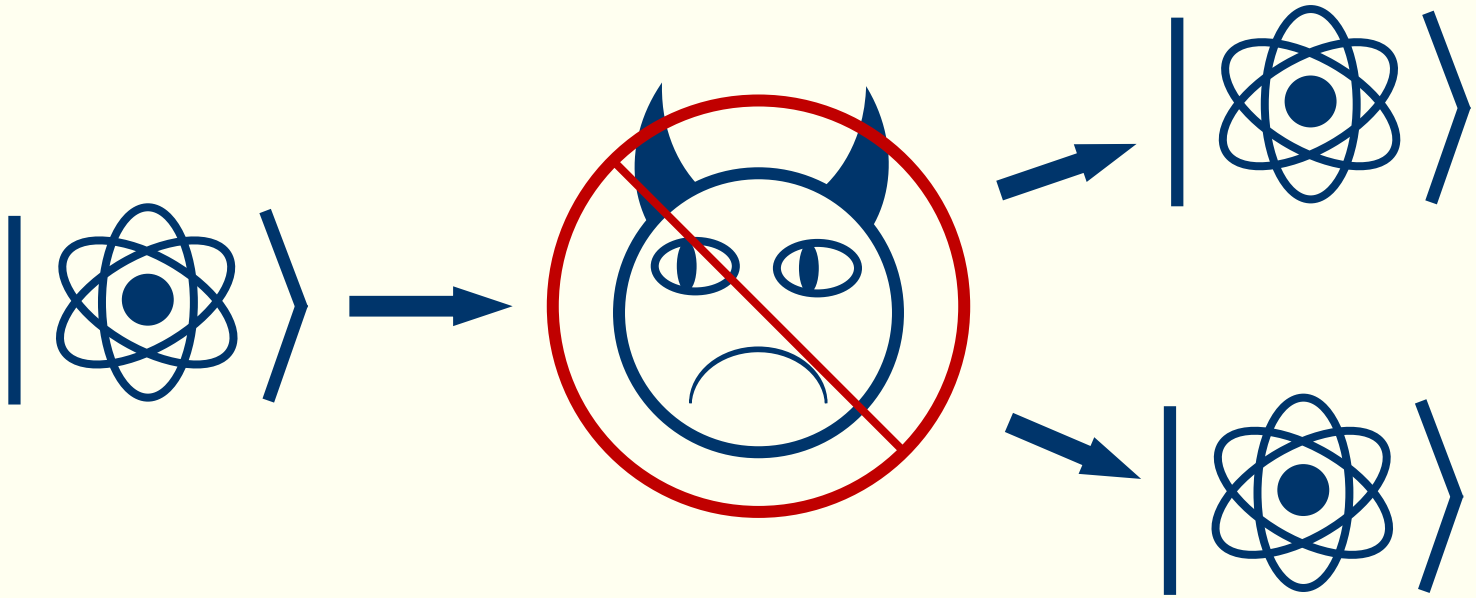
Quantum Lightning from Non-Abelian Group Actions

John Bostanci

Based on joint work with Barak Nehoran and Mark Zhandry

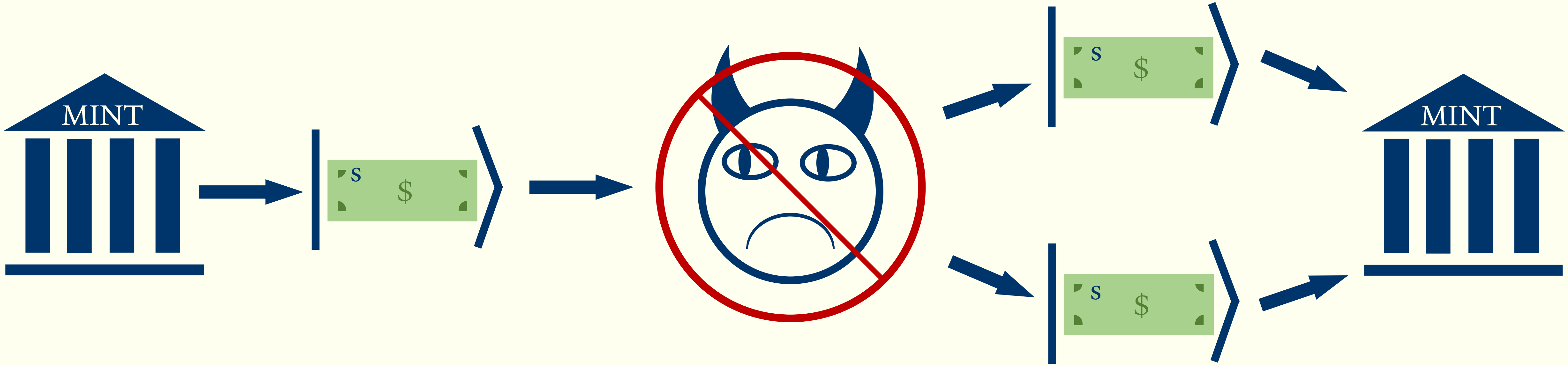
No-cloning

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



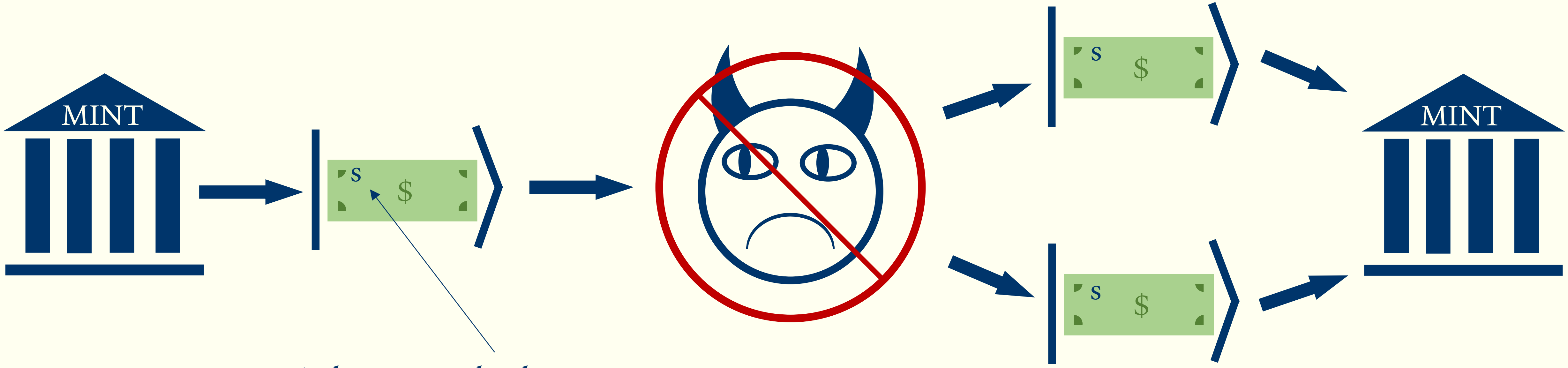
From no-cloning to quantum money

Weisner (in 1970) 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

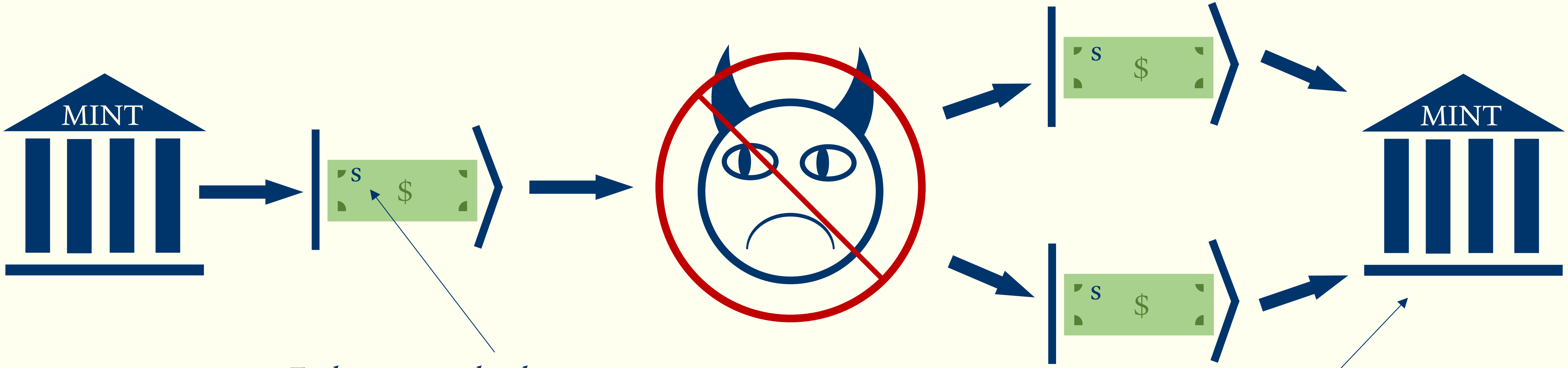
Weisner (in 1970) used this idea to find states that could be efficiently minted, but could not be cloned by any adversary.



Each quantum bank note comes with a classical serial number

From no-cloning to quantum money

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

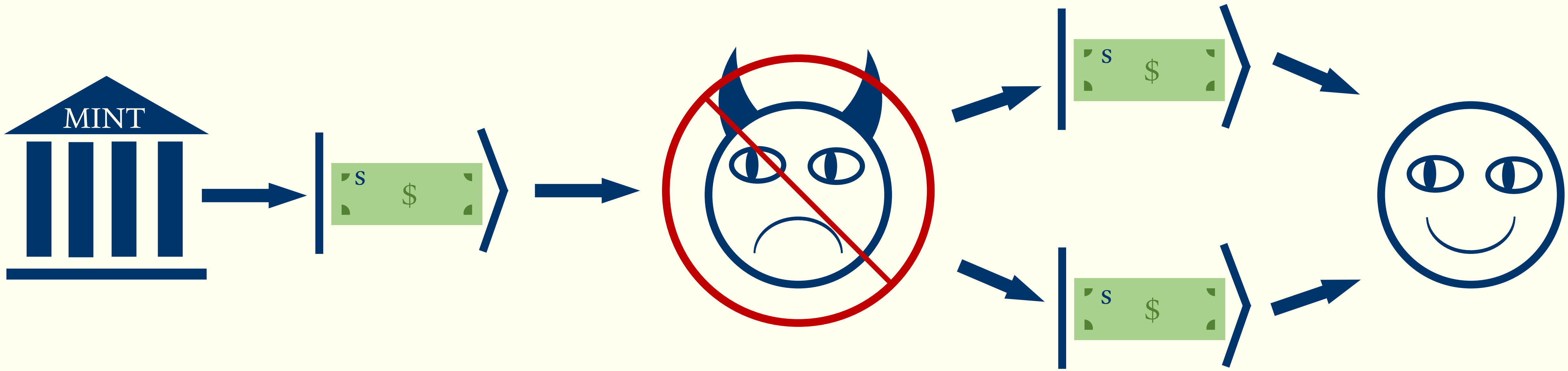


Each quantum bank note comes with a classical serial number

Only the bank can check that the bank notes are valid

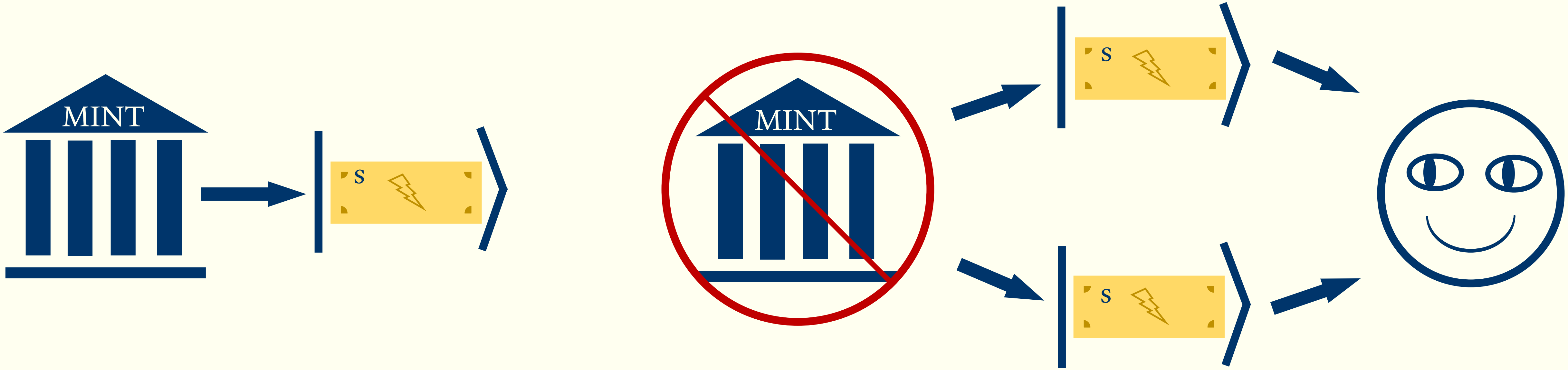
Public-key quantum money

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!

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

- 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

Security in an idealized model

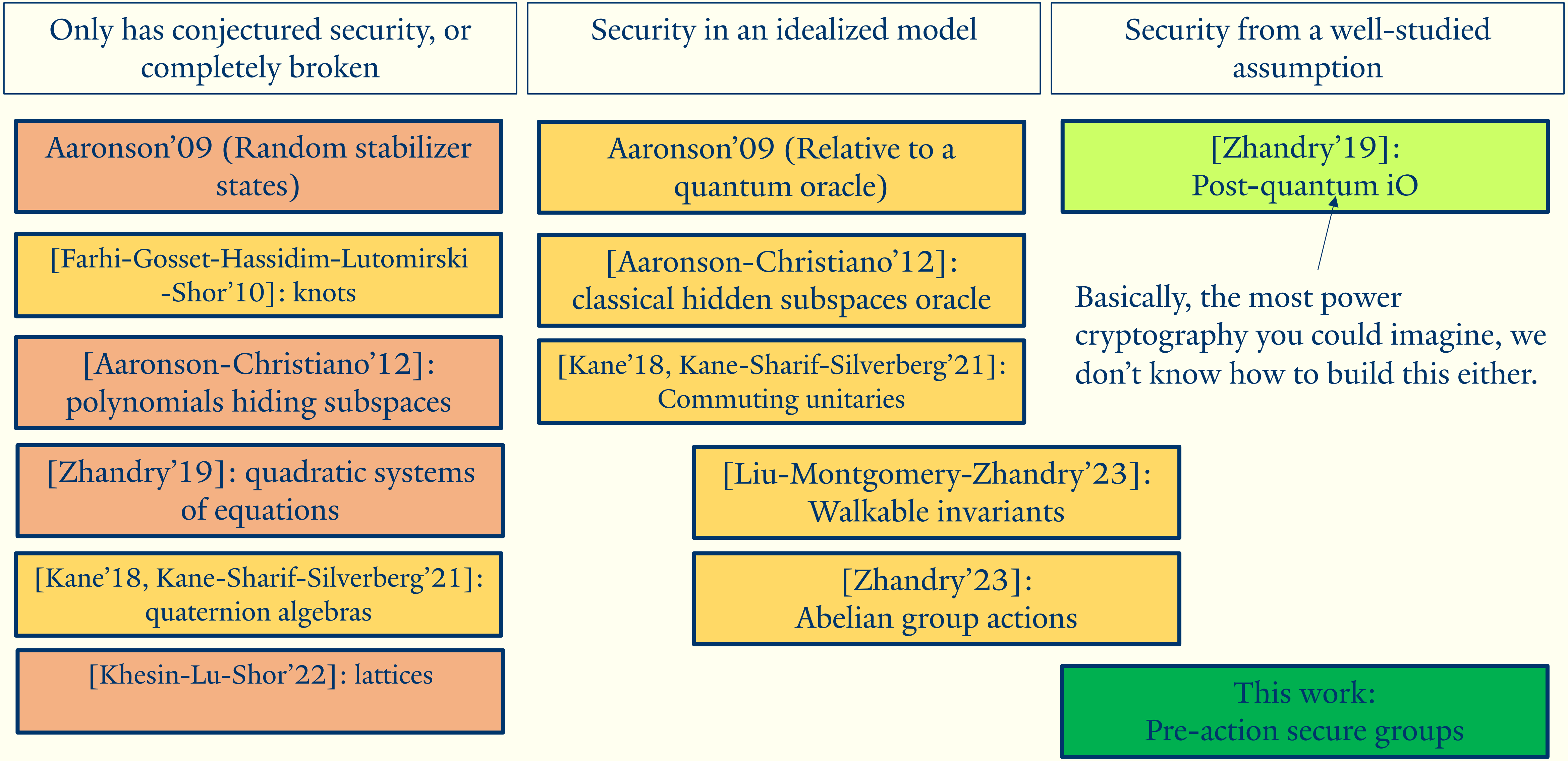
- Aaronson'09 (Relative to a quantum oracle)
- [Aaronson-Christiano'12]: classical hidden subspaces oracle
- [Kane'18, Kane-Sharif-Silverberg'21]: Commuting unitaries
- [Liu-Montgomery-Zhandry'23]: Walkable invariants
- [Zhandry'23]: Abelian group actions

Security from a well-studied assumption

- [Zhandry'19]: Post-quantum iO

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

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

Security in an idealized model

Aaronson’09 (Relative to a quantum oracle)

[Aaronson-Christiano’12]: classical hidden subspaces oracle

[Kane’18, Kane-Sharif-Silverberg’21]: Commuting unitaries

[Liu-Montgomery-Zhandry’23]: Walkable invariants

[Zhandry’23]: Abelian group actions

Security from a well-studied assumption

[Zhandry’19]: Post-quantum iO

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

This work: Pre-action secure groups

A generic recipe for quantum lightning

Ingredients:

1. A collection of subspaces $\{\Pi_i\}$.
2. An initial state $|\mathrm{init}\rangle$ 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:

1. A collection of subspaces $\{\Pi_i\}$.

Invariant subspaces of a group.

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

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

Group actions

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

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

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

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

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!

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

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!

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

We call these irrep labels

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!

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

We call V the quantum Fourier transform

We call these irrep labels

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:

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

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

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

Quantum lightning from group actions

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

- 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 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

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.

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

- 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.

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

Quantum lightning from group actions

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

- Prepare a uniform superposition over group elements.

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

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

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

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

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 $\mathrm{Extract} \cdot |\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$.

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 $\mathrm{Extract} \cdot |\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$.
3. Two operators L and R such that:

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

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:

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.

Going back to dirty fixed point testing

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

Going back to dirty fixed point testing

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

The reason we need to consider "dirty" fixed point testing is exactly because performing the group action will move our state around inside the (λ, i) subspace.

Going back to dirty fixed point testing

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

The reason we need to consider "dirty" fixed point testing is exactly because performing the group action will move our state around inside the (λ, i) subspace.

Implementing the Extract becomes a problem we call "Fourier extraction", and is interesting in it's own right!

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.