$. In some cases, the only invariant subspace may be the full Hilbert space, in which case we say that it is *irreducible*, but this is not generically the case. We consider here only invariant subspaces which are irreducible, and do not break down further into smaller invariant subspaces.

[10] Often called weak Fourier sampling in many contexts

[11] Commonly called strong Fourier sampling

[12] To simplify the notation, we assume here that there is no multiplicity, or degeneracy, in the irreducible representations. We will see later how to handle multiplicity.

[13] Note that such extraction is not generally an efficient transformation for arbitrary subspaces.

Duality. We show that the implementations of representations and the implementations of their Fourier extractions are essentially computationally dual to each other.

Theorem 1.2 (Duality, *informal*)**.** *Let G be a group with an efficient quantum Fourier transform*[14] *and let $\mathcal{R} : G \to U(\mathcal{H})$ be a representation of G. Then the following are equivalent:*

- *$\mathcal{R}$ has an efficient implementation, i.e. $|g\rangle \otimes |\psi\rangle \mapsto |g\rangle \otimes \mathcal{R}(g)\,|\psi\rangle$.*
- *$\mathcal{R}$ has an efficient Fourier extraction, i.e. $|\psi^\lambda_{i,j}\rangle \mapsto |\phi^\lambda_i\rangle\,|\lambda, j\rangle$.*

Further Discussion of Fourier Extraction. In the above discussion, we have glossed over the possibility of *multiplicity* or *degeneracy*, in which the representation acts identically on several different invariant subspaces $\mathsf{W}^\lambda_1, \mathsf{W}^\lambda_2, \ldots, \mathsf{W}^\lambda_m$. Such subspaces are degenerate in the sense that a course Fourier measurement produces the same outcome, λ, on all of them. Thus we have an additional index, i, that runs over this multiplicity of λ.

We write a Fourier extraction as an isometry $|\psi^\lambda_{i,j}\rangle \mapsto |\phi^\lambda_i\rangle\,|\lambda, j\rangle$, where for each λ and i, the states $\{|\psi^\lambda_{i,j}\rangle\}_j$ are a basis for the subspace W^λ_i, and the state $|\phi^\lambda_i\rangle$ is an arbitrary "junk" state that is left behind after measuring λ and extracting j.

In order for it to be an *extraction* of j, rather than a measurement of j, it is crucial that this leftover state has no dependence on j. Consider a superposition $\sum_{j\in[\dim(\mathsf{W}^\lambda_i)]} \alpha_j\,|\psi^\lambda_{i,j}\rangle$ over the subspace W^λ_i. Performing this isometry yields $\sum_j \alpha_j\,|\phi^\lambda_i\rangle\,|\lambda, j\rangle = |\phi^\lambda_i\rangle\,|\lambda\rangle \otimes \sum_j \alpha_j\,|j\rangle$, which extracts the original superposition into a quantum state on the last register with those exact amplitudes. If the leftover junk state had depended on j, for instance if we instead had $|\psi^\lambda_{i,j}\rangle \mapsto |\phi^\lambda_{i,j}\rangle\,|\lambda, j\rangle$, then this would not extract the state properly. We would instead get $\sum_j \alpha_j\,|\phi^\lambda_{i,j}\rangle\,|\lambda, j\rangle$, where the last register is still entangled with the rest of the state, and thus has not been extracted. This is the difference between a *measurement* of j and an *extraction* of j. (See Section 2.2 for more discussion on Fourier extraction.)

We observe that since these leftover junk states $|\phi^\lambda_i\rangle$ are independent of j—that is, they do not depend on which state we started from within the subspace W^λ_i—we can see that these states are instead characteristic of the subspace W^λ_i itself. That is, the Fourier extraction collapses each subspace W^λ_i to a single distinct quantum state $|\phi^\lambda_i\rangle$, which we therefore call the "archetype" states of these subspaces. Despite appearing to be just the "junk" that is left behind during the Fourier extraction, these archetype states are in fact quite useful.

For instance, the existence of these archetype states allows us to use a swap test to distinguish whether two quantum states are in the same subspace or different subspaces. Consider two states $|\psi^\lambda_{i_1,j_1}\rangle \in \mathsf{W}^\lambda_{i_1}$ and $|\psi^\lambda_{i_2,j_2}\rangle \in \mathsf{W}^\lambda_{i_2}$ that live in subspaces corresponding to the same λ, but potentially different such subspaces (that is, $\mathsf{W}^\lambda_{i_1}$ and $\mathsf{W}^\lambda_{i_2}$ are potentially different), and suppose that we wanted to test whether they in fact belong to the same subspace (that is, if $i_1 = i_2$). The ability to perform the representation *does not* in general allow us to measure i. Intuitively, this is because both these states behave identically under the representation. A Fourier measurement/sampling of these states would give us only λ, or both λ and j, but not i. So how can we test if they are in the same subspace? This is in general not possible from such a measurement. However, Fourier extraction is more powerful than Fourier measurement and gives us this ability. Performing a Fourier extraction on both states gives us $|\phi^\lambda_{i_1}\rangle\,|\lambda\rangle\,|j_1\rangle$ for the first state and $|\phi^\lambda_{i_2}\rangle\,|\lambda\rangle\,|j_2\rangle$ for the second state. Now

[14] Note that while not every group is known to have an efficient quantum Fourier transform, this does include a very wide class of groups, and includes, at the very least, all Abelian groups, as well as many important non-Abelian groups. Moreover, *every* fixed-size group is technically efficient (whether Abelian or not), so this condition is only important for some families of groups whose sizes grow exponentially.

we can ignore and discard the last register—the one that indicates which state we had within each subspace—and perform a swap test only on the first register, that is between the archetype states that characterize the subspaces. This turns out to be a crucial tool in the security proof of our quantum lightning construction (see Section 2.4.1 for a discussion on this).

The Special Case of Abelian Groups. Abelian groups have the special property that all of the (irreducible) invariant subspaces are one-dimensional. Since the "quantum state" extracted by the Fourier extraction in this case is one-dimensional, it is actually just a complex phase. We can see that the corresponding isometry simplifies to $|\psi_i^\lambda\rangle \mapsto |\phi_i^\lambda\rangle |\lambda\rangle$, where we have absorbed the phase into $|\phi_i^\lambda\rangle$. This is computationally equivalent to the isometry $|\psi_i^\lambda\rangle \mapsto |\psi_i^\lambda\rangle |\lambda\rangle$ (by copying λ and uncomputing), which we can see is just the course Fourier measurement for the representation—that is, a projective measurement onto the subspaces W^λ. We therefore get the following simplified duality for Abelian groups as a special case: a duality between the efficiency of implementing the representation and that of performing a Fourier measurement,[15] a projective measurement on the subspaces spanned by its invariant states.[16]

Corollary 1.3 (Duality for Abelian Groups, *informal*)**.** *Let G be an Abelian group and let $\mathcal{R} : G \to U(\mathcal{H})$ be a representation of G. Then the following are equivalent:*

- *$\mathcal{R}$ has an efficient implementation, i.e. $|g\rangle \otimes |\psi\rangle \mapsto |g\rangle \otimes \mathcal{R}(g) |\psi\rangle$.*
- *$\mathcal{R}$ has an efficient Fourier measurement, i.e. $|\psi_i^\lambda\rangle \mapsto |\psi_i^\lambda\rangle |\lambda\rangle$.*

1.3 Related Work

Quantum Money, Lightning, etc. There have been several attempts at constructing public-key quantum money [BBBW82, Aar09, FGH+12, AC12, Zha21, KSS22, AGKZ20, KLS22, LMZ23, Zha24]. Unfortunately, a number of them later turned out to be broken [LAF+09, CPDDF+19, Rob21, LMZ23]. In order to gain confidence in constructions, it is therefore important to give security proofs under computational assumptions that have received significant scrutiny from the cryptographic community. Here, the best we currently have are:

- Quantum money from hidden subspaces [AC12], which was proved secure assuming quantum-resistant *indistinguishability obfuscation* (iO) in [Zha21]. Unfortunately, while candidates for quantum-resistant iO are known, their status is still very much open. This scheme also only achieves quantum money, but not quantum lightning.
- Quantum money from random walks [FGH+12, LMZ23], which was shown to be secure under strong quantum "knowledge" assumptions. Such assumptions are not "falsifiable", and there is some doubt about the plausibility of such assumptions [Zha24].
- Quantum money from Abelian group actions [Zha24], which is proven secure under an assumption *plus* in an idealized model of group actions as a black box.

We provide a scheme whose quantum lightning security we prove in the *plain model* (i.e. without making idealized model assumptions) from a plausible and falsifiable computational assumption. We hope that our work motivates further study of the cryptographic uses of non-Abelian group actions, and in particular, of the hardness of preactions.

[15] Note that because representations of Abelian groups have only one-dimensional representations, there is no distinction between the course/weak and the fine/strong versions of Fourier measurement/sampling. Thus, we refer to it as simply Fourier measurement.

[16] The irreducible invariant subspaces are one-dimensional, and are thus individual quantum states.

Comparison to the Duality of Aaronson, Atia, and Susskind. [AAS20] show that there is a duality between, on the one hand, swapping between two orthogonal states, and on the other hand, measuring the positive and negative superpositions of the two states. As a representation, this "swapping" operation, together with the identity, is a representation of $\mathbb{Z}_2$. The invariant subspaces of this representation are the positive and negative superpositions, with eigenvalues $+1$ and -1. Our duality theorem precisely yields the duality theorem from [AAS20] as a special case when applied to $\mathbb{Z}_2$, and recovers the same circuits, showing that our results are a proper generalization.

Theorem 1.2 extends far beyond $\mathbb{Z}_2$, and even beyond Abelian groups, to many of the non-Abelian groups that are important for cryptography. We expect our duality theorem to be applicable to many more settings in quantum cryptography and complexity theory. Our applications to building quantum money, lightning, and fire are just a few demonstrations of the usefulness of our theorem and techniques, and demonstrate the usefulness of considering this quantum duality in its full non-Abelian generalization.

Fourier Measurements and their Applications Fourier measurements/sampling for Abelian groups play an important role in many famous quantum speedups, including the efficient quantum algorithm for Simons problem [Sim97], a key subroutine in the quantum speedup of Shor's factoring algorithm [Sho94]. Fourier measurements also play an important role more generally in algorithms for hidden subgroup problems for general groups [CHW07]. As a result, there has been a long line of work on developing efficient algorithms for Fourier measurements. [Har05] showed how to implement Fourier sampling for arbitrary representations of the symmetric group using an identical circuit to the implementation of Fourier extraction, which they call the generalized phase estimation algorithm. This algorithm can be extended to any arbitrary group that has an efficient quantum Fourier transform. Several works have made progress towards efficient algorithms for performing strong Fourier sampling (fine Fourier measurements) in specific bases of the symmetric group [BCH05, Kro19].

Fourier measurements also appear often in learning theory in the context of the symmetric group. When treating the action of permuting n identical registers as a representation of the symmetric group, Fourier sampling along the joint irreducible subspaces of the symmetric and unitary groups (which arises as a result of Schur-Weyl duality) appears as an important subroutine in many tomography algorithms [Key06, OW16, OW17, HHJ$^+$16, CLL24] and compression algorithms [YCH16].

Problems of computing certain constants associated with the irreducible representations of the symmetric group (Kostka numbers, Littlewood-Richardson coefficients, and Plethysm coefficients) are thought to be problems that might be outside of NP, but in BQP. Fourier measurements play an important role in designing efficient quantum algorithms for computing these numbers [LH24]. The Kronecker coefficients are another set of constants associated with the symmetric group whose complexity remains unknown. Recent work [BCG$^+$24] uses generalized phase estimation and weak Fourier measurement, to design a QMA protocol for computing them.

2 Technical Overview

This work uses the tools of representation theory, and moreover, understanding the principles of representation theory is important for understanding both the statement of our duality theorem as well as the technical details of our quantum lightning construction and security proof. However, since we expect that the duality theorem and our other results will be applicable to researchers from a wide variety backgrounds, we have done our best to write this technical overview with

an expository flavor, by giving a high-level intuition behind the representation-theoretic tools we use and how they lead to our contributions. For a more in-depth introduction to representation theory in the context of quantum computing, we refer to lecture notes by Andrew Childs [Chi17], accompanied by any of a number of great representation theory textbooks, e.g. [S+77, Ste09].

2.1 Quantum Fourier Transforms

In order to give intuition about the duality theorem and quantum lightning construction, we will first need to make a few remarks about the generalized notion of the quantum Fourier transform, specifically its generalization to representations of non-Abelian groups. Every representation $\mathcal{R}$, has a basis in which it is block-diagonal, with the blocks corresponding to its irreducible sub-representations—these are the smallest building blocks that cannot be further decomposed.[17] In other words, in this basis, $\mathcal{R}$ is a direct sum of irreducible representations $\{\varrho_\lambda\}_{\lambda\in\widehat{G}}$, where $\widehat{G}$ is the set of labels corresponding to each possible irreducible representation of G:

$$\mathcal{R}(g) = V^\dagger \left(\bigoplus_{\substack{\lambda\in\widehat{G} \\ i\in[m_\lambda]}} \varrho_\lambda(g) \right) V = V^\dagger \begin{pmatrix} \boxed{\varrho_1(g)} & & & & \\ & \boxed{\varrho_1(g)} & & & \\ & & \boxed{\varrho_2(g)} & & \\ & & & \boxed{\varrho_2(g)} & \\ & & & & \ddots \\ & & & & \boxed{\varrho_k(g)} \end{pmatrix} V\,, \tag{1}$$

where, m_λ denotes the "multiplicity" of the irreducible representation ϱ_λ in $\mathcal{R}$, that is, the number of times it appears repeated in the block-diagonalization, and each individual block has dimension d_λ. We note while that the block decomposition into the larger subspaces[18] $\mathsf{W}^\lambda = \mathrm{span}\{|\lambda, i, j\rangle : i \in [m_\lambda], j \in [d_\lambda]\}$ is unique, for non-Abelian groups, there is flexibility in the actual choice of the basis vectors $|\lambda, i, j\rangle$ of W^λ.

This unitary transformation, V, which optimally block-diagonalizes $\mathcal{R}$, is the *Fourier transform* $\mathrm{QFT}_\mathcal{R}$ of the representation.[19] Although it is not common to think of this transformation as the Fourier transform, it is indeed a generalization of the familiar quantum Fourier transform: the plain Fourier transform of a group G (without any representation specified) is simply the Fourier transform of its left-regular representation, $\mathsf{LeftRegular}_G$ (the representation defined by left multiplication on the group algebra, i.e. $\mathsf{LeftRegular}_G(g)\,|h\rangle = |gh\rangle$). In this case, the quantum Fourier transform can be written as

$$\mathrm{QFT}_G = \mathrm{QFT}_{\mathsf{LeftRegular}_G} = \sum_{g\in G} \sum_{\substack{\lambda\in\widehat{G} \\ i,j\in[d_\lambda]}} \sqrt{\frac{d_\lambda}{|G|}}\, \varrho_\lambda(g)_{j,i}\, |\lambda, i, j\rangle\langle g|\ .$$

We of course recover the most familiar form of the quantum Fourier transform by specializing further to the cyclic group $\mathbb{Z}_N$, and thus setting $d_\lambda = 1$ (since $\mathbb{Z}_N$ is Abelian) and $\varrho_\lambda(g) = e^{2\pi i(g\cdot\lambda)/N}$. The

[17] Note that in the special case of an Abelian representation, all the unitaries commute, and we can therefore go further and fully diagonalize everything simultaneously. In that case, the resulting blocks are simply all of size one. However, for non-Abelian representations, such a simultaneous diagonalization is not possible, and the closest we can get is this block-diagonal form.

[18] These are called the *isotypic components* of λ, which group together all the blocks that behave similarly under $\mathcal{R}$.

[19] Even though this unitary may or may not be efficient, we write it as a *quantum* Fourier transform, $\mathrm{QFT}_\mathcal{R}$, instead of $\mathrm{FT}_\mathcal{R}$ for notational consistency.

basis $\{|\lambda, i, j\rangle\}_{\lambda\in\widehat{G},\, i\in[m_\lambda],\, j\in[d_\lambda]}$ is the Fourier basis of the representation, with classical strings λ, i, and j labeling the irreducible representation, multiplicity index, and basis state within each irreducible invariant subspace, respectively, corresponding to the blocks in Equation (1).

The plain quantum Fourier transform, QFT_G of many groups can be performed efficiently (including for all constant size or polynomial-sized groups, Abelian groups [Cop94], and many important non-Abelian groups such as the dihedral and symmetric groups [Høy97, Bea97, MRR06]). However, even for such groups, the *representation* Fourier transform $\mathrm{QFT}_{\mathcal{R}}$ of many of their representations may still be inefficient. For instance, as we will see, the Fourier transform of a *cryptographic group action* is inefficient even if the Fourier transform of the underlying group is efficient. Therefore, in order to access information about the Fourier basis of a general representation, we need more clever techniques like Fourier sampling and Fourier extraction.

2.2 Fourier Sampling and Fourier Extraction

Despite the lack of an efficient quantum Fourier transform for general representations, you might nevertheless want to access information about the Fourier basis (moreover, the transformed Fourier basis, $\{\mathrm{QFT}_{\mathcal{R}}^\dagger |\lambda, i, j\rangle\}_{\lambda\in\widehat{G},\, i\in[m_\lambda],\, j\in[d_\lambda]}$, which we refer to as the Fourier basis when there is no ambiguity). To demonstrate that this is possible and build intuition, let us start with the simple case of a representation, $\mathcal{R} : G \to U(\mathcal{H})$, of an Abelian group G. Say you want to perform a projective measurement in the Fourier basis of $\mathcal{R}$ on some state $|\psi\rangle \in \mathcal{H}$. Without computational considerations, we aim to implement the circuit in Figure 1, where we perform a representation Fourier transform $\mathrm{QFT}_{\mathcal{R}}$ on $|\psi\rangle$, to get a superposition over classical strings encoding the Fourier basis information (in this case, just the irreducible representation label, λ), copy the classical string λ onto an ancilla register,[20] and then undo the representation Fourier transform to recover the projected state.

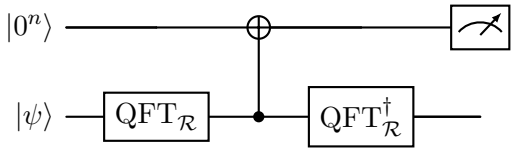
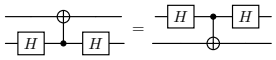


Figure 1: The ideal functionality of a measurement in the Fourier basis of a group representation, $\mathcal{R}$. Here, $\mathrm{QFT}_{\mathcal{R}}$ is not the Fourier transform of the group, but rather the (generally inefficient) Fourier transform of the *representation*.

As is probably clear, however, the circuit in Figure 1 is not actually an explicit algorithm, since there is in general no efficient circuit for the representation Fourier transform $\mathrm{QFT}_{\mathcal{R}}$.

However, if we look at both registers in their respective Fourier bases—the top register in the Fourier basis of the group (or equivalently, of the left-regular representation), and the bottom register in the Fourier basis of the representation $\mathcal{R}$—it turns out that the upwards copy (an upwards group operation of $\widehat{G}$) looks like a downwards copy: a controlled group representation onto the bottom register. Thus, we can pull out Fourier transforms on both wires and flip the circuit diagram to get the equivalent circuit depicted in Figure 2. (This is, of course, similar to,

[20] While we draw this copy operation as a CNOT gate for simplicity, for Abelian groups, this copy can equivalently be seen as the group operation of the group's Pontryagin dual $\widehat{G}$.

and a proper generalization of, the well-known identity  on the group $\mathbb{Z}_2$ and its regular representation.)

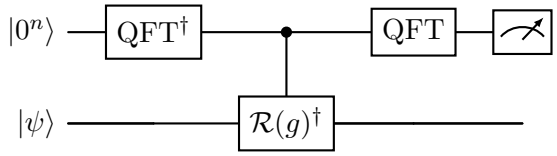


Figure 2: Fourier sampling circuit for the representation $\mathcal{R}$. For Abelian representations, the functionality of this circuit is identical to that of Figure 1, but unlike the circuit drawn there, this circuit depicts an efficient algorithm.

This is called the Fourier sampling circuit, and for Abelian groups, it acts identically to the circuit of Figure 1, but now we have moved from having gates for a *representation* Fourier transform on the bottom wire in Figure 1 to having only gates for the Fourier transform *of the plain group* on the top wire in Figure 2. Now, if our group has an efficient quantum Fourier transform, and we can efficiently implement the controlled representation, then the circuit in Figure 2 is efficiently implementable, even while the original circuit in Figure 1 may not be. Thus, while we may not be able to implement the representation's Fourier transform, we can still recover and measure some information about the Fourier basis of the representation.

Remark 2.1. *A minor comment is that general representations—even representations of Abelian groups—could have multiplicity (the generalization of the concept of degeneracy in the eigenspaces of unitaries). In this case, the same irreducible representation ϱ_λ could appear m_λ different times in the block-diagonal decomposition of $\mathcal{R}$. Therefore, besides the label $\lambda \in \widehat{G}$ of the irreducible representation, we have a multiplicity index $i \in [m_\lambda]$ which indexes which of the irreducible invariant subspaces corresponding to ϱ_λ we have. Since the representation $\mathcal{R}$ does not distinguish between subspaces on which it acts identically, there can be no way to generically use it to measure i. This is captured by the fact that the circuit we get when we do the flipping trick above on Figure 2 is not in fact the circuit in Figure 1, but rather the one in Figure 3, where the information about the label λ of the irreducible representation is copied to the ancilla register, but the information about the multiplicity index i is left untouched.*

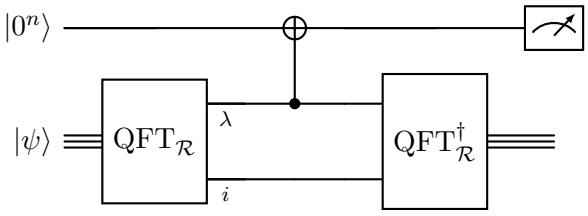
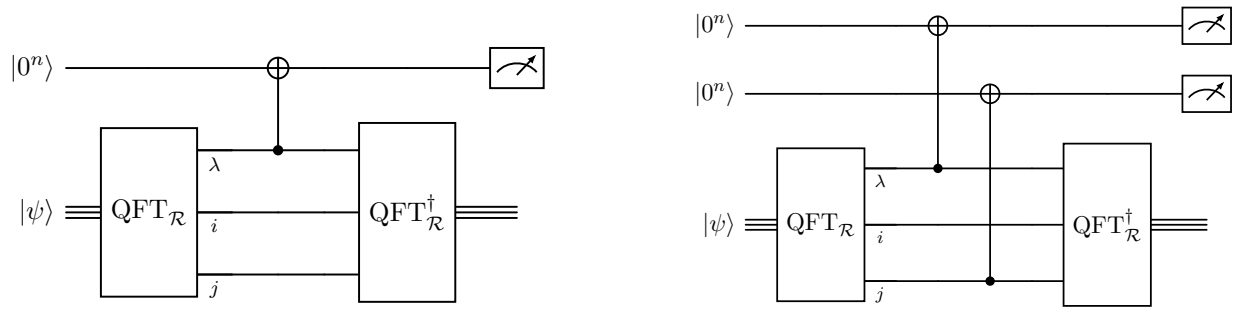


Figure 3: The ideal functionality of a measurement in the Fourier basis of an Abelian representation $\mathcal{R}$ that has multiplicity. The label λ of the irreducible representation is copied up to the ancilla register, while the multiplicity index i is left inaccessible. While this circuit is not efficiently implementable, its functionality is equivalent to that of the efficient Fourier sampling circuit of Figure 2.

Generalizing to Non-Abelian Groups When generalizing to non-Abelian groups, it must be taken into account that there is now not only the possibility of multiplicity, but also the presence of irreducible subspaces of dimensions larger than one. We therefore have a third index, $j \in [d_\lambda]$, which runs over the dimension d_λ of the irreducible subspace. We now have a choice between two kinds of Fourier measurements: a coarser-grained version known as weak Fourier sampling, and a finer-grained version known as strong Fourier sampling (Figure 4).



(a) Ideal functionality of weak Fourier sampling

(b) Ideal functionality of strong Fourier sampling

Figure 4: The ideal functionality of two kinds of measurements in the Fourier basis of a non-Abelian representation $\mathcal{R}$. In both of these, the label λ of the irreducible representation is copied up to an ancilla register, and in the strong case, the state index j is copied up as well. The multiplicity index i is of course always left inaccessible. Neither circuit can be instantiated efficiently, but either functionality can be implemented using the efficient Fourier sampling circuit of Figure 2.

Either type of non-Abelian Fourier sampling is known to be implementable from the representation by using the Fourier sampling circuit of Figure 2. For many purposes, this ends up being sufficient. Indeed, it has long been known that an efficient implementation of the representation (and the group's quantum Fourier transform) is enough to get efficient Fourier sampling.

However, if we want an actual *duality*, the reverse direction must hold as well, which unfortunately it does not: in certain cases, there may very well be a way to get even a strong Fourier sampling functionality for a representation that has no efficient implementation.

Getting a generalized duality is therefore quite a bit more subtle. If we take a closer look at what actually occurs in the Fourier basis of both wires of Figure 2 in the non-Abelian case (Figure 5), we notice something interesting. As expected, the information flow is reversed—going from the bottom to the top wire instead of top to bottom. However, while the information about the irrep label λ is *copied* up to the appropriate ancilla, the information about the state index j moves up, but it is in fact not copied at all—it is extracted!

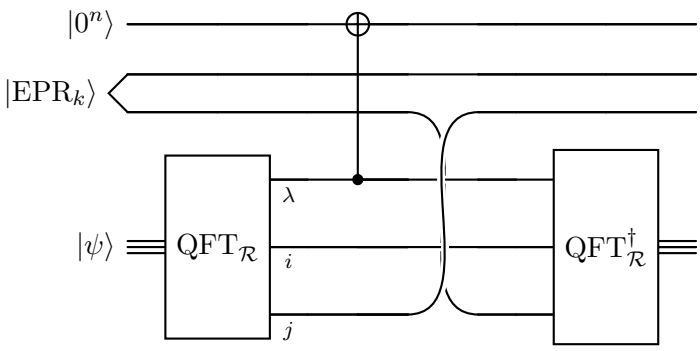


Figure 5: Ideal functionality that occurs for a non-Abelian representation when the circuit of Figure 2, is viewed in the Fourier-transformed bases of both wires (i.e. the group Fourier transform on the top wire and the representation Fourier transform on the bottom wire).[21] Note that the wire corresponding to the state index j is swapped out completely, such that after the second representation Fourier transform, no information about it is left over at the bottom. Thus it is not copied out, but rather *extracted*.

The ideal functionality of Fourier extraction in general is shown in Figure 6, where the irrep label λ is copied out to an ancilla, and the state index j is extracted.

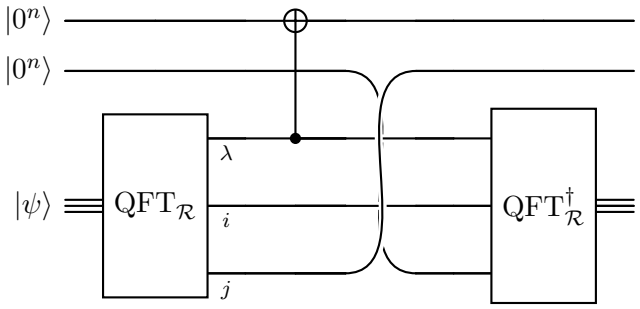


Figure 6: Ideal functionality of Fourier extraction.

2.3 Duality between Fourier Extraction and the Representation of a Group

The duality theorem (Theorem 5.1) states that for all groups where the quantum Fourier transform for the left-regular representation is efficient, implementing a group representation is efficient if and only if the corresponding Fourier extraction is efficient. In some sense, this means that quantum Fourier extraction is the "right" way to generalize the distinguishing task of [AAS20] and Fourier sampling to non-Abelian groups. It is computationally equivalent to implementing the representation.

In order to prove the duality theorem, we need to provide an efficient implementation of a Fourier extraction given a representation, and vice versa. From an implementation view-point,

[21] For simplicity, we are only depicting the functionality of the circuit when the ancilla registers start in all zeros state (which is interpreted as the trivial irrep of the left regular representation). The effect of the circuit for general states of the ancilla registers is considerably more complicated. Also, we depict the entanglement created between the second ancilla register and the working register as a k-qubit EPR pair. This is just for visualization, since in reality, the EPR pair we get has dimension which depends on the dimension of the measured irrep. We omit this for simplicity.

both of the directions of our duality can be viewed as generalizations of [AAS20] to the case of non-Abelian groups.

The forward direction is the same as the Fourier sampling circuit we considered above, with the observation that it performs a Fourier extraction for general non-Abelian groups. That is, given a representation $\mathcal{R} : G \mapsto U(\mathcal{H})$ of a finite group G, we can implement a Fourier extraction of G in $\mathcal{H}$ via two applications of the quantum Fourier transform on the plain group and a single application of the controlled representation, via the circuit in Figure 7.

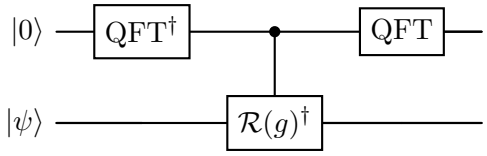


Figure 7: Implementing a Fourier extraction, given the ability to implement a representation $\mathcal{R}$ of a group G.

In the other direction, we show that given access to a Fourier extraction $\mathcal{M}_{\mathcal{R}}$ (and its inverse $\mathcal{M}_{\mathcal{R}}^\dagger$), we can implement the corresponding representation of G in $\mathcal{H}$ via the circuit in Figure 8. Here we assume that the Fourier extraction outputs three registers: one containing a label of an irreducible representation $\lambda \in \widehat{G}$, one containing the archetype $|\phi_i^\lambda\rangle$ of a multiplicity subspace $i \in [m_\lambda]$, and one containing a state index label $j \in [d_\lambda]$.

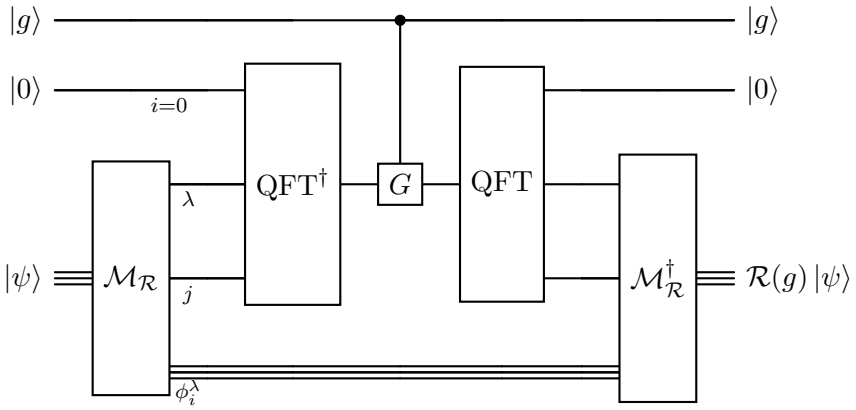


Figure 8: Implementing a representation $\mathcal{R}$ of a group G, given a Fourier extraction $\mathcal{M}_{\mathcal{R}}$. The controlled G gate is a left group operation in the group G.

We also prove an approximate version of this duality, where $\mathcal{R}$ and $\mathcal{M}$ are approximate implementations of a representation or Fourier extraction. In this case we can analyze the performance of our circuits by relating them to "nearby" exact representations and Fourier extractions, which are guaranteed to exist due to the work of Gowers and Hatami [GH16].

2.4 Quantum Money, Lightning, and Fire from Non-Abelian Group Actions

Next, we describe a protocol for constructing quantum money and lightning from any non-Abelian group action. Both the minting and verification procedure mimic the implementation of Fourier

extraction and Fourier sampling, except that we use the specific representation that comes from applying the group action in superposition. For both, we first generate a uniform superposition over group elements (this is essentially the same as the first quantum Fourier transform), apply the group action in superposition, and measure the first register in the Fourier basis.

For minting (Figure 9), we start with a fixed set element of the set acted on by the group. The serial number will be the measured label λ of an irreducible representation of G. We show that this produces a serial number λ with probability proportional to the Plancherel measure of λ.

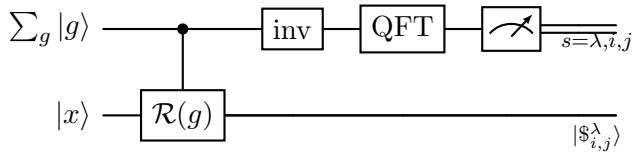


Figure 9: Minting procedure in the quantum lightning scheme from non-Abelian group actions. Here $\mathcal{R}$ is a group action of group G with starting element x, and inv maps g to g^{-1} (this inversion is simply in order to give us the desired $\mathcal{R}(g)^\dagger$ instead of $\mathcal{R}(g)$).

The verification algorithm (Figure 10) implements the same measurement as mint, except that it starts with the claimed banknote $|\pounds\rangle$, and it checks if the measured irreducible representation label λ' matches the claimed serial number.

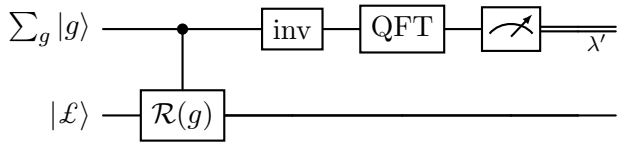


Figure 10: Verification procedure in the quantum lightning scheme from non-Abelian group actions. The verification algorithm measures an irreducible representation label λ' and accepts if λ' is equal to λ from the serial number. Note that this circuit may modify the banknote even if it is valid. However, the resulting modified banknote will also be valid for the same serial number, and furthermore, the circuit can be uncomputed to return the original banknote.

2.4.1 Security of the Scheme from Preactions

The security of the scheme is based on a new assumption we call "preaction security" (see Assumption 2 for the formal statement). Given a group action of G on set X, and a starting set element $x \in X$, the preaction of a group element $h \in G$ maps $g * x$ to $gh^{-1} * x$, and the preaction security assumption is that it is hard to distinguish the case when a random action has been applied to a register from the case when a random preaction and action (which we call a biaction) have been applied to the register.

Quantum lightning security requires it to be inefficient for any adversary to produce two banknote states corresponding to the same serial number. To gain intuition for why preaction security implies the security of our quantum lightning scheme, we need to think about what a preaction does to a state in the Fourier basis. Intuitively, in the Fourier basis of the left-regular representation, acting by a group element g moves a basis state $|\lambda, i, j\rangle$ to a different vector in the same multiplicity subspace, i.e. $\sum_k \alpha_k |\lambda, i, k\rangle$. On the other hand, a preaction acts by moving a vector in a particular multiplicity subspace to a superposition over multiplicity subspaces, i.e. $\sum_k \alpha_k |\lambda, k, j\rangle$.

Because (in general) preactions are hard to implement, an adversary cannot simply measure the multiplicity label i. This means that with only a single copy of the quantum money state (which is a Fourier basis state), it is difficult to determine if this multiplicity label changes. However, an adversary *can* perform Fourier extraction, which allows them to extract an "archetype" state $|\phi_i^\lambda\rangle$ that depends only on i.

Imagine a quantum lightning adversary that is given two copies of a quantum lightning state with the *same* serial number. Assume for simplicity that they are also in the same multiplicity subspace (of course, we do not make this assumption in our proof, but the intuition is much clearer for this case). The adversary can apply the random action or biaction to the first of the two registers, perform Fourier extraction on both, and do a swap test on the archetype states to see if they are equal. A random action, which does not change the multiplicity subspace, will not change the archetype state that results from the Fourier extraction, and thus the swap test will succeed with probability 1. A random preaction, on the other hand, will move the first register to a random multiplicity subspace, and therefore pass the swap test with probability close to $\frac{1}{2}$ (the exact probability depends on the structure of the group's irreps). More care is needed when the quantum lightning states produced by the adversary fall into different multiplicity subspaces, but we leave out the details here. Thus, this adversary breaks preaction security, and, by contradiction, if we start with a preaction secure group action, our quantum lightning scheme is secure.

2.4.2 Instantiation with the Group Action of the McEliece Cryptosystem

While we are able to construct quantum money and lightning from any group action satisfying preaction security, we also propose a few concrete group actions from which to instantiate it. A notable example that we believe may satisfy the necessary conditions is based on a group action implicit in the McEliece cryptosystem [McE78].

Our group action will represent the symmetric group S_n over the set X of $n \times t$ (for $t = \mathsf{poly}(n)$) matrices with entries from $\mathbb{F}_{q^m}$. Given a matrix M and permutation σ, $\sigma * M$ is the matrix where we first permute the columns of M according to σ, and then row-reduce the resulting matrix. The starting element of the group action will be the parity check matrix of a Goppa code [Gop70]. In particular, we sample elements $g_1, \ldots, g_t \in \mathbb{F}_{q^m}$, which defines a degree-t univariate polynomial $g(z) = \sum_{i=1}^{t} g_t z^t$, and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$ satisfying $g(\alpha_j) \neq 0$. Then the starting element corresponding to the choice of $g_1, \ldots, g_t$ and $\alpha_1, \ldots, \alpha_n$ is the following

$$\begin{pmatrix} g_t g(\alpha_1)^{-1} & g_t g(\alpha_2)^{-1} & \ldots & g_t g(\alpha_n)^{-1} \\ (g_t\alpha_1 + g_{t-1})g(\alpha_1)^{-1} & (g_t\alpha_2 + g_{t-1})g(\alpha_2)^{-1} & \ldots & (g_t\alpha_n + g_{t-1})g(\alpha_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ (g_t\alpha_1^{t-1} + g_{t-1}\alpha_1^{t-2} \ldots + g_1)g(\alpha_1)^{-1} & \ldots & \ldots & (g_t\alpha_n^{t-1} + \ldots + g_1)g(\alpha_n)^{-1} \end{pmatrix}.$$

It is commonly assumed that for certain distributions over g and α, these matrices are indistinguishable from a uniformly random matrix even to quantum algorithms [Sin19], and that applying a random column permutation *and* a random $n \times n$ matrix from the right yields a matrix that is indistinguishable from a uniformly random matrix even to adversaries who know the starting element, however these do not directly imply the preaction security of this group action. We conjecture that preaction security holds for this group action, and show that under this assumption, instantiating our framework with this group action yields a concrete secure quantum lightning in the plain model.

2.4.3 Quantum Fire

As part of this work, we also provide a framework for constructing quantum fire in the plain model. We show conditions under which these states are efficiently clonable, but we leave it as an open question to prove that the scheme satisfies untelegraphability. The construction of quantum fire is similar to the construction of quantum lightning and money from non-Abelian group actions, however we make use of the insight that applying a controlled group operation between registers can be used to "copy" information about the irreducible representation to allow for efficient cloning of the states in an inaccessible Fourier basis.

We now describe the construction. Let G and H be two groups and $f : G \mapsto H$ be a one-way injective homomorphism between the two (i.e. $f(g)f(h) = f(gh)$).[22] We can define a representation of G by letting $\mathcal{R}(g)\,|h\rangle = |f(g) \cdot h\rangle$. Then we can spark (the fire equivalent of minting) and verify quantum fire using the same circuits as in the quantum lightning construction, but with this representation.

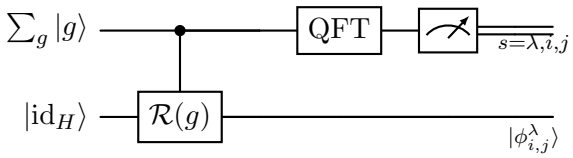


Figure 11: Sparking procedure in the quantum fire scheme from a one-way injective homomorphism. Here $\mathcal{R}(g)$ acts on elements of H by mapping $h \mapsto f(g) \cdot h$, where f is the homomorphism, and id_H is the identity element of H. Verification only checks that the label λ is the same, as in the quantum lightning scheme.

To clone states of this form, we apply the following circuit, which will produce two quantum fire registers $\sum_{k\in[d_\lambda]} |\phi^\lambda_{i,k}\rangle\,|\phi^\lambda_{k,j}\rangle$ with an entangled value of $k \in [d_\lambda]$.

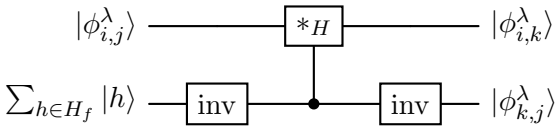


Figure 12: Cloning a quantum fire state. Here H_f is the image of the one-way injective homomorphism, inv is an operation that maps $h \in H$ to $h^{-1} \in H$, and $*_H$ is the group operation of H.

While this process produces an entangled state between the two registers, we note that it is not difficult to then unentangle the registers if we wish. This is done by performing a Fourier extraction on both states to extract the entangled indices $\sum_{k\in[d_\lambda]} |k\rangle\,|k\rangle$. We can then perform the reverse operation to inject a new pair of registers in the state $|j\rangle\,|i\rangle$, to get the tensor product state $|\phi^\lambda_{i,j}\rangle \otimes |\phi^\lambda_{i,j}\rangle$, that is, two identical copies of the original state.

Thus, the registers first become entangled, before then becoming unentangled again. This is thus an efficient cloning operation, that surprisingly does not go through any classical description of the state in question. While we leave open the problem of showing untelegraphability for this scheme under certain assumptions about G, H, or f, the fact that this method of cloning these

[22] We require that f is one-way because otherwise there is a way to telegraph the quantum fire states we describe, so the one-wayness is necessary for security of the scheme, although it is not clear that it is sufficient.

states is inherently an entangling operation justifies that it should not be possible to do across a classical channel.

3 Open Problems and Future Directions

We discuss directions for future work here.

1. Can Fourier extraction be used as a subroutine for other problems? For example, Fourier measurements play an important role in algorithms for the Abelian hidden subgroup problem. For the dihedral hidden subgroup problem it is known that the outcome of Fourier *measurements* on coset states does not yield sufficient information about the hidden subgroup, indicating that this is not the right way to generalize algorithms for the Abelian hidden subgroup problem. Perhaps another generalization, such as Fourier extraction, is the right way to generalize such algorithms to non-Abelian groups.

2. Can we construct other fully-quantum primitives using preaction secure group actions? There are many other primitives, like quantum copy-protection for certain classes of functions [Aar09, ALL+21, CMP24], one-shot signatures [AGKZ20], or quantum state obfuscation [BKNY23, CG24, BBV24] for which we have constructions relative to oracles and sometimes post-quantum indistinguishability obfuscation, but no plausible candidates in the plain model otherwise. Can we use non-Abelian group actions to find plausible candidate constructions for these primitives, and preaction security to prove their security?

3. As written, the preaction security game is not efficiently verifiable. In particular, the challenger in the game must themselves apply a preaction, which should be inefficient if the security holds. One could define a notion of trap-door preaction security, where the challenger has a secret key that allows them to efficiently perform a preaction, while any adversary without the key cannot distinguish between a random biaction and random action. However, we leave open the task of identifying good candidates for such trapdoor preaction security.

4. Can the untelegraphability of our quantum fire scheme be proven under any computational assumption about the groups G and H. We note that any such proof may also provide (under the same assumptions) a separation between QMA and QCMA, as noted in [NZ24].

5. The forward direction (going from the representation to Fourier extraction) of our approximate generalized duality theorem, when applied to $\mathbb{Z}_2$, yields a worse distinguishing advantage than the duality theorem of [AAS20]. This is because the implementation of an approximation of a representation might be off of the true representation by a phase that can depend on the input state. In the case of $\mathbb{Z}_2$, since there are only two states that the representation acts on, the phase can be corrected by applying a global phase corresponding to the difference of the two phases. However, it is not clear how to generalize this strategy past $\mathbb{Z}_2$, leading to our approximate duality not being tight. Can a tight version of our approximate duality theorem be proven?

4 Preliminaries

4.1 Quantum Preliminaries

A register R is a named finite-dimensional Hilbert space. When two registers appear next to each other, as in AB, this refers to the tensor product space of A and B. We write $\mathsf{tr}(\cdot)$ to denote the

trace, and $\mathsf{tr}_{\mathsf{B}}(\cdot)$ to denote the partial trace over a register B. We denote by $\|X\|_1 = \mathsf{tr}(|X|)$ the trace norm, where $|X| = \sqrt{XX^\dagger}$. For a vector space V, we write $\mathrm{GL}(V)$ to denote the general linear group from V to itself, i.e. invertible square matrices, and $U(V)$ to denote the unitary group. For two matrices in $\mathrm{GL}(V)$, we define the Hilbert-Schmidt inner product as follows.

Definition 4.1 (Hilbert-Schmidt inner product)**.** *Let $A, B \in \mathrm{GL}(\mathsf{R})$, then we define the* Hilbert-Schmidt inner product *between A and B to be*

$$\langle A, B\rangle = \frac{1}{\dim(\mathsf{R})}\mathsf{tr}\left[AB^\dagger\right] .$$

This implies a norm in the natural way: $\|A\| = \sqrt{\langle A, A\rangle}$.

4.2 Representation Theory

Definition 4.2 (Representation)**.** *Let G be a finite group. Then a function $\mathcal{R} : G \mapsto U(\mathsf{R})$ is a representation of G if the following holds for all group elements $g, h \in G$:*

$$\mathcal{R}(g)\mathcal{R}(h) = \mathcal{R}(gh) .$$

The vector space R is called a representation space of G. We note that representations need not be defined over Hilbert spaces (they can be defined over any vector space), but we will only ever consider representations that output unitaries in Hilbert spaces. We use the notation $\dim(\mathcal{R})$ to denote the dimension of the representation space R.

We will also need a notion of a function being "almost" a representation. The following is the definition of an ϵ-approximate representation (in Hilbert-Schmidt norm), taken from [GH16].

Definition 4.3 (ϵ-approximate representation [GH16])**.** *Let G be a group, and $\mathcal{R} : G \mapsto U(\mathsf{R})$ be a function taking group elements to unitaries over R. $\mathcal{R}$ is a ϵ-approximate representation if the following holds:*

$$\mathop{\mathbb{E}}_{g,h\in G}\left[\mathrm{Re}\left\langle \mathcal{R}(g)^\dagger\mathcal{R}(h), \mathcal{R}(g^{-1}h)^\dagger\right\rangle\right] \geq 1-\epsilon .$$

Here Re *denotes the real component of a complex number.*

We use the following additional definition of an ϵ-close representation, which is the notation of being close to an exact representation of a group, up to an isometry V.

Definition 4.4 (ϵ-close representation)**.** *Let G be a group and $\mathcal{R} : G \mapsto U(\mathsf{R})$ be a function taking group elements to unitaries over R. We say that $\mathcal{R}$ is ϵ-close to a representation of G if there exists another representation of G, $\mathcal{S} : G \mapsto U(\mathsf{S})$ and an isometry $V : \mathsf{R} \mapsto \mathsf{S}$ such that*

$$\mathop{\mathbb{E}}_{g\in G}\left\|\mathcal{R}(g) - V^\dagger\mathcal{S}(g)V\right\|^2 \leq \epsilon .$$

We will also need some definitions and facts from character theory. A reference for these can be found in, e.g. [S+77].

Definition 4.5 (Irreducible representation)**.** *A representation $\mathcal{R} : G \mapsto \mathrm{GL}(\mathsf{R})$ is an* irreducible representation *of G if for all subspaces $\mathsf{W} \subset \mathsf{R}$, $\mathcal{R}(g)\mathsf{W} \not\subseteq \mathsf{W}$. We sometimes refer to R as the irreducible representation of G. Irreducible representations are often called "*irreps*".*

We will use the notation ϱ to denote irreducible representations (when it is clear from context), and $\mathcal{R}$ to denote representations in general.

Definition 4.6 (Dual of a group)**.** *The* dual *of a group G, denoted $\widehat{G}$, is the set of all irreducible representations of G, up to equivalence by a unitary transformation. For an Abelian group, $\widehat{G}$ will itself have a group structure, but this is not generally the case for non-Abelian groups.*

We will use the notation $\lambda \in \widehat{G}$ to denote a "label" of an irreducible representation (think: a string that uniquely determines the identity of a particular irrep), and ϱ_λ denote the corresponding representation (the function from group elements to unitaries), although we may refer to both as an irreducible representation when it is clear from context.

Lemma 4.7 (Size of the dual)**.** *The size of the dual, $\widehat{G}$, of a group is equal to the number of conjugacy classes of G. In particular, for a finite group G, $\widehat{G}$ is also finite.*

Definition 4.8 (Character)**.** *Let $\mathcal{R} : G \mapsto \mathrm{GL}(\mathsf{R})$ be a representation of G. We define the* character *of $\mathcal{R}$ to be*

$$\chi_{\mathcal{R}}(g) = \mathsf{tr}[\mathcal{R}(g)]\,.$$

Definition 4.9 (Inner product of characters)**.** *Let $\chi_{\mathcal{R}}$ and $\chi_{\mathcal{S}}$ be two characters, then we define their inner product to be*

$$\langle \chi_{\mathcal{R}} | \chi_{\mathcal{S}} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathcal{R}}(g) \chi^\dagger_{\mathcal{S}}(g)\,.$$

Lemma 4.10 (Irreps are norm 1)**.** *For every irreducible representation of a group G, the following holds*

$$\langle \chi_\varrho | \chi_\varrho \rangle = 1\,.$$

Lemma 4.11 (Decomposition into irreps)**.** *Let $\mathcal{R}$ be a representation of a group G with representation space R, and let d_λ be $\langle \chi_{\mathcal{R}}, \chi_{\varrho_\lambda} \rangle$. Then the following holds:*

$$\mathsf{R} \simeq \bigoplus_{\lambda \in \widehat{G}} \mathsf{W}_\lambda^{\oplus d_\lambda}\,.$$

Where $\mathsf{W}_{\varrho_\lambda}$ is the irreducible representation space of ϱ_λ. Furthermore, the decomposition into $\mathsf{W}^{\oplus d_\lambda}$ is unique, the decomposition into further subspaces depends on the choice of basis. In the basis of $\bigoplus_\lambda \mathsf{W}_\lambda^{\oplus d_\lambda}$, $\mathcal{R}(g)$ looks like:

$$\sum_{\lambda \in \widehat{G}} \Pi_{\mathsf{W}_\lambda} \varrho_\lambda(g) \Pi_{\mathsf{W}_\lambda}\,.$$

Here Π_{W_λ} is the projector onto W_λ.

Definition 4.12 (Multiplicity of an irreducible representation)**.** *The number of irreducible representation spaces corresponding to the same irrep λ in $\mathcal{R}$ is its* multiplicity*, which we denote as $m_\lambda^{\mathcal{R}}$ (or m_λ when $\mathcal{R}$ is clear from context). The multiplicity subspaces of an irreducible representation λ within a representation $\mathcal{R}$, are the subspaces W_λ that are irreducible representation spaces of λ. The direct sum of all of the multiplicity subspaces of λ is the course Fourier subspace, also known as the* isotypic component *of λ. In fact, the breakdown of the isotypic component of λ into its multiplicity subspaces is basis-dependent and not unique.*

Definition 4.13 (Right/left regular representation)**.** *The left regular representation of a group G is the following function.*

$$\mathcal{L}(h) = \sum_{g \in G} |hg\rangle\langle g| \ .$$

The right regular representation of a group G is the following function.

$$\mathcal{R}(h) = \sum_{g \in G} |gh^{-1}\rangle\langle g| \ .$$

Lemma 4.14. *For all groups G and all irreducible representations of G, the following holds*

$$\langle \chi_{\mathcal{L}} | \chi_{\varrho} \rangle = \dim(\varrho) \, .$$

and similarly for the right regular representation.

Using this fact, together with the fact that the character of the right (or left) regular representation is equal to $|G|$ at the identity, and 0 elsewhere, we have:

Lemma 4.15. *Let G be a finite group, then the following holds.*

$$\sum_{\lambda \in \hat{G}} \dim(\varrho_\lambda)^2 = |G| \, .$$

Definition 4.16 (Plancherel measure)**.** *The Plancherel measure is a probability distribution over irreducible representations of a group G. The Plancherel measure of an irreducible representation with label λ is given by*

$$\mu(\lambda) = \frac{\dim(\varrho_\lambda)^2}{|G|} \, .$$

We can see that this corresponds to selecting an irreducible representation according to its "weight" in the sum of Lemma 4.15. A concept we will be interested in is the maximum Plancherel measure of any irreducible representation of the group. For example, for the symmetric group, upper and lower bounds are given by the following lemma.

Lemma 4.17 (Plancherel measure of the symmetric group [VK85])**.** *The following inequalities hold for constants $c_0 = 0.2313$ and $c_1 = 2.5651$*

$$e^{-\frac{c_1}{2}\sqrt{n}}\sqrt{n!} \leq \max_{\lambda \in \widehat{S_n}} \dim(\varrho_\lambda) \leq e^{-\frac{c_0}{2}\sqrt{n}}\sqrt{n!} \, .$$

Thus, the maximum Plancherel measure of an irreducible representation of the symmetric group, S_n, is $e^{-c_0\sqrt{n}}$, which is negligible in n.

Lemma 4.18 (Schur orthogonality relations [Iss05])**.** *Let $\varrho, \sigma \in \widehat{G}$ be irreducible representations of G. Then we have that:*

$$\sum_{g \in G} \varrho(g)^*_{i,j} \, \sigma(g)_{k,\ell} = \frac{|G|}{\dim(\varrho)} \delta_{\varrho,\sigma} \delta_{i,k} \delta_{j,\ell} \, .$$

4.2.1 Quantum Fourier Transform

Now we define the quantum Fourier transform for non-Abelian groups.

Definition 4.19 (Quantum Fourier transform)**.** *Let d_λ be the dimension of ϱ_λ for every irreducible representation of a group G. The quantum Fourier transform over a general group G is the following unitary transformation*

$$\mathrm{QFT}_G = \sum_{g\in G} \sum_{\substack{\lambda\in\widehat{G},\\ i,j\in[d_\lambda]}} \sqrt{\frac{d_\lambda}{|G|}}\, \varrho_\lambda(g)_{j,i}\, |\lambda,i,j\rangle\langle g| \ .$$

Its inverse is

$$\mathrm{QFT}_G^\dagger = \sum_{g\in G} \sum_{\substack{\lambda\in\widehat{G},\\ i,j\in[d_\lambda]}} \sqrt{\frac{d_\lambda}{|G|}}\, \varrho_\lambda(g^{-1})_{i,j}\, |g\rangle\langle\lambda,i,j| \ .$$

We will often refer to either one as the quantum Fourier transform over G, and it will be clear from context which one we mean.

We note that for Abelian groups, every irreducible representation is dimension 1, so the sum over i,j goes away, and we recover the usual Abelian quantum Fourier transform.

Definition 4.20 (Fourier basis states)**.** *For a group G, let $\{|\mathcal{L}^\lambda_{ij}\rangle\}_{\lambda\in\widehat{G},\, i,j\in[\dim(\varrho_\lambda)]}$, where $|\mathcal{L}^\lambda_{ij}\rangle := \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j}\, |g\rangle$, be the basis recovered by applying $\mathrm{QFT}_G^\dagger$ to $\{|\lambda,i,j\rangle\}_{\lambda\in\widehat{G},\, i,j\in[\dim(\varrho_\lambda)]}$. We call this the* (left-regular) Fourier basis *of G.*

4.3 Fourier Measurements

4.3.1 Coarse Fourier Measurement

Definition 4.21 (Coarse Fourier measurement)**.** *The coarse Fourier measurement[23] is the measurement of the subspaces corresponding to the irreducible representations, but not the basis of the subspaces. Formally, for a group G and representation $\mathcal{R}$, the coarse Fourier measurement is given by the POVM*

$$\left\{\Pi_{\mathsf{W}_\lambda^{\oplus m_\lambda}}\right\}_{\lambda\in\widehat{G}} \ .$$

Here the decomposition into unique subspaces $\mathsf{W}_\lambda^{\oplus m_\lambda}$ is given by Lemma 4.11.

Performing a measurement using the coarse Fourier measurement to produce a random irreducible representation label is known in the literature as *weak Fourier sampling*.

4.3.2 Fine Fourier Measurement

Definition 4.22 (Fine Fourier measurement)**.** *Let G be a finite group and $\mathcal{R}$ be a representation of that group. Let W_λ be an irreducible representation space of G, let $m_\lambda = \langle\chi_\mathcal{R}|\chi_{\varrho_\lambda}\rangle$, and $\{|\psi^\lambda_{i,j}\rangle\}_{i\in[\dim(\varrho_\lambda)],j\in[m_\lambda]}$ be a basis for the subspace $\mathsf{W}_\lambda^{\oplus m_\lambda}$. Then the fine Fourier measurement[23] is given by the POVM*

$$\{|\psi^\lambda_{i,j}\rangle\langle\psi^\lambda_{i,j}|\}_{\lambda,i,j} \ .$$

Performing a measurement using the fine Fourier measurement (for any choice of basis) is known in the literature as *strong Fourier sampling*.

4.3.3 Fourier Extraction

For our purposes, we require a stronger notion than Fourier *measurement*. We introduce a stronger notion called *Fourier extraction*. Unlike a Fourier measurement which measures and outputs a classical value for each irreducible representation space W_i^λ, Fourier extraction extracts a coherent quantum state out of each W_i^λ, maintaining the original superposition within W_i^λ but expressing it in the standard basis.

Definition 4.23 (Fourier extraction)**.** *Let G be a finite group and $\mathcal{R}$ be a representation of that group. A* Fourier extraction *is a coarse projective measurement $\{\Pi_\lambda\}_{\lambda\in\widehat{G}}$—where each Π_λ projects onto $\mathsf{W}_\lambda^{\oplus d_\lambda} := \bigoplus_{i\in[m_\lambda]} \mathsf{W}_i^\lambda$, the union of the multiplicity subspaces of λ—and a Fourier extraction within each subspace W_i^λ. Specifically, let each W_i^λ have basis $\{|\psi_{i,j}^\lambda\rangle\}_{j\in[\dim(\varrho_\lambda)]}$. Then a Fourier extraction implements a unitary*

$$\mathcal{M} : |\psi_{i,j}^\lambda\rangle\,|0\rangle \mapsto |\phi_i^\lambda\rangle\,|\lambda, j\rangle\ ,$$

*for some orthonormal set of "*archetype*" states $\{|\phi_i^\lambda\rangle\}_{\lambda\in\widehat{G},\, i\in[m_\lambda]}$.*[24]

4.4 Group Actions

A group action is a representation of a group that appears often in the field of cryptography. Formally, it is define as follows

Definition 4.24 (Group action)**.** *A group action consists of a family of groups $G = (G_n)_n$, a family of sets $\mathcal{X} = (\mathcal{X}_n)_n$, and a binary operation $* : G_n \times \mathcal{X}_n \mapsto \mathcal{X}_n$ satisfying the following properties*

- ***Identity:*** *Let $\mathrm{id} \in G$ be the identity element, then $0 * x = x$ for all $x \in \mathcal{X}_n$.*
- ***Representation:*** *For all $g, h \in G_n$ and $x \in \mathcal{X}_n$, $gh * x = g * (h * x)$.*

We sometimes require the following additional properties.

- ***Efficiently computable:*** *There is a quantum polynomial-time algorithm that on input 1^n outputs a description of G_n and an element $x_n \in \mathcal{X}_n$. The binary operation $*$ is also computable by a quantum polynomial-time algorithm.*
- ***Efficiently recognizable:*** *There is a quantum polynomial-time algorithm such that for any n and string y, the algorithm accepts with probability at least $2/3$ if $y \in \mathcal{X}_n$ and rejects with probability at least $2/3$ if $y \notin \mathcal{X}_n$.*
- ***Transitive:*** *There is exactly one orbit. That is, for any two elements $x, y \in \mathcal{X}_n$, exists a $g \in G_n$ such that $y = g * x$.*
- ***Semiregular:*** *(also called "free") There are no fixed points. That is, for every $g \in G_n$ and $y \in \mathcal{X}_n$, $g * x = x$ implies that $g = \mathrm{id}$.*

[23] The literature often refers to course and fine Fourier measurements as *weak* and *strong* Fourier sampling, respectively. We prefer to use the course and fine terminology, capturing how coarse- or fine-grained the decomposition of the space, but we will use the terms interchangeably.

[24] Note that the form of the archetype states does not matter. The only requirement is that they are orthonormal so that $\mathcal{M}$ is an isometry. That is, $\langle\psi_{ij}^\varrho \mid \psi_{k\ell}^\sigma\rangle = \delta_{\varrho\sigma}\delta_{ik}\delta_{j\ell}$.

- ***Regular:*** *Regular group actions are both transitive and semiregular. That is, for every $y \in \mathcal{X}_n$, there is exactly one $g \in G_n$ such that $y = g * x_n$.*

Later in the paper, we will describe additional properties of group actions that will be useful in proving security of cryptographic primitives constructed from group actions.

Definition 4.25 (Orbits of a group action)**.** *The* orbit *of an element $x \in \mathcal{X}$ is the set of elements accessible from x by acting with G:*

$$\mathsf{Orb}(x) = \{y \mid \exists g \in G \ \ \textbf{\textit{s.t.}} \ \ y = g * x\}\,.$$

One important property of group actions is they are representations on the Hilbert space spanned by the elements of $\mathcal{X}$.

Definition 4.26 (Group Action Representation)**.** *A group action of G defines a representation of G by the following unitary:*

$$\mathcal{R}(h)\,|g * x\rangle = |hg * x\rangle\ .$$

Note that this representation is isomorphic to a direct sum of left-regular representations on the different orbits of the group action.

4.5 Quantum Money and Quantum Lightning

Now we define public-key quantum money and quantum lightning. Both primitives have the similar syntax, with differences in how their key generation works.

Definition 4.27 (Public-key quantum money [Aar09])**.** *A public-key quantum money scheme is a triple of efficient quantum algorithms $\mathcal{S} = (\mathsf{KeyGen}, \mathsf{Mint}, \mathsf{Ver})$ where*

- KeyGen *takes as input the security parameter 1^n and outputs a private/public key pair $(\mathsf{sk}, \mathsf{pk})$,*
- $\mathsf{Mint}(\mathsf{sk})$ *outputs a pair $(s, |\$^s\rangle)$ where s is a string representing a serial number and $|\$^s\rangle$ is a quantum state representing a banknote,*[25] *and*
- Ver *takes as input the public key pk, a serial number s, and an alleged banknote σ, and either accepts or rejects.*

A public-key quantum money scheme $\mathcal{S}$ satisfies correctness if for all $n \in \mathbb{N}$,

$$\Pr\left[\mathsf{Ver}(\mathsf{pk}, s, |\$^s\rangle) \text{ accepts} : \begin{array}{c}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^n) \\ (s, |\$^s\rangle) \leftarrow \mathsf{Mint}(\mathsf{sk})\end{array}\right] \geq 1 - \mathsf{negl}(n)\,.$$

Definition 4.28 (Quantum money security)**.** *A public-key quantum money scheme $\mathcal{S}$ satisfies* ϵ-quantum-money security *if for all efficient adversaries A, the success probability of A in the counterfeit security game (Algorithm 1) is at most $\epsilon(n)$.*

Algorithm 1 (**Public-key Quantum Money Counterfeit Security Game**)**.**

1. Generate $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^n)$, $(s, |\$^s\rangle) \leftarrow \mathsf{Mint}(\mathsf{sk})$ and send $(\mathsf{pk}, s, |\$^s\rangle)$ to the adversary.
2. Adversary returns two registers AB in some potentially entangled state σ_{AB}.
3. Run $\mathsf{Ver}(\mathsf{pk}, s, \sigma_{\mathsf{A}})$ and $\mathsf{Ver}(\mathsf{pk}, s, \sigma_{\mathsf{B}})$. If either check rejects, then reject, otherwise accept.

[25] We will refer to these states interchangeably as either quantum money states or banknotes.

In place of full public-key quantum money schemes, we will often make use of quantum money *mini-schemes*, simpler objects that can be upgraded to public-key quantum money schemes using digital signatures [AC12]. Because of this effective equivalence, when it is clear from context, we will also often refer to quantum money mini-schemes as public-key quantum money.

Definition 4.29 (Quantum money mini-scheme [AC12])**.** *A quantum money scheme is a pair of efficient quantum algorithms* $\mathcal{S} = (\mathsf{Mint}, \mathsf{Ver})$ *where*

- $\mathsf{Mint}(1^\lambda)$ *outputs a pair* $(s, |\$^s\rangle)$ *where* s *is a string representing a serial number and* $|\$^s\rangle$ *is the banknote, and*
- Ver *takes as input a serial number* s *and an alleged banknote* σ*, and either accepts or rejects.*

The security is similar to that of full public-key quantum money setting:

Algorithm 2 (**Quantum Money Mini-Scheme Counterfeit Security Game**)**.**

1. Run $(s, |\$^s\rangle) \leftarrow \mathsf{Mint}(1^n)$ and send $(s, |\$^s\rangle)$ to the adversary.
2. Adversary returns two registers AB in some potentially entangled state σ_{AB}.
3. Run $\mathsf{Ver}(s, \sigma_{\mathsf{A}})$ and $\mathsf{Ver}(s, \sigma_{\mathsf{B}})$. If either check rejects, then reject, otherwise accept.

Definition 4.30 (Quantum money mini-scheme security)**.** *A quantum money mini-scheme scheme* $\mathcal{S}$ *satisfies* ϵ-quantum-money security *if for all efficient adversaries* A*, the success probability of* A *in the counterfeit security game (Algorithm 2) is at most* $\epsilon(n)$*.*

Quantum lightning is a stronger security guarantee on quantum money in which *not even the mint* can produce two banknotes for the same serial number [Zha21].

Algorithm 3 (**Quantum Lightning Counterfeit Security Game**)**.**

1. On input 1^n, adversary returns a serial number s and two registers AB in some potentially entangled state σ_{AB}.
2. Run $\mathsf{Ver}(s, \sigma_{\mathsf{A}})$ and $\mathsf{Ver}(s, \sigma_{\mathsf{B}})$. If either check rejects, then reject, otherwise accept.

Definition 4.31 (Quantum lightning security [Zha21])**.** *A quantum money mini-scheme scheme* $\mathcal{S}$ *satisfies* ϵ-quantum-lightning security *if for all efficient adversaries* A*, the success probability of* A *in the counterfeit security game (Algorithm 3) is at most* $\epsilon(n)$*.*

In each of the definitions, when ϵ is a negligible function in n, we say the scheme satisfies "strong" security.

5 Duality Theorem

In this section we present our main theorem, a computational duality between implementing a group representation and implmenting a Fourier extraction. We first present the exact case in Section 5.1.

Then, in Section 5.2, we show how to generalize it to the case of approximate representations and Fourier extractions.

5.1 Exact Case

Now we prove an exact version of the duality theorem, where the implementation of the representation and the Fourier extraction are perfect.

Theorem 5.1 (Quantum Duality for Representations of Groups, Exact Case)**.** *Let G be a finite group with an efficient quantum Fourier transform. Let $\mathcal{R} : G \to U(\mathsf{R})$ be a unitary representation of G, which decomposes into irreducible representations $\{(\lambda, W_i^\lambda)\}_{\lambda\in\widehat{G},i\in[m_\lambda]}$. Then the following are equivalent:*

1. *There exists a quantum circuit, $C_\mathcal{R}$, of size $s_\mathcal{R}$, that implements the representation $\mathcal{R}$. That is, it implements the unitary*

$$|g\rangle \otimes |\psi\rangle \mapsto |g\rangle \otimes \mathcal{R}(g)\,|\psi\rangle$$

   for all $g \in G$ and all $|\psi\rangle \in \mathsf{R}$.

2. *There exists a quantum circuit, $C_\mathcal{M}$, of size $s_\mathcal{M}$, that implements a Fourier extraction, $\mathcal{M}$, on the Fourier subspaces $\{W_i^\lambda\}_{\lambda\in\widehat{G},i\in[m_\lambda]}$. Specifically, let each W_i^λ have basis $\{|\psi_{i,j}^\lambda\rangle\}_{j\in[\dim(\varrho_\lambda)]}$. Then $C_\mathcal{M}$ implements*

$$\mathcal{M} : |\psi_{i,j}^\lambda\rangle\,|0\rangle \mapsto |\phi_i^\lambda\rangle\,|\lambda, j\rangle\ ,$$

   for some orthonormal set of "archetype" states $\{|\phi_i^\lambda\rangle\}_{\lambda\in\widehat{G},\,i\in[m_\lambda]}$.[26]

Going from Item 1 to Item 2, we have that $s_\mathcal{M}$ is $O(s_\mathcal{R} + s_{\mathrm{QFT}})$, where s_{QFT} is the circuit complexity of implementing the quantum Fourier transform of G. In the other direction, we have that $s_\mathcal{R} = O(s_\mathcal{M} + s_{\mathrm{QFT}})$.

Remark 5.2. *In the special case in which the group is* Abelian*, all the irreducible representations are 1-dimensional, so Item 2 above simplifies to a full projective measurement in the Fourier basis of the representation (the basis of states that are fixed by the representation). Moreover, the quantum Fourier transform for Abelian groups can always be implemented efficiently. Thus we get as a special case that for Abelian groups, the representation is directly dual to a Fourier measurement.*

Remark 5.3. *As an even more special case, the duality theorem of [AAS20] is the case in which $G \cong \mathbb{Z}_2$.*

Remark 5.4. *This theorem is phrased in terms of explicit quantum circuits. One might wonder if it still applies in the black-box setting. And indeed, we do not make use of any non-relativizing properties of these circuits, except to assume that we can access the inverse of $C_\mathcal{M}$ (i.e. a Fourier injection) in order to uncompute it. (We similarly require inverse queries to the group's quantum Fourier transform.) Therefore, we can simply modify the statement of Item 2 to require access to both $C_\mathcal{M}$ and $C_\mathcal{M}^\dagger$, and then it would hold the same way in the black-box setting.*

[26] Note that the form of the archetype states does not matter. The only requirement is that they are orthonormal so that $\mathcal{M}$ is an isometry.

Proof of 5.1. We prove both implications separately.

1 ⇒ 2: Suppose that Item 1 is true. That is, we have a circuit of size s that implements the representation $\mathcal{R}$. Let $\varrho_\lambda : G \to U(\mathsf{R})$ be an irreducible representation of G of dimension d_λ and multiplicity m_λ in $\mathcal{R}$, and let $W_1^\lambda, \ldots, W_{m_\lambda}^\lambda$ be the multiplicity subspaces of ϱ_λ in $\mathcal{R}$. For each subspace W_i^λ, take $\{|\psi_{i,j}^\lambda\rangle\}_{j\in[d_\lambda]}$ to be a basis for the subspace such that the corresponding unitary $\varrho_\lambda(g)$ sends $|\psi_{i,j}^\lambda\rangle$ to $\sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j} |\psi_{i,k}^\lambda\rangle$.[27]

Suppose we have a basis state $|\psi_{i,j}^\lambda\rangle$ on which we want to perform Fourier extraction to produce $|\phi_i^\lambda\rangle |\lambda, j\rangle$ (for some set of "archetype" states $|\phi_i^\lambda\rangle$).[28] We begin by preparing the the uniform superposition over the group $\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle$ in an ancilla register and then, controlled on that register, apply the promised circuit $C_\mathcal{R}$ for implementing $\mathcal{R}$ to our state.

$$\begin{aligned}
&\frac{1}{\sqrt{|G|}} \sum_{g\in G} \mathcal{R}(g) |\psi_{i,j}^\lambda\rangle \otimes |g\rangle \\
&= \frac{1}{\sqrt{|G|}} \sum_{g\in G} \sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j} |\psi_{i,k}^\lambda\rangle \otimes |g\rangle \\
&= \sum_{k\in[d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes \frac{1}{\sqrt{|G|}} \sum_{g\in G} \varrho_\lambda(g)_{k,j} |g\rangle
\end{aligned}$$

Inverting the group element in the last register gives

$$\begin{aligned}
&\to \sum_{k\in[d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes \frac{1}{\sqrt{|G|}} \sum_{g\in G} \varrho_\lambda(g)_{k,j} |g^{-1}\rangle \\
&= \sum_{k\in[d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes \frac{1}{\sqrt{|G|}} \sum_{g\in G} \varrho_\lambda(g^{-1})_{k,j} |g\rangle \\
&= \frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes |\mathcal{L}_{k,j}^\lambda\rangle \ ,
\end{aligned}$$

where $|\mathcal{L}_{kj}^\lambda\rangle$ is the jth basis vector of the kth multiplicity subspace of the irrep λ in the *left regular* representation of G. If we now perform a quantum Fourier transform on the second register, we get

$$\frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes |\lambda, k, j\rangle \ .$$

Reordering and regrouping the registers gives us

$$\left(\frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes |k\rangle \right) |\lambda, j\rangle = |\phi_i^\lambda\rangle |\lambda, j\rangle$$

If we wish, we can now measure the register containing λ to get the label of the irreducible representation space containing our state. Note that within subspace W_i^λ, this is a Fourier extraction that extracts out $|j\rangle$—the state in the standard basis corresponding to whichever state inside

[27] Technically, any basis of W_i^λ works fine, and we just need to unitarily transform the unitary $\varrho_\lambda(g)$ accordingly in our minds. However, it is convenient to consider a similar basis for all the subspaces W_i^λ corresponding to λ, so that we can write $\varrho_\lambda(g)$ in terms of its matrix elements $\varrho_\lambda(g)_{i,j}$ in the same way across all of them.

[28] We consider only basis states $|\psi_{i,j}^\lambda\rangle$ without loss of generality because the general case follows from linearity.

W_i^λ we started with[29] —and leaves behind the archetype state $|\phi_i^\lambda\rangle := \frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes |k\rangle$. Interestingly, observe that in this case, the reduced state on the first register of the archetype state for subspace W_i^λ is the fully mixed state on W_i^λ. This is not necessarily the case, however, for a general Fourier extraction, which may have any form of archetype state (as long as the archetype states form an orthonormal basis, which ensures that the Fourier extraction is an isometry).

2 ⇒ 1: Suppose that Item 2 is true. Then we have an circuit $C_{\mathcal{M}}$ implementing the Fourier extraction $\mathcal{M}$, which performs both a projective measurement $\{\Pi_\lambda\}_{\lambda\in\widehat{G}}$, where Π_λ projects onto subspace W^λ, the (possibly empty) union of some set of subspaces $W_1^\lambda, \ldots, W_{m_\lambda}^\lambda$—where each W_i^λ has dimension d_λ and is spanned by some basis $\{|\psi_{i,j}^\lambda\rangle\}_{j\in[d_\lambda]}$—and a Fourier extraction on each subspace W_i^λ:

$$\mathcal{M} : |\psi_{i,j}^\lambda\rangle \mapsto |\phi_i^\lambda\rangle\,|\lambda\rangle\,|j\rangle$$

for some orthonormal set of archetype states $|\phi_i^\lambda\rangle$.

We would like to perform $\mathcal{R}$, the representation defined by each irrep $\lambda \in \widehat{G}$ corresponding to irrep subspaces $W_1^\lambda, \ldots, W_{m_\lambda}^\lambda$. We receive as input a state of the form $|g\rangle\,|\psi\rangle$, with the first register containing a group element $g \in G$ for which we would like to implement its representation $\mathcal{R}(g)$, and the second register containing a quantum state $|\psi\rangle$ on which we would like to perform the representation.

Write $|\psi\rangle$ in the basis of the $|\psi_{i,j}^\lambda\rangle$'s as $|\psi\rangle = \sum_{\lambda,i,j} \alpha_{ij}^\lambda\,|\psi_{i,j}^\lambda\rangle$. We start by applying the promised circuit $C_{\mathcal{M}}$ for implementing $\mathcal{M}$ on $|\psi\rangle$ to get

$$|g\rangle \otimes \mathcal{M}\,|\psi\rangle = |g\rangle \otimes \sum_{\substack{\lambda\in\widehat{G}\\ i\in[m_\lambda]\\ j\in[d_\lambda]}} \alpha_{i,j}^\lambda\,|\phi_i^\lambda\rangle\,|\lambda\rangle\,|j\rangle\ .$$

Now, we claim that we can use two calls to the quantum Fourier transform of G and a single group operation to implement the irrep ϱ_λ, but we will return to this later. Assuming, for now, that we can do this, we apply it to this state to perform $\varrho_\lambda(g)$ on the last register:

$$\begin{aligned}
&|g\rangle \otimes \sum_{\lambda\in\widehat{G},i\in[n_\varrho],j\in[d_\lambda]} \alpha_{i,j}^\lambda\,|\phi_i^\lambda\rangle\,|\lambda\rangle \otimes \varrho_\lambda(g)\,|j\rangle\\
&= |g\rangle \otimes \sum_{\lambda\in\widehat{G},i\in[n_\varrho],j\in[d_\lambda]} \alpha_{i,j}^\lambda\,|\phi_i^\lambda\rangle \sum_{k\in[d_\lambda]} |\lambda\rangle \otimes \varrho_\lambda(g)_{k,j}\,|k\rangle\\
&= |g\rangle \otimes \sum_{\lambda\in\widehat{G},i\in[m_\lambda],j\in[d_\lambda]} \alpha_{i,j}^\lambda \sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j}\,|\phi_i^\lambda\rangle\,|\lambda\rangle\,|k\rangle\ .
\end{aligned}$$

[29] Note that the state that is extracted in the last register does not depend on which basis we chose for W_i^λ before. In fact, our choice was only a mathematical choice and did not actually affect the computation in any way. What determined the basis we got at the output was really our choice of the vectors $|\mathcal{L}_{k,j}^\lambda\rangle$ for the left regular representation, and these are determined simply by which quantum Fourier transform we chose to implement. Interestingly, with a Fourier extraction, since *all* the information about the original state within subspace W_i^λ is extracted into a single register in the standard basis, we do not have to decide on a basis ahead of time! We can convert a Fourier extraction in one basis to one in another basis *after the fact* by applying a unitary to the resulting extracted register.

We now use $C_{\mathcal{M}}^{\dagger}$ to un-compute the Fourier extraction on the last three registers, producing

$$\begin{aligned}
&|g\rangle \otimes \sum_{\lambda\in\widehat{G},i\in[m_\lambda],j\in[d_\lambda]} \alpha_{i,j}^{\lambda} \sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j} \,|\psi_{i,k}^{\lambda}\rangle \\
&= |g\rangle \otimes \sum_{\lambda\in\widehat{G},i\in[m_\lambda],j\in[d_\lambda]} \alpha_{i,j}^{\lambda} \;\; \mathcal{R}(g) \,|\psi_{i,j}^{\lambda}\rangle \\
&= |g\rangle \otimes \mathcal{R}(g) \sum_{\lambda\in\widehat{G},i\in[m_\lambda],j\in[d_\lambda]} \alpha_{i,j}^{\lambda} \,|\psi_{i,j}^{\lambda}\rangle \\
&= |g\rangle \otimes \mathcal{R}(g) \,|\psi\rangle \;.
\end{aligned}$$

We can see that this successfully implements the representation $\mathcal{R}(g)$.

It remains to show how to implement the irreps of G. It was observed by [Jor08] that this is possible using just the group's quantum Fourier transform, and we present it here for completeness. Given a state of the form $|g\rangle\,|\lambda\rangle\,|j\rangle$, where $g \in G$ is the group element for which we would like the perform the irrep, $\lambda \in \widehat{G}$ is the label of the irrep we would like to perform, and $j \in [d_\lambda]$ is a computational basis state within a Hilbert space of appropriate dimension, we would like to map it to $|g\rangle \otimes |\lambda\rangle \otimes \sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j} \,|k\rangle$.

We start by adding a multiplicity label, $i \in [d_\lambda]$. Technically any value will do, since it will have no effect and will be returned untouched, but since we will need to ensure that it fits within the size of of the corresponding irrep, we can always just take the first multiplicity subspace, that is, $i = 0$. We then have a state of the form $|g\rangle\,|\lambda\rangle\,|0\rangle\,|j\rangle$, onto which we apply the inverse quantum Fourier transform of G, to get

$$\begin{aligned}
|g\rangle \otimes \mathrm{QFT}_G^{\dagger}\,|\lambda\rangle\,|0\rangle\,|j\rangle &= |g\rangle\,|\mathcal{L}_{0,j}^{\lambda}\rangle \\
&= |g\rangle \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda(h^{-1})_{0,j} \,|h\rangle \;.
\end{aligned}$$

Applying the group operation of g onto h from the left gives

$$\begin{aligned}
&\to |g\rangle \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda(h^{-1})_{0,j} \,|gh\rangle \\
&= |g\rangle \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda(h^{-1}g)_{0,j} \,|h\rangle \\
&= |g\rangle \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \sum_{k\in[d_\lambda]} \varrho_\lambda(h^{-1})_{0,k} \;\varrho_\lambda(g)_{k,j} \,|h\rangle \\
&= |g\rangle \sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j} \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda(h^{-1})_{0,k} \,|h\rangle \\
&= |g\rangle \sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j} \,|\mathcal{L}_{0,k}^{\lambda}\rangle \;.
\end{aligned}$$

Applying once again the quantum Fourier transform of G produces $|g\rangle\,|\lambda\rangle\,|0\rangle \sum_{k\in[d_\lambda]} \varrho_\lambda(g)_{k,j} \,|k\rangle$, from which we can discard the ancilla to recover the desired state. □

From Theorem 5.1, we get the following interesting corollary, which may be of independent interest. It allows us to implement a representation of a group G by using a circuit for implementing a *different* representation of the same group G, as long as the representation we want shares irrep subspaces with the representation we have.

Corollary 5.5. *Given an efficient implementation of a representation $\mathcal{R} : G \mapsto U(\mathsf{R})$ that breaks R into some set of irreducible subspaces $\{W_i^\lambda\}_{\lambda\in\widehat{G},i\in[m_\lambda]}$, as well an efficiently computable function $r : \widehat{G} \to \widehat{G}$ mapping irrep labels appearing in $\mathcal{R}$ to other irreps of G having the same or smaller size, we can implement the new representation of the same group that acts on the same subspaces, but with each W_i^λ acted on by irrep $r(\lambda)$ instead of λ.*

In other words, given the implementation of one representation, we can implement many different other representations just by being able to compute the new desired irrep labels.

Main Idea. This results from a double application of Theorem 5.1. Once in the forward direction on the first representation to get a Fourier extraction on the subspaces, and then once in the backwards direction to get an implementation of the second representation. □

5.2 Approximate Case

Here we present an approximate duality theorem, in that the conditions of Item 1 and Item 2 have to hold approximately. In order to prove an approximate version of the duality theorem, we will need the following theorem from [GH16] regarding approximate representations.

Theorem 5.6 (Gowers-Hatami [GH16])**.** *Let G be a finite group, $\epsilon \geq 0$ and $\mathcal{R} : G \mapsto U(\mathsf{R})$ be an ϵ-approximate representation of G. Then there exists a register S of dimension $d' = (1+O(\epsilon))\dim(\mathsf{R})$, an isometry $V : \mathsf{R} \mapsto \mathsf{S}$ and an exact representation $\mathcal{S} : G \mapsto U(\mathsf{S})$ such that*

$$\mathop{\mathbb{E}}_{x\in G} \left\| \mathcal{R}(x) - V^\dagger \mathcal{S}(x) V \right\|^2 \leq 2\epsilon\,.$$

Where the norm $\|\cdot\|$ is implied by the dimension-normalized Hilbert-Schmidt inner product $\langle A, B\rangle = \mathsf{tr}[AB^\dagger]/\dim(\mathsf{R})$.

Remark 5.7. *While the matter of approximate representations has been extensively studied in mathematics and quantum computer science, the idea of an approximate measurement into irreducible representations has not been studied as much. In particular, the idea of weak (or strong) Fourier sampling is typically used in algorithms for solving problems in groups. For these kinds of problems, there is a well defined measurement that one can try to approximate. However in our case, as works from representation theory note [GH16, KK82], there may be vector spaces that admit approximate representations, but for which no exact representation exists. This raises the question of what a measurement into an invariant subspace* should *look like. [GH16] proposes a lemma pertaining to "approximately invariant subspaces", but it uses a notion of Fourier transform that is different from the quantum Fourier transform that we often consider. Here we propose a notion of approximate measurement onto an invariant subspace inspired by the result of [GH16], and use it in our duality result.*

Consider the following approximate versions of Theorem 5.1.

Theorem 5.8 (Approximate duality, forward direction)**.** *Let G be a finite group with a Fourier transform that can be implemented with a circuit of size s_{QFT}. Let $\mathcal{R} : G \mapsto U(\mathsf{R})$ be an ϵ-approximate representation of G with a circuit implementation of size $s_{\mathcal{R}}$, with R being an n-qubit*

register. Then there exists a register S*, an exact group representation* $\mathcal{S} : G \mapsto U(\mathsf{S})$ *and an isometry* V *mapping* R *to* S *such that for the Fourier decomposition* $\mathsf{S} = \bigoplus_{\lambda \in \widehat{G}, i \in [m_\lambda]} W_i^\lambda$ *and basis* $\{|\psi_{i,j}^\lambda\rangle\}_{\lambda \in \widehat{G}, i \in [m_\lambda],\, j \in [d_\lambda]}$ *of* $\mathcal{S}$ *as in Item 2 from Theorem 5.1, there is a circuit* C *of size* $O(s_{\mathcal{R}} + s_{\mathrm{QFT}})$*, and a set of archetype states* $\{|\phi_i^\lambda\rangle\}_{\lambda \in \widehat{G}, i \in [m_\lambda]}$*, such that*

$$\frac{1}{\dim(\mathsf{S})} \sum_{\substack{\lambda \in \widehat{G}, i \in [n_\lambda] \\ j \in [d_\lambda]}} \mathrm{Re}\, \langle \phi_i^\lambda | \otimes \langle \lambda, j |\, V C V^\dagger\, |\psi_{i,j}^\lambda\rangle \geq 1 - \epsilon\,.$$

That is, we get an ϵ*-approximate Fourier extraction.*

Proof. We let C be the same circuit as in the exact case, first preparing the state $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle$, and applying the representation $\mathcal{R}(g)$ controlled on that register to the state. We also let the archetype states be $|\phi_i^\lambda\rangle = \frac{1}{\sqrt{d_\lambda}} \sum_{k \in [d_\lambda]} |\psi_{i,k}^\lambda\rangle \otimes |k\rangle$ as in the exact case, where $d_\lambda := \dim(\varrho_\lambda)$. We can compute the quantity from the theorem statement as:

$$
\begin{aligned}
&\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\langle\phi_i^\lambda|\langle\lambda,j|VCV^\dagger|\psi_{i,j}^\lambda\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\langle\phi_i^\lambda|\langle\lambda,j|(V\otimes\mathrm{id})(\mathrm{id}\otimes\mathrm{QFT})\cdot\sum_{g\in G}\mathcal{R}(g)\otimes|g^{-1}\rangle\langle g^{-1}|\cdot(\mathrm{id}\otimes\mathrm{QFT}^\dagger)(V\otimes\mathrm{id})^\dagger|\psi_{i,j}^\lambda\rangle|0\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{\sqrt{d_\lambda}}\sum_k\langle\psi_{i,k}^\lambda|\langle\mathcal{L}_{k,j}^\lambda|(V\otimes\mathrm{id})\cdot\sum_{g\in G}\mathcal{R}(g)\otimes|g^{-1}\rangle\langle g^{-1}|\cdot(\mathrm{id}\otimes\mathrm{QFT}^\dagger)(V\otimes\mathrm{id})^\dagger|\psi_{i,j}^\lambda\rangle|0\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{\sqrt{d_\lambda}}\sum_k\langle\psi_{i,k}^\lambda|\langle\mathcal{L}_{k,j}^\lambda|(V\otimes\mathrm{id})\cdot\sum_{g\in G}\mathcal{R}(g)\otimes|g^{-1}\rangle\langle g^{-1}|\cdot(V\otimes\mathrm{id})^\dagger|\psi_{i,j}^\lambda\rangle\frac{1}{\sqrt{|G|}}\sum_{g'\in G}|g'\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{\sqrt{d_\lambda}}\sum_k\langle\psi_{i,k}^\lambda|\langle\mathcal{L}_{k,j}^\lambda|(V\otimes\mathrm{id})\cdot\left(\frac{1}{\sqrt{|G|}}\sum_{g\in G}\mathcal{R}(g)\otimes\mathrm{id}\right)\cdot(V\otimes\mathrm{id})^\dagger|\psi_{i,j}^\lambda\rangle|g^{-1}\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\frac{1}{\sqrt{d_\lambda}}\sum_k\langle\psi_{i,k}^\lambda|\langle\mathcal{L}_{k,j}^\lambda|(V\otimes\mathrm{id})\cdot(\mathcal{R}(g)\otimes\mathrm{id})\cdot(V\otimes\mathrm{id})^\dagger|\psi_{i,j}^\lambda\rangle|g^{-1}\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\frac{1}{\sqrt{d_\lambda}}\sum_k\langle\psi_{i,k}^\lambda|\langle\mathcal{L}_{k,j}^\lambda|(V\mathcal{R}(g)V^\dagger\otimes\mathrm{id})|\psi_{i,j}^\lambda\rangle|g^{-1}\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\frac{1}{\sqrt{d_\lambda}}\sum_k\langle\psi_{i,k}^\lambda|V\mathcal{R}(g)V^\dagger|\psi_{i,j}^\lambda\rangle\langle\mathcal{L}_{k,j}^\lambda|g^{-1}\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\frac{1}{\sqrt{d_\lambda}}\sum_k\langle\psi_{i,k}^\lambda|V\mathcal{R}(g)V^\dagger|\psi_{i,j}^\lambda\rangle\sqrt{\frac{d_\lambda}{|G|}}\sum_{h\in G}\varrho(h^{-1})_{k,j}^*\langle h|g^{-1}\rangle \qquad (2)\\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{|G|}\sum_{g\in G}\sum_k\varrho_\lambda(g)_{k,j}^*\langle\psi_{i,k}^\lambda|V\mathcal{R}(g)V^\dagger|\psi_{i,j}^\lambda\rangle \\
&=\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\frac{1}{|G|}\sum_{g\in G}\langle\psi_{i,j}^\lambda|\mathcal{S}(g)^\dagger V\mathcal{R}(g)V^\dagger|\psi_{i,j}^\lambda\rangle \qquad (3)\\
&=\mathop{\mathbb{E}}_{g\in G}\frac{1}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\operatorname{Re}\langle\psi_{i,j}^\lambda|\mathcal{S}(g)^\dagger V\mathcal{R}(g)V^\dagger|\psi_{i,j}^\lambda\rangle \\
&=\mathop{\mathbb{E}}_{g\in G}\frac{1}{\dim(\mathsf{S})}\operatorname{Re}\operatorname{tr}\left[\mathcal{S}(g)^\dagger V\mathcal{R}(g)V^\dagger\right] \qquad (4)\\
&=\mathop{\mathbb{E}}_{g\in G}\operatorname{Re}\left\langle\mathcal{S}(g),V^\dagger\mathcal{R}(g)V\right\rangle \qquad (5)\\
&=1-\frac{1}{2}\mathop{\mathbb{E}}_{g\in G}\left\|\mathcal{R}(g)-V^\dagger\mathcal{S}(g)V\right\|^2 \qquad (6)\\
&\geq 1-\epsilon\,.
\end{aligned}
$$

Here the first line is expanding out the definition of the circuit as a quantum Fourier transform, controlled $\mathcal{R}$,[30] and then an inverse quantum Fourier transform. (There is also rearrangement of registers, but this is implicit in order to simplify notation.) The second and third lines applies the inverse Fourier transform to the $|0\rangle$ state, which represents the trivial irrep of G, as well as to

[30]Technically, we control on g^{-1}, but this is just so that we can use the left-regular Fourier transform, rather than the right-regular one. This is not essential, but it slightly simplifies the notation.

the $\langle \lambda, k, j|$ (commuting it past the V, which acts only on the first register). The line labeled 2 expands the definition of $|\mathcal{L}^{\lambda}_{k,j}\rangle$, and line 3 uses the fact that $\mathcal{S}$ exactly performs the representation on the basis of the states $|\psi^{\lambda}_{i,j}\rangle$. Line 4 uses the fact that the states $|\psi^{\lambda}_{i,j}\rangle$ form a complete basis for S. Line 5 uses the definition of the Hilbert Schmidt inner product, line 6 uses the fact that $\|A - B\| = \sqrt{2 - 2\operatorname{Re}\langle A, B\rangle}$, and the last line uses the bound from Theorem 5.6. □

We note that this part of the duality theorem preserves the error between the representation and the measurement.

Remark 5.9. *The forward direction could equivalently be phrased as follows: Let $\mathcal{R}$ be 2ϵ-close to an exact representation $\mathcal{S}$ under isometry V, then there is an implementation of ϵ-approximate Fourier extraction up to V with a circuit whose size of $O(s_{\mathcal{R}} + s_{\mathrm{QFT}})$.*

We can also show the other direction, albeit with (we believe) sub-optimal error scaling.

Theorem 5.10 (Approximate duality, reverse direction)**.** *Let G be a finite group with a Fourier transform that can be implemented with a circuit of size s_{QFT}. Let R and S be two registers with an isometry V mapping R to S, and let $\mathcal{S}$ be an exact representation on S. Say that we have a circuit $C_{\mathcal{M}}$ of size $s_{\mathcal{M}}$ which implements an ϵ-approximate Fourier extraction in R, satisfying*

$$\frac{1}{\dim(\mathsf{S})} \sum_{\lambda,i,j} \operatorname{Re} \langle \phi^{\lambda}_i| \otimes \langle \lambda, j| \, (V \otimes \mathrm{id}) \mathcal{M} (V^\dagger \otimes \mathrm{id}) \, |\psi^{\lambda}_{i,j}\rangle \otimes |0\rangle \geq 1 - \epsilon \,.$$

Then there exists a circuit of size $O(s_{\mathcal{M}} + s_{\mathrm{QFT}})$ which implements a map $\mathcal{R}$ of G on R, that is 2ϵ-close to $\mathcal{S}$, i.e. one satisfying

$$\mathop{\mathbb{E}}_{g \in G} \left\| V \mathcal{R}(g) V^\dagger - \mathcal{S}(g) \right\|^2 \leq 2\epsilon \,.$$

Proof. The implementation of $\mathcal{R}$ will be identical to the one from Theorem 5.1. In particular, $\mathcal{R}(g)$ will first apply $\mathcal{M}$ to measure λ and extract j, then apply $\varrho_\lambda(g)$ to the register containing j, and finally it will un-compute $\mathcal{M}$.

We can proceed by evaluating the average difference between $V\mathcal{R}(g)V^\dagger$ and $\mathcal{S}(g)$ under the Hilbert-Schmidt norm.

$$\begin{aligned}
&\mathop{\mathbb{E}}_{g \in G} \left\| V \mathcal{R}(g) V^\dagger - \mathcal{S}(g) \right\|^2 \\
&\quad = \mathop{\mathbb{E}}_{g \in G} \langle V \mathcal{R}(g) V^\dagger - \mathcal{S}(g), V \mathcal{R}(g) V^\dagger - \mathcal{S}(g) \rangle \\
&\quad = \mathop{\mathbb{E}}_{g \in G} \frac{1}{\dim(\mathsf{S})} \mathsf{tr} \left[V \mathcal{R}(g) V^\dagger V \mathcal{R}(g)^\dagger V^\dagger + \mathcal{S}(g) \mathcal{S}(g)^\dagger - V \mathcal{R}(g)^\dagger V^\dagger \mathcal{S}^\dagger(g) - \mathcal{S}(g) V \mathcal{R}(g) V^\dagger \right] \\
&\quad = 2 - \mathop{\mathbb{E}}_{g \in G} \frac{1}{\dim(\mathsf{S})} \mathsf{tr} \left[V \mathcal{R}(g) V^\dagger \mathcal{S}^\dagger(g) + \mathcal{S}(g) V \mathcal{R}(g)^\dagger V^\dagger \right] \qquad (7)
\end{aligned}$$

Here we note that the implementation of $\mathcal{R}(g)$ is always unitary, and $V^\dagger V = \mathrm{id}$, so the first two terms are the the identity on S. Now we lower bound the second term. We begin by writing it as two times the real component of a trace, and expand the definitions of $\mathcal{S}$ and $\mathcal{R}$.

$$\begin{aligned}
\mathop{\mathbb{E}}_{g \in G} \operatorname{Re} \frac{2}{\dim(\mathsf{S})} \mathsf{tr} \left[V \mathcal{R}(g) V^\dagger \mathcal{S}^\dagger(g) \right] &= \mathop{\mathbb{E}}_{g \in G} \frac{2}{\dim(\mathsf{S})} \operatorname{Re} \sum_{\lambda,i,j} \langle \psi^{\lambda}_{i,j}| \, V \mathcal{R}(g) V^\dagger \mathcal{S}(g) \, |\psi^{\lambda}_{i,j}\rangle \\
&= \mathop{\mathbb{E}}_{g \in G} \frac{2}{\dim(\mathsf{S})} \operatorname{Re} \sum_{\lambda,i,j,k} \varrho_\lambda(g)^\dagger_{k,j} \, \langle \psi^{\lambda}_{i,j}| \, V \mathcal{R}(g) V^\dagger \, |\psi^{\lambda}_{i,k}\rangle \,.
\end{aligned}$$

Now, we expand out the definition of $\mathcal{R}$. This yields the following state.

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{g\in G}\frac{2}{\dim(\mathsf{S})}\mathrm{Re}\sum_{\lambda,i,j,k}\varrho_\lambda(g)^\dagger_{k,j}\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger\varrho_\lambda(g)\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\\
&\quad=\mathop{\mathbb{E}}_{g\in G}\frac{2}{\dim(\mathsf{S})}\mathrm{Re}\sum_{\substack{\lambda,i,j,k\\ \lambda',a,b}}\varrho_\lambda(g)^\dagger_{k,j}(\langle\phi^{\lambda'}_a|\otimes\langle\lambda',b|)(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger\varrho_\lambda(g)(V^\dagger\otimes\mathrm{id})\left|\phi^{\lambda'}_a\right\rangle|\lambda',b\rangle\\
&\quad=\mathop{\mathbb{E}}_{g\in G}\frac{2}{\dim(\mathsf{S})}\mathrm{Re}\sum_{\substack{\lambda,i,j,k\\ \lambda',a,b,c}}\varrho_\lambda(g)^\dagger_{k,j}\varrho_{\lambda'}(g)_{c,b}(\langle\phi^{\lambda'}_a|\otimes\langle\lambda',b|)(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger(V^\dagger\otimes\mathrm{id})\left|\phi^{\lambda'}_a\right\rangle|\lambda',c\rangle\\
&\quad=\mathop{\mathbb{E}}_{g\in G}\frac{2}{\dim(\mathsf{S})}\mathrm{Re}\sum_{\substack{\lambda,i,j,k\\ \lambda',a,b,c}}\varrho_\lambda(g)^\dagger_{k,j}\varrho_{\lambda'}(g)_{c,b}(\langle\phi^{\lambda'}_a|\otimes\langle\lambda',b|)(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger(V^\dagger\otimes\mathrm{id})\left|\phi^{\lambda'}_a\right\rangle|\lambda',c\rangle\\
&\quad=\frac{2}{\dim(\mathsf{S})}\mathrm{Re}\sum_{\substack{\lambda,i,j,k\\ \lambda',a,b,c}}\mathop{\mathbb{E}}_{g\in G}\left[\varrho_\lambda(g)^\dagger_{k,j}\varrho_{\lambda'}(g)_{c,b}\right](\langle\phi^{\lambda'}_a|\otimes\langle\lambda',b|)(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger(V^\dagger\otimes\mathrm{id})\left|\phi^{\lambda'}_a\right\rangle|\lambda',c\rangle\\
&\quad=\frac{2}{\dim(\mathsf{S})}\mathrm{Re}\sum_{\lambda,a,i,j,k}\frac{1}{d_\lambda}(\langle\phi^{\lambda'}_a|\otimes\langle\lambda,j|)(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger(V^\dagger\otimes\mathrm{id})\left|\phi^\lambda_a\right\rangle|\lambda,k\rangle\\
&\quad=\mathrm{Re}\frac{2}{\dim(\mathsf{S})}\mathsf{tr}\left[\sum_{\lambda,i,j,k}\frac{1}{d_\lambda}\mathrm{id}\otimes|\lambda,j\rangle\langle\lambda,k|\,(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger(V^\dagger\otimes\mathrm{id})\right]\\
&\quad=\mathrm{Re}\frac{2}{\dim(\mathsf{S})}\mathsf{tr}\left[\sum_{\lambda,i,j,k}\frac{1}{d_\lambda}\mathrm{id}\otimes|\lambda,j\rangle\langle\lambda,k|\,\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger\right]\\
&\quad=\mathrm{Re}\frac{2}{\dim(\mathsf{S})}\sum_{\lambda,i,j,k}\frac{1}{d_\lambda}\left\langle\phi^\lambda_i\right|\otimes\langle\lambda,k|\,(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,k}\right\rangle\left\langle\psi^\lambda_{i,j}\right|V\mathcal{M}^\dagger(V^\dagger\otimes\mathrm{id})\left|\phi^\lambda_i\right\rangle\otimes|\lambda,j\rangle\\
&\quad\geq\mathrm{Re}\frac{2}{\dim(\mathsf{S})}\sum_{\lambda,i}\frac{1}{d_\lambda}\left(\sum_j\left\langle\phi^\lambda_i\right|\otimes\langle\lambda,j|\,(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,j}\right\rangle\right)^2\\
&\quad\geq\mathrm{Re}\frac{2}{\dim(\mathsf{S})}\sum_{\lambda,i,j}\left\langle\phi^\lambda_i\right|\otimes\langle\lambda,j|\,(V\otimes\mathrm{id})\mathcal{M}V^\dagger\left|\psi^\lambda_{i,j}\right\rangle\\
&\quad\geq 2(1-\epsilon)\\
&\quad\geq 2-2\epsilon\,.
\end{aligned}
$$

Here, we insert identity matrices between ϱ_λ and $\mathcal{M}$, and we use the definition of the inner product. Then, we use the Schur orthogonality relations to cancel the terms where $\varrho_\lambda\neq\varrho_{\lambda'}$ or $(k,j)\neq(c,b)$. Then we use the definition of the trace, and the cyclic property. Finally, since $(V\otimes\mathrm{id})$ commutes with $\mathrm{id}\otimes|\lambda,j\rangle\langle\lambda,k|$, we can move it to the other side using the cyclic property. Then we use the fact that $|\phi^\lambda_i\rangle\langle\phi^\lambda_i|\otimes|\lambda,j\rangle\langle\lambda,k|\preceq\mathrm{id}\otimes|\lambda,j\rangle\langle\lambda,k|$, together with the cyclic property of the trace. Finally, we apply Cauchy-Schwarz twice on the sum over j and k, and the assumption about the performance of $\mathcal{M}$ on an average state from $V^\dagger\mathsf{S}$.

Plugging this back into Equation (7), we get the following upper bound on the average distance

between $\mathcal{S}$ and $\mathcal{R}$:

$$\begin{aligned}\mathop{\mathbb{E}}_{g\in G}\left\|V\mathcal{R}(g)V^\dagger - \mathcal{S}(g)\right\|^2 &\leq 2 - \mathop{\mathbb{E}}_{g\in G}\frac{1}{\dim(\mathsf{S})}\mathsf{tr}\left[V\mathcal{R}(g)V^\dagger\mathcal{S}^\dagger(g) + \mathcal{S}(g)V\mathcal{R}(g)^\dagger V^\dagger\right]\\ &\leq 2 - (2-2\epsilon)\\ &\leq 2\epsilon\,,\end{aligned}$$

as desired. □

We note that while in the forward direction (Theorem 5.8), our duality theorem preserves the inner product error from the approximate representation, we are not able to prove a perfectly tight approximate duality because the reverse direction (Theorem 5.10) yields a different notion of approximate representation, i.e. being close (up to an isometry) to a real representation. Applying the definition of ϵ-approximate representation directly would not yield the same ϵ as we started with in the reverse direction. Note that if we had defined the forward direction in the same way, using the result of [GH16], we would get a perfect duality, but the notion of approximate representation from Definition 4.3 is more widely used. We leave it as an open question whether an ϵ-approximate representation can be recovered in the reverse direction.

Comparison with [AAS20]. We comment on how our approximate duality (Theorems 5.8 and 5.10) relates to the approximate duality theorem from [AAS20, Theorem 2]. Let $|x\rangle$ and $|y\rangle$ be two orthogonal quantum states and U be a unitary such that

$$\begin{aligned}\langle y|\,U\,|x\rangle &= a\\ \langle x|\,U\,|y\rangle &= b\,.\end{aligned}$$

Unlike in the general case of Theorem 5.8, in this case, the fact that $|x\rangle$ and $|y\rangle$ are orthogonal implies that there exists a unitary $\widehat{U}$ in the *same* register such that $\widehat{U}$ exactly swaps $|x\rangle$ and $|y\rangle$. As a representation of $\mathbb{Z}_2$, we thus have the efficient ϵ-close representation $\mathcal{R} : g \mapsto U^g$ and an exact representation $\mathcal{S} : g \mapsto \widehat{U}^g$. We then have the following:

$$\begin{aligned}\mathop{\mathbb{E}}_{g\in\mathbb{Z}_2}\left\|U^g - \widehat{U}^g\right\|^2 &= \frac{1}{2}\left(\|\mathrm{id}-\mathrm{id}\|^2 + \left\|U-\widehat{U}\right\|^2\right)\\ &= \frac{1}{2}\langle U-\widehat{U}, U-\widehat{U}\rangle\\ &= \frac{1}{4}\mathsf{tr}[(U-\widehat{U})(U-\widehat{U})^\dagger]\\ &= \frac{1}{4}\left(4 - \mathsf{tr}[U\widehat{U}^\dagger] - \mathsf{tr}[\widehat{U}U^\dagger]\right)\\ &= 1 - \frac{1}{4}\mathrm{Re}\,(2a+2b)\\ &= 1 - \frac{\mathrm{Re}\,(a+b)}{2} =: 2\epsilon\,.\end{aligned}$$

Here we use the fact that $\mathsf{tr}[U\widehat{U}^\dagger] = \langle x|\,U\,|y\rangle + \langle y|\,U\,|x\rangle = a+b$ since $\widehat{U}$ exactly swaps $|x\rangle$ and $|y\rangle$, and similarly for $\mathsf{tr}[\widehat{U}U^\dagger]$. Let $\mathcal{M}$ be the measurement implied by the forward direction of the approximate duality (the Fourier extraction simplifies to a binary projective measurement for the case of $\mathbb{Z}_2$). This is an approximate distinguishing measurement between the states $|\psi\rangle = \frac{|x\rangle+|y\rangle}{\sqrt{2}}$ and $|\phi\rangle = \frac{|x\rangle-|y\rangle}{\sqrt{2}}$ (i.e. the states corresponding to the two one-dimensional irreducible representations of

$\mathcal{S}$), and we calculate the bias below. We assume here without loss of generality that the probability of accepting $|\psi\rangle$ is higher than the probability of accepting $|\phi\rangle$, and that $|0\rangle\langle 0|$ corresponds to the accept outcome. If these are not the case, then the roles of $|\psi\rangle$ and $|\phi\rangle$ or 0 and 1 can be swapped.

$$\begin{aligned}
|(\mathrm{id}\otimes\langle 0|)\,\mathcal{M}\,|\psi\rangle|^2 - |(\mathrm{id}\otimes\langle 0|)\,\mathcal{M}\,|\phi\rangle|^2 &= |(\mathrm{id}\otimes\langle 0|)\,\mathcal{M}\,|\psi\rangle|^2 - \left(1 - |(\mathrm{id}\otimes\langle 1|)\,\mathcal{M}\,|\phi\rangle|^2\right) \\
&= |(\mathrm{id}\otimes\langle 0|)\,\mathcal{M}\,|\psi\rangle|^2 + |(\mathrm{id}\otimes\langle 1|)\,\mathcal{M}\,|\phi\rangle|^2 - 1 \\
&\geq \frac{1}{2}(|(\mathrm{id}\otimes\langle 0|)\,\mathcal{M}\,|\psi\rangle| + |(\mathrm{id}\otimes\langle 1|)\,\mathcal{M}\,|\phi\rangle|)^2 - 1 \\
&\geq 2\left(\frac{1}{2}\left(\mathrm{Re}\,(\mathrm{id}\otimes\langle 0|)\,\mathcal{M}\,|\psi\rangle + \mathrm{Re}\,(\mathrm{id}\otimes\langle 1|)\,\mathcal{M}\,|\phi\rangle\right)\right)^2 - 1 \\
&\geq 2\left(\frac{1}{2} + \frac{\mathrm{Re}(a+b)}{4}\right)^2 - 1 \\
&= 2\left(\frac{1}{4} + \frac{\mathrm{Re}(a+b)}{4} + \frac{\mathrm{Re}(a+b)^2}{16}\right) - 1 \\
&= \frac{\mathrm{Re}(a+b)}{2} + \frac{\mathrm{Re}(a+b)^2}{8} - \frac{1}{2}\,.
\end{aligned}$$

Here we note that the error bound is much weaker than the tight bound proved in [AAS20]. While our approximate duality theorem is tight with respect to the Hilbert-Schmidt inner product, it does not necessarily recover an optimal *distinguishing* measurement. The bound in [AAS20] in fact modifies modifies the circuit to get a tighter bound, and we comment on this more later.

In the other direction, assume that we have a measurement that accepts $|\psi\rangle$ with probability p and $|\phi\rangle$ probability $p-\Delta$. Then we can first construct a measurement that applies the original measurement, copies the result over, and un-computes the measurement. For this measurement, we have the following:

$$\mathrm{Re}(\mathrm{id}\otimes\langle 0|)\mathcal{M}\,|\psi\rangle = \sqrt{p}\,.$$

and similarly

$$\mathrm{Re}(\mathrm{id}\otimes\langle 1|)\mathcal{M}\,|\phi\rangle = \sqrt{1-(p-\Delta)}\,.$$

Note that in this case Theorem 5.10 works up to any unitary applied to $|\psi\rangle$ and $|\phi\rangle$, since they are still orthogonal and thus are a basis for some exact representation of $\mathbb{Z}_2$. So we can always pick a unitary on the first register such that the archetype states are exactly the residual states of $\mathcal{M}$ after measuring. Then we have the following bound on the condition of Theorem 5.10:

$$\begin{aligned}
1-\epsilon &= \frac{1}{2}\left(\sqrt{p} + \sqrt{1-p+\Delta}\right) \\
&\geq \sqrt{\frac{1+\Delta}{2}}\,.
\end{aligned}$$

Here we minimize this expression over p by setting $p = \frac{1+\Delta}{2}$. Let U be the unitary we implement when applying Theorem 5.10 and $\widehat{U}$ be the unitary that swaps $|x\rangle$ and $|y\rangle$. Combined with our calculation before, we have the following

$$\mathop{\mathbb{E}}_{g\in\mathbb{Z}_2}\left\|U^g - \widehat{U}^g\right\|^2 = 1 - \frac{\mathrm{Re}(a+b)}{2} \leq 2\left(1 - \sqrt{\frac{1+\Delta}{2}}\right)\,.$$

Here a and b are $\langle x|\,U\,|y\rangle$ and $\langle y|\,U\,|x\rangle$ respectively. Rearranging terms, we have that

$$\frac{\mathrm{Re}(a+b)}{2} \geq 2\sqrt{\frac{1+\Delta}{2}} - 1 \geq \Delta\,.$$

The reason we are able to get a tighter duality in this direction is because we can alter the measurement *before hand* so that the real component becomes the same as the absolute value, where as to do the same in the forward direction requires modifying the unitary in a way that depends on the group element, and thus would need to be written into the implementation of the duality theorem itself.

Thus, we recover a non-tight version of the approximate duality from [AAS20]. As noted before, in order to get a tighter bound, the approximate duality of [AAS20] analyzes a slightly different algorithm, in which instead of controlling the swap on the positive superposition between $|0\rangle$ and $|1\rangle$, the control qubit is initialized as $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$, with an arbitrary phase that depends on a and b. In our case, this corresponds to initializing the control register with a state that differs from the uniform positive superposition on the group (i.e. the trivial irrep). Specifically, each group element would receive a phase that depends on the Hilbert Schmidt inner product between the ϵ-close representation and some exact representation on g (since we have the freedom to alter the isometry and unitary, we can take any exact representation). This does not work naïvely, in part because it would seem to require computing an exponential number of complex phases (in the size of the binary representation of the group), but we suspect that such a strategy may be possible in order to get a tighter bound. We leave it to future work to prove a tighter version of the generalized duality theorem.

Remark 5.11. *One might wonder what would happen if we proved a similar theorem, but instead starting from the result of [KK82]. Here, the definition of ϵ-approximate is with respect to the operator norm, but there is no need for an isometry in the resulting exact representation. However, the stricter requirements on this approximate representation make it hard to apply to "approximate adversaries" in the way that we would want. In particular, an adversary that breaks some game with inverse polynomial probability might succeed with very high probability in some cases, but 0 in others. This means that the result of [KK82] does not help us transform these adversaries into other useful adversaries.*

6 Quantum Lightning From Non-Abelian Group Actions

We generalize the construction of quantum money / lightning of [Zha24] to general group actions. This allows us to instantiate the construction from a potentially much wider class of group action instantiations. Generalizing to non-Abelian groups, specifically, also allows us to show a security reduction from a concrete computational assumption *in the plain model*.[31] (See Section 6.3 for a discussion of the assumption.) Below, we present a quantum money construction from non-Abelian group actions.

6.1 The Quantum Lightning Construction

Let G be a group with an efficient quantum Fourier transform and a negligible maximum Plancherel measure (that is, each irrep λ of G has dimension at most $d_\lambda := \dim(\varrho_\lambda) \leq \sqrt{|G|} \cdot \mathsf{negl}(\log|G|)$). For example, we can take G to be the dihedral group D_{2^n} or the symmetric group S_n. Let $* : G \times X \to X$ be a semiregular group action of G on some set X, and let $x \in X$ be a fixed starting element in the set. We build a our quantum lightning scheme as follows:

[31] By contrast, [Zha24] is only able to show a security reduction in the black-box setting of generic group actions.

Mint: To mint a quantum bank note, the mint begins with a copy of the starting element of the group $x \in X$ in a quantum register B, in tensor product with the uniform superposition of all elements of the group.[32]

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_{\mathsf{A}} |x\rangle_{\mathsf{B}} \ .$$

The mint then applies the group action, controlled on register A, yielding the following quantum state:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_{\mathsf{A}} |g * x\rangle_{\mathsf{B}} \ .$$

The mint inverts the group element in register A to get:

$$\begin{aligned}\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g^{-1}\rangle_{\mathsf{A}} |g * x\rangle_{\mathsf{B}} &= \frac{1}{\sqrt{|G|}} \sum_{g \in G} \sum_{\substack{\lambda \in \hat{G} \\ i,j \in [d_\lambda]}} \sqrt{\frac{d_\lambda}{|G|}}\, \varrho_\lambda(g^{-1})_{i,j} |\mathcal{L}^\lambda_{j,i}\rangle_{\mathsf{A}} |g * x\rangle_{\mathsf{B}} \\ &= \frac{1}{\sqrt{|G|}} \sum_{\substack{\lambda \in \hat{G} \\ i,j \in [d_\lambda]}} |\mathcal{L}^\lambda_{j,i}\rangle_{\mathsf{A}} \sqrt{\frac{d_\lambda}{|G|}} \sum_{g \in G} \varrho_\lambda(g^{-1})_{i,j} |g * x\rangle_{\mathsf{B}} \ ,\end{aligned}$$

where $|\mathcal{L}^\lambda_{a,b}\rangle := \sqrt{\frac{d_\lambda}{|G|}} \sum_{h \in G} \varrho_\lambda(h^{-1})_{a,b} |h\rangle$ is the Fourier basis state of the left-regular representation.

The mint then applies the quantum Fourier transform on A, yielding the following state:

$$\frac{1}{\sqrt{|G|}} \sum_{\substack{\lambda \in \hat{G} \\ i,j \in [d_\lambda]}} |\lambda, j, i\rangle_{\mathsf{A}} \sqrt{\frac{d_\lambda}{|G|}} \sum_{g \in G} \varrho_\lambda(g^{-1})_{i,j} |g * x\rangle_{\mathsf{B}} \ . \tag{8}$$

The mint then measures A in the computational basis to get an label $\lambda \in \widehat{G}$, as well as two Fourier indices $i, j \in [d_\lambda]$. The residual state on register B becomes:

$$|\$^\lambda_{i,j}\rangle := \sqrt{\frac{d_\lambda}{|G|}} \sum_{g \in G} \varrho_\lambda(g^{-1})_{i,j} |g * x\rangle \ .$$

Output λ as the serial number, and $|\$^\lambda_{i,j}\rangle$ as the quantum money state. This completes the description of Mint.

Lemma 6.1. *The set possible money states $\{|\$^\lambda_{i,j}\rangle\}_{\lambda \in \widehat{G},\, i,j \in [d_\lambda]}$ is orthonormal. That is $\langle \$^\lambda_{i,j} \,|\, \$^\sigma_{k,\ell} \rangle = \delta_{\lambda,\sigma} \delta_{i,k} \delta_{j,\ell}$.*

Proof. This follows straightforwardly from Schur orthogonality relations (Lemma 4.18) and the fact

[32] This can be attained by performing the inverse quantum Fourier transform on the trivial irrep label of the group.

that the group action is semiregular (that is, $g * x = h * x$ only if $g = x$). We have:

$$\begin{aligned}
\langle \$^{\lambda}_{i,j} \,|\, \$^{\sigma}_{k,\ell} \rangle &= \frac{\sqrt{d_\lambda d_\sigma}}{|G|} \sum_{g,h \in G} \varrho_\lambda(g^{-1})^*_{i,j} \varrho_\sigma(h^{-1})_{k,\ell} \, \langle g * x \,|\, h * x \rangle \\
&= \frac{\sqrt{d_\lambda d_\sigma}}{|G|} \sum_{g \in G} \varrho_\lambda(g^{-1})^*_{i,j} \varrho_\sigma(g^{-1})_{k,\ell} \\
&= \frac{\sqrt{d_\lambda d_\sigma}}{|G|} \cdot \frac{|G|}{d_\lambda} \delta_{\varrho,\sigma} \delta_{i,k} \delta_{j,\ell} \\
&= \delta_{\varrho,\sigma} \delta_{i,k} \delta_{j,\ell} \,.
\end{aligned}$$

□

Lemma 6.2. *The serial number—that is, the irrep label λ—produced by the Minting is sampled according to the Plancherel measure of λ in G. That is, for all $\lambda \in \widehat{G}$,*

$$\Pr\left[\lambda = \sigma \;\middle|\; (\sigma, |\$^{\sigma}_{ij}\rangle) \leftarrow \mathsf{Mint}()\right] = \frac{d_\lambda^2}{|G|} \,.$$

Proof. We note that can write Equation (8) as:

$$\frac{1}{\sqrt{|G|}} \sum_{\substack{\lambda \in \widehat{G} \\ i,j \in [d_\lambda]}} |\lambda, j, i\rangle_{\mathsf{A}} \, |\$^{\lambda}_{i,j}\rangle_{\mathsf{B}} \,.$$

where the $|\$^{\lambda}_{i,j}\rangle$'s are orthonormal by Lemma 6.1. We can see directly that the probability of measuring any triplet of (λ, j, i) in register A is exactly $\frac{1}{|G|}$. Furthermore, since for each $\lambda \in \widehat{G}$, i and j both run over $[d_\lambda]$, λ appears in d_λ^2 such triplets. The total probability of the mint outputting serial number λ is therefore $\frac{d_\lambda^2}{|G|}$, which is the Plancherel measure of λ. □

Lemma 6.3. *For each $\lambda \in \widehat{G}$ and each $i \in [d_\lambda]$, the set $\{|\$^{\lambda}_{i,j}\rangle\}_{j \in [d_\lambda]}$ spans a multiplicity subspace, $W^{\lambda}_{i,x}$, of irreducible representation λ in the group action representation $\mathcal{R}(h) = \sum_{g \in G} |hg * x\rangle\langle g * x|$.*

Proof. Applying $\mathcal{R}(h)$ to $|\$^{\lambda}_{i,j}\rangle$ gives us:

$$\begin{aligned}
\mathcal{R}(h) \, |\$^{\lambda}_{i,j}\rangle &= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g \in G} \varrho_\lambda \left(g^{-1}\right)_{i,j} |hg * x\rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g' = hg \in G} \varrho_\lambda \left((g')^{-1} h\right)_{i,j} |g' * x\rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g \in G} \left(\varrho_\lambda \left(g^{-1}\right) \varrho_\lambda \left(h\right)\right)_{i,j} |g * x\rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g \in G} \sum_{k \in [d_\lambda]} \varrho_\lambda \left(g^{-1}\right)_{i,k} \varrho_\lambda \left(h\right)_{k,j} |g * x\rangle \\
&= \sum_{k \in [d_\lambda]} \varrho_\lambda(h)_{k,j} \sum_{g \in G} \varrho_\lambda(g^{-1})_{i,k} \, |g * x\rangle \\
&= \sum_{k \in [d_\lambda]} \varrho_\lambda(h)_{k,j} \, |\$^{\lambda}_{i,k}\rangle \,.
\end{aligned}$$

We can see that $\mathcal{R}(h)$ acts exactly as the irreducible representation ϱ_λ on the space spanned by the money states $\{|\$^\lambda_{i,j}\rangle\}_{j\in[d_\lambda]}$. They must therefore span the same multiplicity subspace $W^\lambda_{i,x}$ of irreducible representation ϱ_λ in $\mathcal{R}(h)$. □

Corollary 6.4. *For all $\lambda \in \widehat{G}$ and $i,j \in [d_\lambda]$, the money state $|\$^\lambda_{i,j}\rangle$ is in the subspace $W^\lambda_x = \bigoplus_{i\in[d_\lambda]} W^\lambda_{i,x}$ corresponding to irreducible representation ϱ_λ of the group action representation starting from x. Moreover, if the group action has multiple orbits, then the full isotypic component of λ is $W^\lambda = \bigoplus_{y\in\mathsf{Orb}(\mathcal{R})} W^\lambda_y$ where y runs over the set of orbits of the group action, choosing an element from each orbit arbitrarily.*

Ver: To verify, we begin by measuring that the state has support only on the set X. We then repeat essentially the same process as for minting, but starting with the claimed banknote in the second register, rather than $|x\rangle$. Suppose we want to verify a state $|¥^\lambda\rangle$ with claimed serial number λ, we prepare the uniform superposition over group elements, perform the group action on $|¥^\lambda\rangle$ in superposition, and then measure the control register in the Fourier basis. That is, we perform a course Fourier measurement on $|¥^\lambda\rangle$ and check if it has the claimed label.

Suppose that $|¥^\lambda\rangle$ is a valid state for label λ. That is $|¥^\lambda\rangle = \sum_{i,j\in[d_\lambda]} \alpha_{i,j} |\$^\lambda_{i,j}\rangle$ for some coefficients $\alpha_{i,j}$. This gives the following:

$$\begin{aligned}
\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle\,|¥^\lambda\rangle &= \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle \sum_{i,j\in[d_\lambda]}\alpha_{i,j}\,|\$^\lambda_{i,j}\rangle \\
&\xrightarrow[\text{action}]{\text{group}} \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle \sum_{i,j,k\in[d_\lambda]}\alpha_{i,j}\;\varrho_\lambda(g)_{k,j}\,|\$^\lambda_{i,k}\rangle \\
&= \sum_{i,j,k\in[d_\lambda]}\alpha_{i,j}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\varrho_\lambda(g)_{k,j}\,|g\rangle\,|\$^\lambda_{i,k}\rangle \\
&\xrightarrow[g]{\text{invert}} \sum_{i,j,k\in[d_\lambda]}\alpha_{i,j}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\varrho_\lambda(g)_{k,j}\,|g^{-1}\rangle\,|\$^\lambda_{i,k}\rangle \\
&= \sum_{i,j,k\in[d_\lambda]}\alpha_{i,j}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\varrho_\lambda(g^{-1})_{k,j}\,|g\rangle\,|\$^\lambda_{i,k}\rangle \\
&= \sum_{i,j,k\in[d_\lambda]}\frac{\alpha_{i,j}}{\sqrt{d_\lambda}}\,|\mathcal{L}^\lambda_{k,j}\rangle\,|\$^\lambda_{i,k}\rangle
\end{aligned}$$

Now if we perform a course (left-regular) Fourier basis measurement on the first register (perform a Fourier transform and measure the irrep label) we get the correct serial number λ. Now we have two options: we can further perform a fine Fourier basis measurement to get k and j, collapsing the quantum money state to a new state $|\$'^\lambda\rangle = \sum_{i\in[d_\lambda]}\alpha'_{i,k}\,|\$^\lambda_{ik}\rangle$ with different weights on the same set $\{|\$^\lambda_{a,b}\rangle\}_{a,b\in[d_\lambda]}$ of basis states, but nevertheless still a valid quantum money state. Or, alternatively, we can refrain from measuring k and j and simply un-compute the whole process, which, in the case that verification passed with certainty, recovers the original state $|¥^\lambda\rangle$.

Remark 6.5. *Note that states of the form $\sum_{i,j\in[d_\lambda]}\alpha_{i,j}\,|\$^\lambda_{i,j}\rangle$ are not the only states that pass verification. If we denote $|\$^\lambda_{i,j} * x\rangle := \sqrt{\frac{d_\lambda}{|G|}}\sum_{g\in G}\varrho_\lambda\left(g^{-1}\right)_{i,j}|g*x\rangle$ as the quantum money state produced by beginning with starting set element $x\in X$, then states of the form $|\$^\lambda_{i,j} * y\rangle$ for all $y\in X$ and $i,j\in[d_\lambda]$ (and their superpositions) also pass verification. Thus they are also valid*

quantum money states, despite not being the result of the minting process, and must be considered in the security arguments.

6.2 Variations on the Construction

Here, we describe some possible variations of the above scheme.

Membership check. The set X may be a collection of sparse strings. In this case, a quantum money adversary may try to forge with fake banknotes that have support outside of X. If the group action supports membership testing for X, it is natural to also have the verifier check that a supposed banknote has support on X. Such a check is used in [Zha24] to analyze the security of their construction. For may group actions, however, such a membership check is not efficiently feasible. In the case in which the group still acts compatibly (or approximately so) on elements outside of X which cannot be distinguished from X, then this can be treated as the group action having additional orbits. In Section 6.3.3, we show an example of how to handle such a group action.

Irrep check. It may be useful to insist that the serial number of the banknote corresponds to an irrep with certain properties. Notably, we will consider adding checks on the *dimension* of the irrep, assuming the dimension is efficiently computable. For example, we may insist that banknotes come from irreps of dimension at least 2.

For such irrep checks, in order to ensure correctness, we need to ensure that the mint always produces irreps with the given property. If such irreps are at least inverse-polynomially dense according to the Plancherel measure, we can have the mint keep minting banknotes until it produces one with the given property.

The following lemma shows that the irreps of size at least 2 are dense for all non-Abelian groups. Thus, for any non-Abelian group action, we can insist on valid banknotes having irrep dimension at least 2. We will make this assumption in the security analysis of our scheme in the following subsections.

Lemma 6.6. *For any non-Abelian G, let d be the dimension of a random irrep sampled according to the Plancherel measure. Then* $\Pr[d \geq 2] \geq 1/2$.

Proof. The 1-dimensional irreps are in bijection with the quotient of the commutator subgroup $G/[G,G]$. Since $|[G,G]| \geq 2$ for non-Abelian groups, $|G/[G,G]| \leq |G|/2$. The probability of sampling any given 1-dimensional irrep according to the Plancherel measure is $1/|G|$. Over all $\leq |G|/2$ such irreps, the probability of sampling *any* 1-dimensional irrep is at most $1/2$. This means the probability sampling an irrep of dimension 2 or higher is at least $1/2$. □

6.3 Security from Preaction Secure Group Actions

In this subsection we give a security proof from cryptographic group actions that are preaction-secure, which we define here. A *preaction* on a group action is an operation that on input $x, g*x \in X$ computes $h \circ (g * x) := gh^{-1} * x$ for some $h \in G$.[33] That is, it prepends a group element h^{-1} on the right of g, as if h^{-1} had acted *before* g had acted. While for Abelian group actions, this is equivalent to the group action itself (up to inverting h), for non-Abelian groups, this is not generically efficient. Note, however that a preaction *is* itself a group action, as it satisfies

[33] We assume here, as before, that the action is semiregular, so that this is well-defined.

compatibility—that is, $h_1 \circ (h_2 \circ (g * x)) = (h_1 h_2) \circ (g * x)$. And moreover, the preaction of a preaction is the original group action.

We introduce both a search-type assumption and a decision-type assumption, that constitute different levels of preaction security. The search-type assumption, preaction hardness, requires that it is computationally hard to perform a preaction. The decision-type assumption, preaction indistinguishability, requires that it is hard to tell when a preaction has been performed. In both cases, the preactions are defined relative to a predetermined and fixed starting element $x \in X$.

Assumption 1 (ϵ-Preaction Hardness)**.** *Given $g * x$, and h for random $g, h \leftarrow G$, it is hard to output $gh^{-1} * x$. That is, for all QPT adversaries, $\mathcal{A}$,*[34]

$$\Pr\left[z = gh^{-1} * x \ : \ x \leftarrow X,\ g, h \leftarrow G,\ z \leftarrow \mathcal{A}(x, g * x, h)\right] \leq \frac{1}{|G|} + \epsilon\,.$$

Algorithm 4 (**Preaction Indistinguishability Security Game**)**.**

1. Challenger samples $b \in \{0, 1\}$ and two uniformly random group elements $h_1, h_2 \leftarrow G$.
2. Adversary sends a register A to the challenger.
3. If $b = 0$, the challenger applies the action of h_1 to A. Otherwise, the challenger applies both the action of h_1 and the preaction of h_2 to A. Send A back to the adversary.
4. Adversary outputs b' and wins if $b' = b$.

Assumption 2 (ϵ-Preaction Indistinguishability)**.** *It is hard to distinguish whether a preaction has been performed. Formally, no adversary can win at the preaction indistinguishability security game (Algorithm 4) with advantage greater than ϵ. That is, if we write the action of the challenger in Step 3 as $\mathsf{F}_b^{h_1,h_2} \ : \ g * x \ \mapsto \ h_1\, g\, h_2^{-b} * x$. Then for all QPT adversaries, $\mathcal{A}$, that make a single query*[35] *to F,*

$$\left|\Pr\left[0 \leftarrow \mathcal{A}^{\mathsf{F}_0^{h_1,h_2}} \ : \ h_1, h_2 \leftarrow G\right] - \Pr\left[0 \leftarrow \mathcal{A}^{\mathsf{F}_1^{h_1,h_2}} \ : \ h_1, h_2 \leftarrow G\right]\right| \leq \epsilon$$

Note that when $b = 0$, $\mathsf{F}_b^{h_1,h_2}$ performs a group action for a random group element h_1, and when $b = 1$, it performs both a random bi-action*—that is, a random group action with h_1 and a random group pre-action with h_2.*

Definition 6.7. *We say that a group action of group G_λ on set X_λ with starting element x is* ϵ-preaction secure *if both Assumption 1 and Assumption 2 hold for the group action against any QPT adversary with advantage ϵ. We say that the group action is preaction secure if it is* $\mathsf{negl}(\lambda)$*-preaction secure for any negligible function* negl*.*

[34] Note that an adversary can always trivially perform a preaction with probability $\frac{1}{|G|}$ by performing an action with a random group element. This is because the orbits of the action and preaction are always the same. We thus define the advantage as the best that can be done beyond this trivial attack. Groups that are not too far from being Abelian may have a different specialized trivial attack, so it may be convenient to assume the difficulty beyond that, but for simplicity, we do not get into that here.

[35] We could in general define multi-round security game for preaction indistinguishability, in which Steps 2 and 3 are repeated. Preaction security defined this way would be a stronger assumption, and may be useful for other settings. However, we do not formally define the stronger version as we are able to prove security from this weaker assumption, which gives a stronger security guarantee, and is more likely to hold for a larger class of group actions.

Remark 6.8. *Classically, distinguishing preactions in one round is* information-theoretically impossible*. This is because both cases—with or without a preaction—send the element to a uniformly random element in its orbit. Interestingly, as we will see, this is* not *the case for quantum distinguishers, since they are allowed to query* $\mathsf{F}_b^{h_1,h_2}$ *on superpositions of elements.*

Remark 6.9. *For* Abelian *group actions, breaking preaction hardness is trivial, since the preaction is equal to the action. On the other hand, for this same reason, preaction indistinguishability is* information-theoretically impossible*: since the preaction is equal to the action, both cases—with or without a preaction—end up performing a uniformly random group action.*

Because of Remark 6.9, preaction security is a security notion that only makes sense for non-Abelian group actions. Moreover, the security proof for our quantum money scheme makes explicit use of the properties of representations of non-Abelian groups to prove the reduction.

In fact, for quantum adversaries and non-Abelian group actions, preaction indistinguishability is a stronger assumption than preaction hardness:

Theorem 6.10. *Let* $(G, X, *, x)$ *be a semiregular single-orbit group action of a non-Abelian group* G *acting on set* X*. Then if the group action satisfies preaction indistinguishability with advantage* ϵ*, then it also satisfies preaction hardness with advantage* $\theta\left(\sqrt{\epsilon + 2\,\mathbb{E}_{\lambda\in\widehat{G}}\left[\frac{1}{d_\lambda}\right]}\right)$.

Proof sketch. We defer the proof of Theorem 6.10 to Section 6.3.2 because it makes use of the quantum money construction of Section 6.3.1. The main idea is that preactions are themselves a representation of the group, with the Fourier indices exchanging roles relative to their roles for the group action. Thus for semiregular single-orbit group actions, the ability to perform preactions allows us to measure in which multiplicity subspace of the irrep a state lies via the duality theorem (Theorem 5.8), with some advantage. We can then distinguish if a preaction has occurred by testing if it has moved us to a different multiplicity subspace of the irrep. □

Therefore, when working with non-Abelian group actions that are semiregular and single-orbit, it suffices for preaction security to consider only the decision-type assumption of the indistinguishability of preactions.

6.3.1 Construction.

Let (G, X, x) be a semiregular single-orbit group action satisfying the requirements of Section 6.1. The quantum money/lightning construction follows the framework of Section 6.1. We show below that if the group action is preaction secure, then the quantum money construction satisfies lightning security.

6.3.2 Security

Let $|\$^\lambda_{i,j}\rangle \propto \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j}\,|g * x\rangle$ be the quantum money states minted by the scheme. We show a tight connection between the ability to perform preaction (i.e. breaking preaction hardness, Assumption 1) and performing a "right representation" on the quantum money state, that is, coherently mapping the quantum money state as $|\$^\lambda_{i,j}\rangle \mapsto \sum_{k\in[d_\lambda]} \varrho(h^{-1})_{i,k}\,|\$^\lambda_{k,j}\rangle$ on input $h \leftarrow G$. This right representation treats the span of the same vector across the different multiplicity subspaces of λ as a single invariant subspace. In other words, it is to the standard group action representation what the right-regular representation is to the left-regular representation. We say that an adversary can perform the right representation with advantage ϵ if it can perform a unitary with Hilbert-Schmidt inner product at least $\frac{1}{|G|} + \epsilon$ with the ideal right representation.

Lemma 6.11. *Any adversary that performs a preaction $x, g*x, h \mapsto gh^{-1}*x$ with advantage ϵ for a fixed starting element, $x \in X$, and random $g, h \leftarrow G$, can be used to perform a right representation, $|\$^\lambda_{i,j}\rangle \mapsto \sum_{k\in[d_\lambda]} \varrho_\lambda(h^{-1})_{i,k} |\$^\lambda_{k,j}\rangle$ with the same advantage ϵ. Similarly any adversary that performs a right representation with advantage ϵ. can be used to perform a preaction with the same advantage ϵ.*

Proof. Consider an adversary that performs preactions with advantage ϵ, and consider what happens in the ideal case, in which the preaction is performed exactly. We start with the money state

$$|\$^\lambda_{i,j}\rangle \propto \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j} |g * x\rangle \ .$$

We perform a preaction with h to get

$$\begin{aligned}
&\to \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j} |gh^{-1} * x\rangle \\
&= \sum_{g\in G} \varrho_\lambda(h^{-1}g^{-1})_{i,j} |g * x\rangle \\
&= \sum_{\substack{g\in G \\ k\in[d_\lambda]}} \varrho_\lambda(h^{-1})_{i,k}\varrho_\lambda(g^{-1})_{k,j} |g * x\rangle \\
&= \sum_{k\in[d_\lambda]} \varrho_\lambda(h^{-1})_{i,k} \sum_{g\in G} \varrho_\lambda(g^{-1})_{k,j} |g * x\rangle \\
&\propto \sum_{k\in[d_\lambda]} \varrho_\lambda(h^{-1})_{i,k} |\$^\lambda_{i,j}\rangle \ .
\end{aligned}$$

Let $U = \sum_{h,\lambda,i,k,j} |h\rangle\langle h| \otimes \varrho_\lambda(h^{-1})_{i,k} |\$^\lambda_{k,j}\rangle\langle\$^\lambda_{i,j}|$ be the unitary that performs the right representation controlled on a group element h. We can therefore rewrite it as $U = \sum_{h,g} |h\rangle\langle h| \otimes |gh^{-1} * x\rangle\langle g * x|$.

Now suppose that the adversary performs preactions with advantage ϵ. That is, it performs some $\widetilde{U} = \sum_{h,g} |h\rangle\langle h| \otimes |\psi(h, g * x)\rangle\langle g * x|$ where the probability of success is $\frac{1}{|G|^2} \sum_{h,g} \langle gh^{-1} * x \,|\, \psi(h, g * x)\rangle = \frac{1}{|G|} + \epsilon$. Then we have that, by the definition of the Hilbert-Schmidt inner product,

$$\left\langle U, \widetilde{U} \right\rangle = \frac{1}{|G|^2} \sum_{h,g} \langle gh^{-1} * x \,|\, \psi(h, g * x)\rangle = \frac{1}{|G|} + \epsilon \,.$$

Conversely, consider an adversary that performs the right representation with advantage ϵ. That is, it performs some operator $\widetilde{U}$ such that $\left\langle U, \widetilde{U} \right\rangle = \frac{1}{|G|} + \epsilon$, where $U = \sum_{h,\lambda,i,k,j} |h\rangle\langle h| \otimes \varrho_\lambda(h^{-1})_{i,k} |\$^\lambda_{k,j}\rangle\langle\$^\lambda_{i,j}|$ is the ideal unitary that performs the right representation.

Consider what happens when the ideal unitary is run on $|g * x\rangle$. We start by writing $|g * x\rangle$ in the basis of the quantum money states $\{|\$^\lambda_{i,j}\rangle\}_{\lambda\in\widehat{G},\, i,j\in[d_\lambda]}$:

$$|g * x\rangle \propto \sum_{\substack{\lambda\in\widehat{G} \\ i,j\in[d_\lambda]}} \varrho_\lambda(g)_{j,i} |\$^\lambda_{i,j}\rangle \ .$$

Now we perform the right representation to get

$$\begin{aligned}
&\to \sum_{\substack{\lambda\in\widehat{G}\\ i,j\in[d_\lambda]}} \varrho_\lambda(g)_{j,i} \sum_{i'\in[d_\lambda]} \varrho_\lambda(h^{-1})_{i,i'} \left|\$^\lambda_{i',j}\right\rangle \\
&= \sum_{\substack{\lambda\in\widehat{G}\\ i,i',j\in[d_\lambda]}} \varrho_\lambda(g)_{j,i}\varrho_\lambda(h^{-1})_{i,i'} \left|\$^\lambda_{i',j}\right\rangle \\
&= \sum_{\substack{\lambda\in\widehat{G}\\ i',j\in[d_\lambda]}} \varrho_\lambda(gh^{-1})_{j,i'} \left|\$^\lambda_{i',j}\right\rangle \\
&\propto |gh^{-1} * x\rangle \ .
\end{aligned}$$

If instead we run $\widetilde{U}$ on $|g * x\rangle$, and measure in the computational basis, we get the correct preaction with probability

$$\begin{aligned}
\frac{1}{|G|^2}\sum_{h,g\in G} \langle h| \otimes \langle gh^{-1} * x| \widetilde{U} |h\rangle \otimes |g * x\rangle &= \frac{1}{|G|^2}\sum_{h,g\in G} \langle h| \otimes \langle g * x| U^\dagger \widetilde{U} |h\rangle \otimes |g * x\rangle \\
&= \left\langle \widetilde{U}, U \right\rangle = \frac{1}{|G|} + \epsilon \,.
\end{aligned}$$

□

Therefore, pre-action hardness of the group action (Assumption 1) is equivalent to the hardness of performing the right representation on the money states to map one multiplicity subspace of an irrep to another multiplicity subspace of the same irrep.

Corollary 6.12. *For a group action to be δ-preaction secure, at most a fraction $\frac{1}{|G|} + \delta$ of the Plancherel measure of G can be on irreps of dimension 1.*

Proof. Consider an adversary that simply implements the left-regular representation of the group (that is, the original group action). Let Π_{triv} be the projector onto the irreducible representation spaces corresponding to 1-dimensional representations, and note that both the left- and right-regular representations commute with Π_{triv}. Then we have that for every pair of group elements g and h,

$$\begin{aligned}
\left|\langle gh^{-1} * x | hg * x\rangle\right|^2 &= \left|\langle gh^{-1} * x | \Pi_{\text{triv}} | hg * x\rangle\right|^2 + \left|\langle gh^{-1} * x | (\mathrm{id} - \Pi_{\text{triv}}) | hg * x\rangle\right|^2 \\
&\geq \left|\langle gh^{-1} * x | \Pi_{\text{triv}} | hg * x\rangle\right|^2 \\
&= \| \Pi_{\text{triv}} |g * x\rangle \|^2 \,.
\end{aligned}$$

Here, we first use the fact that the left- and right- regular representations are block diagonal in the decomposition into Π_{triv} and $\mathrm{id} - \Pi_{\text{triv}}$. Then we use the fact that on Π_{triv}, the left- and right-regular representations are equal, and thus they cancel each other out in the inner product. Noting that $\| \Pi_{\text{triv}} |g * x\rangle \|^2$ is equal to the Plancherel measure of G on irreps of dimension 1, we have that the adversary that applies the left-regular representation and measures in the computational basis has probability at least the Plancherel measure of G on irreps of dimension 1 of measuring the element $|gh^{-1} * x\rangle$, and thus breaks preaction security unless it is less than $\frac{1}{|G|} + \delta$. □

Remark 6.13. *By Corollary 6.12, we see that for any preaction-secure group action, the event of sampling a multi-dimensional irrep from the Plancherel measure happens with overwhelming probability, strengthening Lemma 6.6, which states that it happens with probability at least $\frac{1}{2}$ for*

general non-Abelian group actions. We can therefore always assume that the quantum money state sampled by the minting algorithm lies in a multi-dimensional irrep. We will assume therefore for the rest of the section that the quantum money verification rejects such 1-dimensional irreps.

Corollary 6.14. *An adversary for preaction hardness with advantage ϵ can be used to perform a **right**-Fourier measurement on the quantum money state with that outputs the correct index i of the multiplicity subspace of ϱ with advantage at least $4\epsilon^2 - \mathbb{E}_\lambda\left[\frac{1}{d_\lambda}\right]$.*[36] *That is, it can be used to measure i for quantum money state $|\$^\lambda_{i,j}\rangle \propto \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j}\,|g * x\rangle$.*

Proof. Intuitively, if we can break pre-action hardness, from Lemma 6.11, we can implement an approximate representation of the group where the Fourier indices i and j exchange roles, and from Theorem 5.8 we can then implement a measurement that correctly outputs the index i of the money state with high probability. To prove this formally, let $\mathcal{M}$ be the approximate measurement implied by Theorem 5.8, with V being the identity (since we know there exists an exact representation in the space, given by performing the exact preaction), we first note that by the definition of breaking preaction hardness with advantage ϵ, and applying Lemma 6.11, together with the fact that $\mathbb{E}_g \left\|\mathcal{R}(g) - \mathcal{S}(g)\right\|^2 = 1 - 2\,\mathbb{E}_g \left\langle \mathcal{R}(g), \mathcal{S}(g)\right\rangle = 1 - 2(\epsilon + \frac{1}{|G|})$ from before (where $\mathcal{S}$ is the exact irrep, used to form U), we get the following lower bound

$$\begin{aligned} 2\left(\epsilon + \frac{1}{|G|}\right) &\leq \frac{1}{|G|} \sum_{\substack{\lambda\in\widehat{G},\, i\in[n_\lambda]\\ j\in[d_\lambda]}} \mathrm{Re}\,\langle\phi^\lambda_i| \otimes \langle\lambda, j|\,\mathcal{M}\,|\psi^\lambda_{i,j}\rangle \\ &\leq \frac{1}{|G|} \sum_{\substack{\lambda\in\widehat{G},\, i\in[n_\lambda]\\ j\in[d_\lambda]}} \left|\langle\phi^\lambda_i| \otimes \langle\lambda, j|\,\mathcal{M}\,|\psi^\lambda_{i,j}\rangle\right| . \end{aligned}$$

Note that this function is the expectation of $|\,\langle\phi^\lambda_i| \otimes \langle\lambda, j|\,V\mathcal{M}^2V^\dagger\,|\psi^\lambda_{i,j}\rangle\,|$, so we can apply Jensen's inequality with the function $f(x) = x^2$ to get the following lower bound

$$\begin{aligned} 4\left(\epsilon + \frac{1}{|G|}\right)^2 &= \left(\frac{1}{|G|} \sum_{\substack{\lambda\in\widehat{G},\, i\in[n_\lambda]\\ j\in[d_\lambda]}} \left|\langle\phi^\lambda_i| \otimes \langle\lambda, j|\,\mathcal{M}\,|\psi^\lambda_{i,j}\rangle\right|\right)^2 \\ &\leq \frac{1}{|G|} \sum_{\substack{\lambda\in\widehat{G},\, i\in[n_\lambda]\\ j\in[d_\lambda]}} \left|\langle\phi^\lambda_i| \otimes \langle\lambda, j|\,\mathcal{M}\,|\psi^\lambda_{i,j}\rangle\right|^2 . \end{aligned}$$

Since this quantity is the average probability of measuring the correct outcome given a uniformly random ϱ, i and j, the advantage is at least $4\epsilon^2 - \mathbb{E}_\lambda\left[\frac{1}{d_\lambda}\right]$, as desired. □

We now show the following lemma which completes the proof of Theorem 6.10, showing that preaction indistinguishability implies preaction hardness for non-Abelian group actions.

Lemma 6.15. *An adversary that can perform a **right**-Fourier measurement on the quantum money state with advantage $4\epsilon^2 - \mathbb{E}_\lambda\left[\frac{1}{d_\lambda}\right]$ can be used to break preaction indistinguishability (Assumption 2) with advantage $2\left(2\epsilon^2 - \mathbb{E}_{\lambda\in\widehat{G}}\left[\frac{1}{d_\lambda}\right]\right)$.*

[36] where the measurement advantage here is defined as $|\Pr_{\varrho,i,j}[i \leftarrow \mathcal{A}(|\$^\varrho_{i,j}\rangle)] - \mathbb{E}_k \Pr_{\varrho,i,j}[i \leftarrow \mathcal{A}(|\$^\varrho_{k,j}\rangle)]\,|$

Proof. Assume at first that we have a perfect such adversary for performing right-Fourier measurements. We start by running the minting algorithm to produce a uniformly random quantum money state $|\$^\lambda_{i,j}\rangle := \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho(g^{-1})_{ij} |g * x\rangle$, along with its classical descriptors, the irreducible representation $\lambda \in \widehat{G}$ sampled according to the Plancherel measure (Lemma 6.2) and uniformly random $i, j \in [d_\lambda]$.[37]

We then apply the challenger given by Assumption 2 to get

$$\begin{aligned}
&\to \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j} |h_1 g h_2^{-b} * x\rangle \\
&= \sum_{g\in G} \varrho_\lambda\left(h_2^{-b} g^{-1} h_1\right)_{i,j} |g * x\rangle \\
&= \sum_{\substack{g\in G \\ k,\ell\in[d_\lambda]}} \varrho_\lambda\left(h_2^{-b}\right)_{i,k} \varrho_\lambda\left(g^{-1}\right)_{k,\ell} \varrho_\lambda\left(h_1\right)_{\ell,j} |g * x\rangle \\
&= \sum_{k,\ell\in[d_\lambda]} \varrho_\lambda\left(h_2^{-b}\right)_{i,k} \varrho_\lambda\left(h_1\right)_{\ell,j} \sum_{g\in G} \varrho_\lambda\left(g^{-1}\right)_{k,\ell} |g * x\rangle \\
&= \sum_{k,\ell\in[d_\lambda]} \varrho_\lambda\left(h_2^{-b}\right)_{i,k} \varrho_\lambda\left(h_1\right)_{\ell,j} |\$^\lambda_{k,\ell}\rangle
\end{aligned} \tag{9}$$

Suppose that $b = 1$. Then when averaged over all pairs of group elements, h_1 and h_2, this gives

$$\begin{aligned}
&\frac{1}{|G|^2} \sum_{h_1,h_2\in G} \sum_{k,k',\ell,\ell'\in[d_\lambda]} \varrho_\lambda\left(h_2\right)^*_{i,k} \varrho_\lambda\left(h_1\right)^*_{\ell,j} \varrho_\lambda\left(h_2\right)_{i,k'} \varrho_\lambda\left(h_1\right)_{\ell',j} |\$^\lambda_{k,\ell}\rangle\langle\$^\lambda_{k',\ell'}| \\
&= \frac{1}{|G|^2} \sum_{k,k',\ell,\ell'\in[d_\lambda]} \sum_{h_1\in G} \varrho_\lambda\left(h_1\right)^*_{\ell,j} \varrho_\lambda\left(h_1\right)_{\ell',j} \sum_{h_2\in G} \varrho_\lambda\left(h_2\right)^*_{i,k} \varrho_\lambda\left(h_2\right)_{i,k'} |\$^\lambda_{k,\ell}\rangle\langle\$^\lambda_{k',\ell'}| \\
&= \frac{1}{d_\lambda^2} \sum_{k,k',\ell,\ell'\in[d_\lambda]} \delta_{\ell,\ell'}\delta_{k,k'} |\$^\lambda_{k,\ell}\rangle\langle\$^\lambda_{k',\ell'}| \\
&= \frac{1}{d_\lambda^2} \sum_{k,\ell,\in[d_\lambda]} |\$^\lambda_{k,\ell}\rangle\langle\$^\lambda_{k,\ell}| \ ,
\end{aligned}$$

where the second equality follows from the Schur orthogonality relations (Lemma 4.18). This is the fully mixed state over the isotypic component of λ—that is, over the union of all of the multiplicity subspaces of irrep λ.

Now with probability $1 - \frac{1}{d_\lambda} \geq \frac{1}{2}$ (since $d_\lambda \geq 2$), we get that $k \neq i$. That is, with probability at least $\frac{1}{2}$, the quantum money state has moved to a different multiplicity subspace of the irrep λ, and measuring it again will confirm this.

If instead $b = 0$, then $k = i$ with certainty (as $\varrho_\lambda((h_2^0))_{i,k} = \varrho_\lambda(\mathrm{id})_{i,k} = \delta_{i,k} \quad \forall \lambda \in \widehat{G}, h_2 \in G$), so we instead get a fully mixed state over the i^{th}multiplicity subspace of λ. So we output $b' = 1$ if $k \neq i$ and 0 otherwise. This gives a distinguishing advantage of at least $\frac{1}{2}$, breaking Assumption 2.

[37] Note that the minting algorithm of the quantum lightning scheme as described in Section 6.1 does not output i and j, since they are not useful for verification (and in fact i is not even verifiable). But they do pop up as part of the minting process, so we can modify the minting algorithm to output them as well. In fact, it is an odd quirk of our quantum lightning scheme that the minting party knows a piece of secret information about the money state—the multiplicity subspace, i, of irrep λ that the money state actually lies in—but that this information is completely useless. Neither the minting party nor anyone else can ever even verify this information! That is, unless they can break preaction hardness, which is what we assume here in this proof.

Now suppose that the right-Fourier measurement adversary, $\mathcal{M}$, has advantage ϵ of measuring the correct multiplicity subspace, over a uniformly random λ, i and j. As shown above, in the case where there is no preaction, then it will never change the multiplicity subspace, while in the case where there is a preaction, it will change to a uniformly random multiplicity subspace.

We therefore have that the distinguishing advantage is

$$\begin{aligned}
&\left|\Pr\left[0 \leftarrow \mathcal{A}^{\mathsf{F}_0^{h_1,h_2}} \ : \ h_1,h_2 \leftarrow G\right] - \Pr\left[0 \leftarrow \mathcal{A}^{\mathsf{F}_1^{h_1,h_2}} \ : \ h_1,h_2 \leftarrow G\right]\right| \\
&= \left| \mathop{\mathbb{E}}_{\substack{\lambda\in\widehat{G} \\ i,j\in[d_\lambda]}} \left|\mathrm{id}\otimes\langle i|\,\mathcal{M}\,|\$_{i,j}^\lambda\rangle\right|^2 - \mathop{\mathbb{E}}_{\substack{\lambda\in\widehat{G} \\ i,j,i',j'\in[d_\lambda]}} \left|\mathrm{id}\otimes\langle i|\,\mathcal{M}\,|\$_{i',j'}^\lambda\rangle\right|^2 \right| \\
&= \left| \mathop{\mathbb{E}}_{\substack{\lambda\in\widehat{G} \\ i,j\in[d_\lambda]}} \left|\mathrm{id}\otimes\langle i|\,\mathcal{M}\,|\$_{i,j}^\lambda\rangle\right|^2 - \mathop{\mathbb{E}}_{\lambda\in\widehat{G}} \frac{1}{d_\lambda} \right| \\
&\geq 4\epsilon^2 - 2 \mathop{\mathbb{E}}_{\lambda\in\widehat{G}} \left[\frac{1}{d_\lambda}\right] \\
&= 2\left(2\epsilon^2 - \mathop{\mathbb{E}}_{\lambda\in\widehat{G}} \left[\frac{1}{d_\lambda}\right]\right) .
\end{aligned}$$

□

We can now complete the proof of Theorem 6.10 by combining Lemmas 6.11 and 6.15 and Corollary 6.14. □

We now turn to the quantum lightning security of the scheme. We argue that any adversary who has two copies of the quantum money state can use them to break preaction indistinguishability (Assumption 2). We therefore get a secure quantum lightning scheme from any group action that satisfies the syntactic requirements and is preaction-secure.

Focusing on the archetype states. For the analysis, before we proceed, it will be useful to consider a proxy for the quantum money states. The money states lie in a potentially large subspace, which is harder to analyze, so it is useful to instead focus on the archetype state that appears after performing a Fourier extraction, which is a unique state that characterizes each such subspace.

Suppose we have a quantum money state $|\$_{i,j}^\lambda\rangle$. We perform a Fourier extraction using Theorem 5.1, and get

$$|\$_{i,j}^\lambda\rangle \xrightarrow{FSE} |\phi_i^\lambda\rangle\,|\lambda\rangle\,|j\rangle = \left(\frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |\$_{i,k}^\lambda\rangle \otimes |k\rangle\right)|\lambda\rangle\,|j\rangle$$

Observation 6.16. *We observe that the archetype state $|\phi_i^\lambda\rangle$ in the first register is unaffected by applying the group action:*

$$|\$_{ij}^\lambda\rangle \xrightarrow{\text{action by } h} \sum_{\ell\in[d_\lambda]} \varrho_\lambda(h)_{\ell,j}\,|\$_{i,\ell}^\lambda\rangle \xrightarrow{FSE} |\phi_i^\lambda\rangle\,|\lambda\rangle \left(\sum_{\ell\in[d_\lambda]} \varrho_\lambda(h)_{\ell,j}\,|\ell\rangle\right)$$

On the other hand, applying the corresponding preaction *performs the (inverted) irreducible representation ϱ_λ onto the set of archetype states $\{|\phi_i^\lambda\rangle\}_{i\in[d_\lambda]}$ for the different multiplicity subspaces*

of ϱ_λ*:*

$$|\$^\lambda_{i,j}\rangle \xrightarrow{\textit{preaction by } h} \sum_{\ell\in[d_\lambda]} \varrho_\lambda(h^{-1})_{i,\ell}\,|\$^\lambda_{\ell,j}\rangle \xrightarrow{FSE} \left(\sum_{\ell\in[d_\lambda]} \varrho_\lambda(h^{-1})_{i,\ell}\,|\phi^\lambda_\ell\rangle\right)|\lambda\rangle\,|j\rangle$$

Proposition 6.17. *Suppose that the group action used in the quantum money construction (Section 6.3.1) is* ϵ*-preaction secure. Then no QPT adversary can produce a quantum state on two registers such that the probability of measuring both registers in the same irreducible representation subspace of* ϱ_λ *is greater than* $2d_\lambda\epsilon/(1+d_\lambda)$*.*

Proof. Assume for the sake of contradiction that an adversary for quantum lightning, $\mathcal{A}$, can prepare a quantum state on two registers, both of which pass verification. By definition, the verifier projects onto W^λ. Since we have shown that $|\$^\lambda_{i,j}\rangle$ is a basis for W^λ, the states produced by $\mathcal{A}$ must be supported on states of the form

$$|\$^\lambda_{i,j}\rangle \otimes |\$^\lambda_{k,\ell}\rangle \qquad \text{where } |\$^\lambda_{i,j}\rangle = \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j}\,|g*x\rangle$$

for some $\lambda \in \widehat{G}$ such that $1 < d_\lambda$. We show that this adversary can be used to break Assumption 2. Let Chal_b be the challenger given in the assumption, which either applies a random action and random pre-action ($b=1$), or just applies a random action ($b=0$).

To demonstrate the idea, we first assume that $i=k$, that is, that the two registers initially lie in the same Fourier subspace of λ. We will see later how to handle the more general case. Suppose that we take only one of the two registers and apply Chal_b. We get (see Equation (9))

$$\sum_{r,s\in[d_\lambda]} \varrho_\lambda\left(h_2^{-b}\right)_{i,r} \varrho_\lambda\left(h_1\right)_{s,j} |\$^\lambda_{r,s}\rangle = \begin{cases} \sum_{s\in[d_\lambda]} \varrho_\lambda\left(h_1\right)_{s,j} |\$^\lambda_{i,s}\rangle & b=0 \\ \sum_{r,s\in[d_\lambda]} \varrho_\lambda\left(h_2^{-1}\right)_{i,r} \varrho_\lambda\left(h_1\right)_{s,j} |\$^\lambda_{r,s}\rangle & b=1 \end{cases}$$

Then if $b=0$ (i.e. the challenger did not apply a pre-action), the state remains in the same Fourier subspace with certainty, and so a swap test between the archetype states produced by performing a Fourier extraction on both registers will succeed with probability 1, and we output $b'=0$.

If $b=1$, then with probability $1-\frac{1}{d_\lambda} \geq \frac{1}{2}$ (since $d_\lambda \geq 2$), the resulting state is in a different Fourier subspace. In this case, the swap test between the archetype states fails with probability $\frac{1}{2}$, in which case we output $b'=1$. Thus, in this case, we output 1 with probability at least $\frac{1}{4}$. The overall success probability is therefore $\frac{1}{2}+\frac{1}{8}=\frac{5}{8}$, breaking Assumption 2.

However, the initial states need not lie in the same initial Fourier subspace, so instead we give the following algorithm that sandwiches an application of Chal_b between two applications of the symmetric subspace projector. Formally, consider the following algorithm.

Algorithm 5. *Adversary for pre-action indistingiuishability given a two-register state, both with support on the same irreducible representation subspace W^λ.*

Input: Two quantum registers that are in valid money states for λ and a query to the blackbox $\mathsf{Chal}_b^{h_1,h_2}$ given by Assumption 2.

1. Perform **Fourier extraction** on the two halves of the input.
2. Perform a **swap test** between the two registers containing the archetype states produced.
3. Uncompute the **Fourier extraction** on both halves of the state.
4. Query $\mathsf{Chal}_b^{h_1,h_2}$ on the first register.
5. Perform **Fourier extraction** on both halves of the state.
6. Perform a second **swap test** between the two registers containing the archetype states produced.
7. If the results of both the first and second swap tests agree, output $b' = 0$ ("no preaction").
8. If the results of the two swap tests disagree, output $b' = 1$ ("preaction").

Case 1: $b = 0$ (there is no preaction). We first claim that in the case where there is no preaction, the algorithm outputs "no preaction" with probability 1. In order to argue this, we analyze the case when the adversary measures the symmetric subspace in the first measurement *after* performing the Fourier extraction, and argue that un-computing the Fourier extraction, applying $\mathsf{Chal}_0^{h_1,h_2}$, and then performing Fourier extraction *always* maps us back into the symmetric subspace on the first register. In this part of the proof, all sums are over $[d_\lambda]$.

Recall that the symmetric subspace is equal to the span of $|\psi\rangle^{\otimes 2}$, for $|\psi\rangle = \sum_{i,j} \alpha_i |\phi_i^\lambda\rangle$, so we can write the state after measuring the symmetric subspace as being in the span of:

$$\left(\sum_{i,k} \alpha_i \alpha_k |\phi_i^\lambda\rangle \otimes |\phi_k^\lambda\rangle\right) \otimes \sum_{j,\ell} \beta_{j,\ell} |\lambda, \lambda, j, \ell\rangle \ .$$

Inverting the Fourier extraction, we get the following state

$$\sum_{i,k,j,\ell} \alpha_i \alpha_k \beta_{j,\ell} |\$_{i,j}^\lambda\rangle \otimes |\$_{k,\ell}^\lambda\rangle \ .$$

Then, after applying $\mathsf{Chal}_0^{h_1,h_2}$ to the first register of this state, we have the following.

$$\sum_{i,j,k,\ell} \sum_s \alpha_i \alpha_k \beta_{j,\ell} \varrho_\lambda(h_1)_{s,j} |\$_{i,s}^\lambda\rangle \otimes |\$_{k,\ell}^\lambda\rangle \ .$$

Then after performing Fourier extraction on both registers, we end up with the following state

$$\begin{aligned}
&\sum_{i,j,k,\ell}\sum_{s}\alpha_i\alpha_k\beta_{j,\ell}\varrho_\lambda(h_1)_{s,j}\left(|\phi_i^\lambda\rangle\otimes|\phi_k^\lambda\rangle\right)\otimes|\lambda,\lambda,s,\ell\rangle\\
&\qquad=\sum_{i,k}\alpha_i\alpha_k\left(|\phi_i^\lambda\rangle\otimes|\phi_k^\lambda\rangle\right)\otimes\sum_{j,s,\ell}\beta_{j,\ell}\varrho_\lambda(h_1)_{s,j}\,|\lambda,\lambda,s,\ell\rangle\\
&\qquad=\sum_{i,k}\alpha_i\alpha_k\left(|\phi_i^\lambda\rangle\otimes|\phi_k^\lambda\rangle\right)\otimes\sum_{s,\ell}\sum_{j}(\beta_{j,\ell}\varrho_\lambda(h_1)_{s,j})\,|\lambda,\lambda,s,\ell\rangle\ .
\end{aligned}$$

Setting $\beta'_{s,\ell}=\sum_j\beta_{j,\ell}\varrho_\lambda(h)_{s,j}$, we get that we are still in the symmetric subspace within the first register. Since this applied to any setting of coefficients, the unitary transformation that composes steps 2, 3 and 4 preserves the symmetric and anti-symmetric subspaces. Thus, if the first measurement has either outcome, the second measurement on step 6 will have the same outcome with probability 1, and the adversary will output 'no preaction' with probability 1.

Case 2: $b=1$ **(there is a preaction).** We perform a similar analysis in the case where there is a pre-action, but now we will need to consider both subspaces. This is because we need to prove that the unitary that the adversary implements in steps 3 through 5 maps *every* vector from the symmetric subspace to something with high overlap with the anti-symmetric subspace, and vice versa. Starting with the symmetric subspace, we have the same starting state after inverting the Fourier extraction.

$$\sum_{i,k,j,\ell}\alpha_i\alpha_k\beta_{j,\ell}\,|\$_{i,j}^\lambda\rangle\otimes|\$_{k,\ell}^\lambda\rangle\ .$$

After applying $\mathsf{Chal}_1^{h_1,h_2}$, we will end up with the following state

$$\sum_{i,k,j,\ell,r,s}\alpha_i\alpha_k\beta_{j,\ell}\varrho_\lambda(h_2^{-1})_{i,r}\varrho_\lambda(h_1)_{s,j}\,|\$_{r,s}^\lambda\rangle\otimes|\$_{k,\ell}^\lambda\rangle\ .$$

After performing Fourier extraction, we end up with the following state.

$$\begin{aligned}
&\sum_{i,k,j,\ell,r,s}\alpha_i\alpha_k\beta_{j,\ell}\varrho_\lambda(h_2^{-1})_{i,r}\varrho_\lambda(h_1)_{s,j}\left(|\phi_r^\lambda\rangle\otimes|\phi_k^\lambda\rangle\right)|\lambda,\lambda,s,\ell\rangle\\
&\qquad=\left(\sum_{r,k}\left(\sum_i\alpha_i\varrho_\lambda(h_2^{-1})_{i,r}\right)\alpha_k\,|\phi_r^\lambda\rangle\otimes|\phi_k^\lambda\rangle\right)\otimes\sum_{s,\ell}\left(\sum_j\beta_{j,\ell}\varrho_\lambda(h_1)_{s,j}\right)|\lambda,\lambda,s,\ell\rangle\\
&\qquad=\left(\sum_r\alpha'_r\,|\phi_r^\lambda\rangle\right)\otimes\left(\sum_k\alpha_k\,|\phi_k^\lambda\rangle\right)\otimes\sum_{s,\ell}\left(\sum_j\beta_{j,\ell}\varrho_\lambda(h_1)_{s,j}\right)|\lambda,\lambda,s,\ell\rangle\ .
\end{aligned}$$

Here in the final line we define $\alpha'_r=\sum_i\alpha_i\varrho(h_2^{-1})_{i,r}$. We can then write out the following expression for the inner product of the first two registers with their swap.

$$\begin{aligned}
\mathrm{F}_{\mathrm{SWAP}}&=\left(\sum_r(\alpha'_r)^\dagger\,\langle\phi_r^\lambda|\right)\otimes\left(\sum_k\alpha_k^\dagger\,\langle\phi_k^\lambda|\right)\mathrm{SWAP}\left(\sum_{r'}\alpha'_{r'}\,|\phi_{r'}^\lambda\rangle\right)\otimes\left(\sum_{k'}\alpha_{k'}\,|\phi_{k'}^\lambda\rangle\right)\\
&=\sum_{r,k}\left((\alpha'_r)^\dagger\,\langle\phi_r^\lambda|\right)\otimes\left(\alpha_k^\dagger\,\langle\phi_k^\lambda|\right)\mathrm{SWAP}\left(\alpha'_k\,|\phi_k^\lambda\rangle\right)\otimes\left(\alpha_r\,|\phi_r^\lambda\rangle\right)\\
&=\sum_{r,k}\left((\alpha'_r)^\dagger\alpha_k^\dagger\alpha_r\alpha'_k\right)\ .
\end{aligned}$$

Now we analyze a single term in the sum. Since α' itself is a sum of more elements, this will make the equations more manageable.

$$\begin{aligned}(\alpha'_r)^\dagger \alpha_k^\dagger \alpha_r^\dagger \alpha'_k &= \sum_{i,i'} \alpha_i^\dagger \varrho_\lambda(h_2^{-1})_{i,r}^\dagger \alpha_k^\dagger \alpha_r \alpha'_i \varrho_\lambda(h_2)_{i',k}^{-1} \\ &= \alpha_k^\dagger \alpha_r \sum_{i,i'} \alpha_i^\dagger \alpha_{i'} \varrho_\lambda(h_2^{-1})_{i,r}^\dagger \varrho_\lambda(h_2^{-1})_{i',k} \,.\end{aligned}$$

Now, computing an average over group elements and adding back in the sum over r and k, we have the following:

$$\begin{aligned}\sum_{r,k} \alpha_k^\dagger \alpha_r \sum_{i,i'} \alpha_i^\dagger \alpha_{i'} \mathop{\mathbb{E}}_{h_2 \in G} \varrho_\lambda(h_2^{-1})_{i,r}^\dagger \varrho_\lambda(h_2^{-1})_{i',k} &= \frac{1}{d_\lambda} \left(\sum_r \alpha_r^\dagger \alpha_r \right) \left(\sum_i \alpha_i^\dagger \alpha_i \right) \\ &= \frac{1}{d_\lambda} \,.\end{aligned}$$

Here we use the fact that $\langle \$^\lambda_{a,b} \,|\, \$^\lambda_{c,d} \rangle = \frac{d_\lambda}{|G|} \sum_{h \in G} \varrho_\lambda(h^{-1})^*_{a,b} \varrho_\lambda(h^{-1})_{c,d} = \delta_{ac}\delta_{bd}$ (Lemma 4.18) to cancel out the terms for which $r \neq k$ and $i \neq i'$, and then we use the fact that α_i come from a normalized quantum state. To complete the proof, the probability that the swap test accepts on the state is given by

$$\frac{1}{2}\left(1 + \mathrm{F}_{\mathrm{SWAP}}\right) = \frac{1}{2} + \frac{1}{2d_\lambda} \,.$$

This means that *every* vector in the symmetric state gets mapped to a vector with overlap $1/2 + 1/2d_\lambda$ with the anti-symmetric state. Thus, if the first swap test returned the symmetric subspace, the second one returns the symmetric subspace with this probability.

Now, we need to analyze the anti-symmetric subspace. Similar to before, we take a basis for the anti-symmetric subspace and analyze what happens. There is a simple basis described by the $\binom{d_\lambda}{2}$ vectors of the form

$$\frac{1}{\sqrt{2}} \left(|\$^\lambda_{i,j}\rangle \otimes |\$^\lambda_{k,\ell}\rangle - |\$^\lambda_{k,j}\rangle \otimes |\$^\lambda_{i,\ell}\rangle \right) .$$

Going through the same steps, after applying Chal, now with a pre-action, we have the following state

$$\frac{1}{\sqrt{2}} \sum_{r,s} \left(\varrho_\lambda(h_2^{-1})_{i,r} \varrho_\lambda(h_1)_{s,j} \, |\$^\lambda_{r,s}\rangle \otimes |\$^\lambda_{k,\ell}\rangle - \varrho_\lambda(h_2^{-1})_{k,r} \varrho_\lambda(h_1)_{s,j} \, |\$^\lambda_{r,s}\rangle \otimes |\$^\lambda_{i,\ell}\rangle \right) .$$

Now we can examine the probability that a state starting from the symmetric subspace is still in the symmetric subspace (and that a state starting from the anti-symmetric subspace is still in the anti-symmetric subspace) after the Fourier extraction and swap test. When we perform Fourier extraction, we have the following state

$$\begin{aligned}|\psi_{i,j,k,\ell}\rangle &= \frac{1}{\sqrt{2}} \sum_{r,s} \left(\varrho_\lambda(h_2^{-1})_{i,r} \varrho_\lambda(h_1)_{s,j} \, |\phi^\lambda_r\rangle \otimes |\phi^\lambda_k\rangle - \varrho_\lambda(h_2^{-1})_{k,r} \varrho_\lambda(h_1)_{s,j} \, |\phi^\lambda_r\rangle \otimes |\phi^\lambda_i\rangle \right) \otimes |\lambda, \lambda, s, \ell\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{r} \left(\varrho_\lambda(h_2^{-1})_{i,r} \, |\phi^\lambda_r\rangle \otimes |\phi^\lambda_k\rangle - \varrho_\lambda(h_2^{-1})_{k,r} \, |\phi^\lambda_r\rangle \otimes |\phi^\lambda_i\rangle \right) \otimes \sum_{s} \varrho_\lambda(h_1)_{s,j} \, |\lambda, \lambda, s, \ell\rangle \,.\end{aligned}$$

Since the operations up until now were unitary, we can write every state in the anti-symmetric subspace as a linear combination of vectors of this form. $\sum_{i,j,k,\ell} \alpha_{i,j,k,\ell} \, |\psi_{i,j,k,\ell}\rangle$. We need to compute the inner product between this state and the swapped version of this state, which we can compute as

$$\mathop{\mathbb{E}}_{h_2\in G}\left[\sum_{\substack{i,j,k,\ell\\ i',j',k',\ell'}}\alpha_{i,j,k,\ell}\alpha^{\dagger}_{i',j',k',\ell'}\left\langle\psi_{i,j,k,\ell}\right|\mathrm{SWAP}\left|\psi_{i',j',k',\ell'}\right\rangle\right]$$

$$= \mathop{\mathbb{E}}_{h_2\in G}\Bigg[\frac{1}{2}\sum_{i,k,k',i'}\sum_{r,r'}\Big(\varrho_\lambda(h_2^{-1})^*_{i',r}\left\langle\phi^\lambda_r\right|\otimes\left\langle\phi^\lambda_{k'}\right| - \varrho_\lambda(h_2^{-1})^*_{k',r}\left\langle\phi^\lambda_r\right|\otimes\left\langle\phi^\lambda_{i'}\right|\Big)$$

$$\Big(\varrho_\lambda(h_2^{-1})_{i,r'}\left|\phi^\lambda_k\right\rangle\otimes\left|\phi^\lambda_{r'}\right\rangle - \varrho_\lambda(h_2^{-1})_{k,r'}\left|\phi^\lambda_i\right\rangle\otimes\left|\phi^\lambda_{r'}\right\rangle\Big)\left(\sum_{j,\ell}\alpha_{i,j,k,\ell}\alpha^\dagger_{i',j,k',\ell}\right)\Bigg]$$

$$= \mathop{\mathbb{E}}_{h_2\in G}\Bigg[\frac{1}{2}\sum_{i,k,k',i'}\sum_{r,r'}\Big(\varrho_\lambda(h_2^{-1})^*_{i',r}\varrho_\lambda(h_2^{-1})_{i,r'}\left\langle\phi^\lambda_r\,\middle|\,\phi^\lambda_k\right\rangle\left\langle\phi^\lambda_{k'}\,\middle|\,\phi^\lambda_{r'}\right\rangle - \varrho_\lambda(h_2^{-1})^*_{i',r}\varrho_\lambda(h_2^{-1})_{k,r'}\left\langle\phi^\lambda_r\,\middle|\,\phi^\lambda_i\right\rangle\left\langle\phi^\lambda_{k'}\,\middle|\,\phi^\lambda_{r'}\right\rangle$$

$$- \varrho_\lambda(h_2^{-1})^*_{k',r}\varrho_\lambda(h_2^{-1})_{i,r'}\left\langle\phi^\lambda_r\,\middle|\,\phi^\lambda_k\right\rangle\left\langle\phi^\lambda_{i'}\,\middle|\,\phi^\lambda_{r'}\right\rangle + \varrho_\lambda(h_2^{-1})^*_{k',r}\varrho_\lambda(h_2^{-1})_{k,r'}\left\langle\phi^\lambda_r\,\middle|\,\phi^\lambda_i\right\rangle\left\langle\phi^\lambda_{i'}\,\middle|\,\phi^\lambda_{r'}\right\rangle\Big)\left(\beta_{i,k,k',i'}\right)$$

$$= \mathop{\mathbb{E}}_{h_2\in G}\Bigg[\frac{1}{2}\sum_{i,k,k',i'}\Big(\varrho_\lambda(h_2^{-1})^*_{i',k}\varrho_\lambda(h_2^{-1})_{i,k'} - \varrho_\lambda(h_2^{-1})^*_{i',i}\varrho_\lambda(h_2^{-1})_{k,k'}$$

$$- \varrho_\lambda(h_2^{-1})^*_{k',k}\varrho_\lambda(h_2^{-1})_{i,i'} + \varrho_\lambda(h_2^{-1})^*_{k',i}\varrho_\lambda(h_2^{-1})_{k,i'}\Big)\beta_{i,k,k',i'}\Bigg]$$

$$= \sum_{i,k}\frac{1}{2}\beta_{i,k,k,i}\Big(\mathop{\mathbb{E}}_{h_2\in G}\left[\left|\varrho_\lambda(h_2^{-1})_{i,k}\right|^2 + \left|\varrho_\lambda(h_2^{-1})_{k,i}\right|^2\right]\Big).$$

In the first equality, the swap only affects the first two registers, so the final two indices must be the same to survive the inner product. In the third equality, we use the fact that $\langle\phi^\lambda_a\,|\,\phi^\lambda_b\rangle = \delta_{ab}$. In getting to the final line, we use the fact that the i indices are never equal to the k indices, by the fact that we are in the anti-symmetric group. Combining this with the fact from before that $\sum_{h\in G}\varrho_\lambda(h^{-1})^*_{a,b}\varrho_\lambda(h^{-1})_{c,d} = \delta_{c,d}\delta_{b,d}$, we can remove the two negative terms when averaging over the group elements. Using the same fact, we have that for the remaining terms, we have

$$\frac{1}{|G|}\sum_{h_2\in G}\left|\varrho_\lambda(h_2^{-1})_{i,k}\right|^2 + \frac{1}{|G|}\sum_{h_2\in G}\left|\varrho_\lambda(h_2^{-1})_{k,i}\right|^2 = \frac{2}{d_\lambda}.$$

Since the $\beta_{i,k,k,i}$ sum to 1 (as they are again the norm of the original vectors), the probability that the swap test succeeds on the second try is exactly

$$\frac{1}{2} + \frac{1}{2}\Big(\frac{1}{d_\lambda}\Big).$$

Now, we have shown that in the case when there is a pre-action, for *all* states, the probability that the second swap test succeeds is given by

$$\frac{1}{2} + \frac{1}{2d_\lambda}.$$

Since the adversary accepts whenever the results are different, the adversary outputs "preaction" with probability at least

$$\frac{1}{2} - \frac{1}{2d_\lambda}.$$

This is also the distinguishing advantage, as we showed that in the case where there is no pre-action, the adversary outputs "no pre-action" with probabiliy 1.

If the adversary starts with a state that is $2d_\lambda\epsilon/(d_\lambda+1)$ close to the tensor product of two copies of W^λ, they can first simply measure the irreducible representation label of both states, and condition on getting λ for both run this test. If the probability they measure λ for both is at least the given probability, then their distinguishing advantage will be at least ϵ. □

6.3.3 Generalizing to Intransitive Group Actions

Previously, we assumed that the group action was *transitive*. That is, it had a single orbit, such that every element of the set X can be reached from a single starting point $x \in X$. In this subsection, we generalize to the case in which the group action is *intransitive*. This means that the space is divided up into multiple orbits, with each orbit operating as a new multiplicity subspace of the whole representation space.

Note that the construction does not need to change for intransitive group actions. We can still have a fixed starting element x, whose orbit will be used by the minting algorithm to mint banknotes. However, for the proof, we can no longer assume that the two registers produced by the adversary have support on the same orbit—the orbit of x. The adversary may in general attempt to mint banknotes with supports on *different orbits*.

We comment on how the security of the previous section generalizes to the intransitive setting.

Intransitive Preaction Security. We modify the definitions of preaction security to the intransitive case. Let $(G, X, *, x)$ be an intransitive group action.

Assumption 3 (Intransitive Preaction Hardness)**.** *Given x, $g*x$, and h for a fixed starting element, $x \in X$, and random $g, h \leftarrow G$, it is hard to output $gh^{-1} * x$. That is, there exists an $\epsilon > 0$ such that for all QPT adversaries, $\mathcal{A}$,*

$$\Pr\left[z = gh^{-1} * x \ : \ x \leftarrow X,\ g, h \leftarrow G,\ z \leftarrow \mathcal{A}(x, g*x, h)\right] \leq \frac{1}{|G|} + \epsilon$$

Assumption 4 (Intransitive Preaction Indistinguishability)**.** *It is hard to distinguish whether a preaction has been performed relative to a set of prefixed starting points. Let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be the orbits of the group action and let $x_1, \ldots, x_m$ be representatives from each orbit ($x_i \in \mathcal{O}_i$). Let $\mathsf{Chal}_b^{h_1,h_2} \ : \ g * x_i \mapsto h_1\, g\, h_2^{-b} * x_i$, for $b \in \{0,1\}$ and $h_1, h_2 \in G$. Then there exists an $\epsilon > 0$ such that for all QPT adversaries, $\mathcal{A}$, that make a single query to $\mathsf{Chal}_b^{h_1,h_2}$,*

$$\Pr\left[b' = b \ : \ h_1, h_2 \leftarrow G,\ b \leftarrow \{0,1\},\ \ b' \leftarrow \mathcal{A}^{\mathsf{F}_b^{h_1,h_2}}\right] \leq \frac{1}{2} + \epsilon$$

Note that when $b = 0$, the challenger $\mathsf{Chal}_b^{h_1,h_2}$ performs a group action for a random group element h_1, and when $b = 1$, it performs both a random group action with h_1 and a random group pre-action with h_2.

Definition 6.18. *We say that a group action of group G_n on set X_n with starting element x is* ϵ-preaction secure *if both Assumption 3 and Assumption 4 hold for the group action against any QPT adversary with advantage ϵ. We say that the group action is preaction secure if it is $\mathsf{negl}(n)$-preaction secure for any negligible function negl.*

We also need an additional technical assumption, which says that it is hard to find "bad" orbits.

Assumption 5 (Intractable bad irreps)**.** *We say that a group action has* δ-intractable bad irreps *if any QPT adversary has probability at most* δ *of producing an* $x \in X$ *and an irreducible representation* λ *such that (1)* $d_\lambda > 1$*, but (2)*λ *only has a single multiplicity subspace in the representation of* G *acting on the orbit* $\mathcal{O}_i$ *containing* x*.*

Note that if all orbits $\mathcal{O}_i$ are in bijection with G, then the representation of G acting on $\mathcal{O}_i$ will have d_λ multiplicity subspaces of each irrep λ. However, if some orbit contains an element x such that $g * x = x$ for some g, then the number of multiplicity subspaces of λ may be smaller. Assumption 5 says that it is hard to find such an irrep and representative of such an orbit.

Proposition 6.19. *Suppose that the group action used in the quantum money construction (Section 6.3.1) is* ϵ*-intrasitive preaction secure and has* δ*-intractable bad irreps. Then no QPT adversary can produce a quantum state on two registers such the probability of measuring both in the same irreducible subspace is greater than* $2\epsilon + \delta$*.*

Proof. First, assume that the adversary does not sample a state in an intractable bad orbit. Since the probability is upper bounded by δ, this increase the probability that they measure a state in the same irreducible subspace by δ.

Similar to the proof of Proposition 6.17, we assume for the sake of contradiction that the adversary has an δ probability of measuring two states in the same irreducible representation. Then we consider the same algorithm, Algorithm 5, for distinguishing a black-box that performs a pre-action from a black-box that does not perform a pre-action.

First, let $|\$_{i,j}^{\lambda,x}\rangle$ be the money state that corresponds to irrep label λ, multiplicity subspace i, basis vector j, and starting element x. Further let $|\phi_i^{\lambda,x}\rangle$ be the archetype state corresponding to irrep λ, multiplicity subspace i and starting element x.

Case 1: $b = 0$ **(there is no preaction).** We begin by analyzing the performance of Algorithm 5 in the case when $b = 0$, first in the case where the symmetric subspace accepts and then the case when it fails. Then we can write every state in the symmetric subspace as follows for some choice of α_i^x and $\beta_{j,\ell}$.

$$\sum_{i,k,x,y} \alpha_i^x \alpha_k^y |\phi_i^{\lambda,x}\rangle \otimes |\phi_k^{\lambda,y}\rangle \otimes \sum_{j,\ell} \beta_{j,\ell} |\lambda, \lambda, j, \ell\rangle \ .$$

Here we note that this encompasses the case when the states span multiple orbits (indexed by starting elements x and y). Then after inverting the Fourier extraction, we get the following state

$$\sum_{i,k,j,\ell,x,y} \alpha_i^x \alpha_j^y \beta_{j,\ell} |\$_{i,j}^{\lambda,x}\rangle \otimes |\$_{k,\ell}^{\lambda,y}\rangle \ .$$

Then after applying the black box (recall that $b = 0$) to the first register, we have the following

$$\sum_{i,k,j,\ell,x,y} \sum_s \alpha_i^x \alpha_j^y \beta_{j,\ell} \varrho_\lambda(h_1)_{s,j} |\$_{i,s}^{\lambda,x}\rangle \otimes |\$_{k,\ell}^{\lambda,y}\rangle \ .$$

After performing Fourier extraction again, we get the following state, following the logic in Proposition 6.17.

$$\sum_{i,k,x,y} \alpha_i^x \alpha_k^y |\phi_i^{\lambda,x}\rangle \otimes |\phi_j^{\lambda,y}\rangle \otimes \sum_{s,\ell,j} (\beta_{j,\ell} \varrho_\lambda(h_1)_{s,j}) |\lambda, \lambda, s, \ell\rangle \ .$$

Thus, we measure a state in the symmetric subspace. Furthermore, since the symmetric subspace is perfectly mapped back to the symmetric subspace under the black box, if the first symmetric subspace measurement outputs the anti-symmetric subspace, the black box will keep the state in the anti-symmetric subspace. Thus, in the case that the $b = 0$, the algorithm accepts with probability 1.

Case 2: $b = 1$ **(there is a preaction).** We first start in the case when the symmetric subspace projector accepts. In this case, we can write the state after the projector accepts, similarly to before as

$$\sum_{i,k,x,y} \alpha_i^x \alpha_k^y \left|\phi_i^{\lambda,x}\right\rangle \otimes \left|\phi_k^{\lambda,y}\right\rangle \otimes \sum_{j,\ell} \beta_{j,\ell} \left|\lambda,\lambda,j,\ell\right\rangle .$$

After applying the black box (this time with a pre-action), we have the following state

$$\begin{aligned}
&\sum_{i,k,x,y,r,s} \alpha_i^x \alpha_k^y \beta_{j,\ell} \varrho_\lambda(h_2^{-1})_{i,r} \varrho_\lambda(h_1)_{s,j} \left|\phi_r^{\lambda,x}\right\rangle \otimes \left|\phi_k^{\lambda,y}\right\rangle \otimes \left|\lambda,\lambda,s,\ell\right\rangle \\
&\quad = \sum_{r,k,x,y} \left(\sum_i \alpha_i^x \varrho_\lambda(h_2^{-1})_{i,r}\right) \alpha_k^y \left|\phi_r^{\lambda,x}\right\rangle \otimes \left|\phi_k^{\lambda,y}\right\rangle \otimes \sum_{s,\ell} \left(\sum_j \beta_{j,\ell} \varrho_\lambda(h_1)_{s,j}\right) \left|\lambda,\lambda,s,\ell\right\rangle \\
&\quad \left(\sum_{r,x} \alpha_r'^x \left|\phi_r^{\lambda,x}\right\rangle\right) \otimes \left(\sum_{k,y} \alpha_k^y \left|\phi_k^{\lambda,y}\right\rangle\right) \otimes \sum_{s,\ell} \left(\sum_j \beta_{j,\ell} \varrho_\lambda(h_1)_{s,j}\right) \left|\lambda,\lambda,s,\ell\right\rangle .
\end{aligned}$$

We can then write the expression for the fidelity of this state and the swapped version if the state as follows.

$$\mathrm{F}_{\mathrm{SWAP}} = \sum_{r,k,x,y} \left(\left(\alpha_r'^x\right)^\dagger \left(\alpha_r^x\right)^\dagger \left(\alpha_k^y\right)^\dagger \left(\alpha_k'^y\right)\right)$$

Here the only difference from before is that the inner product also enforces that the orbits (x and y) are the same between the left and right. Expanding each α' as before, we get the following expression for the fidelity of the state with its swap.

$$\sum_{r,k,x,y} \left(\alpha_k^y\right)^\dagger \left(\alpha_r^x\right)^\dagger \sum_{i,i'} \left(\alpha_i^x\right)^\dagger \alpha_{i'}^y \varrho_\lambda(h_2^{-1})_{i,r}^\dagger \varrho_\lambda(h_2^{-1})_{i',k} .$$

Computing the average over the group and applying Lemma 4.18, we get the following quantity

$$\begin{aligned}
&\sum_{r,k,x,y} \left(\alpha_k^y\right)^\dagger \left(\alpha_r^x\right)^\dagger \sum_{i,i'} \left(\alpha_i^x\right)^\dagger \alpha_{i'}^y \mathop{\mathbb{E}}_{h_2 \in G} \left[\varrho_\lambda(h_2^{-1})_{i,r}^\dagger \varrho_\lambda(h_2^{-1})_{i',k}\right] \\
&\quad = \frac{1}{d_\lambda} \sum_{x,y} \left(\sum_r \left(\alpha_r^x\right)^\dagger \left(\alpha_r^y\right)\right) \left(\sum_i \left(\alpha_i^x\right)^\dagger \left(\alpha_i^y\right)\right) \\
&\quad \leq \frac{1}{d_\lambda} \sqrt{\sum_{x,y} \left(\sum_r \left(\alpha_r^x\right)^\dagger \left(\alpha_r^y\right)\right) \cdot \sum_{x,y} \left(\sum_i \left(\alpha_i^x\right)^\dagger \left(\alpha_i^y\right)\right)} \\
&\quad = \frac{1}{d_\lambda} .
\end{aligned}$$

Here after applying the Schur orthogonality rules, we apply Cauchy-Schwarz and then use the fact that both terms in the square roots are the norm of the original vector, so they are 1. To complete the proof, we note that the probability that the swap test succeeds is given by

$$\frac{1}{2}(1 + \mathrm{F}_{\mathrm{SWAP}}) = \frac{1}{2} + \frac{1}{2d_\lambda} .$$

Now we proceed with the analysis in the case that the symmetric subspace measurements outputs the anti-symmetric subspace. We can similarly write the anti-symmetric subspace on the first

register as the span of the following vectors (and analyzing the action of the rest of the algorithm on those vectors will imply the action on every state in the anti-symmetric subspace).

$$\frac{1}{\sqrt{2}}\left(|\$_{i,j}^{\lambda,x}\rangle \otimes |\$_{k,\ell}^{\lambda,y}\rangle - |\$_{k,j}^{\lambda,y}\rangle \otimes |\$_{i,\ell}^{\lambda,x}\rangle\right).$$

Here we require that $\delta_{x,y}\delta_{i,k} = 0$ (i.e. that at least one of the pairs is different). Similar to before we can write out the state after applying the black box (now with a pre-action), and then the Fourier extraction as follows

$$\begin{aligned}
|\psi_{i,j,k,\ell}^{x,y}\rangle &= \sqrt{1}2\sum_{r,s}\left(\varrho_\lambda(h_2^{-1})_{i,r}\varrho_\lambda(h_1)_{s,j}\,|\phi_r^{\lambda,x}\rangle \otimes |\phi_k^{\lambda,x}\rangle - \varrho_\lambda(h_2^{-1})_{k,r}\varrho_\lambda(h_1)_{s,j}\,|\phi_r^{\lambda,y}\rangle \otimes |\phi_i^{\lambda,x}\rangle\right) \otimes |\lambda,\lambda,s,\ell\rangle \\
&= \frac{1}{\sqrt{2}}\sum_r\left(\varrho_\lambda(h_2^{-1})_{i,r}\,|\phi_r^{\lambda,x}\rangle \otimes |\phi_k^{\lambda,y}\rangle - \varrho_\lambda(h_2^{-1})_{k,r}\,|\phi_r^{\lambda,y}\rangle \otimes |\phi_i^{\lambda,x}\rangle\right) \otimes \sum_s \varrho_\lambda(h_1)_{s,j}\,|\lambda,\lambda,s,\ell\rangle\,.
\end{aligned}$$

Now, in a same fashion as before we can write every state in the anti-symmetric subspace as a linear combination of these basis vectors as $\sum_{i,j,k,\ell,x,y}\alpha_{i,j,k,\ell}^{x,y}|\psi_{i,j,k,\ell}^{x,y}\rangle$. We then need to compute the inner product between this state and the state after swapping with itself, averaged over all group elements. We get the following

$$\begin{aligned}
&\mathop{\mathbb{E}}_{h_2\in G}\left[\sum_{\substack{i,j,k,\ell,x,y\\ i',j',k',\ell',x',y'}}\left(\alpha_{i,j,k,\ell}^{x,y}\right)^\dagger\left(\alpha_{i',j',k',\ell'}^{x',y'}\right)\langle\psi_{i,j,k,\ell}^{x,y}|\,\mathrm{SWAP}\,|\psi_{i',j',k',\ell'}^{x',y'}\rangle\right] \\
&\quad= \mathop{\mathbb{E}}_{h_2\in G}\left[\frac{1}{2}\sum_{x,y,x',y'}\sum_{i,k,i',k'}\sum_{r,r'}\left(\varrho_\lambda(h_2^{-1})_{i',r}^*\,\langle\phi_r^{\lambda,x}| \otimes \langle\phi_{k'}^{\lambda,y}| - \varrho_\lambda(h_2^{-1})_{k',r}^*\,\langle\phi_r^{\lambda,y}| \otimes \langle\phi_{i'}^{\lambda,x}|\right)\right. \\
&\qquad\qquad\left.\left(\varrho_\lambda(h_2^{-1})_{i,r'}\,|\phi_k^{\lambda,y'}\rangle \otimes |\phi_{r'}^{\lambda,x'}\rangle - \varrho_\lambda(h_2^{-1})_{k,r'}\,|\phi_i^{\lambda,x'}\rangle \otimes |\phi_{r'}^{\lambda,y'}\rangle\right)\left(\sum_{j,\ell}\alpha_{i,j,k,\ell}^{x,y}\left(\alpha_{i',j',k',\ell'}^{x',y'}\right)^\dagger\right)\right] \\
&\quad= \mathop{\mathbb{E}}_{h_2\in G}\left[\frac{1}{2}\sum_{x,y,x',y'}\sum_{i,k,i',k'}\sum_{r,r'}\left(\varrho_\lambda(h_2^{-1})_{i',r}^*\varrho_\lambda(h_2^{-1})_{i,r'}\,\langle\phi_r^{\lambda,x}|\phi_k^{\lambda,y'}\rangle\,\langle\phi_{k'}^{\lambda,y}|\phi_{r'}^{\lambda,x'}\rangle\right.\right. \\
&\qquad\qquad - \varrho_\lambda(h_2^{-1})_{i',r}^*\varrho_\lambda(h_2^{-1})_{k,r'}\,\langle\phi_r^{\lambda,x}|\phi_i^{\lambda,x'}\rangle\,\langle\phi_{k'}^{\lambda,y}|\phi_{r'}^{\lambda,y'}\rangle \\
&\qquad\qquad - \varrho_\lambda(h_2^{-1})_{k',r}^*\varrho_\lambda(h_2^{-1})_{i,r'}\,\langle\phi_r^{\lambda,y}|\phi_k^{\lambda,y'}\rangle\,\langle\phi_{i'}^{\lambda,x}|\phi_{r'}^{\lambda,x'}\rangle \\
&\qquad\qquad\left.\left. + \varrho_\lambda(h_2^{-1})_{k',r}^*\varrho_\lambda(h_2^{-1})_{k,r'}\,\langle\phi_r^{\lambda,y}|\phi_i^{\lambda,x'}\rangle\,\langle\phi_{i'}^{\lambda,x}|\phi_{r'}^{\lambda,y'}\rangle\right)\left(\beta_{i,k,k',i'}^{x,y,x',y'}\right)\right]. \\
&\quad= \mathop{\mathbb{E}}_{h_2\in G}\left[\sum_{x,y,x',y'}\sum_{i,k,i',k'}\left((\varrho_\lambda(h_2^{-1})_{i',k})^*\varrho_\lambda(h_2^{-1})_{i,k'}\delta_{x,y'}\delta_{y,x'} - \varrho_\lambda(h_2^{-1})_{i',i}^*\varrho_\lambda(h_2^{-1})_{k,k'}\delta_{x,x'}\delta_{y,y'}\right.\right. \\
&\qquad\qquad\left.\left. - \varrho_\lambda(h_2^{-1})_{k',k}^*\varrho_\lambda(h_2^{-1})_{i,i'}\delta_{x,x'}\delta_{y,y'} + \varrho_\lambda(h_2^{-1})_{k',i}^*\varrho_\lambda(h_2^{-1})_{k,i'}\delta_{x,y'}\delta_{y,x'}\right)(\beta_{i,k,i',k'}^{x,y,x',y'})\right] \\
&= \sum_{x,y}\sum_{i,k}\frac{1}{2}\beta_{i,k,k,i}^{x,y,y,x}\left(\mathop{\mathbb{E}}_{h_2\in G}\left[\left|\varrho_\lambda(h_2^{-1})_{i,k}\right|^2 + \left|\varrho_\lambda(h_2^{-1})_{k,i}\right|^2\right]\right).
\end{aligned}$$

In the first equality, we note that the swap only affects the first two registers, so the final two must be the same to survive the inner product, as before. Then we use the fact that the inner product of

the states $\langle \phi_a^{\lambda,x} | \phi_b^{\lambda,y} \rangle = \delta_{x,y}\delta_{a,b}$. Finally, we use the fact that in the anti-symmetric states, we can not have both the orbits *and* the multiplicity subspaces be the same (as noted in the description of the basis states). This allows us to apply the Schur orthogonality relations and remove the two negative terms when we average over the group elements.

Now, we can apply the same equality that we noted before to bound this by $\frac{2}{d_\lambda}$, again noting that the $\beta_{i,k,k,i}^{x,y,y,x}$ correspond to a normalized vector. Thus, the probability that the swap test succeeds is bounded from above by the following

$$\frac{1}{2} + \frac{1}{2d_\lambda}.$$

At this point, we have completed the analysis of the probability that the state passes the second test. In particular, when there is no preaction, the preaction distinguisher outputs "no preaction" with probability 1, and if there is a preaction the distinguisher outputs preaction with probability at least $\frac{1}{2} - \frac{1}{2d_\lambda}$. Thus, if the adversary instead starts with a state that has probability $d_\lambda \epsilon/(d_\lambda+1) \leq 2\epsilon$ of being measured in the tensor product of two copies of the irreducible space of λ that are not intractable bad irreps, they can first measure the state and then apply this distinguisher to break the preaction indinstinguishability with probability ϵ. Adding in the probability (δ) that the adversary measures a intractable bad irrep, we get the desired bound. □

With this proposition, we have shown that the construction of quantum lightning is secure if instantiated with a ϵ-preaction secure group action (as in Definition 6.18) that has negl-intractable bad irreps. In the next section, we will provide groups that might meet these conditions, providing the first instantiations of quantum lightning in the plain model from plausible assumptions.

6.4 Instantiations of the Construction

Here, we discuss some plausible instantiations of our quantum money scheme. Our main focus will be on *symmetric* group actions. First, we note that symmetric group actions have a negligible maximum Plancherel measure [VK85], a necessary condition for having a secure quantum lightning scheme and for our pre-action security assumption to hold. Symmetric groups also admit an efficient quantum Fourier transform [Bea97], a necessary condition for the efficiency of our protocol. This makes symmetric group actions a natural candidate for instantiating our scheme.

Graph Isomorphism. Given a graph (V, E) with $|V| = n$, the symmetric group S_n acts on (V, E) by permuting the vertices.

Note that the discrete logarithm problem on graphs is exactly the Graph Isomorphism problem. Graph Isomorphism can be solved in (classical) quasi-polynomial time [Bab16]. However, it is still conceivable that there is no polynomial-time algorithm, giving a plausible candidate group action.

We also would like S_n to act regularly. If (V, E) has a trivial automorphism group, then S_n acts semiregularly on the orbit of (V, E). "Most" graphs have trivial automorphism groups [LM17]. Unfortunately, it is in general presumably hard to identify the orbit of a graph (V, E), since this would solve the graph isomorphism problem for (V, E). We therefore appeal to our generalization to intransitive group actions in Section 6.3.3. Therefore, even if there are multiple orbits, our security proof still works.

Permuting Matrices. The symmetric group S_n acts on the set of $n \times n$ symmetric matrices via $\sigma * M = \sigma \cdot M \cdot \sigma^T$. That is, permute the rows and columns of M by σ. This is in fact a generalization of the graph isomorphism group action, using the adjacency matrix of the graph.

McEliece Cryptosystem. The McEliece cryptosystem [McE78] contains an implicit group action. Here, we have the symmetric group acting on matrices, though the operation is quite different. Let $\mathbb{F}$ be a field and $m > n$ be integers. Then consider the set $R_{n,m}$ of row-reduced matrices in $\mathbb{F}^{n\times m}$. Then S_m acts on $R_{n,m}$, with $\sigma * M \to M'$ where M' is the result of:

- First permute the columns of M according to σ.
- Then row-reduce the result.

Note that the McEliece cryptosystem uses the orbit of a specific matrix M that has good error correcting properties. The original proposal in [McE78] is to use binary Goppa codes. This original proposal has so far resisted (quantum) cryptanalysis efforts.

Note that we do not need any specific properties of M, allowing us to use basically any matrix M. Thus, even if the McEliece cryptosystem is broken, we still get a plausible quantum money candidate.

As for regularity, for a sufficiently wide matrix and/or sufficiently large field $\mathbb{F}$, S_m will act semiregularly on the orbit of "most" matrices, as shown in the lemma below. As with the Graph Isomorphism case, we do not expect to be able to identify the orbits of typical matrices, so we instead appeal to our generalization to non-transitive matrices.

Lemma 6.20. *Let $m \geq 2n+1$. Consider sampling M such that (1) the left $n \times n$ matrix is the identity, and (2) the right $n \times (m-n)$ matrix is uniform. Then except with probability $p := m^2n^2|\mathbb{F}|^{-1} + (m!)|\mathbb{F}|^{-n}$, S_m will act semiregularly on the orbit of M. In particular, if $|\mathbb{F}| = m^{\omega(1)}$, then p is negligible.*

Proof. Fix a permutation $\sigma \in S_m$ other than the identity. We bound the probability that $\sigma * M = M$.

Let us first suppose that the right $n \times (m-n)$ sub-matrix of M contains all distinct and non-zero entries. Since the entries are uniform and independent, this occurs with probability at most $[mn(mn-1) + mn]|\mathbb{F}|^{-1} = m^2n^2|\mathbb{F}|^{-1}$.

Now consider permuting the columns of M according to σ. Denote the result by M'. Let M'' then be the result of row-reducing M'. We now consider three cases:

- Suppose $\sigma(i) = i$ for all $i \leq n$, meaning σ does not permute the first n columns. In this case, $M'' = M'$. Since the columns are distinct by our conditions on M and σ is not the identity, we have that $M' \neq M$. Thus, in this case $\sigma * M \neq M$.
- $\sigma(i) > n$ for all $i > n$. In other words, σ separately permutes the first n entries and permutes the remaining $m-n$ entries. In this case, M' is obtained from M by permuting the right $n \times (m-n)$ sub-matrix, and M'' is obtained from M' by simply permuting some of the rows of M'. In other words, M'' is obtained from M by permuting the rows and columns of the right $n \times (m-n)$ sub-matrix. As long as the entries of this sub-matrix are distinct, any such permutation of rows and columns will not preserve the matrix.
- $\sigma(i) \leq n$ for some $i > n$. In this case, $M'' \neq M'$. Let $D \in \mathbb{F}^{n\times n}$ be the matrix such that $M'' = D^{-1} \cdot M'$. Then we know that D is not the identity.

We now focus on the last case above. If the first n columns of M' are not full rank, then $M'' \neq M$. So suppose that the first n columns of M' are full rank. This means that D is exactly the first n columns of M'. If $M'' = M$, we then have that $D \cdot M = M'$. In other words, if we take the first n columns of M' (which is just a permuted version of M), and multiply this with M, we get exactly M'.

Moreover, since we are in the case $\sigma(i) \leq n$ for some $i > n$, this also means that $\sigma(j) > n$ for some $j \leq n$. Thus at least one of the columns of D came from the right $n \times (m-n)$ sub-matrix of M.

Since $m \geq 2n+1$, there will be some column i such that $i > n$ and $\sigma(i) > n$. In other words, this column is not among the first n in either M nor in M'. This column is therefore independent of D. Let v denote the vector of elements in this column.

For $M'' = D \cdot M'$ to be equal to M, we need that $D \cdot v$ is among the original columns of M. There are two possibilities:

- $\sigma(i) \neq i$. In this case, let w be the $\sigma(i)$-th column of M. Then $M'' = M$ implies $D \cdots v = w$. Since v is random and independent of D, w, this occurs with probability $|\mathbb{F}|^{-n}$.
- $\sigma(i) = i$. In this case, $M'' = M$ implies that $D \cdots v = v$. Fix a v such that all the entries of v are non-zero. Since v came from the right sub-matrix of M and we are assuming all the entries there are non-zero, we can assume that v satisfies this property. Now consider sampling D. D contains some columns that are fixed (those that were originally among the first n in M) and some that are random (those that were not among the first n in M). Moreover, at least one of the columns is random, since one of the rows came from the right sub-matrix of M. Since v is non-zero in all positions, it particular it is non-zero in some position corresponding to a random column of D. Thus, $D \cdot v$ is a random vector. The probability $D \cdot v = v$ over the choice of D is therefore at most $|\mathbb{F}|^{-n}$.

Therefore, the probability that there exists some σ such that $\sigma * M = M$ is at most the sum of

- The probability that the right $n \times (m-n)$ sub-matrix contains non-distinct entries, which is upper bounded by $m^2 n^2 |\mathbb{F}|^{-1}$
- For each $\sigma \in S_n$, $|\mathbb{F}|^{-n}$.

Thus, the overall probability that there exists some σ is at most $m^2 n^2 |\mathbb{F}|^{-1} + m! |\mathbb{F}|^{-n}$. □

6.5 Dual-Mode One-way Homomorphisms

In the previous sections, we gave a construction of quantum money/lightning when the group action is easy but its corresponding preaction is hard. In other words, for any group element g, encoded by the group action as $g * x$, we could only act on g from the left to get $hg * x$, but not from the right to get $gh^{-1} * x$. In this section, we explore how the construction of Section 6.1 changes if we explicitly allow acting on the encoded group element from *both sides*. In this case, we have two different but related representations of the same group—one for the action and one for the preaction. One important difference is that this allows verification to recover both of the fine Fourier indices (compare with the hardness of recovering i in Lemma 6.15).

In fact, we will see that when we allow the encoding to be a *homomorphism*, we get the surprising but useful property that four different notions of security are all identical, including the hardness of worst-case cloning, average cloning, minting a collision (i.e., breaking lightning security), and preparing the specific uniform superposition state corresponding to the trivial irrep.

We begin by giving a useful security definition for one-way homomorphisms:

Definition 6.21. *An injective (but not surjective) homomorphism $P : G \to H$[38] is a* dual-mode

[38]Technically, it is a *family* of homomorphisms, $\{P_n : G_n \to H_n\}_{n \in \mathbb{N}}$ but we omit the security parameter in the notation for succinctness.

one-way homomorphism *if there exists a fooling function* $S : G \to H$[39] *such that they satisfy the following properties:*

- ***Efficiency:*** *There is a QPT algorithm to efficiently compute* P*. There are also efficient QPT algorithms for computing the group operations on* G *and* H*.*[40]
- ***Statistical Distance:*** *Let* H_P *be the image of* P *and* H_S *be the image of* S*. Then* H_S *is sufficiently far from* H_P*. Specifically we require that,*[41]

$$\Pr[P(g)S(h) \in H_P \mid g, h \leftarrow G] \leq 1 - \frac{1}{\mathsf{poly}(n)}$$

- ***Indistinguishability:*** *It is hard to distinguish the images of* P *and* S*. Formally, for all QPT adversaries* A*,*

$$\Pr\left[A(h) = b \;\middle|\; \begin{array}{cc} b \leftarrow \{0,1\} & g \leftarrow G \\ h \leftarrow \begin{cases} P(g) & b = 0 \\ S(g) & b = 1 \end{cases} & \end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(n)$$

- ***Inaccessibility:*** *It is hard to sample an element of* $H \setminus H_P$*. Formally, for all QPT adversaries* A*,*

$$\Pr\left[h \in H \setminus H_P \;\middle|\; h \leftarrow A(1^\lambda)\right] \leq \mathsf{negl}(n)$$

Remark 6.22. *Note that while we do not explicitly require* P *to be one-way, this is implied by the definition: any adversary for inverting* P *can be used to break the indistinguishability security.*

Remark 6.23. *Combined with statistical distance, inaccessibility provides that the fooling function* S *is hard to compute even in the forward direction. In a cryptographic implementation we would sample a key pair of a public key* pk *and secret key* sk*, which would allow computing* P *and* S*, respectively (though we omit this in the definition for generality and simplicity). In other words, in the security game,* S *is a "secret" function that only the challenger knows. This is why we call it a dual-mode one-way homomorphism: the is a public mode* P *that is publicly computable, and a private mode* S *that is only privately computable but mimics* P *to the public.*

[39] We refer to P and S as the "public" and "secret" transformations, respectively. S may itself be a homomorphism but it need not be. Notice that we do not require S to be efficiently computable.

[40] In general, the algorithms for computing P and the group operations need only be approximately correct. Moreover, because of the inaccessibility condition, we only the algorithm for group operations on H to be correct and homomorphic on the image of P.

[41] This condition prevents P being a fooling function for itself. Note that it is equivalent to the condition that $\Pr[S(h) \notin H_P \mid h \leftarrow G] \geq \frac{1}{\mathsf{poly}(n)}$. Or in other words, that $|H_S \setminus H_P|/|H_S| \geq \frac{1}{\mathsf{poly}(n)}$ in the case where S is injective (which it need not be). The reason we prefer to write the statistical distance condition in this way is that if the promised algorithm, A, for group operations on H is randomized, we can take the probability to also be over this randomness.

$$\Pr[u \in H_P \mid u \leftarrow A(P(g), S(h)),\ g, h \leftarrow G] \leq 1 - \frac{1}{\mathsf{poly}(n)}$$

Observation 6.24. *We can build a plausible candidate dual-mode one-way homomorphism from any group action for which the computational Diffie-Hellman problem (CDH) is easy but the Discrete Logarithm problem (DLog) is hard.*[42] *Note that cryptographers typically would like CDH to be hard, since it allows for justifying the security of more varied protocols. Our construction therefore gives a "win-win" result, showing that in any group action for which DLog is hard, either (1) the more useful CDH problem is actually also hard, or (2) we obtain a plausible candidate dual-mode one-way homomorphism and hence a plausible quantum lightning scheme based on DLog. This win-win result is remeniscent of win-win results in [Zha21], though the details are entirely different.*

Main idea. We give the informal idea here but we leave a formal construction of dual-mode one-way homomorphisms from group actions to future work. Suppose we have a group G which acts on set X. Assume that the CDH problem is easy, and let A be the CDH adversary, which takes two elements $a * x, b * y \in X$ and outputs $ab * x$ if $x = y$, and behaves arbitrarily if $x \neq y$. We set H to be the set X with the "group operation" defined by A.[43] Let $x, y \in X$ be two set elements in different orbits of the group G, and let $P(g) = g * x$ and $S(g) = g * y$. Statistical distance comes from the fact that x and y are in different orbits.[44] Indistinguishability would come from the hardness of deciding if two elements are in the same orbit (one example being the hardness of the graph isomorphism problem). Inaccessibility would arise from the hardness of sampling a valid set element outside the orbit of any known elements.[45] Although we argue that these are reasonable assumptions, we do not know if any specific instantiations of group actions satisfy these requirements. We leave finding concrete instantiations of dual-mode one-way homomorphisms to future work. □

The lack of concrete instantiation of a dual-mode one-way homomorphism is a certainly disadvantage (as opposed to our construction from preaction security in Section 6.3.1, to which we give concrete candidate instatiations in Section 6.4). However, we believe that our construction from dual-mode one-way homomorphism is interesting in its own right. For instance, we have the property that four different security definitions—including average-case and worst-case cloning, as well as quantum lightning security—are all equivalent. To the best of our knowledge, this is the first plausible quantum money construction to have this useful property.

6.5.1 Quantum Money Construction

Let G be a group satisfying the requirements in Section 6.1, and let (P, S) be a dual-mode one-way homomorphism from G to H. We build a quantum lightning scheme, $(\mathsf{Mint}, \mathsf{Ver})$ as follows:

$\mathsf{Mint}(1^n) \to (\sigma,\ |\$^\sigma\rangle)$**:** Consider the group action of G on H that comes from left-multiplying an element $h \in H$ by the image of a group element $g \in G$ under P, with the starting element $x \in H$ being the identity element of H. That is, we have the group action $g * y \mapsto P(g)\, y$ for any $y \in H$.

[42] Note that such a group action is only possible for non-Abelian groups, since CDH and DLog are known to be computationally equivalent for Abelian groups [MZ22], further demonstrating the necessity of non-Abelian-ness in our generalizations.

[43] Since the adversary may act arbitrarily when $x \neq y$, this is not exactly a group operation. That is, it only defines a group operation on elements within the same orbit, but this will be sufficient for our purposes.

[44] Depending on the CDH adversary, the roles of x and y may need to be reversed in order to formally satisfy the statistical distance property. If the CDH adversary, when run on a random element of the orbit of x and a random element of the orbit of y, is more likely to produce an element of the orbit of x then we switch the roles. In other words, we set $P(g) = g * y$ and $S(g) = g * x$. In any case, one of the two choices suffices.

[45] This can be argued in the generic group model [Zha24].

Observe that because our starting element is the identity of H, we have an efficiently computable preaction as well, by multiplying in the same way on the right.

Minting follows from the construction in Section 6.1, and produces a serial number $\sigma \leftarrow \varrho$ denoting the measured irrep, and quantum money state $|\$^\lambda\rangle = \sum_{i,j\in[d_\lambda]} \alpha_{i,j} |\$^\lambda_{i,j}\rangle$, where

$$|\$^\lambda_{i,j}\rangle := \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda \left(h^{-1}\right)_{i,j} \mid P(h) \rangle$$

$\mathsf{Ver}(\sigma, |\pounds\rangle) \to \{\text{accept, reject}\}$**:** We follow the framework in Section 6.1 to verify under the two group actions (the action and the preaction) consisting of the left and right group operations on the encoded element. Note that within the image of P, this verification accepts any state of the original minted form, as well as states that are of that form, but that are shifted by an element of the center of G. In the security analysis, we show that these are the only states that pass verification.

6.5.2 Security Analysis

Theorem 6.25. *If (P, S) is a secure dual-mode one-way homomorphism for G_n, then $(\mathsf{Mint}, \mathsf{Ver})$ is a secure quantum lightning scheme.*

Proof. Let C be an adversary for the quantum lightning scheme, which outputs a state on two registers which both pass verification for the same serial number ϱ. We will show that it can be used to break the dual-mode one-way homomorphism.

Specifically, we will show that we can use C to break either the inaccessibility security or the indistinguishability security of the dual-mode one-way homomorphism.

Claim 6.26. *We can assume without loss of generality that the output of C is a tensor product and that the states both have the form $|\$^\lambda_{i,j}\rangle$, where*

$$|\$^\lambda_{i,j}\rangle := \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda \left(g^{-1}\right)_{i,j} \mid P(g) \rangle$$

for some $i, j \in [d_\lambda]$.

Proof. We begin by observing that if the quantum money state had non-negligible support on $H \backslash H_P$, then we can measure to get an element outside of the image of P and break the inaccessibility security of the dual-mode one-way homomorphism. Therefore, up to negligible error, we can assume that they both have support only on the image of P. Furthermore, we can assume that both have the same i and j, since we can perform a Fourier extraction twice on each state—both on the action and on the preaction—to get the corresponding i and j, and then change them to match. This gives us a tensor product state $|\$^\lambda_{i,j}\rangle \otimes |\$^\lambda_{i,j}\rangle$. □

We now show how to break indistinguishability security. We consider one of the copies, setting aside the other copy for now.

Suppose we get as input an element $z \in H$ that is either a in the image of P, that is $z = P(h)$, or the image of S, $z = S(h)$, for group element $h \in G_\lambda$. We left-multiply the quantum money state

by z. If it is in the image of P, then we get

$$\begin{aligned}
z \cdot |\$^{\lambda}_{i,j}\rangle &= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda\left(g^{-1}\right)_{i,j} \mid P(h)P(g) \rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda\left(g^{-1}\right)_{i,j} \mid P(hg) \rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda\left(g^{-1}h\right)_{i,j} \mid P(g) \rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G, k\in[d_\lambda]} \varrho_\lambda\left(g^{-1}\right)_{i,k} \varrho_\lambda\left(h\right)_{k,j} \mid P(g) \rangle \\
&= \sum_{k\in[d_\lambda]} \varrho_\lambda\left(h\right)_{k,j} \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda\left(g^{-1}\right)_{i,k} \mid P(g) \rangle \\
&= \sum_{k\in[d_\lambda]} \varrho_\lambda\left(h\right)_{k,j} |\$^{\lambda}_{i,k}\rangle
\end{aligned}$$

If it is in the image of S, then we similarly get

$$\begin{aligned}
z * |\$^{\lambda}_{i,j}\rangle &= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda\left(g^{-1}\right)_{i,j} \mid S(h) * P(g) \rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda\left(g^{-1}\right)_{i,j} \mid \tilde{S}(hg) \rangle \\
&= \sum_{k\in[d_\lambda]} \varrho_\lambda\left(h\right)_{k,j} \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda\left(g^{-1}\right)_{i,k} \mid \tilde{S}(g) \rangle
\end{aligned}$$

where $\tilde{S}$ is some function implied by S that is guaranteed by the statistical distance property of Definition 6.21 to have at least inverse polynomial support outside of the image of P.[46]

We finally perform a Fourier extraction and swap test with the copy that was set aside. If z was in the image of P, then the swap test will certainly pass. Otherwise, we observed that the two tested states will have orthogonal support that is at least inverse polynomial (since $\tilde{S}$ is far from P), and the swap test will fail with probability $1 - \frac{1}{\mathsf{poly}(n)}$. This therefore breaks the indistinguishability security of the dual-mode one-way homomorphism. □

6.5.3 Worst-case to Average-case Reduction for Cloning

Remarkably, the problem of cloning any specific (worst-case) money state in this construction can be reduced to that of producing two copies of an an average case money state, and therefore to cloning an average-case state. Moreover, all of these are equivalent to the problem of preparing the trivial irrep state (that is, the positive uniform superposition over the image of P).

[46] Note that this does not break inaccessibility security, since in this case we are given z which is itself already outside the image of P.

Theorem 6.27 (Worst-case to Average-case Cloning Reduction and Money/Lightning Equivalence)**.** *For the quantum money/lightning scheme defined in Section 6.5.1, the following are equivalent:*

1. *There exists an efficient worst-case cloner that clones all valid money states* $|\$^{\lambda}_{i,j}\rangle$.
2. *There exists an efficient average-case cloner that clones an average-case money state* $|\$^{\lambda}_{i,j}\rangle$*, where* λ *is sampled according the the Plancherel measure of the group.*
3. *There exists an efficient lightning adversary that produces two copies of the same money state* $|\$^{\lambda}_{i,j}\rangle$*, where* λ *is sampled according the the Plancherel measure of the group.*
4. *There exists an efficient preparation device that prepares the trivial irrep state* $|\$^{\mathrm{id}}\rangle$*, that is, the positive uniform superposition over image of the homomorphism* P*.*

In other words, all four tasks (worst-case cloning, average-case cloning, sampling state doublets, and trivial irrep state preparation) are computationally equivalent.

Proof. It can be seen directly that 1 $\Rightarrow$ 2 (since cloning in the worst case trivially implies doing so in the average case), and that 2 $\Rightarrow$ 3 (using the Mint function to mint a state and then using the cloner to clone it). So it remains to show that 3 $\Rightarrow$ 4 and that 4 $\Rightarrow$ 1. We start by showing that 4 $\Rightarrow$ 1, and then 3 $\Rightarrow$ 4 will follow from applying the same process in reverse on the doublet produced by the lightning adversary.

Suppose that we had a quantum money state with irrep label λ that we would like to clone:

$$|\$^{\lambda}_{i,j}\rangle = \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda \left(h^{-1}\right)_{i,j} \mid P(h) \rangle$$

We run the trivial irrep state preparation adversary to prepare the positive uniform superposition over the image of P:

$$|\$^{\mathrm{id}}\rangle = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \mid P(g) \rangle$$

We left multiply the first register (the money state) by the inverse of the second register (the trivial irrep state), producing

$$\begin{aligned}
|\$^{\lambda}_{i,j}\rangle \otimes |\$^{\mathrm{id}}\rangle &\to \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda \left(h^{-1}\right)_{i,j} \mid P(g^{-1}h) \rangle \otimes \frac{1}{\sqrt{|G|}} \sum_{g\in G} \mid P(g) \rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda \left(h^{-1}g^{-1}\right)_{i,j} \mid P(h) \rangle \otimes \frac{1}{\sqrt{|G|}} \sum_{g\in G} \mid P(g) \rangle \\
&= \sqrt{\frac{d_\lambda}{|G|}} \sum_{k\in[d_\lambda]} \sum_{h\in G} \varrho_\lambda \left(h^{-1}\right)_{i,k} \varrho_\lambda \left(g^{-1}\right)_{k,j} \mid P(h) \rangle \otimes \frac{1}{\sqrt{|G|}} \sum_{g\in G} \mid P(g) \rangle \\
&= \frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} \sqrt{\frac{d_\lambda}{|G|}} \sum_{h\in G} \varrho_\lambda \left(h^{-1}\right)_{i,k} \mid P(h) \rangle \otimes \sqrt{\frac{d_\lambda}{|G|}} \sum_{g\in G} \varrho_\lambda \left(g^{-1}\right)_{k,j} \mid P(g) \rangle \\
&= \frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |\$^{\lambda}_{i,k}\rangle \otimes |\$^{\lambda}_{k,j}\rangle \qquad (10)
\end{aligned}$$

We now have two states that are both valid quantum money states for irrep label λ.

Observation 6.28. *If we would like both registers to be exact copies of the original state in tensor product, we can do that as well.*

Proof of Observation 6.28. We apply a left Fourier measurement on the left register (that is, a Fourier measurement corresponding to left action by plaintext group elements) and a right Fourier measurement on the right register (corresponding to right action), to produce

$$\frac{1}{{d_\lambda}^{3/2}} \sum_{k,\ell,m\in[d_\lambda]} |\$^\lambda_{i,\ell}\rangle \otimes |L^\lambda_{\ell,k}\rangle \otimes |L^\lambda_{k,m}\rangle \otimes |\$^\lambda_{m,j}\rangle$$
$$\xrightarrow{\text{QFT}} \frac{1}{{d_\lambda}^{3/2}} \sum_{k,\ell,m\in[d_\lambda]} |\$^\lambda_{i,\ell}\rangle \otimes |\lambda,\ell,k\rangle \otimes |\lambda,k,m\rangle \otimes |\$^\lambda_{m,j}\rangle$$

Now note that the registers containing k are in the pure state $\frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |k\rangle\,|k\rangle$, in tensor product with the rest of the state. Replace these registers with the state $|j\rangle\,|i\rangle$ to get

$$\frac{1}{d_\lambda} \sum_{\ell,m\in[d_\lambda]} |\$^\lambda_{i,\ell}\rangle \otimes |\lambda,\ell,j\rangle \otimes |\lambda,i,m\rangle \otimes |\$^\lambda_{m,j}\rangle$$

Now uncompute the two Fourier extractions we have just performed to get $|\$^\lambda_{i,j}\rangle \otimes |\$^\lambda_{i,j}\rangle$ as desired. □

We now continue with the proof of Theorem 6.27 and show that 3 ⇒ 4. Given a doublet pair of quantum money states for the same irrep label, we show how to prepare the trivial irrep state $|\$^{\text{id}}\rangle = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \big|\ P(g)\ \big\rangle$. This doublet produced by the lightning adversary will be a state on two registers that passes verification, of the form[47]

$$\sum_{i,j,k,\ell\in[d_\lambda]} \alpha_{i,j,k,\ell}\ |\$^\lambda_{i,j}\rangle \otimes |\$^\lambda_{k,\ell}\rangle$$

As above, we can use Fourier extractions to convert this to the state $|\$^\lambda_{i,j}\rangle \otimes |\$^\lambda_{i,j}\rangle$ or even to the state $\frac{1}{\sqrt{d_\lambda}} \sum_{k\in[d_\lambda]} |\$^\lambda_{i,k}\rangle \otimes |\$^\lambda_{k,j}\rangle$. By reversing the process described above, from Equation (10) backwards, we then recover the state $|\$^\lambda_{i,j}\rangle \otimes |\$^{\text{id}}\rangle$, where the second register is the trivial irrep state, as desired. □

So cloning an average-case state is as hard as cloning a worst case state, both of which are as hard as preparing the positive uniform superposition over the image of the homomorphism (the trivial irrep state). Moreover, quantum money security and quantum lightning security are equivalent for this scheme.

Remark 6.29. *Note that a task that is absent from Theorem 6.27 is the ability to prepare any quantum money state given its irrep label (ie. its serial number). An adversary for this task would clearly imply one for all four of the tasks mentioned in Theorem 6.27, but it is not clear if the opposite is true. That is, an adversary that breaks the quantum money/lightning scheme nevertheless might not be able to prepare specific money states on command (only at random). In section Section 7, we take advantage of precisely this gap to propose a new quantum cryptographic primitive: quantum* fire.

[47] This is assuming the inaccessibility security of the dual-mode one-way homomorphism, which is what prevents the state from having non-negligible support outside the image of P.

7 Quantum Fire: Quantum States that are Clonable but Untelegraphable

In this section, we introduce a new quantum cryptographic primitive, "quantum fire", a cryptographic version of the clonable-but-untelegraphable states introduced by [NZ24]. Much like fire is an entropic state of matter that is hard to spark on command, but easy to spread around as long as it is kept alive, *quantum fire* is a quantum state that is hard to prepare but easy to clone as long as it is maintained in coherent quantum form. More specifically, a *quantum fire state*, $|\phi_i\rangle$, comes from a collection $\{|\phi_i\rangle\}_i$ of states that

- **Efficiently sparked:** there is an efficient sparking algorithm that outputs a random $|\phi_i\rangle$, from some distribution over i,
- **Efficiently clonable:** there is an efficient cloner that maps one copy of $|\phi_i\rangle$ to two copies,
- **Un-telegraphable**: no efficient adversary can encode $|\phi_i\rangle$ into a classical string that can later be revived back into $|\phi_i\rangle$.

We also allow an efficiently verifiable version, in which we have the additional property,

- **Verifiable:** there is a verification algorithm that takes a label i as well as a claimed state $|\phi_i'\rangle$, and outputs whether $|\phi_i'\rangle$ is a valid quantum fire state.[48]

Quantum fire has been demonstrated to exist relative to a quantum oracle in [NZ24]. However, until now, no plausible construction in the plain model was known. Even the task of finding quantum states that are efficiently clonable without an oracle—but not trivial enough to be described classically—has been a challenge. We give the first candidate construction of quantum fire in the plain model. We challenge the cryptographic community to find either a proof of its security from reasonable assumptions or to break it. We further challenge the community to find and propose other reasonable candidate constructions for quantum fire. Much like the 15-year challenge of finding reasonable constructions of public-key quantum money has led to a variety of new techniques for proving unclonability, we expect the task of finding candidate quantum fire constructions to prove to be a challenging task and to require new and specialized techniques for showing untelegraphability.

7.1 Definition

Quantum fire was implicit in the oracle construction of [NZ24], but no formal definition was given. We give a definition of public-key quantum fire here.

Definition 7.1 (Public-key Quantum Fire)**.** *A* public-key quantum fire *scheme consists of four quantum algorithms* $\mathcal{S} = (\mathsf{KeyGen}, \mathsf{Spark}, \mathsf{Clone}, \mathsf{Ver})$ *where*

- $\mathsf{KeyGen}(1^n)$ *takes as input the security parameter* 1^n *and outputs a private/public key pair* $(\mathsf{sk}, \mathsf{pk})$*,*
- $\mathsf{Spark}(\mathsf{pk})$ *takes the public key and outputs a serial number* s *and a quantum fire state* $|\phi^s\rangle$*, which we refer to as a* flame*,*

[48] In the general case, the verification algorithm for the quantum fire state may allow a larger space of states than those that would be produced by the sparking algorithm. In this case the cloning algorithm and the telegraphing adversary must output any state(s) that pass verification.

- $\mathsf{Clone}(\mathsf{pk}, s, |\phi^s\rangle)$ *takes as input the public key* pk*, a serial number* s*, and a flame* $|\phi^s\rangle$*, and outputs two registers* AB *in some potentially entangled state* σ^s_{AB}*,*
- $\mathsf{Ver}(\mathsf{pk}, s, \sigma)$ *takes as input the public key* pk*, a serial number* s*, and an alleged flame* σ*, and either accepts or rejects.*[49]

A quantum fire scheme $\mathcal{S}$ *satisfies correctness if for all* λ*, sparking is correct*

$$\Pr\left[\mathsf{Ver}(\mathsf{pk}, s, |\phi^s\rangle) \text{ accepts} \;\middle|\; \begin{array}{c}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\ (s, |\phi^s\rangle) \leftarrow \mathsf{Spark}(\mathsf{pk})\end{array}\right] \geq 1 - \mathsf{negl}(n)\,,$$

and cloning is correct[50]

$$\Pr\left[\mathsf{Ver}(\mathsf{pk}, s, \cdot) \text{ accepts both registers of } \sigma^s_{\mathsf{AB}} \;\middle|\; \begin{array}{c}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\ (s, |\phi^s\rangle) \leftarrow \mathsf{Spark}(\mathsf{pk})\\ \sigma^s_{\mathsf{AB}} \leftarrow \mathsf{Clone}(\mathsf{pk}, s, |\phi^s\rangle)\end{array}\right] \geq 1 - \mathsf{negl}(n)\,.$$

Untelegraphability [NZ24] of quantum fire means that it is hard to encode a flame as a classical encoding which can later be brought back. That is, once the flame is extinguished, it is gone. We model this as a pair of adversaries. The first is tasked with deconstructing the flame into a classical message, and the second must use the deconsructed classical message to reconstruct the state.[51]

Algorithm 6 (**Quantum Fire Telegraphing Security Game**)**.**

1. Challenger generates $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$, $(s, |\phi^s\rangle) \leftarrow \mathsf{Spark}(\mathsf{sk})$ and send $(\mathsf{pk}, s, |\phi^s\rangle)$ to adversary A.
2. Adversary A returns a classical encoding of the flame $c \in \{0,1\}^*$.
3. Challenger passes $c \in \{0,1\}^*$ to adversary B.
4. Adversary B returns a claimed quantum state σ.
5. Challenger runs $\mathsf{Ver}(\mathsf{pk}, s, \sigma)$ and outputs the result.[52]

Definition 7.2 (Quantum fire security)**.** *A quantum fire scheme* $\mathcal{S}$ *satisfies* ϵ-quantum-fire security *if for all pairs of efficient adversaries* A *and* B*, the success probability of* A *in the Telegraphing Security Game (Algorithm 6) is at most* $\epsilon(n)$*.*

[49] Ver may not exist for unverifiable quantum fire, or it may require the secret key sk for secretly verifiable quantum fire.

[50] Technically, we need that cloning is correct even for the outputs of the cloner itself. That is, we should be able to apply the cloner repeatedly on its own outputs any polynomial number of times. This rules out trivial cases such as where the sparking mints two quantum money states, and verification accepts either one or both of them, but they are otherwise unclonable. This would allow "cloning" once by dividing up the two money states, but those two "copies" cannot be cloned further. Quantum fire definitionally requires its flame states to be unboundedly clonable.

[51] Note that the two adversaries should *not* be entangled, as this allows them to *teleport* the state. Furthermore, maintaining any entanglement implies having to store a quantum register, which is what telegraphing aims to avoid.

[52] In the case of unverifiable quantum fire, the challenger verifies the telegraphing by measuring in a basis containing the valid flame $|\phi^s\rangle$.

We require that Spark and Clone are efficient (QPT) algorithms. Ver may be an efficient public verification, an efficient private verification, or an inefficient verification, leading to three different kinds of quantum fire (publicly verifiable quantum fire, privately verifiable quantum fire, and statistically verifiable quantum fire). Furthermore, the weaker notion of security is against standard non-interactive telegraphing. A stronger security notion, and one that is more amenable to cryptographic applications, additionally rules out interactive telegraphing, where A and B may exchange any number of classical messages in Algorithm 6.

7.2 Construction

Let G and H be two groups, and let $f : G \to H$ be an injective homomorphism between them, which we assume to be one-way. Let H_f be the image of f. Let $\mathcal{R} : G \to U(\mathcal{H})$ be the representation of G which acts as $\mathcal{R}(g)\,|h\rangle = |f(g) \cdot h\rangle$. Let the set of quantum fire labels (or serial numbers) be $\widehat{G}$, the set of irreps of G, and for each $\lambda \in \widehat{G}$, we let valid flames be any state in isotypic component of irrep λ, that is, any state of the form

$$|\phi^{\lambda}_{i,j}\rangle = \sum_{g \in G} \varrho_{\lambda}(g^{-1})_{i,j}\,|f(g)\rangle$$

We further assume that there is an efficient algorithm to prepare a uniform superposition over the image group H_f: $|\Phi\rangle = \sum_{h \in H_f} |h\rangle$, or a quantum state that approximates it.[53]

Verification and Sparking. Verification is the same as verification for the quantum money construction of Section 6.1: we perform a course Fourier measurement to produce the irrep label λ and compare with the claimed quantum fire label. Likewise, to spark a quantum fire state—that is, to prepare a fire state with a random label—run the same verification process on the identity element of H, which samples the irrep label λ according to the Plancherel measure of G.

Cloning. We are given a quantum fire state $|\phi^{\lambda}_{i,j}\rangle$ with label λ, and we would like to output two such fire states, both of which pass verification for the same label λ.

We first prepare $|\Phi\rangle = \sum_{h \in H_f} |h\rangle$, a uniform superposition over the image group H_f. Together with the fire state, we now have the overall state

$$|\phi^{\lambda}_{i,j}\rangle \otimes |\Phi\rangle = \sum_{\substack{g \in G \\ h \in H_f}} \varrho_{\lambda}(g^{-1})_{i,j}\,|f(g)\rangle\,|h\rangle\ .$$

Since f is injective, and therefore bijective between G and H_f, we can reindex the sum over h as

$$= \sum_{g,h \in G} \varrho_{\lambda}(g^{-1})_{i,j}\,|f(g)\rangle\,|f(h)\rangle$$

Both registers contain an element of H. We apply the inverse group operation of the second

[53] Supposedly, this image group is known to all parties, while the specific mapping between G and H_f could be arbitrary.

register into the first register on the left to get

$$\begin{aligned}
&\to \sum_{g,h\in G} \varrho_\lambda(g^{-1})_{i,j} \left|f(h)^{-1}\cdot f(g)\right\rangle \left|f(h)\right\rangle \\
&= \sum_{g,h\in G} \varrho_\lambda(g^{-1})_{i,j} \left|f(h^{-1}\cdot g)\right\rangle \left|f(h)\right\rangle \\
&= \sum_{g,h\in G} \varrho_\lambda(g^{-1}\cdot h^{-1})_{i,j} \left|f(g)\right\rangle \left|f(h)\right\rangle \\
&= \sum_{\substack{g,h\in G\\ k\in[d_\lambda}} \varrho_\lambda(g^{-1})_{ik}\varrho_\lambda(h^{-1})_{k,j} \left|f(g)\right\rangle \left|f(h)\right\rangle \\
&= \sum_{k\in[d_\lambda]} \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,k} \left|f(g)\right\rangle \sum_{h\in G} \varrho_\lambda(h^{-1})_{k,j} \left|f(h)\right\rangle \\
&= \sum_{k\in[d_\lambda]} \left|\phi^\lambda_{i,k}\right\rangle \otimes \left|\phi^\lambda_{k,j}\right\rangle
\end{aligned}$$

This produces two quantum fire states that both pass verification for the same original label λ. While not necessary, if we wish, we could even force the two new fire states to have the same i and j values as the original, and in doing so disentangle them. We simply perform a Fourier extraction on both states from both the left and right side to extract out the new i and j values, replace them with the old i and j, and uncompute[54] to get the tensor product:

$$\left|\phi^\lambda_{i,j}\right\rangle \otimes \left|\phi^\lambda_{i,j}\right\rangle$$

Untelegraphability. We have shown above that these states are efficiently clonable. In order for the construction to be a secure quantum fire scheme, the states must also be *untelegraphable*. That is, there must be no way to deconstruct the states into a classical message that can later be reconstructed back into the quantum state, or at least one that properly passes verification. We leave as an open problem to find sufficient conditions on the one-way homomorphism that would allow showing untelegraphability in the plain model.

Remark 7.3. *The untelegraphability of such a scheme is known to be difficult to prove even relative to a classical oracle: Nehoran and Zhandry [NZ24] show the security of their implicit quantum fire scheme relative to a unitary quantum oracle. Unfortunately, they also show that the same quantum fire construction leads to a unitary oracle separation between the complexity classes* clonableQMA *and* QCMA*, and therefore between* QMA *and* QCMA*. As generalization of this, they observe that any provably secure and public-key quantum fire scheme relative to a* classical *oracle will likely lead to a* classical *oracle separation between* QMA *and* QCMA*, an major longstanding open problem of Aharonov and Naveh [AN02] that remains unresolved despite recent progress.*

Observation 7.4. *We observe that while one-wayness may not be a sufficient condition for untelegraphability, is a* necessary *condition. This is because if we can invert the homomorphism—and we can also perform a quantum Fourier transform on the group—then we can telegraph the state as the classical description of λ, i, and j.*

[54] See Observation 6.28 for more details on how to do this.

Proof sketch. Suppose, for instance, that we can invert f perfectly. Then we can do the following. Alice starts with a quantum fire state $|\phi^{\lambda}_{i,j}\rangle = \sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j} |f(g)\rangle$ and inverts f to get

$$\sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j} |f(g)\rangle |g\rangle \ .$$

She now uncomputes $f(g)$ in the first register to get

$$\sum_{g\in G} \varrho_\lambda(g^{-1})_{i,j} |g\rangle \ ,$$

which is the left-regular Fourier basis state $|\mathcal{L}^{\lambda}_{i,j}\rangle$. Taking the quantum Fourier transform of this state then yields $|\lambda\rangle |i\rangle |j\rangle$, which is a classical string that Alice can send to Bob. Bob can then invert this process to recover $|\phi^{\lambda}_{i,j}\rangle$. □

The notion of quantum fire was featured implicitly in the work of Nehoran and Zhandry [NZ24], where they show that such an object exists relative to a unitary quantum oracle. Their construction uses two oracles: a (quantumly accessible) random oracle, which serves effectively as a verification oracle, and a unitary oracle, which is used for cloning the resulting states. Unfortunately, the scheme of [NZ24] offers little hope of leading to a plain-model instantiation. This is because, as they note, the unitary implemented by the unitary cloning oracle is one that cannot be implemented efficiently.

One approach to strengthen their result is to give a construction from classical functionality. A priori, however, it is not even clear that *any* classical functionality can bestow clonability on a state that cannot be encoded classically. To the best of our knowledge, every known method of efficiently cloning quantum states first passes through the classical description of the states, copies this classical description, and then recovers two clones of the quantum state from the classical descriptions. However, this automatically means that such states are efficiently telegraphable—they can be stored as their classical descriptions. *How can we clone a quantum state (using efficient classical functionality) without ever going through a classical description?*

We answer this question here by giving a proof of concept that this kind of cloning is in fact possible, along with a framework for using it to construct quantum fire with conjectured security. An interesting aspect of our cloning procedure is that the quantum states of the two registers inherently become entangled during the course of the procedure, and only become disentangled at the end. Furthermore, it requires applying a controlled group operation between the two registers. These aspects together give intuitive justification for the untelegraphability of this cloning procedure: controlled operations and more general entangling procedures *cannot* occur over a classical channel.

Acknowledgments

The authors thank Henry Yuen, Chinmay Nirkhe, Adam Bouland, and Tudor Giurgica-Tiron for insightful discussions that contributed to the direction of the paper, and we thank Takashi Yamakawa, Tomoyuki Morimae, and Dakshita Khurana for enlightening discussions on the significance of our results and further cryptographic applications of our duality theorem. J.B. is supported by Henry Yuen's AFORS (award FA9550-21-1-036) and NSF CAREER (award CCF2144219). This work was done in part while J.B. and B.N. were visiting the Simons Institute for the Theory of Computing, supported by NSF QLCI Grant No. 2016245.

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Proceedings of the 2009 24th Annual IEEE Conference on Computational Complexity*, CCC '09, pages 229–242, Washington, DC, USA, 2009. IEEE Computer Society.

[AAS20] Scott Aaronson, Yosi Atia, and Leonard Susskind. On the hardness of detecting macroscopic superpositions, 2020.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '12, page 41–60, New York, NY, USA, 2012. Association for Computing Machinery.

[AGKZ20] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *52nd ACM STOC*, pages 255–268. ACM Press, June 2020.

[ALL+21] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 526–555. Springer, 2021.

[AN02] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey, 2002.

[Bab16] László Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, page 684–697, New York, NY, USA, 2016. Association for Computing Machinery.

[BBBW82] Charles H Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in cryptology: Proceedings of Crypto 82*, pages 267–275. Springer, 1982.

[BBV24] James Bartusek, Zvika Brakerski, and Vinod Vaikuntanathan. Quantum state obfuscation from classical oracles. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1009–1017, 2024.

[BCG+24] Sergey Bravyi, Anirban Chowdhury, David Gosset, Vojtěch Havlíček, and Guanyu Zhu. Quantum complexity of the kronecker coefficients. *PRX Quantum*, 5(1):010329, 2024.

[BCH05] Dave Bacon, Isaac L Chuang, and Aram W Harrow. The quantum schur transform: I. efficient qudit circuits. *arXiv preprint quant-ph/0601001*, 2005.

[BDS23] Shalev Ben-David and Or Sattath. Quantum Tokens for Digital Signatures. *Quantum*, 7:901, January 2023.

[Bea97] Robert Beals. Quantum computation of Fourier transforms over symmetric groups. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 48–53, 1997.

[BKNY23] James Bartusek, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Obfuscation of pseudo-deterministic quantum circuits. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1567–1578, 2023.

[CG24] Andrea Coladangelo and Sam Gunn. How to use quantum indistinguishability obfuscation. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1003–1008, 2024.

[Chi17] Andrew M Childs. Lecture notes on quantum algorithms. *Lecture notes at University of Maryland*, 5, 2017.

[CHW07] Andrew M Childs, Aram W Harrow, and Paweł Wocjan. Weak fourier-schur sampling, the hidden subgroup problem, and the quantum collision problem. In *STACS 2007: 24th Annual Symposium on Theoretical Aspects of Computer Science, Aachen, Germany, February 22-24, 2007. Proceedings 24*, pages 598–609. Springer, 2007.

[CLL24] Sitan Chen, Jerry Li, and Allen Liu. An optimal tradeoff between entanglement and copy complexity for state tomography. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1331–1342, 2024.

[CMP24] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. *Quantum*, 8:1330, 2024.

[Cop94] D. Coppersmith. An approximate Fourier transform useful in quantum factoring, 1994.

[CPDDF+19] Marta Conde Pena, Raul Durán Díaz, Jean-Charles Faugère, Luis Hernández Encinas, and Ludovic Perret. Non-quantum cryptanalysis of the noisy version of aaronson–christiano's quantum money scheme. *IET Information Security*, 13(4):362–366, 2019.

[FGH+12] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor. Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, page 276–289, New York, NY, USA, 2012. Association for Computing Machinery.

[GH16] W. T. Gowers and O. Hatami. Inverse and stability theorems for approximate representations of finite groups, 2016.

[Gop70] Valerii Denisovich Goppa. A new class of linear correcting codes. *Problemy Peredachi Informatsii*, 6(3):24–30, 1970.

[Har05] Aram W Harrow. Applications of coherent classical communication and the schur transform to quantum information theory. *arXiv preprint quant-ph/0512255*, 2005.

[HHJ+16] Jeongwan Haah, Aram W. Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, page 913–925, New York, NY, USA, 2016. Association for Computing Machinery.

[HKNY24] Taiga Hiroka, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Robust combiners and universal constructions for quantum cryptography. In *TCC*, 2024.

[HMY23] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 639–667. Springer, 2023.

[Høy97] Peter Høyer. Efficient quantum transforms, 1997.

[Iss05] S Issai. Neue begründung der theorie der gruppencharaktere, 1905.

[Jor08] Stephen P Jordan. Fast quantum algorithms for approximating some irreducible representations of groups. *arXiv preprint arXiv:0811.0562*, 2008.

[Key06] Michael Keyl. Quantum state estimation and large deviations. *Reviews in Mathematical Physics*, 18(01):19–60, 2006.

[KK82] David Kazhdan and David Kazhdan. On ε-representations. *Israel Journal of Mathematics*, 43:315–323, 1982.

[KLS22] Andrey Boris Khesin, Jonathan Z. Lu, and Peter W. Shor. Publicly verifiable quantum money from random lattices, 2022.

[KMNY24] Fuyuki Kitagawa, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum public-key encryption with tamper-resilient public keys from one-way functions. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 93–125, Cham, 2024. Springer Nature Switzerland.

[Kro19] Hari Krovi. An efficient high dimensional quantum Schur transform. *Quantum*, 3:122, February 2019.

[KSS22] Daniel M. Kane, Shahed Sharif, and Alice Silverberg. Quantum money from quaternion algebras. *Mathematical Cryptology*, 2(1):60–83, Oct. 2022.

[LAF+09] Andrew Lutomirski, Scott Aaronson, Edward Farhi, David Gosset, Avinatan Hassidim, Jonathan Kelner, and Peter Shor. Breaking and making quantum money: toward a new quantum cryptographic protocol, 2009.

[LH24] Martin Larocca and Vojtech Havlicek. Quantum algorithms for representation-theoretic multiplicities. *arXiv preprint arXiv:2407.17649*, 2024.

[LM17] Nati Linial and Jonathan Mosheiff. On the rigidity of sparse random graphs. *Journal of Graph Theory*, 85(2):466–480, 2017.

[LMZ23] Jiahui Liu, Hart Montgomery, and Mark Zhandry. Another round of breaking and making quantum money: How to not build it from lattices, and more. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*, pages 611–638. Springer, Heidelberg, April 2023.

[McE78] Robert J McEliece. A public-key cryptosystem based on algebraic coding theory. *Coding Thv*, 4244:114–116, 1978.

[MRR06] Cristopher Moore, Daniel Rockmore, and Alexander Russell. Generic quantum Fourier transforms. *ACM Transactions on Algorithms (TALG)*, 2(4):707–723, 2006.

[MW24] Giulio Malavolta and Michael Walter. Robust quantum public-key encryption with applications to quantum key distribution. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 126–151, Cham, 2024. Springer Nature Switzerland.

[MYY25] Tomoyuki Morimae, Shogo Yamada, and Takashi Yamakawa. Quantum unpredictability. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–32. Springer, 2025.

[MZ22] Hart Montgomery and Mark Zhandry. Full quantum equivalence of group action dlog and cdh, and more. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–32. Springer, 2022.

[NZ24] Barak Nehoran and Mark Zhandry. A Computational Separation Between Quantum No-Cloning and No-Telegraphing. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 82:1–82:23, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[OW16] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, page 899–912, New York, NY, USA, 2016. Association for Computing Machinery.

[OW17] Ryan O'Donnell and John Wright. Efficient quantum tomography ii. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, page 962–974, New York, NY, USA, 2017. Association for Computing Machinery.

[Rob21] Bhaskar Roberts. Security analysis of quantum lightning. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 562–567, Cham, 2021. Springer International Publishing.

[S+77] Jean-Pierre Serre et al. *Linear representations of finite groups*, volume 42. Springer, 1977.

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Sim97] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.

[Sin19] Harshdeep Singh. Code based cryptography: Classic McEliece. *arXiv preprint arXiv:1907.12754*, 2019.

[Ste09] Benjamin Steinberg. Representation theory of finite groups. *Carleton University*, 341, 2009.

[VK85] Anatoly M Vershik and Sergei V Kerov. Asymptotic of the largest and the typical dimensions of irreducible representations of a symmetric group. *Functional analysis and its applications*, 19(1):21–31, 1985.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[Yan22] Jun Yan. General properties of quantum bit commitments. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 628–657, Cham, 2022. Springer Nature Switzerland.

[YCH16] Yuxiang Yang, Giulio Chiribella, and Masahito Hayashi. Optimal compression for identically prepared qubit states. *Phys. Rev. Lett.*, 117:090502, Aug 2016.

[Zha21] Mark Zhandry. Quantum lightning never strikes the same state twice. or: quantum money from cryptographic assumptions. *Journal of Cryptology*, 34:1–56, 2021.

[Zha24] Mark Zhandry. Quantum Money from Abelian Group Actions. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 101:1–101:23, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.