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

Hirofumi Yoshioka[1], Wakaha Ogata[1], and Keitaro Hashimoto†[2]

[1]Tokyo Institute of Technology
fumisket@gmail.com, ogata.w.aa@m.titech.ac.jp
[2]National Institute of Advanced Industrial Science and Technology (AIST)
keitaro.hashimoto@aist.go.jp

1 Introduction

This paper is a report on how we tackled constructing a digital signature scheme whose *multi-user security with corruption* can be *tightly* reduced to *search assumptions*. First, We reveal two new properties of signature schemes whose security cannot be tightly reduced to standard assumptions. More precisely, we generalize the negative result of Pan and Wagner [11], which shows that the reduction loss of the concrete signature scheme, called the Parallel-OR signature scheme, is lower bounded by the number of users. From this negative result, we have precious knowledge about designing a signature scheme that is tightly secure in multi-user settings with corruption. Next, we show a concrete construction of signature schemes based on the first result. Our scheme's multi-user security can be reduced to the CDH assumption, and the reduction loss does not depend on the number of users, but, unfortunately, the loss linearly depends on the number of random oracle queries issued by the adversary. So, it remains open whether we can construct a signature scheme whose multi-user security with corruption can be tightly reduced to search assumptions.

2 Preliminaries

Notations. Let $\lambda \in \mathbb{N}$ be a security parameter. For natural number N, let $[N] := \{1, 2, \ldots, N\}$. For an algorithm X and its input x, let $\mathsf{X}(x)$ be the set of all output. For random variables X and Y, $\mathsf{SD}(X; Y)$ denotes the statistical distance between them.

*The authors thank the anonymous reviewers of CFAIL 2024 for their constructive comments and suggestions.

†Partially supported by JST CREST JPMJCR22M1, Japan.

Computational assumption. Let $\mathbb{G}$ be a multiplicative group with prime order p and $g \in \mathbb{G}$ be its generator. We say that the computational Diffie-Hellman (CDH) assumption holds in $\mathbb{G}$ if for any ppt adversary, the advantage defined by the following is negligibly small.

$$\mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{A}}(\lambda) := \Pr[Z = g^{xy} : x, y \leftarrow\!\!\$\ \mathbb{Z}_p; Z \leftarrow \mathcal{A}(g, g^x, g^y)].$$

Digital signature. A digital signature scheme $\mathsf{SIG} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ is defined as follows.

- $\mathsf{Setup}(1^\lambda)$, taking the security parameter λ as an input, generates a system parameter par, which describes spaces of public keys K_p, secret keys K_s, messages M and signatures S. We may omit par as input in the following algorithms.
- $\mathsf{Gen}(\mathsf{par})$ generates a pair of a public key and a secret key $(\mathsf{pk}, \mathsf{sk}) \in K_p \times K_s$.
- $\mathsf{Sig}(\mathsf{sk}, \mathsf{m})$, taking a secret key sk and message $\mathsf{m} \in M$, computes a signature $\sigma \in S$.
- $\mathsf{Ver}(\mathsf{pk}, \mathsf{m}, \sigma)$, taking a public key pk, message m, and a signature σ, outputs a bit $b \in \{0, 1\}$.

A signature scheme is said to be correct[1] if for any $\lambda \in \mathbb{N}$, $\mathsf{par} \in \mathsf{Setup}(1^\lambda)$, $(\mathsf{pk}, \mathsf{sk}) \in \mathsf{Gen}(\mathsf{par})$, $\mathsf{m} \in M$, and $\sigma \in \mathsf{Sig}(\mathsf{sk}, \mathsf{m})$, $\mathsf{Ver}(\mathsf{pk}, \mathsf{m}, \sigma)$ always outputs 1.

For a public key pk, we define the following set:

$$SK(\mathsf{pk}) := \{\mathsf{sk} \mid (\mathsf{pk}, \mathsf{sk}) \in \mathsf{Gen}(\mathsf{par})\}.$$

Multi-user security with adaptive corruption of signature schemes is defined as follows.

[1]In this paper, we only consider the perfect correctness.

Algorithm 1 N-MU-UF-CMA-C$^{\mathcal{A}}_{\mathsf{SIG}}(\lambda)$

$\mathsf{par} \leftarrow \mathsf{Setup}(1^\lambda)$
for $i \in [N]$ **do** $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{par})$
$(i^*, \mathsf{m}^*, \sigma^*) \leftarrow \mathcal{A}^{\mathtt{Corr},\mathtt{Sig}}(\mathsf{par}, (\mathsf{pk}_i)_{i\in[N]})$
if $i^* \in \mathcal{L}_{id}$ **then return** 0
if $\exists \sigma : (i^*, \mathsf{m}^*, \sigma) \in \mathcal{L}_m$ **then return** 0
return $\mathsf{Ver}(\mathsf{pk}_{i^*}, \mathsf{m}^*, \sigma^*)$
Oracle $\mathtt{Corr}(i)$
$\mathcal{L}_{id} := \mathcal{L}_{id} \cup \{i\}$
return sk_i
Oracle $\mathtt{Sig}(i, \mathsf{m})$
$\sigma \leftarrow \mathsf{Sig}(\mathsf{sk}_i, \mathsf{m})$
$\mathcal{L}_m := \mathcal{L}_m \cup \{(i, \mathsf{m}, \sigma)\}$
return σ

Algorithm 2 N-MU-UF-S$^{\mathcal{A}}_{\mathsf{SIG}}(\lambda)$

$\mathsf{par} \leftarrow \mathsf{Setup}(1^\lambda)$
for $i \in [N]$ **do** $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{par})$
$(j, St_{\mathcal{A}}) \leftarrow \mathcal{A}_1(\mathsf{par}, (\mathsf{pk}_i)_{i\in[N]})$
if $j \notin [N]$ **then return** 0
$(\mathsf{m}^*, \sigma^*) \leftarrow \mathcal{A}_2(St_{\mathcal{A}}, (\mathsf{sk}_i)_{i\in[N]\setminus\{j\}})$
return $\mathsf{Ver}(\mathsf{pk}_j, \mathsf{m}^*, \sigma^*)$

Definition 1 (Multi-user security [11]). *For a signature scheme* SIG*, consider a game* N-**MU-UF-CMA-C** *shown in Algorithm 1. We say* SIG *has* N-MU-UF-CMA-C *security if for any ppt adversary* $\mathcal{A}$*, the advantage*

$$\mathsf{Adv}^{N\text{-MU-UF-CMA-C}}_{\mathcal{A},\mathsf{SIG}}(\lambda) := \Pr[N\text{-}\mathbf{MU\text{-}UF\text{-}CMA\text{-}C}^{\mathcal{A}}_{\mathsf{SIG}}(\lambda) \Rightarrow 1]$$

in negligibly small.

As in [11], we introduce the following weaker security notion, multi-user security with *static* corruption *without signing oracle*. We note that impossibility results in the weaker security notion imply that in the stronger notion.

Definition 2 (Static security [11]). *For signature scheme* SIG*, consider a game* N-**MU-UF-S** *shown in Algorithm 2. If for any ppt adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage*

$$\mathsf{Adv}^{N\text{-MU-UF-S}}_{\mathcal{A},\mathsf{SIG}}(\lambda) := \Pr[N\text{-}\mathbf{MU\text{-}UF\text{-}S}^{\mathcal{A}}_{\mathsf{SIG}}(\lambda) \Rightarrow 1]$$

in negligibly small, we say SIG *has* N-MU-UF-S *security.*

Definition 3 (Key-pair Verifiability). *If there exists a ppt algorithm* VerK *such that the next equation holds for any* $\lambda \in \mathbb{N}$*,* $\mathsf{par} \in \mathsf{Setup}(1^\lambda)$*,* $\mathsf{pk} \in K_p$*, and* $\mathsf{sk} \in K_s$*, then* SIG *is said to be key-pair verifiable.*

$$\mathsf{VerK}(\mathsf{par}, \mathsf{pk}, \mathsf{sk}) = 1 \iff (\mathsf{pk}, \mathsf{sk}) \in \mathsf{Gen}(\mathsf{par})$$

Algorithm 3 $\mathbf{NIP}^{\mathsf{X}}_{\mathsf{NIP}}(\lambda)$ $\quad (\mathsf{X} \in \{\mathcal{A}, \mathsf{U}\})$

$(c, w) \leftarrow \mathsf{T}(1^\lambda)$
$s \leftarrow \mathsf{X}(c)$
return $\mathsf{V}(c, w, s)$

If $\mathsf{VerK}(\mathsf{par}, \mathsf{pk}, \mathsf{sk}) = 1$*,* sk *is a valid secret key of* pk.

Hereafter, we assume any signature scheme has key-pair verifiability, since we can verify the validity of a given pair $(\mathsf{pk}, \mathsf{sk})$ by repeating the procedure of computing a signature of a random message using sk and verifying it using pk enough number of times.

Non-interactive problems (NIP) and simple reductions. Existing impossibility results [3, 11] are for *simple* reductions that reduce the security of signature schemes to *non-interactive problems*. *Non-interactive problems* (NIP) is a wide class of mathematical problems such that, given an instance of the problem, the solver needs to output an answer without accessing any oracles. This class includes both decision problems such as DDH and search problems such as DLP and CDH.[2]

Definition 4 (Non-interactive problem [3, 11]). *Non-interactive problem is formalized as a tuple of algorithms* $\mathsf{NIP} = (\mathsf{T}, \mathsf{U}, \mathsf{V})$*.*

- $\mathsf{T}(1^\lambda)$*, taking the security parameter* λ *as an input, outputs an instance* c *and its witness* w*.*
- $\mathsf{U}(c)$ *takes an instance* c *as input, and outputs a candidate of solutions* s*.*
- $\mathsf{V}(c, w, s)$ *takes* c, w, s *as input, and outputs a bit.*

Consider the game **NIP** *depicted in Algorithm 3. For an algorithm* $\mathcal{A}$*, its advantage is defined as*

$$\mathsf{Adv}^{\mathsf{NIP}}_{\mathcal{A}}(\lambda) := \left|\Pr[\mathbf{NIP}^{\mathcal{A}}_{\mathsf{NIP}}(\lambda) \Rightarrow 1] - \Pr[\mathbf{NIP}^{\mathsf{U}}_{\mathsf{NIP}}(\lambda) \Rightarrow 1]\right|.$$

If the advantage is negligibly small for any ppt algorithms $\mathcal{A}$*, we say* NIP *is hard.*

Roughly speaking, a *simple* reduction is a reduction that has black-box access to the adversary algorithm $\mathcal{A}$ only once and without rewinding. In this paper, we only deal with simple reductions that reduce the N-MU-UF-S security of signature schemes to an NIP.

[2] NIP includes both decision problems and search problems, but not one-more type problems, since the solver is given an oracle.

Algorithm 4 $\mathcal{R}^{\mathcal{A}}(c)$

$(St_{\mathcal{R}}, \mathsf{par}, (\mathsf{pk}_i)_{i\in[N]}) \leftarrow \mathcal{R}_1(c)$
$(j, St_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathsf{H}}(\mathsf{par}, (\mathsf{pk}_i)_{i\in[N]})$
$(St_{\mathcal{R}}, (\mathsf{sk}_i)_{i\in[N]\setminus\{j\}}) \leftarrow \mathcal{R}_2(St_{\mathcal{R}}, j)$
$(\mathsf{m}^*, \sigma^*) \leftarrow \mathcal{A}_2^{\mathsf{H}}(St_{\mathcal{A}}, (\mathsf{sk}_i)_{i\in[N]\setminus\{j\}})$
return $\mathcal{R}_3(St_{\mathcal{R}}, j, \mathsf{m}^*, \sigma^*)$
Oracle $\mathsf{H}(\mathsf{query})$
$(St_{\mathcal{R}}, h) \leftarrow \mathcal{R}_{\mathrm{RO}}(St_{\mathcal{R}}, \mathsf{query})$
return h

Definition 5 (Simple reduction [11]). *A simple* (NIP, SIG)*-reduction* $\mathcal{R} = (\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_{\mathrm{RO}})$ *is a tuple of algorithms to solve* NIP*, having a black-box access to* $\mathcal{A}$ *only once, where* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *is an adversary against* SIG*'s* N-MU-UF-S *security. Without loss of generality, we assume that only* $\mathcal{R}_1$ *is a probabilistic algorithm, and* $\mathcal{R}_2$, $\mathcal{R}_3$, $\mathcal{R}_{\mathrm{RO}}$ *are deterministic.*

- $\mathcal{R}_1(c)$ *receives an instance* c *of* NIP*, and outputs own state information* $St_{\mathcal{R}}$*, parameters* par *of the signature scheme, and a list of public keys* $(\mathsf{pk}_i)_{i\in[N]}$.
- $\mathcal{R}_2(St_{\mathcal{R}}, j)$ *receives an index* $j \in [N]$ *from* $\mathcal{A}$ *addition to the current state* $St_{\mathcal{R}}$*, and outputs a new state* $St_{\mathcal{R}}$ *and a list of secret keys* $(\mathsf{sk}_i)_{i\in[N]\setminus\{j\}}$.
- $\mathcal{R}_3(St_{\mathcal{R}}, j, \mathsf{m}^*, \sigma^*)$ *receives* $j \in [N]$, m^*, σ^* *from* $\mathcal{A}$ *as well as the current state. It outputs a solution* s *of the instance* c *of* NIP.
- $\mathcal{R}_{\mathrm{RO}}(St_{\mathcal{R}}, \mathsf{query})$ *receives* query *and the current state. It outputs a new state* $St_{\mathcal{R}}$ *and a hash value* h.

Algorithm 4 shows the interaction between $\mathcal{R}$ *and* $\mathcal{A}$*. Let* $V_{\mathcal{R}}$ *and* V_{real} *be random variables representing* $\mathcal{A}$*'s view interacting with* $\mathcal{R}$ *and that interacting with the challenger in* N-**MU-UF-S** *game, respectively. For a function* L*, we say that* $\mathcal{R}$ *is* $(N, \delta_{\mathcal{R}}, L)$*-simple if*

$$\mathsf{SD}(V_{\mathcal{R}}; V_{real}) \leq \delta_{\mathcal{R}},$$
$$\mathsf{Adv}^{\mathsf{NIP}}_{\mathcal{R}^{\mathcal{A}}}(\lambda) \geq L(\lambda, N, \mathsf{Adv}^{N\text{-MU-UF-S}}_{\mathcal{A},\mathsf{SIG}}(\lambda))$$

holds for any ppt adversary $\mathcal{A}$.

3 New Impossibility Result

First, we introduce two new properties of digital signature schemes SIG.

Definition 6 (Signature statistically close). *Let* $SIG(\mathsf{sk}, \mathsf{m})$ *be a random variable representing the output of* $\mathsf{Sig}(\mathsf{sk}, \mathsf{m})$. SIG *is said to be* $\varepsilon_{\mathsf{Sig}}$*-signature statistically close if for any* $\mathsf{m} \in M$*,* $\mathsf{pk} \in K_p$ *and two valid secret keys* $\mathsf{sk}, \mathsf{sk}' \in SK(\mathsf{pk})$*, it holds that*

$$\mathsf{SD}(SIG(\mathsf{sk}, \mathsf{m}); SIG(\mathsf{sk}', \mathsf{m})) \leq \varepsilon_{\mathsf{Sig}}.$$

Definition 7 (RO statistically close). *Let* $Q(\mathsf{sk}, \mathsf{m})$ *be a random variable representing the random oracle queries issued in the run of* $\mathsf{Sig}^{\mathsf{H}}(\mathsf{sk}, \mathsf{m})$. SIG *is said to be* $\varepsilon_{\mathrm{RO}}$-RO *statistically close if for any* $\mathsf{m} \in M$*,* $\mathsf{pk} \in K_p$ *and two valid secret keys* $\mathsf{sk}, \mathsf{sk}' \in SK(\mathsf{pk})$*, it holds that*

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

By using the above properties, we obtain the following impossibility result. Due to page limitations, we omit the full proof.

Theorem 1. *Let* SIG *be a* $\varepsilon_{\mathsf{Sig}}$*-signature statistically close and* $\varepsilon_{\mathrm{RO}}$-RO *statistically close signature scheme. For any* $(N, \delta_{\mathcal{R}}, L)$*-simple* (NIP, SIG)*-reduction* $\mathcal{R}$*, there exists an algorithm* $\mathcal{M}$ *that solves* NIP *such that*

$$\mathsf{Adv}^{\mathsf{NIP}}_{\mathcal{M}}(\lambda) \geq L(\lambda, N, 1) - (2\delta_{\mathcal{R}} + \varepsilon_{\mathsf{Sig}} + \varepsilon_{\mathrm{RO}}) - 1/N,$$
$$\mathbf{T}(\mathcal{M}) \leq N \cdot \mathbf{T}(\mathcal{R}) + N(N-1)\mathbf{T}(\mathsf{VerK}) + \mathbf{T}(\mathsf{Sig}),$$

where $\mathbf{T}(X)$ *denotes the running time of* X.

Proof overview. The proof proceeds similarly to the proof of the existing impossibility results [6, 11]. We construct a meta-reduction that interacts with a reduction $\mathcal{R}$ by simulating a hypothetical adversary who breaks the scheme with overwhelming probability. Our proof differs from the existing ones in arguing the indistinguishability of the simulated adversary from the real adversary. The existing works used the key-randomizability ([6]) or the property of the specific construction ([11]) to argue it. Instead, we use signature statistical closeness and RO statistical closeness for this purpose. □

From Theorem 1, the reduction loss from the multi-user security to an NIP is lower bounded by the number of users N, if $\varepsilon_{\mathsf{Sig}}, \varepsilon_{\mathrm{RO}}, \delta_{\mathcal{R}}$ are negligibly small.[3]

Discussion. Theorem 1 implies that to achieve tight security, at least one of the following conditions should be hold.

(C1) SIG's security is based on interactive problems,

(C2) SIG is not signature statistically close, ($\varepsilon_{\mathsf{Sig}} \neq \mathsf{negl}$)

(C3) SIG is not RO statistically close, ($\varepsilon_{\mathrm{RO}} \neq \mathsf{negl}$)

[3] Theorem 1 can be generalized for r-simple reduction that is allowed to rewind $\mathcal{A}$ r times sequentially. The lower bound is preserved for generalized reductions.

Table 1: Conditions existing tightly secure schemes satisfy to avoid the impossibility results.

Scheme	(C1) not NIP	(C2) $\varepsilon_{\mathsf{Sig}} \neq \mathsf{negl}$	(C3) $\varepsilon_{\mathrm{RO}} \neq \mathsf{negl}$	(C4) $\delta_{\mathcal{R}} \neq \mathsf{negl}$
[12]	✓	-	-	-
[9]	-	✓	-	-
[4, 5, 1]	-	-	-	✓
[7, 2]	-	-	✓	✓
Ours	-	-	✓	-

(C4) The adversary's view given by a reduction $\mathcal{R}$ is statistically distinguishable from that in the real N-**MU-UF-S** ($\delta_{\mathcal{R}} \neq \mathsf{negl}$).

Table 1 summarizes which conditions existing tightly-secure signature schemes satisfy. Further,

- we do not want to rely on the hardness of interactive problems (unlike [12]),
- $\mathsf{Sig}(\mathsf{sk}, \mathsf{m})$ and $\mathsf{Sig}(\mathsf{sk}', \mathsf{m})$ should be indistinguishable. If they are not statistically close, they should be computationally indistinguishable, meaning that a decisional assumption is needed (as in [9]), and
- the adversary's view given by a reduction should be distinguishable from that in the real game. If they are not statistically close, they should be computationally indistinguishable, meaning that a decisional assumption is needed (as in [4, 5, 1, 7, 2]).

From the above considerations, we take the approach that makes $Q(\mathsf{sk}, \mathsf{m})$ and $Q(\mathsf{sk}', \mathsf{m})$ distinguishable, shown in the last row in Table 1.

4 New Construction

We provide our (failed) approach to construct the desired signature scheme. Our idea is the combination of the CDH-based 5-move identification scheme [10] and the sequential-OR technique for multi-round interactive proofs, proposed in [8]. The construction is as follows.

- $\mathsf{Setup}(1^\lambda)$: Output the description of a multiplicative group $\mathbb{G}$, its order p, its generator g, and the description of hash functions $\mathsf{H} : \{0,1\}^* \to \mathbb{G}$ and $\mathsf{H}' : \{0,1\}^* \to \mathbb{Z}_p$ as par.
- $\mathsf{Gen}(\mathsf{par})$: Sample $\mathsf{sk}_0, \mathsf{sk}_1 \leftarrow\!\$\ \mathbb{Z}_p$, $b \leftarrow\!\$\ \{0,1\}$ and compute $\mathsf{pk}_0 = g^{\mathsf{sk}_0}, \mathsf{pk}_1 = g^{\mathsf{sk}_1}$. Output $\mathsf{sk} := (\mathsf{sk}_b, b), \mathsf{pk} := (\mathsf{pk}_0, \mathsf{pk}_1)$.
- $\mathsf{Sig}(\mathsf{sk}, \mathsf{m})$: Simulate a transcript of the 5-move ID protocol for pk_{1-b} with its simulation algorithm Sim:

$$(R_{1-b}, h_{1-b}, R'_{1-b}, h'_{1-b}, s_{1-b}) \leftarrow \mathsf{Sim}(\mathsf{pk}_{1-b})$$

Then, compute a real transcript of the 5-move ID protocol for pk_b with its prover algorithm $P = (P_1, P_2, P_3)$:

$$\begin{aligned}
A_b &:= (a_b, a'_b) \leftarrow\!\$\ \mathbb{G} \times \mathbb{Z}_p, \\
(R_b, r) &\leftarrow P_1(\mathsf{sk}_b) = g^r \quad (r \leftarrow\!\$\ \mathbb{Z}_p) \\
a_{1-b} &:= h_{1-b}/\mathsf{H}(\mathsf{pk}_{1-b}, R_0, R_1, A_b, \mathsf{m}) \\
a'_{1-b} &:= h'_{1-b} - \mathsf{H}'(\mathsf{pk}_{1-b}, R_0, R_1, R'_{1-b}, A_b, \mathsf{m}) \\
A_{1-b} &:= (a_{1-b}, a'_{1-b}) \\
h_b &:= \mathsf{H}(\mathsf{pk}_b, R_0, R_1, A_{1-b}, \mathsf{m}) \times a_b \\
R'_b &\leftarrow P_2(\mathsf{sk}_b, R_b, h_b, r) = (R_{Lb} := h_b^{\mathsf{sk}_b}, R_{Rb} := h_b^r) \\
h'_b &:= \mathsf{H}'(\mathsf{pk}_b, R_0, R_1, R'_b, A_{1-b}, \mathsf{m}) + a'_b \\
s_b &\leftarrow P_3(\mathsf{sk}_b, R_b, h_b, R'_b, h'_b, r) = \mathsf{sk}_b \cdot h'_b + r.
\end{aligned}$$

Output $\sigma := (R_0, R'_0, R_1, R'_1, A_0, A_1, s_0, s_1)$.

- $\mathsf{Ver}(\mathsf{pk}, \mathsf{m}, \sigma = (R_0, R'_0, R_1, R'_1, A_0, A_1, s_0, s_1))$: Parse $A_0 = (a_0, a'_0), A_1 = (a_1, a'_1)$. For each $b \in \{0,1\}$, compute

$$\begin{aligned}
h_b &:= \mathsf{H}(\mathsf{pk}_b, R_0, R_1, A_{1-b}, \mathsf{m}) \times a_b, \\
h'_b &:= \mathsf{H}'(\mathsf{pk}_b, R_0, R_1, R'_b, A_{1-b}, \mathsf{m}) + a'_b, \\
v_b &\leftarrow V(\mathsf{pk}_b, R_b, R'_b, h_b, h'_b, s_b) \\
&= [R_b = g^{s_b} \mathsf{pk}_b^{-h'_b} \wedge R_{Rb} = h_b^{s_b} R_{Lb}^{-h'_b}].
\end{aligned}$$

If $v_0 = v_1 = 1$, output 1; otherwise, output 0.

The correctness of the scheme follows from the correctness of the identification scheme and the OR-proof technique. We now show its security.

Theorem 2. *Under the CDH assumption, the above scheme has N-MU-UF-CMA-C security with the reduction loss of $O(q_H)$ in the random oracle model, where q_H is the number of H queries made by $\mathcal{A}$.*

Proof. Let $(i^*, \sigma^* = (R_0^*, R'^*_0, R_1^*, R'^*_1, A_0^*, A_1^*, s_0^*, s_1^*), \mathsf{m}^*)$ be $\mathcal{A}$'s final output, and let $b^* = b_{i^*}$,

$$\begin{aligned}
H_b &= \mathsf{H}(\mathsf{pk}_{i^*,b}, R_0^*, R_1^*, A_{1-b}^*, \mathsf{m}^*), \\
H'_b &= \mathsf{H}'(\mathsf{pk}_{i^*,b}, R_0^*, R_1^*, R'^*_b, A_{1-b}^*, \mathsf{m}^*)
\end{aligned}$$

for $b \in \{0,1\}$. Consider the following games, and let $\epsilon_i := \Pr[\text{Game } i \text{ outputs } 1]$.

Game 0: It is the same as N-$\mathbf{MU\text{-}UF\text{-}CMA\text{-}C}^{\mathcal{A}}_{\mathsf{SIG}}(\lambda)$.

$$\epsilon_0 = \mathsf{Adv}^{N\text{-MU-UF-CMA-C}}_{\mathcal{A},\mathsf{SIG}}(\lambda).$$

Game 1: After $\mathcal{A}$ outputs the final output, 0 is output if H_{b^*} was queried before H_{1-b^*}. Since $\mathcal{A}$ has no information about b^*, we have $\epsilon_1 = \epsilon_0/2$.

Game 2: After $\mathcal{A}$ outputs the final output, 0 is output if H'_{b^*} was queried before H_{b^*}. By using the power of random oracles, we can show that σ^* is rejected with probability $1 - 1/p$ if H'_{b^*} was queried before H_{b^*}. Thus,

$$|\epsilon_2 - \epsilon_1| = 1/p.$$

We next upper bound ϵ_2. To do so, we construct a reduction $\mathcal{R}$ from Game 2 to the CDH problem.

Let $X = g^x, Y = g^y$ be an instance of the CDH problem. For each $i \in [N]$, $\mathcal{R}$ chooses $b_i \leftarrow\!\$\ \{0,1\}$, generates $(\mathsf{pk}_{i,1-b_i}, \mathsf{sk}_{i,1-b_i})$ normally, and sets $\mathsf{pk}_{i,b_i} := Xg^{x_i}$ ($x_i \leftarrow\!\$\ \mathbb{Z}_p$), $\mathsf{pk}_i := (\mathsf{pk}_{i,0}, \mathsf{pk}_{i,1})$. Then, $\mathcal{R}$ runs $\mathcal{A}$ on input $\{\mathsf{pk}_i\}_{i\in[N]}$ and answers oracle queries as follows:

- $\mathsf{H}'(\mathsf{pk}, R_0, R_1, R', A, \mathsf{m})$ query: $\mathcal{R}$ returns randomly chosen $h' \leftarrow\!\$\ \mathbb{Z}_p$. Note that if the same input has been queried, the consistent value is returned.
- $\mathsf{H}(\mathsf{pk}, R_0, R_1, a, a', \mathsf{m})$ query: if $\mathsf{pk} = \mathsf{pk}_{i,b_i}$, $\mathcal{R}$ returns $H \leftarrow\!\$\ \mathbb{G}$ and adds $(\mathsf{pk}_{i,b_i}, R_0, R_1, a, a', \mathsf{m})$ to L_1. If $\mathsf{pk} = \mathsf{pk}_{i,1-b_i}$ and there exists $(\mathsf{pk}_{i,b_i}, R_0, R_1, a_{1-b_i}, a'_{1-b_i}, \mathsf{m}) \in L_1$ for some (a_{1-b_i}, a'_{1-b_i}) (if there are multiple a_{1-b_i}, choose one randomly), then $\mathcal{R}$ chooses $y_j \leftarrow\!\$\ \mathbb{Z}_p$ and returns Yg^{y_j}/a_{1-b_i}. Add $(\mathsf{pk}_{i,1-b_i}, R_0, R_1, a, a', \mathsf{m}, y_j)$ to L_2. Otherwise, returns $H \leftarrow\!\$\ \mathbb{G}$.
- $\mathtt{Corr}(i)$ query: $\mathcal{R}$ returns $\mathsf{sk}_{i,1-b_i}$.
- $\mathtt{Sig}(i, \mathsf{m})$ query: $\mathcal{R}$ generates a signature by using $\mathsf{sk}_{i,1-b_i}$, and returns the signature.

Finally, $\mathcal{A}$ outputs $(i^*, \mathsf{m}^*, \sigma^*)$. If H_{b^*} was queried before H_{1-b^*}, H'_{b^*} was queried before H_{b^*}, or $\mathsf{Ver}(\mathsf{pk}_{i^*}, \mathsf{m}^*, \sigma^*) = 0$, $\mathcal{R}$ outputs randomly chosen element $Z \leftarrow\!\$\ \mathbb{G}$.

Now we can assume that $H_{1-b^*}, H_{b^*}, H'_{b^*}$ were queried in this order, and $\mathsf{Ver}(\mathsf{pk}_{i^*}, \mathsf{m}^*, \sigma^*) = 1$. In this case, $(\mathsf{pk}_{i^*,1-b^*}, R^*_0, R^*_1, a^*_{b^*}, a'^*_{b^*}, \mathsf{m}^*) \in L_1$.

Suppose that there is only one entry $(\mathsf{pk}_{i^*,1-b^*}, R^*_0, R^*_1, a, a', \mathsf{m}^*)$ in L_1. In this case, $H_{b^*} = Yg^{y_j}/a^*_{b^*}$ holds and there exists $(\mathsf{pk}_{i^*,b^*}, R^*_0, R^*_1, a^*_{1-b^*}, a'^*_{1-b^*}, \mathsf{m}^*, y_j)$ in L_2. Thus, $\mathcal{R}$ outputs

$$Z := R^*_{Lb^*}/X^{y_j}Y^{x_{i^*}}g^{x_{i^*}y_j}.$$

Now define $\tilde{y}$ as

$$h_{b^*} := H_{b^*} \times a^*_{b^*} = Yg^{y_j} = g^{\tilde{y}}.$$

From the property of the random oracle, we can show that σ^* is rejected with probability $1 - 1/p$ if

$$R^*_{b^*} = \mathsf{pk}^{\tilde{y}}_{i^*,b^*} \tag{1}$$

does not hold.

If Equation (1) holds, the $\mathcal{R}$'s output satisfies

$$Z = \frac{(Xg^{x_{i^*}})^{\tilde{y}}}{X^{y_j}Y^{x_{i^*}}g^{x_{i^*}y_j}} = \frac{g^{(x+x_{i^*})(y+y_j)}}{X^{y_j}Y^{x_{i^*}}g^{x_{i^*}y_j}} = g^{xy}.$$

Therefore,

$$\begin{aligned}\mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{R}}(\lambda) &= \Pr[\text{Eq. (1) holds}] \\ &\geq \Pr[\text{Eq. (1) holds} \wedge \sigma^* \text{ is accepted in Game 2}] \\ &\geq \Pr[\sigma^* \text{ is accepted in Game 2}] - 1/p, \\ \therefore \epsilon_2 &\leq \mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{R}}(\lambda) + 1/p.\end{aligned}$$

Consequently, we have

$$\mathsf{Adv}^{N\text{-MU-UF-CMA-C}}_{\mathcal{A},\mathsf{SIG}}(\lambda) \leq 2(\mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{R}}(\lambda) + 2/p).$$

If there are q_H entries in L_1: In this case, we have to estimate the success probability as

$$\mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{R}}(\lambda) = \frac{1}{q_H}\Pr[\text{Eq. (1) holds}].$$

Thus we have

$$\mathsf{Adv}^{N\text{-MU-UF-CMA-C}}_{\mathcal{A},\mathsf{SIG}}(\lambda) \leq 2(q_H\mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{R}}(\lambda) + 2/p).$$

□

5 Conclusion

In this work, we tried to construct a signature scheme whose *multi-user security with corruption* can be *tightly* reduced to *search assumptions*. We first revealed the new conditions that the highest secure signature schemes must satisfy. This result suggests that constructions based on the OR-proof are promising. Second, by combining the 5-move CDH-based identification scheme [10] and the OR-Proof technique for multi-round interactive protocols [8], we constructed a new signature scheme. As a result, we made the reduction loss from its multi-user security with corruption to the CDH assumption independent of the number of users. However, this approach failed as its loss depended on the number of queries to the RO. The existence of the highest secure signature schemes remains still open.

References

[1] M. Abdalla, F. Benhamouda, and D. Pointcheval. On the tightness of forward-secure signature reductions. *Journal of Cryptology*.

[2] M. Abe, M. Ambrona, A. Bogdanov, M. Ohkubo, and A. Rosen. Non-interactive composition of sigma-protocols via share-then-hash. *ASIACRYPT 2020, Part III*, 2020.

[3] M. Abe, J. Groth, and M. Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. *ASIACRYPT 2011*, 2011.

[4] C. Bader. Efficient signatures with tight real world security in the random-oracle model. *CANS 14*, 2014.

[5] C. Bader, D. Hofheinz, T. Jager, E. Kiltz, and Y. Li. Tightly-secure authenticated key exchange. *TCC 2015, Part I*, 2015.

[6] C. Bader, T. Jager, Y. Li, and S. Schäge. On the impossibility of tight cryptographic reductions. *EUROCRYPT 2016, Part II*, 2016.

[7] D. Diemert, K. Gellert, T. Jager, and L. Lyu. More efficient digital signatures with tight multi-user security. *PKC 2021, Part II*, 2021.

[8] P.-A. Fouque, A. Georgescu, C. Qian, A. Roux-Langlois, and W. Wen. A generic transform from multi-round interactive proof to NIZK. *PKC 2023, Part II*, 2023.

[9] K. Gjøsteen and T. Jager. Practical and tightly-secure digital signatures and authenticated key exchange. *CRYPTO 2018, Part II*, 2018.

[10] E. Kiltz, J. Loss, and J. Pan. Tightly-secure signatures from five-move identification protocols. *ASIACRYPT 2017, Part III*, 2017.

[11] J. Pan and B. Wagner. Lattice-based signatures with tight adaptive corruptions and more. *PKC 2022, Part II*, 2022.

[12] G. Wu, J.-C. Lai, F.-C. Guo, W. Susilo, and F.-T. Zhang. Tightly secure public-key cryptographic schemes from one-more assumptions. *Journal of Computer Science and Technology*.