Quantum State Group Actions

Saachi Mutreja (Columbia)
Mark Zhandry (NTT Research and Stanford University)

Cryptographic Groups

- A pair $(G, \star)$ consisting of a set G and a binary operation $\star : G \times G \to G$ is an abelian group if the following properties hold:
  - Identity: $\exists e \in G : e \star a = a \star e = a, \forall a \in G$.
  - Inverse: $\forall a \in G, \exists b : b \star a = a \star b = e$.
  - Associativity: $(a \star b) \star c = a \star (b \star c)$
  - Commutativity: $a \star b = b \star a$

Cryptographic Groups

- A pair $(\mathbb{G}, \star)$ consisting of a set $\mathbb{G}$ and a binary operation $\star : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ is an abelian group if the following properties hold:
  - Identity: $\exists e \in G : e \star a = a \star e = a, \forall a \in G$.
  - Inverse: $\forall a \in G, \exists b : b \star a = a \star b = e$.
  - Associativity: $(a \star b) \star c = a \star (b \star c)$
  - Commutativity: $a \star b = b \star a$

- [Diffie-Hellman '76]: Hardness assumptions on (cyclic) groups $\mathbb{G}$.
  - Discrete log: $g, g^a \to a$
  - CDH: $g, g^a, g^b \to g^{ab}$
  - DDH: g, g^a, g^b, g^{ab} vs g, g^a, g^b, g^c

Quantum Computers break Cryptographic Groups

- Finding discrete log is easy:

Suppose $h = g^a$, want to find a

Define $F(x, y) = g^x h^y$

F is periodic: $F((x, y) + (-a, 1)) = F(x, y)$

Thm [Shor'94]: Quantum algorithms can easily find periods

Quantum Computers break Cryptographic Groups

- Finding discrete log is easy:

Suppose $h = g^a$, want to find a

Define $F(x, y) = g^x h^y$

F is periodic: $F((x, y) + (-a, 1)) = F(x, y)$

Thm [Shor'94]: Quantum algorithms can easily find periods

How can we use group-theoretic problems in a quantum secure manner?

Cryptographic Group *Actions* [Brassard-Yung'91]

- (Abelian) group $\mathbb{G}$ acting on set X via an action $\star$.

  - Identity:

    If e is identity in $\mathbb{G}$, then $e \star x = x, \forall x \in X$.

  - Compatibility:

    $$g \star (h \star x) = (g \cdot h) \star x,\ \forall g, h \in \mathbb{G}, \forall x \in X.$$

Cryptographic Group *Actions* [Brassard-Yung'91]

- (Abelian) group $\mathbb{G}$ acting on set X via an action $\star$.

  - Identity:

    If e is identity in $\mathbb{G}$, then $e \star x = x, \forall x \in X$.

  - Compatibility:

    $$g \star (h \star x) = (g \cdot h) \star x,\ \forall g, h \in \mathbb{G}, \forall x \in X.$$

  - Discrete log:

    $$(x, g \star x) \rightarrow g$$

  - Groups are a special case of group actions:

    $\mathbb{Z}_p$ acts on $\mathbb{G}$ via $a \star x = x^a$.

Understanding the security of Group Actions

Justifying security in classical group + classical attack

↓

Prove security under hardness of some computational problem on group.

↓

Justify hardness of the problem. (Can be justified in the *generic black box model*)

Understanding the security of Group Actions

Justifying security in classical group action + quantum attack

↓

Prove security under hardness of some computational problem on group action.

↓

Justify hardness of the problem?

[EH00,EHK04]:

- there exist algorithms w/ polynomial query complexity (but super poly run time) that break crypto assumptions on GAs.

Understanding the security of Group Actions

Justifying security in classical group action + quantum attack

↓

Prove security under hardness of some computational problem on group.

↓

Justify hardness of the problem?

[EH00,EHK04]:

- there exist algorithms w/ polynomial query complexity (but super poly run time) that break crypto assumptions on GAs.
- Unconditional lower bounds not possible!

Prove unconditional hardness for similar assumptions on ***Quantum State Group Actions.***

Quantum State Group Actions

- A quantum state group action will consist of:
    - A classical group action $(\mathbb{G}, X, \star)$.
    - A collection of states $\psi = (|\psi_x> \in \mathscr{H})_{x \in X}$.
    - Distinguished starting element $x_* \in X$.
    - QPT procedure Start: produces $|\psi_{x_*}>$.
    - QPT procedure Act $(g \in \mathbb{G}, |\psi_x> \in \mathscr{H})$ produces $|\psi_{g \star x}> = g \star |\psi_x>$.

Quantum State Group Actions

- A quantum state group action will consist of:
  - A classical group action $(\mathbb{G}, X, \star)$.
  - A collection of states $\psi = (|\psi_x>)_{x \in X}$.
  - Distinguished starting element $x_* \in X$.
  - QPT procedure <u>Start:</u> produces $|\psi_{x_*}>$.
  - QPT procedure <u>Act</u> $(g \in \mathbb{G}, |\psi_x> \in \mathscr{H})$ produces $|\psi_{g\star x}> = g \star |\psi_x>$.

- Assume:
  - $(g, x) \to (g \star x, x)$ is a bijection.

Quantum State Group Actions

- A quantum state group action will consist of:
  - A classical group action $(\mathbb{G}, X, \star)$.
  - A collection of states $\psi = (|\psi_x>)_{x \in X}$.
  - Distinguished starting element $x_* \in X$.
  - QPT procedure <u>Start:</u> produces $|\psi_{x_*}>$.
  - QPT procedure <u>Act</u> $(g \in \mathbb{G}, |\psi_x> \in \mathscr{H})$ produces $|\psi_{g \star x}> = g \star |\psi_x>$.

- Assume:
  - $(g, x) \to (g \star x, x)$ is a bijection.
- Orthogonal if:
  - $\forall x, y \in X :< \psi_x | \psi_y > = 0.$

Quantum State Group Actions

- A quantum state group action will consist of:
  - A classical group action $(\mathbb{G}, X, \star)$.
  - A collection of states $\psi = (|\psi_x >)_{x \in X}$.
  - Distinguished starting element $x_* \in X$.
  - QPT procedure Start: produces $|\psi_{x_*} >$.
  - QPT procedure Act $(g \in \mathbb{G}, |\psi_x > \in \mathscr{H})$ produces $|\psi_{g \star x} > = g \star |\psi_x >$.

- Assume:
  - $(g, x) \to (g \star x, x)$ is a bijection.
- Orthogonal if:
  - $\forall x, y \in X :< \psi_x | \psi_y > = 0.$

- Remark: $|\psi_{g \star x_*} >$ is not necessarily clonable, hard problems on quantum group action parametrized by number of copies.

Quantum State Group Actions

- ℓ-DDH:

$$|\psi_a>^{\otimes \ell} |\psi_b>^{\otimes \ell} |\psi_{a+b}>^{\otimes \ell} \approx |\psi_a>^{\otimes \ell} |\psi_b>^{\otimes \ell} |\psi_c>^{\otimes \ell}$$

- ℓ- Discrete log:

$$\Pr[g \leftarrow \mathscr{A}(|\psi_{g \star x_*}>^{\otimes \ell})] \leq \text{negl}$$

Hard (without parametrization by ℓ) if ℓ-hard for all polynomials ℓ.

Quantum State Group Actions

- Generalized Matrix Problem (GMP):
    - Family of matrix assumptions parameterized by $M \in \mathbb{Z}_N^{n \times m}$.

Quantum State Group Actions

- <u>Generalized Matrix Problem (GMP):</u>
  - Family of matrix assumptions parameterized by $M \in \mathbb{Z}_N^{n \times m}$.
  - Consider
    - $\mathscr{D}_0$- output $|\psi_{g_1}>, \ldots |\psi_{g_n}>$, $g = (g_1, \ldots g_n) = M \cdot s, s \in \mathbb{Z}_N^m$.
    - $\mathscr{D}_1$- output $|\psi_{g_1}>, \ldots |\psi_{g_n}>$, $g = (g_1, \ldots g_n)$ is uniformly random.

$\mathscr{D}_0 \approx \mathscr{D}_1$, given M (not s, g).

Quantum State Group Actions

- Generalized Matrix Problem (GMP):
  - Family of matrix assumptions parameterized by $M \in \mathbb{Z}_N^{n \times m}$.
  - Consider
    - $\mathscr{D}_0$- output $|\psi_{g_1} > , \ldots |\psi_{g_n} >$, $g = (g_1, \ldots g_n) = M \cdot s, s \in \mathbb{Z}_N^m$.
    - $\mathscr{D}_1$- output $|\psi_{g_1} > , \ldots |\psi_{g_n} >$, $g = (g_1, \ldots g_n)$ is uniformly random.

$\mathscr{D}_0 \approx \mathscr{D}_1$, given M (not s, g).

  - DDH- special case of GMP with $M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$

Quantum State Group Actions

- Generalized Matrix Problem (GMP):
  - Family of matrix assumptions parameterized by $M \in \mathbb{Z}_N^{n \times m}$.
  - Consider
    - $\mathcal{D}_0$- output $|\psi_{g_1} > , \ldots |\psi_{g_n} >$, $g = (g_1, \ldots g_n) = M \cdot s, s \in \mathbb{Z}_N^m$.
    - $\mathcal{D}_1$- output $|\psi_{g_1} > , \ldots |\psi_{g_n} >$, $g = (g_1, \ldots g_n)$ is uniformly random.

$\mathcal{D}_0 \approx \mathcal{D}_1,$ given M (not s, g).

  - DDH- special case of GMP with $M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$
  - Linear Hidden Shift assumption: Generalizing GMP to non-uniform $s \in \{0,1\}^m$, uniformly random M.
  - Extended Linear Hidden Shift assumption: Generalizing GMP to structured M.

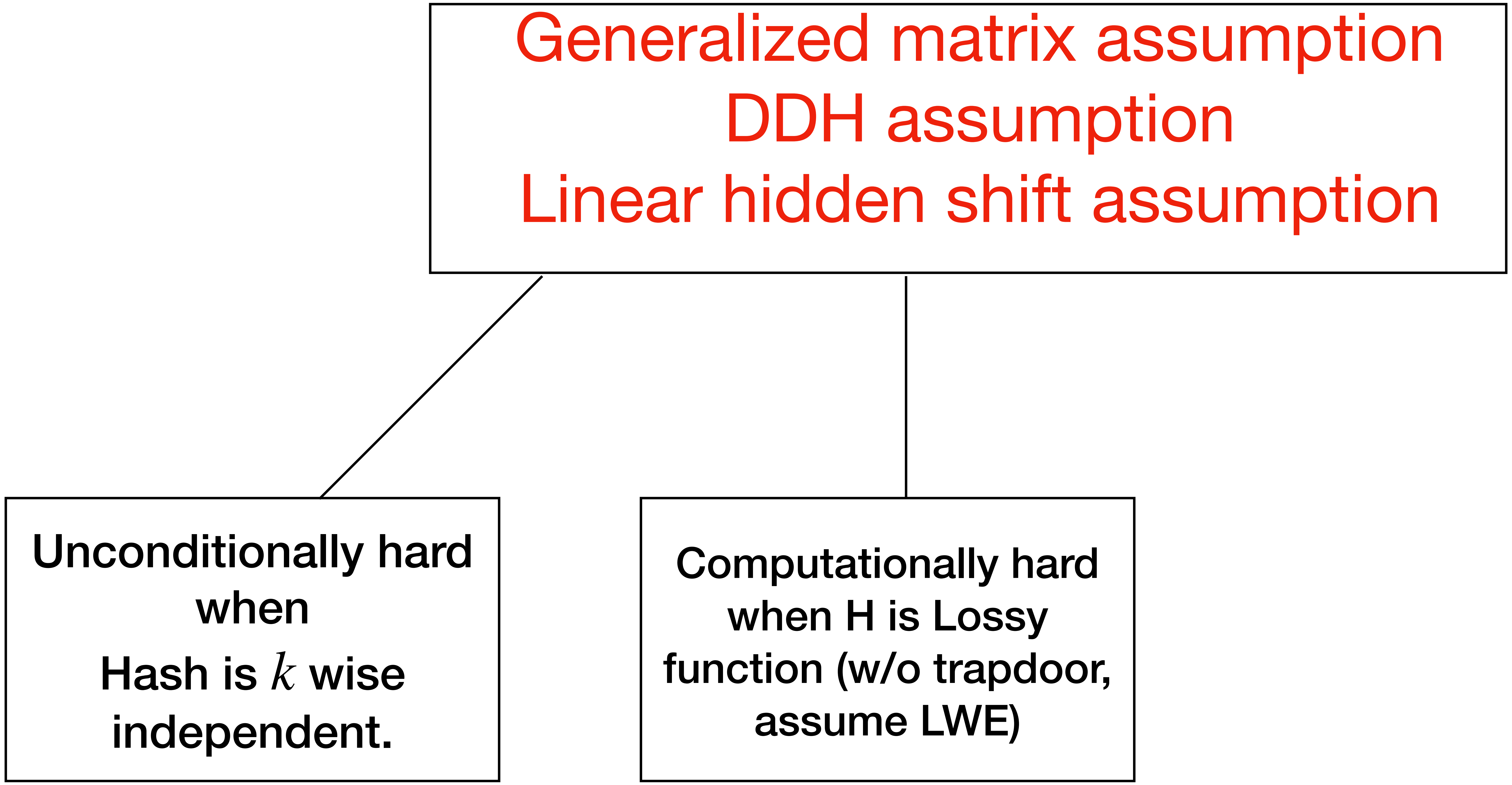
Main Results

- **A Hash based construction of Quantum State group actions**
  - Generalized matrix assumption
  - DDH assumption
  - Linear hidden shift assumption

Unconditionally hard when Hash is k wise independent.

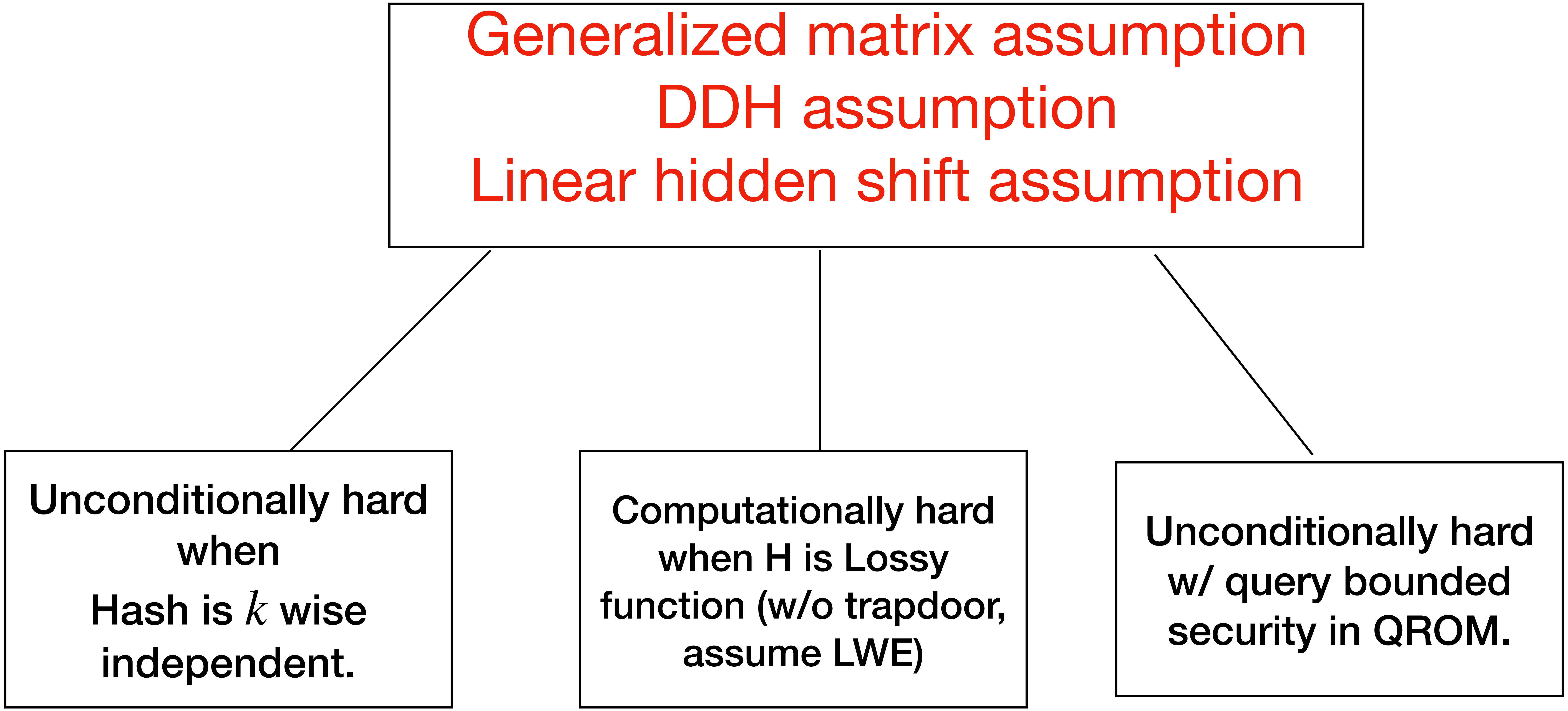
Main Results

- **A Hash based construction of Quantum State group actions**



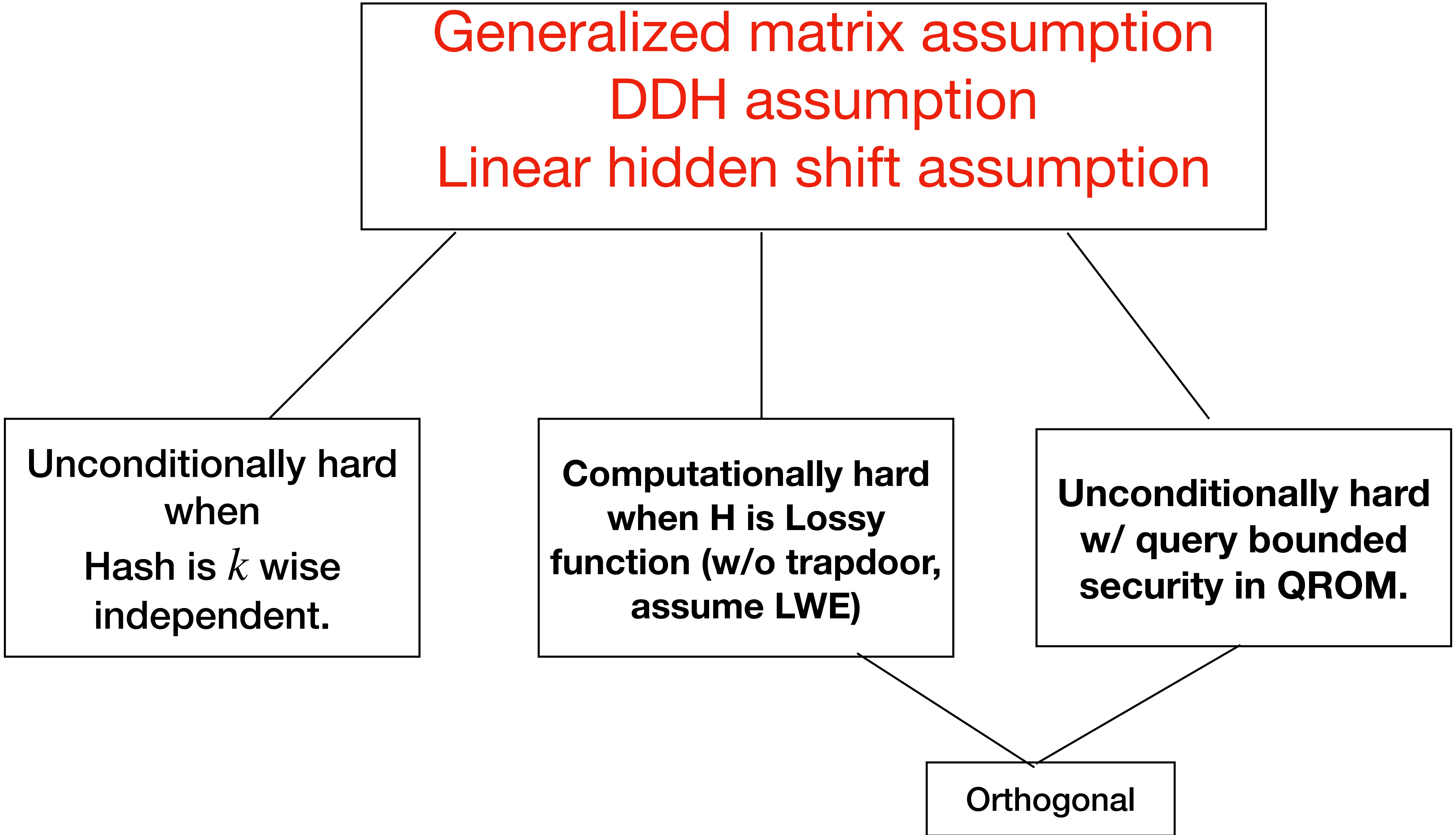
Main Results

- **A Hash based construction of Quantum State group actions**



Main Results

- **<u>A Hash based construction of Quantum State group actions</u>**



Main Results

- **An attack in the "many copy" regime:**
  - When hash based construction is *orthogonal:* **query bounded , computationally inefficient** quantum coset sampling attacks [EH00, EHK04] on classical group actions generalize given multiple copies.

Main Results

- **Unifying Quantum Money:**

- [Zha24]: constructed Quantum Money from abelian GA.

Generalize construction to quantum state group actions **+** instantiate w/ Hash based construction

↓

[Zha19]: Quantum Money construction from non collapsing hash functions.

Hash Based Quantum State Group Action

- Ingredients: $H : R \to \mathbb{Z}_N$, $|\phi>$: efficiently constructible state, superposition over elements in R.

Hash Based Quantum State Group Action

- Ingredients: $H : R \to \mathbb{Z}_N$, $|\phi>$: efficiently constructible state, superposition over elements in R.

    - Underlying classical group action: $\mathbb{G} = X = \mathbb{Z}_N$, with $g \star x = g + x$.

Hash Based Quantum State Group Action

- Ingredients: $H : R \to \mathbb{Z}_N$, $|\phi>$: efficiently constructible state, superposition over elements in R.
    - Underlying classical group action: $\mathbb{G} = X = \mathbb{Z}_N$, with $g \star x = g + x$.
    - Start: create state $|\phi>$.
    - Act ($g \in \mathbb{Z}_N$, $|\psi> = \sum_{r \in R} \alpha_r |r>$): $P_g|\psi>$, $P_g : |r> \to \omega_N^{g \cdot H(r)}|r>$

Hash Based Quantum State Group Action

- Ingredients: $H : R \to \mathbb{Z}_N$, $|\phi>$: efficiently constructible state, superposition over elements in R.

  - Underlying classical group action: $\mathbb{G} = X = \mathbb{Z}_N$, with $g \star x = g + x$.

  - Start: create state $|\phi>$.

  - Act $(g \in \mathbb{Z}_N, |\psi> = \sum_{r \in R} \alpha_r |r>)$: $P_g|\psi>, P_g : |r> \to \omega_N^{g \cdot H(r)}|r>$

$$= \sum_{r \in R} \alpha_r \omega_N^{g \cdot H(r)} |r>$$

Hash Based Quantum State Group Action

- Ingredients: $H : R \to \mathbb{Z}_N$, $|\phi>$: efficiently constructible state, superposition over elements in R.

  - Underlying classical group action: $\mathbb{G} = X = \mathbb{Z}_N$, with $g \star x = g + x$.

  - Start: create state $|\phi>$.

  - Act $(g \in \mathbb{Z}_N, |\psi> = \sum_{r \in R} \alpha_r |r>)$: $P_g |\psi>$, $P_g : |r> \to \omega_N^{g \cdot H(r)} |r>$

$$= \sum_{r \in R} \alpha_r \omega_N^{g \cdot H(r)} |r>$$

  - $P_g P_h = P_{g+h}$ (additive notion for group operation).

Hash Based Quantum State Group Action

- Proving DDH security of hash based construction:

$$|\psi_{g_1}>|\psi_{g_2}>|\psi_{g_1+g_2}> =$$

Hash Based Quantum State Group Action

- Proving DDH security of hash based construction:

$$|\psi_{g_1}>|\psi_{g_2}>|\psi_{g_1+g_2}> =$$

$$\sum_x \omega_N^{H(x)\cdot g_1}|x> \sum_y \omega_N^{H(y)\cdot g_2}|y> \sum_z \omega_N^{H(z)\cdot (g_1+g_2)}|z>$$

Hash Based Quantum State Group Action

- Proving DDH security of hash based construction:

$$|\psi_{g_1}>|\psi_{g_2}>|\psi_{g_1+g_2}> =$$

$$\sum_x \omega_N^{H(x)\cdot g_1}|x>\sum_y \omega_N^{H(y)\cdot g_2}|y>\sum_z \omega_N^{H(z)\cdot(g_1+g_2)}|z> =$$

$$\sum_{x,y,z} \omega_N^{H(x)\cdot g_1+H(y)\cdot g_2+H(z)\cdot(g_1+g_2)}|x,y,z>$$

Hash Based Quantum State Group Action

- Proving DDH security of hash based construction:

$$|\psi_{g_1}> |\psi_{g_2}> |\psi_{g_1+g_2}> =$$

$$\sum_x \omega_N^{H(x)\cdot g_1} |x> \sum_y \omega_N^{H(y)\cdot g_2} |y> \sum_z \omega_N^{H(z)\cdot (g_1+g_2)} |z> =$$

$$\sum_{x,y,z} \omega_N^{H(x)\cdot g_1 + H(y)\cdot g_2 + H(z)\cdot (g_1+g_2)} |x, y, z> =$$

$$\sum_{x,y,z} \omega_N^{(H(x)+H(z))\cdot g_1 + (H(y)+H(z))\cdot g_2} |x, y, z>$$

Hash Based Quantum State Group Action

- Proving DDH security of hash based construction:

$$|\psi_{g_1}>|\psi_{g_2}>|\psi_{g_1+g_2}> =$$

$$\sum_{x,y,z} \omega_N^{H(x)\cdot g_1 + H(y)\cdot g_2 + H(z)\cdot (g_1+g_2)} |x, y, z>$$

$$|\psi_{g_1}>|\psi_{g_2}>|\psi_{g_3}> =$$

$$\sum_{x,y,z} \omega_N^{H(x)\cdot g_1 + H(y)\cdot g_2 + H(z)\cdot g_3} |x, y, z>$$

Hash Based Quantum State Group Action

- Proving DDH security of hash based construction:

$$|\psi_{g_1}> |\psi_{g_2}> |\psi_{g_1+g_2}> = \sum_{x,y,z} \omega_N^{H(x)\cdot g_1+H(y)\cdot g_2+H(z)\cdot(g_1+g_2)} |x, y, z>$$

$$|\psi_{g_1}> |\psi_{g_2}> |\psi_{g_3}> = \sum_{x,y,z} \omega_N^{H(x)\cdot g_1+H(y)\cdot g_2+H(z)\cdot g_3} |x, y, z>$$

Averaging over choice of g_1, g_2, g_3- resulting mixed states close if:

- $f'(x, y, z) = (H(x), H(y), H(z))$ and
- $f(x, y, z) = (H(x) + H(z), H(y) + H(z))$

are almost injective.

Unifying Quantum Money

[Zha24] Q-Money Scheme from abelian group actions.

$$\sum_{g\in\mathbb{G}} |g\rangle$$

$\downarrow *$

$$\sum_{g\in\mathbb{G}} |g, g * x\rangle$$

$\downarrow$ QFT

$$\sum_{g,h\in\mathbb{G}} e^{i2\pi gh/N} |h, g * x\rangle$$

$h =$ Serial #

$$\$ \propto \sum_{g} e^{i2\pi gh/N} |g * x\rangle$$

Unifying Quantum Money

Plugging in hash-based quantum state group action:

$$|\$_h> = \sum_g \omega_N^{gh} |\psi_{g\star x_*}>$$

$$\downarrow$$

$$\sum_r \alpha_r \omega_N^{g\cdot H(r)} |r>$$

Unifying Quantum Money

Plugging in hash-based quantum state group action:

$$|\$_h> = \sum_g \omega_N^{gh} |\psi_{g \star x_*}> = \sum_{g,x} \omega_N^{gh+gH(x)} |x>$$

Unifying Quantum Money

Plugging in hash-based quantum state group action:

$$|\$_h> = \sum_g \omega_N^{gh} |\psi_g> = \sum_{g,x} \omega_N^{gh+gH(x)} |x>$$

zero's out every term w/ $h + H(x) \neq 0$!

Unifying Quantum Money

Plugging in hash-based quantum state group action:

$$|\$_h> = \sum_g \omega_N^{gh} |\psi_g> = \sum_{g,x} \omega_N^{gh+gH(x)} |x>$$

zero's out every term w/ $h + H(x) \neq 0$!

$$= \sum_{x:H(x)=-h} |x>$$

Unifying Quantum Money

Plugging in hash-based quantum state group action:

$$|\$_h> = \sum_g \omega_N^{gh} |\psi_g> = \sum_{g,x} \omega_N^{gh+gH(x)} |x>$$

zero's out every term w/ $h + H(x) \neq 0$!

$$= \sum_{x:H(x)=-h} |x>$$

↓

Money state from [Zha19] with non collapsing CRHF H.