That's AmorE Amortized Efficiency for Pairing Delegation

ia.cr/2025/542



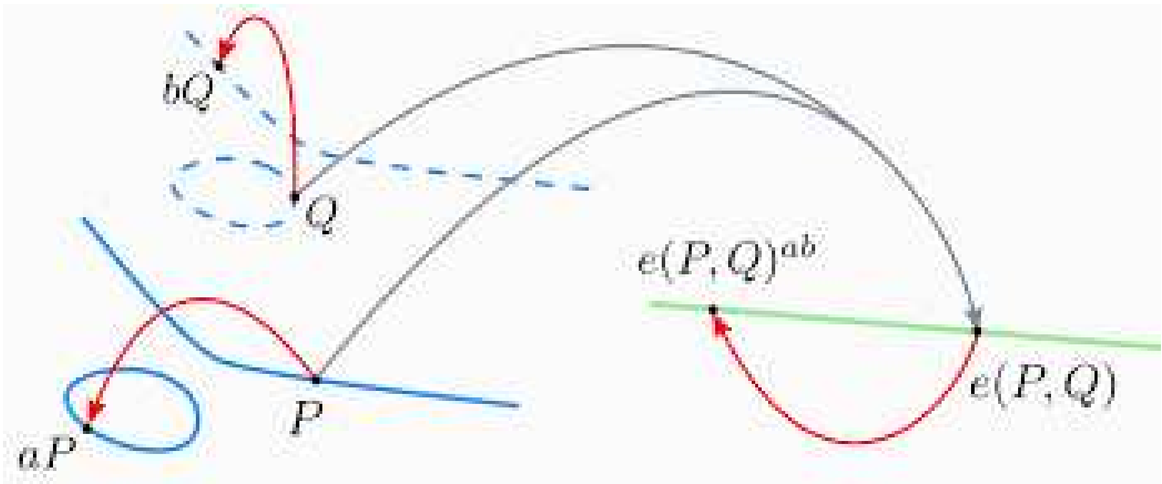

Adrian P. Keilty *Diego F. Aranha* *Elena Pagnin* *Francisco Rodríguez Henríquez*

Affiliations: AarhusU (DK), ChalmersU (SE), GöteborgU (SE), TII (UAE)

What are "Pairings"?

bilinear maps on ***groups***

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

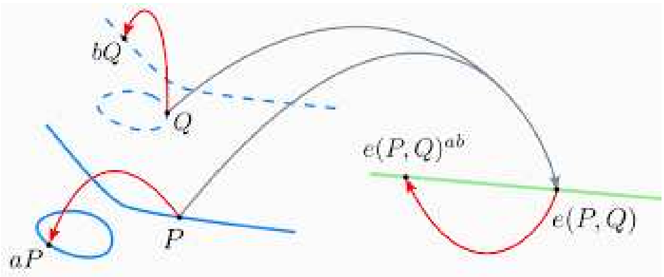


$$e(aP, bQ) = e(P, Q)^{ab}$$

What are "Pairings"?

bilinear maps on ***groups***

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$



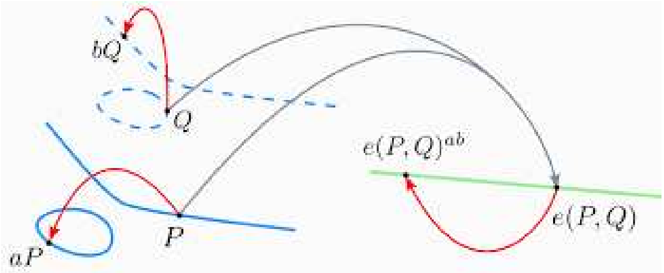
$$e(aP, bQ) = e(P,Q)^{ab}$$

... in Cryptography

What are "Pairings"?

bilinear maps on ***groups***

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$



$$e(aP, bQ) = e(P,Q)^{ab}$$

... in Cryptography

very abridged reference list

Joux: A **one round** protocol for **tripartite** Diffie-Hellman (2000)
Boneh, Lynn,Shacham: **Short Signatures** from the Weil Pairing (2004)
Sahai, Waters: **Fuzzy identity-based encryption** (2005)
Kate,Zaverucha,Goldberg: **Constant-size commitments to polynomials** [..] (2010)
Groth: **Short** pairing-based **non-interactive** zero-knowledge **arguments** (2010)
Boneh,Drijvers,Neven: **Compact multi-signatures** for smaller blockchains (2018)
Gailly,Maller,Nitulescu, : **SnarkPack**: Practical SNARK aggregation (2022)
Garg,Jain,Mukherjee+: **hints**: Threshold signatures with silent setup (2024)

So, What's the Catch?

costs in 10^3 clock cycles on BLS12-381

So, What's the Catch?

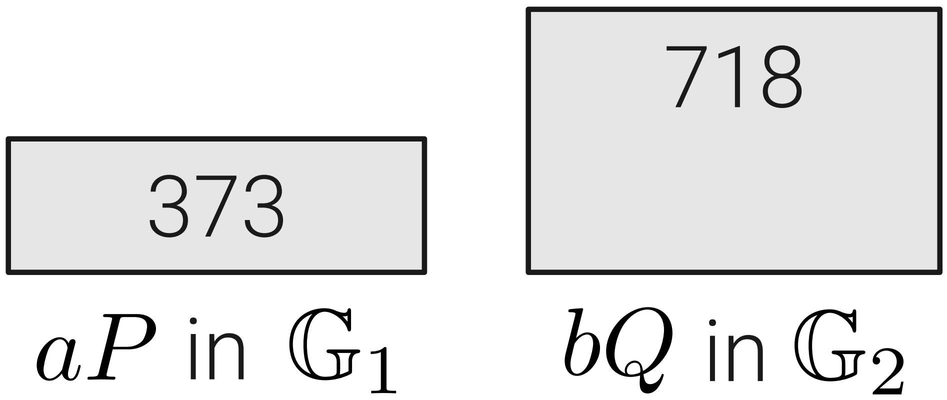
costs in 10^3 clock cycles on BLS12-381

373

aP in $\mathbb{G}_1$

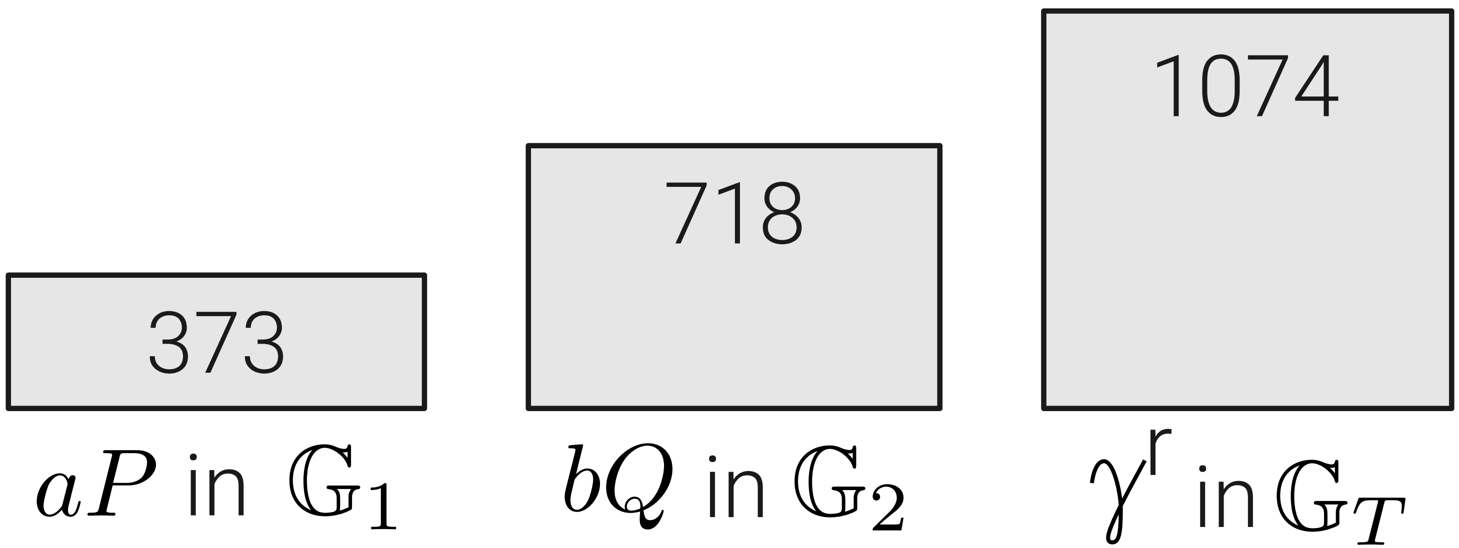
So, What's the Catch?

costs in 10^3 clock cycles on BLS12-381

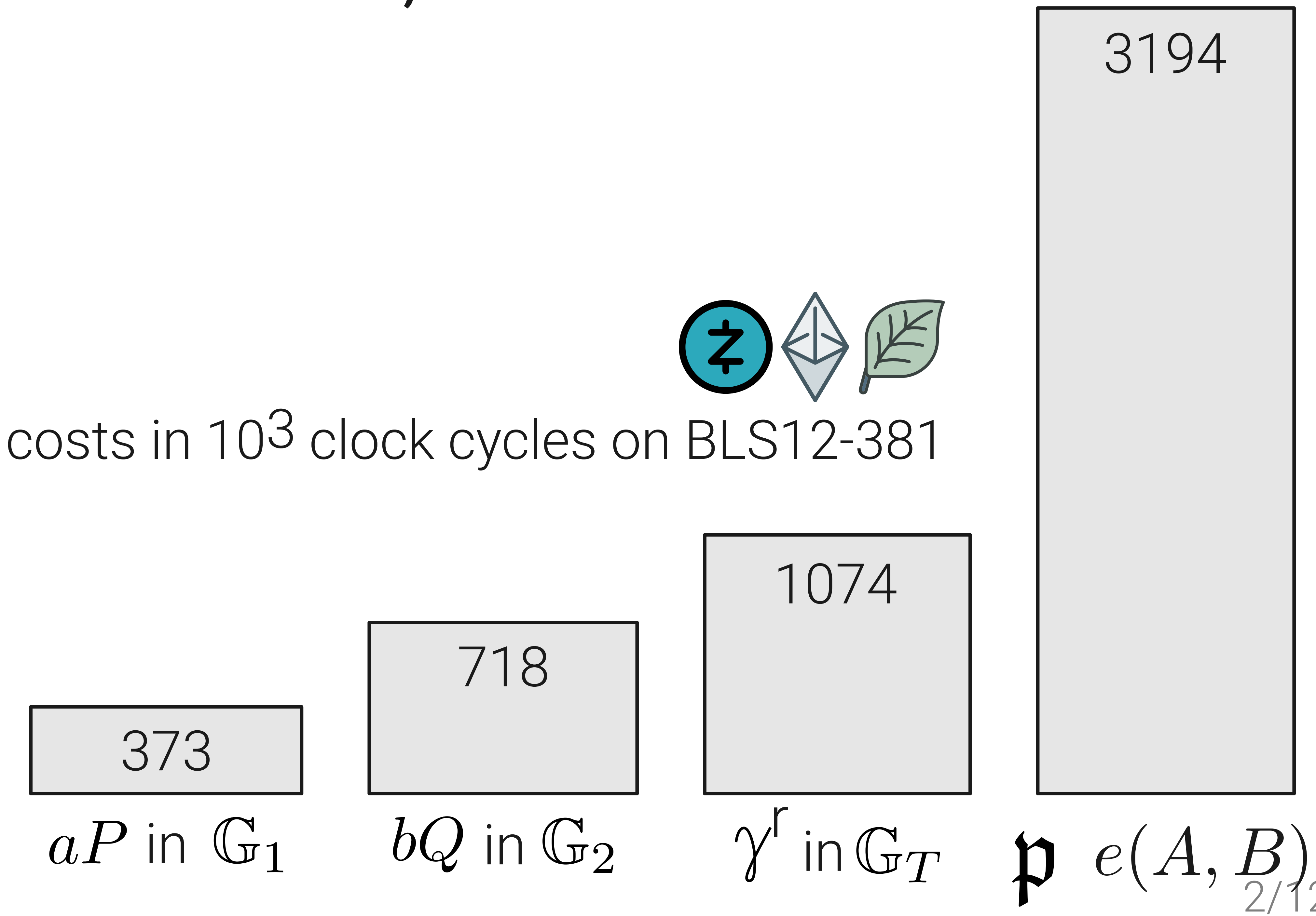


So, What's the Catch?

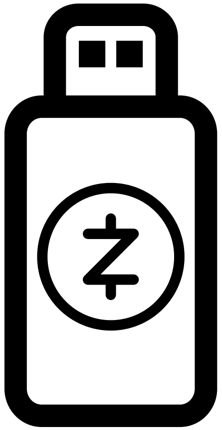
costs in 10^3 clock cycles on BLS12-381



So, What's the Catch?

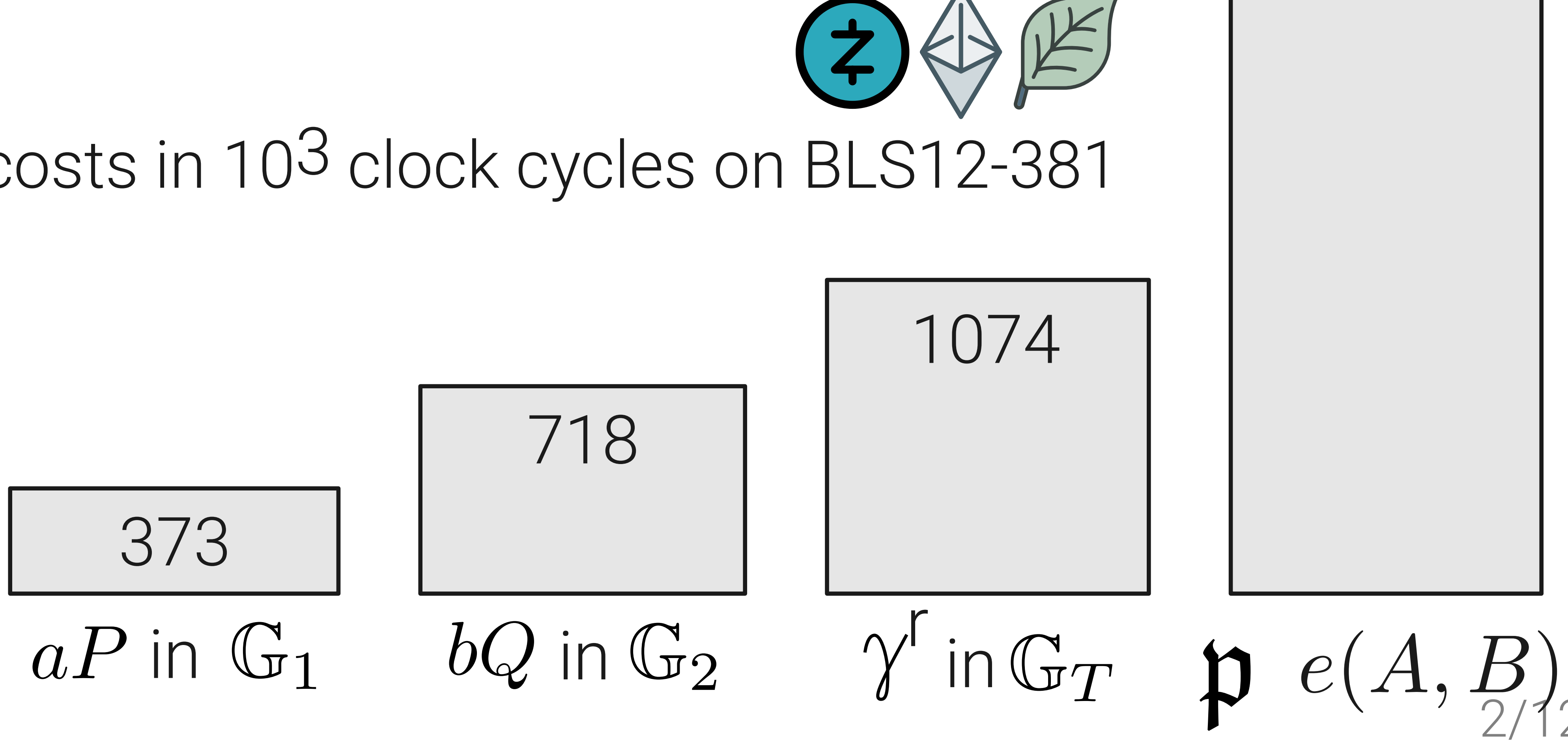


So, What's the Catch?



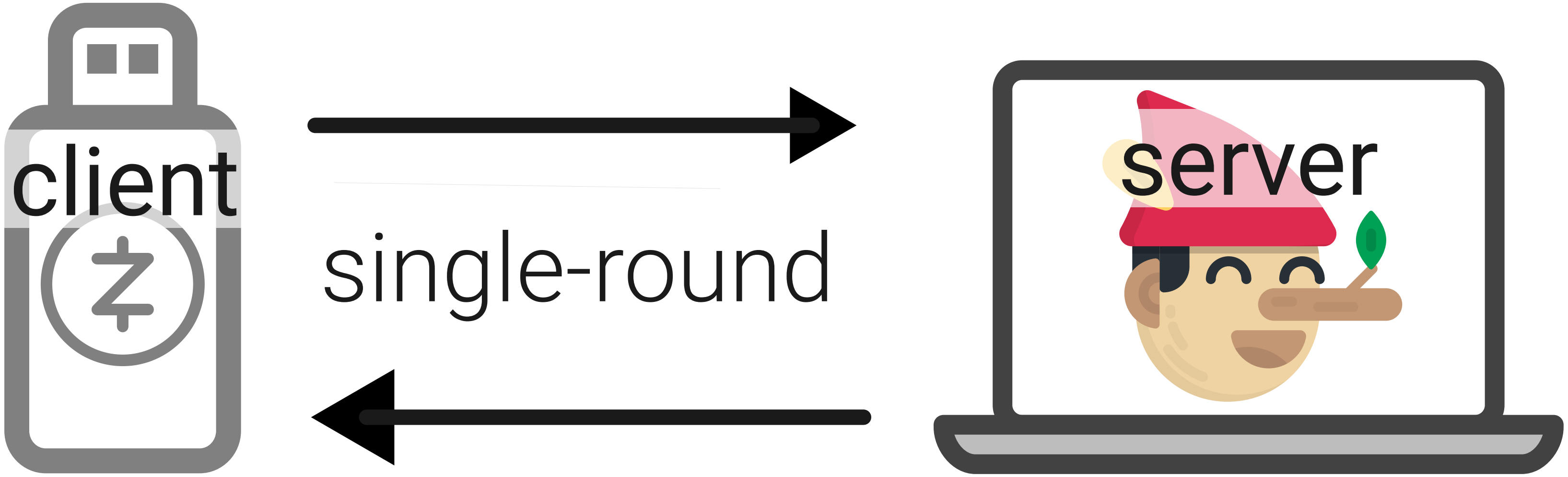
pairings are ***prohibitive***
on weaker IoT devices
(incl. hardware wallets)

costs in 10^3 clock cycles on BLS12-381



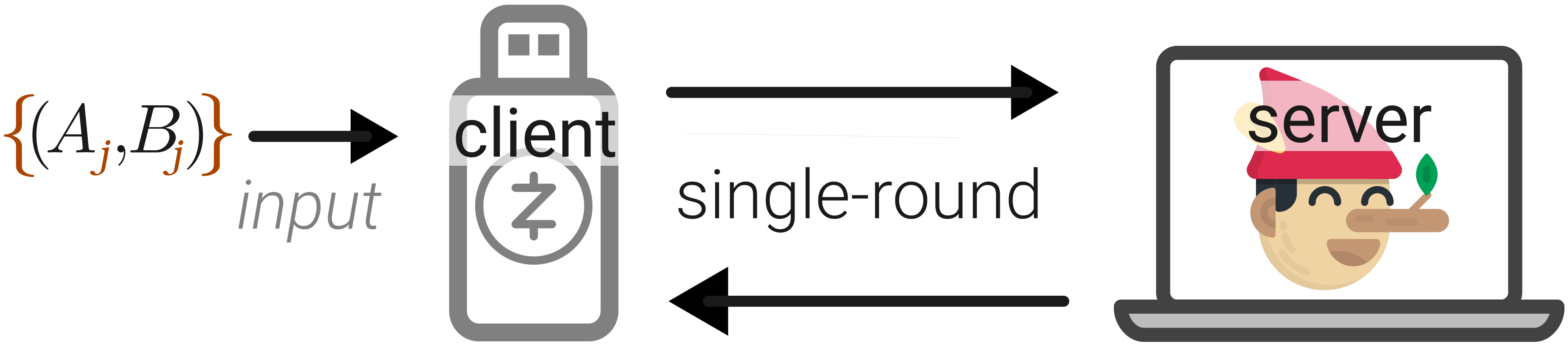
Pairing Delegation Protocols

since 2005



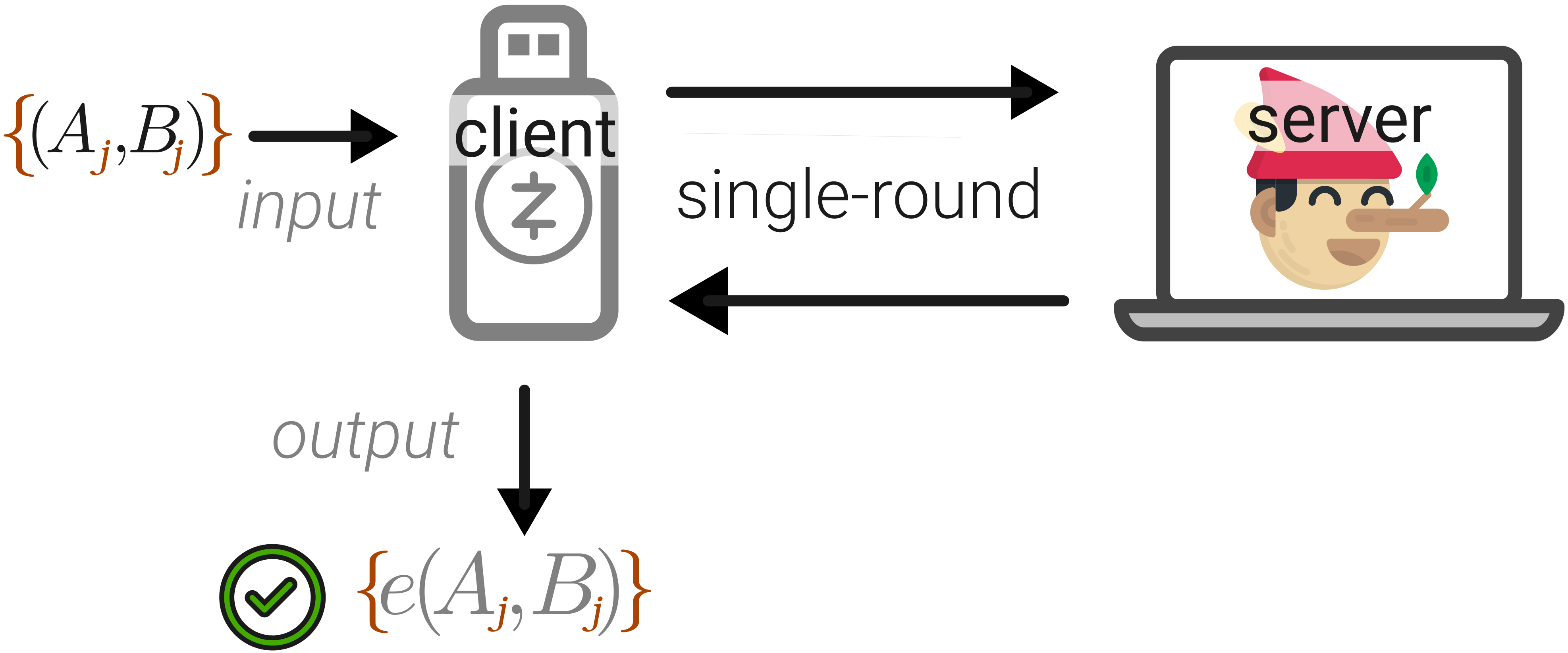
Pairing Delegation Protocols

since 2005



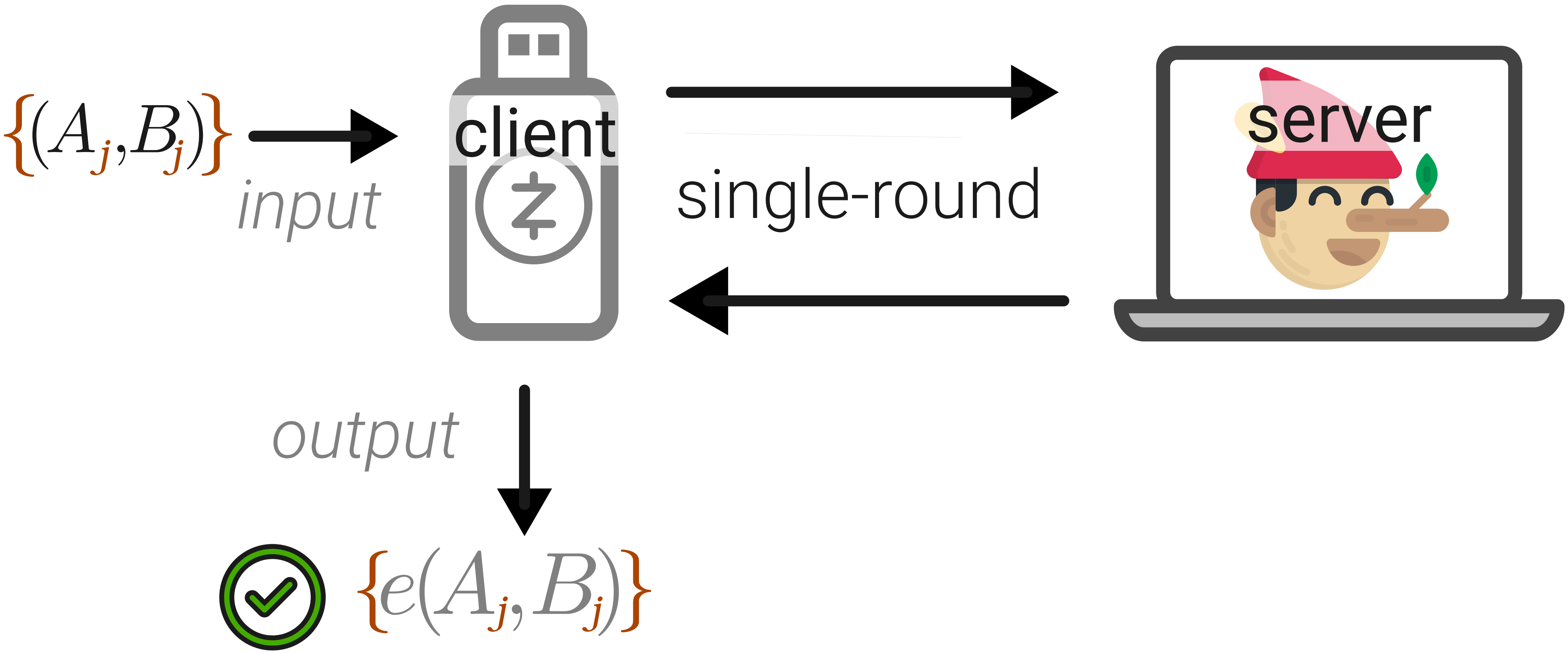
Pairing Delegation Protocols

since 2005

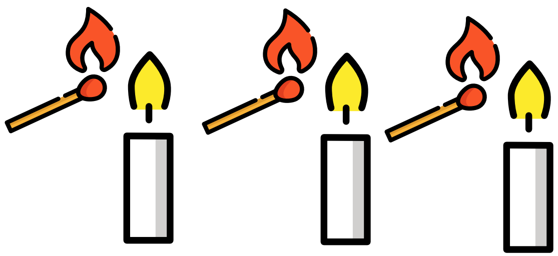


Pairing Delegation Protocols

since 2005



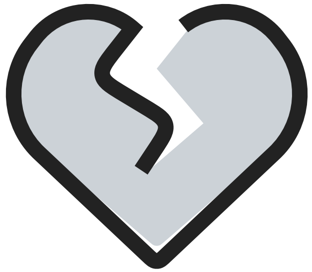
The one-shot framework



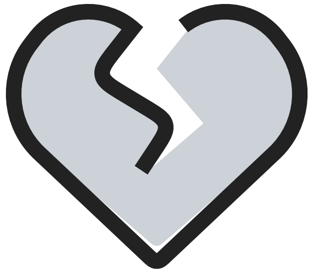
Client PreComp + **One Delegation**

State of the Art

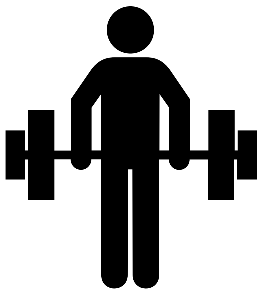
State of the Art

Category 1   2 recent protocols broken by *our work*

State of the Art

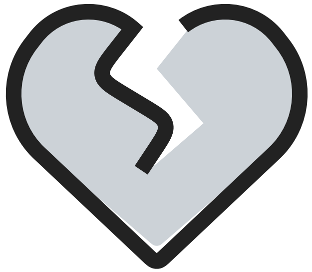
Category 1  

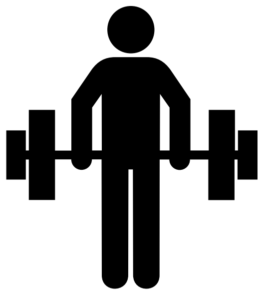
2 recent protocols broken by *our work*

Category 2  

unconditional security one-shot framework

State of the Art

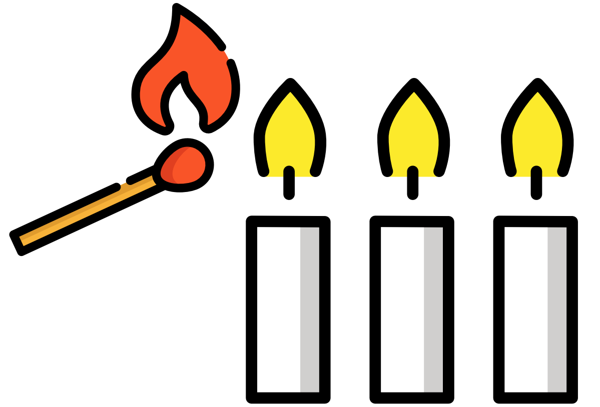
Category 1   2 recent protocols broken by *our work*

Category 2   unconditional security one-shot framework

WANTED: a pairing delegation protocol that is

reasonably *secure* **and** *efficient*

Our Approach

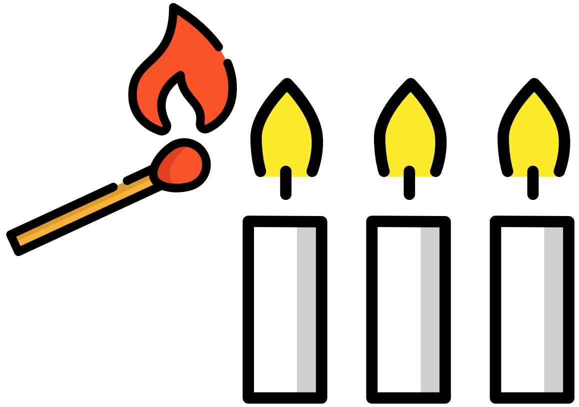


1. ~~one-shot~~ **Sequential Framework**

Client PreComp + *Delegation 1* + + *Delegation N*

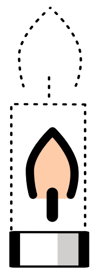
Our Approach

1. ~~one-shot~~ **Sequential Framework**

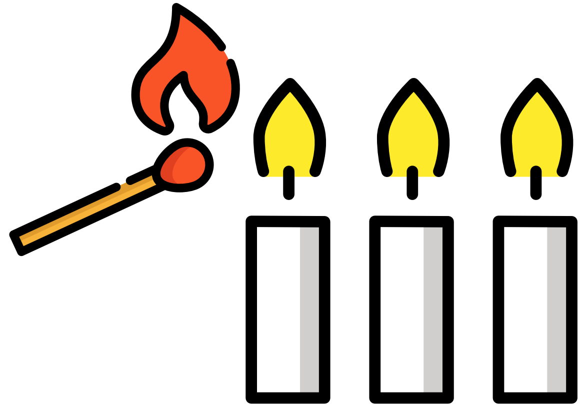


Client PreComp + *Delegation 1* + + *Delegation N*

2. ~~unconditional~~ **Everlasting Security**

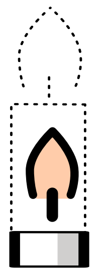


Our Approach



1. ~~one-shot~~ **Sequential Framework**

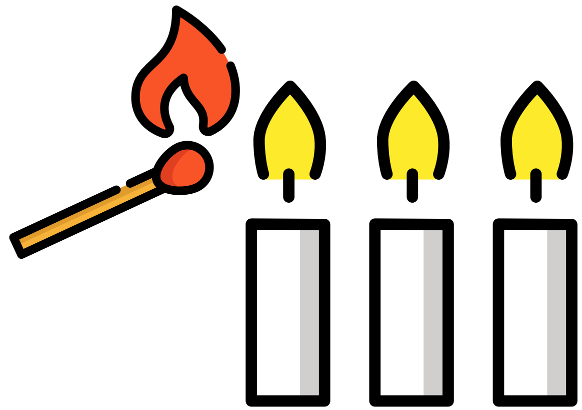
Client PreComp + *Delegation 1* + + *Delegation N*



2. ~~unconditional~~ **Everlasting Security**

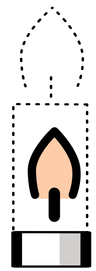
3. ~~oddly powerful~~ **Realistic Adversaries**

Our Approach



1. ~~one-shot~~ **Sequential Framework**

Client PreComp + *Delegation 1* + + *Delegation N*



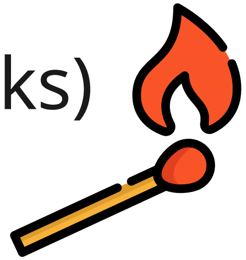
2. ~~unconditional~~ **Everlasting Security**

3. ~~oddly powerful~~ **Realistic Adversaries**

4. **New Security Assumption**

Our Contribution

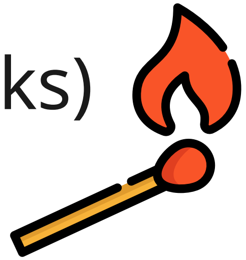
1. **Impossibility result** (inspired by our new attacks)



- client PreComp needs to be expensive

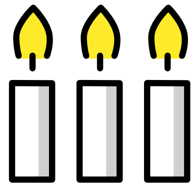
Our Contribution

1. **Impossibility result** (inspired by our new attacks)



- client PreComp needs to be expensive

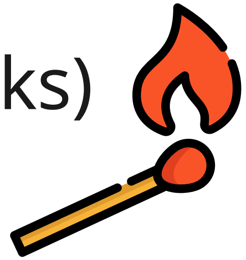
2. A **Framework** for **Sequential** Pairing Delegation



- cost(PreCom) is amortized over several delegations

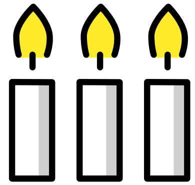
Our Contribution

1. **Impossibility result** (inspired by our new attacks)



- client PreComp needs to be expensive

2. A **Framework** for **Sequential** Pairing Delegation

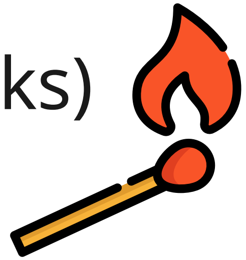


- cost(PreCom) is amortized over several delegations

3. The **AmorE Protocol** (Amortized Efficiency)

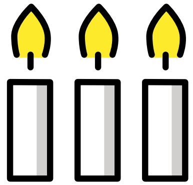
Our Contribution

1. **Impossibility result** (inspired by our new attacks)



   client PreComp needs to be expensive

2. A **Framework** for **Sequential** Pairing Delegation



   cost(PreCom) is amortized over several delegations

3. The **AmorE Protocol** (Amortized Efficiency)

4. A **Novel Proof Technique**

Our Contribution

1. **Impossibility result** (inspired by our new attacks)

   client PreComp needs to be expensive

2. A **Framework** for **Sequential** Pairing Delegation

   cost(PreCom) is amortized over several delegations

3. The **AmorE Protocol** (Amortized Efficiency)

4. A **Novel Proof Technique**

5. **Experimental Validation**

   and Efficient Short Scalar Sampling

Our Contribution

1. **Impossibility result** (inspired by our new attacks)

   client PreComp needs to be expensive

2. A **Framework** for **Sequential** Pairing Delegation

   cost(PreCom) is amortized over several delegations

3. The **AmorE Protocol** (Amortized Efficiency)

4. A **Novel Proof Technique**

5. **Experimental Validation**

   and Efficient Short Scalar Sampling

AmorE
in a Nutshell

AmorE in a Nutshell

OneTimeSetup

$$\xi \xleftarrow{\$} \mathbb{G}_T$$

$$\mathsf{t}_{\mathsf{start}} \leftarrow \texttt{time.now}()$$

AmorE in a Nutshell

exponentiation in $\mathbb{G}_T$

time lapse check

OneTimeSetup

$\xi \xleftarrow{\$} \mathbb{G}_T$

$\mathtt{t}_{\mathsf{start}} \leftarrow \mathtt{time.now}()$

AmorE in a Nutshell

OneTimeSetup

$\xi \xleftarrow{\$} \mathbb{G}_T$

$\mathsf{t}_{\mathsf{start}} \leftarrow \texttt{time.now}()$

exponentiation in $\mathbb{G}_T$

time lapse check

↓

Setup$(\overrightarrow{A}, \overrightarrow{B})$

$r_j \xleftarrow{\$} \{1, \ldots, 2^{\varphi}\} \subsetneq \mathbb{Z}_q^*,$

$\mathsf{pub} \xleftarrow{\$} \mathsf{routine}\left(\overrightarrow{A}, \overrightarrow{B}, \overrightarrow{r}\right)$

AmorE in a Nutshell

OneTimeSetup

$\xi \xleftarrow{\$} \mathbb{G}_T$

$\texttt{t}_{\text{start}} \leftarrow \texttt{time.now}()$

exponentiation in $\mathbb{G}_T$

time lapse check

$\downarrow$

Setup$(\overrightarrow{A}, \overrightarrow{B})$

$r_j \xleftarrow{\$} \{1, \ldots, 2^{\varphi}\} \subsetneq \mathbb{Z}_q^*,$

$\text{pub} \xleftarrow{\$} \text{routine}\left(\overrightarrow{A}, \overrightarrow{B}, \overrightarrow{r}\right)$

φ : efficiency

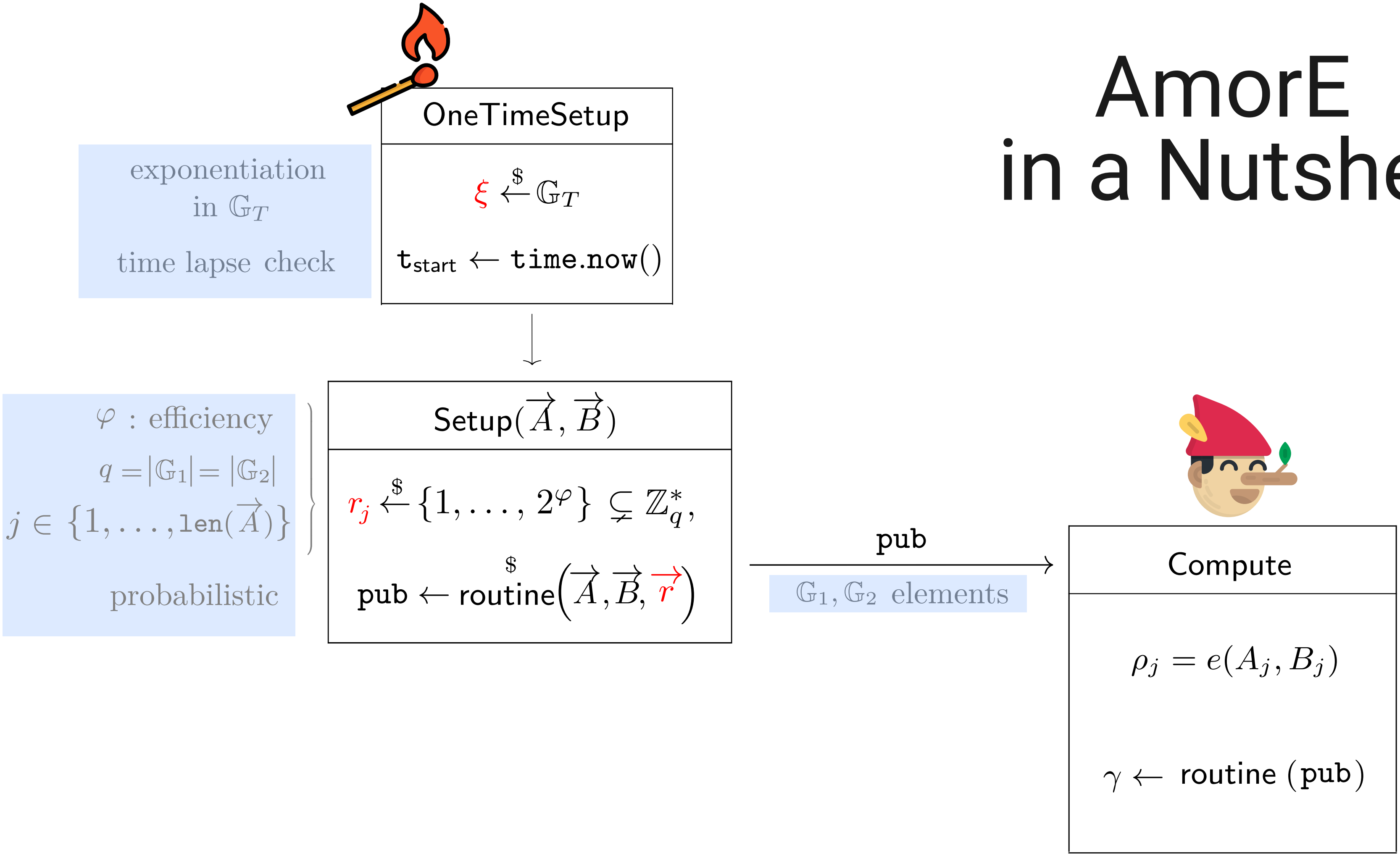
$q = |\mathbb{G}_1| = |\mathbb{G}_2|$

$j \in \{1, \ldots, \texttt{len}(\overrightarrow{A})\}$

probabilistic

$\mathbb{G}_1, \mathbb{G}_2$ elements

AmorE in a Nutshell



AmorE in a Nutshell

OneTimeSetup

$\xi \xleftarrow{\$} \mathbb{G}_T$

$\mathtt{t}_{\mathsf{start}} \leftarrow \mathtt{time.now}()$

exponentiation in $\mathbb{G}_T$

time lapse check

Setup$(\vec{A}, \vec{B})$

$r_j \xleftarrow{\$} \{1, \ldots, 2^{\varphi}\} \subsetneq \mathbb{Z}_q^*,$

$\mathtt{pub} \xleftarrow{\$} \mathsf{routine}(\vec{A}, \vec{B}, \vec{r})$

φ : efficiency

$q = |\mathbb{G}_1| = |\mathbb{G}_2|$

$j \in \{1, \ldots, \mathtt{len}(\vec{A})\}$

probabilistic

$\mathtt{pub}$ →

$\mathbb{G}_1, \mathbb{G}_2$ elements

Compute

$\rho_j = e(A_j, B_j)$

$\gamma \leftarrow \mathsf{routine}(\mathtt{pub})$

pairing evaluations

deterministic

AmorE in a Nutshell

OneTimeSetup

$\xi \xleftarrow{\$} \mathbb{G}_T$

$\mathsf{t}_{\mathsf{start}} \leftarrow \mathtt{time.now}()$

exponentiation in $\mathbb{G}_T$

time lapse check

Setup$(\vec{A}, \vec{B})$

$r_j \xleftarrow{\$} \{1, \ldots, 2^{\varphi}\} \subsetneq \mathbb{Z}_q^*,$

$\mathtt{pub} \leftarrow \mathsf{routine}^{\$}\left(\vec{A}, \vec{B}, \vec{r}\right)$

φ : efficiency

$q = |\mathbb{G}_1| = |\mathbb{G}_2|$

$j \in \{1, \ldots, \mathtt{len}(\vec{A})\}$

probabilistic

$\mathtt{pub}$ →

$\mathbb{G}_1, \mathbb{G}_2$ elements

Compute

$\rho_j = e(A_j, B_j)$

$\gamma \leftarrow \mathsf{routine}\,(\mathtt{pub})$

pairing evaluations

deterministic

← $\mathtt{out} = (\gamma, \vec{\rho})$

$\mathbb{G}_T$ elements

Verify

$\mathtt{time.now}() - \mathsf{t}_{\mathsf{start}} \stackrel{?}{>} \tau$

$\rho_j \stackrel{?}{\in} \mathbb{G}_T$

$\xi \stackrel{?}{=} \left(\prod_{j=1}^{\mathtt{len}(\vec{A})} \rho_j^{r_j}\right) \cdot \gamma$

AmorE in a Nutshell

OneTimeSetup

$\xi \xleftarrow{\$} \mathbb{G}_T$

$\mathtt{t}_{\mathsf{start}} \leftarrow \mathtt{time.now}()$

exponentiation in $\mathbb{G}_T$

time lapse check

Setup$(\vec{A}, \vec{B})$

$r_j \xleftarrow{\$} \{1, \ldots, 2^{\varphi}\} \subsetneq \mathbb{Z}_q^*,$

$\mathtt{pub} \xleftarrow{\$} \mathsf{routine}(\vec{A}, \vec{B}, \vec{r})$

φ : efficiency

$q = |\mathbb{G}_1| = |\mathbb{G}_2|$

$j \in \{1, \ldots, \mathtt{len}(\vec{A})\}$

probabilistic

pub →

$\mathbb{G}_1, \mathbb{G}_2$ elements

Compute

$\rho_j = e(A_j, B_j)$

$\gamma \leftarrow \mathsf{routine}\,(\mathtt{pub})$

pairing evaluations

deterministic

← $\mathtt{out} = (\gamma, \vec{\rho})$

$\mathbb{G}_T$ elements

Verify

$\mathtt{time.now}() - \mathtt{t}_{\mathsf{start}} \overset{?}{>} \tau$

$\rho_j \overset{?}{\in} \mathbb{G}_T$

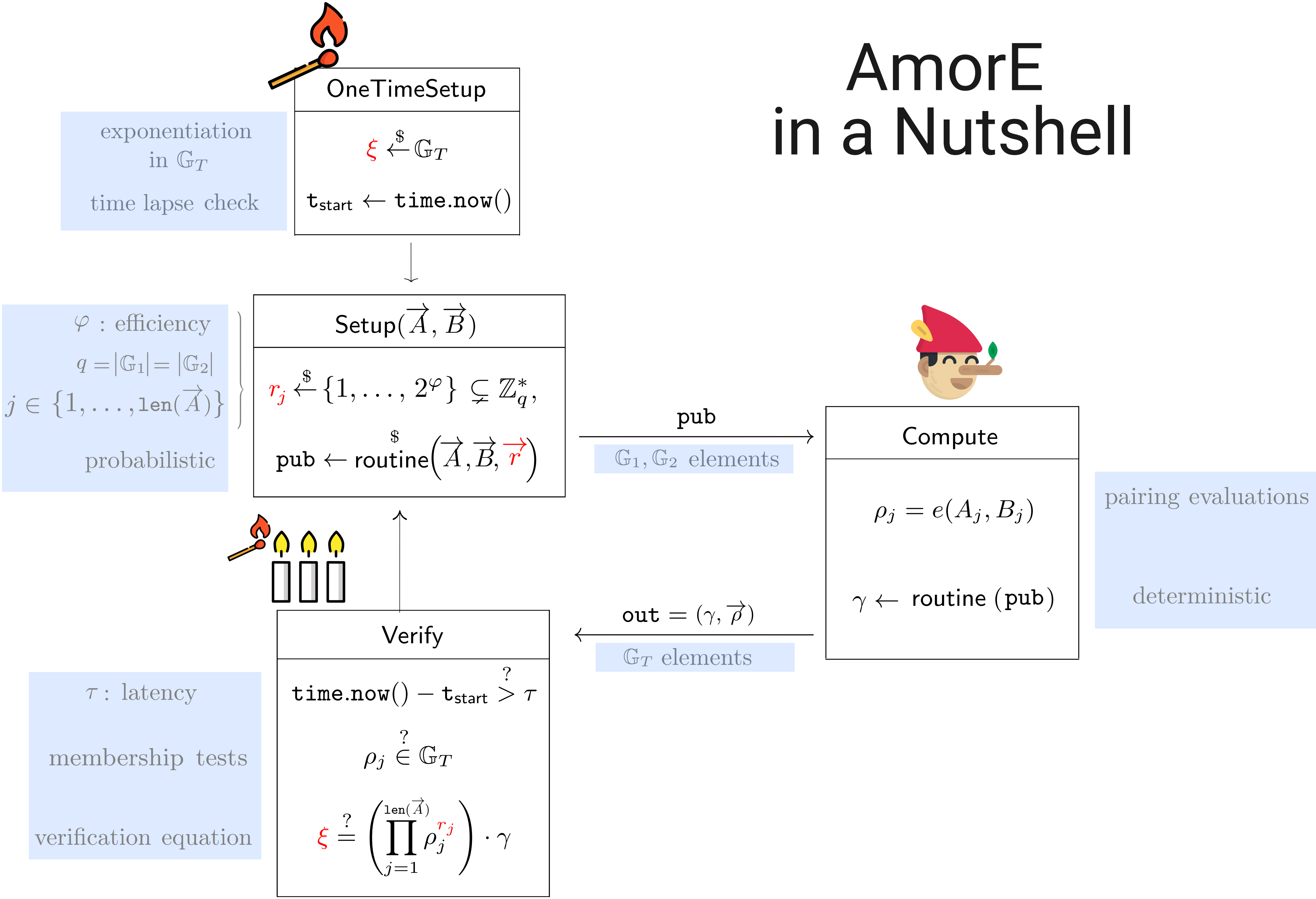
$\xi \overset{?}{=} \left(\prod_{j=1}^{\mathtt{len}(\vec{A})} \rho_j^{r_j} \right) \cdot \gamma$

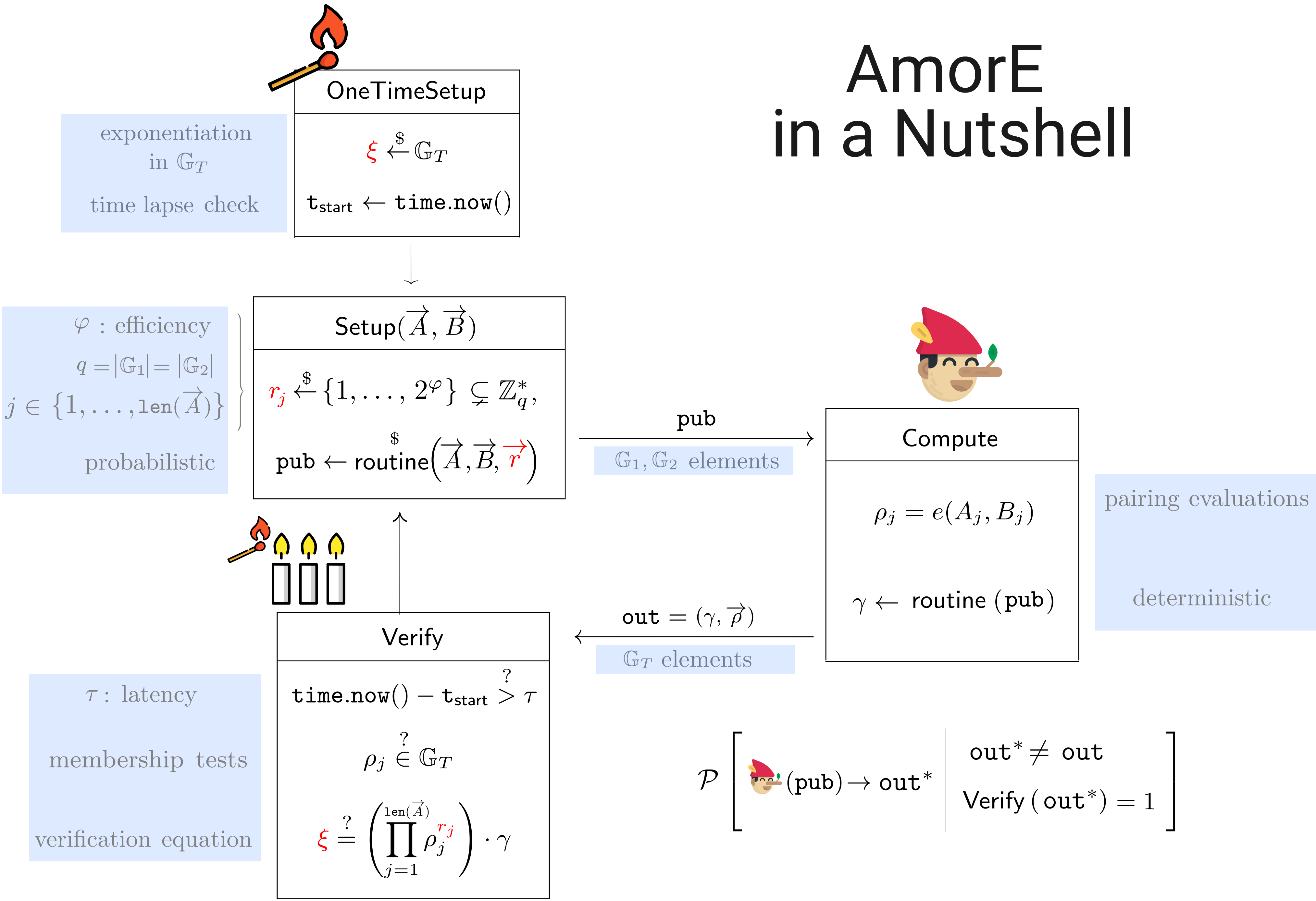
τ : latency

membership tests

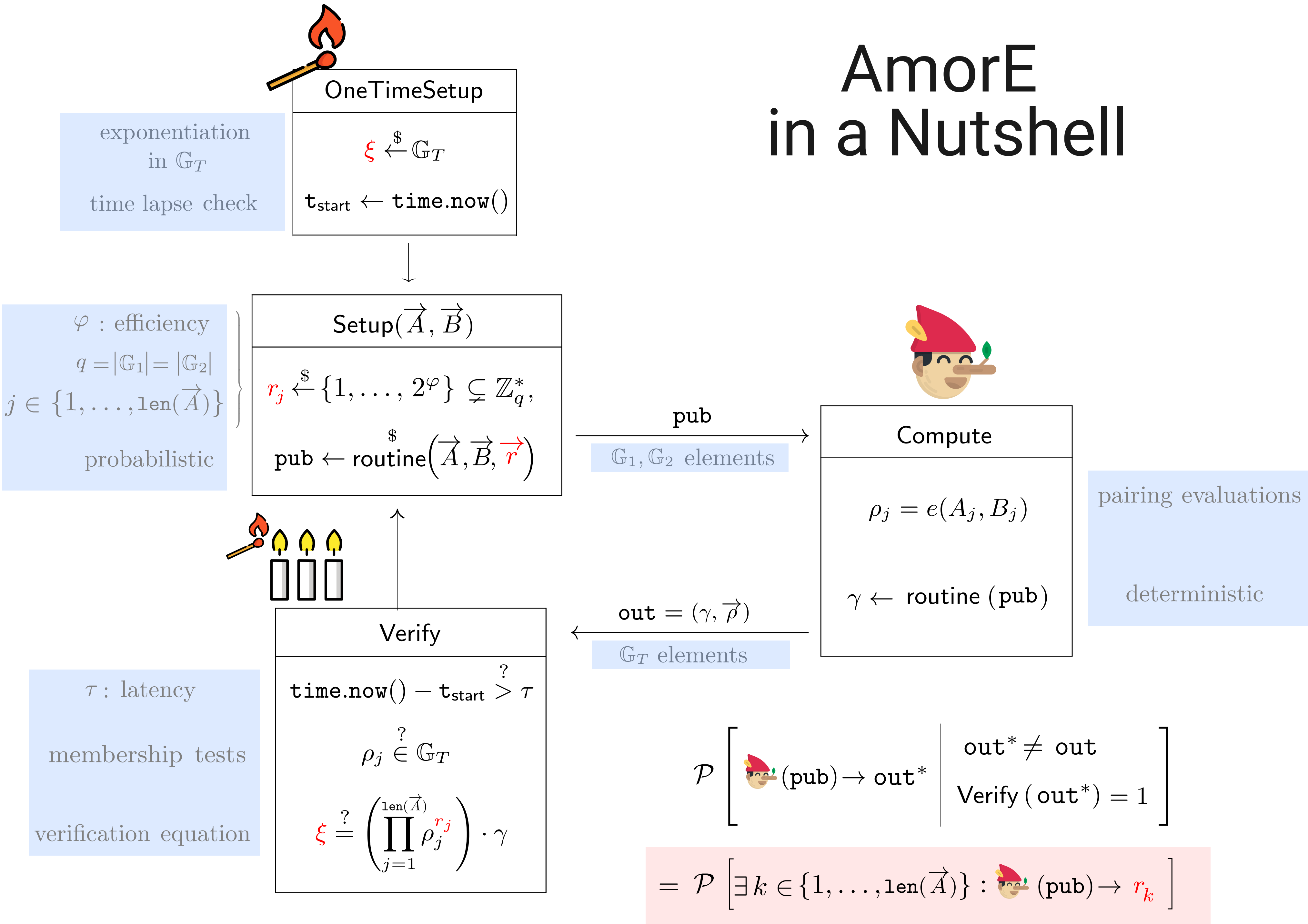
verification equation

AmorE in a Nutshell




AmorE
in a Nutshell
exponentiation in $\mathbb{G}_T$
time lapse check
OneTimeSetup
$\xi \xleftarrow{\$} \mathbb{G}_T$
$\mathsf{t}_{\mathsf{start}} \leftarrow \mathtt{time.now}()$
φ : efficiency
$q = |\mathbb{G}_1| = |\mathbb{G}_2|$
$j \in \{1, \dots, \mathtt{len}(\vec{A})\}$
probabilistic
Setup$(\vec{A}, \vec{B})$
$r_j \xleftarrow{\$} \{1, \dots, 2^{\varphi}\} \subsetneq \mathbb{Z}_q^*,$
$\mathtt{pub} \xleftarrow{\$} \mathsf{routine}(\vec{A}, \vec{B}, \vec{r})$
pub
$\mathbb{G}_1, \mathbb{G}_2$ elements
Compute
$\rho_j = e(A_j, B_j)$
$\gamma \leftarrow \mathsf{routine}(\mathtt{pub})$
pairing evaluations
deterministic
$\mathtt{out} = (\gamma, \vec{\rho})$
$\mathbb{G}_T$ elements
τ : latency
membership tests
verification equation
Verify
$\mathtt{time.now}() - \mathsf{t}_{\mathsf{start}} \overset{?}{>} \tau$
$\rho_j \overset{?}{\in} \mathbb{G}_T$
$\xi \overset{?}{=} \left(\prod_{j=1}^{\mathtt{len}(\vec{A})} \rho_j^{r_j} \right) \cdot \gamma$
$\mathcal{P}\left[(\mathtt{pub}) \rightarrow \mathtt{out}^* \;\middle|\; \begin{array}{l} \mathtt{out}^* \neq \mathtt{out} \\ \mathsf{Verify}(\mathtt{out}^*) = 1 \end{array} \right]$

AmorE in a Nutshell



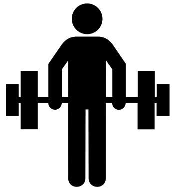
Security and Efficiency Trade-Off

Security and Efficiency Trade-Off

Unconditional

Security and Efficiency Trade-Off

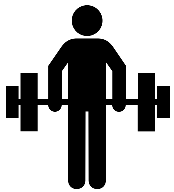
Unconditional $\iff$



`pub` is expensive

Security and Efficiency Trade-Off

Unconditional $\iff$

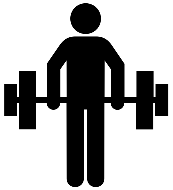


`pub` is expensive $\iff$ $\color{red}{\vec{r}}$ masked

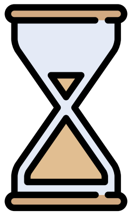
Security and Efficiency Trade-Off


Unconditional

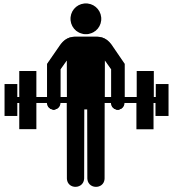
$\Longleftrightarrow$


`pub` is expensive

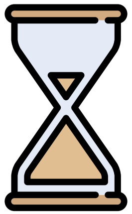
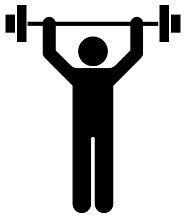
$\Longleftrightarrow$ $\vec{r}$ masked


Time-bound

Security and Efficiency Trade-Off

 $\iff$  $\iff$ $\vec{r}$ masked

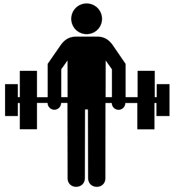
Unconditional — `pub` is expensive

 $\rightsquigarrow$ 

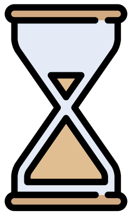
Time-bound — `pub` is cheap

Security and Efficiency Trade-Off

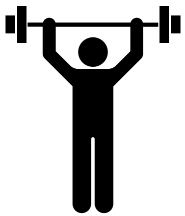
Unconditional $\Longleftrightarrow$



`pub` is expensive $\Longleftrightarrow$ $\vec{r}$ masked



Time-bound $\leadsto$



`pub` is cheap

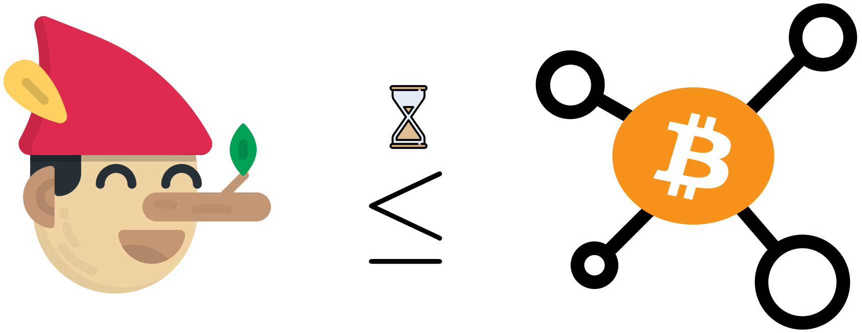
...but $\vec{r}$ extractable after x computations

Adversary Bound

Adversary Bound

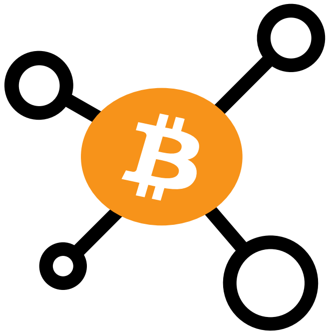
$\leq$

Adversary Bound



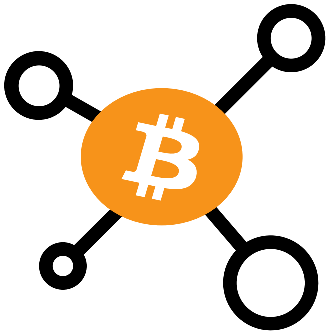
Adversary Bound

$\leq$



$\leq \quad 2^{70}\ \mathrm{H/s}$

Adversary Bound

  $\leq$  $\leq \quad 2^{70}\ \mathrm{H/s} \quad \leq \quad 2^{70}\ \bar{\mathfrak{m}}_{\iota}/\mathrm{s}$

(Fair) assumption:

$$\mathsf{cost}\left(\text{block header hash}\right) < \mathsf{cost}\left(\text{short scalar multiplication in } \mathbb{G}_1\right)$$

Security Analysis Intuition

Let $(\mathbb{G} = \langle P \rangle, +)$ be a cyclic group of prime order q and $\varepsilon \xleftarrow{\$} \mathbb{Z}_q^*$, $\xi = [\varepsilon]P$.

Security Analysis Intuition

Let $(\mathbb{G} = \langle P \rangle, +)$ be a cyclic group of prime order q and $\varepsilon \xleftarrow{\$} \mathbb{Z}_q^*$, $\xi = [\varepsilon]P$.

- $r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q^*$
- $r_1, r_2 \xleftarrow{\$} [\![2^\varphi]\!] = \{1, \ldots, 2^\varphi\} \subsetneq \mathbb{Z}_q^*$

Security Analysis Intuition

Let $(\mathbb{G} = \langle P \rangle, +)$ be a cyclic group of prime order q and $\varepsilon \xleftarrow{\$} \mathbb{Z}_q^*$, $\xi = [\varepsilon]P$.

- $r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q^*$

- $r_1, r_2 \xleftarrow{\$} [\![2^\varphi]\!] = \{1, \ldots, 2^\varphi\} \subsetneq \mathbb{Z}_q^*$

$$\text{pub} = \begin{cases} C = [r_1]\xi + X \\ D = [r_2]\xi + Y \end{cases}$$

where $X, Y \in \mathbb{G}$ are public and $X \neq C$, $Y \neq D$

Security Analysis Intuition

Let $(\mathbb{G} = \langle P \rangle, +)$ be a cyclic group of prime order q
and $\varepsilon \xleftarrow{\$} \mathbb{Z}_q^*$, $\xi = [\varepsilon]P$.

- $r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q^*$

- $r_1, r_2 \xleftarrow{\$} [\![2^\varphi]\!] = \{1, \ldots, 2^\varphi\} \subsetneq \mathbb{Z}_q^*$

$$\mathtt{pub} = \begin{cases} C = [r_1]\xi + X \\ D = [r_2]\xi + Y \end{cases}$$

where $X, Y \in \mathbb{G}$ are public
and $X \neq C$, $Y \neq D$

$\Downarrow$

$q - 1$ equiprobable
secret tuples (r_1, r_2, ε)

Security Analysis Intuition

Let $(\mathbb{G} = \langle P \rangle, +)$ be a cyclic group of prime order q and $\varepsilon \xleftarrow{\$} \mathbb{Z}_q^*$, $\xi = [\varepsilon]P$.

- $r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q^*$
- $r_1, r_2 \xleftarrow{\$} [\![2^\varphi]\!] = \{1, \ldots, 2^\varphi\} \subsetneq \mathbb{Z}_q^*$

$$\texttt{pub} = \begin{cases} C = [r_1]\xi + X \\ D = [r_2]\xi + Y \end{cases}$$

where $X, Y \in \mathbb{G}$ are public and $X \neq C$, $Y \neq D$

unconditionally secure

$\Downarrow$

$q - 1$ equiprobable secret tuples (r_1, r_2, ε)

Security Analysis Intuition

Let $(\mathbb{G} = \langle P \rangle, +)$ be a cyclic group of prime order q and $\varepsilon \xleftarrow{\$} \mathbb{Z}_q^*$, $\xi = [\varepsilon]P$.

- $r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q^*$
- $r_1, r_2 \xleftarrow{\$} [\![2^\varphi]\!] = \{1, \ldots, 2^\varphi\} \subsetneq \mathbb{Z}_q^*$

$$\text{pub} = \begin{cases} C = [r_1]\xi + X \\ D = [r_2]\xi + Y \end{cases}$$

where $X, Y \in \mathbb{G}$ are public and $X \neq C$, $Y \neq D$

unconditionally secure

$\swarrow$

$q - 1$ equiprobable secret tuples (r_1, r_2, ε)

$\searrow$

$$\xi \in \text{set } \{[r^{-1}](C - X) : r \in [\![2^\varphi]\!]\} \cap \text{set } \{[r^{-1}](D - Y) : r \in [\![2^\varphi]\!]\}$$

Security Analysis Intuition

Let $(\mathbb{G} = \langle P \rangle, +)$ be a cyclic group of prime order q and $\varepsilon \xleftarrow{\$} \mathbb{Z}_q^*$, $\xi = [\varepsilon]P$.

- $r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q^*$
- $r_1, r_2 \xleftarrow{\$} [\![2^\varphi]\!] = \{1, \ldots, 2^\varphi\} \subsetneq \mathbb{Z}_q^*$

unconditionally secure

$$\text{pub} = \begin{cases} C = [r_1]\xi + X \\ D = [r_2]\xi + Y \end{cases}$$

where $X, Y \in \mathbb{G}$ are public and $X \neq C$, $Y \neq D$

broken after up to $2^{\varphi+1}$ scalar computations in $\mathbb{G}$

$\swarrow$ $\searrow$

$q - 1$ equiprobable secret tuples (r_1, r_2, ε)

$$\xi \in \text{set } \{[r^{-1}](C - X) : r \in [\![2^\varphi]\!]\} \cap \text{set } \{[r^{-1}](D - Y) : r \in [\![2^\varphi]\!]\}$$

Adversary Winning Probability

Time-bound: computes no more than 2^κ short scalar multiplications in τ seconds.

Adversary Winning Probability

Time-bound:  computes no more than 2^{κ} short scalar multiplications in τ seconds.

Best strategy: choose $S_1, S_2 \subset [\![2^{\varphi}]\!] \ : \ |S_1| + |S_2| \leq 2^{\kappa}$ and intersect the generated sets.

Adversary Winning Probability

Time-bound: computes no more than 2^κ short scalar multiplications in τ seconds.

Best strategy: choose $S_1, S_2 \subset [\![2^\varphi]\!] \ : \ |S_1| + |S_2| \leq 2^\kappa$ and intersect the generated sets.

$$\mathcal{P}\left[(\texttt{pub}) \to \texttt{out}^* \ \middle|\ \begin{array}{l} \texttt{out}^* \neq \texttt{out} \\ \mathsf{Verify}(\texttt{out}^*) = 1 \end{array} \right]$$

Adversary Winning Probability

Time-bound:  computes no more than 2^{κ} short scalar multiplications in τ seconds.

Best strategy: choose $S_1, S_2 \subset [\![2^{\varphi}]\!] \ : \ |S_1|+|S_2| \leq 2^{\kappa}$ and intersect the generated sets.

$$\mathcal{P}\left[\text{\includegraphics{adv}}(\mathtt{pub}) \rightarrow \mathtt{out}^* \ \middle| \ \begin{array}{c} \mathtt{out}^* \neq \mathtt{out} \\ \mathsf{Verify}(\mathtt{out}^*) = 1 \end{array} \right]$$

$$\leq \ \mathcal{P}\left[\xi \in \begin{array}{c} \mathsf{set}\left\{[r^{-1}](C - X) : r \in S_1\right\} \\ \bigcap \\ \mathsf{set}\left\{[r^{-1}](D - Y) : r \in S_2\right\} \end{array} \right]$$

Adversary Winning Probability

Time-bound:  computes no more than 2^{κ} short scalar multiplications in τ seconds.

Best strategy: choose $S_1, S_2 \subset [\![2^{\varphi}]\!] \;:\; |S_1| + |S_2| \leq 2^{\kappa}$ and intersect the generated sets.

$\mathcal{P}\Bigg[$  $(\mathtt{pub}) \to \mathtt{out}^* \;\Bigg|\; \begin{matrix} \mathtt{out}^* \neq \mathtt{out} \\ \mathsf{Verify}(\mathtt{out}^*) = 1 \end{matrix} \Bigg]$

$$\leq \mathcal{P}\left[\xi \in \begin{matrix} \mathsf{set}\left\{[r^{-1}](C - X) : r \in S_1\right\} \\ \bigcap \\ \mathsf{set}\left\{[r^{-1}](D - Y) : r \in S_2\right\} \end{matrix} \right]$$

$$= \mathcal{P}\left[\begin{matrix} \mathsf{event}\left\{r_1 \in S_1\right\} \\ \bigwedge \\ \mathsf{event}\left\{r_2 \in S_2\right\} \end{matrix} \right]$$

Adversary Winning Probability

Time-bound:  computes no more than 2^{κ} short scalar multiplications in τ seconds.

Best strategy: choose $S_1, S_2 \subset [\![2^{\varphi}]\!] \,:\, |S_1| + |S_2| \leq 2^{\kappa}$ and intersect the generated sets.

$$\mathcal{P}\left[\text{(adversary)}(\mathrm{pub}) \to \mathtt{out}^* \;\middle|\; \begin{array}{l} \mathtt{out}^* \neq \mathtt{out} \\ \mathsf{Verify}(\mathtt{out}^*) = 1 \end{array} \right]$$

$$\leq \mathcal{P}\left[\xi \in \begin{array}{c} \mathsf{set}\,\{[r^{-1}](C - X) : r \in S_1\} \\ \bigcap \\ \mathsf{set}\,\{[r^{-1}](D - Y) : r \in S_2\} \end{array} \right]$$

$$= \mathcal{P}\left[\begin{array}{c} \mathsf{event}\,\{r_1 \in S_1\} \\ \bigwedge \\ \mathsf{event}\,\{r_2 \in S_2\} \end{array} \right] \leq 2^{-\sigma}$$

$\hookrightarrow$ if $\varphi = \left\lceil \frac{\sigma - 1}{2} + \kappa \right\rceil$

Adversary Winning Probability

Time-bound:  computes no more than 2^{κ} short scalar multiplications in τ seconds.

Best strategy: choose $S_1, S_2 \subset [\![2^{\varphi}]\!] \,:\, |S_1|+|S_2| \le 2^{\kappa}$ and intersect the generated sets.

$$\mathcal{P}\left[\; \text{(adversary)}(\texttt{pub}) \to \texttt{out}^* \;\middle|\; \begin{array}{c} \texttt{out}^* \neq \texttt{out} \\ \mathsf{Verify}(\texttt{out}^*) = 1 \end{array} \right]$$

$$\le \mathcal{P}\left[\xi \in \begin{array}{c} \mathsf{set}\,\{[r^{-1}](C - X) : r \in S_1\} \\ \cap \\ \mathsf{set}\,\{[r^{-1}](D - Y) : r \in S_2\} \end{array} \right]$$

$$= \mathcal{P}\left[\begin{array}{c} \mathsf{event}\,\{r_1 \in S_1\} \\ \wedge \\ \mathsf{event}\,\{r_2 \in S_2\} \end{array} \right] \le 2^{-\sigma}$$

↳ if $\varphi = \left\lceil \frac{\sigma - 1}{2} + \kappa \right\rceil$

In this work:

$\tau = 1$	latency
$\kappa = 70$	computational
$\sigma = 40$	statistical
$\varphi = 90$	efficiency

Result Overview

Result Overview

Curve	Protocol	Client cost	Security
BLS12-381	CDS14	$1.41\ \mathfrak{p}$	
	CKKS20	$2.01\ \mathfrak{p}$	
	LOVE	$1.90\ \mathfrak{p}$	
	AmorE	$0.68\ \mathfrak{p}$	

$\mathtt{len}(\overrightarrow{A}) = 1$

Result Overview

Curve	Protocol		Client cost	Security
BLS12-381	CDS14	$\texttt{len}(\overrightarrow{A}) = 1$	1.41 $\mathfrak{p}$	
	CKKS20		2.01 $\mathfrak{p}$	
	LOVE		1.90 $\mathfrak{p}$	
	AmorE		0.68 $\mathfrak{p}$	
	MV19	$\texttt{len}(\overrightarrow{A}) = 3$	1.04 $\mathfrak{p}$	
	CKC23		1.65 $\mathfrak{p}$	
	AmorE		0.45 $\mathfrak{p}$	

Result Overview

Curve	Protocol		Client cost	Security
BLS12-381	CDS14	$\texttt{len}(\overrightarrow{A}) = 1$	1.41 $\mathfrak{p}$	
	CKKS20		2.01 $\mathfrak{p}$	
	LOVE		1.90 $\mathfrak{p}$	
	AmorE		0.68 $\mathfrak{p}$	
	MV19	$\texttt{len}(\overrightarrow{A}) = 3$	1.04 $\mathfrak{p}$	
	CKC23		1.65 $\mathfrak{p}$	
	AmorE		0.45 $\mathfrak{p}$	

Table: Amortized Efficiency obtained over $N = 10$ delegations and 40 bits of statistical security (RELIC implementations).

Thank you for your attention :)

Open-source tools used for our presentation:

Inkscape

Sozi

SVG repo