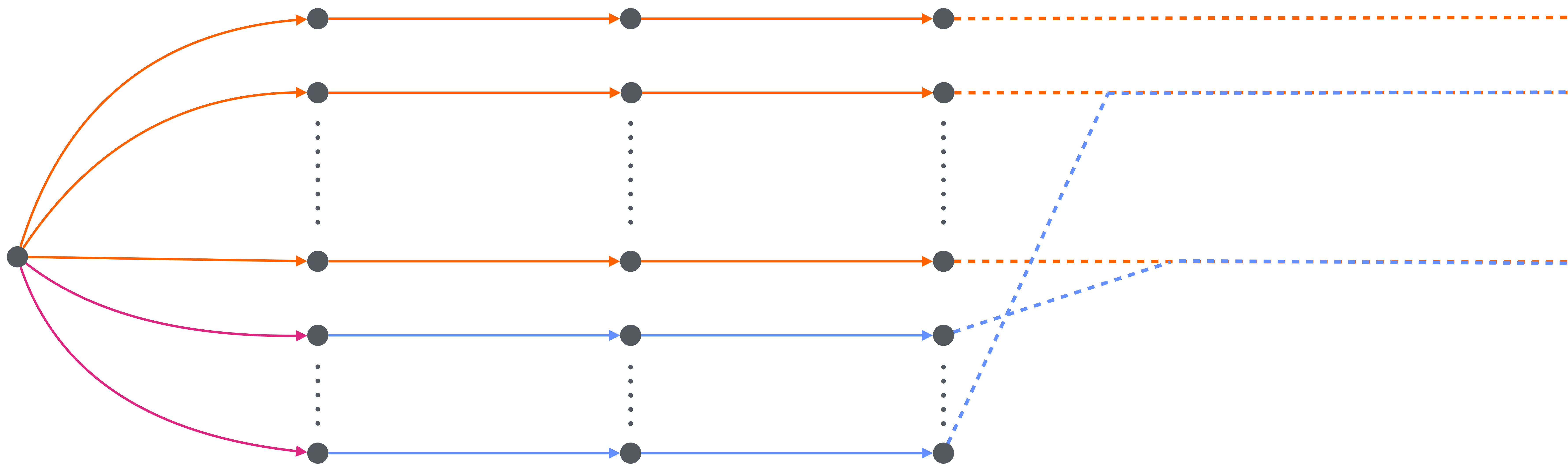
Multiple Group Action Dlogs With(out) Precomputation

Alexander May, Massimo Ostuzzi

Funded by
the European Union

RUHR UNIVERSITÄT BOCHUM RUB



PKC 2025, 14/05/25

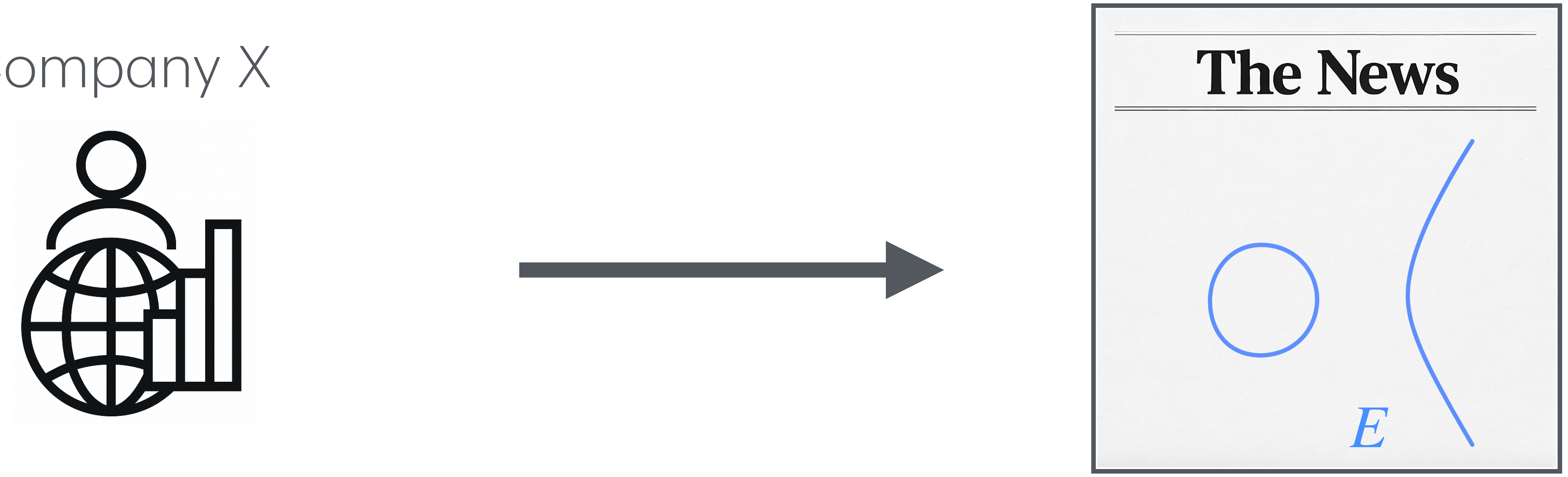
Precomputation Attacks

Precomputation Attacks

Company X

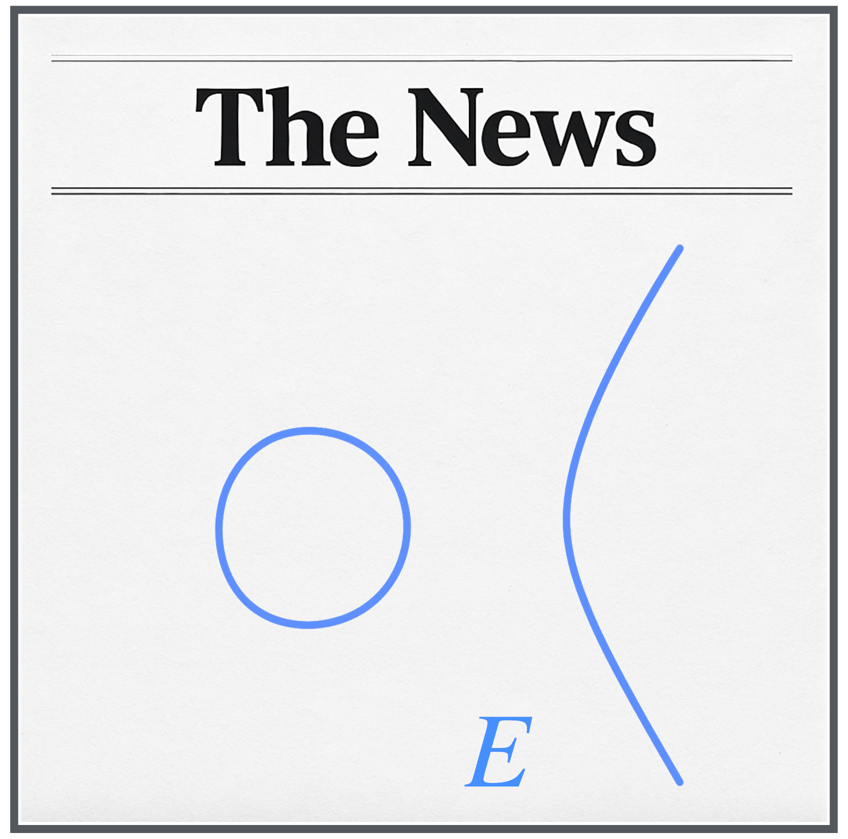
Precomputation Attacks

Company X



Precomputation Attacks

Company X

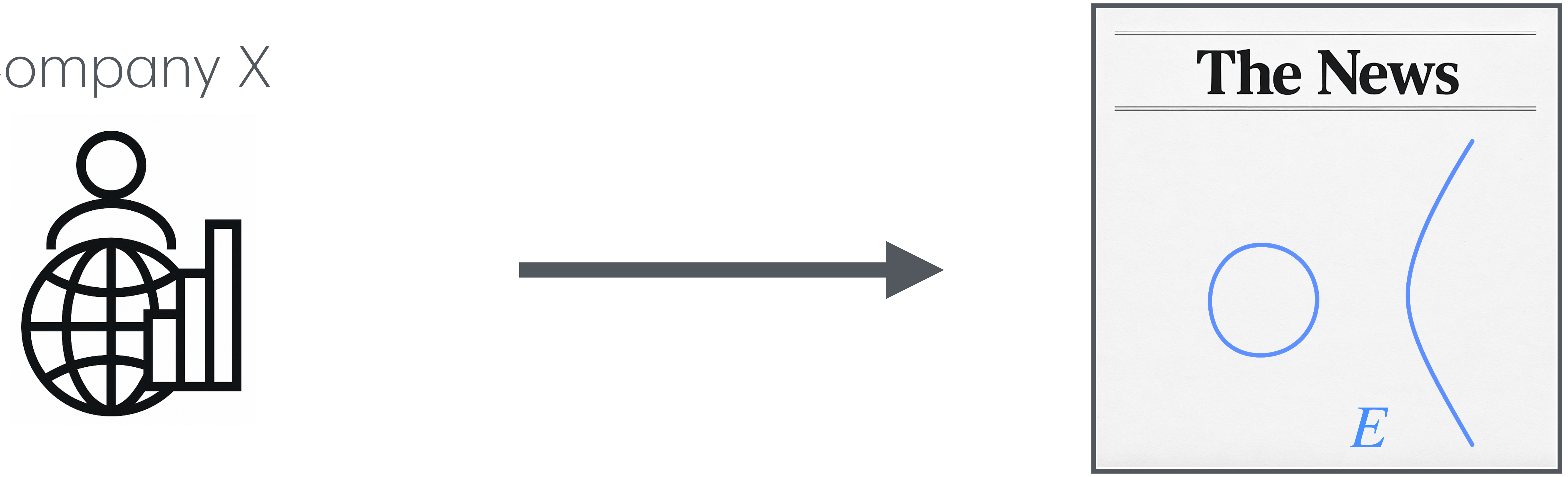


EC97: Shoup

If $|E| = N$, the time *lower bound* to solve one Dlog instance on E is $N^{1/2}$

Precomputation Attacks

Company X



EC97: Shoup

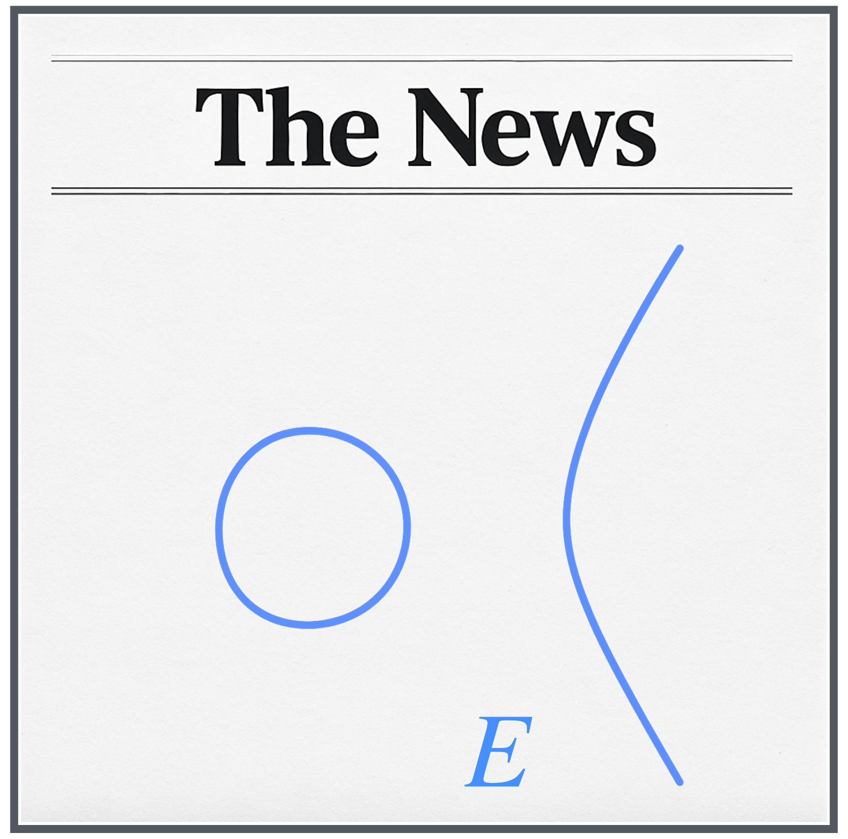
If $|E| = N$, the time *lower bound* to solve one Dlog instance on E is $N^{1/2}$

Trivial Precomputation Attack

Compute and store the whole E → Upon receiving an instance, look up the corresponding Dlog

Precomputation Attacks

Company X



EC97: Shoup

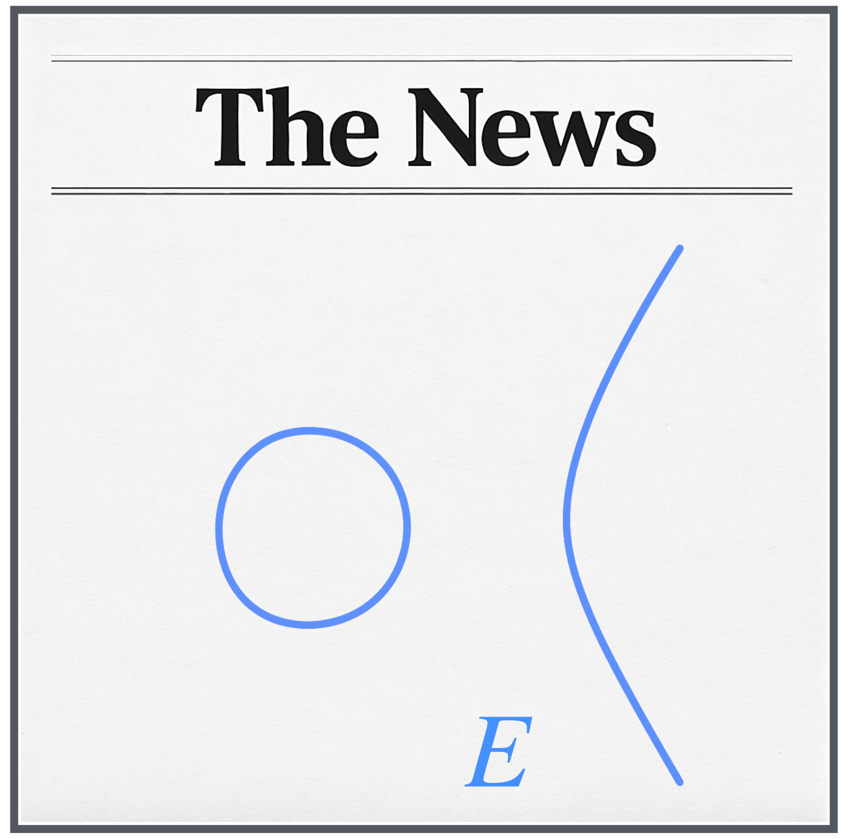
If $|E| = N$, the time *lower bound* to solve one Dlog instance on E is $N^{1/2}$

EC18: Corrigan-Gibbs & Kogan

Precomputation of time: $N^{2/3}$ → Online time: $N^{1/3}$ <u>instead of</u> $N^{1/2}$

Precomputation Attacks

Company X



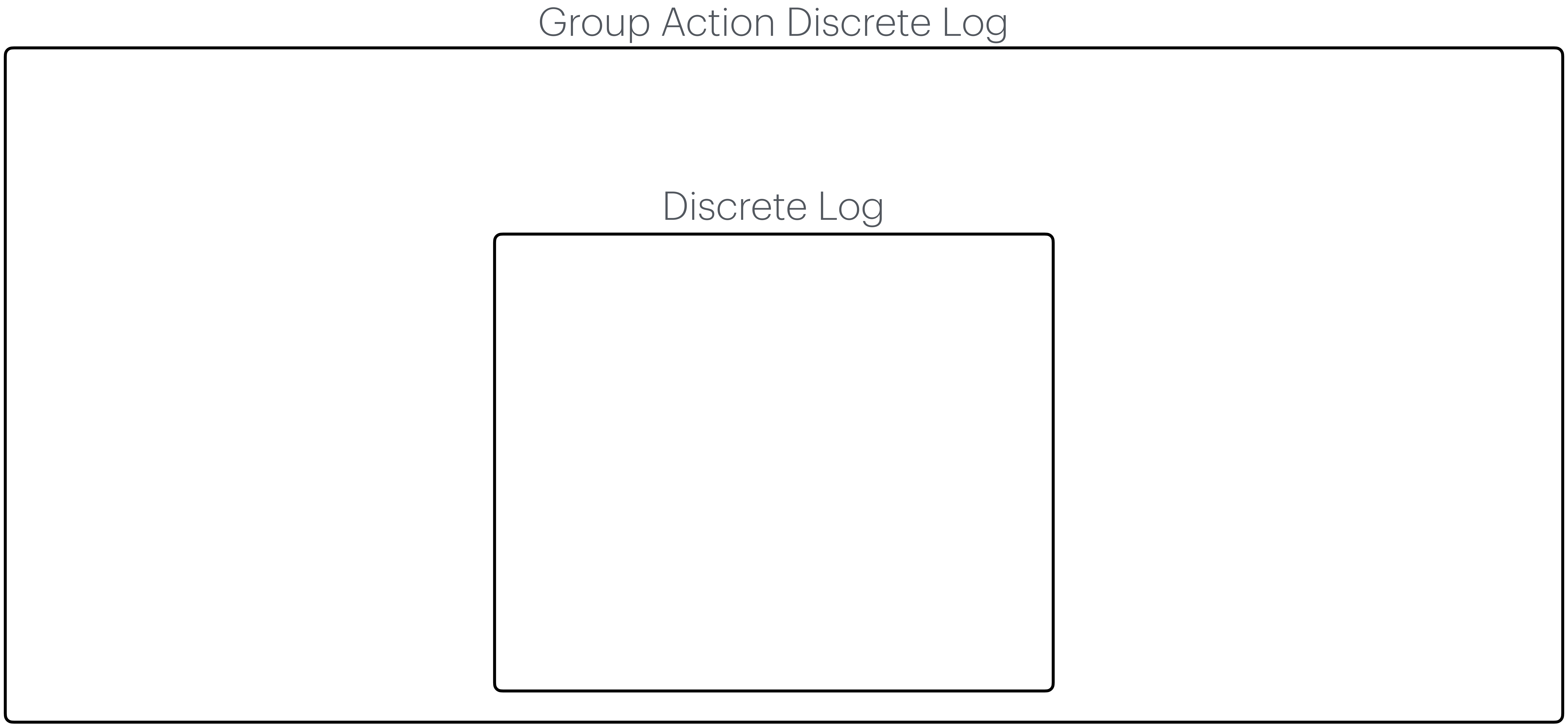
Precomputation Phase

Online Phase

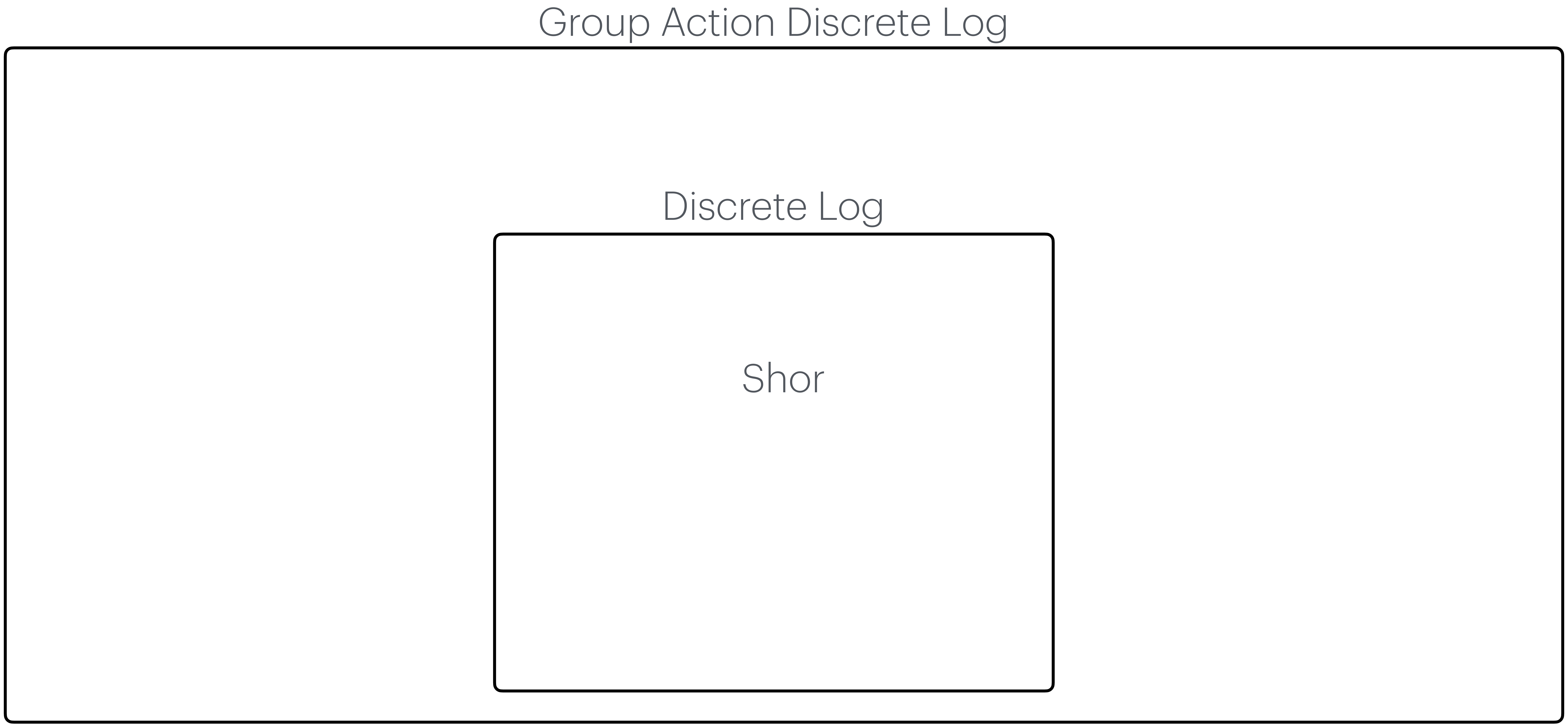
Perform (heavy) *instance-independent* computations to obtain a hint

Upon receiving an instance, leverage the hint to solve faster

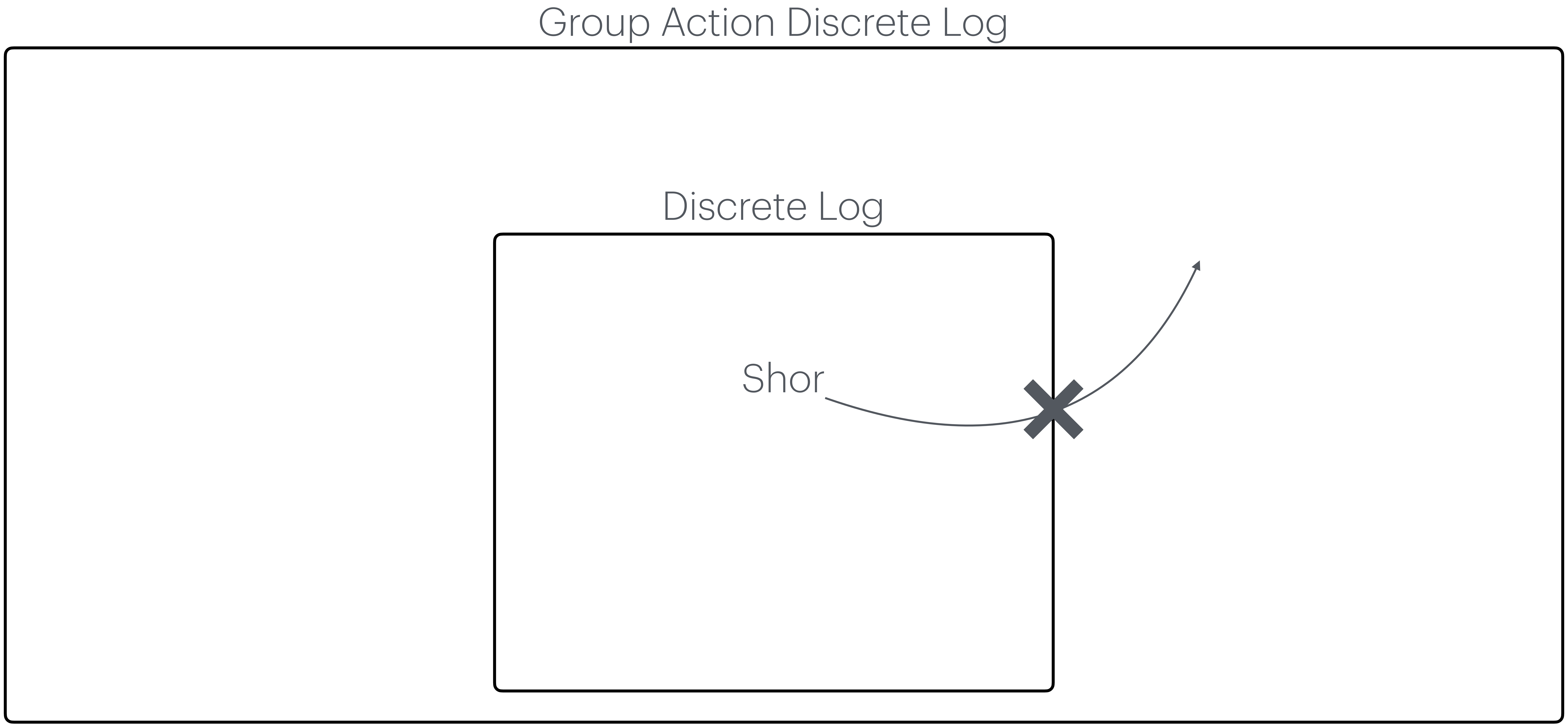
Extensions?



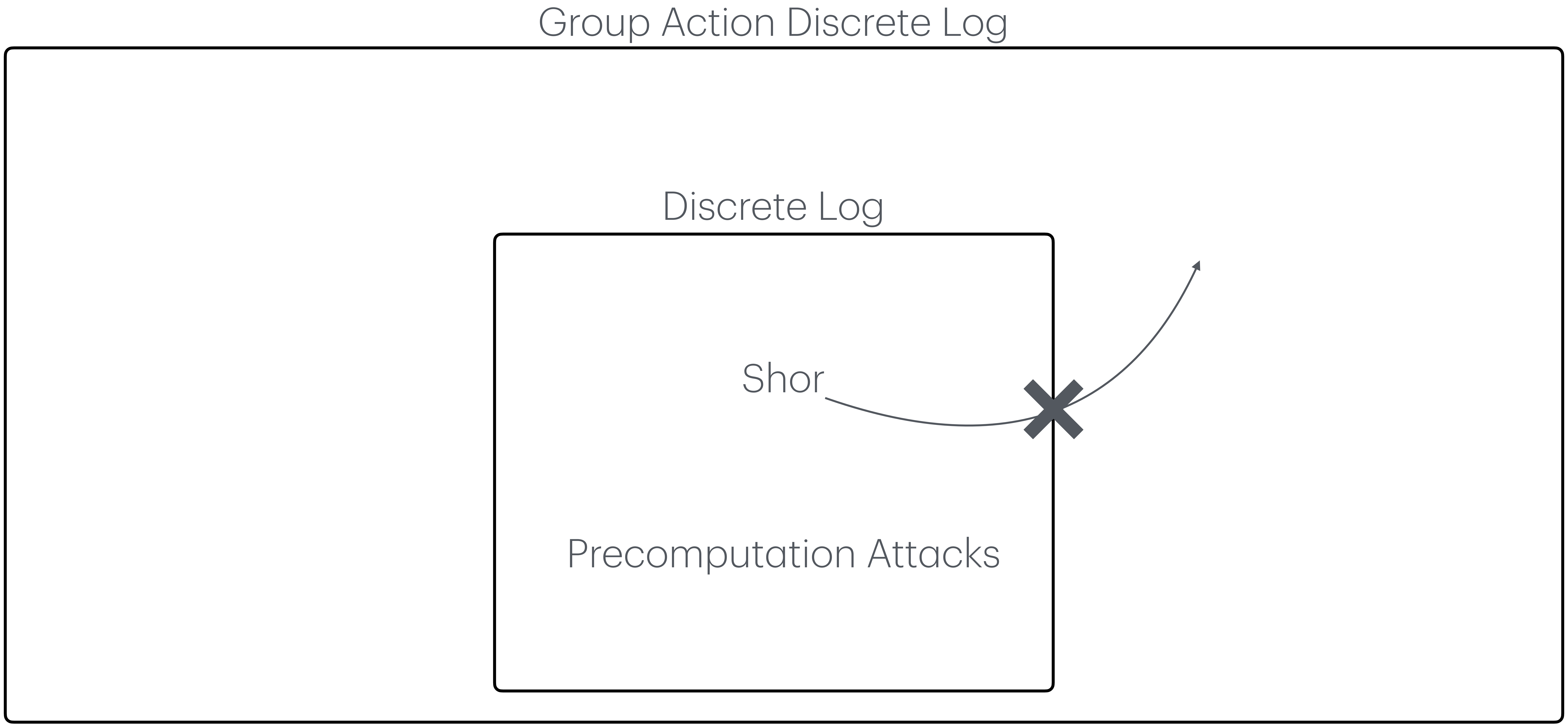
Extensions?



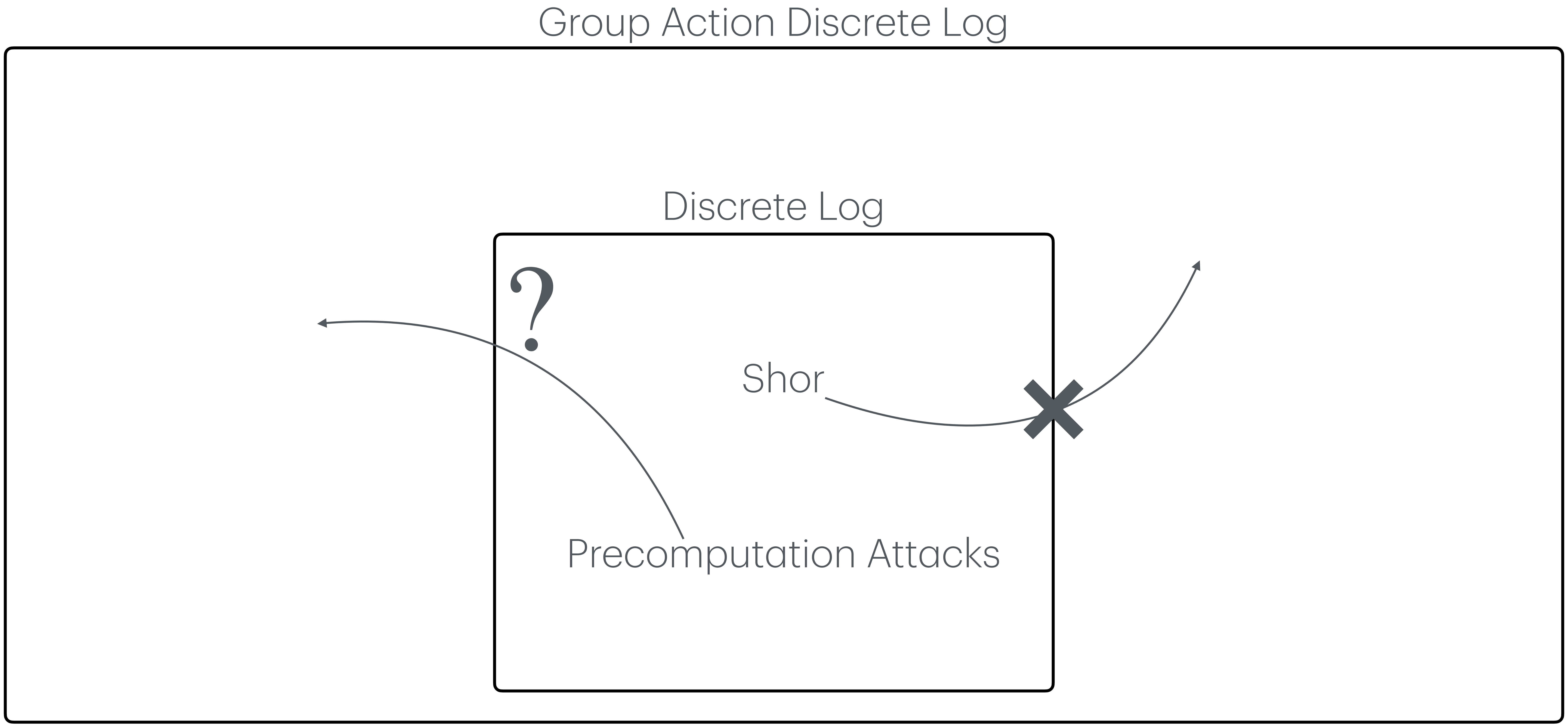
Extensions?



Extensions?


Group Action Discrete Log
Discrete Log
Shor
Precomputation Attacks

Extensions?


Group Action Discrete Log
Discrete Log
?
Shor
Precomputation Attacks

Group Actions

Basic Definitions

Group Actions

Basic Definitions

Given...

Any set $\mathcal{X}$, with a distinguished element $x \in \mathcal{X}$, called *origin*

A finitely generated abelian group $\mathcal{G} = \langle g_1, \ldots, g_n \rangle$, $|\mathcal{G}| = N$

Group Actions

Basic Definitions

Given...

Any set $\mathcal{X}$, with a distinguished element $x \in \mathcal{X}$, called *origin*

A finitely generated abelian group $\mathcal{G} = \langle g_1, \ldots, g_n \rangle$, $|\mathcal{G}| = N$

Then...

A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a *group action* if it satisfies:

Identity: $1 \star y = y$ for all $y \in \mathcal{X}$

Compatibility: $g \star (h \star y) = (gh) \star y$ for all $g, h \in \mathcal{G}$ and $y \in \mathcal{X}$

Group Actions

Basic Definitions

Given...

Any set $\mathcal{X}$, with a distinguished element $x \in \mathcal{X}$, called *origin*

A finitely generated abelian group $\mathcal{G} = \langle g_1, \ldots, g_n \rangle$, $|\mathcal{G}| = N$

Then...

A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a *group action* if it satisfies:

Identity: $1 \star y = y$ for all $y \in \mathcal{X}$

Compatibility: $g \star (h \star y) = (gh) \star y$ for all $g, h \in \mathcal{G}$ and $y \in \mathcal{X}$

A special and familiar example...

$\mathcal{X} = H = \langle h \rangle$ a finite cyclic group

Let $1 \in H$ be the origin, $|H| = N$

$\mathcal{G} = \mathbb{Z}_N$

$\star : \mathbb{Z}_N \times H \to H$, $(v, g) \mapsto h^v \cdot g$

Group Actions

GA-Dlogs

A special and familiar example...

$\mathcal{X} = H = \langle h \rangle$ a finite cyclic group

Let $1 \in H$ be the origin, $|H| = N$

$\mathcal{G} = \mathbb{Z}_N$

$\star : \mathbb{Z}_N \times H \to H$, $(v, g) \mapsto h^v \cdot g$

Group Actions

GA-Dlogs

Notation...

For $v \in \mathbb{Z}^n$, write $\mathbf{g}^v = g_1^{v_1} \cdot \cdots \cdot g_n^{v_n}$.

Denote by Λ the kernel of the map $v \mapsto \mathbf{g}^v$

A special and familiar example...

$\mathcal{X} = H = \langle h \rangle$ a finite cyclic group

Let $1 \in H$ be the origin, $|H| = N$

$\mathcal{G} = \mathbb{Z}_N$

$\star : \mathbb{Z}_N \times H \to H$, $(v, g) \mapsto h^v \cdot g$

Group Actions

GA-Dlogs

Notation...

For $v \in \mathbb{Z}^n$, write $\mathbf{g}^v = g_1^{v_1} \cdot \cdots \cdot g_n^{v_n}$.

Denote by Λ the kernel of the map $v \mapsto \mathbf{g}^v$

GA-Dlog

Given: one element $y \in \mathcal{X}$

Find: $v \in \mathbb{Z}^n$ such that $y = \mathbf{g}^v \star x$, modulo Λ

A special and familiar example...

$\mathcal{X} = H = \langle h \rangle$ a finite cyclic group

Let $1 \in H$ be the origin, $|H| = N$

$\mathcal{G} = \mathbb{Z}_N$

$\star : \mathbb{Z}_N \times H \to H$, $(v, g) \mapsto h^v \cdot g$

Group Actions

GA-Dlogs

Notation...

For $v \in \mathbb{Z}^n$, write $\mathbf{g}^v = g_1^{v_1} \cdot \cdots \cdot g_n^{v_n}$.

Denote by Λ the kernel of the map $v \mapsto \mathbf{g}^v$

GA-Dlog

Given: one element $y \in \mathcal{X}$

Find: $v \in \mathbb{Z}^n$ such that $y = \mathbf{g}^v \star x$, modulo Λ

A special and familiar example...

$\mathcal{X} = H = \langle h \rangle$ a finite cyclic group

Let $1 \in H$ be the origin, $|H| = N$

$\mathcal{G} = \mathbb{Z}_N$

$\star : \mathbb{Z}_N \times H \to H$, $(v, g) \mapsto h^v \cdot g$

$\star$ is a regular action

Group Actions

GA-Dlogs

Notation...

For $v \in \mathbb{Z}^n$, write $\mathbf{g}^v = g_1^{v_1} \cdot \cdots \cdot g_n^{v_n}$.

Denote by Λ the kernel of the map $v \mapsto \mathbf{g}^v$

GA-Dlog

Given: one element $y \in \mathcal{X}$

Find: $v \in \mathbb{Z}^n$ such that $y = \mathbf{g}^v \star x$, modulo Λ

A special and familiar example...

$\mathcal{X} = H = \langle h \rangle$ a finite cyclic group

Let $1 \in H$ be the origin, $|H| = N$

$\mathcal{G} = \mathbb{Z}_N$

$\star : \mathbb{Z}_N \times H \to H$, $(v, g) \mapsto h^v \cdot g$

$\star$ is a regular action

The GA-Dlog is the usual Dlog

Our Results

For GA-Dlogs

Extend the generic precomputation algorithms to the *Group Action Dlog* setting:

- Single-instance with precomputation
- Multi-instance with precomputation

Multi-instance "without" precomputation algorithm for GA-Dlogs

Multi-instance "without" precomputation algorithm for usual Dlogs

Finding GA-Dlogs

$N = |\mathcal{G}|$

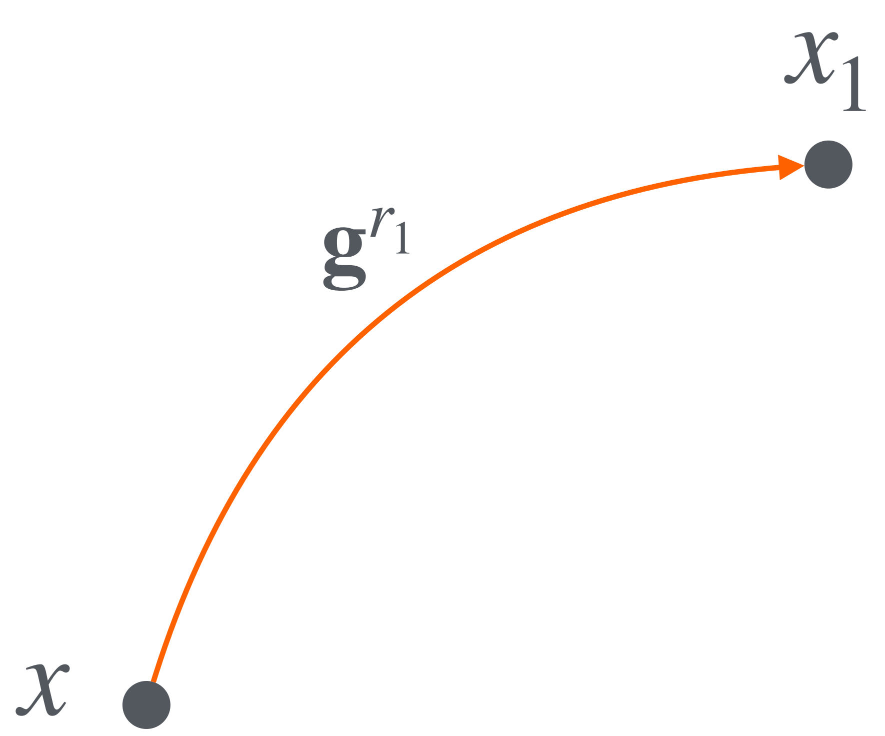
Single: Precomputation Phase

x

Finding GA-Dlogs

$N = |\mathcal{G}|$

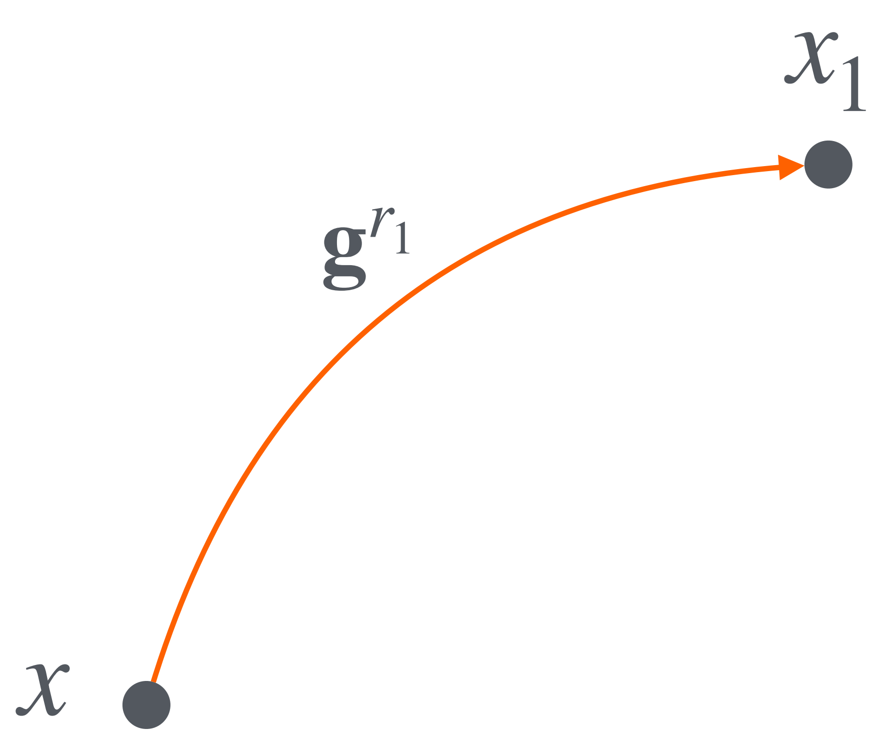
Single: Precomputation Phase



Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Precomputation Phase



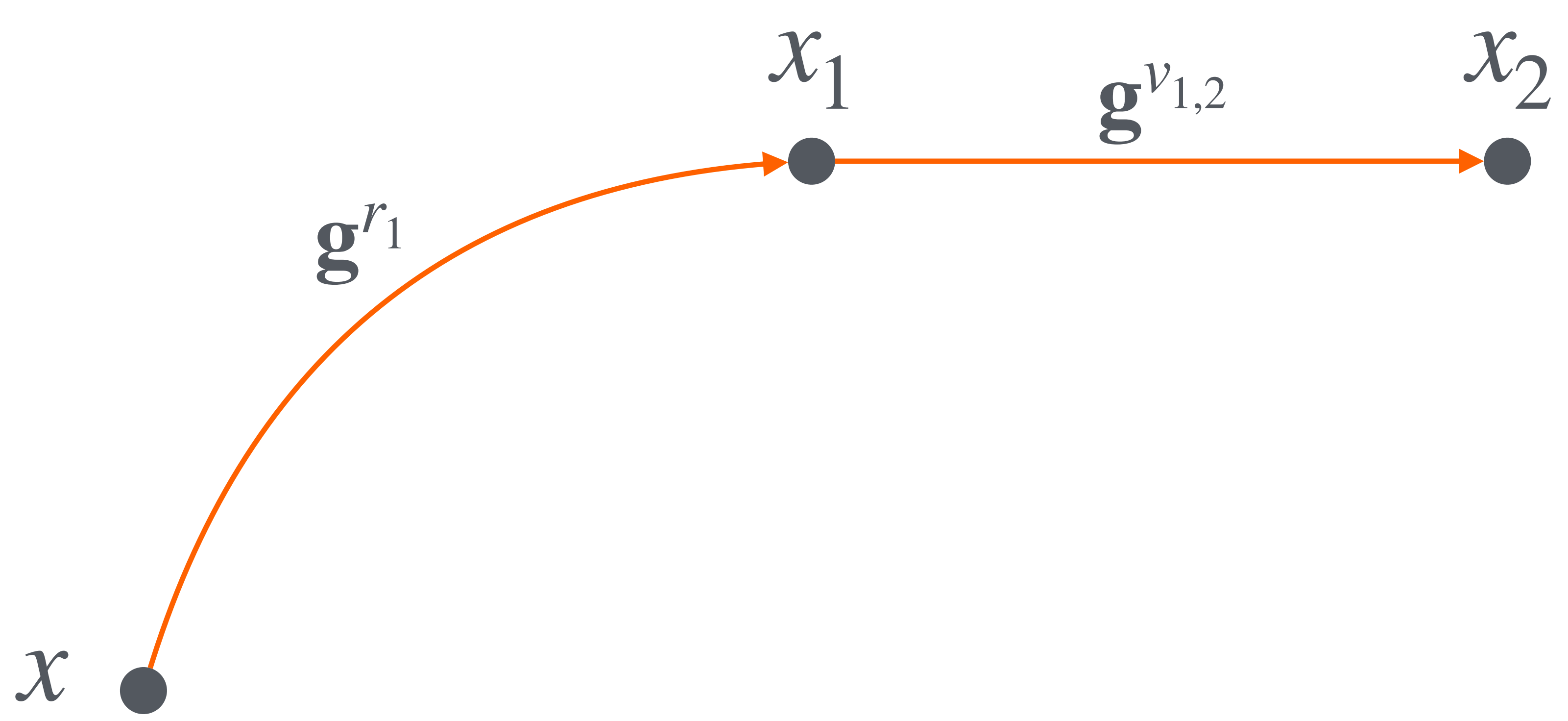
Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Precomputation Phase



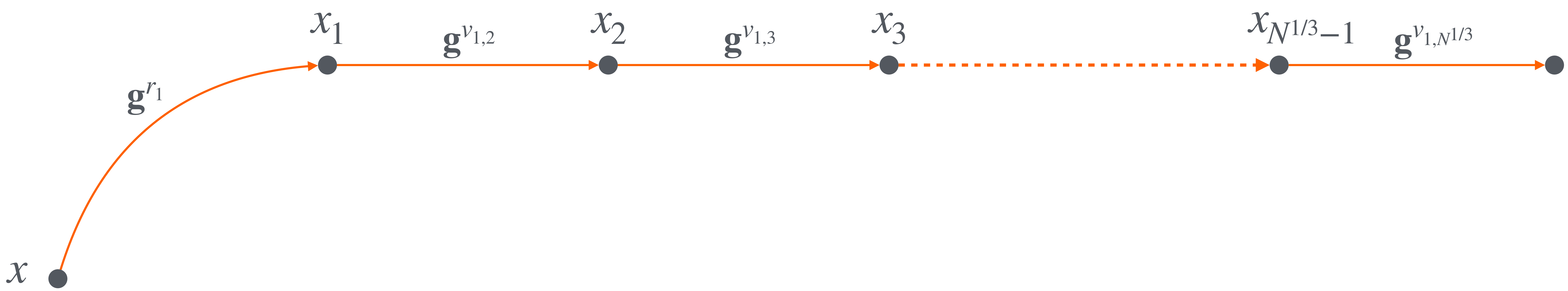
Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Precomputation Phase



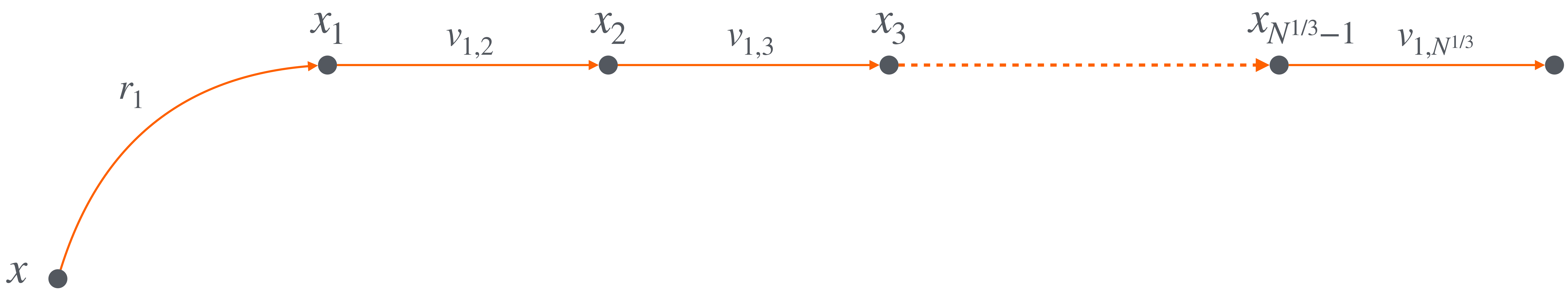
Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Precomputation Phase



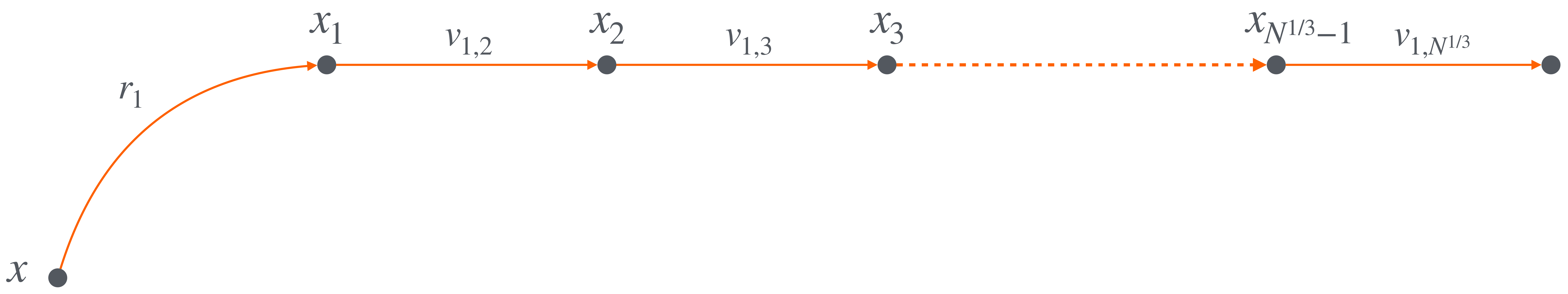
Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

Finding GA-Dlogs

Single: Precomputation Phase

$N = |\mathcal{G}|$



Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

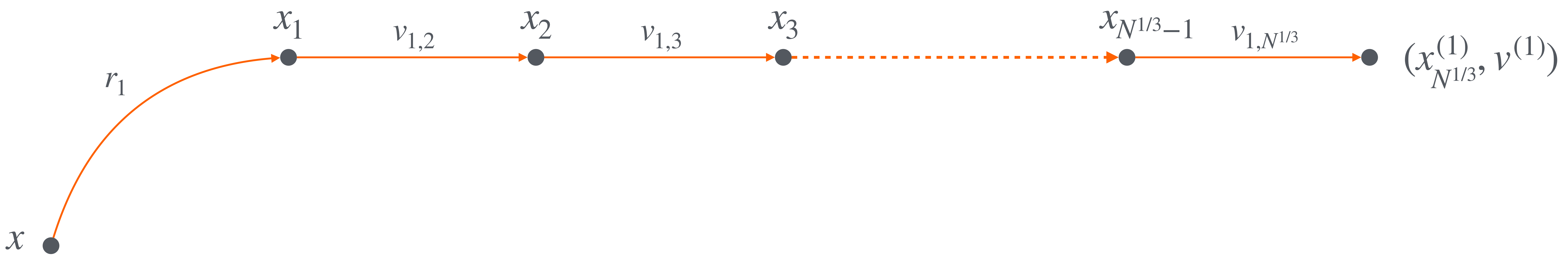
Notation

$$v^{(1)} := r_1 + v_{1,2} + \cdots + v_{1,N^{1/3}}$$

Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Precomputation Phase



Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

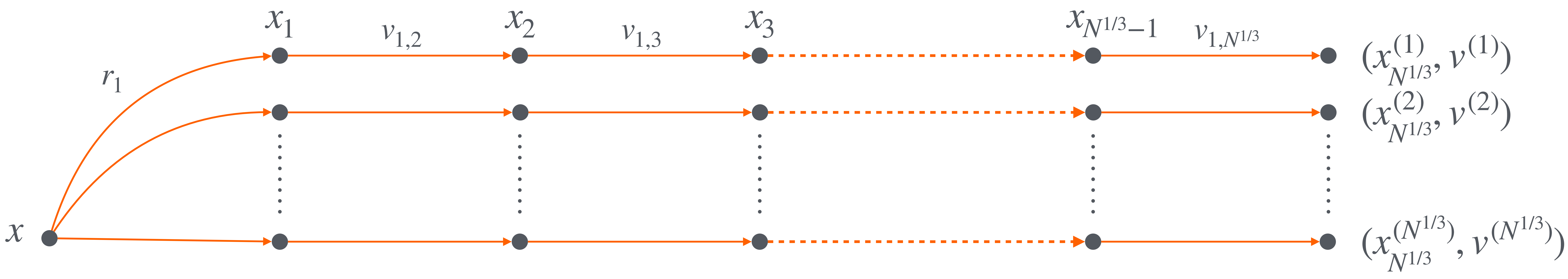
Notation

$$v^{(1)} := r_1 + v_{1,2} + \cdots + v_{1,N^{1/3}}$$

Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Precomputation Phase



Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

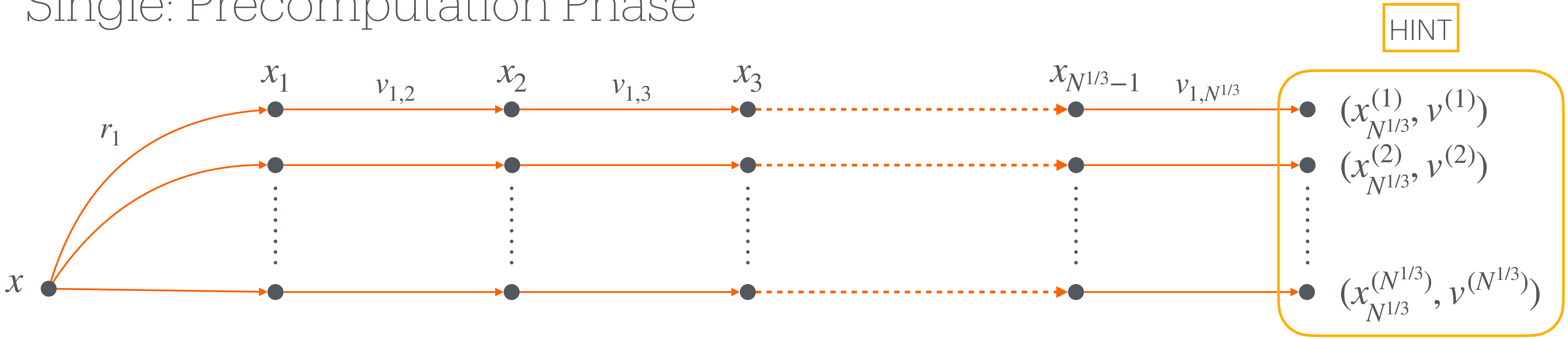
Notation

$$v^{(1)} := r_1 + v_{1,2} + \cdots + v_{1,N^{1/3}}$$

Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Precomputation Phase



Memoryless Walk

The next step of the walk only depends on the vertex *currently* visited

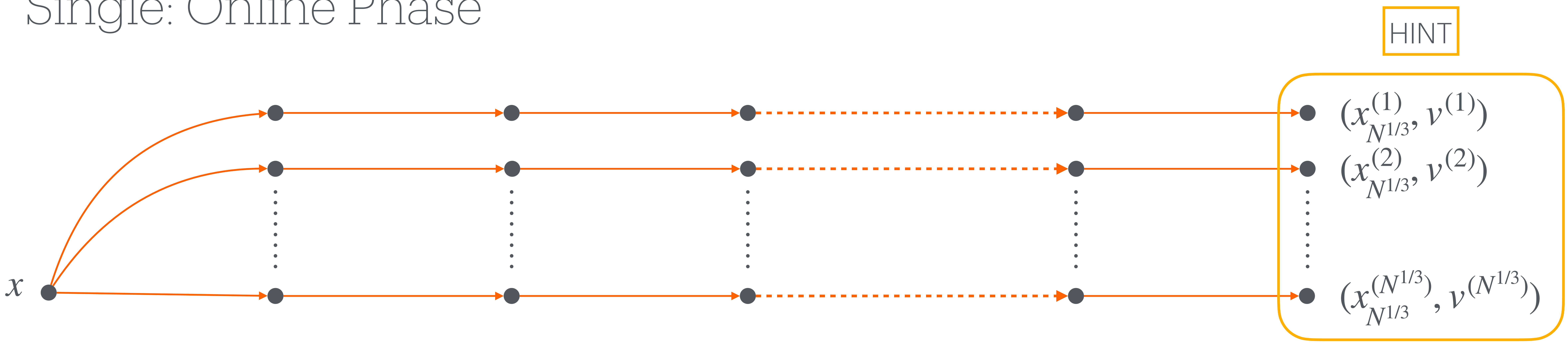
Notation

$$v^{(1)} := r_1 + v_{1,2} + \cdots + v_{1,N^{1/3}}$$

Finding GA-Dlogs

$N = |\mathcal{G}|$

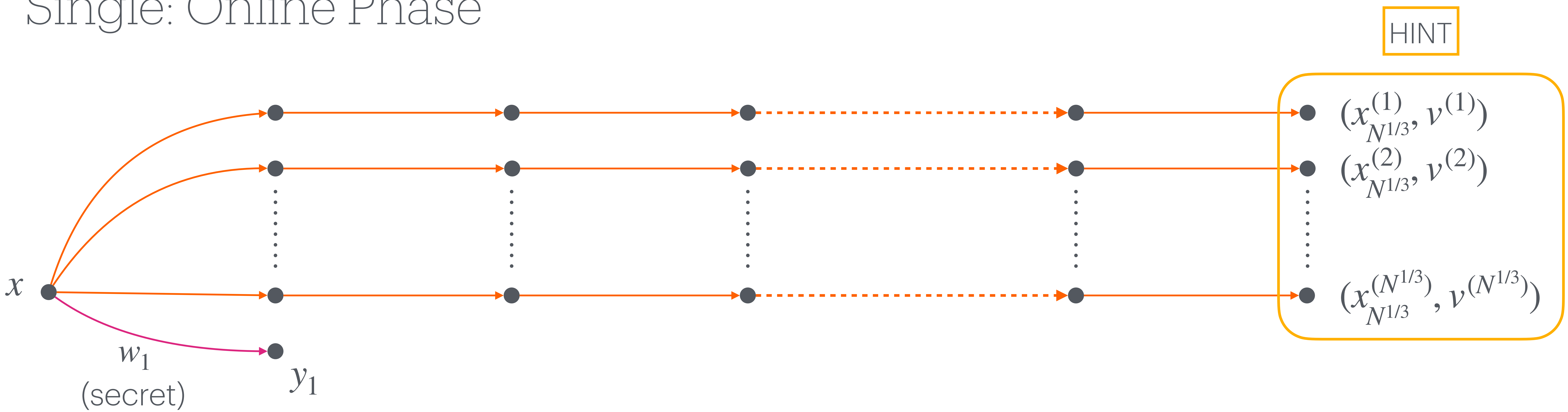
Single: Online Phase



Finding GA-Dlogs

$N = |\mathcal{G}|$

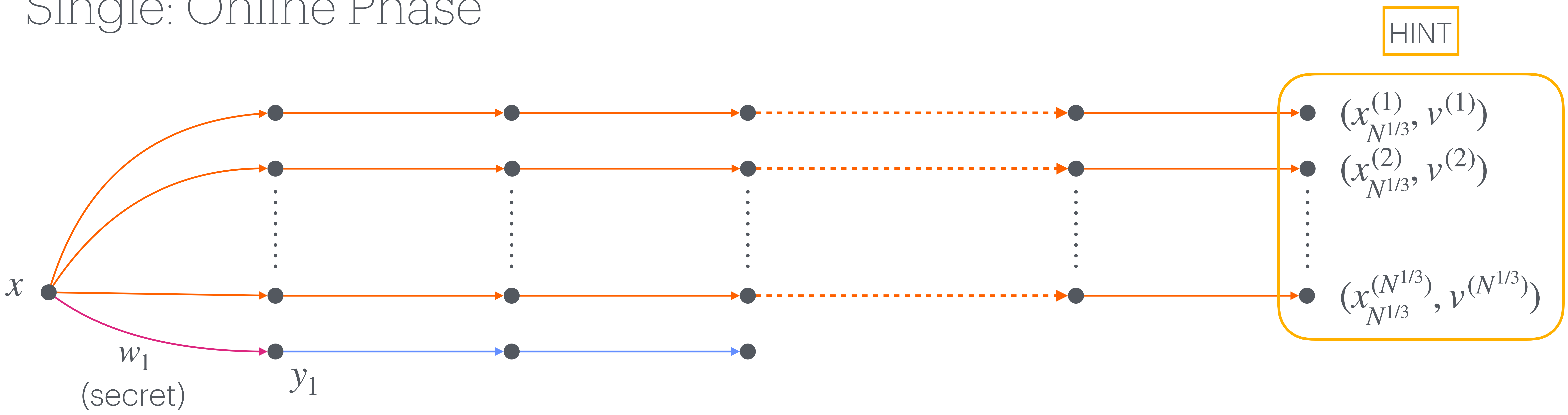
Single: Online Phase



Finding GA-Dlogs

$N = |\mathscr{G}|$

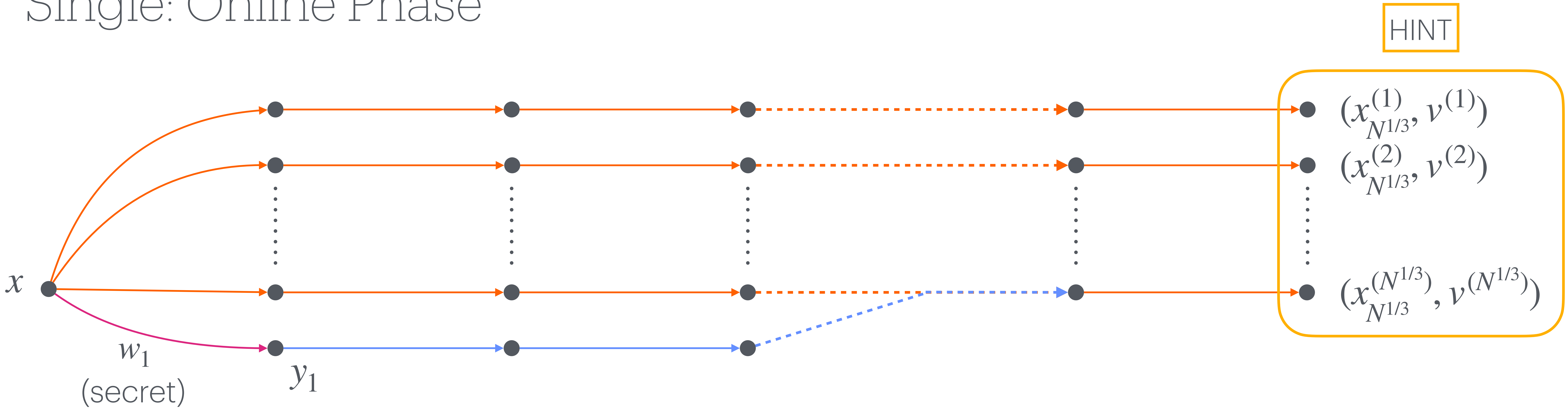
Single: Online Phase



Finding GA-Dlogs

$N = |\mathcal{G}|$

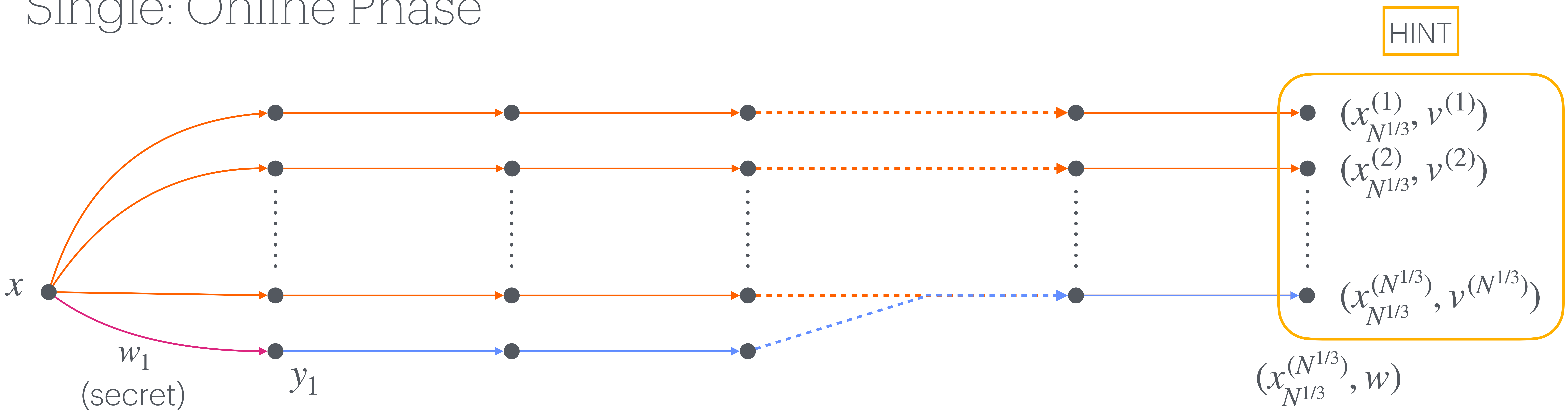
Single: Online Phase



Finding GA-Dlogs

$N = |\mathcal{G}|$

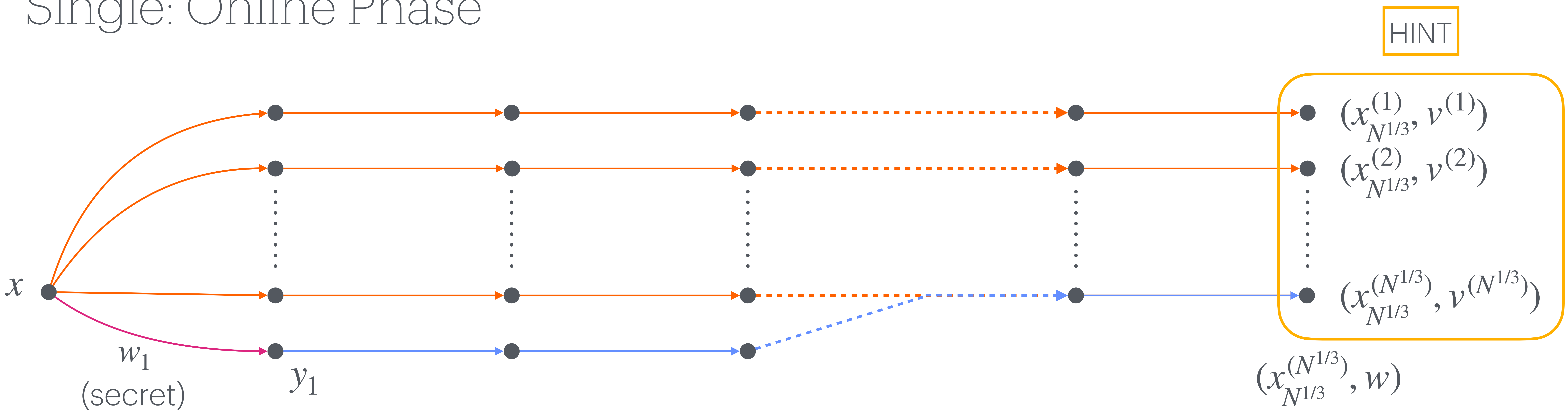
Single: Online Phase



Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Online Phase



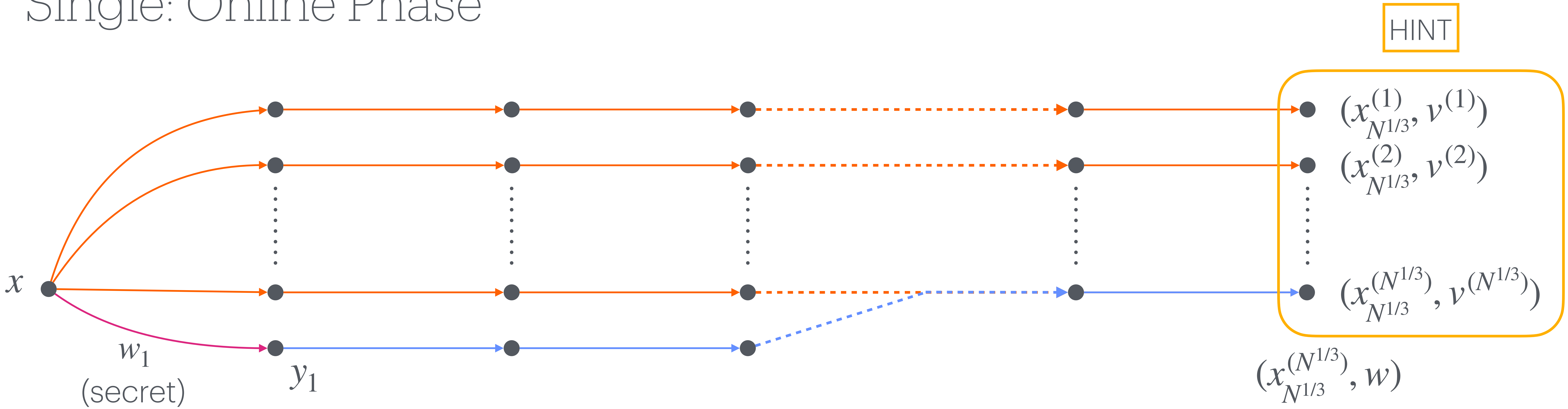
Collision Solves GA-Dlog:

$$x_{(N^{1/3})}^{(N^{1/3})} = \mathbf{g}^{w} \star y_1 \text{ and } x_{(N^{1/3})}^{(N^{1/3})} = \mathbf{g}^{v^{(N^{1/3})}} \star x \longrightarrow \mathbf{g}^{w} \star y_1 = \mathbf{g}^{v^{(N^{1/3})}} \star x \longrightarrow y_1 = \mathbf{g}^{v^{(N^{1/3})}-w} \star x$$

Finding GA-Dlogs

$N = |\mathcal{G}|$

Single: Online Phase



Precomputation: $N^{1/3} \cdot N^{1/3} = N^{2/3}$

Space: $N^{1/3}$

Online: $N^{1/3}$

→ Solve ONE GA-Dlog with Constant Success Probability

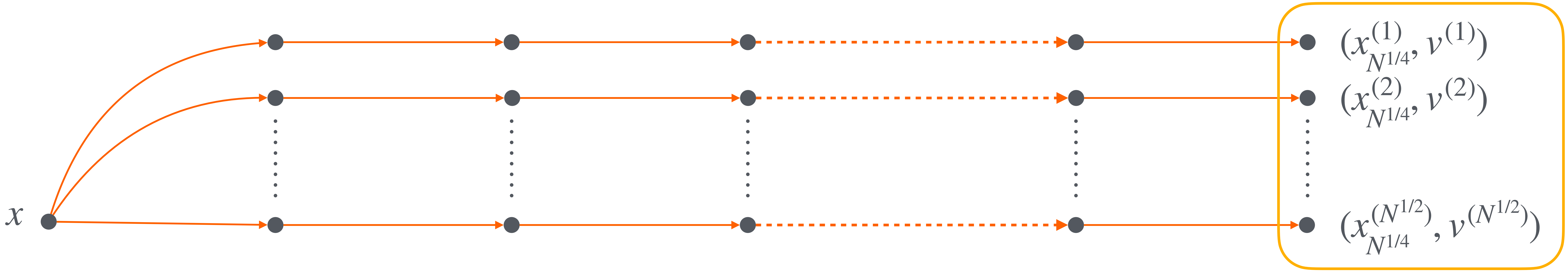
Finding GA-Dlogs

Multiple

$N = |\mathcal{G}|$

$N^{1/4}$ instances

HINT



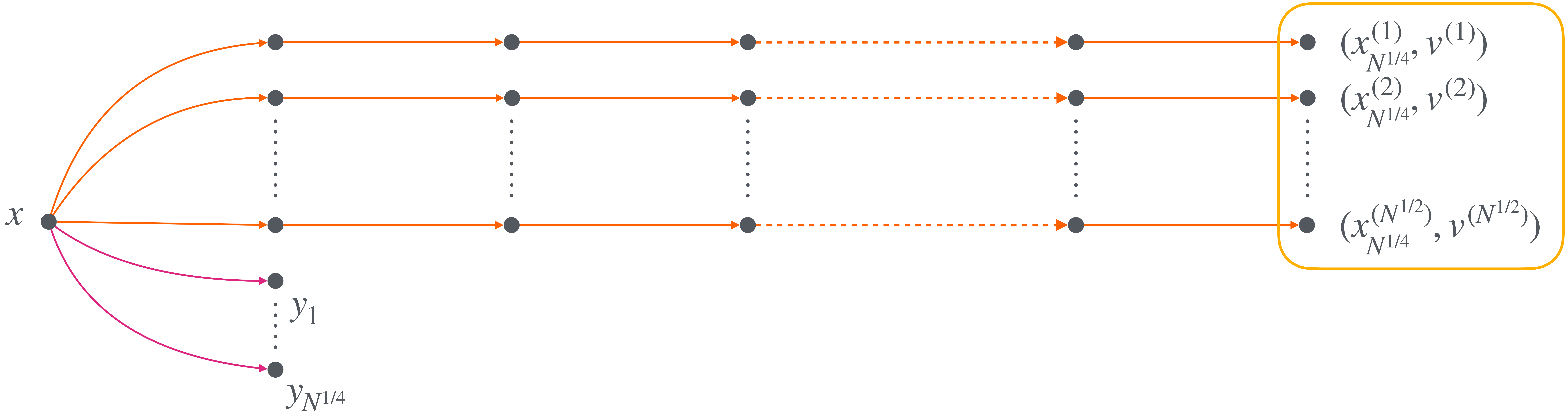
Finding GA-Dlogs

Multiple

$N = |\mathcal{G}|$

$N^{1/4}$ instances

HINT



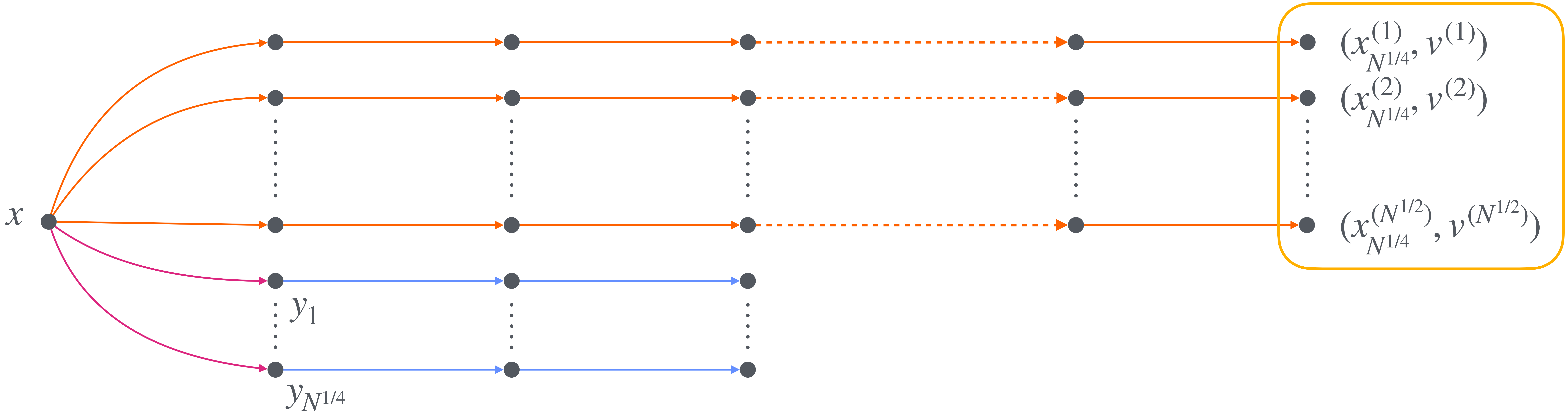
Finding GA-Dlogs

Multiple

$N = |\mathcal{G}|$

$N^{1/4}$ instances

HINT



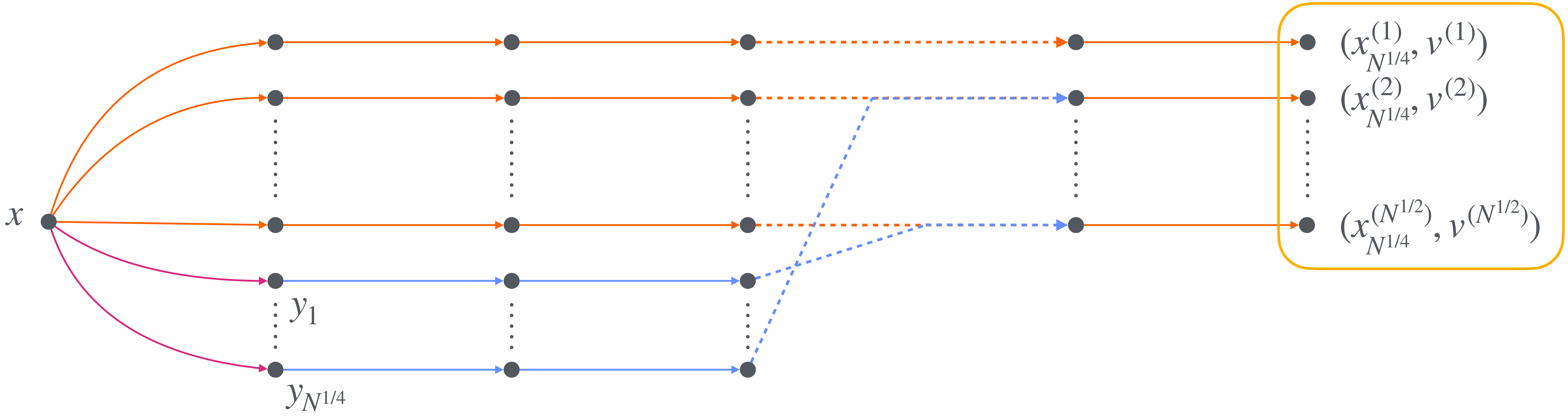
Finding GA-Dlogs

Multiple

$N = |\mathcal{G}|$

$N^{1/4}$ instances

HINT



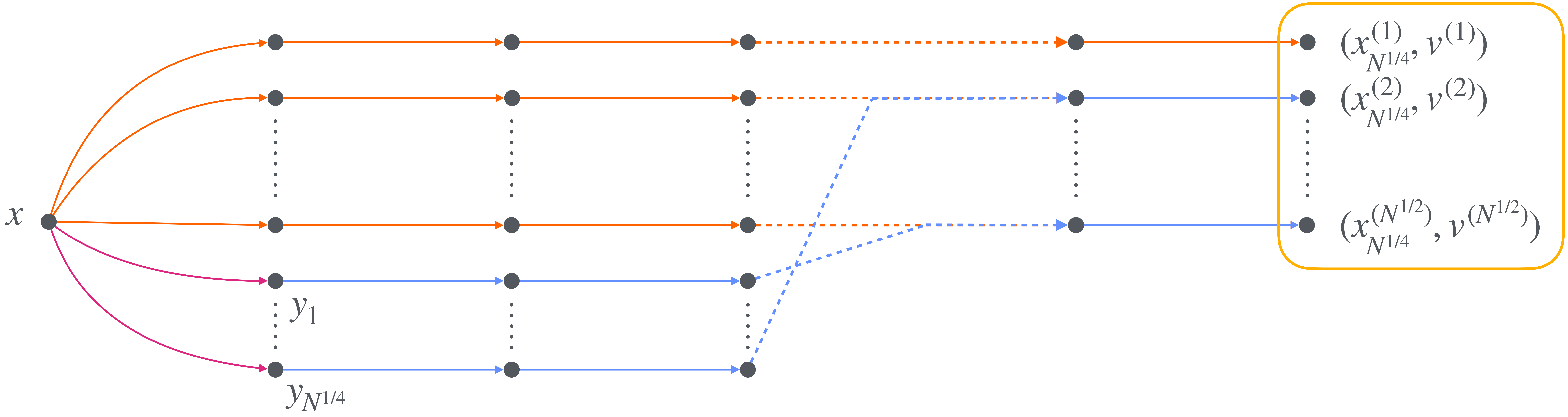
Finding GA-Dlogs

Multiple

$N = |\mathcal{G}|$

$N^{1/4}$ instances

HINT



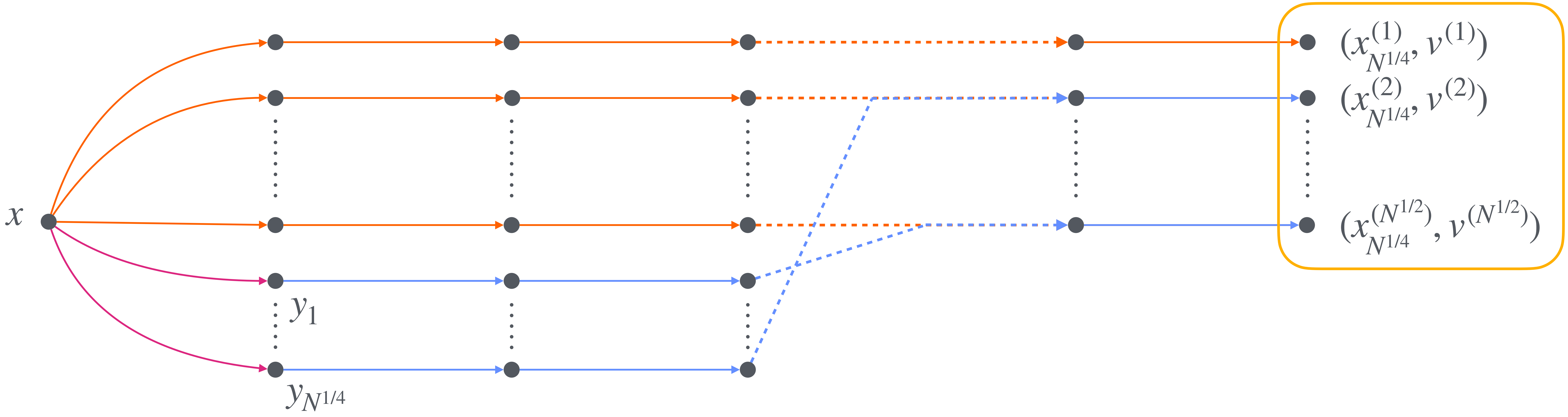
Finding GA-Dlogs

Multiple

$N = |\mathcal{G}|$

$N^{1/4}$ instances

HINT



Precomputation: $N^{1/4} \cdot N^{1/2} = N^{3/2}$

Space: $N^{1/2}$

Online: $N^{1/4} \cdot N^{1/4} = N^{1/2}$ (expected)

→ Solve ALL GA-Dlog with Constant Success Probability

Finding GA-Dlogs

Multiple, “without” Precomputation

Finding GA-Dlogs

Multiple, "without" Precomputation

Naïvely

Repeat the $N^{1/2}$ algorithm m times	→	Solve ALL m GA-Dlog in time $m \cdot N^{1/2}$

Finding GA-Dlogs

Multiple, "without" Precomputation

Naïvely

Repeat the $N^{1/2}$ algorithm m times	→	Solve ALL m GA-Dlog in time $m \cdot N^{1/2}$

Balancing Precomputation and Online times...

Precomputation: $m^{1/2} \cdot N^{1/2}$ Space: m Online: $m^{1/2} \cdot N^{1/2}$	→	Solve ALL m GA-Dlog with runtime $m^{1/2} \cdot N^{1/2}$

Experiments

On CSIDH

From the Theorems...	In practice...

Experiments

On CSIDH

From the Theorems...	In practice...
The probability of success of the online phase is $\geq 1/8$ ↓ On average, online phase needs to be repeated 8 times	

Experiments

On CSIDH

From the Theorems...

The probability of success of the online phase is $\geq 1/8$

↓

On average, online phase needs to be repeated 8 times

In practice...

$\log N$	# of runs
5	1.3
8	1.0
10	1.2
12	1.0
15	1.0
18	1.0
21	1.1
24	1.2
27	1.1
29	1.1

Summary

Precomputation Attacks for Dlog can be extended to the GA-Dlog framework

New multi-instance “without” precomputation attack as a corollary

In practice, the technique performs better than in theory

Summary

Precomputation Attacks for Dlog can be extended to the GA-Dlog framework

New multi-instance “<u>without</u>” precomputation attack as a corollary

In practice, the technique performs better than in theory

Thank you!

Questions?

ePrint 2024/564