Generic Models for Group Actions

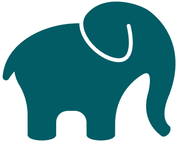
Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, Doreen Riepel

Ruhr University Bochum

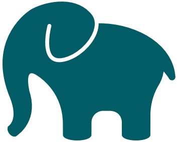
May 8th, 2023

Post-Quantum Cryptography

Post-Quantum Cryptography

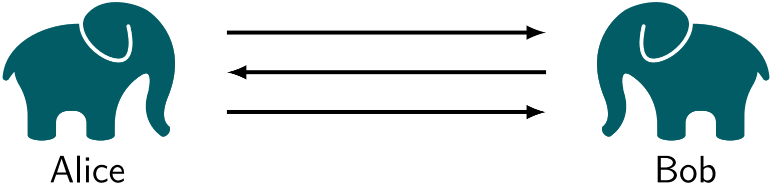


Alice

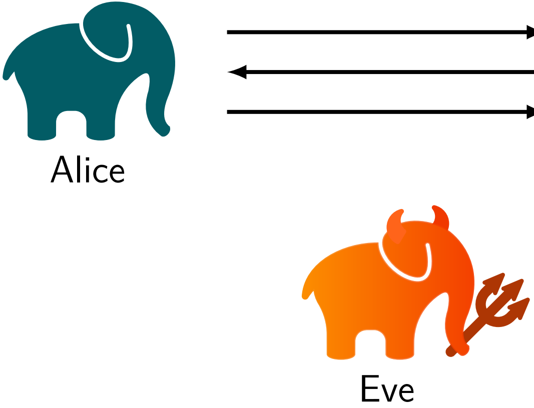


Bob

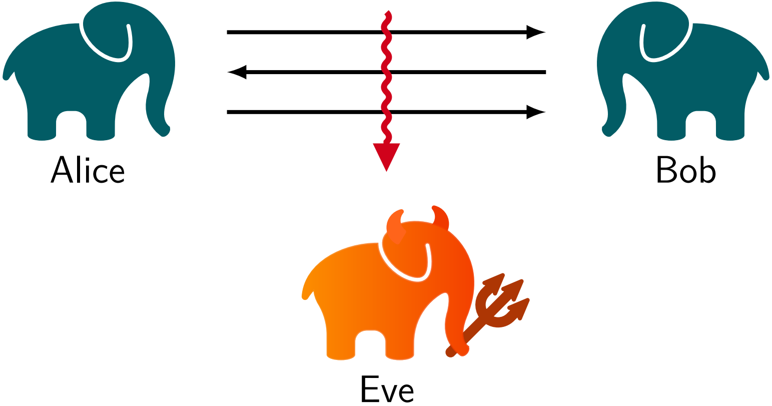
Post-Quantum Cryptography



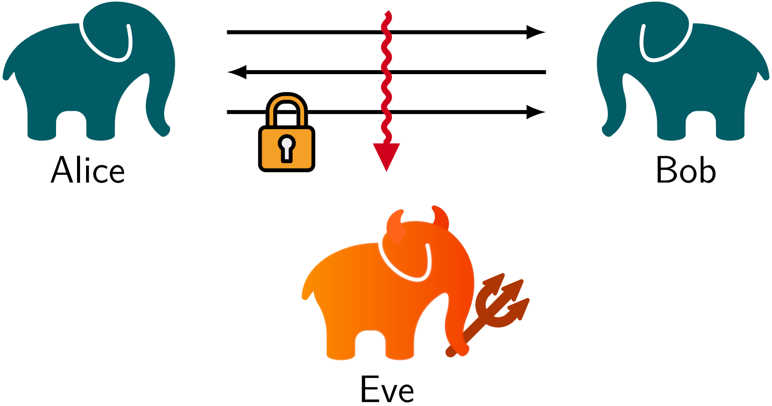
Post-Quantum Cryptography



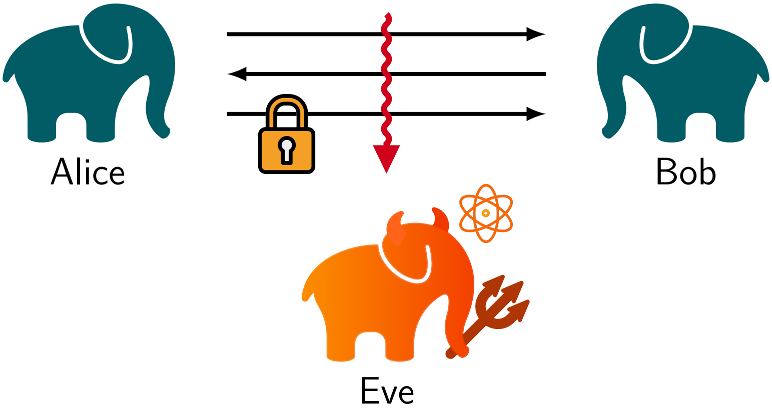
Post-Quantum Cryptography



Post-Quantum Cryptography



Post-Quantum Cryptography



Post-Quantum Cryptography

Post-Quantum Cryptography

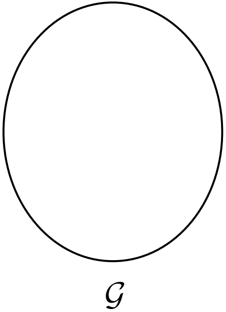
- Existing constructions mostly based on **lattices**

Post-Quantum Cryptography

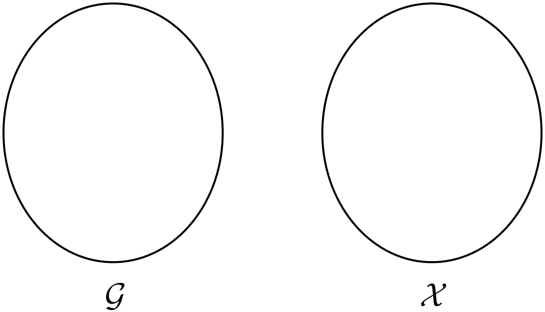
- Existing constructions mostly based on **lattices**
- Popular alternative: Cryptographic Group Actions
  - Based on **isogenies**

Group Actions

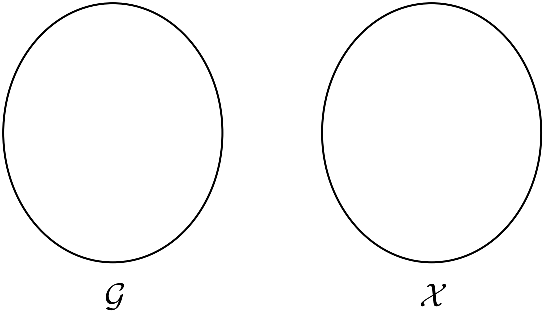
Group Actions



Group Actions

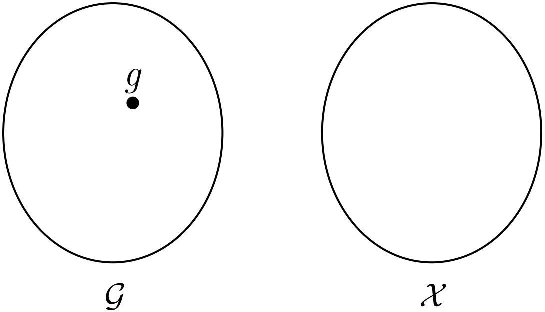


Group Actions



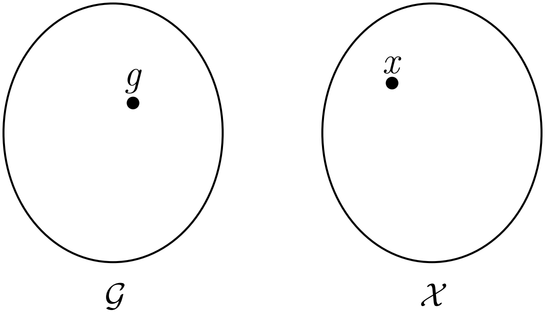
$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

Group Actions



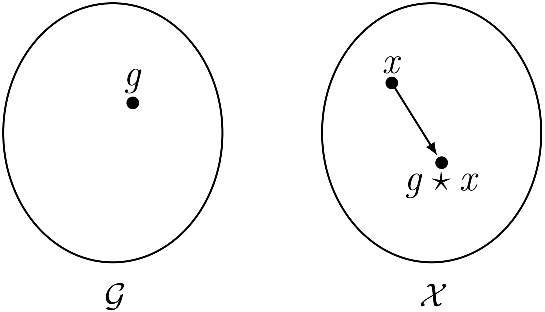
$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

Group Actions



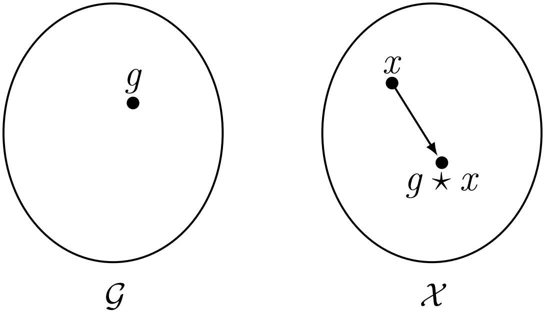
$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

Group Actions



$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

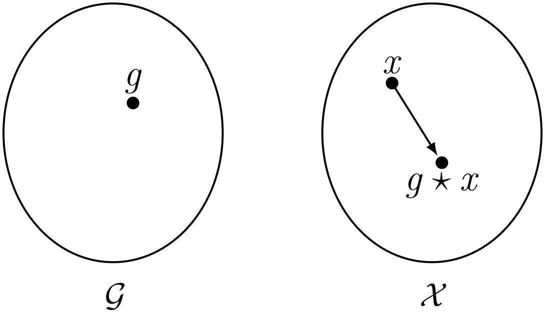
Group Actions



- Identity:
  $e \star x = x$

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

Group Actions



$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

- Identity:
  $e \star x = x$
- Compatibility:
  $g \star (h \star x) = (g + h) \star x$

Standard Group Action Assumptions

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

Standard Group Action Assumptions

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

DLOG

Given x and $g \star x$ compute g.

Standard Group Action Assumptions

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

DLOG

Given x and $g \star x$ compute g.

CDH

Given x, $g \star x$ and $h \star x$ compute $(g + h) \star x$.

Standard Group Action Assumptions

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

DLOG

Given x and $g \star x$ compute g.

CDH

Given x, $g \star x$ and $h \star x$ compute $(g + h) \star x$.

DDH

Given x, $g \star x$, $h \star x$ and z decide if $z = (g + h) \star x$

Standard Group Action Assumptions

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

DLOG

Given x and $g \star x$ compute g.

CDH

Given x, $g \star x$ and $h \star x$ compute $(g + h) \star x$.

DDH

Given x, $g \star x$, $h \star x$ and z decide if $z = (g + h) \star x$

Quantum Hardness

Kuperberg (subexponential)

Non-Standard Group Action Assumptions

Non-Standard Group Action Assumptions

Strong CDH

Non-Standard Group Action Assumptions

Strong CDH

Given x, $g \star x$, $h \star x$ compute $(g+h) \star x$

Non-Standard Group Action Assumptions

Strong CDH

Given x, $g \star x$, $h \star x$ compute $(g+h) \star x$ while having access to oracles

$$\mathsf{DDH}(g \star x, \cdot, \cdot) \qquad \text{and} \qquad \mathsf{DDH}(h \star x, \cdot, \cdot).$$

Non-Standard Group Action Assumptions

Strong CDH

Given x, $g \star x$, $h \star x$ compute $(g + h) \star x$ while having access to oracles

$$\text{DDH}(g \star x, \cdot, \cdot) \qquad \text{and} \qquad \text{DDH}(h \star x, \cdot, \cdot).$$

- Underlies the security of the CSIDH key exchange [DHK+22]

Non-Standard Group Action Assumptions

Strong Square Inverse CDH

Non-Standard Group Action Assumptions

Strong Square Inverse CDH

Given x, $g \star x$ compute a tuple $(y, 2g \star y, -g \star y)$

Non-Standard Group Action Assumptions

Strong Square Inverse CDH

Given x, $g \star x$ compute a tuple $(y, 2g \star y, -g \star y)$ while having access to oracles

$$\mathsf{DDH}(g \star x, \cdot, \cdot) \qquad \text{and} \qquad \mathsf{DDH}(2g \star x, \cdot, \cdot).$$

Non-Standard Group Action Assumptions

Strong Square Inverse CDH

Given x, $g \star x$ compute a tuple $(y, 2g \star y, -g \star y)$ while having access to oracles

$$\mathsf{DDH}(g \star x, \cdot, \cdot) \qquad \text{and} \qquad \mathsf{DDH}(2g \star x, \cdot, \cdot).$$

- Underlies the security of group action based PAKE [AEK+22] and oblivious transfer [LGd21]

Non-Standard Group Action Assumptions

Strong Square Inverse CDH

Given x, $g \star x$ compute a tuple $(y, 2g \star y, -g \star y)$ while having access to oracles

$$\mathsf{DDH}(g \star x, \cdot, \cdot) \qquad \text{and} \qquad \mathsf{DDH}(2g \star x, \cdot, \cdot).$$

- Underlies the security of group action based PAKE [AEK$^+$22] and oblivious transfer [LGd21]

Quantum Hardness

Unclear

This Work

This Work

- Define the **generic** group action model

This Work

- Define the **generic** group action model
  - Lifting Lemma: GGAM $\subset$ GGM under certain conditions

This Work

- Define the **generic** group action model
  - Lifting Lemma: GGAM $\subset$ GGM under certain conditions
  - Classical lower bounds for DLOG, CDH $\ldots$

This Work

- Define the **generic** group action model
  - Lifting Lemma: GGAM $\subset$ GGM under certain conditions
  - Classical lower bounds for DLOG, CDH . . .
  - Impossibility of *quantum* lower bounds

This Work

- Define the **generic** group action model
  - Lifting Lemma: GGAM $\subset$ GGM under certain conditions
  - Classical lower bounds for DLOG, CDH ...
  - Impossibility of *quantum* lower bounds
- Define the **algebraic** group action model

This Work

- Define the **generic** group action model
  - Lifting Lemma: GGAM $\subset$ GGM under certain conditions
  - Classical lower bounds for DLOG, CDH . . .
  - Impossibility of *quantum* lower bounds
- Define the **algebraic** group action model
  - *Classical* and *quantum* reductions between (non-standard) assumptions and DLOG

Generic Group Action Model

Generic Group Action Model

$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

Generic Group Action Model

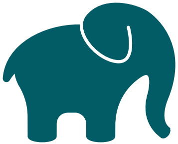
$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$

Generic Group Action Model

$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

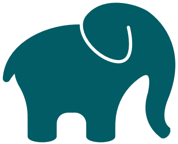
Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$



Generic Group Action Model

$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$

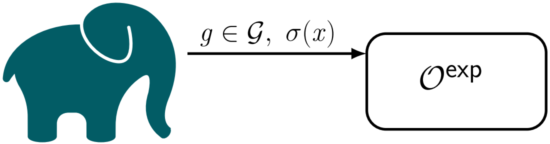


$\mathcal{O}^{\mathsf{exp}}$

Generic Group Action Model

$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

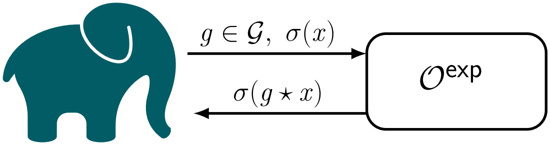
Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$



Generic Group Action Model

$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

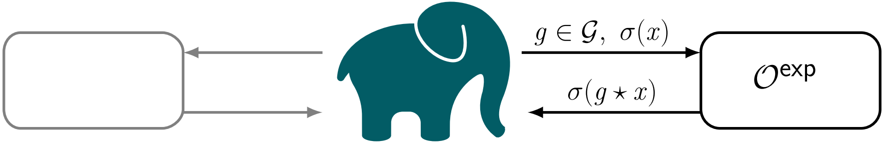
Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$



Generic Group Action Model

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}, \text{ labeling function } \sigma : \mathcal{X} \to \{0,1\}^n$$

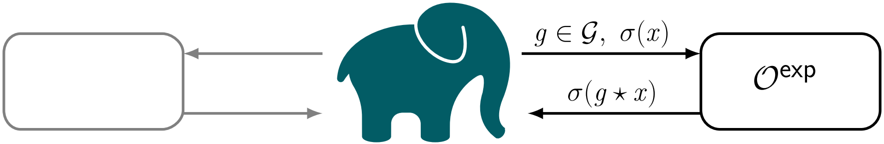
Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$



Generic Group Action Model

$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$

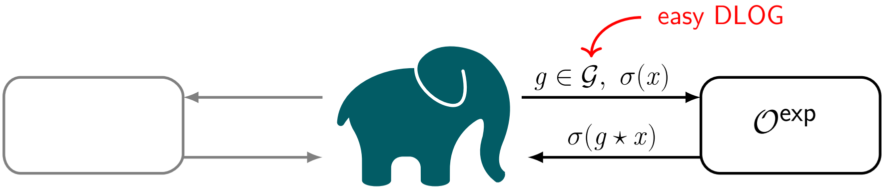


Runtime measured in # oracle queries

Generic Group Action Model

$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, labeling function $\sigma : \mathcal{X} \to \{0,1\}^n$

Generic Group Action $\star : \mathcal{G} \times \{0,1\}^n \to \{0,1\}^n$



Runtime measured in # oracle queries

GGM vs. GGAM

Lemma (Lifting Lemma)

If $|\mathcal{G}| + 1$ *is prime then the GGM contains the GGAM.*

GGM vs. GGAM

Lemma (Lifting Lemma)

If $|\mathcal{G}|+1$ *is prime then the GGM contains the GGAM.*

$\Rightarrow$ In GGM exponents are **multiplicative** instead of **additive**.

GGM vs. GGAM

Lemma (Lifting Lemma)

If $|\mathcal{G}| + 1$ is prime then the GGM contains the GGAM.

$\Rightarrow$ In GGM exponents are **multiplicative** instead of **additive**.

Corollary

If $|\mathcal{G}| + 1$ is prime then for a DLOG *adversary $\mathcal{A}$ in the GGAM*

$$\epsilon \leq q^2/N.$$

GGM vs. GGAM

Lemma (Lifting Lemma)

If $|\mathcal{G}| + 1$ is prime then the GGM contains the GGAM.

$\Rightarrow$ In GGM exponents are **multiplicative** instead of **additive**.

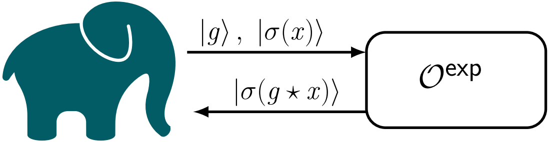
Corollary

~~*If $|\mathcal{G}| + 1$ is prime then*~~ *for a* DLOG *adversary $\mathcal{A}$ in the GGAM*

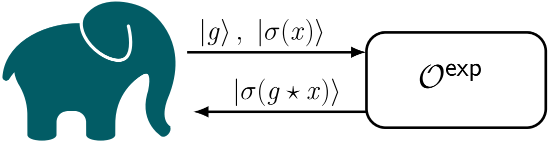
$$\epsilon \leq \mathcal{O}(q^2/N).$$

Quantum GGAM

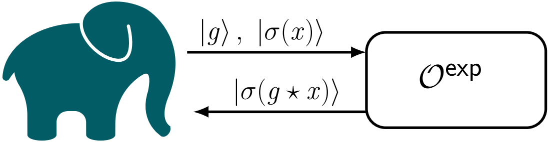
Quantum GGAM



Quantum GGAM



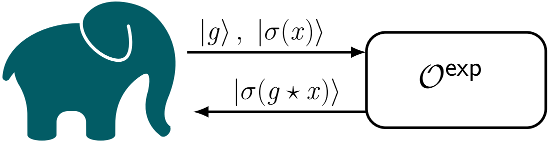
Ettinger-Høyer:



Ettinger-Høyer:

- **Generic** quantum algorithm solving DLOG

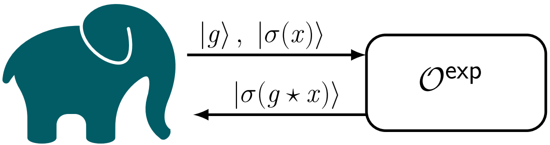
Quantum GGAM



Ettinger-Høyer:

- **Generic** quantum algorithm solving DLOG
- Polynomial **oracle** complexity

Quantum GGAM



Ettinger-Høyer:

- **Generic** quantum algorithm solving DLOG
- Polynomial **oracle** complexity

$\Rightarrow$ Not even DLOG is hard

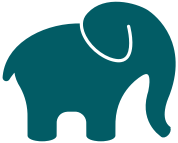
Algebraic Group Action Model

Quantum Algebraic Group Action Model

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$

Quantum Algebraic Group Action Model

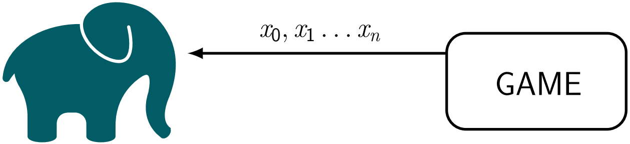
$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$



GAME

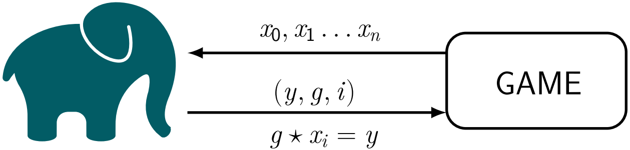
Quantum Algebraic Group Action Model

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$



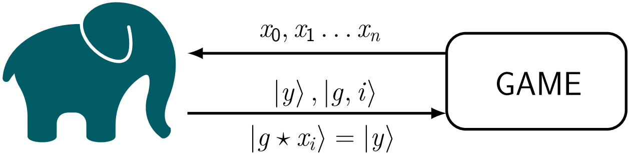
Quantum Algebraic Group Action Model

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$



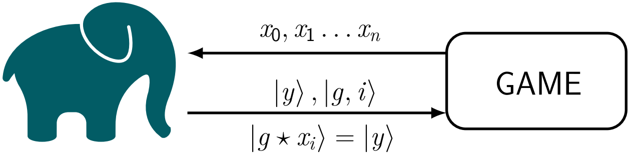
Quantum Algebraic Group Action Model

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$



Quantum Algebraic Group Action Model

$$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$$



Runtime measured in # unit operations

Results in the QAGAM

Results in the QAGAM

Strong CDH (St-CDH)

Given x, $g \star x$, $h \star x$ compute $(g + h) \star x$ while having access to oracles

$$\mathsf{DDH}(g \star x, \cdot, \cdot) \qquad \text{and} \qquad \mathsf{DDH}(h \star x, \cdot, \cdot).$$

Results in the QAGAM

Strong CDH (St-CDH)

Given x, $g \star x$, $h \star x$ compute $(g+h) \star x$ while having access to oracles

$$\mathrm{DDH}(g \star x, \cdot, \cdot) \qquad \text{and} \qquad \mathrm{DDH}(h \star x, \cdot, \cdot).$$

Theorem (DLOG $\Rightarrow$ St-CDH)

For every ***quantum*** *adversary $\mathcal{A}$ in the* ***quantum algebraic*** *group action model against* St-CDH *there exists $\mathcal{B}, \mathcal{C}$ against* DLOG *with*

$$\epsilon_{\mathcal{A}} \leq \sqrt{(q+1) \cdot \epsilon_{\mathcal{B}}} + \epsilon_{\mathcal{C}}.$$

Summary

- Adapted the GGM and AGM to the group action setting.
  - Include further algebraic properties of isogenies like **twists**.
- Proved information-theoretic lower bounds in the **generic** group action model.
- Gave algebraic reductions between non-standard assumptions and DLOG in the **algebraic** group action model.

https://ia.cr/2023/186

References I

[AEK+22] Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel. Password-authenticated key exchange from group actions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 699–728. Springer, Heidelberg, August 2022.

[DHK+22] Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, and Doreen Riepel. Group action key encapsulation and non-interactive key exchange in the QROM. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part II*, volume 13792 of *LNCS*, pages 36–66. Springer, Heidelberg, December 2022.

[LGd21] Yi-Fu Lai, Steven D. Galbraith, and Cyprien de Saint Guilhem. Compact, efficient and UC-secure isogeny-based oblivious transfer. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 213–241. Springer, Heidelberg, October 2021.