Strongly Unforgeable ID-based Signatures Without Random Oracles

Chifumi Sato, Takeshi Okamoto and Eiji Okamoto

Abstract. There is an open problem to construct ID-based signature schemes which satisfy strongly EUF-ID-CMA, without random oracles. It is known that strongly EUF-ID-CMA is a concept of the strongest security in ID-based signatures. In this paper, we propose a solution to the open problem, that is an ID-based signature scheme, which satisfies strongly EUF-ID-CMA, without random oracles for the first time. Security of the scheme is based on the difficulty to solve three problems related to the Diffie–Hellman problem and a one-way isomorphism.

Keywords. Digital signatures, ID-based signatures, Strongly EUF-ID-CMA, Standard models.

1. Introduction

In 1984, Shamir [17] introduced the concept of ID-based cryptosystem, in which the private key of an entity was generated from his identity information (e.g. an e-mail address, a telephone number, etc.) and a master key of a trusted third party called a Private Key Generator (PKG). The advantage of this cryptosystem is that certificates as used in a traditional public key infrastructure can be eliminated.

The first ID-based signature (IBS) scheme was proposed by Shamir [17]. Later, many IBS schemes were presented in [14, 12, 11, 7]. However, security of these schemes need for the assumption that hash functions are random oracles. Since commonly used hash functions such as MD-5 or SHA-1 are not random oracles, constructing schemes whose security can be proved without random oracles is one of the most important themes of study for signatures [10, 8, 2, 6, 19, 18, 5] or ID-based encryptions [3, 18].

So far, the only IBS scheme without random oracles was proposed by Paterson–Schuldt [13]. This scheme satisfied security of weakly existential unforgeable under an adaptive chosen message attack (weakly EUF-ID-CMA). Roughly speaking, this means that an adversary who is given the private key for a few identities of

his choice in Extract Queries and the signature for a few pairs of identities and messages of his choice in Signature Queries should not be able to produce a new signature σ_* for an identity and a message, (ID_*, M_*), that the adversary has not made either the Extract Query on ID_* or the Signature Query on (ID_*, M_*).

Unfortunately, the Paterson–Schuldt scheme did not satisfy security of strongly EUF-ID-CMA, where the $(\mathrm{ID}_*, M_*, \sigma_*)$ on the weakly EUF-ID-CMA IBS was extended to that the adversary has not made either the Extract Query on ID_* or the Signature Query on $(\mathrm{ID}_*, M_*, \sigma_*)$. This is a concept of the strongest security in IBS. In such a scheme, if a legitimate signature for an identity and a message exists, then an adversary can forge a signature for the identity and the message that is valid in Verification. Hence, Paterson–Schuldt [13] suggested an open problem to construct IBS schemes which satisfy strongly EUF-ID-CMA, without random oracles.

In this paper, we propose a solution of this open problem, that is a "strongly" EUF-ID-CMA IBS scheme without random oracles for the first time. Security is based on the difficulty to solve three problems related to the Diffie–Hellman problem [9] and a one-way isomorphism [15, 16]. The method of our security proof is quite original, since many varieties of signature schemes that have been proposed are based on the methods in the Boneh–Boyen signature [2] or Waters signature [18].

Our scheme seems to be inefficient, since the bilinear map (the pairing) is used six times and the signature is constructed from five group parameters, during one iteration of the scheme. However, after certification between the signer and verifier has been performed once, the scheme then becomes as efficient as the Waters signature scheme [18]. Since our proposal satisfies the strongest security, our next step is to propose more efficient schemes with the same security.

The paper is organized in the following way. In Section 2, we prepare for the construction of our scheme and protocol, along with its proof of security. In Section 3, we will provide two new assumptions related to the DH problem, and make a proposal for our ID-based signature scheme. We prove our scheme satisfying security of strongly EUF-ID-CMA in Section 4, and provide conclusions in Section 5.

2. Preliminaries

The aim of this section is to define a one-way isomorphism, a bilinear map, the Diffie–Hellman (DH) problem, an ID-based signature scheme and the strongly EUF-ID-CMA.

2.1. One-Way Isomorphism and Bilinear Map

The following definitions are due to [15, 4]. We assume that

- $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are multiplicative cyclic groups of prime order p;
- g_2 is a generator of $\mathbb{G}_2$;

- f: $\mathbb{G}_2 \to \mathbb{G}_1$ is a one-way isomorphism satisfying $f(g_2^x) = g_1^x$, where $x \in \mathbb{Z}_p$ and g_1 is a generator of $\mathbb{G}_1$;
- $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is the cryptographic *bilinear map* satisfying the following properties:
  Bilinearity: $e(u^a, v^b) = e(u, v)^{ab}$ for any $u \in \mathbb{G}_1,\ v \in \mathbb{G}_2$ and any $a, b \in \mathbb{Z}$.
  Non-degenerate: $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$ for $\langle g_1 \rangle = \mathbb{G}_1$ and $\langle g_2 \rangle = \mathbb{G}_2$.
  Computable: There is an efficient algorithm to compute $e(u, v)$ for any $u \in \mathbb{G}_1$ and any $v \in \mathbb{G}_2$.

2.2. The Diffie–Hellman problem

We provide the DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$ as follows. Given

$$(g_2, g_2^x, g_2^y)$$

as input for random generators $g_2 \in_{\mathrm{R}} \mathbb{G}_2$ and random numbers $x, y \in_{\mathrm{R}} \mathbb{Z}_p^*$, compute g_1^{xy} for $g_1 \in_{\mathrm{R}} \mathbb{G}_1$. We say that algorithm $\mathcal{A}$ has an advantage ε in solving the DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$ if

$$\Pr\left[\mathcal{A}\left(g_2, g_2^x, g_2^y\right) = g_1^{xy}\right] \geq \varepsilon\ ,$$

where the probability is over the choice $g_1 \in_{\mathrm{R}} \mathbb{G}_1,\ g_2 \in_{\mathrm{R}} \mathbb{G}_2,\ x, y \in_{\mathrm{R}} \mathbb{Z}_p^*$ and the random bits of $\mathcal{A}$.

Assumption 1. *The (t, ε)-Diffie-Hellman (DH) Assumption in $(\mathbb{G}_2, \mathbb{G}_1)$ if no t-time adversary has an advantage of at least ε in solving the DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$.*

2.3. ID-based Signature Schemes

The definition of the IBS Scheme in this section is due to [4, 13].

An IBS scheme consists of four phases: *Setup, Extract, Sign* and *Verify* as follows.

Setup. A security parameter is taken as input and returns `params` (system parameters) and `master-key`. The system parameters include a decision of a finite message space $\mathcal{M}$, and a decision of a finite signature space $\mathcal{S}$. Intuitively, the system parameters will be publicly known, while the `master-key` will be known only to the Private Key Generator (PKG).

Extract. The output from Setup (`params`, `master-key`) is taken along with an arbitrary ID $\in \{0,1\}^*$ as input, and returns a private key d. Here ID is an arbitrary string that will be used as a public key, and d is the corresponding private sign key. The Extract phase extracts a private key from the given public key.

Sign. A message $M \in \mathcal{M}$, a private key d and `params` are taken as input. It returns a signature $\sigma \in \mathcal{S}$.

Verify. A message $M \in \mathcal{M}$, $\sigma \in \mathcal{S}$, ID and `params` are taken as input. It returns `valid` or `invalid`.

These phases must satisfy the standard consistency constraint, namely when d is the private key generated by phase *Extract* when it is given ID as the public key,

then

$$\forall M \in \mathcal{M},\ \forall \sigma := \mathit{Sign}(\mathtt{params}, d, M) :\ \Pr[\mathit{Verify}(\mathtt{params}, \mathrm{ID}, M, \sigma) = \mathtt{valid}] = 1\ .$$

2.4. Strongly EUF-ID-CMA

The definition of the strongly EUF-ID-CMA in this section is due to [4, 5, 13]. In particular, Paterson–Schuldt [13] defined the weakly EUF-ID-CMA and the strongly EUF-ID-CMA. However, their construction of the IBS scheme satisfied only the weakly EUF-ID-CMA.

Strongly EUF-ID-CMA is defined using the following game between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$:

Setup. The challenger $\mathcal{B}$ takes a security parameter k and runs the Setup phase of the IBS scheme. It gives the adversary $\mathcal{A}$ the resulting system parameters `params`. It keeps the `master-key` to itself.

Queries. The adversary $\mathcal{A}$ adaptively makes a number of different queries to the challenger $\mathcal{B}$. Each query can be one of the following.

– **Extract Queries** ($\mathbf{ID}_i$)**.** The challenger $\mathcal{B}$ responds by running phase Extract to generate the public key d_i corresponding to the public key (ID_i). It sends d_i to the adversary $\mathcal{A}$.

– **Signature Queries** ($\mathbf{ID}_i, M_{i,j}$)**.** For each query ($\mathrm{ID}_i, M_{i,j}$) issued by $\mathcal{A}$ the challenger $\mathcal{B}$ responds by running Sign to generate a signature σ_i of ($\mathrm{ID}_i, M_{i,j}$), and sending σ_i to $\mathcal{A}$.

Output. Finally $\mathcal{A}$ outputs a pair ($\mathrm{ID}_*, M_*, \sigma_*$). If σ_* is a valid signature of (ID_*, M_*) according to Verify, and $\mathcal{A}$ has neither made an Extract Query on ID_* nor a Signature Query on ($\mathrm{ID}_*, M_*, \sigma_*$), then $\mathcal{A}$ wins.

We define $\mathtt{AdvSig}_{\mathcal{A}}$ to be the probability that $\mathcal{A}$ wins the above game, taken over the coin tosses made by $\mathcal{B}$ and $\mathcal{A}$.

Definition 2.1. An adversary $\mathcal{A}$ $(q_{\mathrm{e}}, q_{\mathrm{s}}, t, \varepsilon)$-breaks an ID-based signature (IBS) scheme if $\mathcal{A}$ runs in a time of at most t, $\mathcal{A}$ makes at most q_{e} Extract Queries, at most q_{s} Signature Queries, and $\mathtt{AdvSig}_{\mathcal{A}}$ is at least ε. An IBS scheme is $(q_{\mathrm{e}}, q_{\mathrm{s}}, t, \varepsilon)$-strongly existential unforgeable under an adaptive chosen message attack, strongly EUF-ID-CMA, if no adversary $(q_{\mathrm{e}}, q_{\mathrm{s}}, t, \varepsilon)$-breaks it.

3. Our Scheme

In this section, we provide two new assumptions and propose an IBS scheme.

3.1. Underlying Proposed Problems

We provide Assumptions 2 and 3 related to the DH problem.

The first problem is defined as follows. Given

$$\left(g_1, g_2, g_1^x, g_2^{r_i}, g_2^{x+1/r_i} \,\middle|\, i = 1, \ldots, q\right)$$

as input for random generators $g_1 \in_{\mathrm{R}} \mathbb{G}_1$, $g_2 \in_{\mathrm{R}} \mathbb{G}_2$ and random numbers $x, r_1, \ldots, r_q \in_{\mathrm{R}} \mathbb{Z}_p^*$, compute $\left(g_1^{r_*}, g_2^{x+1/r_*}\right)$ for some $r_* \in \mathbb{Z}_p^*$ and $r_* \notin \{r_1, \ldots, r_q\}$. Note that the index $x + 1/r_i$ means $x + (1/r_i)$. We say that algorithm $\mathcal{A}$ has an advantage ε in solving the first problem if

$$\Pr\left[\mathcal{A}\left(g_1, g_2, g_1^x, g_2^{r_i}, g_2^{x+1/r_i} \,\middle|\, i = 1, \ldots, q\right) = \left(g_1^{r_*}, g_2^{x+1/r_*}\right)\right] \geq \varepsilon \ ,$$

where the probability is over the choice $g_1 \in_{\mathrm{R}} \mathbb{G}_1$, $g_2 \in_{\mathrm{R}} \mathbb{G}_2$, $x, r_1, \ldots, r_q \in_{\mathrm{R}} \mathbb{Z}_p^*$, some $r_* \in \mathbb{Z}_p^*$, $r_* \notin \{r_1, \ldots, r_q\}$ and the random bits of $\mathcal{A}$.

Assumption 2. *A (q, t, ε)-Assumption II holds if no t-time adversary has an advantage of at least ε in solving the first problem.*

The second problem is defined as follows. Given

$$\left(g_1, g_2, g_1^x, g_2^{1/x}, g_2^{r_i}, g_2^{xr_i}, g_2^{x+1/r_i} \,\middle|\, i = 1, \ldots, q\right)$$

as input for random generators $g_1 \in_{\mathrm{R}} \mathbb{G}_1$, $g_2 \in_{\mathrm{R}} \mathbb{G}_2$ and random numbers $x, r_1, \ldots, r_q \in_{\mathrm{R}} \mathbb{Z}_p^*$, compute $\left(g_2^{r_*}, g_2^{xr_*}, g_2^{x+1/r_*}\right)$ for some $r_* \in \mathbb{Z}_p^*$ and $r_* \notin \{r_1, \ldots, r_q\}$. We say that algorithm $\mathcal{A}$ has an advantage ε in solving the second problem if

$$\Pr\left[\mathcal{A}\left(g_1, g_2, g_1^x, g_2^{1/x}, g_2^{r_i}, g_2^{xr_i}, g_2^{x+1/r_i} \,\middle|\, i = 1, \ldots, q\right) = \left(g_2^{r_*}, g_2^{xr_*}, g_2^{x+1/r_*}\right)\right] \geq \varepsilon \ ,$$

where the probability is over the choice $g_1 \in_{\mathrm{R}} \mathbb{G}_1$, $g_2 \in_{\mathrm{R}} \mathbb{G}_2$, $x, r_1, \ldots, r_q \in_{\mathrm{R}} \mathbb{Z}_p^*$, some $r_* \in \mathbb{Z}_p^*$, $r_* \notin \{r_1, \ldots, r_q\}$ and the random bits of $\mathcal{A}$.

Assumption 3. *A (q, t, ε)-Assumption III holds if no t-time adversary has an advantage of at least ε in solving the second problem.*

Notice that, if we set $g_1 := f(g_2) \in \mathbb{G}_1$ for the one-way isomorphism $f : \mathbb{G}_2 \to \mathbb{G}_1$ and the random generator $g_2 \in_{\mathrm{R}} \mathbb{G}_2$, then the generator g_1 is not random in the two assumptions. The existence of f was proved by Saito–Hoshino–Uchiyama–Kobayashi [15], on multiplicative cyclic groups constructed on non-supersingular elliptic curves. Security of our scheme is essentially based on the DH assumption, our proposed two assumptions, and the isomorphism f. In particular, our proposed two assumptions which are defined in a rigorous manner contribute to prove the security of strongly EUF-ID-CMA for our scheme.

3.2. Scheme

We shall give an IBS scheme. This scheme consists of four phases: *Setup, Extract, Sign* and *Verify*. For the moment we shall assume that the identity ID are elements

in $\{0,1\}^{n_1}$, but the domain can be extended to all of $\{0,1\}^*$ using a collision-resistant hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{n_1}$. Similarly, we shall assume that the signature message M to be signed are elements in $\{0,1\}^{n_2}$.

Setup: The PKG chooses multiplicative cyclic groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ of sufficiently large prime order p, a random generator g_2 of $\mathbb{G}_2$, the one-way isomorphism $f : \mathbb{G}_2 \to \mathbb{G}_1$ with $g_1 := f(g_2)$, and the cryptographic bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. He generates $MK := g_2^{\alpha} \in \mathbb{G}_2$ from a random number $\alpha \in_{\mathrm{R}} \mathbb{Z}_p^*$, and calculates $A_1 := f(MK)\ (= g_1^{\alpha}) \in \mathbb{G}_1$.

$$\begin{array}{ccccc} \mathbb{Z}_p^* & \longrightarrow & \mathbb{G}_2 & \xrightarrow{f} & \mathbb{G}_1 \\ \alpha & \longmapsto & MK := g_2^{\alpha} & \longmapsto & A_1 := f(MK)\ (= g_1^{\alpha}) \end{array}$$

Also he generates $u' := g_2^{x'} \in \mathbb{G}_2, U = (u_1, \ldots, u_{n_1}) := (g_2^{x_1}, \ldots, g_2^{x_{n_1}}) \in \mathbb{G}_2^{n_1}, v' := g_2^{y'} \in \mathbb{G}_2$, and $V = (v_1, \ldots, v_{n_2}) := (g_2^{y_1}, \ldots, g_2^{y_{n_2}}) \in \mathbb{G}_2^{n_2}$ for random numbers $x', x_1, \ldots, x_{n_1}, y', y_1, \ldots, y_{n_2} \in_{\mathrm{R}} \mathbb{Z}_p^*$. The master secret is SK and the public parameter are

$$\mathtt{params} := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, f, g_1, g_2, A_1, u', U, v', V)\ .$$

Extract: Let ID be an n_1-bit identity and id_k $(k = 1, \ldots, n_1)$ denote the kth bit of ID. To generate a private key d_{ID} for $\mathrm{ID} \in \{0,1\}^{n_1}$, the PKG picks a random number $s \in_{\mathrm{R}} \mathbb{Z}_p^*$, and computes

$$d_{\mathrm{ID}} = (d_1, d_2) := \left(g_2^s, g_2^{\alpha} \cdot \left(u' \prod_{k=1}^{n_1} u_k^{\mathrm{id}_k} \right)^{1/s} \right) \in \mathbb{G}_2^2\ .$$

Sign: Let M be an n_2-bit signature message to be signed and m_k $(k = 1, \ldots, n_2)$ denote the kth bit of M. A signature $\sigma := (\sigma_1, \ldots, \sigma_5)$ of (ID, M) is generated as follows.

$$\begin{aligned} (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5) &:= \left(f(d_1), g_2^r, d_1^r, d_2, d_1 \cdot \left(v' \prod_{k=1}^{n_2} v_k^{m_k} \right)^{1/r} \right) \\ &= \left(g_1^s, g_2^r, g_2^{sr},\ g_2^{\alpha} \cdot \left(u' \prod_{k=1}^{n_1} u_k^{\mathrm{id}_k} \right)^{1/s}, g_2^s \cdot \left(v' \prod_{k=1}^{n_2} v_k^{m_k} \right)^{1/r} \right) \end{aligned}$$

for a random number $r \in \mathbb{Z}_p^*$.

Verify: Suppose we wish to check if $\sigma = (\sigma_1, \ldots, \sigma_5)$ is a signature for (ID, M). The signature is accepted if

$$\begin{aligned} e(\sigma_1, \sigma_2) &= e(g_1, \sigma_3) \ , \\ e\left(A_1^{-1} \cdot f(\sigma_4), \sigma_3\right) &= e\left(f(\sigma_2), u' \prod_{k=1}^{n_1} u_k^{\mathrm{id}_k}\right) \text{ and} \\ e\left(\sigma_1^{-1} \cdot f(\sigma_5), \sigma_2\right) &= e\left(g_1, v' \prod_{k=1}^{n_2} v_k^{m_k}\right) \ , \end{aligned}$$

and rejected otherwise.

If an entity with identity ID constructs a signature $\sigma = (\sigma_1, \ldots, \sigma_5)$ on a message M as described in the Sign phase above, it is easy to see that σ will be accepted by a verifier:

$$\begin{aligned} e(\sigma_1, \sigma_2) &= e(g_1^s, g_2^r) = e(g_1, g_2^{sr}) = e(g_1, \sigma_3) \ , \\ e\left(A_1^{-1} \cdot f(\sigma_4), \sigma_3\right) &= e\left(f\left(u' \prod_{k=1}^{n_1} u_k^{\mathrm{id}_k}\right)^{1/s}, g_2^{sr}\right) = e\left(g_1^r, u' \prod_{k=1}^{n_1} u_k^{\mathrm{id}_k}\right) \\ e\left(\sigma_1^{-1} \cdot f(\sigma_5), \sigma_2\right) &= e\left(f\left(v' \prod_{k=1}^{n_2} v_k^{m_k}\right)^{1/r}, g_2^r\right) = e\left(g_1, v' \prod_{k=1}^{n_2} v_k^{m_k}\right) \ . \end{aligned}$$

Thus the scheme is correct.

4. Security Proof

Theorem 4.1. *Suppose that the (t_0, ε_0)-DH Assumption in $(\mathbb{G}_2, \mathbb{G}_1)$, $(q_1, t_1, \varepsilon_1)$-Assumption II and $(q_2, t_2, \varepsilon_2)$-Assumption III hold with $g_1 := f(g_2)$. Then the proposed ID-based signature scheme is $(q_\mathrm{e}, q_\mathrm{s}, t, \varepsilon)$-strongly EUF-ID-CMA, provided that $q_\mathrm{e} \leq q_1$, $q_\mathrm{s} \leq q_2$, $t \leq \min(t_0, t_1, t_2) - O((q_\mathrm{e} + q_\mathrm{s})T)$ and $\varepsilon\,(1 - 2(q_\mathrm{e} + q_\mathrm{s})/p) \geq \varepsilon_0 + \varepsilon_1 + \varepsilon_2$, where T is the maximum time for an exponentiation in $\mathbb{G}_2$.*

Outline of our proof for the theorem is done in the following manner. Suppose that there exists an adversary, $\mathcal{A}$, who (q, t, ε)-breaks our IBS scheme in Section 3, and a challenger, $\mathcal{B}$, takes the Assumption II challenge. After $\mathcal{A}$ and $\mathcal{B}$ execute the strongly EUF-ID-CMA game, $\mathcal{A}$ outputs a valid tuple for an identity, a message and a signature. Then $\mathcal{B}$ will compute the Assumption II response which is valid. The tuple from $\mathcal{A}$ must not contradict the DH assumption and the Assumption III .

Proof. We construct a simulator, $\mathcal{B}$, to play the Assumption II game. The simulator $\mathcal{B}$ will take the Assumption II challenge

$$\left(g_1, g_2, g_1^{\alpha}, g_2^{s_i}, g_2^{\alpha+1/s_i} \,\middle|\, i = 1, \ldots, q_1\right)$$

for $\alpha, s_1, \ldots, s_{q_1} \in_{\mathrm{R}} \mathbb{Z}_p^*$, and run $\mathcal{A}$ executing the following steps.

A. Simulator Description

Setup: The simulator $\mathcal{B}$ generates $u' := g_2^{x'} \in \mathbb{G}_2, U = (u_1, \ldots, u_{n_1}) := (g_2^{x_1}, \ldots, g_2^{x_{n_1}}) \in \mathbb{G}_2^{n_1}, v' := g_2^{y'} \in \mathbb{G}_2$, and $V = (v_1, \ldots, v_{n_2}) := (g_2^{y_1}, \ldots, g_2^{y_{n_2}}) \in \mathbb{G}_2^{n_2}$ for random numbers $x', x_1, \ldots, x_{n_1}, y', y_1, \ldots, y_{n_2} \in_{\mathrm{R}} \mathbb{Z}_p^*$, and sends

$$(g_1, g_2, g_1^{\alpha}, u', U, v', V)$$

to $\mathcal{A}$.

Queries: The adversary $\mathcal{A}$ adaptively makes a number of different queries to the challenger $\mathcal{B}$.

Assume that $\mathcal{U}_{\mathrm{e}}$ is the subscript set of identities in Extract Queries, $\mathcal{U}_{\mathrm{s}}$ is that of identities in Signature Queries, $\mathcal{U} := \mathcal{U}_{\mathrm{e}} \vee \mathcal{U}_{\mathrm{s}}$, and $\mathcal{M}_{\mathrm{s}}^i$ is that of messages in Signature Queries for the ID_i ($i \in \mathcal{U}_{\mathrm{s}}$).

Each query can be one of the following.

– **Extract Queries:** The adversary $\mathcal{A}$ adaptively issues Extract Queries ID_i ($i \in \mathcal{U}_{\mathrm{e}}$). Assume that

$$X_i := x' + \sum_{k=1}^{n_1} \mathrm{id}_{i,k}\ x_k\ , \tag{4.1}$$

where $\mathrm{ID}_i := (\mathrm{id}_{i,1}, \ldots, \mathrm{id}_{i,n_1}) \in \{0,1\}^{n_1}$.

(A-E1) If $X_i \equiv 0 \pmod{p}$, $\mathcal{B}$ aborts this game.

(A-E2) Otherwise (i.e. $X_i \not\equiv 0 \pmod{p}$), $\mathcal{B}$ does not abort the game, and generates $d_i = (d_{i,1}, d_{i,2})$ of ID_i:

$$\begin{aligned}
(d_{i,1}, d_{i,2}) &:= \left((g_2^{s_i})^{X_i}, g_2^{\alpha+1/s_i}\right) && (4.2)\\
&= \left(g_2^{\overline{s_i}}, g_2^{\alpha} \cdot \left(g_2^{X_i}\right)^{1/\overline{s_i}}\right) \\
&= \left(g_2^{\overline{s_i}}, g_2^{\alpha} \cdot \left(u' \prod_{k=1}^{n_1} u_k^{\mathrm{id}_{i,k}}\right)^{1/\overline{s_i}}\right) && (4.3)
\end{aligned}$$

and sends it to $\mathcal{A}$. Here $\overline{s_i} := s_i X_i \bmod p$ $(i \in \mathcal{U}_{\rm e})$. (Notice that, by eliminating all $s_i \in_{\rm R} \mathbb{Z}_p^*$ in (4.2), we can regard all $\overline{s_i} \in_{\rm R} \mathbb{Z}_p^*$ as random numbers in (4.3)).

– **Signature Queries:** The adversary $\mathcal{A}$ adaptively issues Signature Queries $({\rm ID}_i, M_{i,j})$ $\left(i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i\right)$. Assume that X_i is from (4.1) for $i \in \mathcal{U}_{\rm s}$ and

$$Y_{i,j} := y' + \sum_{k=1}^{n_2} m_{i,j,k}\ y_k\ , \tag{4.4}$$

where $M_{i,j} := (m_{i,j,1}, \ldots, m_{i,j,n_2}) \in \{0,1\}^{n_2}$.

(A-S1) If $X_i \equiv 0 \pmod p$ or $Y_{i,j} \equiv 0 \pmod p$, $\mathcal{B}$ aborts this game.

(A-S2) Otherwise (i.e. $X_i \not\equiv 0 \pmod p$ and $Y_{i,j} \not\equiv 0 \pmod p$), $\mathcal{B}$ does not abort the game, and generates $\sigma_{i,j} = (\sigma_{i,j,1}, \ldots, \sigma_{i,j,5})$ of $({\rm ID}_i, M_{i,j})$:

$$\left\{\begin{array}{ll}
\sigma_{i,j,1} & := (g_1^{s_i})^{X_i} = g_1^{\overline{s_i}} \\
\sigma_{i,j,2} & := (g_2)^{r_{i,j} Y_{i,j}/X_i} = g_2^{\overline{r_{i,j}}} \\
\sigma_{i,j,3} & := (g_2^{s_i})^{r_{i,j} Y_{i,j}} = g_2^{\overline{s_i}\ \overline{r_{i,j}}} \\
\sigma_{i,j,4} & := g_2^{\alpha + 1/s_i} = g_2^{\alpha} \cdot \left(g_2^{X_i}\right)^{1/\overline{s_i}} = g_2^{\alpha} \cdot \left(u' \displaystyle\prod_{k=1}^{n_1} u_k^{{\rm id}_{i,k}}\right)^{1/\overline{s_i}} \\
\sigma_{i,j,5} & := \left(g_2^{s_i + 1/r_{i,j}}\right)^{X_i} = g_2^{\overline{s_i}} \cdot \left(g_2^{Y_{i,j}}\right)^{1/\overline{r_{i,j}}} = g_2^{\overline{s_i}} \cdot \left(v' \displaystyle\prod_{k=1}^{n_2} v_k^{m_{i,j,k}}\right)^{1/\overline{r_{i,j}}}
\end{array}\right.$$

and sends it to $\mathcal{A}$. Here $\overline{s_i} := s_i X_i \bmod p$ $(i \in \mathcal{U}_{\rm s})$ and $\overline{r_{i,j}} := r_{i,j} Y_{i,j}/X_i \bmod p$ $\left(i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i\right)$. (Notice that, by eliminating all $s_i, r_{i,j} \in_{\rm R} \mathbb{Z}_p^*$, we can regard all $\overline{s_i}, \overline{r_{i,j}} \in_{\rm R} \mathbb{Z}_p^*$ as random numbers.

Output: The adversary $\mathcal{A}$ outputs $({\rm ID}_*, M_*, \sigma_*)$ such that $\sigma_* = (\sigma_{*,1}, \ldots, \sigma_{*,5}) \in \mathbb{G}_2^5$ is a valid signature of $({\rm ID}_*, M_*)$, without making an Extract Query on ${\rm ID}_*$ nor a Signature Query on $({\rm ID}_*, M_*, \sigma_*)$.

Artificial Abort: Assume that

$$\begin{aligned}
X_* &:= x' + \sum_{k=1}^{n_1} {\rm id}_{*,k}\ x_k\ , \\
Y_* &:= y' + \sum_{k=1}^{n_2} m_{*,k}\ y_k\ ,
\end{aligned} \tag{4.5}$$

where ${\rm ID}_* := ({\rm id}_{*,1}, \ldots, {\rm id}_{*,n_1}) \in \{0,1\}^{n_1}$ and $M_* := (m_{*,1}, \ldots, m_{*,n_2}) \in \{0,1\}^{n_2}$. If ${\rm ID}_* \neq {\rm ID}_i$ and $X_* \equiv X_i \pmod p$ for some $i \in \mathcal{U}$, or if $M_* \neq M_{i,j}$ and $Y_* \equiv Y_{i,j} \pmod p$ for some $i \in \mathcal{U}_{\rm s}$ and $j \in \mathcal{M}_{\rm s}^i$, then $\mathcal{B}$ aborts this game.

B. Analysis

The adversary $\mathcal{A}$ cannot distinguish the above game from Simulator Description with the abort when $X_i \equiv 0 \pmod p$ or $Y_{i,j} \equiv 0 \pmod p$, and the strongly EUF-ID-CMA game without this abort, since

$$\Pr\left[\bigvee_{i\in\mathcal{U}} X_i \equiv 0 \pmod p \vee \bigvee_{\substack{i\in\mathcal{U}_{\rm s},\\ j\in\mathcal{M}_{\rm s}^i}} Y_{i,j} \equiv 0 \pmod p\right] \leq \frac{q_{\rm e}+q_{\rm s}}{p}$$

and this probability is negligible when $q_{\rm e}+q_{\rm s} \ll p$. Thus we shall consider only the game from Simulator Description.

Since σ_* is valid, we assume that

$$\begin{cases} \sigma_{*,1} := g_1^{\overline{s_*}} \\ \sigma_{*,2} := g_2^{\overline{r_*}} \\ \sigma_{*,3} := g_2^{\overline{s_*}\ \overline{r_*}} \\ \sigma_{*,4} := g_2^{\alpha} \cdot \left(u' \prod_{k=1}^{n_1} u_k^{{\rm id}_{*,k}}\right)^{1/\overline{s_*}} = g_2^{\alpha+X_*/\overline{s_*}} \\ \sigma_{*,5} := g_2^{\overline{s_*}} \cdot \left(v' \prod_{k=1}^{n_2} v_k^{m_{*,k}}\right)^{1/\overline{r_*}} = g_2^{\overline{s_*}+Y_*/\overline{r_*}} \end{cases}$$

where $\overline{s_*}, \overline{r_*} \in \mathbb{Z}_p^*$.

(B-1) If $X_* \equiv 0 \pmod p$, $\sigma_{*,4} = g_2^{\alpha}$. Then $\mathcal{B}$ generates $\left(g_1^{s_*}, g_2^{\alpha+1/s_*}\right)$ for some $s_* \in \mathbb{Z}_p^*$ and $s_* \notin \{s_1, \ldots, s_q\}$. which is a valid output of the Assumption II challenge.

(B-2) Otherwise (i.e. $X_* \not\equiv 0 \pmod p$).

(B-2.1) Suppose that ${\rm ID}_* \notin \{{\rm ID}_i \mid i \in \mathcal{U}_{\rm e}\}$ (which is an assumption of the strongly EUF-ID-CMA) and $({\rm ID}_*, \overline{s_*}) \notin \{({\rm ID}_i, \overline{s_i}) \mid i \in \mathcal{U}_{\rm s}\}$. Then, it is sufficient to consider

$$\begin{aligned} &\Pr\Big[\mathcal{A}\Big(g_1, g_2, g_1^{\alpha}, g_2^{x'}, g_2^{x_1}, \ldots, g_2^{x_{n_1}}, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, \\ &\quad g_2^{X_i}, g_2^{Y_{i,j}}, g_2^{\overline{s_i}}, g_2^{\overline{r_{i,j}}}, g_2^{\overline{s_i}\ \overline{r_{i,j}}}, g_2^{\alpha+X_i/\overline{s_i}}, g_2^{\overline{s_i}+Y_{i,j}/\overline{r_{i,j}}} \Big| \ i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i\Big) \\ &\quad = \left(g_2^{X_*}, g_2^{Y_*}, g_1^{\overline{s_*}}, g_2^{\overline{r_*}}, g_2^{\overline{s_*}\ \overline{r_*}}, g_2^{\alpha+X_*/\overline{s_*}}, g_2^{\overline{s_*}+Y_*/\overline{r_*}}\right)\Big] \ . \end{aligned} \tag{4.6}$$

in the case that $\mathcal{A}$ knows the all $g_2^{\overline{s_i}}$ $(= d_{i,1})$. This means that $\mathcal{U} = \mathcal{U}_{\rm e} = \mathcal{U}_{\rm s}$.
(B-2.1.1) Assume that there exists a number $l \in \mathcal{U}$ such that $s_* = s_l$. In (4.6), if $\mathcal{A}$ knows all $\overline{s_i}, \overline{r_{i,j}}$ $(i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i)$ and $g_2^{\alpha} \in \mathbb{G}_2$, then we can eliminate

$$\left(g_1^{\alpha}, g_2^{\overline{s_i}}, g_2^{\overline{r_{i,j}}}, g_2^{\overline{s_i}\ \overline{r_{i,j}}}, g_2^{\alpha+X_i/\overline{s_i}}, g_2^{\overline{s_i}+Y_{i,j}/\overline{r_{i,j}}}\right) \ .$$

from (4.6). Also, since $X_*/\overline{s_*} \equiv X_l/\overline{s_l} \pmod p$, we replace the third parameter of the output by

$$g_1^{X_*/X_l} \left(= \left(g_1^{\overline{s_l} X_*/X_l} \right)^{1/\overline{s_l}} = \left(g_1^{\overline{s_*}} \right)^{1/\overline{s_l}} \right)$$

and eliminate the remaining parameters. Thus $\mathcal{A}$ has an advantage of ε' in solving

$$\Pr\Big[\mathcal{A}\Big(g_1, g_2, g_2^{x'}, g_2^{x_1}, \ldots, g_2^{x_{n_1}}, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{X_i}, g_2^{Y_{i,j}}, \\ \Big| \ i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i \Big) = g_1^{X_*/X_l} \Big] \ , \tag{4.7}$$

where the probability is over the choice $g_2 \in_{\rm R} \mathbb{G}_2$, $x', x_1, \ldots, x_{n_1}, y', y_1, \ldots, y_{n_2} \in_{\rm R} \mathbb{Z}_p^*$, X_i $(i \in \mathcal{U})$ in (4.1), X_* in (4.5), $Y_{i,j}$ $(i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i)$ in (4.4), Y_* in (4.5), and the random bits of $\mathcal{A}$. Set

$$L_{i,*} := \sum_{k=1}^{n_1} (\mathrm{id}_{i,k} - \mathrm{id}_{*,k}) \ x_k$$

for $i \in \mathcal{U}$. Since

$$x' \equiv X_* - \sum_{k=1}^{n_1} \mathrm{id}_{*,k} \ x_k \pmod p \equiv X_i - \sum_{k=1}^{n_1} \mathrm{id}_{i,k} \ x_k \pmod p \ (i \in \mathcal{U}) \ ,$$

$\mathcal{A}$ is able to calculate

$$\begin{cases} g_2^{x'} = g_2^{X_l - \sum_{k=1}^{n_1} \mathrm{id}_{l,k} x_k} , \\ g_2^{X_i} = g_2^{X_l - \sum_{k=1}^{n_1} (\mathrm{id}_{l,k} - \mathrm{id}_{i,k}) x_k} \ (i \in \mathcal{U} \text{ and } i \neq l) \\ g_2^{X_*} = g_2^{X_l - \sum_{k=1}^{n_1} (\mathrm{id}_{l,k} - \mathrm{id}_{*,k}) x_k} = g_2^{X_l - L_{l,*}} \end{cases}$$

from $g_2^{X_l}, g_2^{x_1}, \ldots, g_2^{x_{n_1}}$, $\mathrm{ID}_i (i \in \mathcal{U}), \mathrm{ID}_*$, and eliminates these parameters from (4.7). Also, since $g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{i,j}} (i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i)$ are unrelated to the out put $g_1^{X_*/X_l}$, the adversary $\mathcal{A}$ can eliminate these parameters as input. By substituting

$$g_2^{X_*/X_l} = g_2^{(X_l - L_{l,*})/X_l} = g_2 \cdot g_2^{-L_{l,*}/X_l}$$

to $g_2^{L_{l,*}/X_l}$ in (4.7), $\mathcal{A}$ has an advantage of ε' in solving

$$\Pr\left[\mathcal{A}\left(g_2, g_2^{x_1}, \ldots, g_2^{x_{n_1}}, g_2^{X_l}\right) = g_1^{L_{l,*}/X_l}\right] \geq \varepsilon' \ .$$

Notice that $L_{l,*} \not\equiv 0 \pmod p$ since $\mathrm{ID}_* \neq \mathrm{ID}_l$ even when $\overline{s_*} \neq \overline{s_l}$. Assume that $h := X_l \bmod p$. Then, since $x' \in_{\rm R} \mathbb{Z}_p^*$ has been eliminated, we can regard h as a random number in $\mathbb{Z}_p^*$. It is equivalent to that $\mathcal{A}$ has an advantage of ε' in solving

$$\Pr\left[\mathcal{A}\left(g_2, g_2^y, g_2^h\right) = g_1^{y/h}\right] \geq \varepsilon' \ ,$$

where the probability is over $g_2 \in \mathbb{G}_2$, $y, h \in_{\rm R} \mathbb{Z}_p^*$ and the random bits of $\mathcal{A}$. From [1], it is equivalent to that $\mathcal{A}$ has an advantage of ε' in solving

$$\Pr\left[\mathcal{A}\left(g_2, g_2^y, g_2^h\right) = g_1^{yh}\right] \geq \varepsilon' \ .$$

where the probability is over $g_2 \in \mathbb{G}_2$, $g_1(= f(g_2)) \in \mathbb{G}_1$, $y, h \in_{\mathrm{R}} \mathbb{Z}_p^*$ and the random bits of $\mathcal{A}$. This means that $\mathcal{A}$ solves the DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$ with a non-negligible probability.

(B-2.1.2) Otherwise (i.e. $s_* \notin \{s_i \mid i \in \mathcal{U}\}$), suppose that $\mathcal{A}$ knows $x', x_1, \ldots, x_{n_1}$, $y', y_1, \ldots, y_{n_2}$. Then

$$\left(g_2^{x'}, g_2^{x_1}, \ldots, g_2^{x_{n_1}}, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{X_i}, g_2^{Y_{i,j}}\right)$$

can be eliminated from (4.6). Also, considering the pair

$$\left(g_1^{s_*}, g_2^{\alpha+1/s_*}\right) := \left(\left(g_1^{\overline{s_*}}\right)^{1/H_*}, g_2^{\alpha+H_*/\overline{s_*}}\right)$$

as an output of the Assumption II challenge,

$$\left(g_2^{\overline{r_{i,j}}}, g_2^{\overline{s_i}\ \overline{r_{i,j}}}, g_2^{\overline{s_i}+Y_{i,j}/\overline{r_{i,j}}}\right)$$

can be eliminated from (4.6). These mean that the probability (4.6) can be deformed to a contradiction of Assumption II.

(B-2.2) Otherwise (i.e. $\mathrm{ID}_* \notin \{\mathrm{ID}_i \mid i \in \mathcal{U}_{\mathrm{e}}\}$ and $(\mathrm{ID}_*, \overline{s_*}) = (\mathrm{ID}_l, \overline{s_l})$ for some $l \in \mathcal{U}_{\mathrm{s}}$), then $X_* = X_l$. It is sufficient to consider

$$\Pr\Big[\mathcal{A}\Big(g_1, g_2, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{l,j}}, g_{\mathbf{1}}^{\overline{s_l}}, g_2^{1/\overline{s_l}}, g_2^{\overline{r_{l,j}}}, g_2^{\overline{s_l}\ \overline{r_{l,j}}}, g_2^{\overline{s_l}+Y_{l,j}/\overline{r_{l,j}}}\Big| \ j \in \mathcal{M}_{\mathrm{s}}^l\Big) = \left(g_2^{Y_*}, g_2^{\overline{r_*}}, g_2^{\overline{s_l}\ \overline{r_*}}, g_2^{\overline{s_l}+Y_*/\overline{r_*}}\right)\Big] \tag{4.8}$$

in the case that $\mathcal{A}$ knows $x', x_1, \ldots, x_{n_1}$ and g_2^{α}.

(B-2.2.1) Suppose that $M_* \notin \{M_{l,j} |\ j \in \mathcal{M}_{\mathrm{s}}^l\}$.

(B-2.2.1.1) Assume that there exists a number $k \in \mathcal{M}_{\mathrm{s}}^l$ such that $r_* = r_{l,k}$. In (4.8), if $\mathcal{A}$ knows the all $\overline{r_{l,j}}$ $(j \in \mathcal{M}_{\mathrm{s}}^l)$ and $\overline{s_l} \in \mathbb{Z}_p^*$, then we can eliminate

$$\left(g_1, g_1^{\overline{s_l}}, g_2^{1/\overline{s_l}}, g_2^{\overline{r_{l,j}}}, g_2^{\overline{s_l}\ \overline{r_{l,j}}}, g_2^{\overline{s_l}+Y_{l,j}/\overline{r_{l,j}}}, g_2^{\overline{s_l}\ \overline{r_*}}\Big| \ j \in \mathcal{M}_{\mathrm{s}}^l\right)$$

from (4.8). Also, since $Y_*/\overline{r_*} \equiv Y_{l,k}/\overline{r_{l,k}} \pmod{p}$, we replace the second parameter of the output by

$$g_2^{Y_*/Y_{l,k}}\left(= \left(g_2^{\overline{r_{l,k}}Y_*/Y_{l,k}}\right)^{1/\overline{r_{l,k}}} = \left(g_2^{\overline{r_*}}\right)^{1/\overline{r_{l,k}}}\right)$$

and eliminate the third and fourth parameters. Thus $\mathcal{A}$ has an advantage of ε' in solving

$$\Pr\Big[\mathcal{A}\Big(g_2, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{l,j}}\Big| \ j \in \mathcal{M}_{\mathrm{s}}^l\Big) = \left(g_2^{Y_*}, g_2^{Y_*/Y_{l,k}}\right)\Big] \geq \varepsilon' \ , \tag{4.9}$$

where the probability is over the choice $g_2 \in_{\mathrm{R}} \mathbb{G}_2$, $y', y_1, \ldots, y_{n_2} \in_{\mathrm{R}} \mathbb{Z}_p^*$, $Y_{l,j} (j \in \mathcal{M}_{\mathrm{s}}^l)$ in (4.4), Y_* in (4.5), and the random bits of $\mathcal{A}$. Set

$$K_{l,j,*} := \sum_{i=1}^{n_2} (m_{l,j,i} - m_{*,i})\ y_i$$

for $j \in \mathcal{M}_{\rm s}^l$. Since

$$y' \equiv Y_* - \sum_{i=1}^{n_2} m_{*,i}\ y_i \pmod p \equiv Y_{l,j} - \sum_{i=1}^{n_2} m_{l,j,i}\ y_i \pmod p\ (j \in \mathcal{M}_{\rm s}^l)\ ,$$

$\mathcal{A}$ is able to calculate

$$\begin{cases} g_2^{y'} &= g_2^{Y_{l,k} - \sum_{i=1}^{n_2} m_{l,k,i} y_i}\ , \\ g_2^{Y_{l,j}} &= g_2^{Y_{l,k} - \sum_{i=1}^{n_2} (m_{l,k,i} - m_{l,j,i}) y_i}\ (j \in \mathcal{M}_{\rm s}^l, j \neq k)\ , \\ g_2^{Y_*} &= g_2^{Y_{l,k} - \sum_{i=1}^{n_2} (m_{l,k,i} - m_{*,i}) y_i} = g_2^{Y_{l,k} - K_{l,k,*}} \end{cases}$$

from $g_2^{Y_{l,k}}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, M_{l,j} (j \in \mathcal{M}_{\rm s}^l), M_*$, and eliminates these parameters from (4.9). By substituting

$$g_2^{Y_*/Y_{l,k}} = g_2^{(Y_{l,k} - K_{l,k,*})/Y_{l,k}} = g_2 \cdot g_2^{-K_{l,k,*}/Y_{l,k}}$$

to $g_2^{K_{l,k,*}/Y_{l,k}}$ in (4.9), $\mathcal{A}$ has an advantage of ε' in solving

$$\Pr\left[\mathcal{A}\left(g_2, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{l,k}}\right) = g_2^{K_{l,k,*}/Y_{l,k}}\right] \geq \varepsilon'\ .$$

Such as (B-2.1.1), this means that $\mathcal{A}$ solves the DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$ with a non-negligible probability.

(B-2.2.1.2) Otherwise (i.e. $r_* \notin \{r_{l,j} | \ j \in \mathcal{M}_{\rm s}^l\}$), suppose that $\mathcal{A}$ knows $y', y_1, \ldots, y_{n_2}$ as well as $x', x_1, \ldots, x_{n_1}$. Then, from the equalities $s_l = \overline{s_l}/X_l$, $r_{l,i} = \overline{r_{l,i}} X_l / Y_{l,i}$ and $r_* = \overline{r_*} X_l / Y_*$, the probability (4.8) can be deformed to a contradiction of Assumption III.

(B-2.2.2) Otherwise (i.e. $M_* = M_{l,k}$ for some $k \in \mathcal{M}_{\rm s}^l$), assume that $i_1, \ldots, i_c \in \mathcal{M}_{\rm s}^l$ are all the numbers such that $M_* = M_{l,i_1} = \cdots = M_{l,i_c}$. Then $r_* \notin \{r_{l,i_1}, \ldots, r_{l,i_c}\}$ from $\overline{r_*} \notin \{\overline{r_{l,i_1}}, \ldots, \overline{r_{l,i_c}}\}$, $Y_* = Y_{l,i_1} = \cdots = Y_{l,i_c} \not\equiv 0 \pmod p$, $r_* = \overline{r_*} X_* / Y_* \bmod p \in_{\rm R} \mathbb{Z}_p^*$, and $r_{l,i} = \overline{r_{l,i}} X_l / Y_{l,i} \bmod p \in_{\rm R} \mathbb{Z}_p^*$ $(i = i_1, \ldots, i_c)$.

Let $\{j_1, \ldots, j_w\}$ be the complement of $\{i_1, \ldots, i_c\}$ in $\mathcal{M}_{\rm s}^l$ with $w + c = |\mathcal{M}_{\rm s}^l|$. Then this means that $M_* \notin \{M_{l,j_1}, \ldots, M_{l,j_w}\}$.

(B-2.2.2.1) Assume that $c \neq |\mathcal{M}_{\rm s}^l|$ and there exists a number $k \in \{j_1, \ldots, j_w\}$ such that $r_* = r_k$. Then, like (B-2.2.1.1), $\mathcal{A}$ solves the DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$ with a non-negligible probability.

(B-2.2.2.2) Otherwise (i.e. $c = |\mathcal{M}_{\rm s}^l|$ or $r_* \notin \{r_{l,j_1}, \ldots, r_{l,j_w}\}$), the pair $\left(g_2^{r_*}, g_2^{s_l r_*}, g_2^{s_l + 1/r_*}\right)$ is a valid output of the Assumption III challenge.

The probability of the simulation neither aborting in the case $X_i \equiv 0 \pmod p$ $(i \in \mathcal{U})$, $X_* \equiv X_i \pmod p$ $(i \in \mathcal{U})$, $Y_{i,j} \equiv 0 \pmod p$ $(i \in \mathcal{U}_{\rm s}, j \in \mathcal{M}_{\rm s}^i)$ nor $Y_* \equiv Y_{i,j}$

$(\mathrm{mod}\ p)$ $(i \in \mathcal{U}_{\mathrm{s}}, j \in \mathcal{M}_{\mathrm{s}}^i)$ is

$$\begin{aligned}
&\Pr\left[\bigwedge_{i\in\mathcal{U}}\left(X_i \overset{(p)}{\not\equiv} 0 \wedge X_* \overset{(p)}{\not\equiv} X_i\right) \wedge \bigwedge_{\substack{i\in\mathcal{U}_{\mathrm{s}},\\ j\in\mathcal{M}_{\mathrm{s}}^i}}\left(Y_{i,j} \overset{(p)}{\not\equiv} 0 \wedge Y_* \overset{(p)}{\not\equiv} Y_{i,j}\right)\right] \\
&= \Pr\left[\bigwedge_{i\in\mathcal{U}}\left(X_i \overset{(p)}{\not\equiv} 0 \wedge L_{i,*} \overset{(p)}{\not\equiv} 0\right) \wedge \bigwedge_{\substack{i\in\mathcal{U}_{\mathrm{s}},\\ j\in\mathcal{M}_{\mathrm{s}}^i}}\left(Y_{i,j} \overset{(p)}{\not\equiv} 0 \wedge K_{i,j,*} \overset{(p)}{\not\equiv} 0\right)\right] \\
&\geq 1 - \sum_{i\in\mathcal{U}}\left(\Pr\left[X_i \overset{(p)}{\equiv} 0\right] + \Pr\left[L_{i,*} \overset{(p)}{\equiv} 0\right]\right) - \sum_{\substack{i\in\mathcal{U}_{\mathrm{s}},\\ j\in\mathcal{M}_{\mathrm{s}}^i}}\left(\Pr\left[Y_{ij} \overset{(p)}{\equiv} 0\right] + \Pr\left[K_{i,j,*} \overset{(p)}{\equiv} 0\right]\right) \\
&= 1 - \frac{2(q_{\mathrm{e}}+q_{\mathrm{s}})}{p}
\end{aligned}$$

where $x \overset{(p)}{\equiv} y$ denotes $x \equiv y\ (\mathrm{mod}\ p)$. Thus we have

$$\begin{aligned}
&\Pr\left[\bigwedge_{i\in\mathcal{U}}\left(X_i \overset{(p)}{\not\equiv} 0 \wedge X_* \overset{(p)}{\not\equiv} X_i\right) \wedge \bigwedge_{j\in\mathcal{M}_{\mathrm{s}}^l}\left(Y_{l,j} \overset{(p)}{\not\equiv} 0 \wedge Y_* \overset{(p)}{\not\equiv} Y_{l,j}\right) \;\middle|\; \mathcal{A}\ (q_{\mathrm{e}}, q_{\mathrm{s}}, t, \varepsilon)\text{-breaks } \mathcal{S}\right] \\
&\geq \varepsilon\left(1 - \frac{2(q_{\mathrm{e}}+q_{\mathrm{s}})}{p}\right) \qquad (4.10)
\end{aligned}$$

in the proposed scheme $\mathcal{S}$. From (B-1) and (B-2), the probability

$$\begin{aligned}
\Pr\Bigg[&\mathcal{B}\left(g_1, g_2, g_1^{\alpha}, g_2^{r_i}, g_2^{\alpha+1/r_i} \;\middle|\; i \in \mathcal{U}\right) = \left(g_1^{r_*}, g_2^{\alpha+1/r_*}\right) \vee\ \mathcal{A}\left(g_2, g_2^{x}, g_2^{y}\right) = g_1^{xy} \\
&\vee \mathcal{A}\Big(g_1, g_2, g_1^{s_l}, g_2^{1/s_l}, g_2^{r_{l,j}}, g_2^{s_l r_{l,j}}, g_2^{s_l+1/r_{l,j}} \;\Big|\; j \in \mathcal{M}_{\mathrm{s}}^l\Big) = \left(g_2^{r_*}, g_2^{s_l r_*}, g_2^{s_l+1/r_*}\right)\Bigg]
\end{aligned}$$

is at least the probability of the left-hand side of (4.10). Since

$$\Pr\left[A_1 \vee A_2\right] = \Pr[A_1] + \Pr[A_2] - \Pr\left[A_1 \wedge A_2\right]$$

for events A_1 and A_2, $|\mathcal{U}| \leq q_{\mathrm{e}}$ and $|\mathcal{M}_{\mathrm{s}}^l| \leq q_{\mathrm{s}}$, we have

$$\begin{aligned}
&\varepsilon_1 + \varepsilon_0 + \varepsilon_2 \\
&> \Pr\left[\mathcal{B}\left(g_1, g_2, g_1^{\alpha}, g_2^{r_i}, g_2^{\alpha+1/r_i} \;\middle|\; i \in \mathcal{U}\right) = \left(g_1^{r_*}, g_2^{\alpha+1/r_*}\right)\right] + \Pr\left[\mathcal{A}\left(g_2, g_2^{x}, g_2^{y}\right) = g_1^{xy}\right] \\
&\quad + \Pr\left[\mathcal{A}\Big(g_1, g_2, g_1^{s_l}, g_2^{1/s_l}, g_2^{r_{l,j}}, g_2^{s_l r_{l,j}}, g_2^{s_l+1/r_{l,j}} \;\Big|\; j \in \mathcal{M}_{\mathrm{s}}^l\Big) = \left(g_2^{r_*}, g_2^{s_l r_*}, g_2^{s_l+1/r_*}\right)\right] \\
&\geq \varepsilon\left(1 - \frac{2(q_{\mathrm{e}}+q_{\mathrm{s}})}{p}\right)
\end{aligned}$$

This is a contradiction of the (t_0, ε_0)-DH Assumption, $(q_1, t_1, \varepsilon_1)$-Assumption II and $(q_2, t_2, \varepsilon_2)$-Assumption III in the theorem. Therefore, our protocol is $(q_{\mathrm{e}}, q_{\mathrm{s}}, t, \varepsilon)$-strongly EUF-ID-CMA.

If $\mathcal{B}$ outputs a valid forgery to the game from Simulator Description with the probability ε in time t, then $\mathcal{A}$ succeeds in the Assumption III game, or $\mathcal{B}$ succeeds in the DH game or Assumption III game, in time $t + O((q_e + q_s)T)$ with the probability $\varepsilon(1 - 2(q_e + q_s)/p)$. Thus we need assumptions that $t_i \geq t + O((q_e + q_s)T)$ $(i = 0, 1, 2)$. This means that $t \leq \min(t_0, t_1, t_2) - O((q_e + q_s)T)$.

This completes the proof of Theorem 4.1. □

The security proof in the Boneh–Boyen signature scheme [2] and the Waters signature scheme [18] are done in a skillful manner, each using a mathematical assumption. Thus, it seems difficult to extend to strongly EUF-ID-CMA IBS schemes. On the other hand, our IBS scheme satisfies the strongest security. One of the reasons is that its proof is straight-forward with three mathematical assumptions and the one-way isomorphism f.

5. Conclusions

In this paper, we proposed a solution of the open problem suggested by Paterson–Schuldt [13], namely we proposed a strongly EUF-ID-CMA IBS scheme without random oracles for the first time. Security was based on the difficulty to solve three problems related to the Diffie–Hellman problem and a one-way isomorphism.

References

[1] F. Bao, R.H. Deng and H. Zhu, *Variations of Diffie–Hellman Problem,* Proc. ICICS2003, Springer-Verlag, 2003.

[2] D. Boneh and X. Boyen, *Short signatures without random oracles,* Proc. Eurocrypt 2004, LNCS 3027, pp.56–73, 2004.

[3] D. Boneh and X. Boyen, *Efficient selective-ID secure identity based encryption without random oracles,* Proc. Eurocrypt 2004, LNCS 3027, pp.223–238, 2004.

[4] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing,* Proc. Crypto 2001, LNCS 2139, pp.213–229, 2001.

[5] D. Boneh, E. Shen and B. Waters, *Strongly unforgeable signatures based on computational Diffie–Hellman,* Proc. PKC 2006, LNCS 3958, pp.229–240, 2006.

[6] J. Camenisch and A. Lysyanskaya, *Signature schemes and anonymous credentials from bilinear maps,* Proc. Crypto 2004, LNCS 3152, pp.56–72, 2004.

[7] J.C. Choon and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups ,* Proc. PKC 2003, LNCS 2567, pp.18–30, 2003.

[8] R. Cramer and V. Shoup, *Signature schemes based on the strong RSA assumption,* ACM TISSEC, vol.3, pp.161–185, 2000. Extended abstract Proc. 6th ACM CCS, 1999.

[9] W. Diffie and M.E. Hellman, *New directions in cryptography,* IEEE Trans. Inf. Theory, vol.22, pp.644–654, 1976.

[10] R. Gennaro, S. Halevi and T. Rabin, *Secure hash-and-sign signatures without the random oracle,* Proc. Eurocrypt 1999, LNCS 1592, pp.123–139, 1999.

[11] F. Hess, *Efficient identity based signature schemes based on pairings,* In Selected Areas in Cryptography-SAC'02, LNCS 2595, pp.310–324, 2003.

[12] K.G. Paterson, *ID-based signatures from pairings on elliptic curves,* Cryptology ePrint Archive, available at `http://eprint.iacr.org/2002/004/`.

[13] K.G. Paterson and J.C.N. Schuldt, *Efficient Identity-based signatures secure in the standard model,* Proc. ACIS 2006, LNCS 4058, pp.207–222, 2006.

[14] R. Sakai, K. Ohgishi and M. Kasahara, *Cryptosystems based on pairing,* In SCIS 2000, Okinawa, Japan, 2000.

[15] T. Saito, F. Hoshino, S. Uchiyama and T. Kobayashi, *Candidate one-way functions on non-supersingular elliptic curves,* IEICE Trans. Fundamentals, vol.E89, pp.144–150, 2006.

[16] C. Sato, T. Okamoto and E. Okamoto, *Sender authenticated key agreements without random oracles,* Proc. ICCIT 2007, IEEE CS Press, pp.2156–2162, 2007.

[17] A. Shamir, *Identity-based cryptosystems and signature schemes,* Proc. Crypto'84, LNCS 196, pp.47–53, 1984.

[18] B. Waters, *Efficient identity-based encryption without random oracles,* Proc. Eurocrypt 2005, LNCS 3027, pp.223–238, 2005.

[19] F. Zhang, X. Chen, W. Susilo, and Y. Mu, *A new short signature scheme without random oracles from bilinear pairings,* Proc. Vietcrypt 2006, LNCS 4341, pp.67–80, 2006.

Chifumi Sato
C4 Technology, Inc., Meguro Tokyu Bldg., 5th Floor, 2–13–17 Kamiosaki Shinagawa-Ku Tokyo, 141–0021, Japan
e-mail: `c-sato@c4t.jp`

Takeshi Okamoto
Graduate School of Systems and Information Engineering, University of Tsukuba, 1–1–1 Tennodai Tsukuba-shi, Ibaraki, 305–8573, Japan
e-mail: `ken@risk.tsukuba.ac.jp`

Eiji Okamoto
Graduate School of Systems and Information Engineering, University of Tsukuba, 1–1–1 Tennodai Tsukuba-shi, Ibaraki, 305–8573, Japan
e-mail: `okamoto@risk.tsukuba.ac.jp`