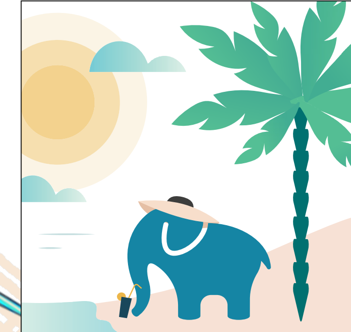


A Simpler and Tighter Reduction from DLog to CDH for Abelian Group Actions

la.cr/2024/191; PKC2024

Steven Galbraith, **Yi-Fu Lai,** Hart Montgomery

CASA / Ruhr-University Bochum
University of Auckland, Linux Foundation

Content

- Background
  - Group Actions
  - Assumptions: DLog and CDH
  - Quantum Equivalence of DLog and CDH
- Contributions
- Technical Overview
- Open Problems

Group Actions

Let G be a group and $\mathscr{E}$ be a set. We say G acts on $\mathscr{E}$ by an action $\star : G \times \mathscr{E} \to \mathscr{E}$ if

1. (Identity) $1 \star E = E$ for any $E \in \mathscr{E}$.

2. (Associativity) $a \star (b \star E) = (ab) \star E$

Group Actions

Let G be a group and $\mathscr{E}$ be a set. We say G acts on $\mathscr{E}$ by an action $\star : G \times \mathscr{E} \to \mathscr{E}$ if

1. (Identity) $1 \star E = E$ for any $E \in \mathscr{E}$.
2. (Associativity) $a \star (b \star E) = (ab) \star E$

We require the group to be abelian.

We further require regular (transitive and free) in this slides:

- For any $E_1, E_2 \in \mathscr{E}$, there exists a unique $g \in G$ s.t. $g \star E_1 = E_2$.

Group Actions

Let G be a group and $\mathscr{E}$ be a set. We say G acts on $\mathscr{E}$ by an action $\star : G \times \mathscr{E} \to \mathscr{E}$ if

1. (Identity) $1 \star E = E$ for any $E \in \mathscr{E}$.
2. (Associativity) $a \star (b \star E) = (ab) \star E$

We require the group to be abelian.

We further require regular (transitive and free) in this slides:

- For any $E_1, E_2 \in \mathscr{E}$, there exists a unique $g \in G$ s.t. $g \star E_1 = E_2$.

Group Actions

Let G be a group and $\mathscr{E}$ be a set. We say G acts on $\mathscr{E}$ by an action $\star : G \times \mathscr{E} \to \mathscr{E}$ if

1. (Identity) $1 \star E = E$ for any $E \in \mathscr{E}$.
2. (Associativity) $a \star (b \star E) = (ab) \star E$

We require the group to be abelian.

We further require regular (transitive and free) in this slides:

- For any $E_1, E_2 \in \mathscr{E}$, there exists a unique $g \in G$ s.t. $g \star E_1 = E_2$.

Also, say we have a (statistically uniform) sampling method over G and a distinguished element $E \in \mathscr{E}$.

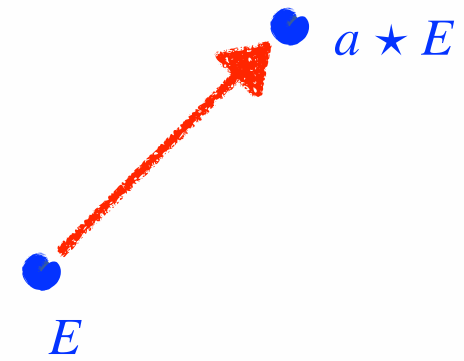
Applications

- Non-interactive Key Exchange: [AC: CLMRP18]
- PKE in standard model: [AC:MOT20] [PQC:BP21]
- Oblivious Transfer: [EC:LGD21] [PKC:BMM+23]
- PRF-
  - PRF: [AC:ADMP20] [AC:MOT20]
  - OPRF: [AC:BKW20] [PKC:DP24]
  - VRF: [Lai23]
- …etc
- Signature-
  - Signature Scheme: [EC:DG19], [AC:BKV19]
  - Linkable Ring Signature: [AC:BKP20]
  - Threshold Signature: [PKC:DM20]
  - Accountable Ring Signature; Group Signature: [EC:BDLKP22]
  - Blind Signature: [C:KLLQ23]

Assumptions: DLog and CDH

- **Group Action Inverse Problem (GAIP / DLog):**

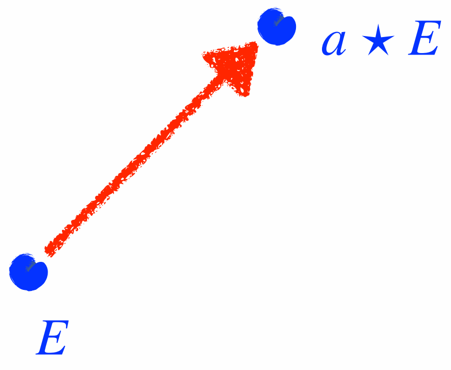
  Given $(E, a \star E)$, the goal is to recover a.



Assumptions: DLog and CDH

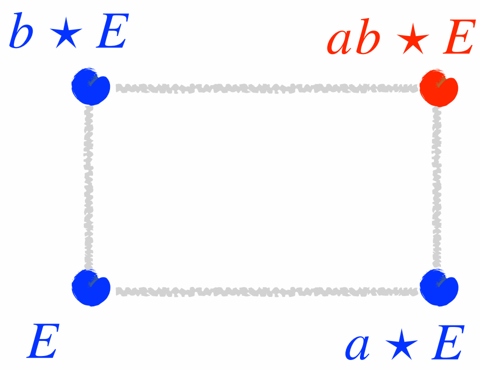
- **Group Action Inverse Problem (GAIP / DLog):**

  Given $(E, a \star E)$, the goal is to recover a.



- **Computational Diffie-Hellman Problem (CDH):**

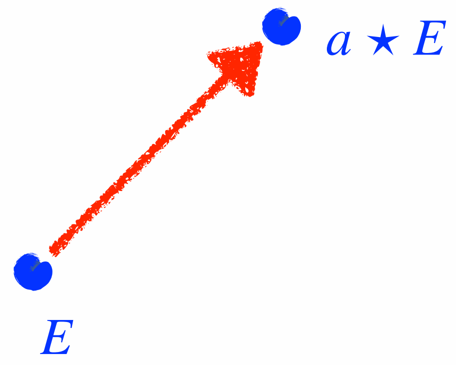
  Given $(E, a \star E, b \star E)$, the goal is to compute $ab \star E$.



Assumptions: DLog and CDH

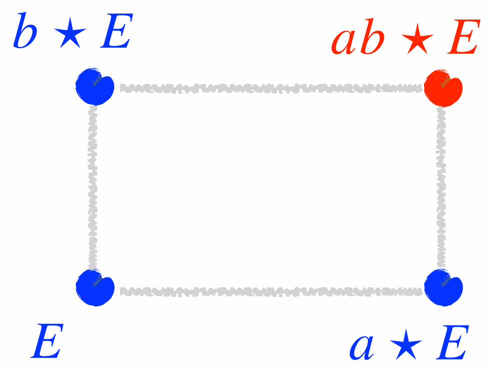
- **Group Action Inverse Problem (GAIP / DLog):**

  Given $(E, a \star E)$, the goal is to recover a.



- **Computational Diffie-Hellman Problem (CDH):**

  Given $(E, a \star E, b \star E)$, the goal is to compute $ab \star E$.



Obviously,

DLog $\geq$ CDH.

Is the reverse true?

Full Quantum Equivalence of DLog and CDH

Full Quantum Equivalence of DLog and CDH

- Galbraith, Panny, Smith, Vercauteren [GPSV18] gives a quantum algorithm (Shor's algorithm) solving DLog with $O\left(\log_2(|G|)\right)$ quantum queries to a perfect CDH oracle.

  ➡i.e. CDH oracle always outputs the correct answer.

Full Quantum Equivalence of DLog and CDH

- Galbraith, Panny, Smith, Vercauteren [GPSV18] gives a quantum algorithm (Shor's algorithm) solving DLog with $O\left(\log_2(|G|)\right)$ quantum queries to a perfect CDH oracle.

    ➡i.e. CDH oracle always outputs the correct answer.

What if the CDH oracle can only succeeds with a chance $\epsilon = 1/\text{poly}(\lambda)$,

Can we still have the reduction CDH $\geq$ DLog?

Full Quantum Equivalence of DLog and CDH

- Galbraith, Panny, Smith, Vercauteren [GPSV18] gives a quantum algorithm (Shor's algorithm) solving DLog with $O\left(\log_2(|G|)\right)$ quantum queries to a perfect CDH oracle.

  ➡i.e. CDH oracle always outputs the correct answer.

What if the CDH oracle can only succeeds with a chance $\epsilon = 1/\text{poly}(\lambda)$,

Can we still have the reduction CDH $\geq$ DLog?

- [AC:MZ22] gives an affirmative answer with a reduction using $\tilde{O}(\epsilon^{-21})$ queries to an imperfect CDH oracle.

Contributions

Contributions

- We give the following improvements:
  - a full black-box reduction of
  - $\mathcal{O}\left(\epsilon^{-4}\right)$ queries to the oracle using
  - simple math: a bunch of Chernoff bounds + group definition.

Content

- Background
  - Group Actions
  - Assumptions: DLog and CDH
  - Quantum Equivalence of DLog and CDH
- Contributions
- Technical Overview
- Open Problems

Self-randomized

- Throughout the slides, let's assume the oracle has been "self-randomized":

$$\mathcal{O}\left(a \star E, b \star E\right) := (r_1 r_2)^{-1} \star \mathcal{O}\left((r_1 a) \star E, (r_2 b) \star E\right).$$

where $r_1, r_2 \leftarrow_\$ G$.

▶ So the success rate will be independent to the input.

Easy Case

Easy Case

- If the error is "quite random" each time,

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ \text{a random set element (curve)}, & \text{with } 1 - \epsilon \end{cases}$$

then to amplify the success rate is easy by running $\mathcal{O}$ multiple times and output the majority.

Model: An Oracle w. Structured Errors

- [AC:MZ22] considers an imperfect oracle with *structured errors*.
- $\mathcal{O}$ is modeled as:

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\boxed{\delta_1} ab) \star E, & \text{with } \epsilon_1 \\ (\boxed{\delta_2} ab) \star E, & \text{with } \epsilon_2 \\ \vdots & \end{cases}$$

where $\delta_i \in G$ is some unknown group element (aka error).

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots & \end{cases}$$

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots & \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1' ab) \star E, & \text{with } \epsilon_1' \\ (\delta_2' ab) \star E, & \text{with } \epsilon_2' \\ \vdots & \end{cases}$$

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1' ab) \star E, & \text{with } \epsilon_1' \\ (\delta_2' ab) \star E, & \text{with } \epsilon_2' \\ \vdots \end{cases}$$

Let $x \star E$ be the DLog challenge.

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots & \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1' ab) \star E, & \text{with } \epsilon_1' \\ (\delta_2' ab) \star E, & \text{with } \epsilon_2' \\ \vdots & \end{cases}$$

Let $x \star E$ be the DLog challenge.

1. Sieving the oracle $\mathcal{O}$ into $\mathcal{O}'$ where the errors δ_i' are all in some SMALL subgroup S.
   - $\mathcal{O}^{\mathsf{Siv}}$ is a perfect CDH oracle on the group G/S acting on the set $\mathcal{X}/\{S \star E\}$.

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta'_1 ab) \star E, & \text{with } \epsilon'_1 \\ (\delta'_2 ab) \star E, & \text{with } \epsilon'_2 \\ \vdots \end{cases}$$

Let $x \star E$ be the DLog challenge.

1. Sieving the oracle $\mathcal{O}$ into $\mathcal{O}'$ where the errors δ'_i are all in some SMALL subgroup S.
   - $\mathcal{O}^{\mathsf{Siv}}$ is a perfect CDH oracle on the group G/S acting on the set $\mathcal{X}/\{S \star E\}$.
2. Apply [GPSV18] to solving DLog of $x \star E$ over $G/S \curvearrowright \mathcal{X}/\{S \star E\}$ and obtain xS.

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots & \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1' ab) \star E, & \text{with } \epsilon_1' \\ (\delta_2' ab) \star E, & \text{with } \epsilon_2' \\ \vdots & \end{cases}$$

Let $x \star E$ be the DLog challenge.

1. Sieving the oracle $\mathcal{O}$ into $\mathcal{O}'$ where the errors δ_i' are all in some SMALL subgroup S.
   - $\mathcal{O}^{\mathsf{Siv}}$ is a perfect CDH oracle on the group G/S acting on the set $\mathcal{X}/\{S \star E\}$.
2. Apply [GPSV18] to solving DLog of $x \star E$ over $G/S \curvearrowright \mathcal{X}/\{S \star E\}$ and obtain xS.
3. Retrieve x by enumerating elements in xS.

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1' ab) \star E, & \text{with } \epsilon_1' \\ (\delta_2' ab) \star E, & \text{with } \epsilon_2' \\ \vdots \end{cases}$$

ϵ^{-16}

Let $x \star E$ be the DLog challenge.

1. Sieving the oracle $\mathcal{O}$ into $\mathcal{O}'$ where the errors δ_i' are all in some SMALL subgroup S.
   - $\mathcal{O}^{\mathsf{Siv}}$ is a perfect CDH oracle on the group G/S acting on the set $\mathcal{X}/\{S \star E\}$.
2. Apply [GPSV18] to solving DLog of $x \star E$ over $G/S \curvearrowright \mathcal{X}/\{S \star E\}$ and obtain xS.
3. Retrieve x by enumerating elements in xS.

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1' ab) \star E, & \text{with } \epsilon_1' \\ (\delta_2' ab) \star E, & \text{with } \epsilon_2' \\ \vdots \end{cases}$$

ϵ^{-16}

ϵ^{-5}

Let $x \star E$ be the DLog challenge.

1. Sieving the oracle $\mathcal{O}$ into $\mathcal{O}'$ where the errors δ_i' are all in some SMALL subgroup S.
   - $\mathcal{O}^{\mathsf{Siv}}$ is a perfect CDH oracle on the group G/S acting on the set $\mathcal{X}/\{S \star E\}$.
2. Apply [GPSV18] to solving DLog of $x \star E$ over $G/S \curvearrowright \mathcal{X}/\{S \star E\}$ and obtain xS.
3. Retrieve x by enumerating elements in xS.

[MZ22]'s Strategy

$$\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots \end{cases}$$

$$\mathcal{O}^{\mathsf{Siv}}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1' ab) \star E, & \text{with } \epsilon_1' \\ (\delta_2' ab) \star E, & \text{with } \epsilon_2' \\ \vdots \end{cases}$$

ϵ^{-16}

Let $x \star E$ be the DLog challenge.

1. Sieving the oracle $\mathcal{O}$ into $\mathcal{O}'$ where the errors δ_i' are all in some SMALL subgroup S.

ϵ^{-5}

- $\mathcal{O}^{\mathsf{Siv}}$ is a perfect CDH oracle on the group G/S acting on the set $\mathcal{X}/\{S \star E\}$.

2. Apply [GPSV18] to solving DLog of $x \star E$ over $G/S \curvearrowright \mathcal{X}/\{S \star E\}$ and obtain xS.

3. Retrieve x by enumerating elements in xS.

ϵ^{-21}

The Main Idea in [AC:MZ22]

We have

$$\mathcal{O}(a \star E, b \star E) \sim \mathcal{O}(E, ab \star E).$$

$\langle proof \rangle$ By definition,

The Main Idea in [AC:MZ22]

We have

$$\mathcal{O}(a \star E, b \star E) \sim \mathcal{O}(E, ab \star E).$$

$\langle proof \rangle$ By definition,

1. $\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots & \end{cases}$

The Main Idea in [AC:MZ22]

We have

$$\mathcal{O}(a \star E, b \star E) \sim \mathcal{O}(E, ab \star E).$$

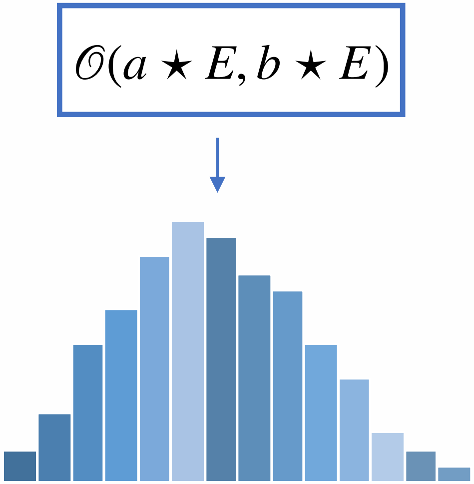
$\langle proof \rangle$ By definition,

1. $\mathcal{O}(a \star E, b \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots \end{cases}$

2. $\mathcal{O}(E, ab \star E) = \begin{cases} ab \star E, & \text{with } \epsilon \\ (\delta_1 ab) \star E, & \text{with } \epsilon_1 \\ (\delta_2 ab) \star E, & \text{with } \epsilon_2 \\ \vdots \end{cases}$

Sieving in [MZ22]

[MZ22] sieves $\mathcal{O}(a \star E, b \star E)$ proceeds as follows.



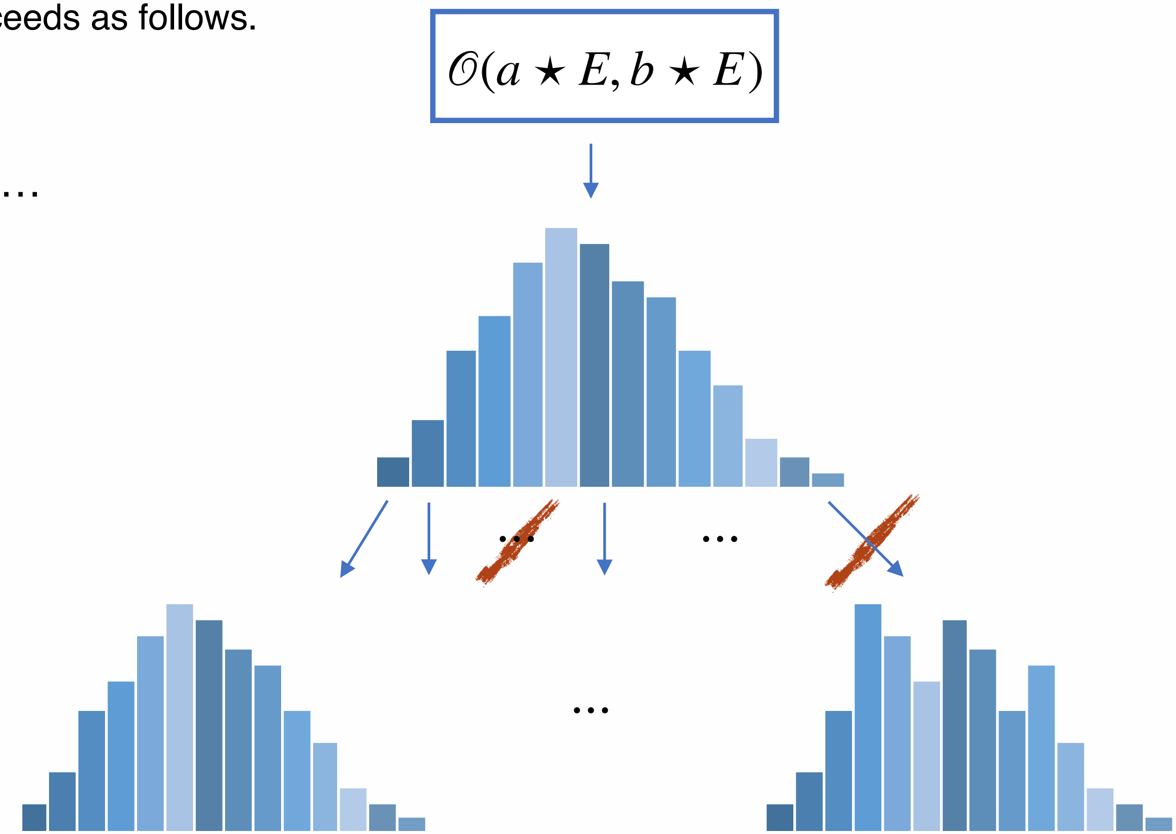
Running $\mathcal{O}(a \star E, b \star E)$...

Sieving in [MZ22]

[MZ22] sieves $\mathscr{O}(a \star E, b \star E)$ proceeds as follows.

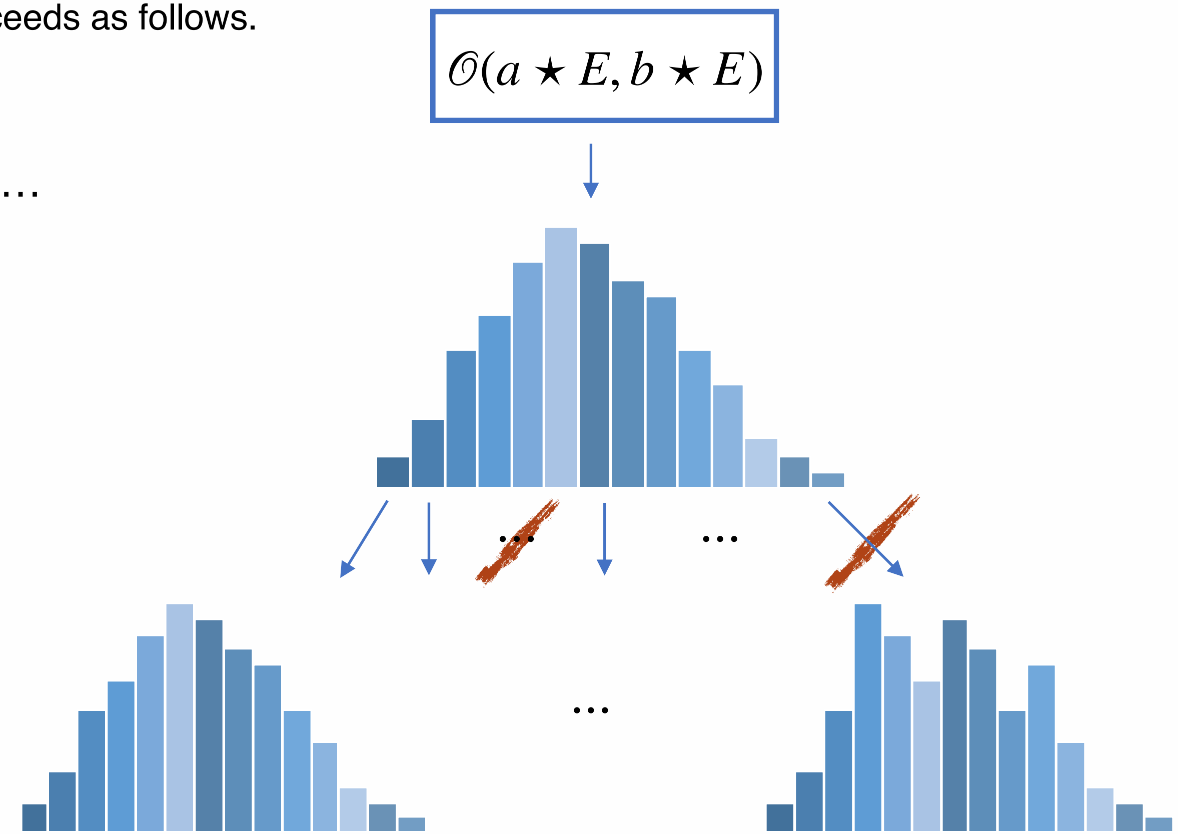
Running $\mathscr{O}(a \star E, b \star E)$...

Running $\mathscr{O}(\square, E)$...



Sieving in [MZ22]

[MZ22] sieves $\mathcal{O}(a \star E, b \star E)$ proceeds as follows.



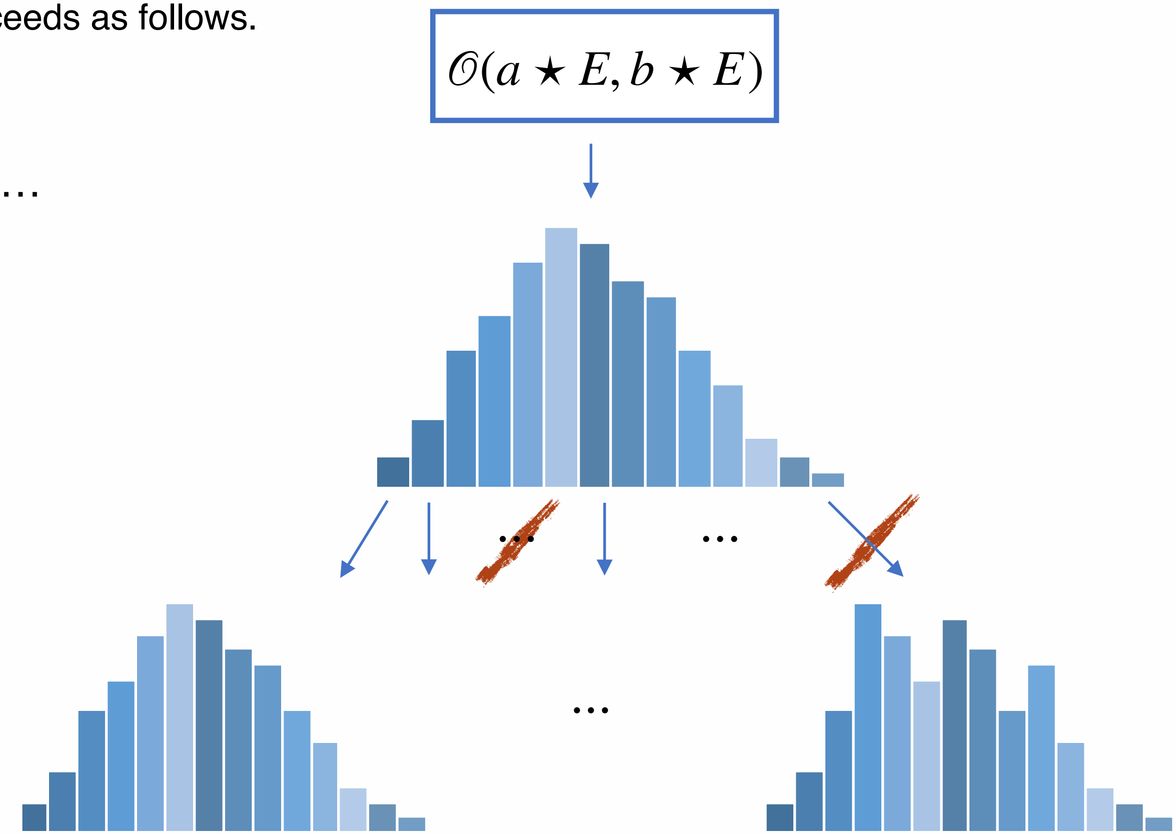
Running $\mathcal{O}(a \star E, b \star E)$...

Running $\mathcal{O}(\square, E)$...

Estimate the statistical distance.

Sieving in [MZ22]

[MZ22] sieves $\mathcal{O}(a \star E, b \star E)$ proceeds as follows.



Running $\mathcal{O}(a \star E, b \star E)$...

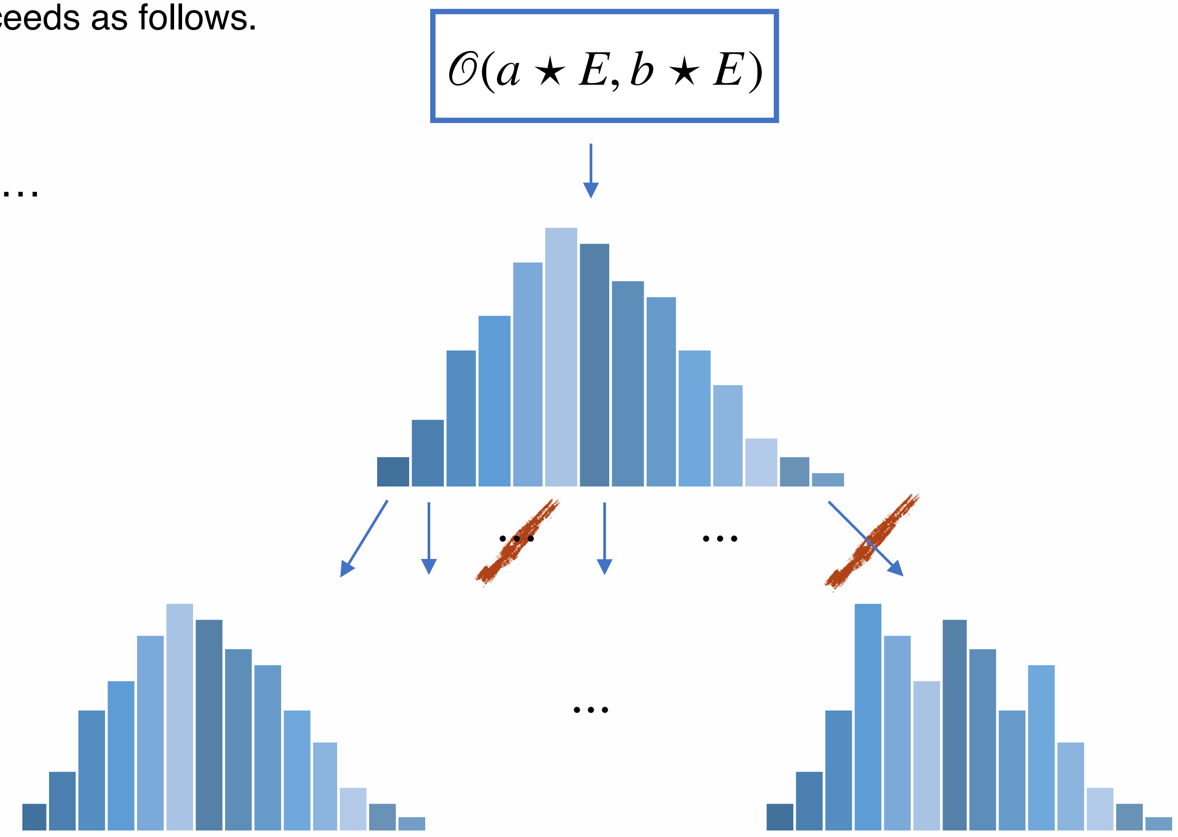
Running $\mathcal{O}(\square, E)$...

Estimate the statistical distance.

Sieving…

Sieving in [MZ22]

[MZ22] sieves $\mathcal{O}(a \star E, b \star E)$ proceeds as follows.



Running $\mathcal{O}(a \star E, b \star E)$…

Running $\mathcal{O}(\square, E)$…

Estimate the statistical distance.

Sieving…

Return the resulting elements.

Sieving in [MZ22]

[MZ22] sieves $\mathcal{O}(a \star E, b \star E)$ proceeds as follows.

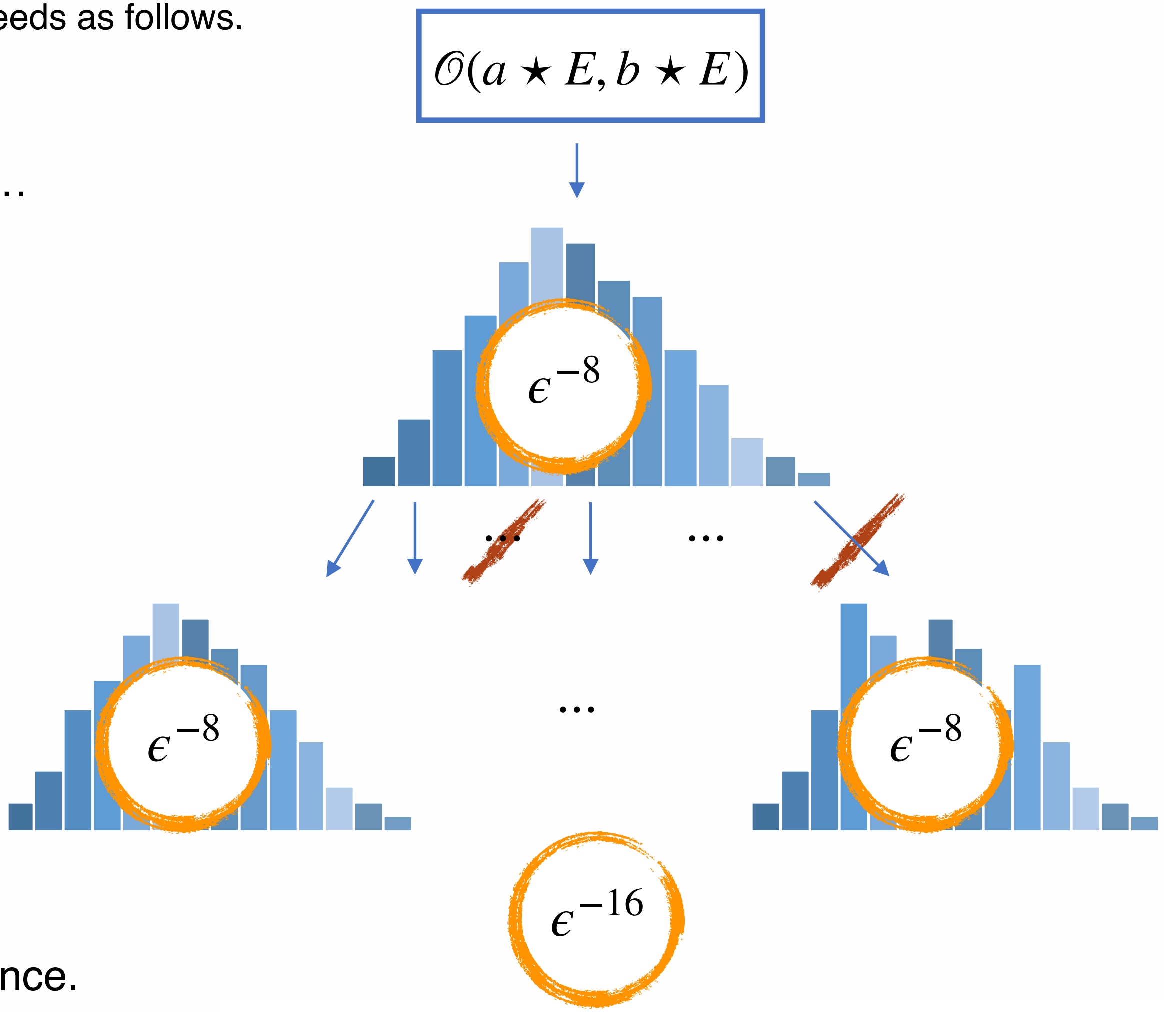
Running $\mathcal{O}(a \star E, b \star E)$...

Running $\mathcal{O}(\square, E)$...

Estimate the statistical distance.

Sieving…

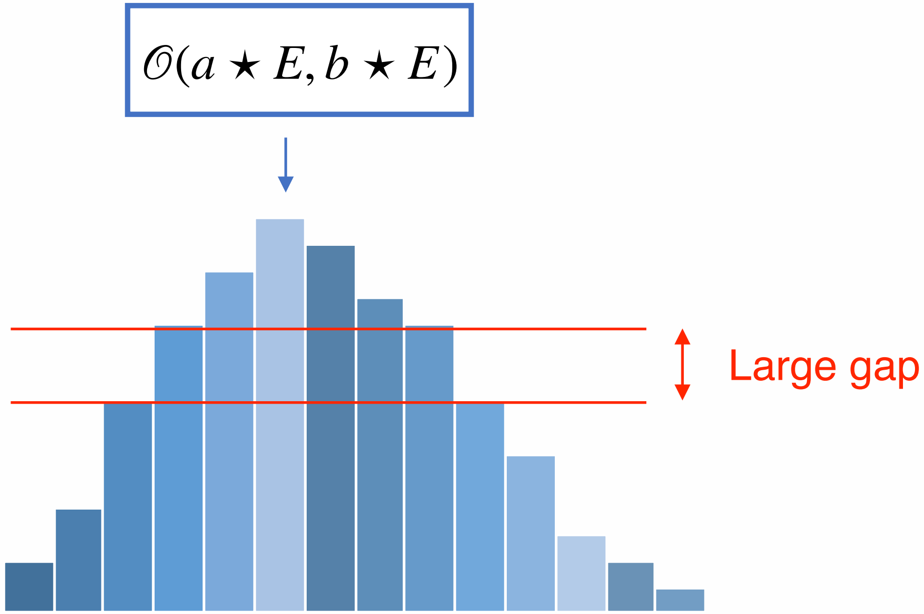
Return the resulting elements.



Distinguishing distributions is expensive.

Key Idea of our Improvement

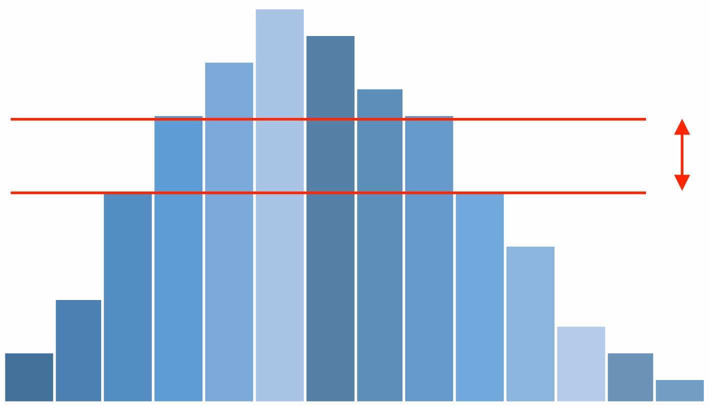
Running $\mathcal{O}(a \star E, b \star E)$...



Key Idea of our Improvement

Running $\mathcal{O}(a \star E, b \star E)$...

$$\boxed{\mathcal{O}(a \star E, b \star E)}$$



Large gap

If there is a large gap,

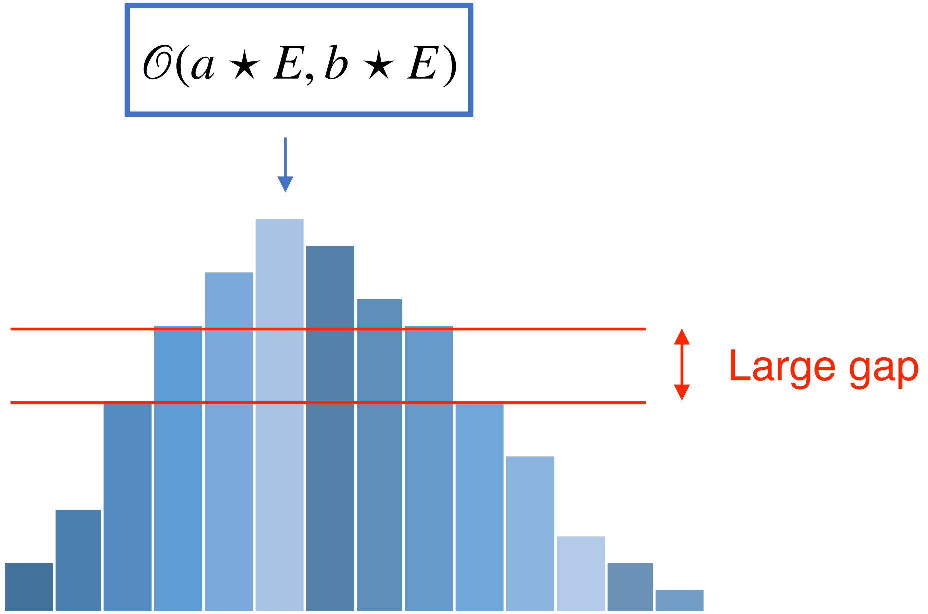
the “heavy elements” above the gap

are quite **stable**,

like an ``invariance”.

Key Idea of our Improvement

Running $\mathcal{O}(a \star E, b \star E)$...



If there is a large gap,

the “heavy elements” above the gap

are quite **stable**,

like an ``invariance”.

Intuitively, due to the large gap,

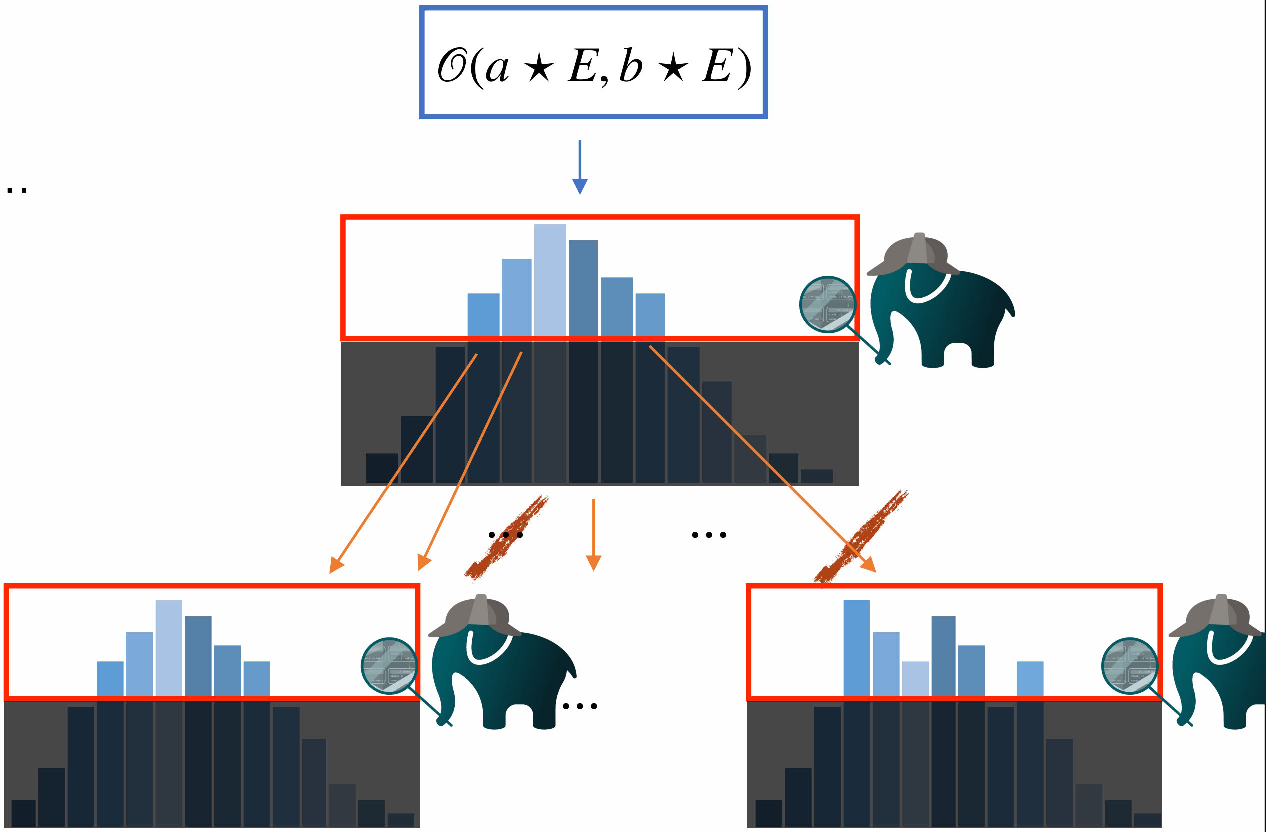
the last element above the gap &

the first element below the gap are unlikely to be swapped.

Key Idea

Running $\mathcal{O}(a \star E, b \star E)$...

Running $\mathcal{O}(\square, E)$...



Compare the heaviest elements.

Sieving...

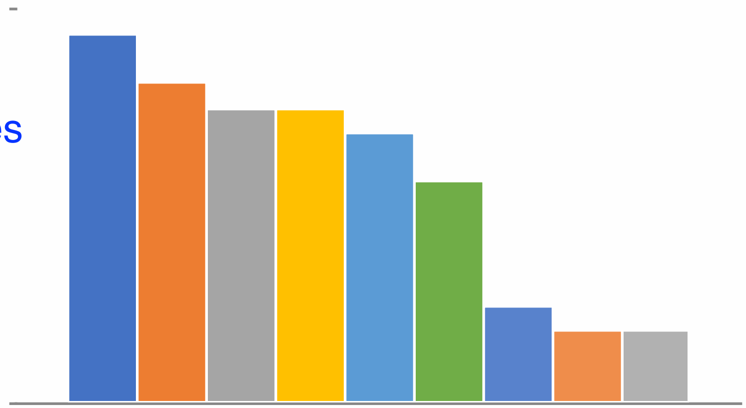
Return the resulting elements.

This reduce the # of queries significantly (to $O(\epsilon^{-4})$).

Gap Finding

1. Run $T = O(\epsilon^{-3})$ times

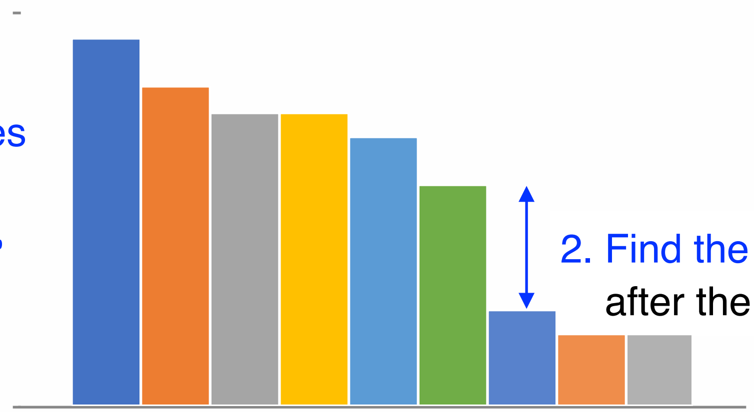
$\mathcal{O}(a \star E, b \star E)$



Gap Finding

1. Run $T = O(\epsilon^{-3})$ times

$\mathcal{O}(a \star E, b \star E)$

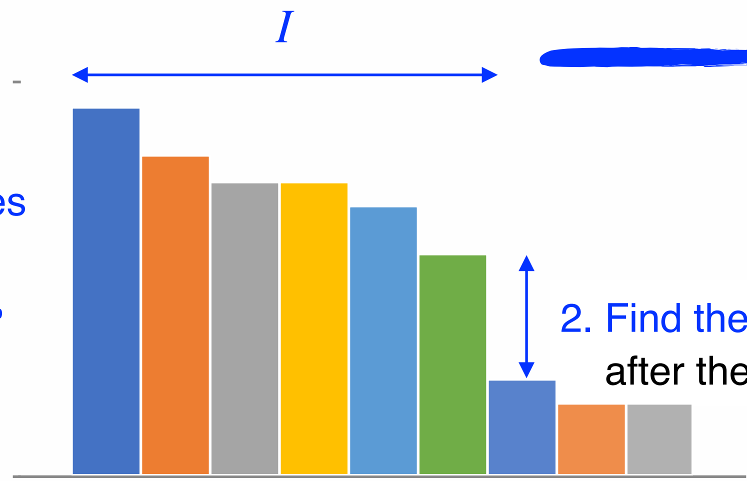


2. Find the first large gap of $T \cdot \epsilon^2/4$ after the ϵ^{-1}-th element.

Gap Finding

1. Run $T = O(\epsilon^{-3})$ times

$\mathcal{O}(a \star E, b \star E)$



2. Find the first large gap of $T \cdot \epsilon^2/4$ after the ϵ^{-1}-th element.

3. Record the index I.

Thresholding using I

We introduce an intermediate $\mathcal{O}_I^{\mathsf{Thr}}(a \star E, b \star E)$

to compute the ``invariance'' (heaviest I elements).

I

$\mathcal{O}(a \star E, b \star E)$

Thresholding using I

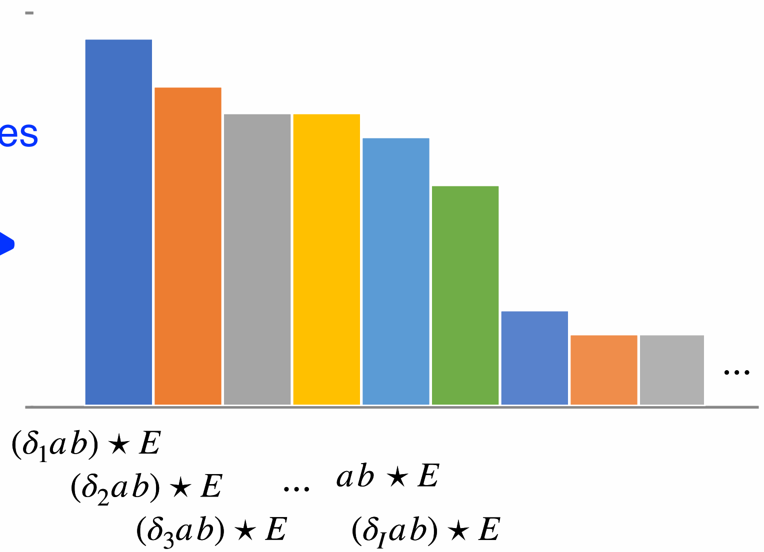
We introduce an intermediate $\mathcal{O}_I^{\mathsf{Thr}}(a \star E, b \star E)$

to compute the ``invariance'' (heaviest I elements).

I

1. Run $T = O(\epsilon^{-3})$ times

$\mathcal{O}(a \star E, b \star E)$



Thresholding using I

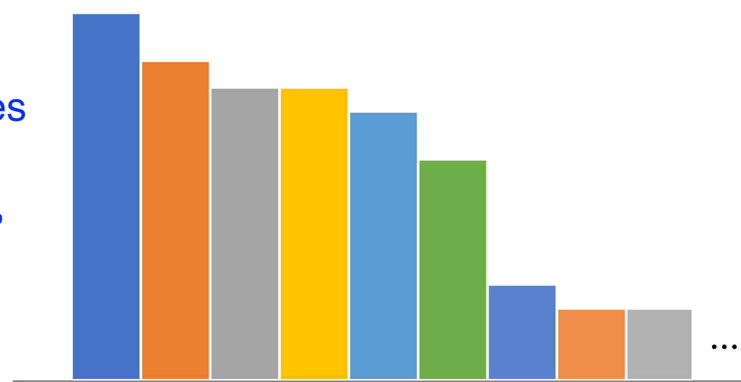
We introduce an intermediate $\mathcal{O}_I^{\text{Thr}}(a \star E, b \star E)$

to compute the ``invariance'' (heaviest I elements).

I

1. Run $T = O(\epsilon^{-3})$ times

$\mathcal{O}(a \star E, b \star E)$



$(\delta_1 ab) \star E$ $(\delta_2 ab) \star E$ $(\delta_3 ab) \star E$ ... $ab \star E$ $(\delta_I ab) \star E$

2. Return the heaviest I elements (Ignoring the frequency).

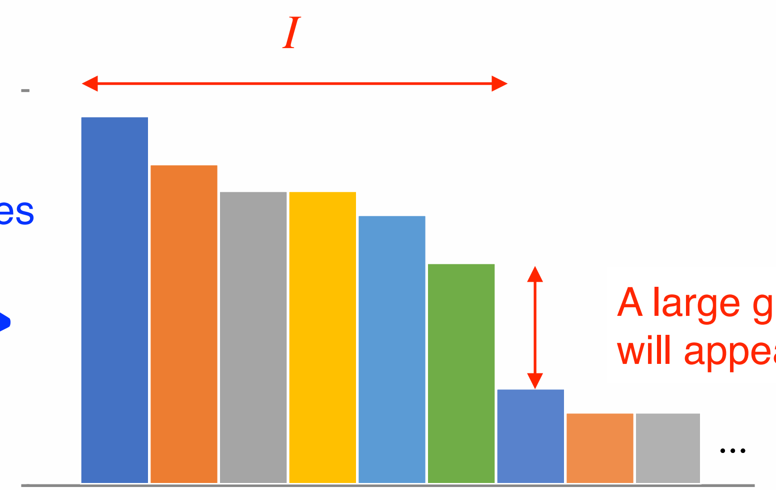
Thresholding using I

We introduce an intermediate $\mathcal{O}_I^{\text{Thr}}(a \star E, b \star E)$

to compute the ``invariance'' (heaviest I elements).

1. Run $T = O(\epsilon^{-3})$ times

$\mathcal{O}(a \star E, b \star E)$



A large gap (might not as large) will appear right at the same place.

$(\delta_1 ab) \star E$ $(\delta_2 ab) \star E$ $(\delta_3 ab) \star E$ ... $ab \star E$ $(\delta_I ab) \star E$

2. Return the heaviest I elements (Ignoring the frequency).

Propositions of Thresholding

1. $\mathcal{O}_I^{\mathsf{Thr}}$ is deterministic with an overwhelming chance when I is chosen properly.
2. $\mathcal{O}_I^{\mathsf{Thr}}(a \star E, b \star E) = \mathcal{O}_I^{\mathsf{Thr}}(ab \star E, E)$.

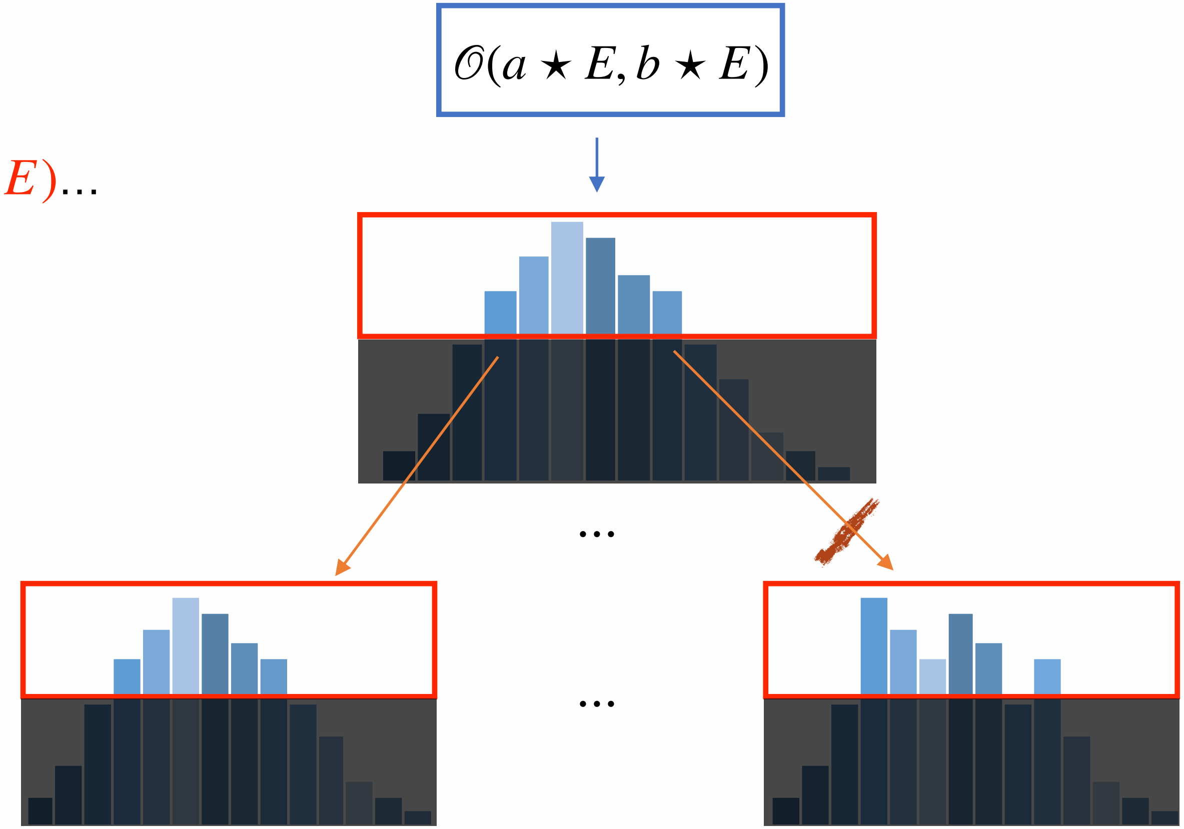
- That is, say $E' \in L_0 \leftarrow \mathcal{O}_I^{\mathsf{Thr}}(a \star E, b \star E)$, and let $L' \leftarrow \mathcal{O}_I^{\mathsf{Thr}}(E', E)$. If $E' = ab \star E$ (the correct answer), then $L_0 = L'$.

- View $\mathcal{O}_I^{\mathsf{Thr}}$ as an ``invariant'' wrt the input $\Rightarrow$ Cheaper and more effective for comparison.

Our Sieving

Running $\mathcal{O}_I^{\mathsf{Thr}}(a \star E, b \star E)$…

Running $\mathcal{O}_I^{\mathsf{Thr}}(\square, E)$…



Compare the heaviest elements.

Sieving…

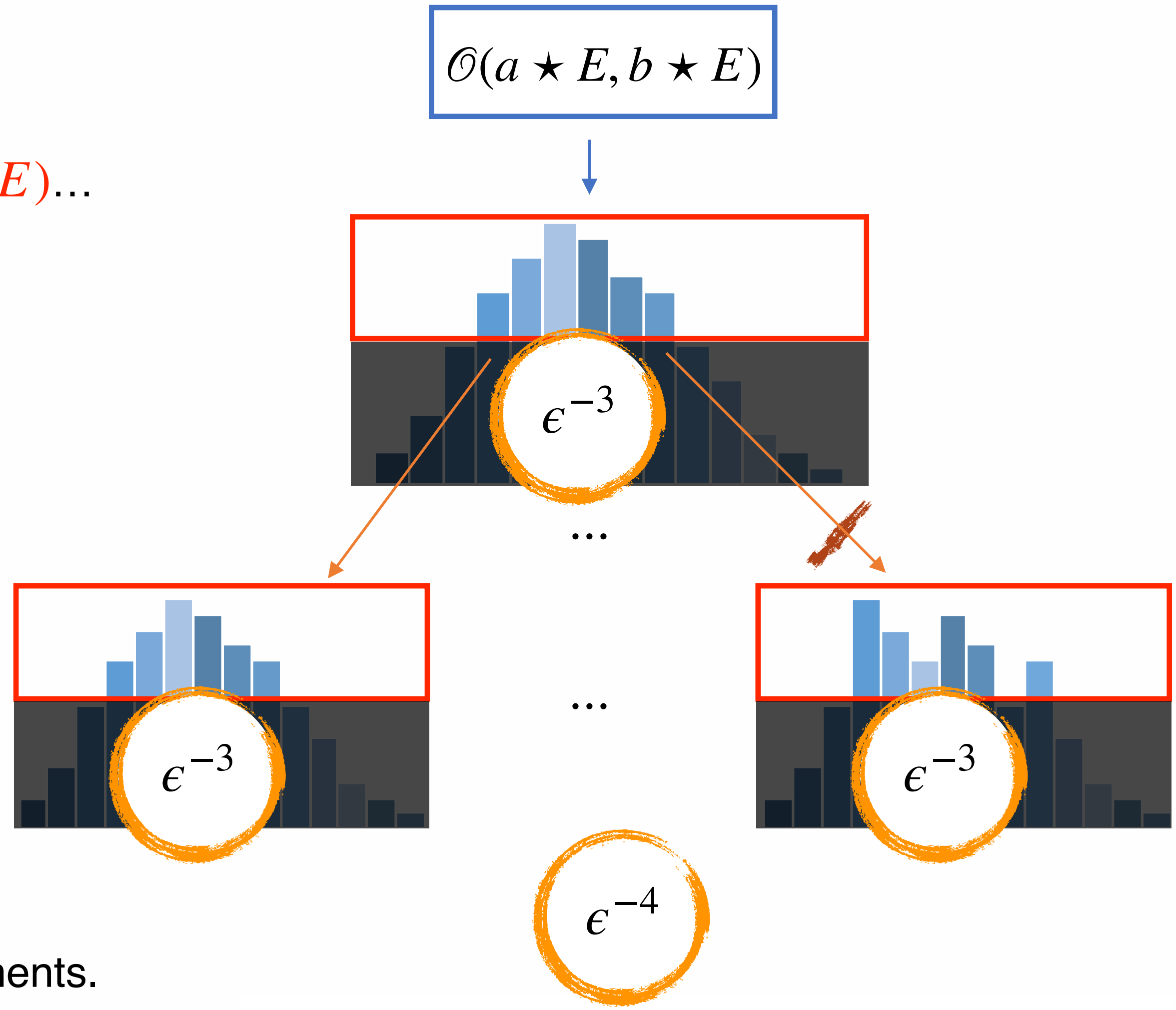
Return the resulting elements.

This reduce # of sampling significantly.

Our Sieving

Running $\mathcal{O}_I^{\mathsf{Thr}}(a \star E, b \star E)$...

Running $\mathcal{O}_I^{\mathsf{Thr}}(\square, E)$...



Compare the heaviest elements.

Sieving…

Return the resulting elements.

This reduce # of sampling significantly.

Improvement

	Ours	[MZ22]
Sieving $\mathcal{O} \to \mathcal{O}^{\mathsf{Siv}}$	Sampling + Thresholding (deterministic) And compare ϵ^{-4}	Sampling (probabilistic) And compare ϵ^{-16}
Error Terms of $\mathcal{O}^{\mathsf{Siv}}$ i.e. $\{1\} \cup \{\delta_i'\}_i$	An immediate small subgroup.	A set generates a small subgroup.
Query of $\mathcal{O}^{\mathsf{Siv}}$ for [GPSV18]	Constant in ϵ. 1	poly in ϵ. ϵ^{-5}
Overall Cost	ϵ^{-4}	ϵ^{-21}

Open Problems

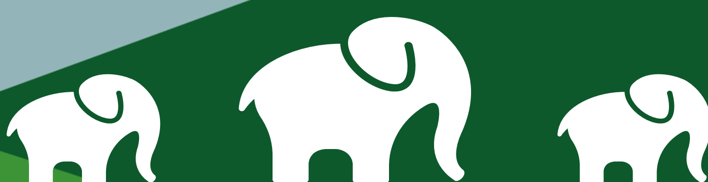
- Quantum Boost?
  - There exist classical/quantum algorithms (ϵ-test) from [SODA:CDVV14, ITCS:GL20] to accelerate [MZ22] (to roughly ϵ^{-9}) but not applicable to our results.

- Lower bound argument for the best plausible tightness between CDH and DLog?

CASA

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Thank you for listening!



casa.rub.de