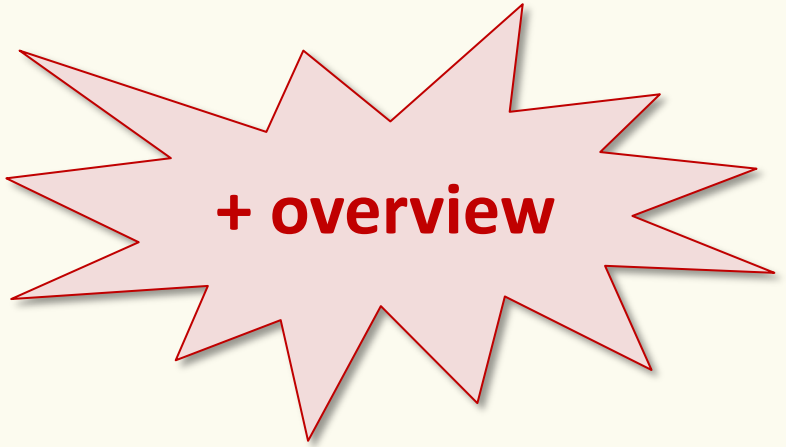
Short Pairing-Free Blind Signatures with Exponential Security

Based on joint work with **Chenzhi Zhu** (EUROCRYPT '22)



Stefano Tessaro

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

tessaro@cs.washington.edu

Agenda

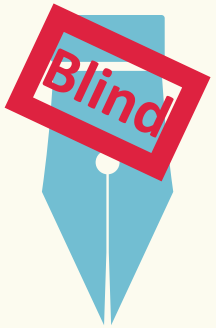
- Blind signatures: Review & state of the art
- Blind Schnorr & ROS Attacks
- Blind signatures with exponential security
- Open directions & perspective

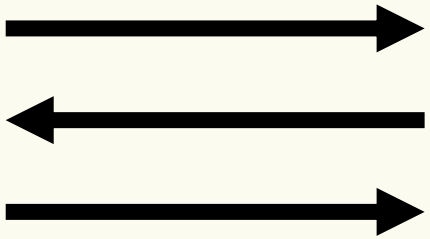
Blind Signatures [Chaum '83]

One-more unforgeability: Only one msg/sig pair per session!

$(sk, pk) \xleftarrow{\$} \text{KeyGen}$

sk





pk, M

σ

Blindness: Can't link (M, σ) to session that generated it!

$\text{Verify}(pk, M, \sigma) = \text{Accept}$

Applications of Blind Signatures

- **Anonymous e-cash** [Chaum '83; Chaum, Fiat, Naor, '88]

- **Anonymous tokens**
  - e.g., PrivacyPass, Google TrustTokens, Apple PCM, …

Research axes

- Assumptions
- Round complexity
- Communication complexity
- Signature size & type
- Concurrent vs sequential security
- Statistical vs computational blindness
- Ideal-model proof vs. standard-model proof
- Post-quantum security
- …

Practical Blind Signatures

RSA-based

Blind RSA

[Chaum '83; Bellare, Namprempre, Pointcheval, Semanko, '03; Lysyanskaya '22]

RFC draft

Round-optimal 👍

Large keys & sigs 👎

Pairing-friendly curves

Blind BLS

[Boneh-Lynn-Shacham '01, Boldyreva, '03]

Round-optimal 👍

Short keys & sigs 👍

Slow verification 👎

Needs pairing 👎

Also: SPS-EQ [HS14, ...]

Standard curves

(It's complicated)

None is post-quantum secure (I will come back to this!)

Agenda

- Blind signatures: Review & state of the art
- Blind Schnorr & ROS Attacks
- Blind signatures with exponential security
- Open directions & perspective

Review – Schnorr Signatures

Cyclic group $\mathbb{G} = \langle g \rangle \quad pk = g^{sk}$

$$\text{Sign}(sk, M) = (A = g^{\alpha}, \alpha + H(M, A) \cdot sk) \qquad \alpha \xleftarrow{\$} \mathbb{Z}_p$$

$$\text{Verify}(pk, M, (A, s)) = \left(g^{s} = A \cdot pk^{H(M,A)}\right)$$

Interactive Schnorr Signatures

$sk \in \mathbb{Z}_p$

$\alpha \xleftarrow{\$} \mathbb{Z}_p$

$A = g^{\alpha}$

c

$c \leftarrow H(M, A)$

$s = \alpha + c \cdot sk$

$M, pk = g^{sk}$

$\sigma = (A, s)$

Blind Schnorr Signatures

$sk \in \mathbb{Z}_p$

$\alpha \xleftarrow{\$} \mathbb{Z}_p$

$A = g^{\alpha}$ →

$M, pk = g^{sk}$

$\boldsymbol{\gamma}, \boldsymbol{\delta} \xleftarrow{\$} \mathbb{Z}_p$

$A' \leftarrow A \cdot pk^{\boldsymbol{\delta}} \cdot g^{\boldsymbol{\gamma}}$

← $c + \boldsymbol{\delta}$

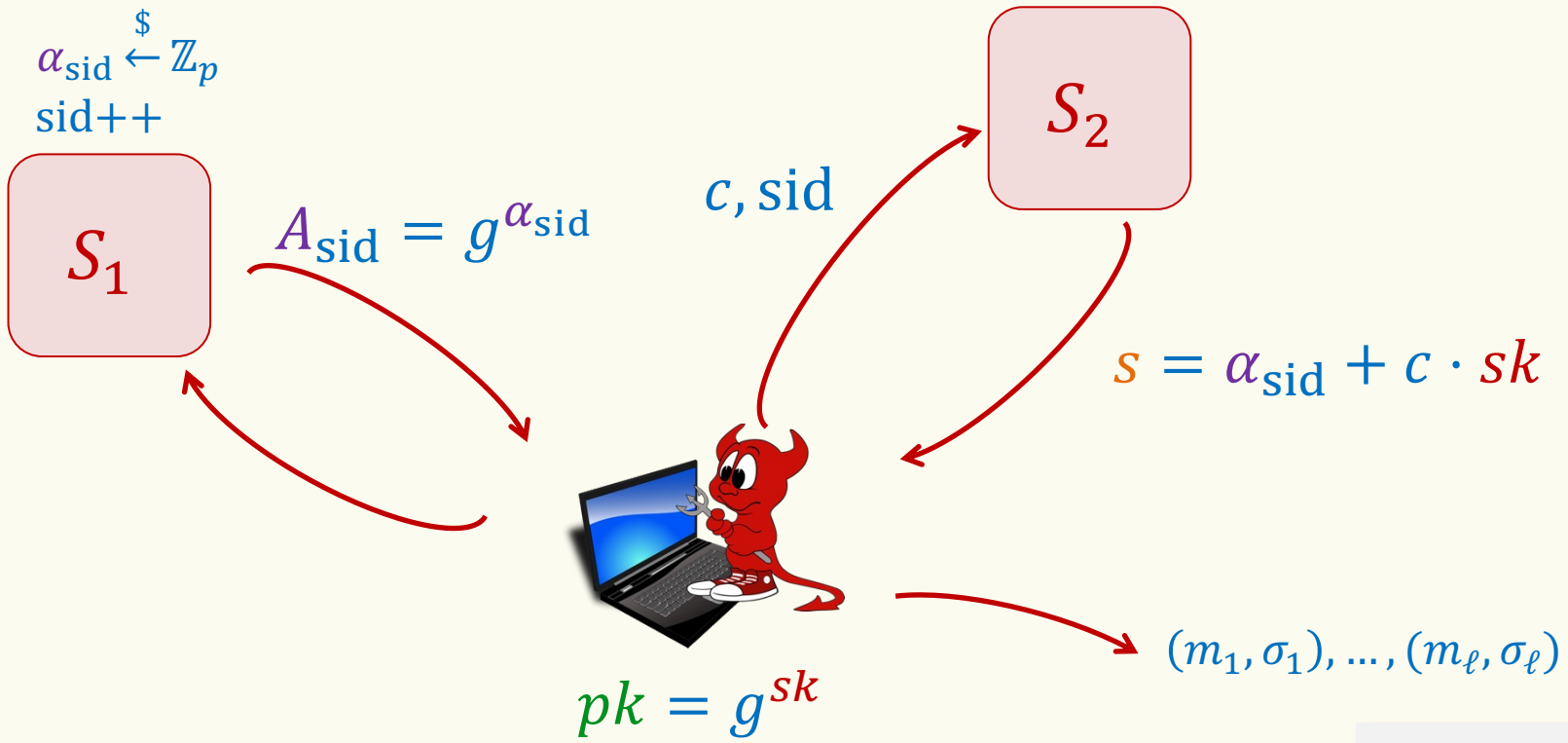
$c \leftarrow H(M, A')$

Perfect blindness! 👍

$s = \alpha + (c + \boldsymbol{\delta}) \cdot sk$ →

$\sigma = (A', s + \boldsymbol{\gamma})$

One-More Unforgeability (OMUF)



Win if distinct, valid, and $\ell > \text{sid}$

$$\text{Adv}^{\text{omuf}}_{\text{Schnorr}}(\mathcal{A}) = \Pr[\text{WIN}]$$

Blind Schnorr Signatures

- Sequentially OMUF-secure [Kastner, Loss, Xu, '22]
- Sub-exponentially OMUF-secure for $< \log p$ sessions
  [Fuchsbauer, Plouviez, Seurin, '20]

AGM + OMDL + ROM

- Polynomial-time break for $\geq \log p$ sessions
  [Benhamouda et al., '21]

$\log p = 256$

Main issue: Linearity

$$A_1 = g^{\alpha_1} \qquad s_1 = \alpha_1 + c_1 \cdot sk$$
$$A_2 = g^{\alpha_2} \qquad s_2 = \alpha_2 + c_2 \cdot sk$$

λ_1, λ_2

$$\underbrace{\lambda_1 s_1 + \lambda_2 s_2}_{s} = \underbrace{\lambda_1 \alpha_1 + \lambda_2 \alpha_2}_{} + (\lambda_1 c_1 + \lambda_2 c_2) \cdot sk$$

$\sigma = (A_1^{\lambda_1} A_2^{\lambda_2}, s)$ valid for M iff $H\left(M, A_1^{\lambda_1} A_2^{\lambda_2}\right) = \lambda_1 c_1 + \lambda_2 c_2$

Closer look – Parallel Attacks

$pk = g^{sk}$

$\vec{A} = (g^{\alpha_1}, \ldots, g^{\alpha_\ell})$

$\vec{c} = (c_1, \ldots, c_\ell)$

$\vec{s} = (s_1, \ldots, s_\ell)$

$s_i = \alpha_i + c_i \cdot sk$

Can the attacker produce $\ell + 1$ signatures?

Linear Structure

$$\langle \vec{\alpha}, \vec{\lambda} \rangle = \lambda_1 \alpha_1 + \cdots + \lambda_\ell \alpha_\ell$$

$$\langle \vec{c}, \vec{\lambda} \rangle = \lambda_1 c_1 + \cdots + \lambda_\ell c_\ell$$

$$\langle \vec{s}, \vec{\lambda} \rangle = \lambda_1 s_1 + \cdots + \lambda_\ell s_\ell$$

$$\vec{A} = (g^{\alpha_1}, \ldots, g^{\alpha_\ell})$$

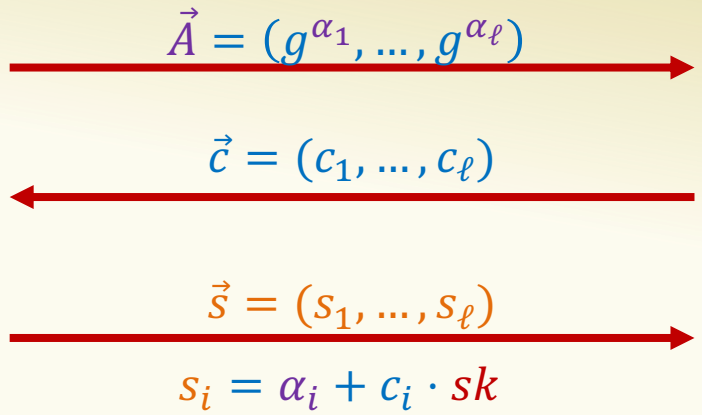
$$\vec{c} = (c_1, \ldots, c_\ell)$$

$$\vec{s} = (s_1, \ldots, s_\ell)$$

$$s_i = \alpha_i + c_i \cdot sk$$

$$H\left(M, g^{\langle \vec{\alpha}, \vec{\lambda} \rangle}\right) = \langle \vec{c}, \vec{\lambda} \rangle \quad \Rightarrow \quad \left(g^{\langle \vec{\alpha}, \vec{\lambda} \rangle}, \langle \vec{s}, \vec{\lambda} \rangle\right) \text{ is valid sig}$$

Linear Structure - Generalization



Goal: Find $\vec{\lambda}^{(1)}, \ldots, \vec{\lambda}^{(k)}, M_1, \ldots, M_k, \vec{c}$ s.t.

$$H\left(M_i, g^{\left\langle \vec{\alpha}, \vec{\lambda}^{(i)} \right\rangle}\right) = \left\langle \vec{c}, \vec{\lambda}^{(i)} \right\rangle \text{ for all } i = 1, \ldots, k$$

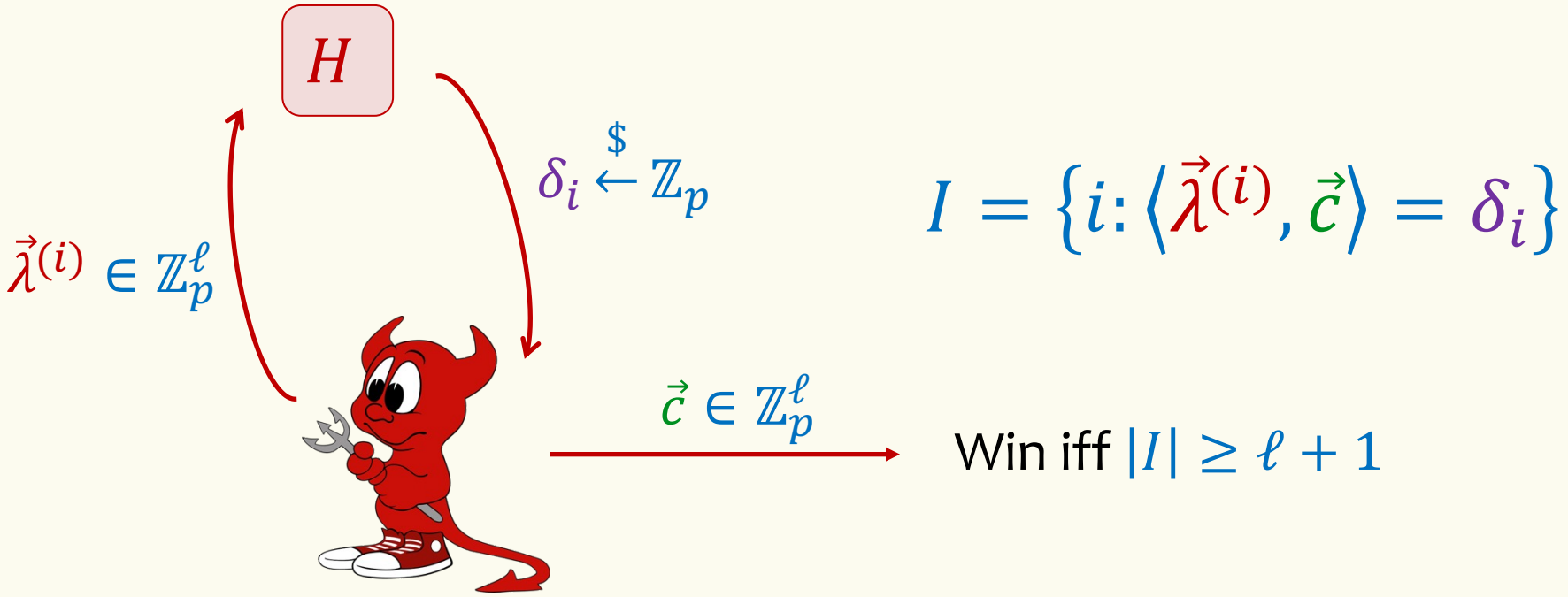
$$\left(g^{\left\langle \vec{\alpha}, \vec{\lambda}^{(i)} \right\rangle}, \left\langle \vec{s}, \vec{\lambda}^{(i)} \right\rangle\right) \text{ valid for all } i = 1, \ldots, k$$

Solution for $k \leq \ell$: Uninteresting & easy – just solve equations!

Solution for $k > \ell$? OMUF break!

Abstraction: ROS Problem

[Random inhomogeneities in an Overdetermined Solvable system of linear equations] [Schnorr, '01]



$$I = \left\{ i : \left\langle \vec{\lambda}^{(i)}, \vec{c} \right\rangle = \delta_i \right\}$$

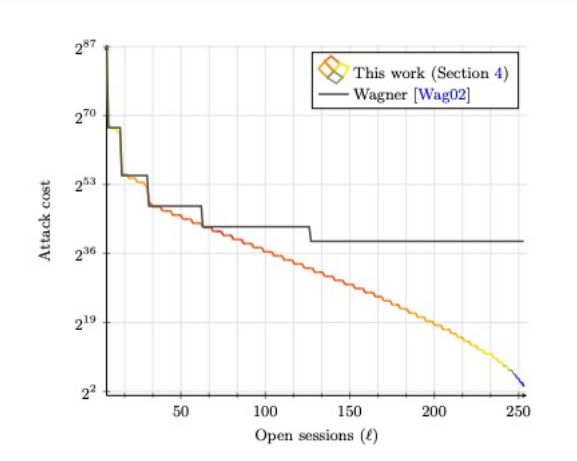
Win ROS → OMUF break

How hard?

Hardness of ROS – Best Attacks

[Wagner '02] $(\ell + 1)2^{\frac{\log p}{1+\log \ell}}$ (Any ℓ)

[Benhamouda et al. '21] $\tilde{O}(\ell)$ 😮 $(\ell \geq \log p)$



Source: [Benhamouda et al. '21]

Combined attack for any ℓ

Next: How do we prevent ROS attacks?

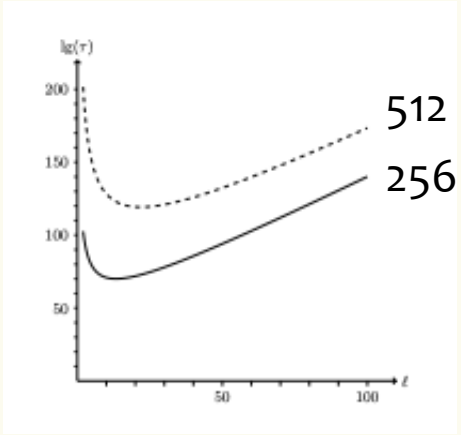
Prior Works

AGM + ROM

	Signature Size	Communication	OMUF	Blindness
[Abe '01]	$2\,\mathbb{G} + 6\,\mathbb{Z}_p$	λ bits $+ 3\,\mathbb{G} + 6\,\mathbb{Z}_p$	**DL** [KLX '22]	**DDH**
Clause Blind Schnorr [Fuchsbauer, Plouviez, Seurin, '20]	$1\mathbb{G} + 1\,\mathbb{Z}_p$	$2\,\mathbb{G} + 4\,\mathbb{Z}_p$	**OMDL** **mROS**	**Perfect**

It's a Schnorr Sig! 👍

Sub-exponential attack



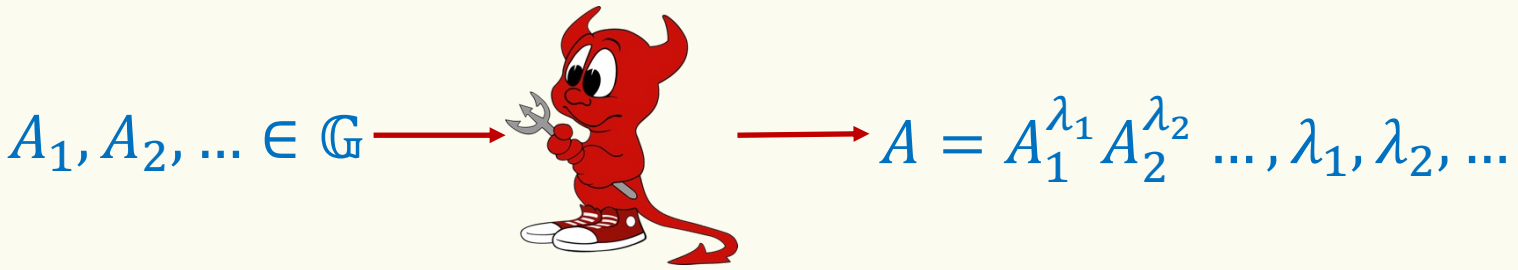
Detour – GGM & AGM

Generic Group Model [Shoup '97; Maurer '04]

- $X = g^x$ replaced by $\phi(x)$ for random injection $\phi: \mathbb{Z}_p \to \{0,1\}^\lambda$
- Oracle $\mathrm{MULT}(\phi(x), \phi(y)) = \phi(x + y)$

Algebraic Group Model [Fuchsbauer, Kiltz, Loss, '19]

- Security only for algebraic adversaries which output representation output group elements wrt input group elements



This Work

AGM + ROM

	Signature Size	Communication	OMUF	Blindness
[Abe '01]	$2\,\mathbb{G} + 6\,\mathbb{Z}_p$	λ bits $+ 3\,\mathbb{G} + 6\,\mathbb{Z}_p$	DL [KLX '22]	DDH
Clause Blind Schnorr [Fuchsbauer, Plouviez, Seurin, '20]	$1\,\mathbb{G} + 1\,\mathbb{Z}_p$	$2\,\mathbb{G} + 4\,\mathbb{Z}_p$	OMDL **mROS**	Perfect
Scheme I	$1\,\mathbb{G} + 2\,\mathbb{Z}_p$	$2\,\mathbb{G} + 3\,\mathbb{Z}_p$	**GGM**	Perfect
Scheme II	$1\,\mathbb{G} + 3\,\mathbb{Z}_p$	$2\,\mathbb{G} + 4\,\mathbb{Z}_p$	DL	Perfect

Can be made partially blind!

Can be shortened to $1\,\mathbb{G} + 2\,\mathbb{Z}_p$ [Crites, Komlo, Maller, '22]

Recall: Linearity

$$A_1 = g^{\alpha_1} \qquad s_1 = \alpha_1 + c_1 \cdot sk$$
$$A_2 = g^{\alpha_2} \qquad s_2 = \alpha_2 + c_2 \cdot sk$$

λ_1, λ_2

$$\underbrace{\lambda_1 s_1 + \lambda_2 s_2}_{s} = \underbrace{\lambda_1 \alpha_1 + \lambda_2 \alpha_2}_{} + (\lambda_1 c_1 + \lambda_2 c_2) \cdot sk$$

$\sigma = (A_1^{\lambda_1} A_2^{\lambda_2}, s)$ valid for M iff $H\left(M, A_1^{\lambda_1} A_2^{\lambda_2}\right) = \lambda_1 c_1 + \lambda_2 c_2$

Our Approach: Linearity Breaking!

y_i **random** and **hidden** prior to picking c_i

$$s_1 = \alpha_1 + c_1 \cdot y_1 \cdot sk$$
$$s_2 = \alpha_2 + c_2 \cdot y_2 \cdot sk$$

λ_1, λ_2

$$\lambda_1 s_1 + \lambda_2 s_2 = \lambda_1 \alpha_1 + \lambda_1 \alpha_2 + (\lambda_1 c_1 y_1 + \lambda_2 c_2 y_2) \cdot sk$$

$$\neq$$

$$\lambda_1 s_1 + \lambda_2 s_2 = \lambda_1 \alpha_1 + \lambda_1 \alpha_2 + (\lambda_1 c_1 + \lambda_2 c_2) \cdot y^* \cdot sk$$

Approach - Blueprint

$sk \in \mathbb{Z}_p$

$\alpha, y \xleftarrow{\$} \mathbb{Z}_p$

$M, pk = g^{sk}$

$A = g^{\alpha}, Y = \mathrm{Com}(y)$ →

c ←

$c \leftarrow H(M, A, Y)$

$s = \alpha + c \cdot y \cdot sk, \quad y$ →

$\sigma = (A, s, y)$

Instantiation I

$\mathrm{Com}(y) = pk^y$

$sk \in \mathbb{Z}_p$

$\alpha, y \xleftarrow{\$} \mathbb{Z}_p$

$A = g^\alpha, Y = pk^y$ →

$M, pk = g^{sk}$

← c

$c \leftarrow H(M, A, Y)$

$s = \alpha + c \cdot y \cdot sk, \quad y$ →

$\sigma = (A, s, y)$

Instantiation I – Blind Version

$sk \in \mathbb{Z}_p$

$\alpha, y \xleftarrow{\$} \mathbb{Z}_p$

$A = g^{\alpha}, Y = pk^{y}$ →

$M, pk = g^{sk}$

$\boldsymbol{\gamma}, \boldsymbol{\delta_1}, \boldsymbol{\delta_2} \xleftarrow{\$} \mathbb{Z}_p$

$Y' \leftarrow Y^{\boldsymbol{\gamma}}$

$A' \leftarrow g^{\boldsymbol{\delta_1}} \cdot A^{\boldsymbol{\gamma}} \cdot Y'^{\boldsymbol{\delta_2}}$

← $c + \boldsymbol{\delta_2}$

$c \leftarrow H(M, A', Y')$

$s = \alpha + (c + \boldsymbol{\delta_2}) \cdot y \cdot sk, y$ →

$\sigma = (A', \boldsymbol{\gamma} s + \boldsymbol{\delta_1}, \boldsymbol{\gamma} y)$

Instantiation II

$\mathrm{Com}(y;\rho) = g^{\rho} h^{y}$

$sk \in \mathbb{Z}_p$

$\alpha, y, \rho \xleftarrow{\$} \mathbb{Z}_p$

$A = g^{\alpha}, Y = g^{\rho} h^{y}$ →

$M, pk = g^{sk}$

← c

$c \leftarrow H(M, A, Y)$

$s = \alpha + c \cdot y \cdot sk, \rho, y$ →

$\sigma = (A, s, y, \rho)$

Our results (informally)

Main ingredient: New problem – **Weighted Fractional ROS (WFROS)**

Theorem 1. WFROS hard ⇒ Scheme 1 is secure in the GGM.

Theorem 2. WFROS + DL hard ⇒ Scheme 2 is secure in the AGM

Theorem 3. WFROS is (exponentially) hard

Linearity

$$A_1 = g^{\alpha_1} \quad Y_1 = pk^{y_1} \quad s_1 = \alpha_1 + c_1 \cdot y_1 \cdot sk$$
$$A_2 = g^{\alpha_2} \quad Y_2 = pk^{y_2} \quad s_2 = \alpha_2 + c_2 \cdot y_2 \cdot sk$$

λ_1, λ_2

$$\lambda_1 s_1 + \lambda_2 s_2 = \lambda_1 \alpha_1 + \lambda_1 \alpha_2 + (\lambda_1 c_1 y_1 + \lambda_2 c_2 y_2) \cdot sk$$

$\sigma = (A_1^{\lambda_1} A_2^{\lambda_2}, Y_1^{\gamma_1} Y_2^{\gamma_2}, \lambda_1 s_1 + \lambda_2 s_2)$ valid for M iff

$$H\left(M, A_1^{\lambda_1} A_2^{\lambda_2}\right) \cdot (\gamma_1 y_1 + \gamma_2 y_2) = \lambda_1 c_1 y_1 + \lambda_2 c_2 y_2$$

This is harder!

$\vec{A} = (g^{\alpha_1}, \ldots, g^{\alpha_\ell})$

$\vec{Y} = (pk^{y_1}, \ldots, pk^{y_\ell})$

Goal: Find $\vec{\lambda}^{(i)}, \vec{\gamma}^{(i)} \in \mathbb{Z}_p^\ell$ + $\vec{c} \in \mathbb{Z}_p^\ell$ s.t.

$$H\left(M_i, g^{\langle \vec{\alpha}, \vec{\lambda}^{(i)} \rangle}, pk^{\langle \vec{y}, \vec{\gamma}^{(i)} \rangle}\right) = \frac{\sum_j c_j \cdot \lambda_j^{(i)} \cdot y_j}{\sum_j \gamma_j^{(i)} \cdot y_j}$$

$\vec{c} = (c_1, \ldots, c_\ell)$

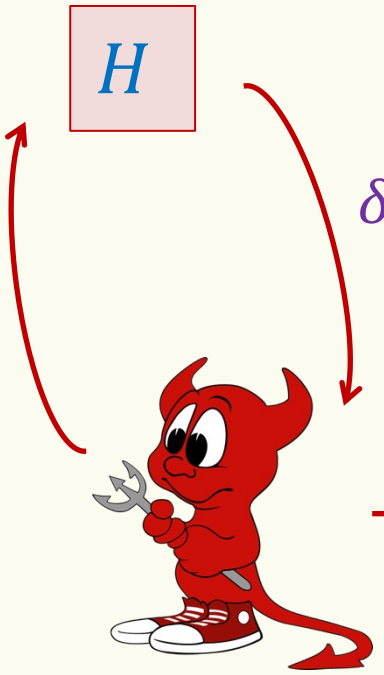
$\vec{s} = (s_1, \ldots, s_\ell)$

$\vec{y} = (y_1, \ldots, y_\ell)$

$s_i = \alpha_i + c_i \cdot y_i \cdot sk$

Problem: We learn $\vec{y}$ <u>after</u> fixing choice of $\vec{c}$

WFROS Game (Toy version)

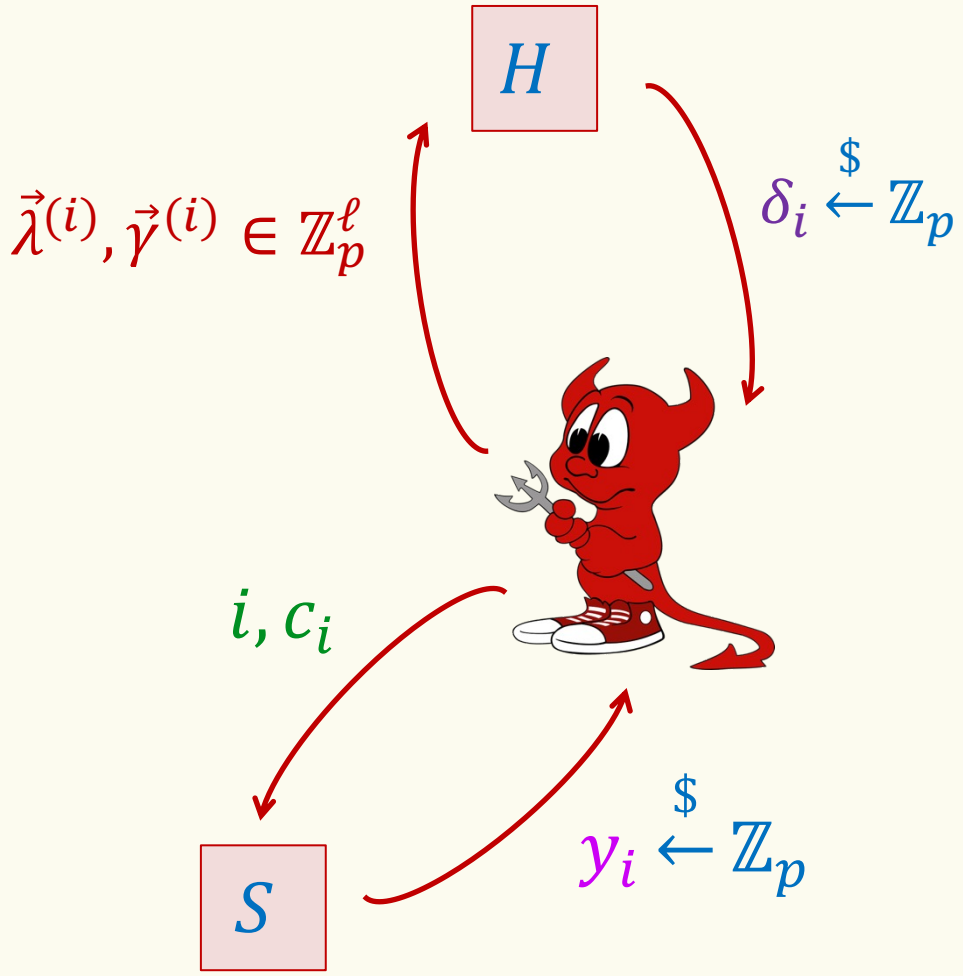


$$\vec{y} \xleftarrow{\$} \mathbb{Z}_p^\ell$$

$$I = \left\{ i : \frac{\sum_j c_j \cdot \lambda_j^{(i)} \cdot y_j}{\sum_j \gamma_j^{(i)} \cdot y_j} = \delta_i \right\}$$

Win iff $|I| \geq \ell + 1$

WFROS Game (Actual version)



$$I = \left\{ i : \frac{\sum_j c_j \cdot \lambda_j^{(i)} \cdot y_j}{\sum_j \gamma_j^{(i)} \cdot y_j} = \delta_i \right\}$$

Win iff $|I| \geq \ell + 1$

WFROS – Exponential Hardness

Theorem. For any adversary $\mathcal{A}$ issuing Q_H queries to H, the probability of solving WFROS is

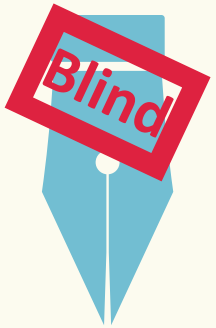
$$\mathrm{Adv}^{\mathsf{wfros}}_{\ell,p}(\mathcal{A}) \leq \frac{Q_H(Q_H + 2\ell)}{p-1}$$

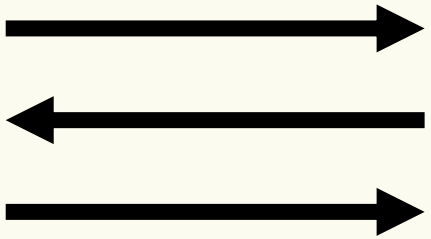
Thus, for a break we need $\max\{Q_H, \ell\} \geq \Omega(\sqrt{p})$

Partially-Blind Signatures Signatures [Abe, Fujisaki, '96]

$(sk, pk) \xleftarrow{\$} \text{KeyGen}$

sk, inp





pk, M, inp

σ

$\text{Verify}(pk, M, \text{inp}, \sigma) = \text{Accept}$

Partially Blind Scheme

$$\mathrm{Com}(y;\rho) = g^{\rho} H'(\mathrm{inp})^{y}$$

sk, inp

$M, pk,$ inp

$\alpha, y, \rho \xleftarrow{\$} \mathbb{Z}_p$

$A = g^{\alpha}, Y = g^{\rho} H'(\mathrm{inp})^{y}$ →

← c

$c \leftarrow H(M, A, Y)$

$s = \alpha + c \cdot y \cdot sk, \rho, y$ →

$\sigma = (A, s, y, \rho)$

Agenda

- Blind signatures: Review & state of the art
- Blind Schnorr & ROS Attacks
- Blind signatures with exponential security
- Open directions & perspective

Technical Challenges & Open Questions

- **It is not Schnorr**
- **Not round-optimal / stateful**
  - Certain applications are inherently stateless (e.g., PrivacyPass)
  - Other can be stateful (e.g., UProve)
  - Opportunity for DoS attacks, implementation errors & reset attacks
- **Security proofs require AGM/GGM**

- **Alternative:** Pairing-free instantiation of [Fischlin '06]
  - Round optimal, but hardly practical (non-black box techniques)

What about post-quantum?

OMUF Security

Scheme	Assumption	Sig Size	Moves	Key size
[BLS]	SDH	48 B	2	96 B
[This work]	DL	96 B	3	32 B
[AKSY22]	om-ISIS	45 KB	2	?

[128-bit security]

Blindness

Many schemes offer statistical and/or perfect blindness (automatically post-quantum secure!)

Main question: To what extent is post-quantum OMUF a priority?

Thank you!