A General Quantum Duality for Representations of Groups

and Applications to Quantum Money, Lightning, and Fire

John Bostanci

Based on joint work with Barak Nehoran and Mark Zhandry

Discovery Fiction: Quantum Lightning from Abelian Group Actions

- Zhandry'23 described an elegant and simple way to construct quantum money from Abelian group actions.

Discovery Fiction: Quantum Lightning from Abelian Group Actions

- Zhandry'23 described an elegant and simple way to construct quantum money from <u>Abelian</u> group actions.
- However, restricting to Abelian groups meant that the security proof required a black-box assumption, and complicated the scheme.

Discovery Fiction: Quantum Lightning from Abelian Group Actions

- Zhandry'23 described an elegant and simple way to construct quantum money from <u>Abelian</u> group actions.
- However, restricting to Abelian groups meant that the security proof required a black-box assumption, and complicated the scheme.

- We hoped that generalizing the construction to non-Abelian groups might fix these problems, but it's not that easy.

Discovery Fiction: Quantum Lightning from Abelian Group Actions

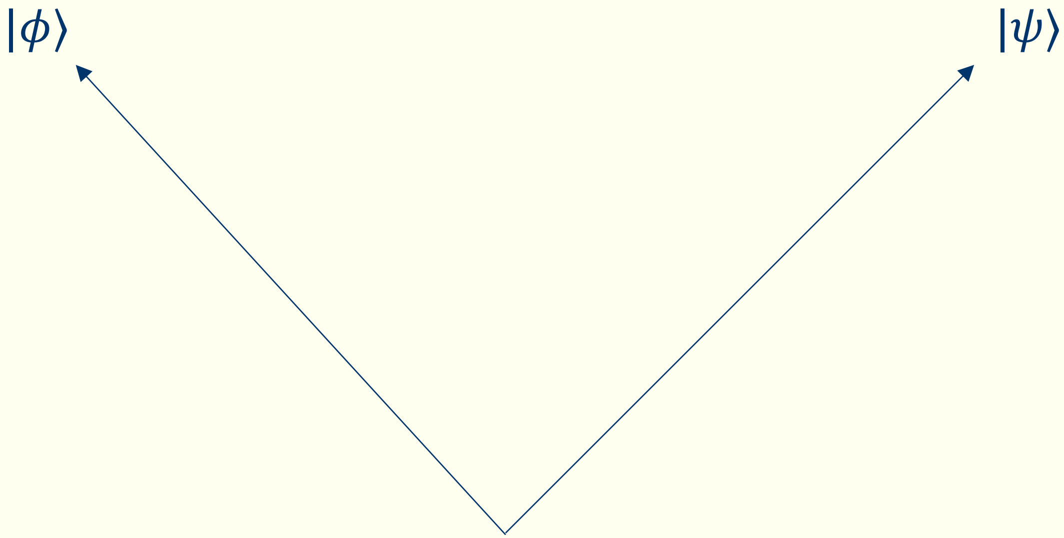
- Zhandry'23 described an elegant and simple way to construct quantum money from <u>Abelian</u> group actions.
- However, restricting to Abelian groups meant that the security proof required a black-box assumption, and complicated the scheme.

- We hoped that generalizing the construction to non-Abelian groups might fix these problems, but it's not that easy.
- Along the way, identified an interesting algorithmic task concerning representations of groups.

The General Quantum Duality Theorem for Representations of Groups

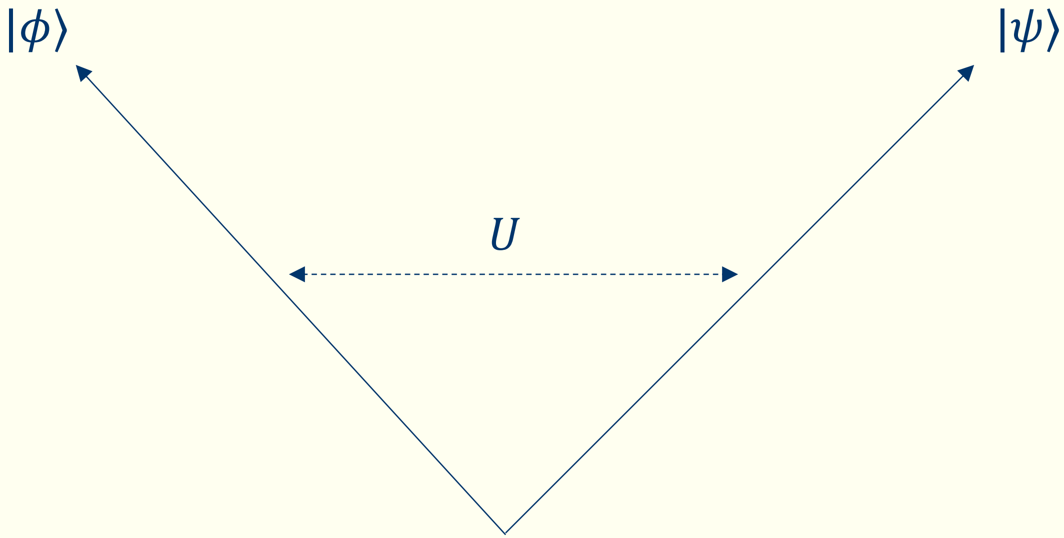
Swapping-distinguishing duality

Imagine we have two orthogonal states, $|\psi\rangle$ and $|\phi\rangle$.



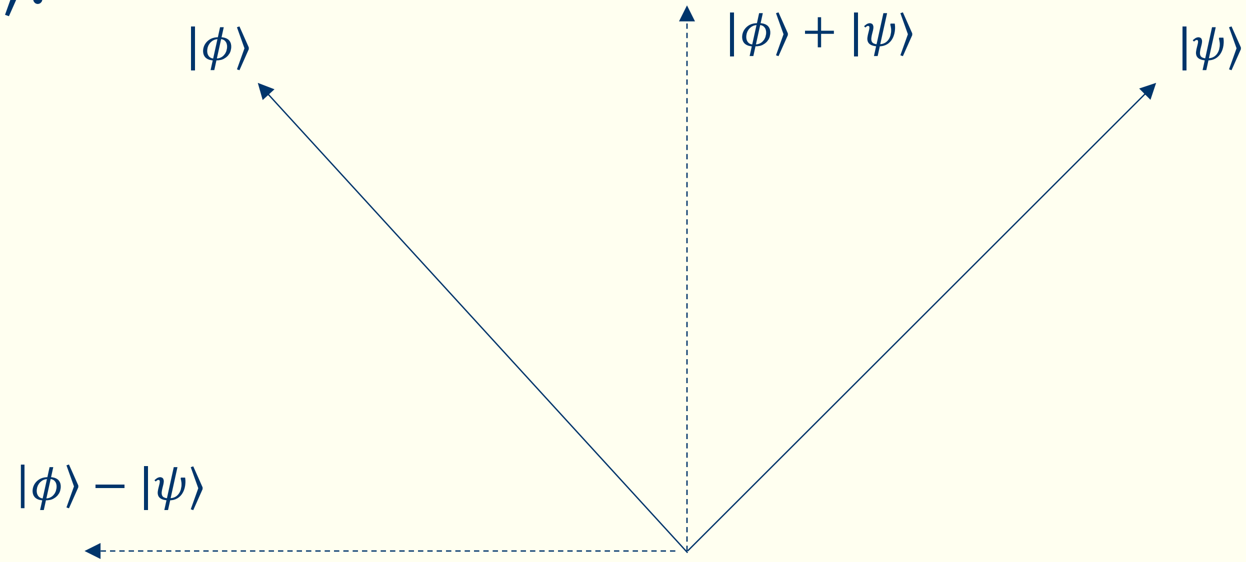
Swapping-distinguishing duality

How hard is it to (approximately) swap $|\psi\rangle \leftrightarrow |\phi\rangle$?



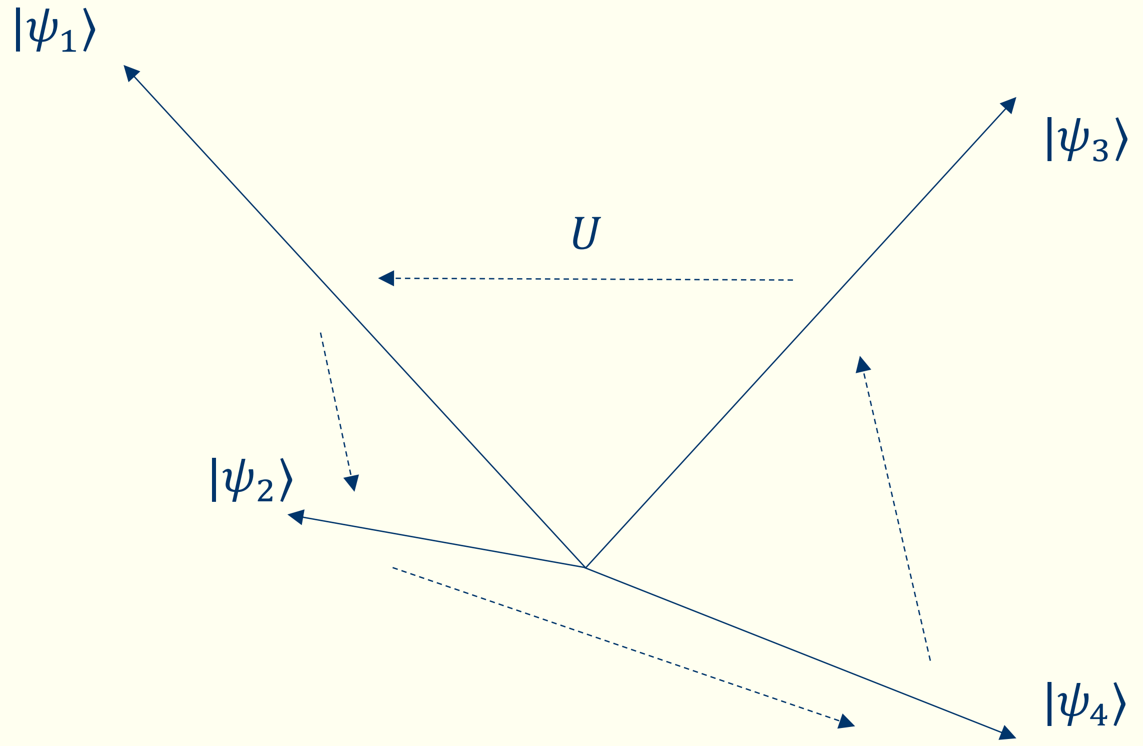
Swapping-distinguishing duality

Theorem [AAS'20]: You can efficiently implement swap between $|\phi\rangle$ and $|\psi\rangle$ if and only if you can efficiently distinguish between $|\phi\rangle + |\psi\rangle$ and $|\phi\rangle - |\psi\rangle$.



Generalized duality

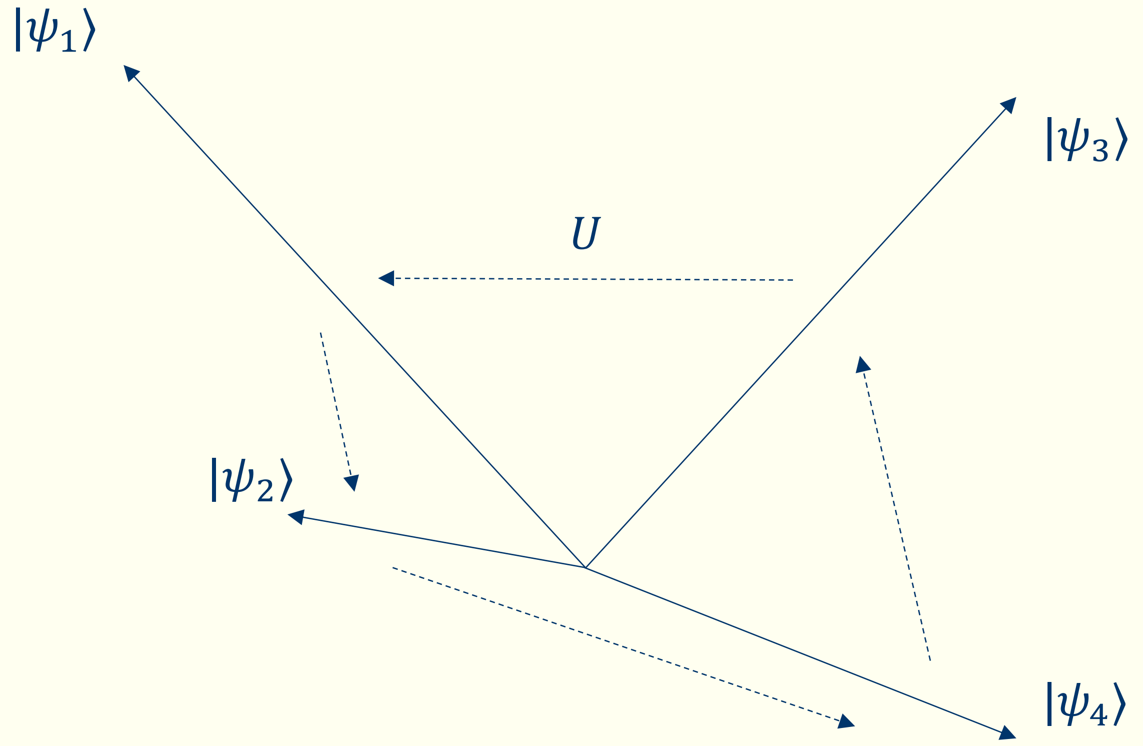
Now say that I have many states $\{|\psi_x\rangle\}$ and a collection of mappings between then, $\{U_g\}$. Is there some measurement that characterizes the complexity of implementing all of those mappings?



Generalized duality

Now say that I have many states $\{|\psi_x\rangle\}$ and a collection of mappings between then, $\{U_g\}$. Is there some measurement task that characterizes the complexity of implementing all of those mappings?

Representation of a group



Representations of groups

A representation of a group is mapping from a group G to unitary matrices on some vector space V.

$$\mathcal{R} : G \mapsto U(V)$$

Representations of groups

A representation of a group is mapping from a group G to unitary matrices on some vector space V.

$$\mathcal{R} : G \mapsto U(V)$$

What makes it a representation is that it also respects the group action:

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

Irreducible representations

For every group G, there is a dual group $\hat{G}$, and a collection of representations of G,

$$\{\rho^{\lambda}(g) : \lambda \in \hat{G}\}$$

Which we call the irreducible representations of G.

Irreducible representations

Important fact about irreps: For every representation $\mathcal{R}$ on vector space V, there is a decomposition of V into a direct sum of subspaces

$$V = \bigoplus_{\lambda,i} W_{\lambda,i}$$

Such that for every group element,

$$\mathcal{R}(g) \simeq \bigoplus_{\lambda,i} \varrho^{\lambda}(g)$$

Irreducible representations

Recall that if all of these unitaries commuted, we could simultaneously diagonalize all of them.

$$\mathcal{R}(g) = V^{\dagger}\left(\sum_{\lambda} \alpha_{\lambda}(g)|\psi_{\lambda}\rangle\langle\psi_{\lambda}|\right)V$$

Irreducible representations

Recall that if all of these unitaries commuted, we could simultaneously diagonalize all of them.

$$\mathcal{R}(g) = V^\dagger \left(\sum_\lambda \alpha_\lambda(g) |\psi_\lambda\rangle\langle\psi_\lambda| \right) V$$

For general groups, we can only block diagonalize them!

$$\mathcal{R}(\mathrm{g}) = V^\dagger \left(\bigoplus_\lambda \varrho^\lambda(g) \right) V$$

Irreducible representations

Recall that if all of these unitaries commuted, we could simultaneously diagonalize all of them.

$$\mathcal{R}(g) = V^{\dagger}\left(\sum_{\lambda} \alpha_{\lambda}(g)|\psi_{\lambda}\rangle\langle\psi_{\lambda}|\right)V$$

For general groups, we can only block diagonalize them!

$$\mathcal{R}(\mathrm{g}) = V^{\dagger}\left(\bigoplus_{\lambda} \underbrace{\varrho^{\lambda}(g)}\right)V$$

These are the irreducible representations
(you can't break them down anymore)

Irreducible representations

Recall that if all of these unitaries commuted, we could simultaneously diagonalize all of them.

$$\mathcal{R}(g) = V^\dagger \left(\sum_\lambda \alpha_\lambda(g) |\psi_\lambda\rangle\langle\psi_\lambda| \right) V$$

For general groups, we can only block diagonalize them!

$$\mathcal{R}(\mathrm{g}) = V^\dagger \left(\bigoplus_\lambda \underbrace{\varrho^\lambda(g)}_{\text{These are the irreducible representations (you can't break them down anymore)}} \right) V$$

We call V the quantum Fourier transform

These are the irreducible representations
(you can't break them down anymore)

Fourier extraction

If we write basis for each $W_{\lambda,i}$ as follows:

$$W_{\lambda,i} = \operatorname{span}\{|\psi^{\lambda}_{i,j}\rangle\}.$$

Then doing a full measurement in the Fourier basis is like mapping:

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

Fourier extraction

If we write basis for each $W_{\lambda,i}$ as follows:

$$W_{\lambda,i} = \operatorname{span}\{|\psi^{\lambda}_{i,j}\rangle\}.$$

Then doing a full measurement in the Fourier basis is like mapping:

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

The representation behaves identically on different copies of $W_{\lambda,i}$, making it difficult to figure out i in a black-box way.

Fourier extraction

Equivalent of a "coherent" measurement in the Fourier basis, up to the decomposition of different copies of the same W_λ.

$$\sum_j \alpha_j |\psi^\lambda_{i,j}\rangle \mapsto |\phi^\lambda_i\rangle|\lambda\rangle \otimes \sum_j \alpha_j |j\rangle$$

Fourier extraction

Equivalent of a “coherent” measurement in the Fourier basis, up to the decomposition of different copies of the same W_λ.

$$\sum_j \alpha_j |\psi^\lambda_{i,j}\rangle \mapsto |\phi^\lambda_i\rangle |\lambda\rangle \otimes \sum_j \alpha_j |j\rangle$$

Information about j has been “extracted” leaving behind a state that only depends on λ, i.

Fourier extraction

Equivalent of a "coherent" measurement in the Fourier basis, up to the decomposition of different copies of the same W_λ.

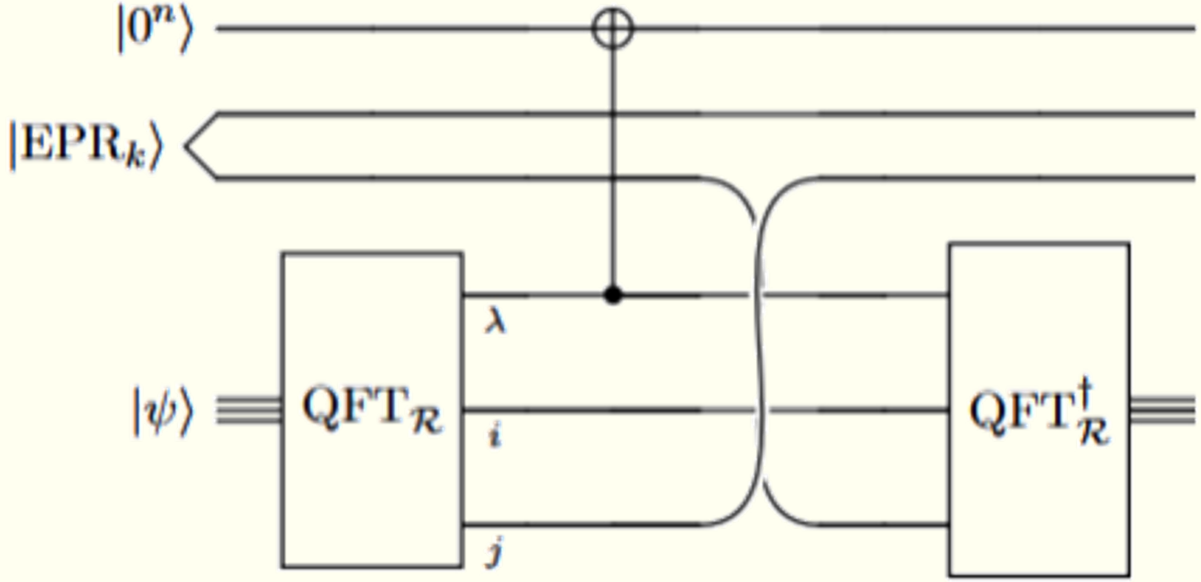
$$\sum_j \alpha_j |\psi^\lambda_{i,j}\rangle \mapsto |\phi^\lambda_i\rangle|\lambda\rangle \otimes \sum_j \alpha_j |j\rangle$$

Think of this as a hidden basis state that encodes information about i.

Information about j has been "extracted" leaving behind a state that only depends on λ, i.

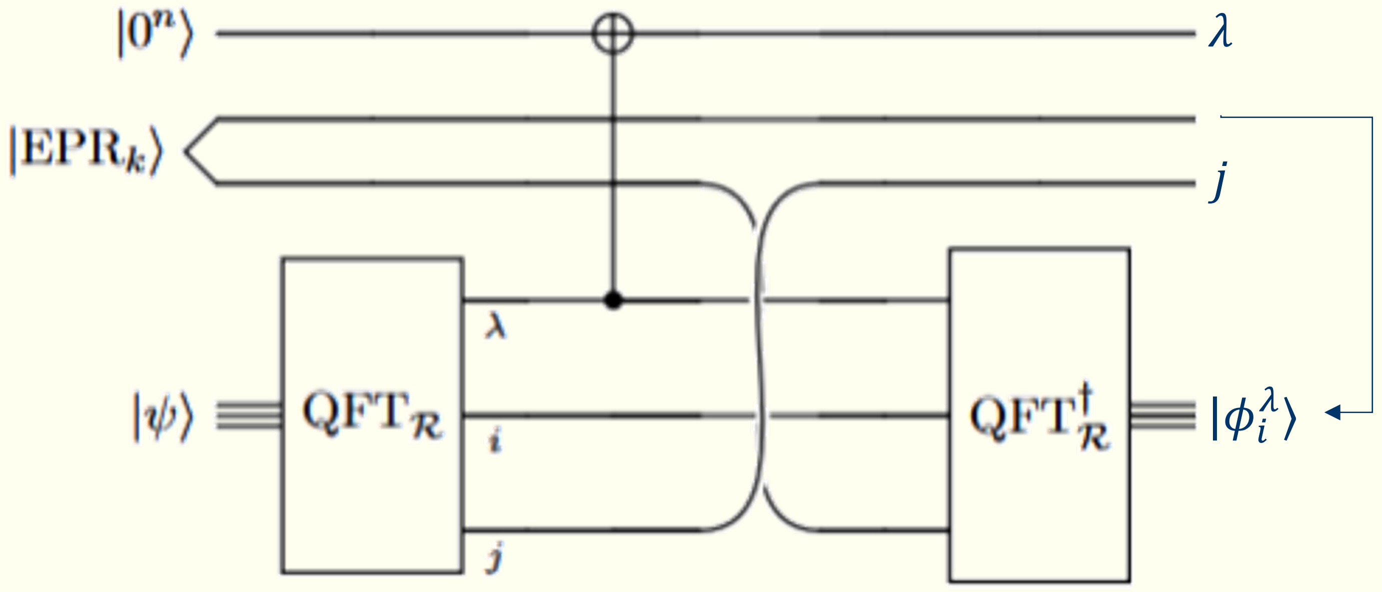
Fourier extraction

Here is what "ideal" Fourier extraction looks like:



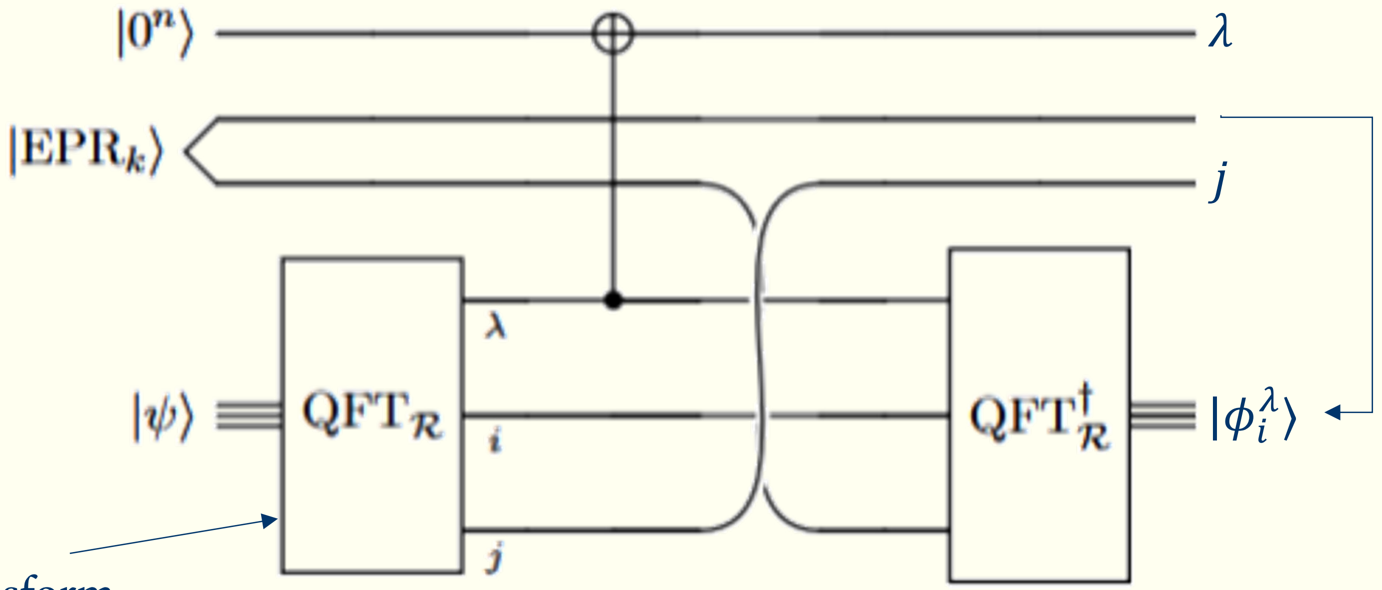
Fourier extraction

Here is what "ideal" Fourier extraction looks like:



Fourier extraction

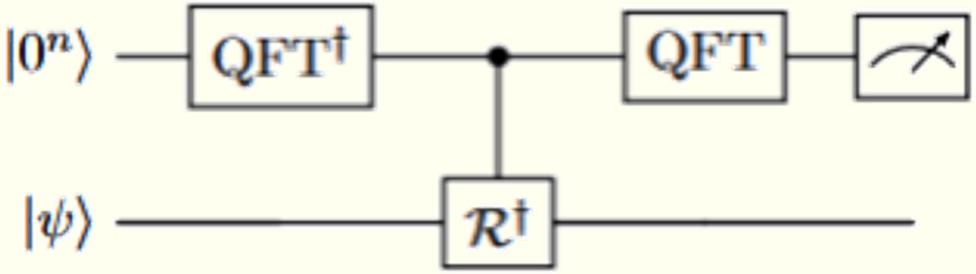
Here is what "ideal" Fourier extraction looks like:



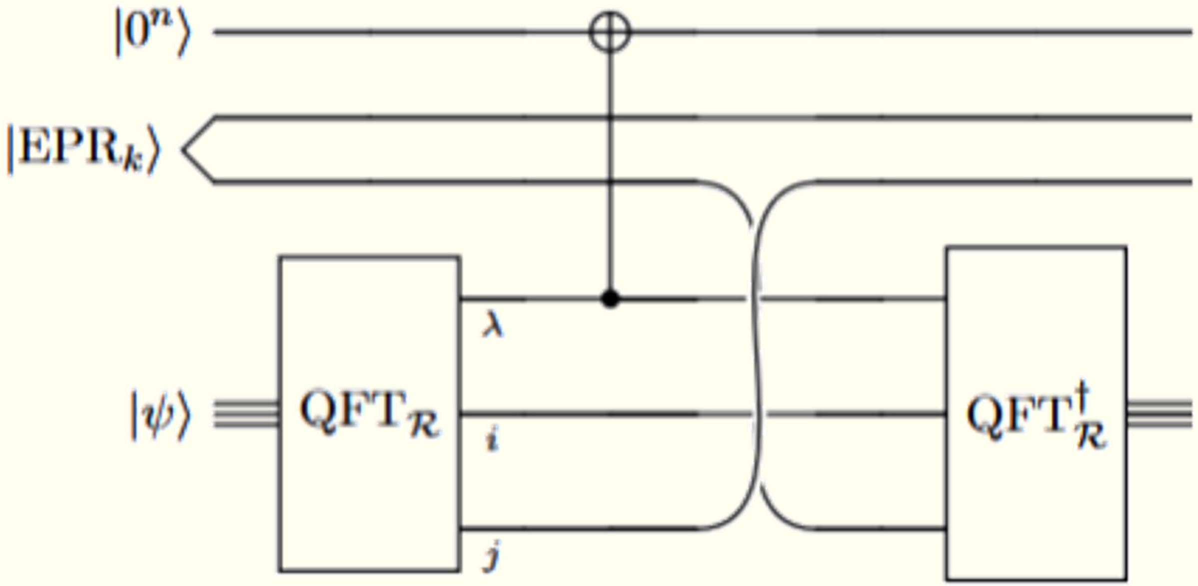
This is not the normal Fourier transform, but the Fourier transform for an arbitrary representation!

Fourier extraction

Turns out, it's equivalent to the following (where the measurement is only on the irrep label).



$\approx$



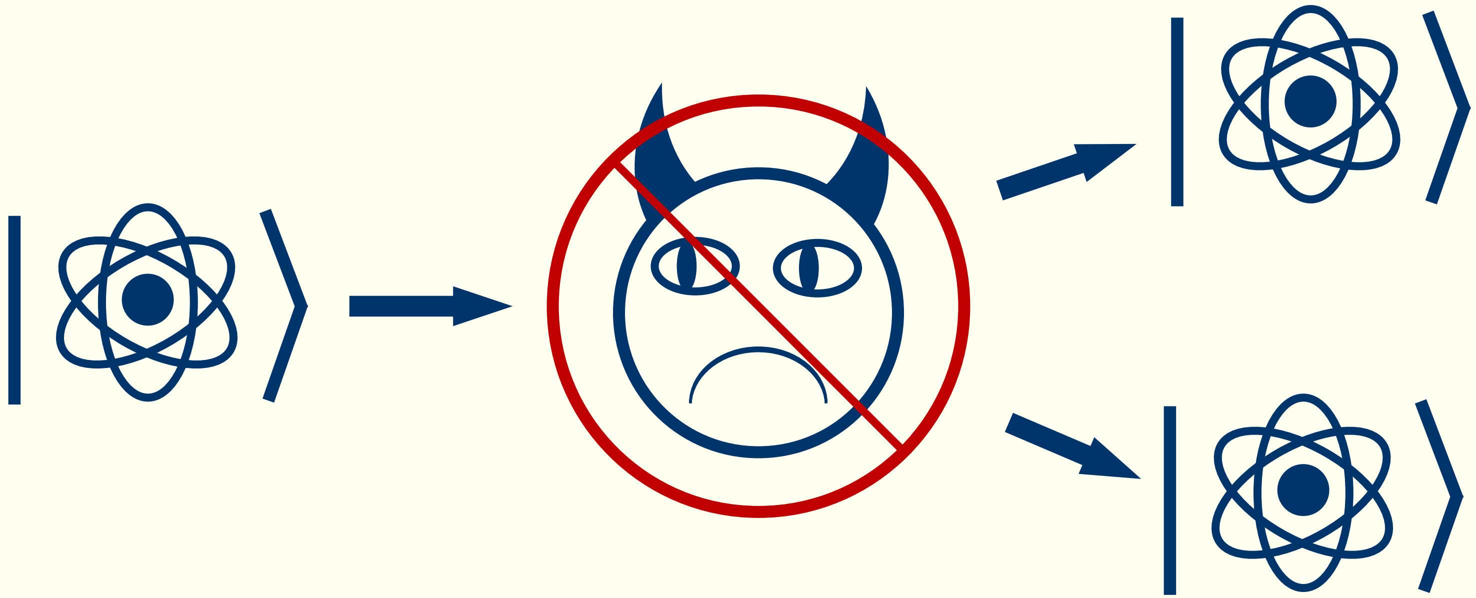
General duality theorem

Theorem: You can efficiently implement a group representation $\mathcal{R}$ if and only if you can efficiently implement Fourier extraction for the irreducible subspaces of $\mathcal{R}$.

Quantum Lightning from Non-Abelian Group Actions

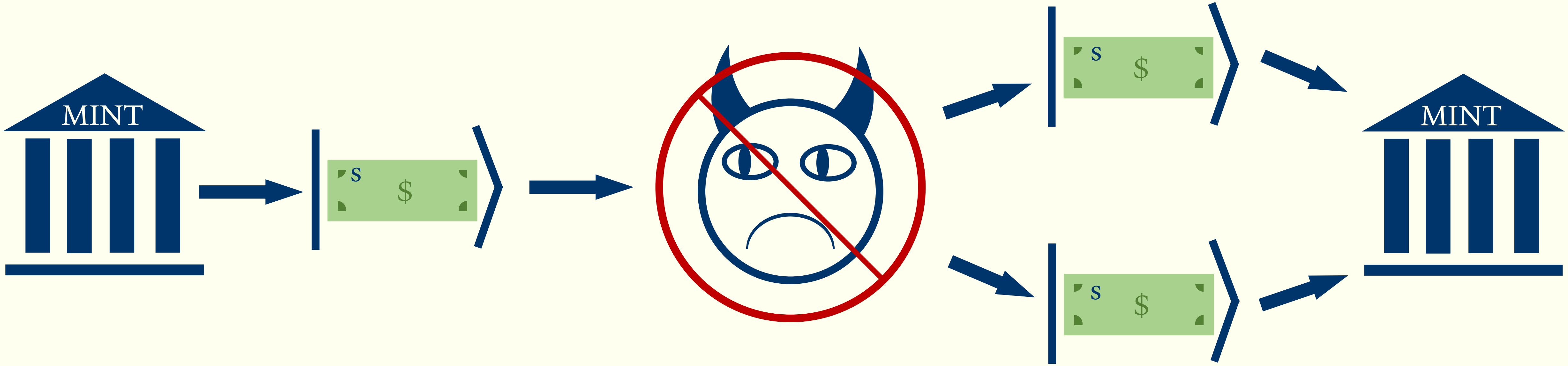
The no-cloning theorem

No cloning says no one can clone an **arbitrary** quantum state.



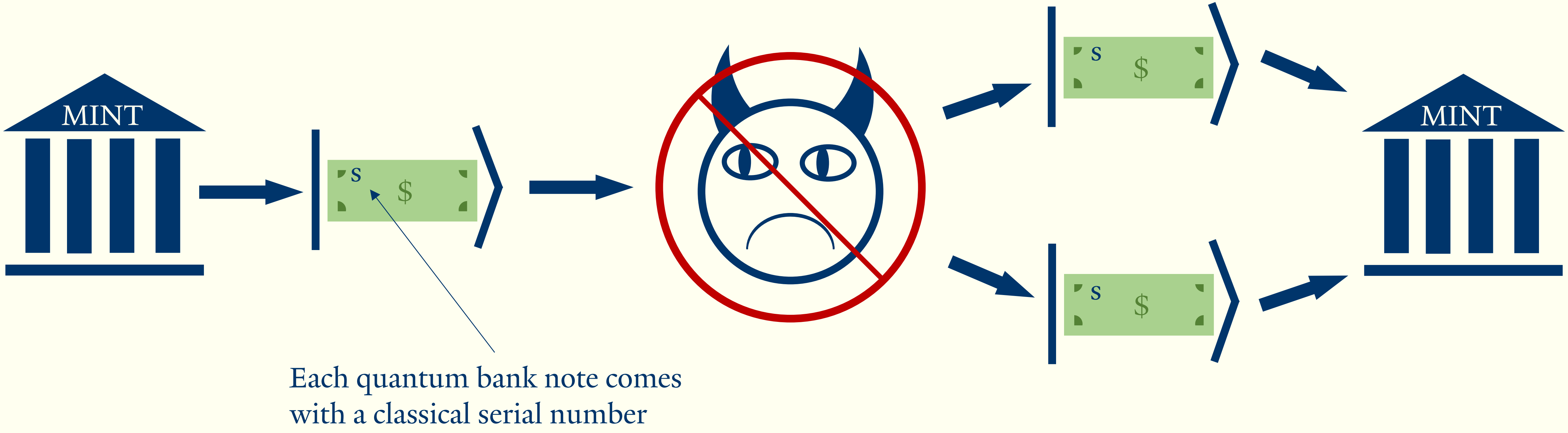
Private-key quantum money

Weisner (in 1970) used this idea to find states that could be efficiently minted, but could not be cloned by any adversary.



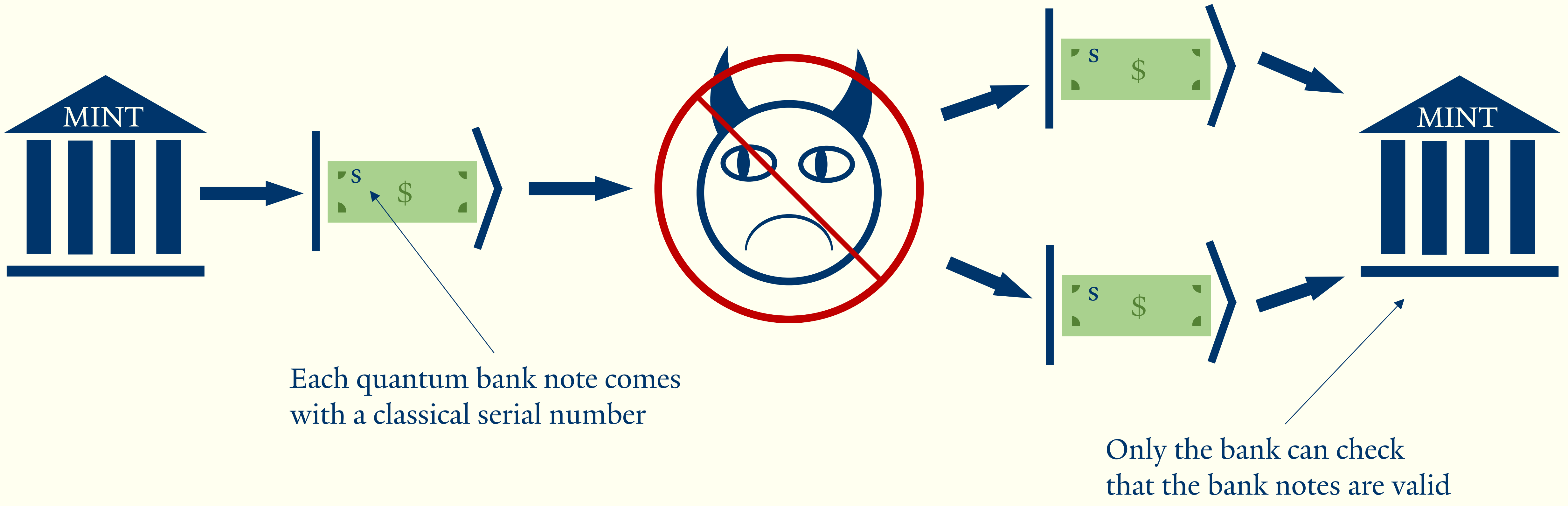
Private-key quantum money

Weisner (in 1970) used this idea to find states that could be efficiently minted, but could not be cloned by any adversary.



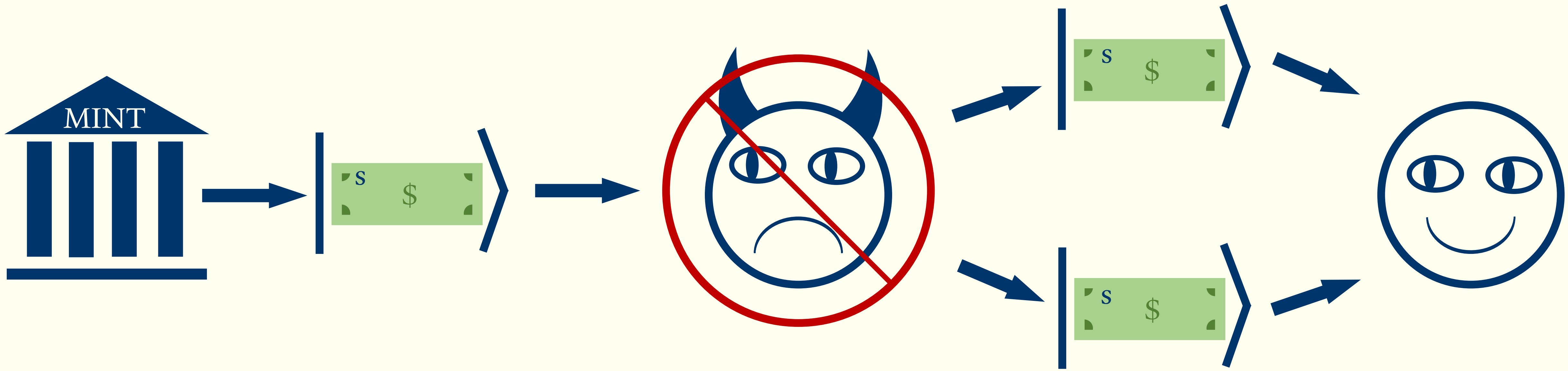
Private-key quantum money

Weisner (in 1970) used this idea to find states that could be efficiently minted, but could not be cloned by any adversary.



Public-key quantum money

Aaronson (2009) proposed quantum money that anyone can verify.



Public-key quantum lightning

Zhandry (2019) proposed a variant of quantum money that is "collision resistant".

Not even the mint can make two notes
that have the same serial number!

Adapted from Zhandry'23

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a plain-model computational assumption

Adapted from Zhandry'23

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a plain-model computational assumption

Aaronson'09 (Random stabilizer states)

[Farhi-Gosset-Hassidim-Lutomirski -Shor'10]: knots

[Aaronson-Christiano'12]: polynomials hiding subspaces

[Zhandry'19]: quadratic systems of equations

[Kane'18, Kane-Sharif-Silverberg'21]: quaternion algebras

[Khesin-Lu-Shor'22]: lattices

Adapted from Zhandry'23

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a plain-model computational assumption
Aaronson'09 (Random stabilizer states)	Aaronson'09 (Relative to a quantum oracle)	
[Farhi-Gosset-Hassidim-Lutomirski-Shor'10]: knots	[Aaronson-Christiano'12]: classical hidden subspaces oracle	
[Aaronson-Christiano'12]: polynomials hiding subspaces	[Kane'18, Kane-Sharif-Silverberg'21]: Commuting unitaries	
[Zhandry'19]: quadratic systems of equations		
[Kane'18, Kane-Sharif-Silverberg'21]: quaternion algebras		
[Khesin-Lu-Shor'22]: lattices		

Adapted from Zhandry'23

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a plain-model computational assumption
Aaronson'09 (Random stabilizer states)	Aaronson'09 (Relative to a quantum oracle)	
[Farhi-Gosset-Hassidim-Lutomirski-Shor'10]: knots	[Aaronson-Christiano'12]: classical hidden subspaces oracle	
[Aaronson-Christiano'12]: polynomials hiding subspaces	[Kane'18, Kane-Sharif-Silverberg'21]: Commuting unitaries	
[Zhandry'19]: quadratic systems of equations	[Liu-Montgomery-Zhandry'23]: Walkable invariants	
[Kane'18, Kane-Sharif-Silverberg'21]: quaternion algebras	[Zhandry'23]: Abelian group actions	
[Khesin-Lu-Shor'22]: lattices		

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a plain-model computational assumption
Aaronson'09 (Random stabilizer states)	Aaronson'09 (Relative to a quantum oracle)	[Zhandry'19]: Post-quantum iO
[Farhi-Gosset-Hassidim-Lutomirski-Shor'10]: knots	[Aaronson-Christiano'12]: classical hidden subspaces oracle	
[Aaronson-Christiano'12]: polynomials hiding subspaces	[Kane'18, Kane-Sharif-Silverberg'21]: Commuting unitaries	
[Zhandry'19]: quadratic systems of equations	[Liu-Montgomery-Zhandry'23]: Walkable invariants	
[Kane'18, Kane-Sharif-Silverberg'21]: quaternion algebras	[Zhandry'23]: Abelian group actions	
[Khesin-Lu-Shor'22]: lattices		

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a plain-model computational assumption
Aaronson'09 (Random stabilizer states)	Aaronson'09 (Relative to a quantum oracle)	[Zhandry'19]: Post-quantum iO
[Farhi-Gosset-Hassidim-Lutomirski -Shor'10]: knots	[Aaronson-Christiano'12]: classical hidden subspaces oracle	
[Aaronson-Christiano'12]: polynomials hiding subspaces	[Kane'18, Kane-Sharif-Silverberg'21]: Commuting unitaries	
[Zhandry'19]: quadratic systems of equations	[Liu-Montgomery-Zhandry'23]: Walkable invariants	
[Kane'18, Kane-Sharif-Silverberg'21]: quaternion algebras	[Zhandry'23]: Abelian group actions	
[Khesin-Lu-Shor'22]: lattices		This work: Preaction secure groups

Basically, the most power cryptography you could imagine, we don't know how to build this either

Group actions

A group action is a pair of a group G, and set X, a starting element $x \in X$, and an operation

$$*: G \times X \mapsto X$$

Group actions

A group action is a pair of a group G, and set X, a starting element $x \in X$, and an operation

$$*: G \times X \mapsto X$$

What makes it a group action is that it is also a group representation:

$$g * (h * x) = gh * x$$

Group actions

A group action is a pair of a group G, and set X, a starting element $x \in X$, and an operation

$$*: G \times X \mapsto X$$

What makes it a group action is that it is also a group representation:

$$g * (h * x) = gh * x$$

Product in the group

Reminder: the quantum Fourier transform

Recall, we call any transformation that maps from the standard basis to the Fourier basis the "Fourier transform".

For the left-regular representation, $U_g|h\rangle \mapsto |gh\rangle$, one nice Fourier transform looks like this:

$$\mathrm{QFT} = \sum_{g\in G} \sum_{\lambda,i,j\in[\dim(W^\lambda)]} \sqrt{\frac{d_\lambda}{|G|}}\, \varrho^\lambda(g)_{i,j} |\lambda, i, j\rangle\langle g|$$

Reminder: the quantum Fourier transform

Recall, we call any transformation that maps from the standard basis to the Fourier basis the "Fourier transform".

For the left-regular representation, $U_g|h\rangle \mapsto |gh\rangle$, one nice Fourier transform looks like this:

The "textbook" definition of the QFT for general groups

$$\mathrm{QFT} = \sum_{g \in G} \sum_{\lambda, i, j \in [\dim(W^\lambda)]} \sqrt{\frac{d_\lambda}{|G|}} \varrho^\lambda(g)_{i,j} |\lambda, i, j\rangle\langle g|$$

Quantum lightning from group actions

In the construction, we'll need to start with a group action for a group that has an **efficient quantum Fourier transform**, e.g.

1. Any group whose size doesn't scale in n.
2. Dihedral group.
3. Symmetric group.

Quantum lightning from group actions

$\mathsf{Mint}(1^\lambda)$:

Quantum lightning from group actions

$\mathrm{Mint}(1^{\lambda})$:

- Prepare a uniform superposition over group elements.

$$\sum_{g \in G} |g\rangle \otimes |x\rangle .$$

Quantum lightning from group actions

$\mathrm{Mint}(1^{\lambda})$:

- Prepare a uniform superposition over group elements.

$$\sum_{g\in G} |g\rangle \otimes |x\rangle .$$

- Apply the group action.

$$\sum_{g\in G} |g\rangle \otimes |g * x\rangle .$$

Quantum lightning from group actions

$\mathrm{Mint}(1^\lambda)$:

- Prepare a uniform superposition over group elements.

$$\sum_{g \in G} |g\rangle \otimes |x\rangle .$$

- Apply the group action.

$$\sum_{g \in G} |g\rangle \otimes |g * x\rangle .$$

- Apply a quantum Fourier transform to the first register.

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

Quantum lightning from group actions

$\mathrm{Mint}(1^{\lambda})$:

- Prepare a uniform superposition over group elements.

$$\sum_{g\in G} |g\rangle \otimes |x\rangle .$$

- Apply the group action.

$$\sum_{g\in G} |g\rangle \otimes |g * x\rangle .$$

- Apply a quantum Fourier transform to the first register.

$$\sum_{\lambda,i,j} |\lambda, i, j\rangle \otimes \underbrace{\sum_{g\in G} \varrho^{\lambda}(g^{-1})_{i,j} |g * x\rangle}_{|\$^{s}\rangle}$$

s

Quantum lightning from group actions

$\mathrm{Ver}(\mathrm{s}{=}\lambda,\ |\pounds\rangle = |\$^{\lambda,i,j}\rangle)$:

Quantum lightning from group actions

Ver(s=λ, $|£\rangle = |\$^{\lambda,i,j}\rangle$):

- Prepare a uniform superposition over group elements.

$$\sum_g |g\rangle \otimes |£\rangle.$$

Quantum lightning from group actions

Ver(s=λ, $|£\rangle = |\$^{\lambda,i,j}\rangle$):

- Prepare a uniform superposition over group elements.

$$\sum_g |g\rangle \otimes |£\rangle.$$

- Apply the group action.

$$\sum_{g\in G} |g\rangle \otimes |g * £\rangle\,.$$

Quantum lightning from group actions

Ver(s=λ, $|£\rangle = |\$^{\lambda,i,j}\rangle$):

- Prepare a uniform superposition over group elements.

$$\sum_g |g\rangle \otimes |£\rangle.$$

- Apply the group action.

$$\sum_{g \in G} |g\rangle \otimes |g * £\rangle \propto \sum_k \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle.$$

Quantum lightning from group actions

Ver(s=λ, $|£\rangle = |\$^{\lambda,i,j}\rangle$):

- Prepare a uniform superposition over group elements.

$$\sum_g |g\rangle \otimes |£\rangle.$$

- Apply the group action.

$$\sum_{g \in G} |g\rangle \otimes |g * £\rangle \propto \sum_k \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle\,.$$

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

Quantum lightning from group actions

Ver(s=λ, $|£\rangle = |\$^{\lambda,i,j}\rangle$):

- Prepare a uniform superposition over group elements.

$$\sum_{g} |g\rangle \otimes |£\rangle.$$

- Apply the group action.

$$\sum_{g \in G} |g\rangle \otimes |g * £\rangle \propto \sum_{k} \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle.$$

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

- Apply a QFT to the first register and measure λ.

Quantum lightning from group actions

Ver(s=λ, $|£\rangle = |\$^{\lambda,i,j}\rangle$):

- Prepare a uniform superposition over group elements.

$$\sum_{g} |g\rangle \otimes |£\rangle.$$

- Apply the group action.

$$\sum_{g \in G} |g\rangle \otimes |g * £\rangle \propto \sum_{k} \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle.$$

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

- Apply a QFT to the first register and measure λ.

Basically, measure in the Fourier basis, but only check the irrep label.

Security of the scheme

In order to prove lightning security, we need to answer the following question:

"What is something that you can do with two copies, but not with one copy of a quantum state?"

Security of the scheme

In order to prove lightning security, we need to answer the following question:

“What is something that you can do with two copies, but not with one copy of a quantum state?”

Our answer: Distinguish between an operation that preserves your state (up to an arbitrary phase), and one that moves your state around.

Preaction security

Recall that a group action by element h acts as follows:

$$|g * x\rangle \mapsto |hg * x\rangle$$

Preaction security

Recall that a group action by element h acts as follows:

$$|g * x\rangle \mapsto |hg * x\rangle$$

A preaction by h acts as follows:

$$|g * x\rangle \mapsto |gh^{-1} * x\rangle$$

Preaction security

A preaction by h acts as follows:

$$|g * x\rangle \mapsto |gh^{-1} * x\rangle$$

Preaction security:

Preaction security

A preaction by h acts as follows:

$$|g * x\rangle \mapsto |gh^{-1} * x\rangle$$

Preaction security:

Preaction Hardness:

It's hard to implement a random preaction
(with high probability over the choice of group
element)

Preaction security

A preaction by h acts as follows:

$$|g * x\rangle \mapsto |gh^{-1} * x\rangle$$

Preaction security:

Preaction Hardness:

It's hard to implement a random preaction (with high probability over the choice of group element)

Preaction Indistinguishability:

It's hard to distinguish between a challenger that applies a random action, versus a challenger that applies a random action and a random preaction.

Security reduction (simplified)

Given two copies of the money state:

Security reduction (simplified)

Given two copies of the money state:

1. Send one copy to the preaction security challenger.

Security reduction (simplified)

Given two copies of the money state:

1. Send one copy to the preaction security challenger.
2. Perform Fourier subspace extraction on both.

Security reduction (simplified)

Given two copies of the money state:

1. Send one copy to the preaction security challenger.
2. Perform Fourier subspace extraction on both.
3. Do a SWAP test between the $|\phi_i^\lambda\rangle$ registers.

Security reduction (simplified)

Given two copies of the money state:

1. Send one copy to the preaction security challenger.
2. Perform Fourier subspace extraction on both.
3. Do a SWAP test between the $|\phi_i^\lambda\rangle$ registers.

This test tells us if i stayed the same. A preaction will randomize $|\phi_i^\lambda\rangle$, but the (left) group action won't, so we can distinguish the two cases.

Quantum Lightning from Preaction Security

Theorem: Given any group action that is preaction secure, the scheme we described is a secure quantum lightning scheme.

Instantiations

Group action from the McEliece cryptosystem. The group action is the symmetric group, set elements are $n \times m$ matrices with entries from some finite field $\mathbb{F}$ (think: codewords of an error correcting code).

Instantiations

Group action from the McEliece cryptosystem. The group action is the symmetric group, set elements are $n \times m$ matrices with entries from some finite field $\mathbb{F}$ (think: codewords of an error correcting code).

A permutation (in S_m) acts on a set element by:

1. Permute the columns of the matrix.
2. Row-reduce the matrix.

Instantiations

Group action from the McEliece cryptosystem. The group action is the symmetric group, set elements are $n \times m$ matrices with entries from some finite field $\mathbb{F}$ (think: codewords of an error correcting code).

A permutation (in S_m) acts on a set element by:

1. Permute the columns of the matrix.
2. Row-reduce the matrix.

We conjecture that this is preaction secure.

Open questions

- Can you reduce preaction security to a “standard” assumption, like discrete log being hard, or the hidden subgroup problem being hard?

- Can you build other things from preaction secure group actions? For example, one-shot signatures, or copy-protected software?

- Can we find an efficiently falsifiable variant of preaction indistinguishability? For example, if the group action had a trapdoor that allowed the challenger to implement a random preaction.