Breaking Parallel ROS: Implication for Isogeny and Lattice-based Blind Signatures

la.cr/2023/1603; PKC2024

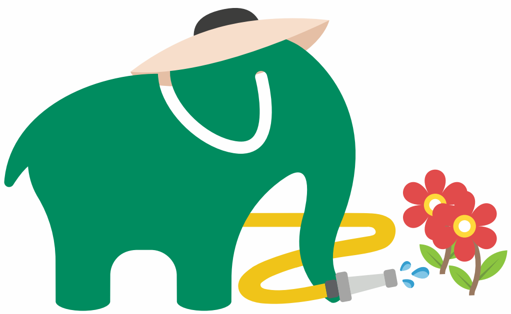
Shuichi Katsumata, **Yi-Fu Lai,** Michael Reichle

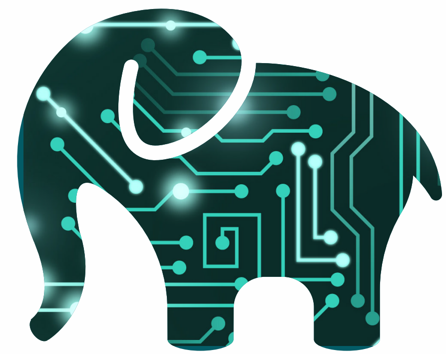
CASA / Ruhr-University Bochum
AIST, PQShield, ETH Zurich

Content

- Blind Signatures
- The Concurrent Attack
- Open Problems

Blind Signatures

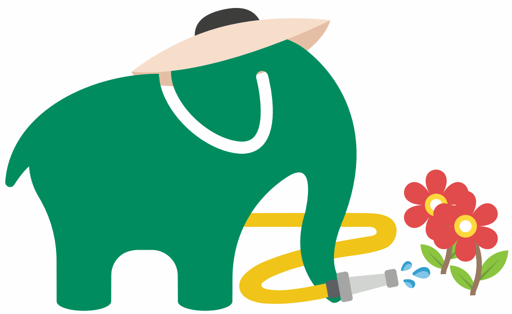


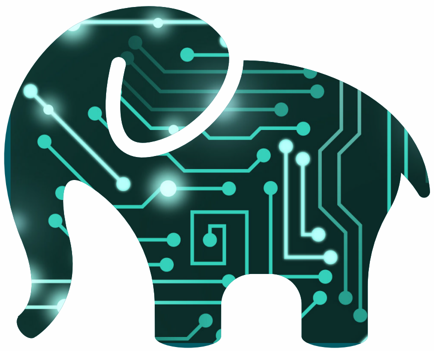


Blind Signatures

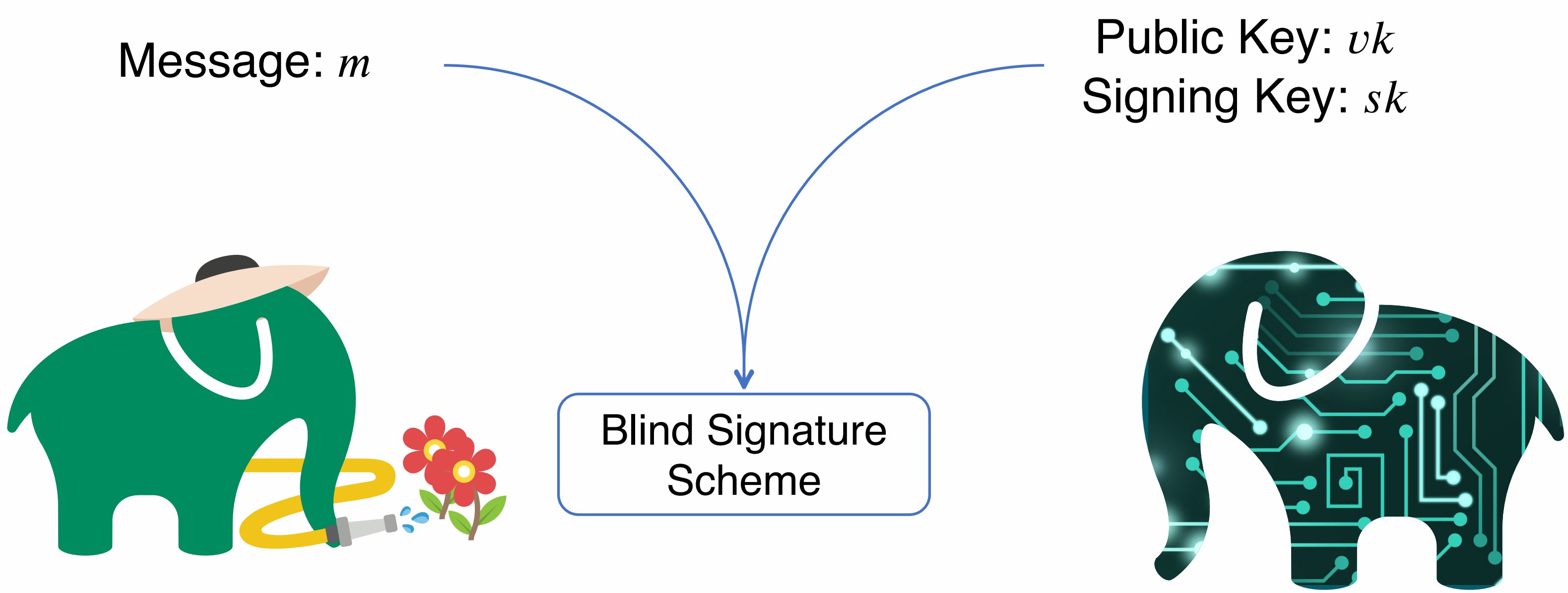
Message: m

Public Key: vk
Signing Key: sk





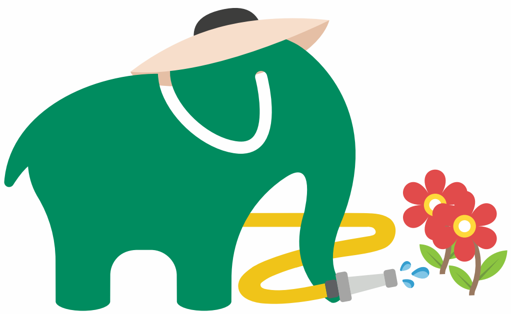
Blind Signatures



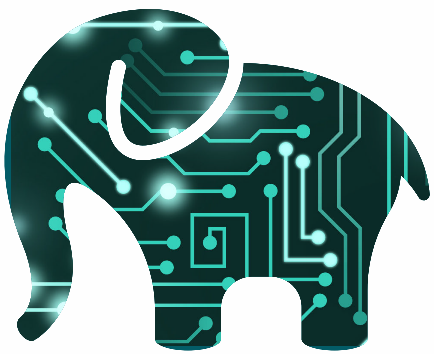
Blind Signatures

Message: m

Public Key: vk
Signing Key: sk



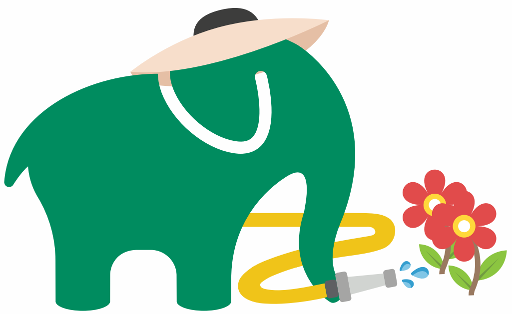
Blind Signature Scheme



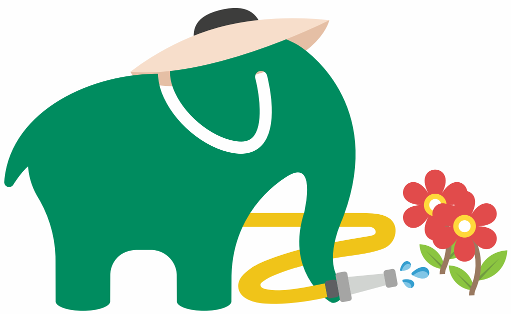
$\left(m,\ sign_{sk}(m)\right)$

$\perp$

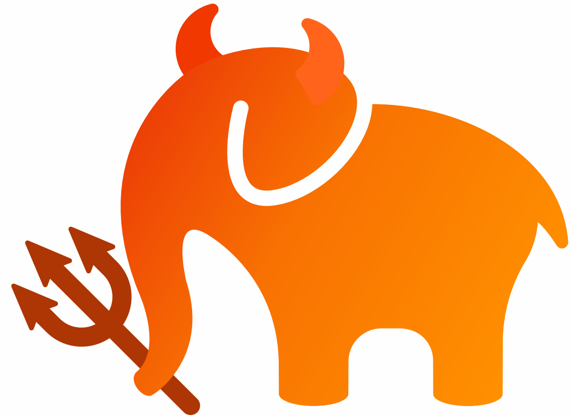
Notion: Blindness



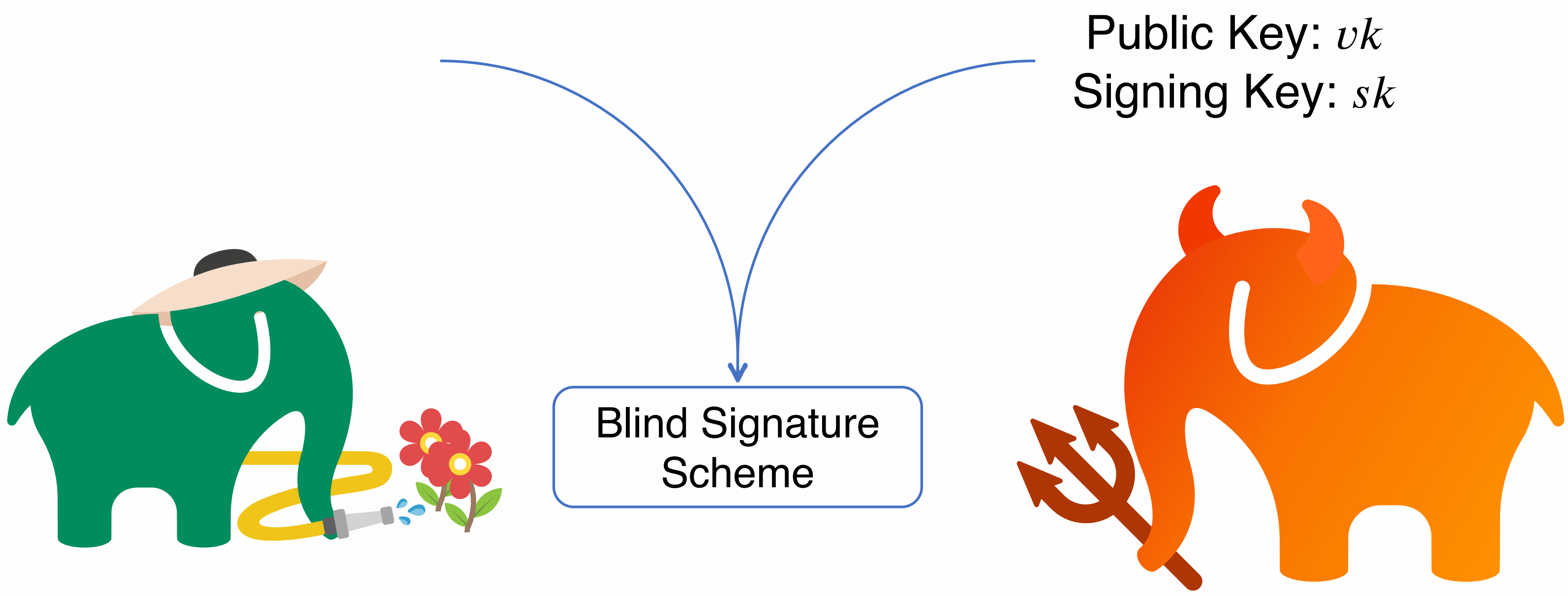
Notion: Blindness



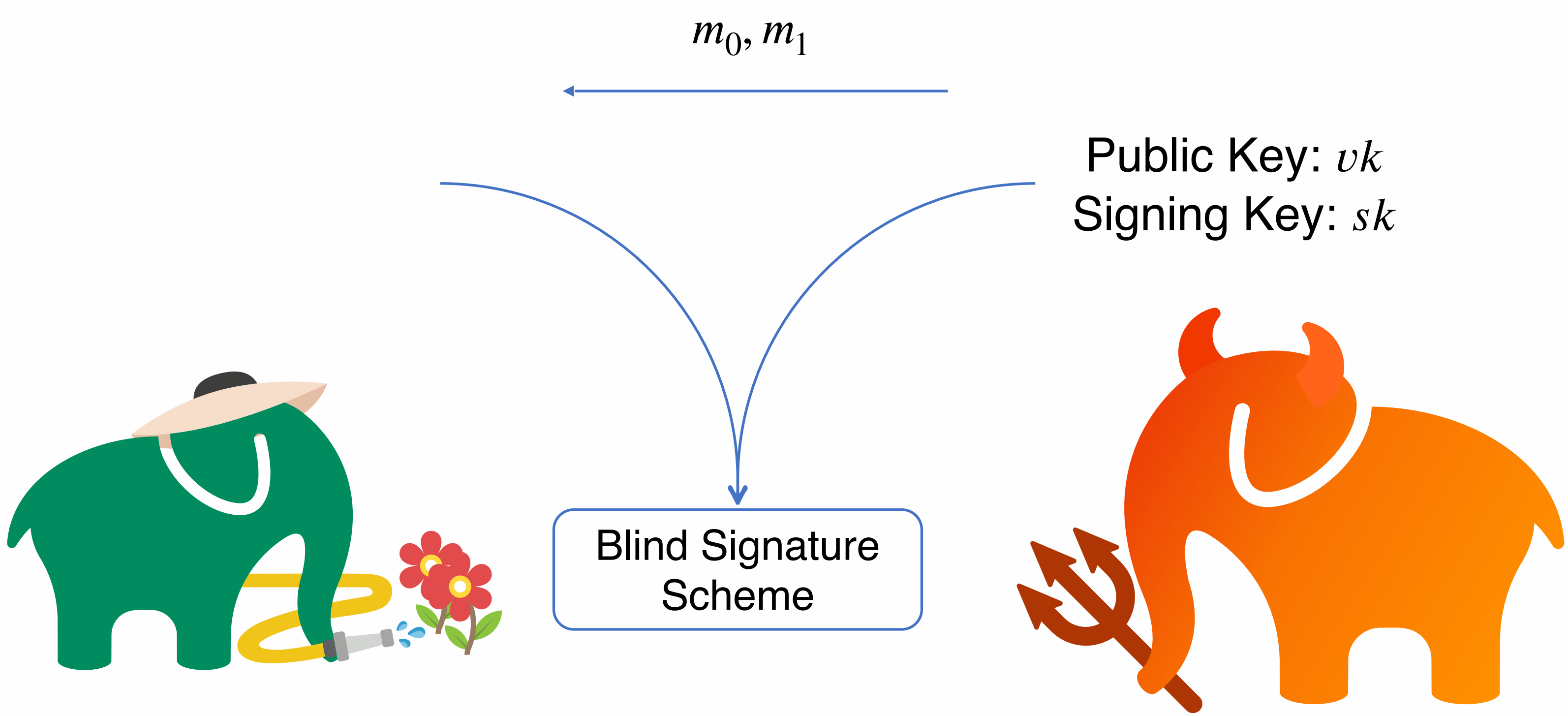
Public Key: vk
Signing Key: sk



Notion: Blindness



Notion: Blindness

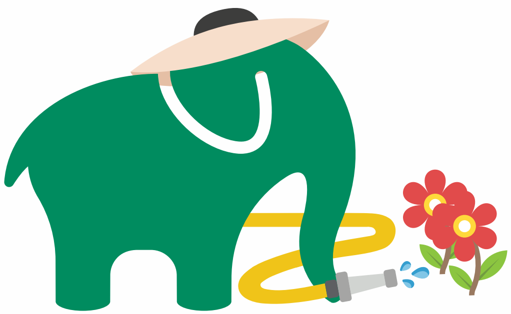


Notion: Blindness

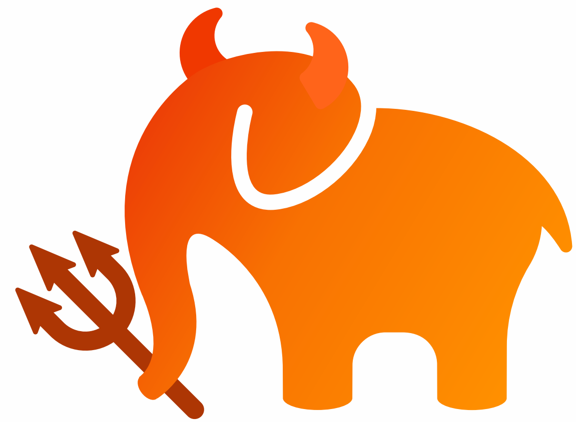
m_0, m_1

$\color{red}{b} \leftarrow_{\$} \{0,1\}$

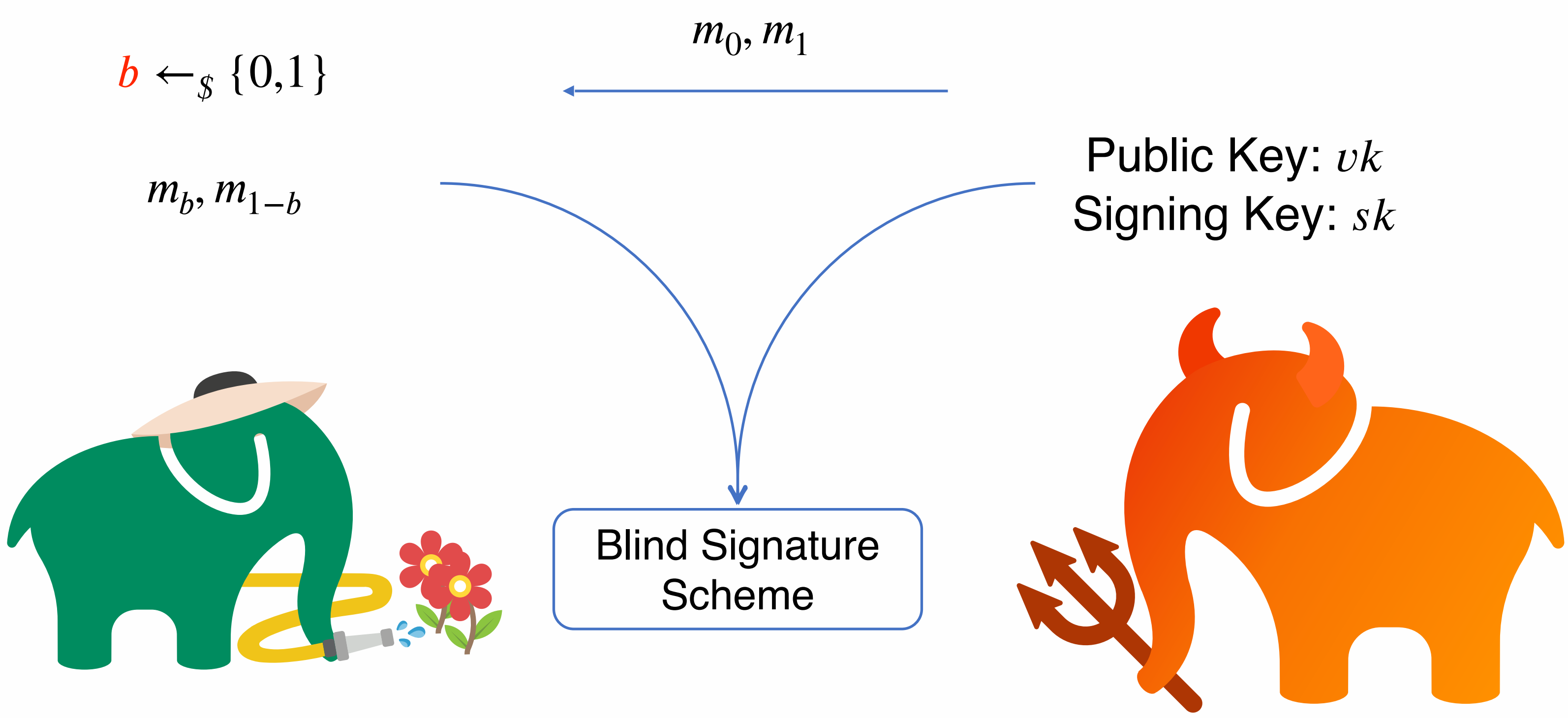
Public Key: vk
Signing Key: sk



Blind Signature Scheme



Notion: Blindness



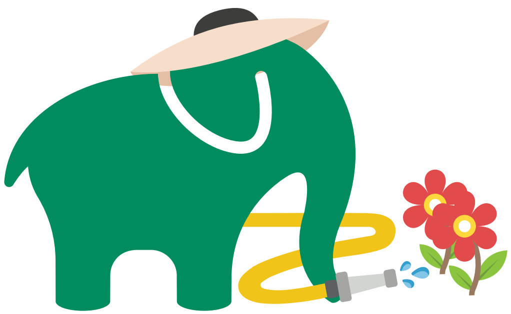
Notion: Blindness

m_0, m_1

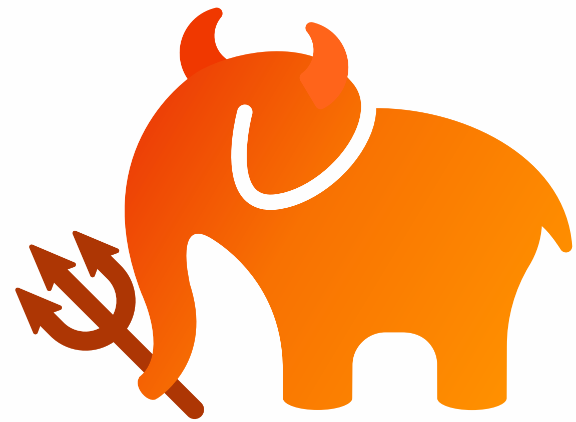
$\color{red}{b} \leftarrow_\$ \{0,1\}$

m_b, m_{1-b}

Public Key: vk
Signing Key: sk



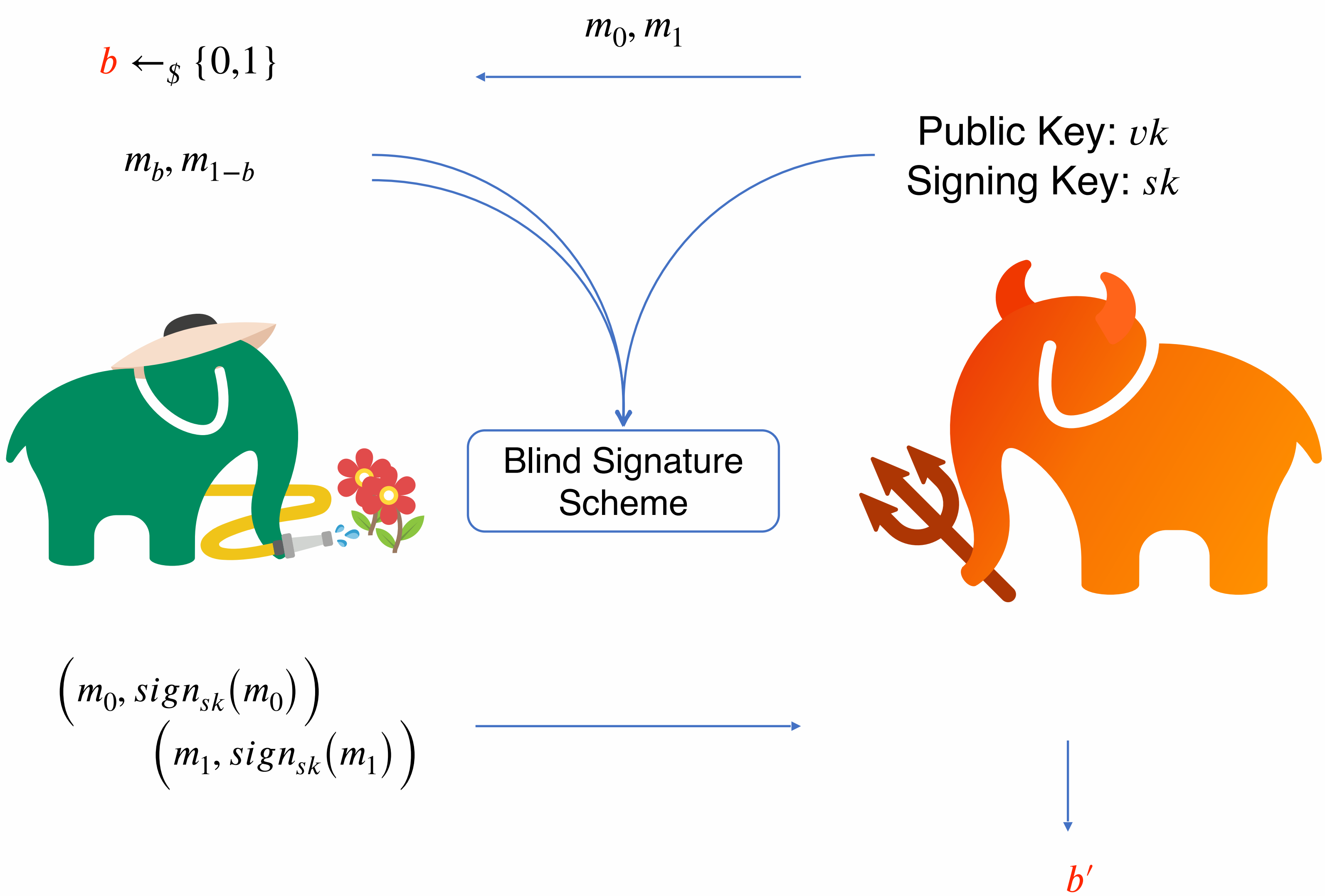
Blind Signature Scheme



$\left(m_0, sign_{sk}(m_0)\right)$

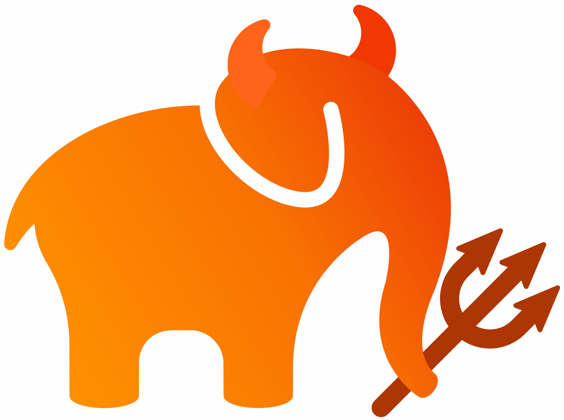
$\left(m_1, sign_{sk}(m_1)\right)$

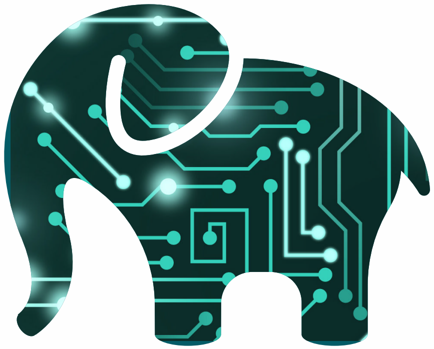
Notion: Blindness



Notion: ℓ-One-More Unforgeability (OMUF)

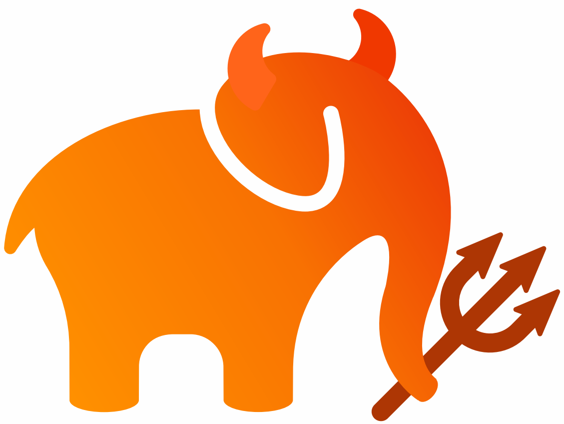
$m_1, \ldots, m_\ell$



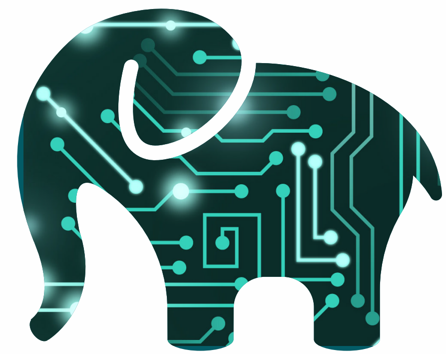


Notion: ℓ-One-More Unforgeability (OMUF)

$m_1, \ldots, m_\ell$



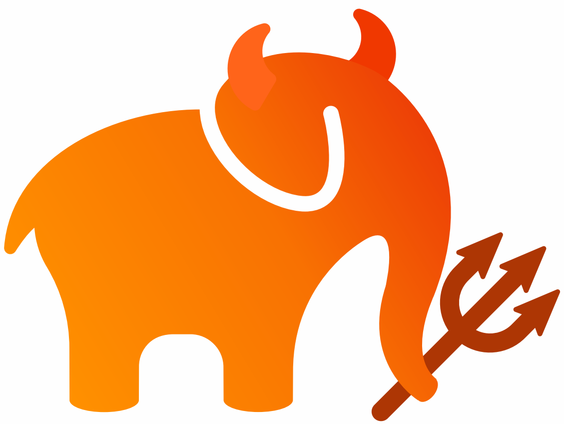
Public Key: vk
Signing Key: sk



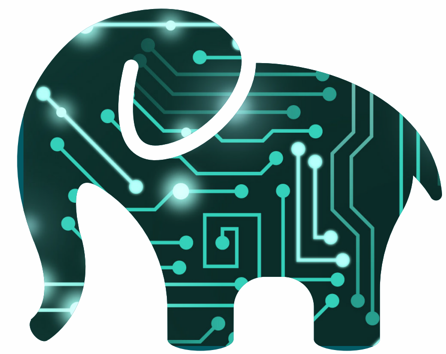
Notion: ℓ-One-More Unforgeability (OMUF)

$m_1, \ldots, m_\ell$

Public Key: vk
Signing Key: sk



Blind Signature Scheme

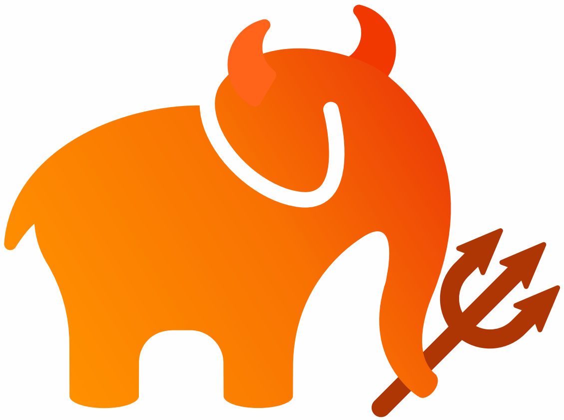


Notion: ℓ-One-More Unforgeability (OMUF)

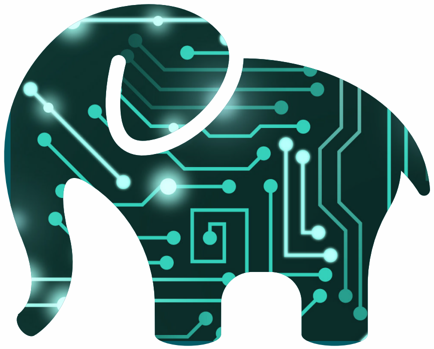
Adaptively/
Concurrently

$m_1, \ldots, m_\ell$

Public Key: vk
Signing Key: sk



Blind Signature Scheme



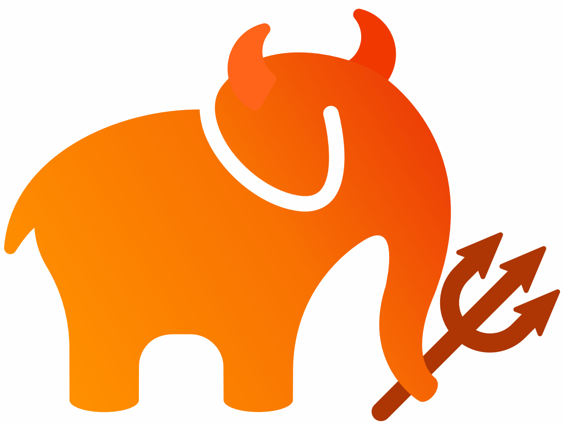
$\perp$

Notion: ℓ-One-More Unforgeability (OMUF)

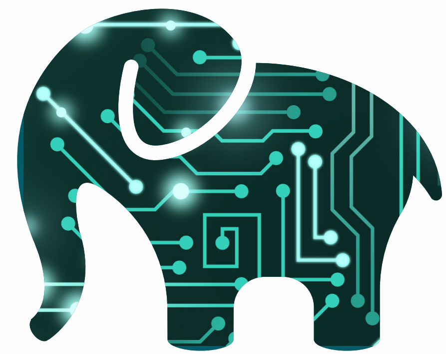
Adaptively/
Concurrently

$m_1, \ldots, m_\ell$

Public Key: vk
Signing Key: sk



Blind Signature
Scheme



(m_1, σ_1)

$\ddots$

(m_ℓ, σ_ℓ)

$(m_{\ell+1}, \sigma_{\ell+1})$

$\perp$

Blind Signature

- Proposed by Chaum in 1982.

- Getting more attention these years because of its application (e-cash (initial application), e-voting, anonymous credentials), adding
  - anonymity for cryptocurrency transactions [ASIACCS:YL19]),
  - Hiding metadata in secure messaging [CCS:KKP22]
  - Privacy-preserving authentication tokens [Google22]

How To?

Typically, there are two main approaches doing this.

1. **Fischlin's framework** [Fis06]:

   • This leads to a round-optimal (2-round) scheme but requires a proof system for a complex relation. ([PinKat22, BLKS23]). (involving the encrypted commitment and the signature verification.) This is naturally immune to the adaptive attacks.

2. **From sigma-protocol-based signatures (Σ-based Blind Signature):**

   • E.g. [PoiSte96, PoiSte00, AbeOka00]. This typically requires some special properties of the underlying scheme, and results in 3-round blind signature.

Post-Quantum Blind Signature

- There are only 4 Σ-based post-quantum blind signatures:
  - Lattice:
    - HKLN20 (Crypto'20): Hauck, Kiltz, Loss, Nguyen.
    - BLAZE+ (FC/ACISP'20): Alkadri, Bansarkhani, Buchmann
    - BlindOR (CANS'21): Alkadri, Harasser, Janson
  - Isogeny:
    - CSI-Otter (Crypto'23): Katsumata, Lai, LeGrow, Qin

- It worthwhile to remark that along with the development of the lattice-based ZKP, [C:dK22,CCS:AKSY22,BLNS23] Fischlin's method [C:Fis06] can give more compact results (20~100KB).

Contributions

- We break 3 Σ-based post-quantum blind signatures CSI-Otter, Blaze+ and BlindOR.

- As an independent and theoretical interest, we also propose an abstract parallelROS problem and establish the connection to the ROS problem.

Why There can be an Attack?

In the OMUF of CSI-Otter,

- The OMUF proof has loss in $\binom{Q_H}{\ell+1}$ where Q_H is the number of hash queries and ℓ is the number of concurrent signing sessions due to restriction on the number of hash queries made in CSI-Otter.

Why There can be an Attack?

In the OMUF of CSI-Otter,

- The OMUF proof has loss in $\binom{Q_H}{\ell+1}$ where Q_H is the number of hash queries and ℓ is the number of concurrent signing sessions due to restriction on the number of hash queries made in CSI-Otter.

- This only guarantees sequentially secure and $\log(\lambda)$ concurrently secure.

Why There can be an Attack?

In the OMUF of CSI-Otter,

- The OMUF proof has loss in $\binom{Q_H}{\ell+1}$ where Q_H is the number of hash queries and ℓ is the number of concurrent signing sessions due to restriction on the number of hash queries made in CSI-Otter.

- This only guarantees sequentially secure and $\log(\lambda)$ concurrently secure.

- The loss is common in the sigma-protocol-based blind signatures.

Why There can be an Attack?

In the OMUF of CSI-Otter,

- The OMUF proof has loss in $\binom{Q_H}{\ell+1}$ where Q_H is the number of hash queries and ℓ is the number of concurrent signing sessions due to restriction on the number of hash queries made in CSI-Otter.

- This only guarantees sequentially secure and $\log(\lambda)$ concurrently secure.

- The loss is common in the sigma-protocol-based blind signatures.

Why There can be an Attack?

In the OMUF of CSI-Otter,

- The OMUF proof has loss in $\binom{Q_H}{\ell+1}$ where Q_H is the number of hash queries and ℓ is the number of concurrent signing sessions due to restriction on the number of hash queries made in CSI-Otter.
- This only guarantees sequentially secure and $\log(\lambda)$ concurrently secure.
- The loss is common in the sigma-protocol-based blind signatures.
- **What will happen if we sign concurrently and exceed the bound?**

Blind Schnorr and the ROS Attack

Blind Schnorr

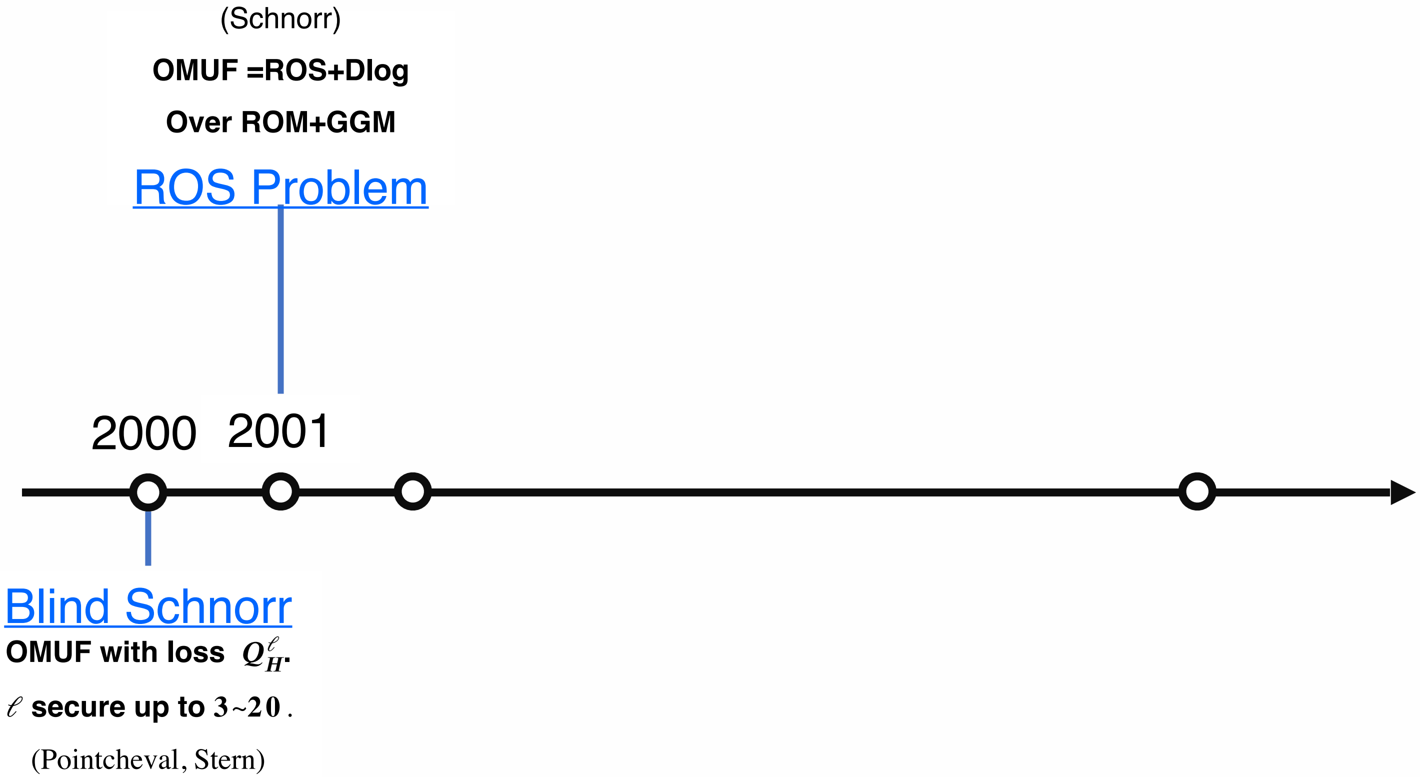
OMUF with loss Q_H^ℓ.

ℓ secure up to $3{\sim}20$.

(Pointcheval, Stern)

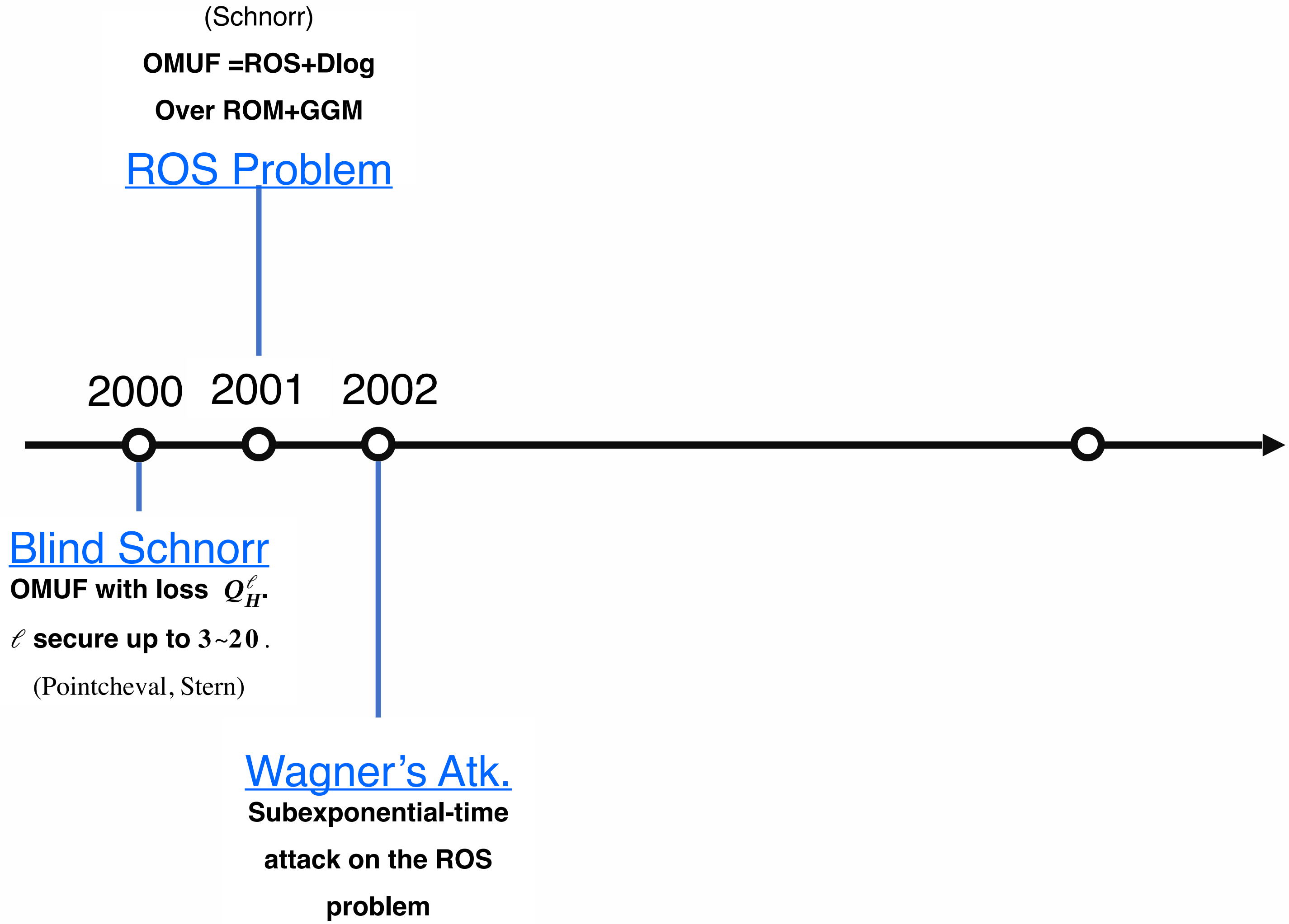
ROS: Random inhomogeneities in an Overdetermined Solvable system of linear equations.

Blind Schnorr and the ROS Attack



ROS: Random inhomogeneities in an Overdetermined Solvable system of linear equations.

Blind Schnorr and the ROS Attack



ROS: Random inhomogeneities in an Overdetermined Solvable system of linear equations.

Blind Schnorr and the ROS Attack

(Schnorr)

OMUF =ROS+Dlog

Over ROM+GGM

ROS Problem

Is large ℓ a problem

for Blind Schnorr?

2000 2001 2002

Blind Schnorr

OMUF with loss Q_H^ℓ.

ℓ **secure up to** $3\sim 20$.

(Pointcheval, Stern)

Wagner's Atk.

Subexponential-time attack on the ROS problem

ROS: Random inhomogeneities in an Overdetermined Solvable system of linear equations.

Blind Schnorr and the ROS Attack

(Schnorr)

OMUF =ROS+Dlog

Over ROM+GGM

ROS Problem

Is large ℓ a problem

for Blind Schnorr?

Blind Schnorr

OMUF with loss Q_H^ℓ.

ℓ **secure up to** $3\sim20$.

(Pointcheval, Stern)

Wagner's Atk.

Subexponential-time attack on the ROS problem

Polynomial-time ROS Atk. (EC:BLLOR21)

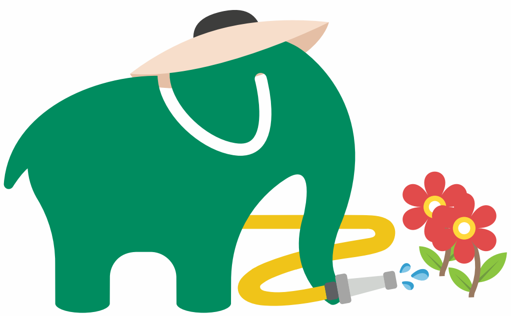
Breaking the ROS problem in polynomial time.

(Benhamouda, Lepoint, Loss, Orrù, Raykova)

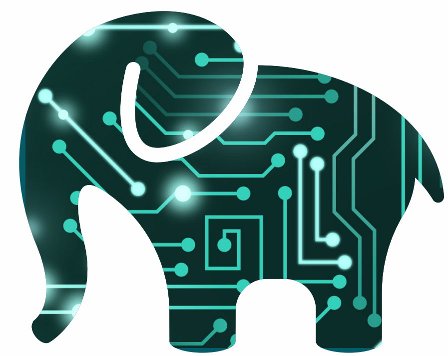
ROS: Random inhomogeneities in an Overdetermined Solvable system of linear equations.

Sigma-Protocol-Based Signature

Verifier



Prover/Signer



(Commitment)

com $\leftarrow$

(Challenge)

$c = H(\mathsf{com}, m)$ $\rightarrow$

(Response)

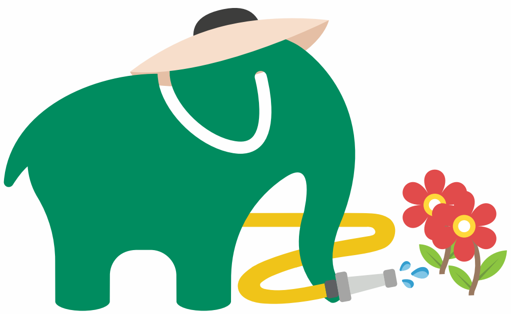
resp $\leftarrow$

Signature

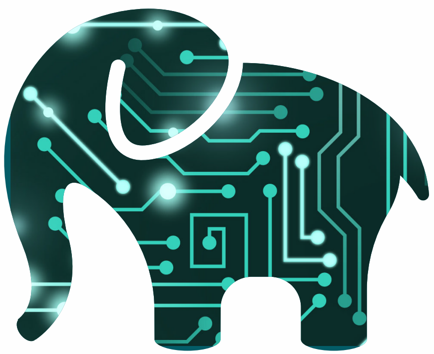
(c, resp)

Unblinded Blind Signature

User



Signer



(Commitment)

com ←

(Challenge)

$c = H(\text{com}, m)$ →

(Response)

resp ←

↓

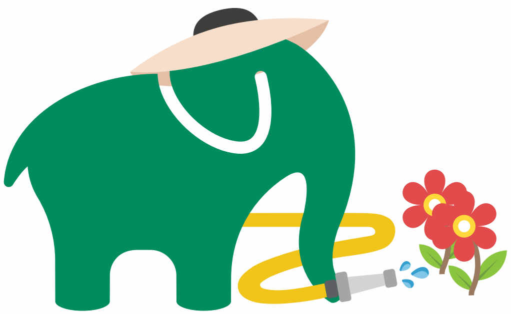
Signature

(c, resp)

Unblinded Blind Signature with Parallel Repetition

User

Signer



(Commitment)

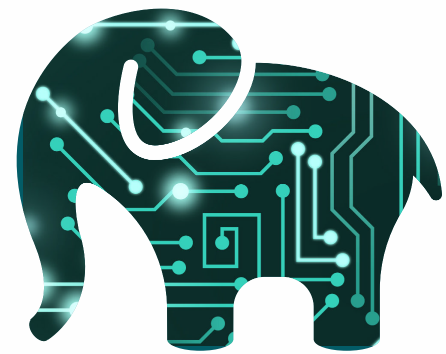
$$\text{com} = (\text{com}_1, \cdots, \text{com}_\lambda)$$

(Challenge)

$$c = H(\text{com}, m) = (c_1, \cdots, c_\lambda)$$

(Response)

$$\text{resp} = (\text{resp}_1, \cdots, \text{resp}_\lambda)$$

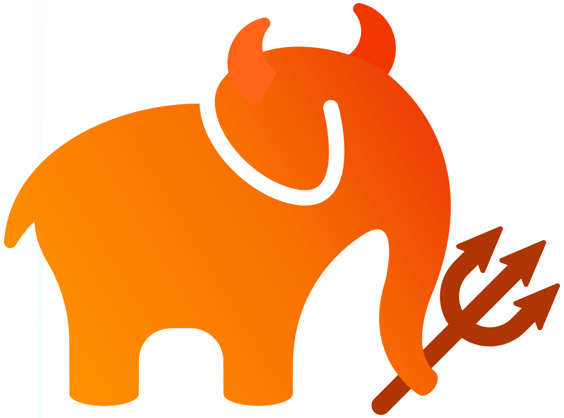


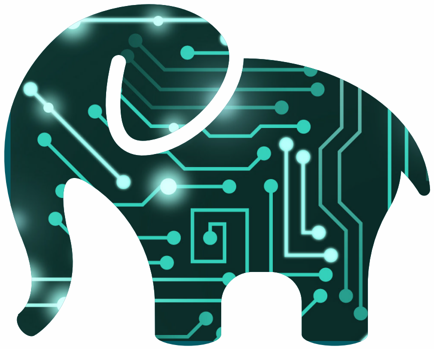
Signature

(c, resp)

Attack on CSI-Otter / BlindOR

λ-concurrent sessions.

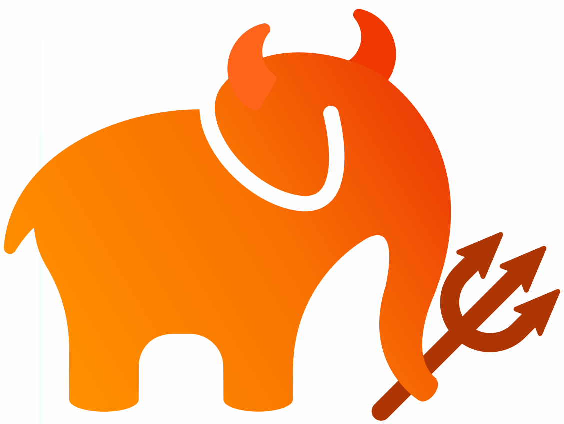


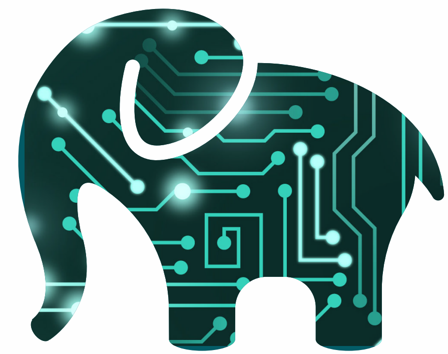


Attack on CSI-Otter / BlindOR

λ-concurrent sessions.

$$\mathsf{com}_1 = (\boxed{\mathsf{com}_{11}}, \mathsf{com}_{12} \cdots, \mathsf{com}_{1\lambda})$$
$$\mathsf{com}_2 = (\mathsf{com}_{21}, \boxed{\mathsf{com}_{22}} \cdots, \mathsf{com}_{2\lambda})$$
$$\vdots$$
$$\mathsf{com}_\lambda = (\mathsf{com}_{\lambda 1}, \mathsf{com}_{22} \cdots, \boxed{\mathsf{com}_{\lambda\lambda}})$$

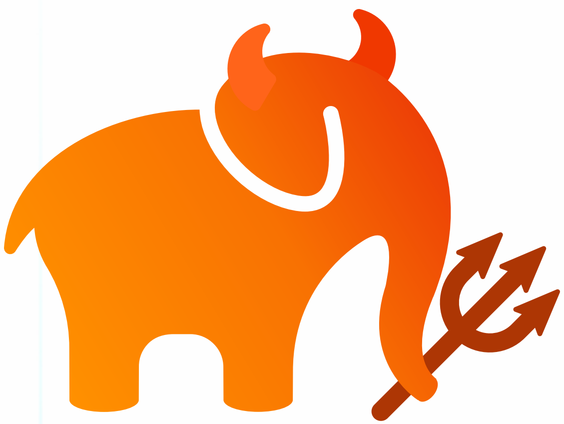




Attack on CSI-Otter / BlindOR

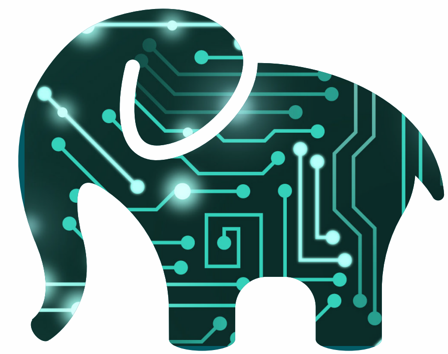
λ-concurrent sessions.

$$\mathsf{com}_1 = \boxed{(\mathsf{com}_{11}}, \mathsf{com}_{12} \cdots, \mathsf{com}_{1\lambda})$$
$$\mathsf{com}_2 = (\mathsf{com}_{21}, \boxed{\mathsf{com}_{22}} \cdots, \mathsf{com}_{2\lambda})$$
$$\vdots$$
$$\mathsf{com}_\lambda = (\mathsf{com}_{\lambda 1}, \mathsf{com}_{22} \cdots, \boxed{\mathsf{com}_{\lambda\lambda}})$$



$H(\mathsf{com}_{11}, \mathsf{com}_{22}, \cdots, \mathsf{com}_{\lambda\lambda}, m)$

$(c'_{11}, c'_{22}, \cdots, c'_{\lambda\lambda}) \leftarrow$

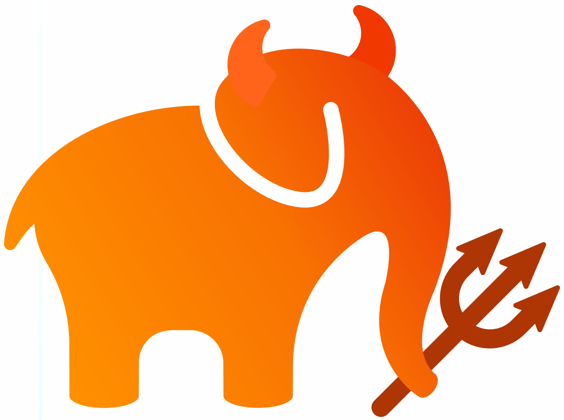


Attack on CSI-Otter / BlindOR

λ-concurrent sessions.

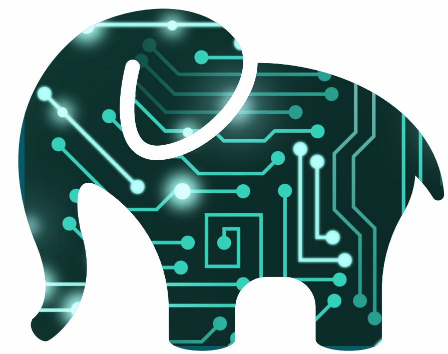
$$\mathsf{com}_1 = \boxed{(\mathsf{com}_{11}}, \mathsf{com}_{12} \cdots, \mathsf{com}_{1\lambda})$$
$$\mathsf{com}_2 = (\mathsf{com}_{21}, \boxed{\mathsf{com}_{22}} \cdots, \mathsf{com}_{2\lambda})$$
$$\vdots$$
$$\mathsf{com}_\lambda = (\mathsf{com}_{\lambda 1}, \mathsf{com}_{22} \cdots, \boxed{\mathsf{com}_{\lambda\lambda})}$$

$$\boxed{(c'_{11}}, c_{12}, \cdots, c_{1\lambda}) \leftarrow H(\mathsf{com}_1, m_1)$$
$$(c_{21}, \boxed{c'_{22}}, \cdots, c_{2\lambda}) \leftarrow H(\mathsf{com}_2, m_2)$$
$$\vdots$$
$$(c_{\lambda 1}, c_{\lambda 2}, \cdots, \boxed{c'_{\lambda\lambda})} \leftarrow H(\mathsf{com}_\lambda, m_\lambda)$$



$H(\mathsf{com}_{11}, \mathsf{com}_{22}, \cdots, \mathsf{com}_{\lambda\lambda}, m)$

$(c'_{11}, c'_{22}, \cdots, c'_{\lambda\lambda}) \leftarrow$

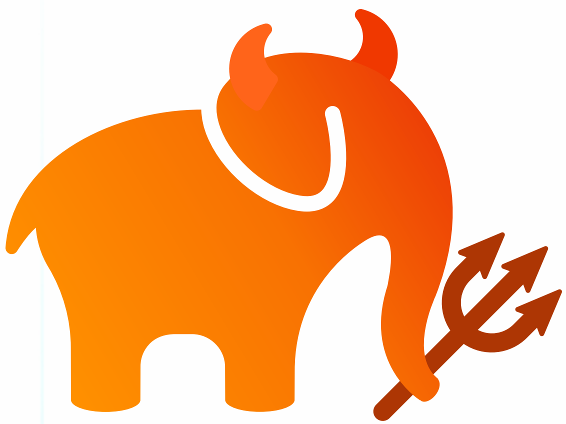


Choose proper m_i
Feasible if challenge space is small.

Attack on CSI-Otter / BlindOR

λ-concurrent sessions.

$$\mathsf{com}_1 = \boxed{(\mathsf{com}_{11}}, \mathsf{com}_{12} \cdots, \mathsf{com}_{1\lambda})$$
$$\mathsf{com}_2 = (\mathsf{com}_{21}, \boxed{\mathsf{com}_{22}} \cdots, \mathsf{com}_{2\lambda})$$
$$\vdots$$
$$\mathsf{com}_\lambda = (\mathsf{com}_{\lambda 1}, \mathsf{com}_{22} \cdots, \boxed{\mathsf{com}_{\lambda\lambda})}$$

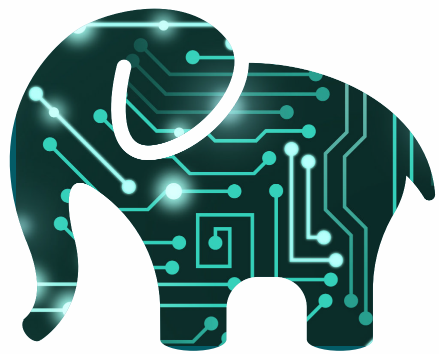


$H(\mathsf{com}_{11}, \mathsf{com}_{22}, \cdots, \mathsf{com}_{\lambda\lambda}, m)$

$(c'_{11}, c'_{22}, \cdots, c'_{\lambda\lambda}) \leftarrow$

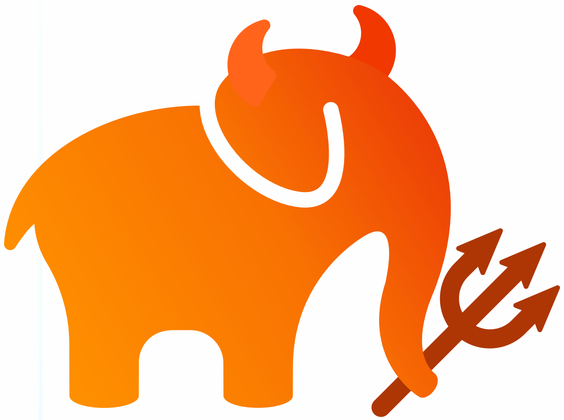
$$\boxed{(c'_{11}}, c_{12}, \cdots, c_{1\lambda}) \leftarrow H(\mathsf{com}_1, m_1)$$
$$(c_{21}, \boxed{c'_{22},} \cdots, c_{2\lambda}) \leftarrow H(\mathsf{com}_2, m_2)$$
$$\vdots$$
$$(c_{\lambda 1}, c_{\lambda 2}, \cdots, \boxed{c'_{\lambda\lambda})} \leftarrow H(\mathsf{com}_\lambda, m_\lambda)$$

$$\boxed{(\mathsf{resp}_{11}}, \mathsf{resp}_{12} \cdots, \mathsf{resp}_{1\lambda})$$
$$(\mathsf{resp}_{21}, \boxed{\mathsf{resp}_{22}} \cdots, \mathsf{resp}_{2\lambda})$$
$$\vdots$$
$$(\mathsf{resp}_{\lambda 1}, \mathsf{resp}_{\lambda 2} \cdots, \boxed{\mathsf{resp}_{\lambda\lambda})}$$



Choose proper m_i
Feasible if challenge space is small.

Optimizing …



$$\mathsf{com}_1 = (\boxed{\mathsf{com}_{11}}, \boxed{\mathsf{com}_{12}}, \cdots, \mathsf{com}_{1\lambda})$$

$$\vdots$$

$$\mathsf{com}_{\lambda/2} = (\mathsf{com}_{\lambda 1}, \cdots, \boxed{\mathsf{com}_{\lambda/2,\lambda-1}}, \boxed{\mathsf{com}_{\lambda/2,\lambda}})$$

$$(\boxed{c'_{11}}, \boxed{c_{12}}, \cdots, c_{1\lambda}) \leftarrow H(\mathsf{com}_1, m_1)$$

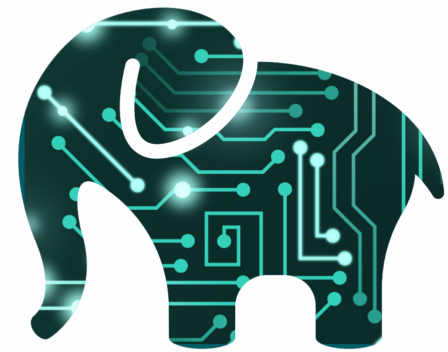
$$\vdots$$

$$(c_{\lambda 1}, \cdots, \boxed{c'_{\lambda/2,\lambda-1}}, \boxed{c'_{\lambda/2,\lambda}}) \leftarrow H(\mathsf{com}_\lambda, m_\lambda)$$

$$(\boxed{\mathsf{resp}_{11}}, \boxed{\mathsf{resp}_{12}}, \cdots, \mathsf{resp}_{1\lambda})$$

$$\vdots$$

$$(\mathsf{resp}_{\lambda 1}, \cdots, \boxed{\mathsf{resp}_{\lambda/2,\lambda-1}}, \boxed{\mathsf{resp}_{\lambda/2,\lambda}})$$



Choose proper m_i

Optimizing …

$\lambda/2$-concurrent sessions.

$$\mathsf{com}_1 = (\mathsf{com}_{11}, \mathsf{com}_{12}, \cdots, \mathsf{com}_{1\lambda})$$

$$\vdots$$

$$\mathsf{com}_{\lambda/2} = (\mathsf{com}_{\lambda 1}, \cdots, \mathsf{com}_{\lambda/2,\lambda-1}, \mathsf{com}_{\lambda/2,\lambda})$$

$$(c'_{11}, c_{12}, \cdots, c_{1\lambda}) \leftarrow H(\mathsf{com}_1, m_1)$$

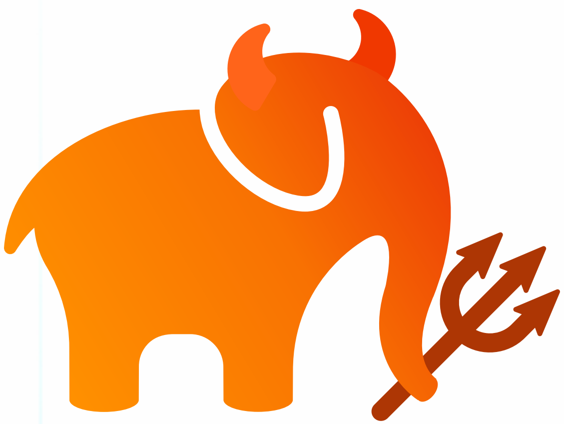
$$\vdots$$

$$(c_{\lambda 1}, \cdots, c'_{\lambda/2,\lambda-1}, c'_{\lambda/2,\lambda}) \leftarrow H(\mathsf{com}_\lambda, m_\lambda)$$

$$(\mathsf{resp}_{11}, \mathsf{resp}_{12}, \cdots, \mathsf{resp}_{1\lambda})$$

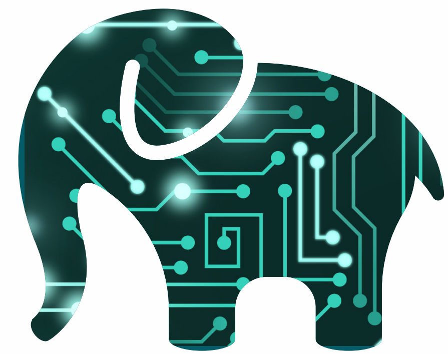
$$\vdots$$

$$(\mathsf{resp}_{\lambda 1}, \cdots, \mathsf{resp}_{\lambda/2,\lambda-1}, \mathsf{resp}_{\lambda/2,\lambda})$$



$H(\mathsf{com}_{11}, \mathsf{com}_{12}, \cdots, \mathsf{com}_{\lambda/2,\lambda}, m)$

$(c'_{11}, c'_{12}, \cdots, c'_{\lambda\lambda}) \leftarrow$



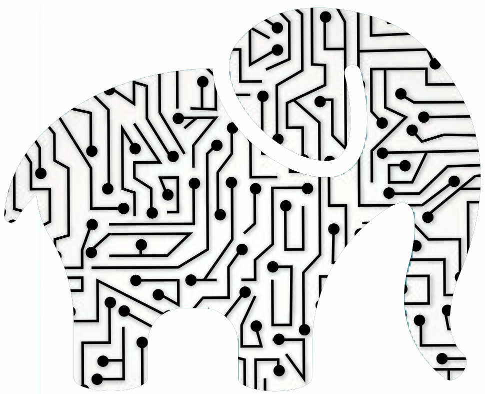
Choose proper m_i

Look Deeper

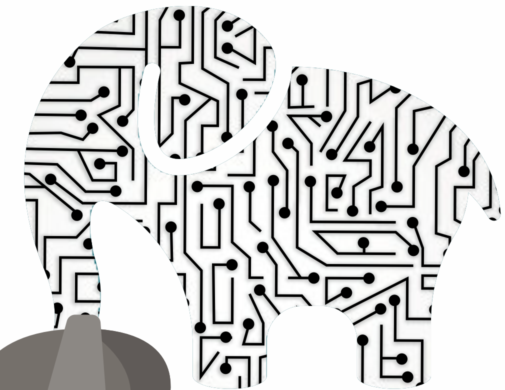
$$\mathrm{com}_1 = (\boxed{\mathrm{com}_{11}}, \mathrm{com}_{12} \cdots, \mathrm{com}_{1\lambda})$$
$$\mathrm{com}_2 = (\mathrm{com}_{21}, \boxed{\mathrm{com}_{22}} \cdots, \mathrm{com}_{2\lambda})$$
$$\vdots$$
$$\mathrm{com}_\lambda = (\mathrm{com}_{\lambda 1}, \mathrm{com}_{22} \cdots, \boxed{\mathrm{com}_{\lambda\lambda}})$$

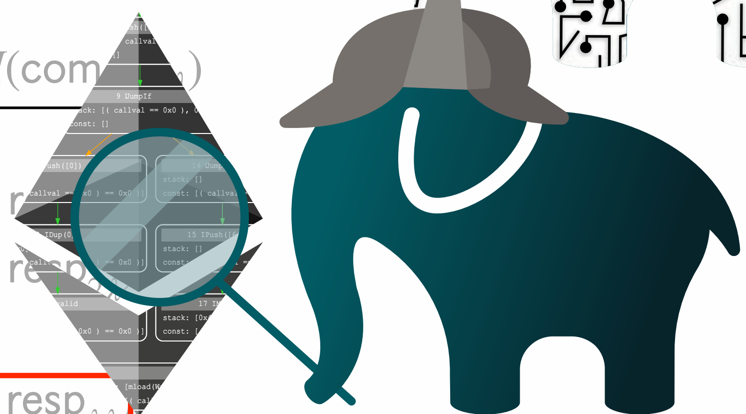
$$(\boxed{c'_{11}}, c_{12}, \cdots, c_{1\lambda}) \leftarrow H(\mathrm{com}_1, m_1)$$
$$(c_{21}, \boxed{c'_{22}}, \cdots, c_{2\lambda}) \leftarrow H(\mathrm{com}_2, m_2)$$
$$\vdots$$
$$(c_{\lambda 1}, c_{\lambda 2}, \cdots, \boxed{c'_{\lambda\lambda}}) \leftarrow H(\mathrm{com} \ldots)$$

$$(\boxed{\mathrm{resp}_{11}}, \mathrm{resp}_{12} \cdots, \mathrm{r}\ldots$$
$$(\mathrm{resp}_{21}, \boxed{\mathrm{resp}_{22}} \cdots, \mathrm{re}\ldots$$
$$\vdots$$
$$(\mathrm{resp}_{\lambda 1}, \mathrm{resp}_{\lambda 2} \cdots \boxed{\mathrm{resp}_{\lambda\lambda}})$$

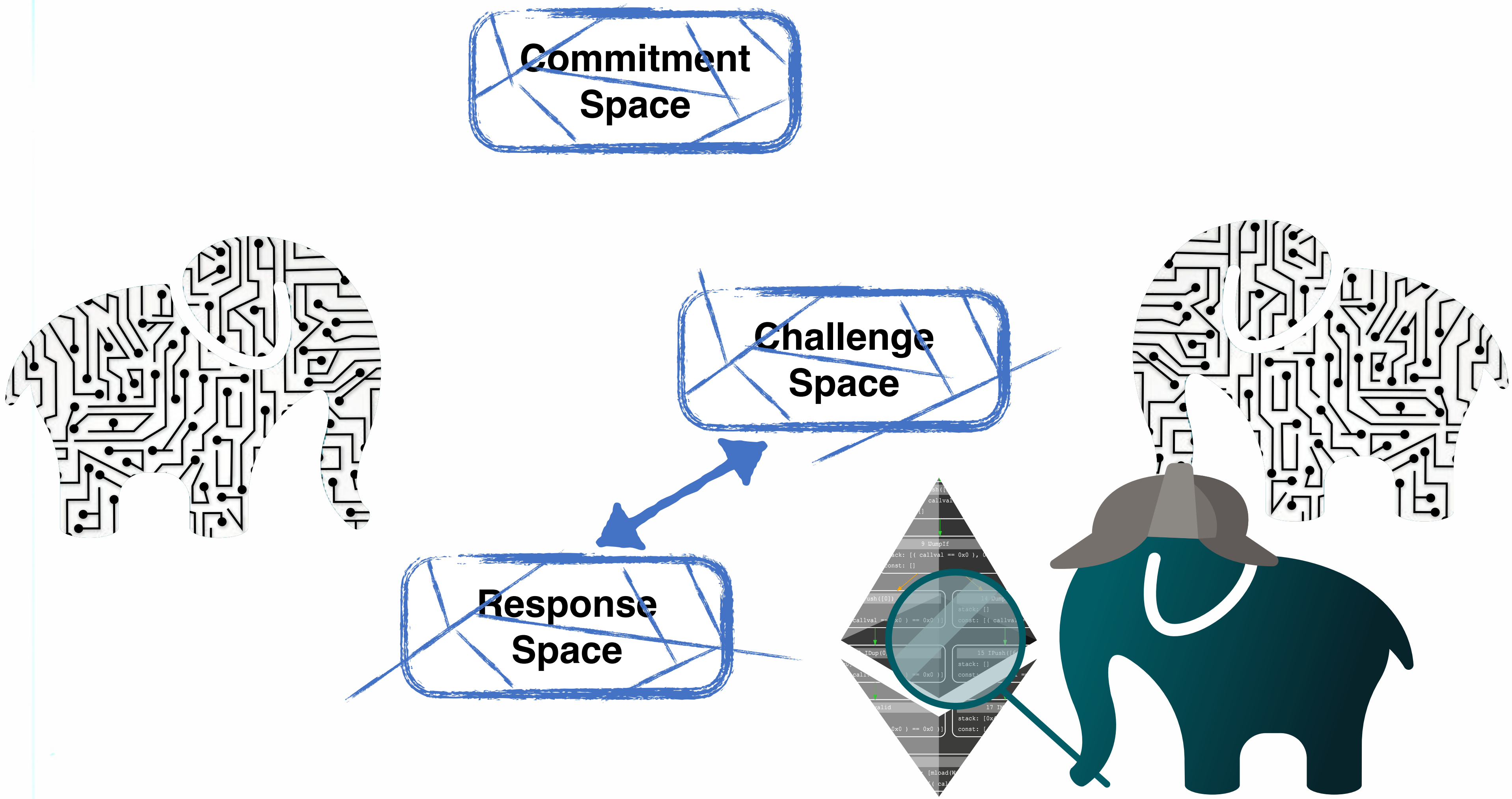


$$H(\mathrm{com}_{11}, \mathrm{com}_{22}, \cdots, \mathrm{com}_{\lambda\lambda})$$
$$(c'_{11}, c'_{22}, \cdots, c'_{\lambda\lambda}) \leftarrow$$





Spirit of Our Attack



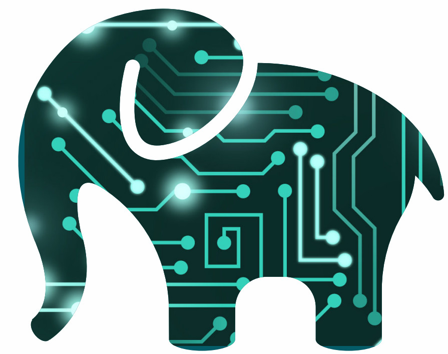
Attack on Blaze+

Challenge space:

ternary polynomial over $R_q := \mathbf{Z}_q[x]/\langle x^n + 1 \rangle$

of Hamming weight ω

We can write $c := \Sigma_{i \in [\omega]} c_i$ where c_i: monomial.



This induces the **response decomposition in degree:**

$$\mathbf{z} = \Sigma_{i \in [\omega]}(\mathbf{s}c_i + \mathbf{r}_i)$$

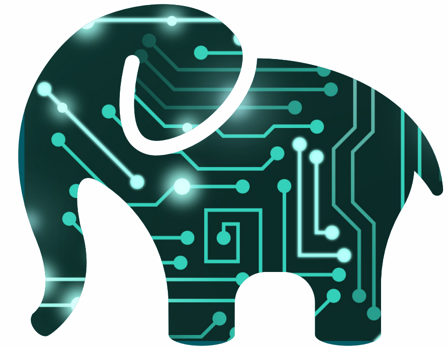
$$y = \Sigma_{i \in [\omega]}(ec_i + e_i')$$

Attack on Blaze+

Challenge space:

ternary polynomial over $R_q := \mathbf{Z}_q[x]/\langle x^n + 1\rangle$ of Hamming weight ω

We can write $c := \Sigma_{i\in[\omega]} c_i$ where c_i: monomial.



This induces the **response decomposition in degree:**

$$\mathbf{z} = \Sigma_{i\in[\omega]}(\mathbf{s}c_i + \mathbf{r}_i)$$

$$y = \Sigma_{i\in[\omega]}(ec_i + e_i')$$

Note: We are ``aggregating" responses through summation.
The resulting response might be invalid due to its length.

Efficiency

	(Concurrent sessions/ # of hashes)	Probability
CSI-Otter	$(4,\ 2^{34})$	$\approx 100\,\%$
Blaze+	$(4,\ 2^{43})$	$\approx 7\,\%$
BlindOR	$(4,\ 2^{43})$	$\approx 100\,\%$
Parallel Schnorr	$(256\lambda,\ 512\lambda)$	$\approx 100\,\%$

Open Problems

- Can we break [HKLN20]?
  - We cannot find a nice norm-preserving decomposition wrt the response and challenge space.

- Can we have post-quantum adaptively/concurrently secure Σ-based blind signatures?
  - Adaptively secure Σ-based blind signature is possible in the classical world [EC:TesZhu22].
  - Small challenge space is inevitable for some group action related signature schemes (e.g. CSIDH, MEDS, LESS, (LIP)).

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

Thank you for listening!

casa.rub.de