# Towards a Tightly Secure Signature in Multi-User Setting with Corruptions Based on Search Assumptions

Hirofumi Yoshioka
Tokyo Tech

Wakaha Ogata
Tokyo Tech

**Keitaro Hashimoto**
AIST

CFAIL 2024; 8/17/2024
Full version: ia.cr/2024/1286

We are the first CFAIL presenter from Japan!

# Our Problem and Results

**Can we construct a tightly secure signature**
**in multi-user setting with corruptions**
**based on search assumptions?**

* Open problem mentioned in [PR20,PQR21]

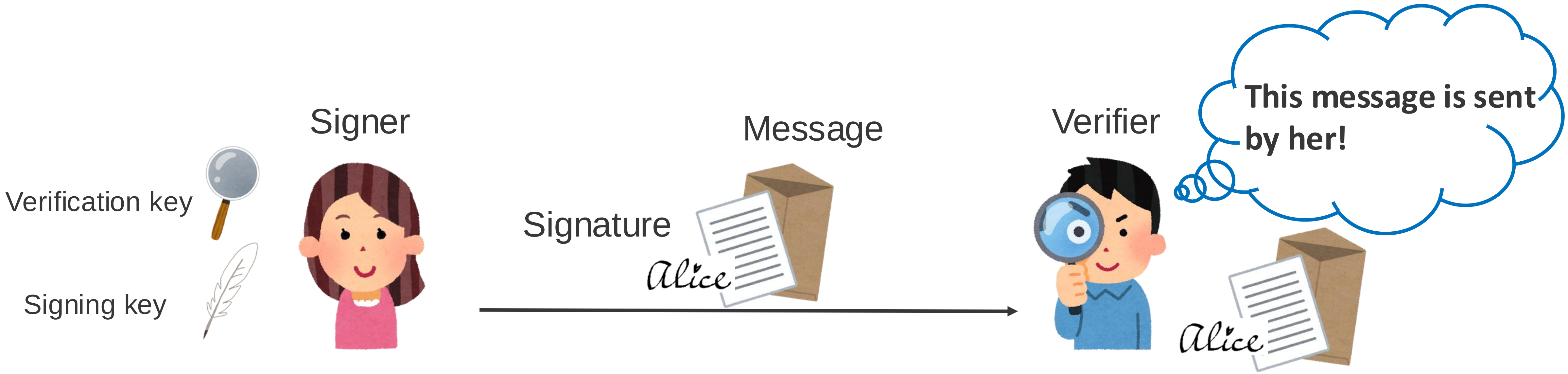
- Reveal new conditions that make tightly secure signatures impossible
  - This leaves room for tightly-secure signatures from search assumptions

    ⇒ Fail to prove impossibility…
- Construct a new signature in multi-user setting with corruptions from CDH
  - It does not contradict the known impossibility results
  - Reduction loss is independent of #users, but depends on #RO-query

    ⇒ Fail to prove possibility…

# Background

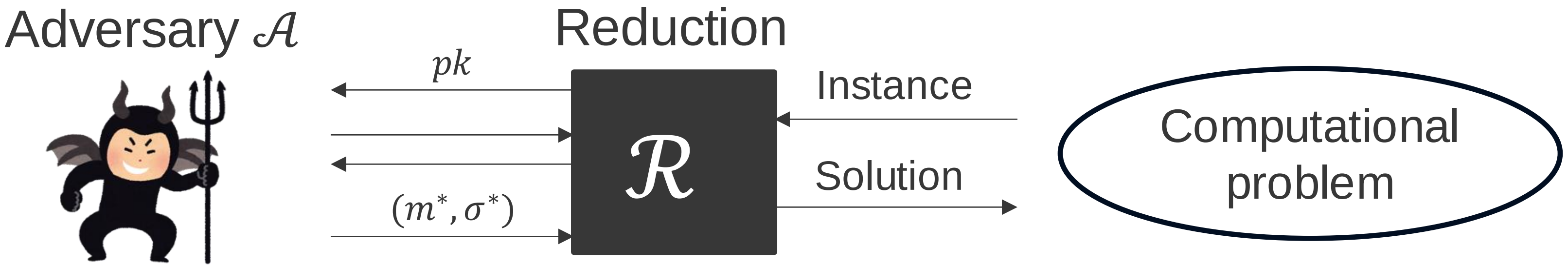
# Digital Signature




- Cryptographic primitive for user authentication
  - Building block for secure protocols, e.g., authenticated key exchange
- Its security analysis is important for real-world protocols
  - There are many metric to evaluate security
  - Our focus: reduction loss, security model, and computational problem

# Reduction and Reduction Loss

- To prove the security of signature schemes, we show a reduction $\mathcal{R}$
  - $\mathcal{R}$ solves a computational problem by using an adversary $\mathcal{A}$




- $\mathcal{R}$ is constructed so that its advantage Adv and running time $\mathbf{T}$ satisfy

$$\frac{\mathrm{Adv}_{\mathcal{A}}}{\mathbf{T}(\mathcal{A})} \leq L \cdot \frac{\mathrm{Adv}_{\mathcal{R}}}{\mathbf{T}(\mathcal{R})}$$

- The coefficient $\boldsymbol{L}$ is called **reduction loss**
  - Reduction is tight if $L$ is small constant (i.e., independent of $\mathcal{A}$'s activity etc.)
  - Since $L$ has an impact on parameter size, tight reduction is desirable

# Security Model for Signatures

- We consider multi-user setting with corruptions (MU-EUF-CMA-C)
  - Generalization of standard single-user security (EUF-CMA)

Adversary $\mathcal{A}$

$(pk_i)_{i\in[N]}$

$i \in [N]$

$sk_i$

$(i, m)$

$\sigma$

$(i^*, m^*, \sigma^*)$

Game MU−UF−CMA−C

For $i \in [N]$ : $(pk_i, sk_i) \leftarrow$ Gen

$\mathrm{Corr}$

$\mathrm{Sig}$

***N* users**

**Corrupt users adaptively**

- EUF-CMA implies MU-EUF-CMA-C with reduction loss $L = \#\mathrm{Users}$

# Computational Problems

## Search problems: e.g., CDH

$\mathbb{G}$: cyclic groups with order $p$
$g$: generator in $\mathbb{G}$
$\alpha, \beta \in \{0, \ldots, p-1\}$

$(g, g^{\alpha}, g^{\beta}) \longrightarrow$

$\xrightarrow{g^{\alpha\beta}}$

## Decision problems: e.g., DDH

$\alpha, \beta, \gamma \in \{0, \ldots, p-1\}$

Set $S$ $\longrightarrow (g, g^{\alpha}, g^{\beta}, g^{\alpha\beta})$
or
Set $S'$ $\longrightarrow (g, g^{\alpha}, g^{\beta}, g^{\gamma})$

$\longrightarrow$

$\xrightarrow{S \text{ or } S'}$

- Search problems are more difficult than decision problems
  ⇒ Signature schemes based on search problems are more secure

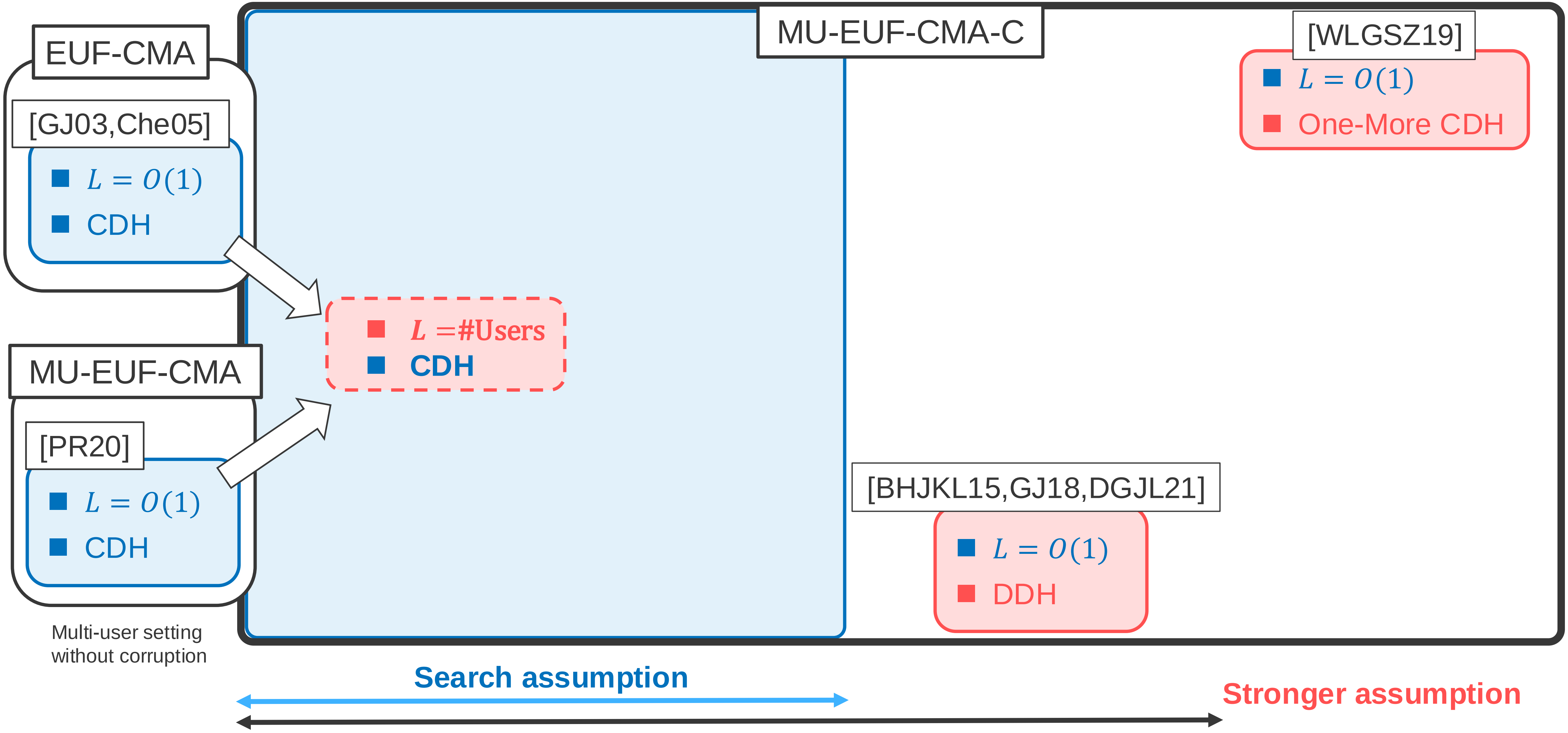
# Existing Tightly-Secure Signatures (All in the ROM)

| Scheme | Security model | Assumption |
|---|---|---|
| **[GJ03,Che05,KLP17]** | Single-user ❌ | CDH ✅ |
| **[PR20]** | Multi-user w/o corruption ❌ | CDH ✅ |
| **[WLGSZ19]** | Multi-user w/ corruption ✅ | One-More CDH ❌ |
| **[Bader14]** | Multi-user w/ corruption ✅ | SXDH ❌ |
| **[BHJKL15]** | Multi-user w/ corruption ✅ | DLIN ❌ |
| **[GJ18]** | Multi-user w/ corruption ✅ | CDH+DDH ❌ |
| **[DGJL21,PW22]** | Multi-user w/ corruption ✅ | DDH ❌ |

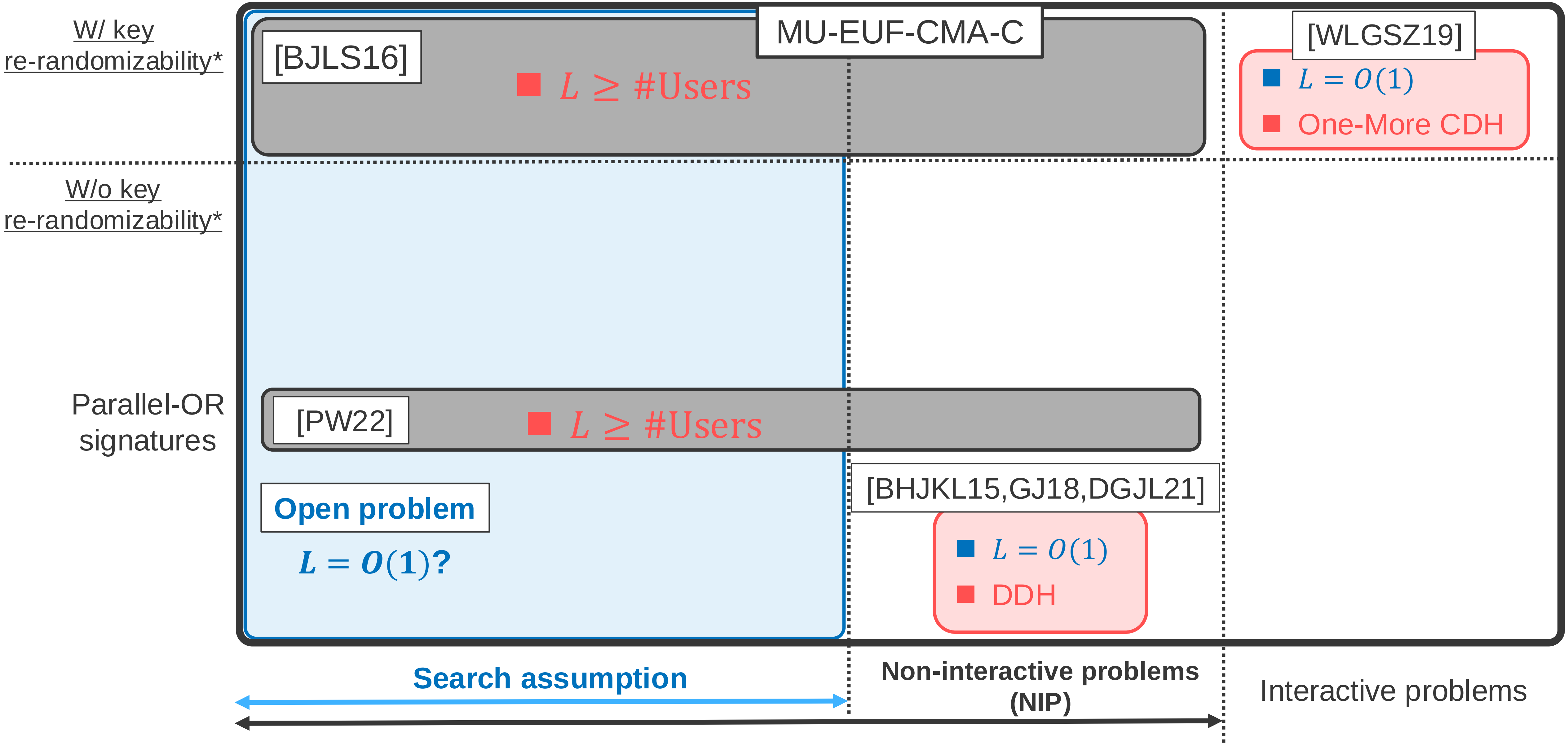
**Can we construct a tightly secure signature scheme in multi-user w/ corruption based on search assumptions?**

Open problem mentioned in [PR20,PQR21]

# Existing Tightly-Secure Signatures (All in the ROM)

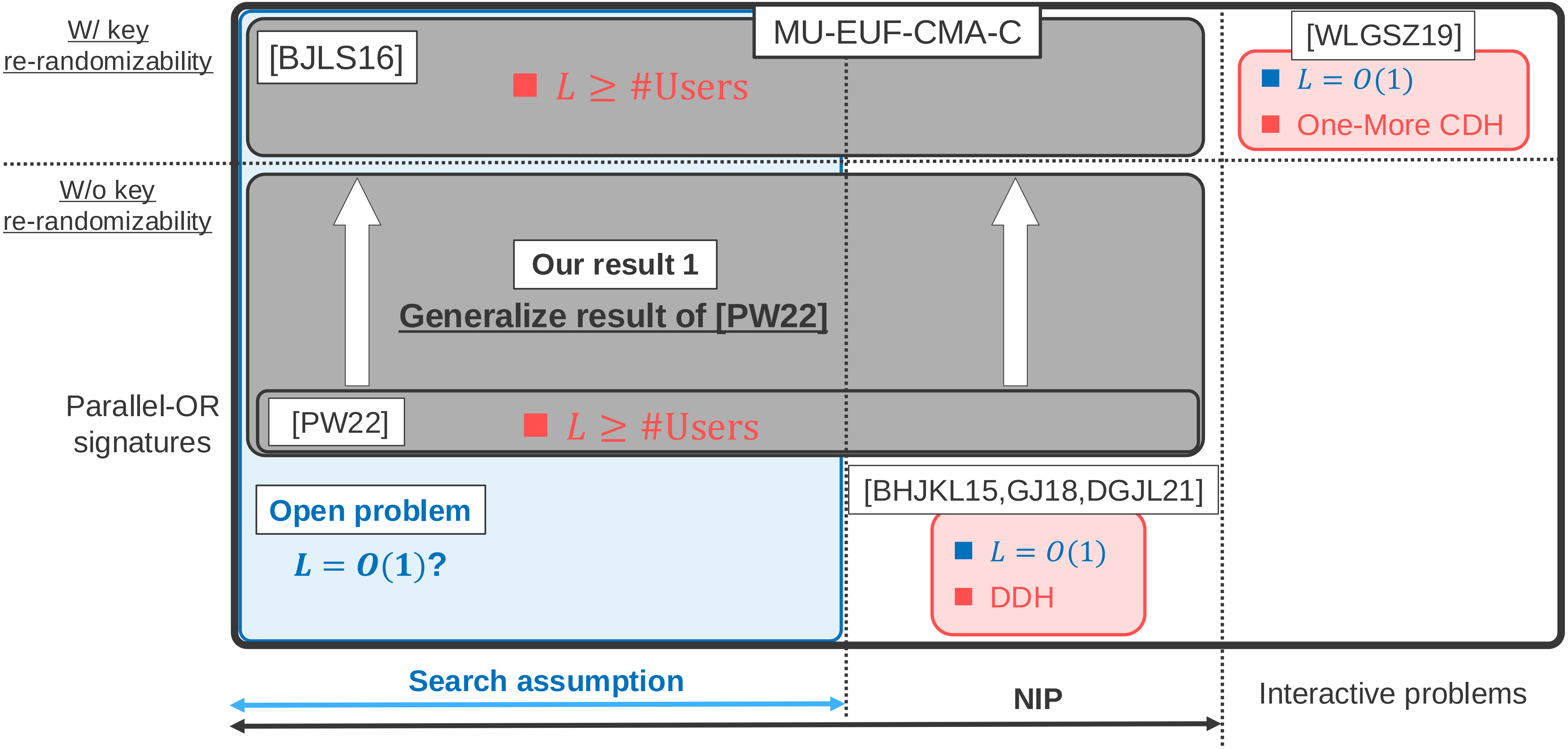


# Impossibility Results on Tightly-Secure Signatures

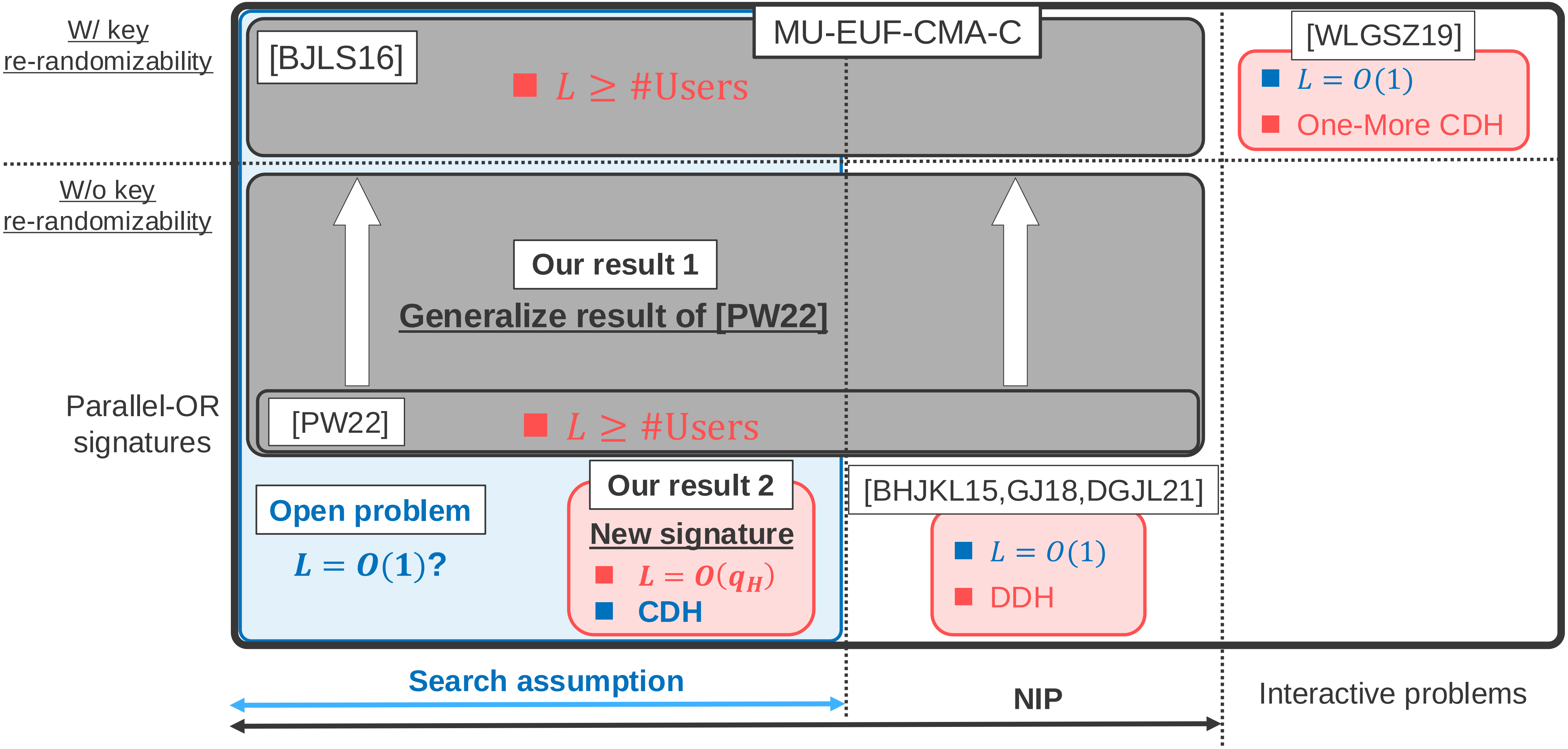



* There exists a PPT algorithm ReRand(pk, sk) → sk' that samples sk' w.r.t. pk uniformly at random.

# Our Results: New Impossibility Result



# Our Results: New Impossibility Result and New Signature



# Our result 1: New Impossibility Result

# Our Impossibility Result

- Assume SIG satisfies the following properties (explain later)
  - **$\varepsilon_{RO}$-RO statistically close**
  - **$\varepsilon_{SIG}$-signature statistically close**
- Then, reduction loss $L$ from MU-EUF-CMA-C of SIG to NIP satisfies

$$L \geq \frac{1}{\mathrm{Adv}_{\mathcal{RA}}^{\mathrm{NIP}} + (\cancel{2}4\delta_{\mathcal{R}} + \varepsilon_{RO} + \varepsilon_{SIG}) + \frac{1}{\#\mathrm{Users}}}$$

$\delta_{\mathcal{R}}$: statistical distance between MU-EUC-CMA-C game and $\mathcal{R}$'s simulating game

If $\mathrm{Adv}_{\mathcal{RA}}^{\mathrm{NIP}}$, $\delta_{\mathcal{R}}$ , $\varepsilon_{SIG}$, $\varepsilon_{RO}$ are all negligibly small, $L \geq \#\mathrm{Users}$

# New Property of Signature (1)

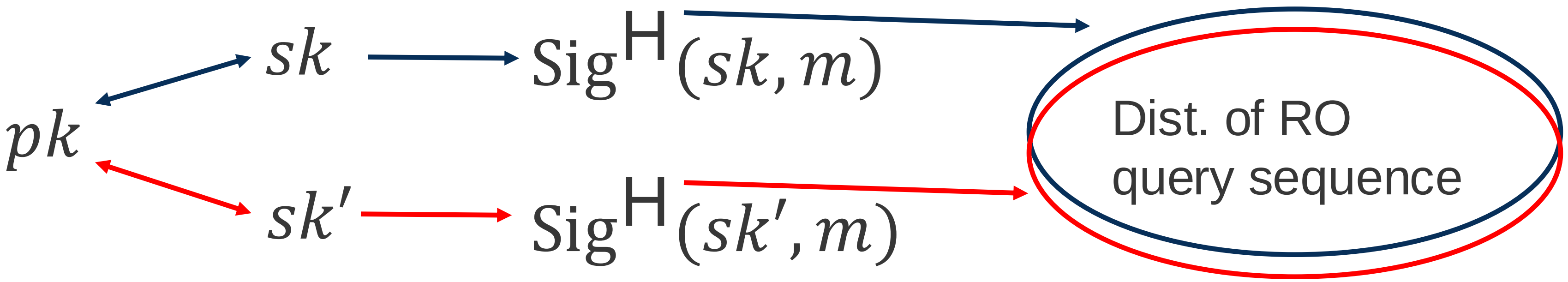
- We observe why Parallel-OR signature cannot achieve tight security [PW22]
- This is due to the property w.r.t. RO queries during signature generation

**Formalize this property**

**$\varepsilon_{RO}$-RO statistically close:** For any $m$, $pk$, and $sk, sk'$ w.r.t. $pk$

$$\mathrm{SD}(Q(sk,m); Q(sk',m)) \leq \varepsilon_{RO}$$

$Q(sk,m)$: random variable representing the RO queries issued in the run of $\mathrm{Sig}^{\mathrm{H}}(sk,m)$



# New Property of Signature (2)

- We notice [GJ18] achieve tight security <u>even it is RO statistically close…</u>
- We compare Parallel-OR (w/ $L \geq N$) and [GJ18] (w/ $L = O(1)$)
  ⇒ <u>Their distribution of signatures are different!</u>

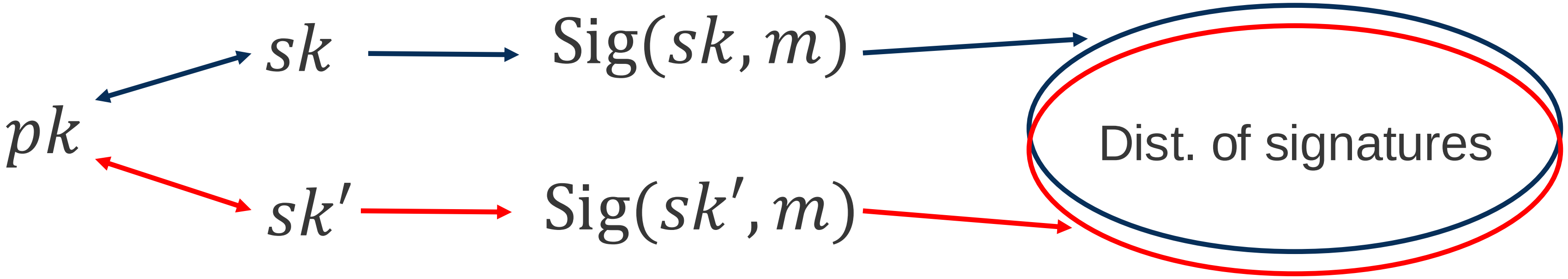
⬇ **Formalize this property**

**$\varepsilon_{SIG}$-signature statistically close:**

For any $m$, $pk$, and $sk, sk'$ w.r.t. $pk$

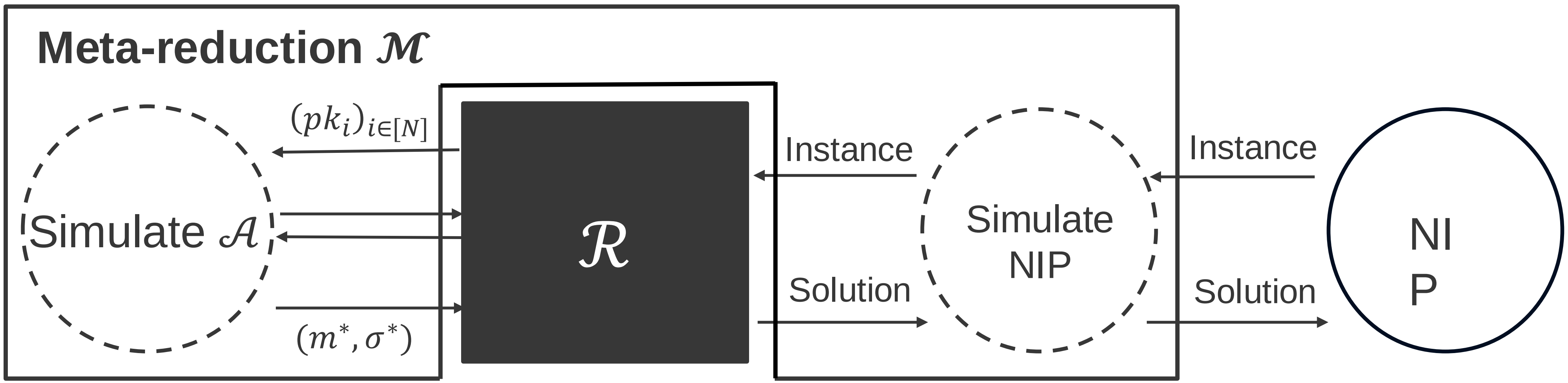
$$\mathrm{SD}(SIG(sk,m); SIG(sk',m)) \leq \varepsilon_{SIG}$$

$SIG(sk,m)$: random variable representing the output of $\mathrm{Sig}(sk,m)$



# Preliminaries for Proof: Meta-Reduction

1. Assume reduction $\mathcal{R}$ that solves NIP by interacting $\mathcal{A}$
2. Construct meta-reduction $\mathcal{M}$ that efficiently simulates $\mathcal{A}$ against $\mathcal{R}$
3. Prove that $\mathcal{R}$'s output does not change if $\mathcal{A}$ is simulated by $\mathcal{M}$




The existence of $\mathcal{M}$ contradicts the hardness of NIP
$\Rightarrow$ Such an $\mathcal{R}$ does not exist!

# Preliminaries for Proof: Weaker Security Definition for SIG

- To prove impossibility results, we consider weaker security definition
  - No message attacks in multi-user setting with static corruptions (MU-EUF-S)
  - Proving $L \geq \#\mathrm{Users}$ for MU-EUF-S is sufficient

Adversary $\mathcal{A}$

$(pk_i)_{i \in [N]}$ ←

$j \in [N]$ →

$(sk_i)_{i \in [N]/\{j\}}$ ←

query →

$h$ ←

$(m^*, \sigma^*)$ →

**Game MU-EUF-S**

For $i \in [N]$ : $(pk_i, sk_i) \leftarrow$ Gen

**Chose corrupted users statically**

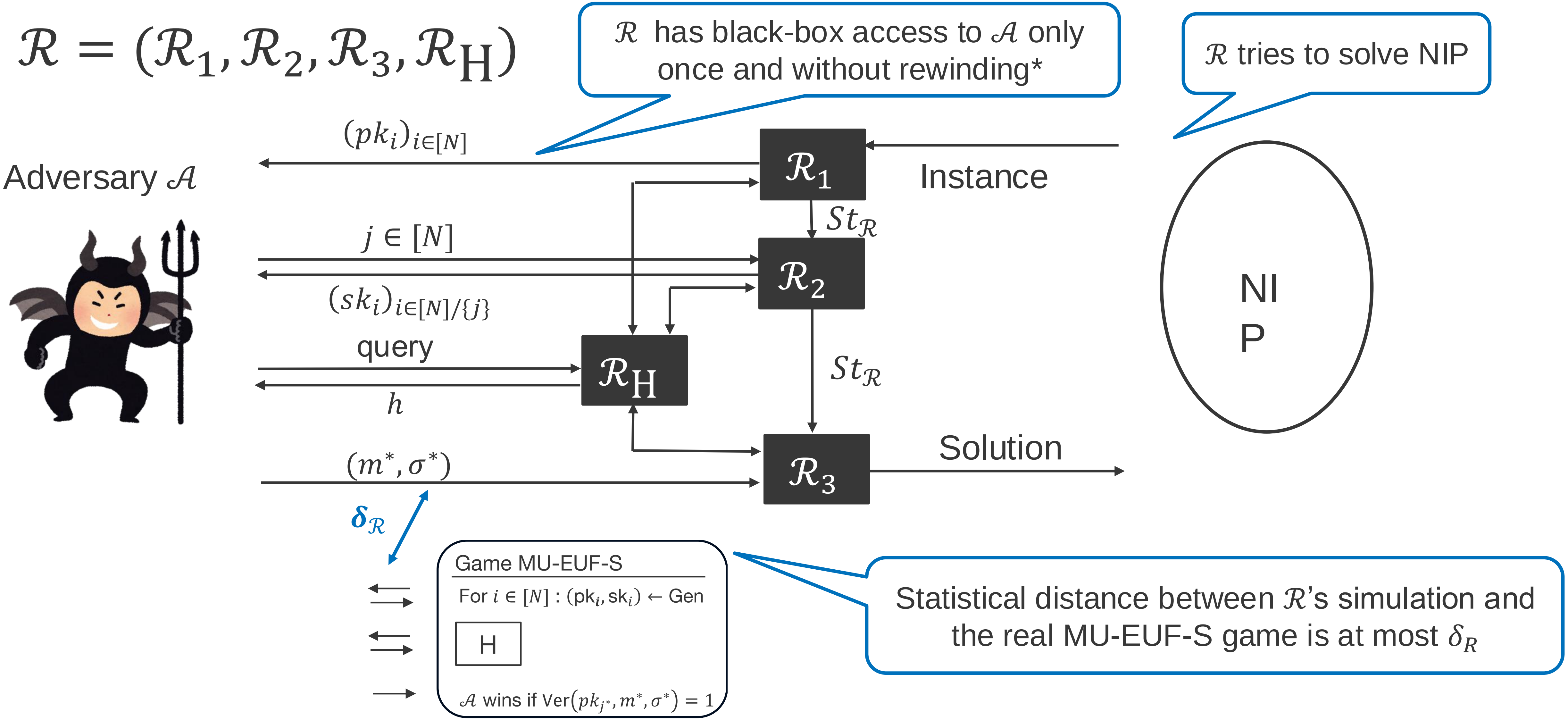
$\boxed{\mathrm{H}}$

**No signing oracle**

$\mathcal{A}$ wins if Ver$\left(pk_j, m^*, \sigma^*\right) = 1$

# Preliminaries for Proof: Modeling Reduction $\mathcal{R}$

$$\mathcal{R} = (\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_{\mathrm{H}})$$




* Such an $\mathcal{R}$ is said to be simple [PW22]. In the security proofs of many cryptographic primitives, reductions are simple.

# Proof Overview of Our Impossibility Result

## Meta-reduction $\mathcal{M}$

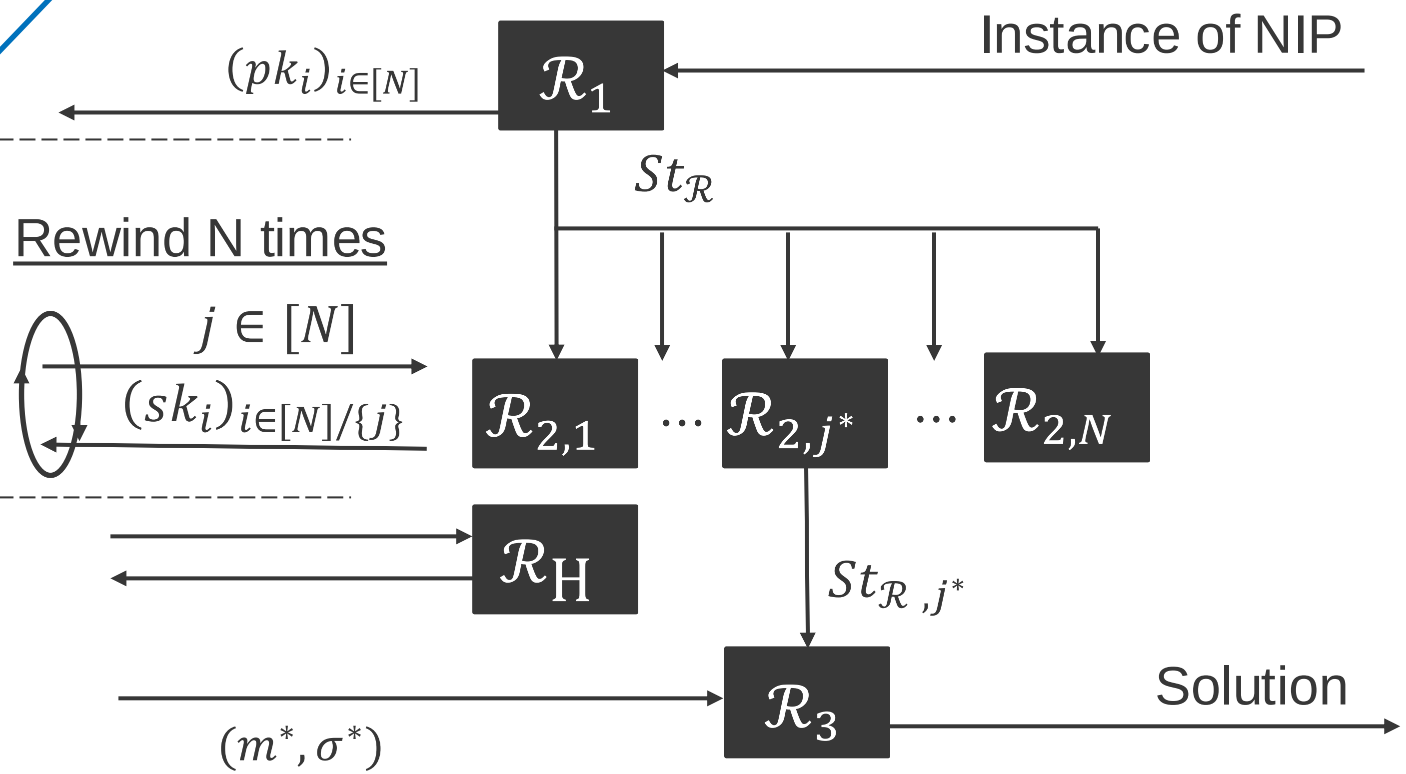
Identical to the proof in [BJLS16,PW22]

1. $\mathcal{M}$ inputs its instance into $\mathcal{R}_1$ as it is.

2. Run $\mathcal{R}_2$ for all $j \in [N]$ and store obtained secret keys.

3. Chose $j^* \in [N]$ at random and run $\mathcal{R}_3$ with state $St_{R,j^*}$

**4. Generate a forgery $(\boldsymbol{m}^*, \boldsymbol{\sigma}^*)$ with stored $\mathbf{sk}_{j^*}$**




RO-statistically close and signature statistically-close ensures that $\mathcal{R}_3$'s output interacting $\mathcal{A}$ and interacting $\mathcal{M}$ are indistinguishable

([BJLS16] ensures it with key re-randomizability)

# Our Impossibility Result (repeated)

- Assume SIG satisfies the following properties
  - $\boldsymbol{\varepsilon_{RO}}$**-RO statistically close**
  - $\boldsymbol{\varepsilon_{SIG}}$**-signature statistically close**
- Then, reduction loss $L$ from MU-EUC-CMA-C of SIG to NIP satisfies

$$L \geq \frac{1}{\mathrm{Adv}_{\mathcal{R}\mathcal{A}}^{\mathrm{NIP}} + (4\delta_{\mathcal{R}} + \varepsilon_{RO} + \varepsilon_{SIG}) + \frac{1}{\#\mathrm{Users}}}$$

$\delta_{\mathcal{R}}$: statistical distance between MU-EUC-CMA-C game and $\mathcal{R}$'s simulating game

If $\mathrm{Adv}_{\mathcal{R}\mathcal{A}}^{\mathrm{NIP}}$ , $\delta_{\mathcal{R}}$ , $\varepsilon_{SIG}$, $\varepsilon_{RO}$ are all negligibly small, $L \geq \#\mathrm{Users}$

# Discussion on Our Impossibility Result

To achieve tight security, at least one of the conditions is satisfied

1. SIG's security is based on <u>interactive problems</u>
   - Already done by [WLGSZ19]
2. $\mathcal{A}$'s view by $\mathcal{R}$ is not stat. close from the real game (i.e., $\delta_{\mathcal{R}} \neq negl$)
   - If so, they should be computationally indistinguishable
     $\Rightarrow$ <u>Decision problem is needed</u> as in [Bader14,BHJKL15, DGJL21]
3. SIG is not signature-statistically close (i.e., $\varepsilon_{SIG} \neq negl$)
   - If so, they should be computationally indistinguishable
     $\Rightarrow$ <u>Decision problem is needed</u> as in [GJ18]
4. SIG is not RO-statistically close (i.e., $\varepsilon_{RO} \neq negl$)
   - <u>**Decision problem may not be required…**</u>

# Our results 2: New SIG from CDH

## - reduction loss is independent of #Users -

# Our Approach

## Signatures based on sequential-OR proof is not RO statistically close

### Prior work

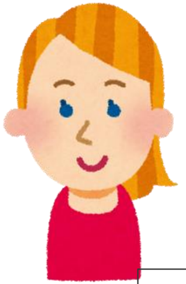
3-round lossy identification based on DDH [CP92] + Sequential-OR for 3-round IP [FHJ20] = Tight MU-EUF-CMA-C SIG based on DDH [DGJL21,PW22]

* To make $\delta_{\mathcal{R}} \neq negl$, DDH is required

### Our approach

5-round identification based on CDH [KLP17] + Sequential-OR for multi-round IP [FGQRW23] = Tight MU-EUF-CMA-C SIG based on CDH???

# 5-round Identification from CDH [KLP17]

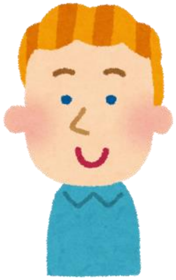


Prover

**$\mathrm{IGen}(1^\lambda) \to (sk, pk)$**

$sk \leftarrow_\$ \mathbb{Z}_p$
$pk := g^{sk}$

Verifier



**$\mathrm{Sim}(pk) \to Tran$**

$s, v, h' \leftarrow_\$ \mathbb{Z}_p$
$h := g^v$
$R := g^s \cdot x^{-h'}$
$R_L := pk^v, R_R := R^v$
$R' := (R_L, R_R)$
$Tran := (R, h, R', h', s)$

**$\mathrm{P}_1(sk) \to R$**

$st := r \leftarrow_\$ \mathbb{Z}_p$
$R := g^r$

$\xrightarrow{\quad R \quad}$

$h \leftarrow_\$ \mathbb{G}$

$\xleftarrow{\quad h \quad}$

**$\mathrm{P}_2(st, sk, R, h) \to R'$**

$R_L := h^{sk}, R_R := h^r$
$R' := (R_L, R_R)$
$st' := r$

$\xrightarrow{\quad R' \quad}$

This is a ZK protocol for language showing $(g, pk, h, R_L)$ is a DH tuple

$h' \leftarrow_\$ \mathbb{Z}_p$

$\xleftarrow{\quad h' \quad}$

**$\mathrm{P}_3(st', sk, R, R', h, h') \to s$**

$s := wh' + r \bmod p$

$\xrightarrow{\quad s \quad}$

**$\mathrm{V}(pk, R, R', h, h', s) \to 1/0$**

Iff $R = g^s \cdot pk^{-h'} \land R_R = h^s \cdot R_L^{-h'}$
return 1

# Intuition of Security Proof for [KLP17]

Adversary against [KLP17]

$pk$ (←)

$R$ (→)

$h$ (←)

$R'$ (→)

$h'$ (←)

$(R, R', h, h', s)$ (→)

$\mathcal{R}$

$x' \leftarrow_\$ \mathbb{Z}_p$
$pk \coloneqq X \cdot g^{x'}$ } KGen

$y_i \leftarrow_\$ \mathbb{Z}_p$
$h \coloneqq Y \cdot g^{y_j}$ } RO $H$

If $\mathsf{V}(pk, R, R', h, h', s) = 1$,
$(g, pk, h, R_L)$ is a DH tuple
$\Rightarrow$ Since $pk = X \cdot g^{x}$, $h = Y \cdot g^{y_j}$,

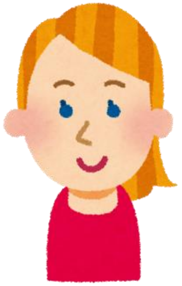
$$R_L = g^{(x+x')(y+y_j)}$$

$\Rightarrow \mathcal{R}$ sets $Z = R_L \cdot X^{-y_j} \cdot Y^{-x'} \cdot g^{-x' y_j}$

CDH instance $x, y \leftarrow_\$ \mathbb{Z}_p$
$X \coloneqq g^x, Y \coloneqq g^y$

Solution $Z$

# Convert 5-round ID into NI Sequential OR-Proof [FGQRW23]

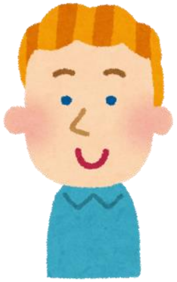


Prover

$\mathrm{IGen}_{\mathrm{OR}}(1^\lambda)$

$b \leftarrow_\$ \{0,1\}$
$(pk_0, sk_0) \leftarrow_\$ IGen(1^\lambda)$
$(pk_1, sk_1) \leftarrow_\$ IGen(1^\lambda)$
Return $\left(pk \coloneqq (pk_0, pk_1), sk \coloneqq (sk_b, b)\right)$

Verifier



$\mathrm{P}_{\mathrm{OR}}(pk, sk)$

$A_b \coloneqq (a_b, a'_b) \leftarrow_\$ \mathbb{G} \times \mathbb{Z}_p$
$Tran_{1-b} \coloneqq Sim(pk_{1-b})$
$a_{1-b} \coloneqq h_{1-b} / H(R_{1-b}, A_b)$
$a'_{1-b} \coloneqq h'_{1-b} - H'(R_{1-b}, R'_{1-b}, A_b)$
$A_{1-b} \coloneqq (a_{1-b}, a'_{1-b})$
$(R_b, st_b) \leftarrow_\$ P_1(sk_b)$
$h_b \coloneqq H(R_b, A_{1-b}) \times a_b$
$(R'_b, st'_b) \leftarrow_\$ P_2(st_b, sk_b, R_b, h_b)$
$h'_b \coloneqq H'(R_b, R'_b, A_{1-b}) + a'_b$
$s_b \leftarrow P_3(st'_b, sk_b, R_b, R'_b, h_b, h'_b)$
Return $s \coloneqq (R_0, R'_0, R_1, R'_1, A_0, A_1, s_0, s_1)$

To convert multi-round IP into OR-proof, offset $a$ is required to computes ID's challenge $h$

$\xrightarrow{\quad s \quad}$

$\mathrm{V}_{\mathrm{OR}}(pk, s)$

$h_0 \coloneqq H(R_0, A_1) \times a_0$
$h'_0 \coloneqq H'(R_0, R'_0, A_1) + a'_0$
$h_1 \coloneqq H(R_1, A_0) \times a_1$
$h'_1 \coloneqq H'(R_1, R'_1, A_0) + a'_1$
$v_0 \leftarrow V_0(pk_0, R_0, R'_0, h_0, h'_0, A_0, s_0)$
$v_1 \leftarrow V_1(pk_1, R_1, R'_1, h_1, h'_1, A_1, s_1)$
Return $(v_0 \wedge v_1)$

# New Signature from [KLP17]+[FGQRW23]

Signer

$\underline{\mathrm{KGen}(1^\lambda)}$

$(pk, sk) \leftarrow_\$ \mathrm{IGen}_{\mathrm{OR}}(1^\lambda)$
Return $(pk, sk)$

Verifier

$\underline{\mathrm{Sign}(pk, sk, m)}$

$A_b \coloneqq (a_b, a'_b) \leftarrow_\$ \mathbb{G} \times \mathbb{Z}_p$
$Tran_{1-b} \coloneqq Sim(pk_{1-b})$
$(R_b, st_b) \leftarrow_\$ P_1(sk_b)$
$a_{1-b} \coloneqq h_{1-b}/H(pk_{1-b}, R_0, R_1, A_b, m)$
$a'_{1-b} \coloneqq h'_{1-b} - H'(pk_{1-b}, R_0, R_1, R'_{1-b}, A_b, m)$
$A_{1-b} \coloneqq (a_{1-b}, a'_{1-b})$
$h_b \coloneqq H(pk_b, R_0, R_1, A_{1-b}, m) \times a_b$
$(R'_b, st'_b) \leftarrow_\$ P_2(st_b, sk_b, R_b, h_b)$
$h'_b \coloneqq H'(pk_b, R_0, R_1, R'_b, A_{1-b}, m) + a'_b$
$s_b \leftarrow P_3(st'_b, sk_b, R_b, R'_b, h_b, h'_b)$
Return $\sigma \coloneqq (R_0, R'_0, R_1, R'_1, A_0, A_1, s_0, s_1)$

$\xrightarrow{\sigma}$

$\underline{\mathrm{Verify}(pk, m, \sigma)}$

$h_0 \coloneqq H(pk_0, R_0, R_1, A_1, m) \times a_0$
$h'_0 \coloneqq H'(pk_0, R_0, R_1, R'_0, A_1, m) + a'_0$
$h_1 \coloneqq H(pk_1, R_0, R_1, A_0, m) \times a_1$
$h'_1 \coloneqq H'(pk_1, R_0, R_1, R'_1, A_0, m) + a'_1$
$v_0 \leftarrow V_0(pk_0, R_0, R'_0, h_0, h'_0, A_0, s_0)$
$v_1 \leftarrow V_1(pk_1, R_1, R'_1, h_1, h'_1, A_1, s_1)$
Return $(v_0 \land v_1)$

# Security Proof for New Signature

- We first take the similar proof approach as [KLP17]

MU-EUF-CMA-C adversary

$(pk_i)_{i\in[N]}$ ←

$\alpha$ →

$\beta$ ←

⋮

$(i^*, m^*, \sigma^*)$ →

$\mathcal{R}$

For $i = 1 \dots N$

$b_i \leftarrow_\$ \{0,1\}$

$(pk_{b_i}, sk_{b_i}) \leftarrow_\$ \mathrm{IGen}(1^\lambda)$

$x_i \leftarrow_\$ \mathbb{Z}_p$

$pk_{1-b_i} \coloneqq X \cdot g^{x_i}$

KGen

$y_i \leftarrow_\$ \mathbb{Z}_p$

$H(\alpha) \coloneqq Y \cdot g^{y_j}$

RO $H$

Simulation of Sig, Corrupt, RO $H'$ are omitted

CDH instance $x, y \leftarrow_\$ \mathbb{Z}_p$

$X \coloneqq g^x, Y \coloneqq g^y$

Solution $Z$

# Can $\mathcal{R}$ Extract CDH Solution from Forgery?

- Forged signature:

$$\sigma^* := \left(R_0^*, {R_0'}^*, R_1^*, {R_1'}^*, A_0^*, A_1^*, s_0^*, s_1^*\right),\ {R'}^*_{1-b} := \left(R^*_{L,1-b}, R^*_{R,1-b}\right)$$

- If $\mathrm{Verify}(pk^*, m^*, \sigma^*) = 1$, following is a DH tuple

$$\left(g, pk^*_{1-b}, h^*_{1-b} = H(\cdot) \times a^*_{1-b} = Yg^{y_j} \times a^*_{1-b}, R^*_{L,1-b}\right)$$

# Can $\mathcal{R}$ Extract CDH Solution from Forgery?

- Forged signature:

$$\sigma^* := \left(R_0^*, R_0'^*, R_1^*, R_1'^*, A_0^*, A_1^*, s_0^*, s_1^*\right),\ R_{1-b}'^* := \left(R_{L,1-b}^*, R_{R,1-b}^*\right)$$

- If $\mathrm{Verify}(pk^*, m^*, \sigma^*) = 1$, following is a DH tuple

$$\left(g, pk_{1-b}^*, h_{1-b}^* = H(\cdot) \times a_{1-b}^* = Yg^{y_j} \times a_{1-b}^*, R_{L,1-b}^*\right)$$

- Therefore,

$$R_{L,1-b}^* = {a_{1-b}^*}^{sk_{1-b}^*} \times Y^x \times \underbrace{X^{y_{j^*}} \times Y^{x_{i^*}} \times g^{x_{i^*}y_{j^*}}}_{\mathcal{R}\text{ can compute them by itself}}$$

$\mathcal{R}$ cannot compute this term since it does not know $sk_{1-b,i^*}$ and DL of $a_{1-b}^*$

**Solution of CDH instance**

**$\mathcal{R}$ cannot solve CDH problem…**

# Our Idea to Allow $\mathcal{R}$ to Solve CDH Instance

- To get $\left(g, pk_{1-b}^{*}, Yg^{y_j}, R_{L,1-b}^{*}\right)$ as DH tuple, $\mathcal{R}$ programs RO $H$ as

$$H(\cdot) = \frac{Yg^{y_j}}{a_{1-b}}$$

← Divide by offset in advance

- Then,

$$R_{L,1-b}^{*} = Y^{x} \times \underbrace{X^{y_{j^*}} \times Y^{x_{i^*}} \times g^{x_{i^*} y_{j^*}}}_{\mathcal{R}\text{ can compute them by itself}}$$

Solution of CDH instance

**$\mathcal{R}$ can solve CDH problem!**

# Our Idea to Allow $\mathcal{R}$ to Solve CDH Instance

- To get $\left(g, pk^*_{1-b}, Yg^{y_j}, R^*_{L,1-b}\right)$ as DH tuple, $\mathcal{R}$ programs RO $H$ as

$$H(\cdot) = \frac{Yg^{y_j}}{a_{1-b}}$$

← Divide by offset in advance

- Then,

$$R^*_{L,1-b} = Y^x \times \underbrace{X^{y_{j^*}} \times Y^{x_{i^*}} \times g^{x_{i^*}y_{j^*}}}_{\mathcal{R}\text{ can compute them by itself}}$$

**Solution of CDH instance**

**$\mathcal{R}$ can solve CDH problem!**

- <u>How $\mathcal{R}$ decides offset $a$ to program $H$?</u>
  ⇒ $\mathcal{A}$ sends $a^*_{1-b}$ to $H$ to generate the forged signature
  ⇒ $\mathcal{A}$ makes $q_H$ queries and $\mathcal{R}$ cannot detect which one is used for $\sigma^*$
  ⇒ **$\mathcal{R}$ chooses $a^*_{1-b}$ from $q_H$ queries, which incurs $q_H$ loss…**

# Summary

# Our Problem and Results

**Can we construct a tightly secure signature scheme in multi-user setting with corruptions based on search assumptions?**

* Open problem mentioned in [PR20,PQR21]

- Reveal new conditions that make tightly secure signatures impossible
  - This leaves room for tightly-secure signatures from search assumptions

    ⇒ Fail to prove impossibility…
- Construct a new signature in multi-user setting with corruptions from CDH
  - Reduction loss is ind. of #users, but depends on #RO query

    ⇒ Fail to prove possibility…

**Problem is still open!**


Full version: ia.cr/2024/1286

# References


- [CP92] D. Chaum and T. P. Pedersen, “Wallet databases with observers CRYPTO 1992.
- [GJ03] E. Goh and S. Jarecki, “A Signature Scheme as Secure as the Diffie-Hellman Problem,” EUROCRYPT 2003.
- [Che05] B. Chevallier-Mames, “An Efficient CDH-Based Signature Scheme with a Tight Security Reduction,” CRYPTO 2005.
- [Bader14] C. Bader, “Efficient signatures with tight real world security in the random-oracle model,” CANS 2014.
- [BHJKL15] C. Bader, D. Hofheinz, T. Jager, E. Kiltz, Y. Li, “Tightly-Secure Authenticated Key Exchange,” TCC 2015.
- [BJLS16] C. Bader, T. Jager, Y. Li, S. Schäge, “On the Impossibility of Tight Cryptographic Reductions,” EUROCRYPT 2016.
- [KLP17] E. Kiltz, J. Loss, J. Pan, “Tightly-Secure Signatures from Five-Move Identification Protocols,” ASIACRYPT 2017.
- [GJ18] K. Gjøsteen and T. Jager, “Practical and Tightly-Secure Digital Signatures and Authenticated Key Exchange,” CRYPTO 2018.
- [WLGSZ19] G. Wu, J. Lai, F. Guo, W. Susilo, F. Zhang, “Tightly Secure Public-Key Cryptographic Scheme from One-More Assumption.” Journal of Computer Science and Technology, 2019.
- [FHJ20] M. Fischlin, P. Harasser, C. Janson, “Signatures from Sequential-OR Proofs,” EUROCRYPT 2020,
- [PR20] J. Pan and M. Ringerud, “Signatures with Tight Multi-User Security from Search Assumptions,” ESORICS 2020.
- [DGJL21] D. Diemert, K. Gellert, T. Jager, L. Lyu, “More Efficient Digital Signatures with Tight Multi-User Security,” PKC 2021.
- [PQR21]J. Pan, C. Qian, and M. Ringerud, “Signed (Group) Diffie-Hellman Key Exchange with Tight Security,” CT-RSA 2021.
- [PW22] J. Pan and B. Wagner, “Lattice-Based Signatures with Tight Adaptive Corruptions and More,” PKC 2022.
- [FGQRW23], P.-A. Fouque, Adela Georgescu, Chen Qian, Adeline Roux-Langlois, Weiqiang Wen, “A Generic Transform from Multi-round Interactive Proof to NIZK,” PKC 2023.