A General Duality for Representations of Groups

with Applications to Quantum Money, Lightning, and Fire

John Bostanci

Based on joint work with Barak Nehoran and Mark Zhandry

Flipping-Distinguishing duality

Aaronson, Atia, and Susskind showed that the following tasks are computationally equivalent:

1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.
2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Flipping-Distinguishing duality

Aaronson, Atia, and Susskind showed that the following tasks are computationally equivalent:

1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.
2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Is this just part of a more general equivalence between measurement-type tasks and mapping-type tasks?

Flipping-Distinguishing duality

Aaronson, Atia, and Susskind showed that the following tasks are computationally equivalent:

1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.
2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Is this just part of a more general equivalence between measurement-type tasks and mapping-type tasks?

Yes! But things get weird

Flipping-Distinguishing duality

Aaronson, Atia, and Susskind showed that the following tasks are computationally equivalent:

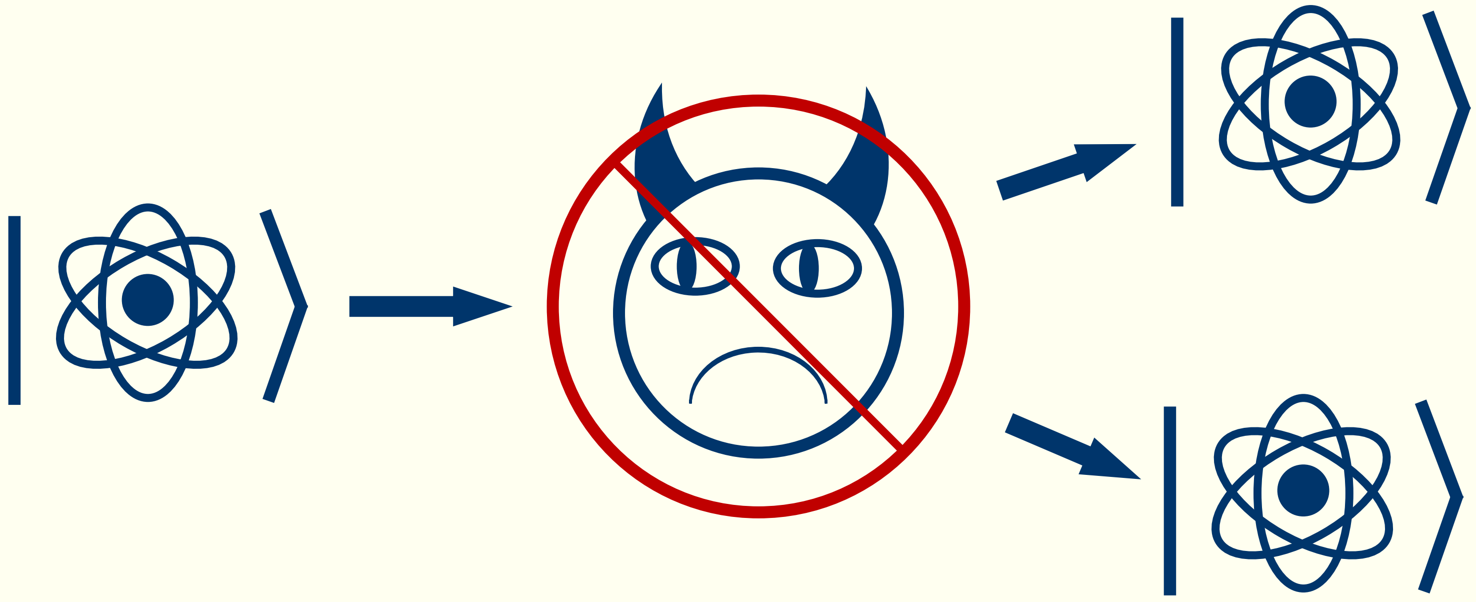
1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.
2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Is this just part of a more general equivalence between measurement-type tasks and mapping-type tasks?

Yes! But things get weird (in a good way)

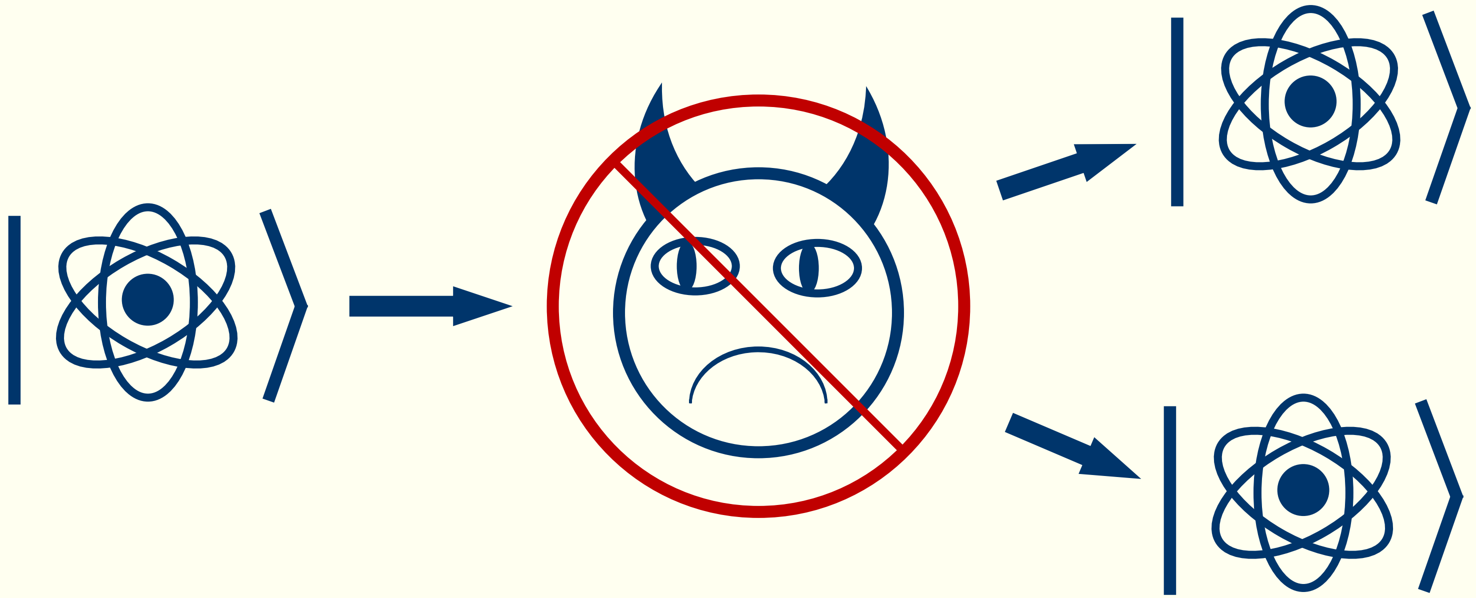
No-cloning

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



No-cloning

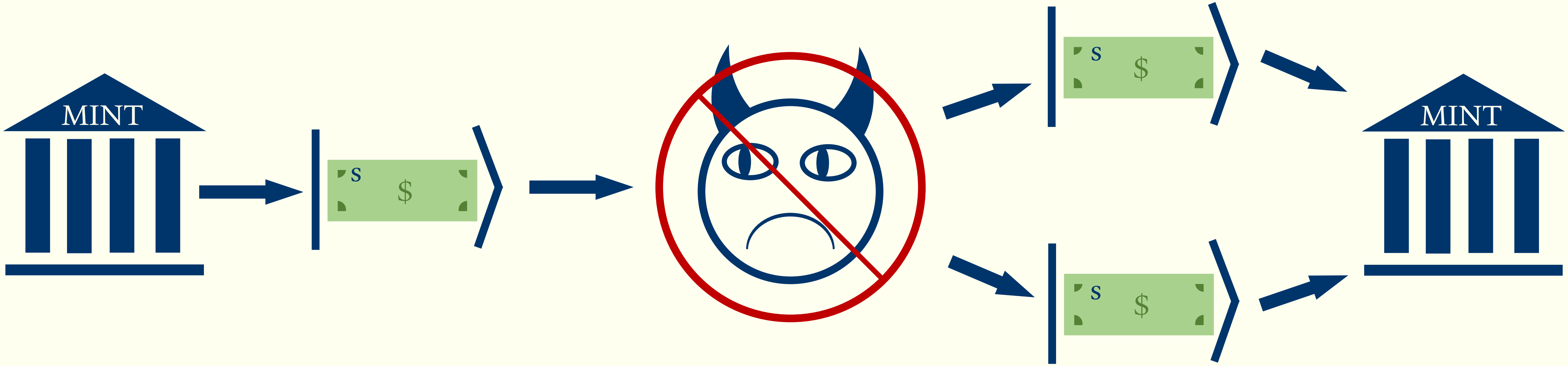
No cloning says no one can clone an arbitrary quantum state.



Does this also hold for a family of **useful** quantum states?

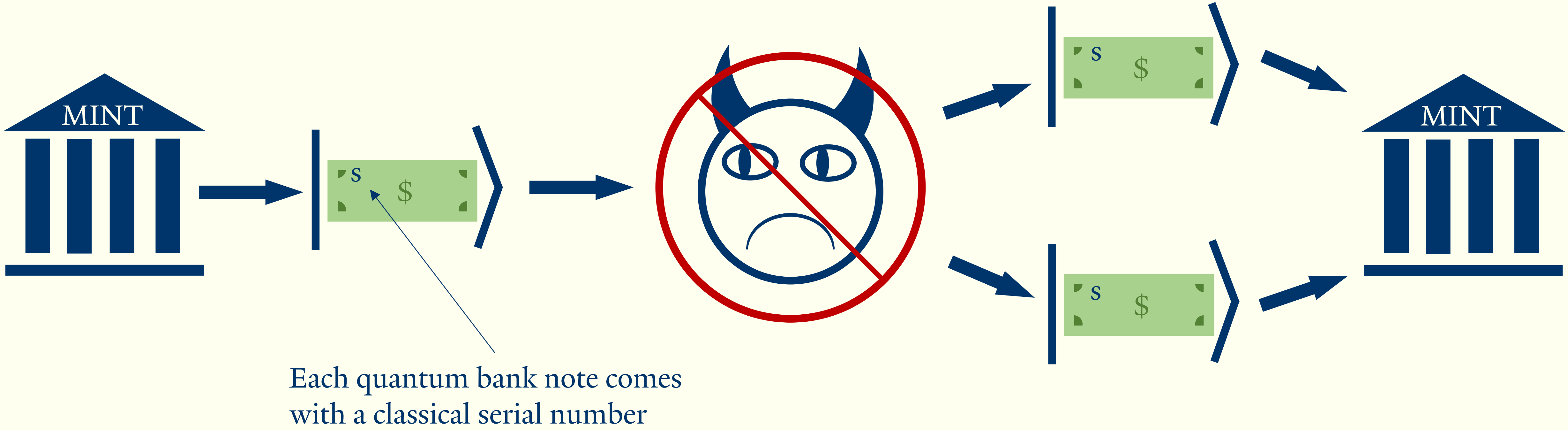
From no-cloning to quantum money

Weisner (in 1968) used this idea to find states that could be efficiently minted, but could not be cloned by any adversary.



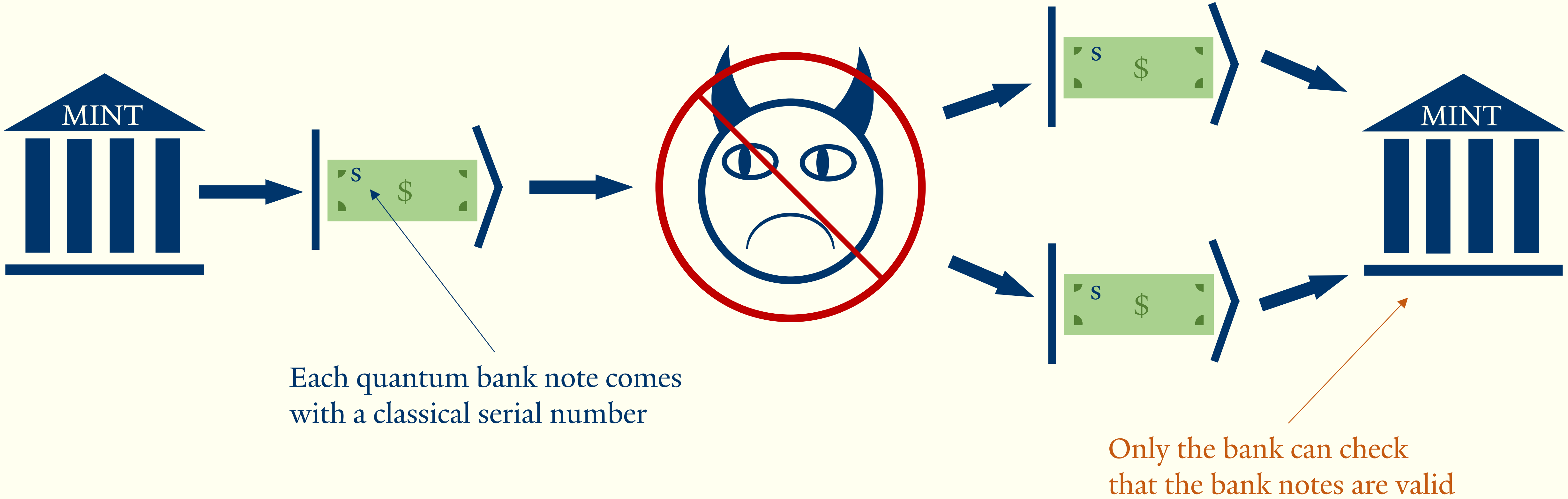
From no-cloning to quantum money

Weisner (in 1968) used this idea to find states that could be efficiently minted, but could not be cloned by any adversary.



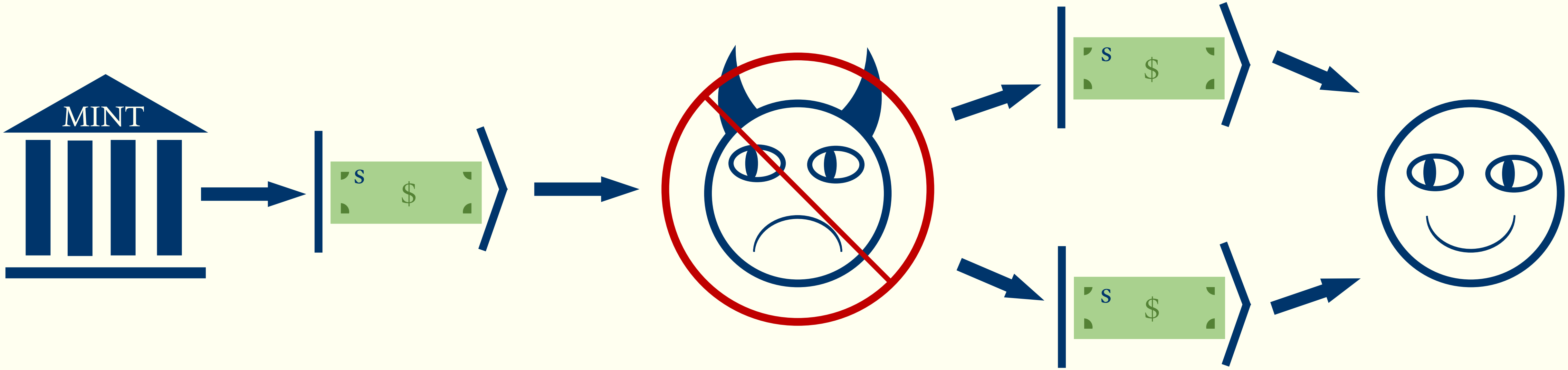
From no-cloning to quantum money

Weisner (in 1968) used this idea to find states that could be efficiently minted, but could not be cloned by any adversary.



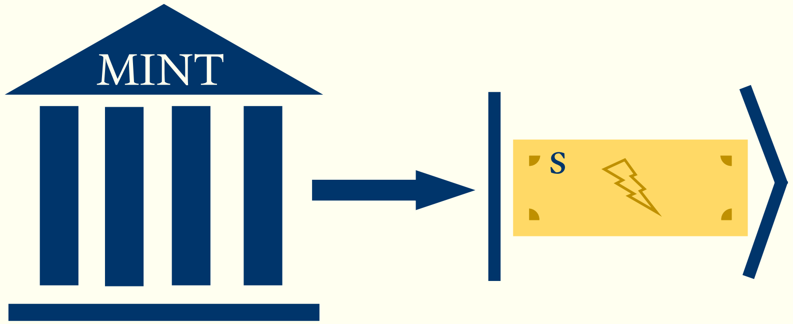
Public-key quantum money

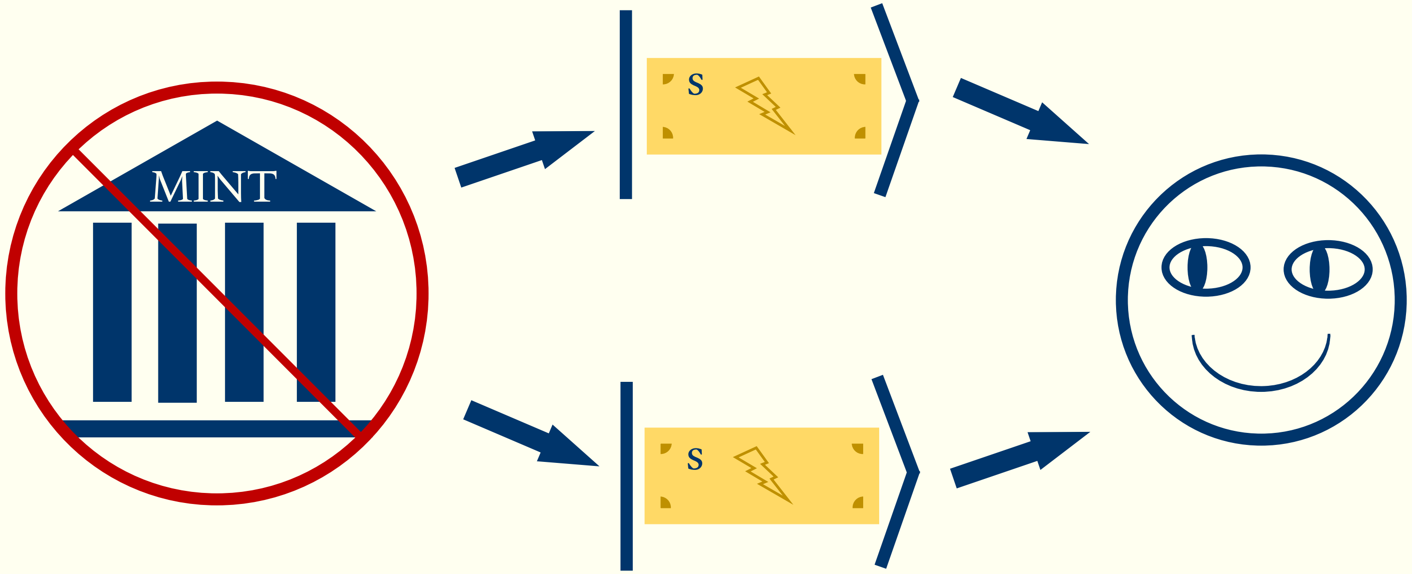
Wiesner, Breidbart, Bennet, Brassard (1982) and Aaronson (2009) proposed quantum money that anyone can verify.



Public-key quantum lightning

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





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

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a well-studied 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 well-studied 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		

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

Unfortunately, constructing quantum money has been really hard!

Only has conjectured security, or completely broken	Security in an idealized model	Security from a well-studied 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: Pre-action secure groups

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

A generic recipe for quantum lightning

Ingredients:

1. A collection of subspaces $\{\Pi_i\}$.
2. An initial state $|\text{init}\rangle$ that is "spread out" over the subspaces.

A generic recipe for quantum lightning

Ingredients:

1. A collection of subspaces $\{\Pi_i\}$.
2. An initial state $|\text{init}\rangle$ that is "spread out" over the subspaces.

A candidate quantum lightning construction:

1. Prepare the initial state $|\text{init}\rangle$.
2. Measure the POVM $\{\Pi_i\}$ to get a serial number and lightning state.

A generic recipe for quantum lightning

Ingredients:

Invariant subspaces of a group.

1. A collection of subspaces $\{\Pi_i\}$.
2. An initial state $|\text{init}\rangle$ that is "spread out" over the subspaces.

An EPR pair of "group elements"

A candidate quantum lightning construction:

1. Prepare the initial state $|\text{init}\rangle$.
2. Measure the POVM $\{\Pi_i\}$ to get a serial number and lightning state.

Quantum lightning from group actions

To understand the construction, we first need to understand three things:

- Group actions.
- Irreducible representations of groups.
- Quantum Fourier transforms for non-Abelian groups.

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 respects group structure:

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

Group actions

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

$$*\colon G \times X \mapsto X$$

What makes it a group action is that it respects group structure:

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

Product in the group

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 respects group structure:

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

Product in the group

When we say we can implement a group action, we mean we can do:

$$|g\rangle|y\rangle \mapsto |g\rangle|g * y\rangle$$

Representations and irreps

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:

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

Representations and irreps

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

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

Representations and irreps

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!

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

Representations and irreps

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)

Representations and irreps

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!

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

We call these irrep labels

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

Representations and irreps

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!

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

We call V the quantum Fourier transform

We call these irrep labels

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

The quantum Fourier transform

While the quantum Fourier transform from the last slide might seem weird, it has the "usual" form when we consider the left-regular representation:

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

For this representation, the quantum Fourier transform looks like:

$$\mathrm{QFT}_G = \sum_{\lambda,i,j,g} \sqrt{\frac{d_\lambda}{|G|}} \varrho^\lambda(g)_{i,j} |\lambda, i, j\rangle\langle g| .$$

The quantum Fourier transform

While the quantum Fourier transform from the last slide might seem weird, it has the “usual” form when we consider the left-regular representation:

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

For this representation, the quantum Fourier transform looks like:

$$\mathrm{QFT}_G = \sum_{\lambda,i,j,g} \sqrt{\frac{d_\lambda}{|G|}}\varrho^\lambda(g)_{i,j}|\lambda, i, j\rangle\langle g|\,.$$

For Abelian groups, i, j only go up to 1 and d_λ is 1 for all irreps.

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

Mint(1^λ):

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

Mint(1^λ):

- Prepare a uniform superposition over group elements.

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

- Apply the controlled group action and then inverse the group element.

$$\sum_{g \in G} |g^{-1}\rangle \otimes |g * x\rangle .$$

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 controlled group action and then inverse the group element.

$$\sum_{g \in G} |g^{-1}\rangle \otimes |g * x\rangle \,.$$

- 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 controlled group action and then inverse the group element.

$$\sum_{g\in G} |g^{-1}\rangle \otimes |g * x\rangle .$$

- Apply a quantum Fourier transform to the first register.

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

Quantum lightning from group actions

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

Quantum lightning from group actions

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

- Prepare a uniform superposition over group elements.

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

Quantum lightning from group actions

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

- Prepare a uniform superposition over group elements.

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

- Apply the controlled group action and invert the group element.

$$\sum_{g \in G} |g^{-1}\rangle \otimes |g * £\rangle.$$

Quantum lightning from group actions

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

- Prepare a uniform superposition over group elements.

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

- Apply the controlled group action and invert the group element.

$$\sum_{g\in G} |g^{-1}\rangle \otimes |g * £\rangle \propto \sum_{k} \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle.$$

Quantum lightning from group actions

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

- Prepare a uniform superposition over group elements.

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

- Apply the controlled group action and invert the group element.

$$\sum_{g\in G} |g^{-1}\rangle \otimes |g * £\rangle \propto \sum_k \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle .$$

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

Quantum lightning from group actions

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

- Prepare a uniform superposition over group elements.

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

- Apply the controlled group action and invert the group element.

$$\sum_{g\in G} |g^{-1}\rangle \otimes |g * £\rangle \propto \sum_k \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle.$$

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

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

Quantum lightning from group actions

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

- Prepare a uniform superposition over group elements.

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

- Apply the controlled group action and invert the group element.

$$\sum_{g\in G} |g^{-1}\rangle \otimes |g * £\rangle \propto \sum_{k} \left|\mathcal{L}^{\lambda,k,j}\right\rangle \otimes |\$^{\lambda,i,k}\rangle.$$

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

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

We only need the irrep label.

Dirty fixed point testing and security

To prove security, we need to find a task that should be

1. hard with a single copy, and
2. easy with two copies.

Dirty fixed point testing and security

To prove security, we need to find a task that should be

1. hard with a single copy, and
2. easy with two copies.

Our candidate problem is called "dirty fixed point testing".

Dirty fixed point testing and security

Simplified setup for dirty fixed point testing:

1. An “extraction” unitary, Extract
2. A state $|\psi\rangle$ such that $\text{Extract} \cdot |\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$.

Dirty fixed point testing and security

Simplified setup for dirty fixed point testing:

1. An “extraction” unitary, Extract
2. A state $|\psi\rangle$ such that $\text{Extract} \cdot |\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$.
3. Two operators L and R such that:

$$\text{Extract} \cdot L\,|\psi\rangle = |\phi_1\rangle \otimes |\phi_2'\rangle, \text{ and}$$
$$\text{Extract} \cdot R\,|\psi\rangle \text{ is far from } |\phi_1\rangle \otimes \text{id}.$$

Question: Determine if a challenger is applying L or R.

Dirty fixed point testing and security

Dirty fixed point testing is definitely easy with two copies of $|\psi\rangle$:

1. Send one copy to the adversary.
2. Run Extract on both copies.
3. Swap test the first registers.

Dirty fixed point testing and security

Dirty fixed point testing is definitely easy with two copies of $|\psi\rangle$:

1. Send one copy to the adversary.
2. Run Extract on both copies.
3. Swap test the first registers.

Now we need to find hard instances!

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

A preaction by h acts as follows:

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

Preaction security:

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.

Going back to dirty fixed point testing

L and R will be the group action, and a pre-action and group action.

Going back to dirty fixed point testing

L and R will be the group action, and a pre-action and group action.

"Dirty" fixed point testing because performing the group action will fix the information in the j register, but move around the i subspace.

Going back to dirty fixed point testing

L and R will be the group action, and a pre-action and group action.

"Dirty" fixed point testing because performing the group action will fix the information in the j register, but move around the i subspace.

Implementing the Extract becomes Fourier extraction.

Recall AAS duality:

1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.

2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Back to duality

We show that the following tasks are computationally equivalent:

1. Implementing a representation of a group, U_g.

2. Implementing a Fourier extraction in the irreps of the representation.

Recall AAS duality:

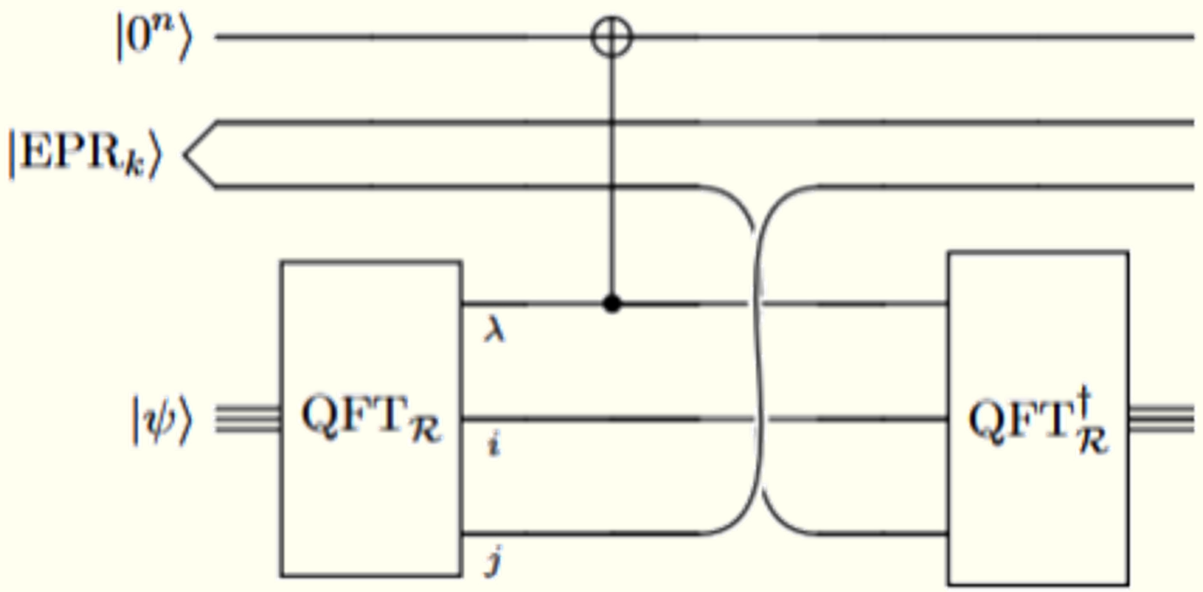
1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.

2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Back to duality

We show that the following tasks are computationally equivalent:

1. Implementing a representation of a group, U_g.
2. Implementing a Fourier extraction in the irreps of the representation.



Recall AAS duality:

1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.

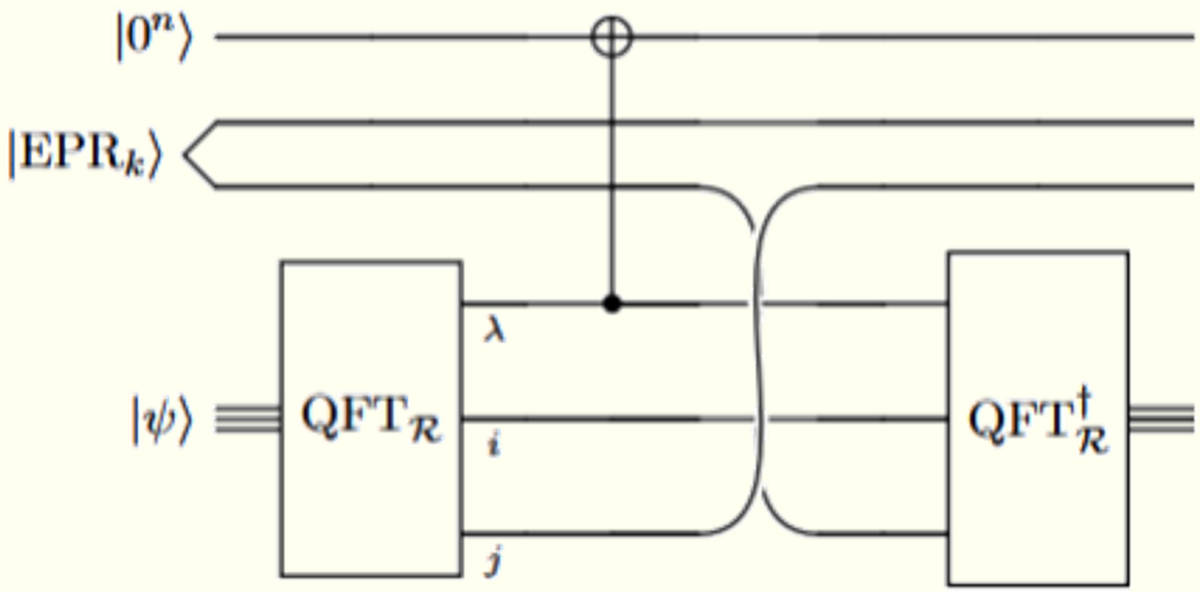
2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Back to duality

We show that the following tasks are computationally equivalent:

1. Implementing a representation of a group, U_g.

2. Implementing a Fourier extraction in the irreps of the representation.



λ is measured

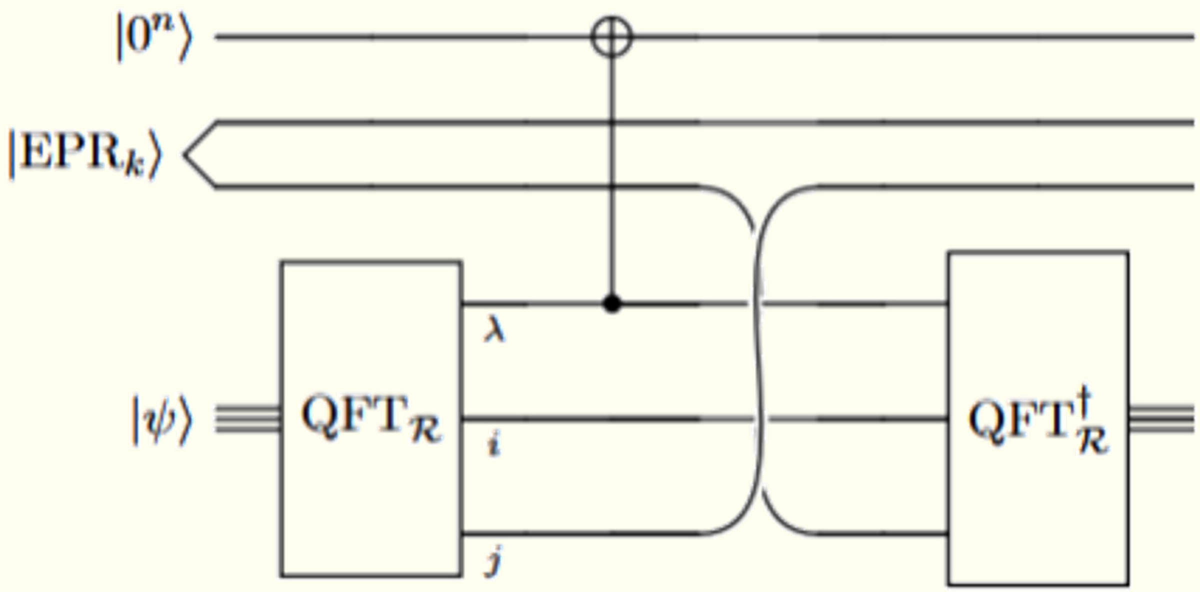
Recall AAS duality:

1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.
2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Back to duality

We show that the following tasks are computationally equivalent:

1. Implementing a representation of a group, U_g.
2. Implementing a Fourier extraction in the irreps of the representation.



λ is measured

j information is extracted

Recall AAS duality:

1. Flipping between two states $|\psi\rangle$ and $|\phi\rangle$.

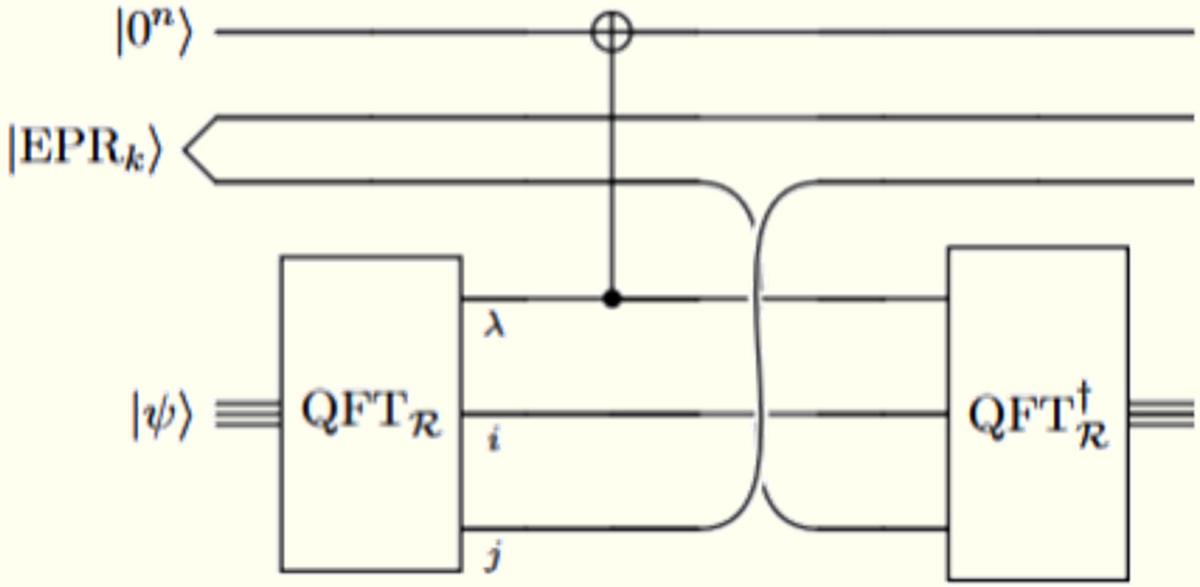
2. Distinguishing between $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$.

Back to duality

We show that the following tasks are computationally equivalent:

1. Implementing a representation of a group, U_g.

2. Implementing a Fourier extraction in the irreps of the representation.



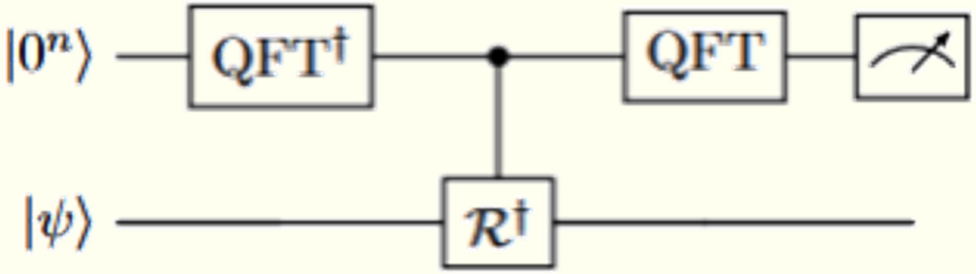
λ is measured

j information is extracted

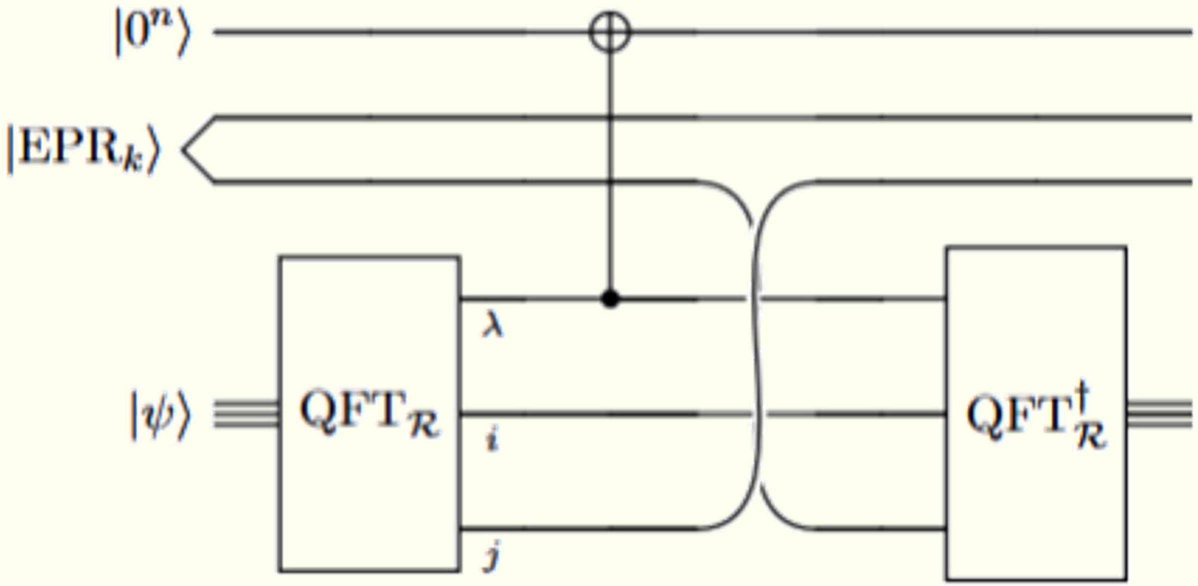
Rest of the state depends only on i

Implementing Fourier extraction

Turns out, the following simple circuit implements Fourier extraction:



$\approx$



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 a falsifiable variant of preaction indistinguishability? For example, if the group action had a trapdoor that allowed the challenger to implement a random preaction.