Strongly Unforgeable ID-based Signatures Without Random Oracles

Chifumi Sato[1], Takeshi Okamoto[2], and Eiji Okamoto[3]

[1] SBI Net Systems Co., Ltd., Meguro Tokyu Bldg., 5th Floor, 2–13–17 Kamiosaki Shinagawa-Ku Tokyo, 141–0021, Japan
c-sato@sbins.co.jp

[2] Department of Computer Science, Faculty of Health Sciences, Tsukuba University of Technology, 4–12–7 Kasuga Tsukuba-shi, Ibaraki, 305–0821, Japan
ken@cs.k.tsukuba-tech.ac.jp

[3] Graduate School of Systems and Information Engineering, University of Tsukuba, 1–1–1 Tennodai Tsukuba-shi, Ibaraki, 305–8573, Japan
okamoto@risk.tsukuba.ac.jp

Abstract. In this paper, we construct a strongly unforgeable ID-based signature scheme without random oracles.[4] The signature size of our scheme is smaller than that of other schemes based on varieties of the Diffie–Hellman problem or the discrete logarithm problem. The security of the scheme relies on the difficulty to solve three problems related to the Diffie–Hellman problem and a one-way isomorphism.

Keywords: Digital signatures, ID-based signatures, Strong unforgeability, Standard models

1 Introduction

In 1984, Shamir [20] introduced the concept of ID-based cryptosystems, 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 [20]. Later, many IBS schemes were presented in [19, 16, 13, 8].

For (ID-based) signatures [12, 9, 4, 7, 22, 21, 6, 17] or ID-based encryptions [3, 21], constructing schemes whose security can be proved without random oracles is one of the most important themes of study, since commonly used hash functions such as MD5 or SHA-1 are not random oracles.

It is known that strongly unforgeable IBS schemes can be constructed with the approach of attaching certificates to strongly unforgeable (non-ID-based) signatures. This approach is mentioned in passing within several papers [10, 2, 11].

[4] An extended abstract of this paper appears in Proceedings of ISPEC 2009, LNCS 5451, pp.35–46, Springer-Verlag, 2009.

We can construct strongly unforgeable IBS schemes without random oracles by applying the approach to strongly unforgeable signature schemes without random oracles such as the Boneh–Boyen [4], the Zhang–Chen–Susilo–Mu [22], the Camenisch–Lysyanskaya [7], the Okamoto [15] or the Boneh–Shen–Waters [6]. However, these constructions need at least six signature parameters to include a public key of the signer and two ordinary signatures (one from the signer and one from the PKG).

Also, Huang–Wong–Zhao [14] proposed a general method to transform (weakly) unforgeable IBS schemes into strongly unforgeable ones by attaching strong one-time signatures. Therefore, this enables us to construct strongly unforgeable IBS schemes without random oracles by applying it on them to any unforgeable ones such as the Paterson–Schuldt [17]. However, in this transformation, signature sizes of the IBS scheme depend on the public key size and signature size of the underlying strong one-time signature scheme. Almost all the current one-time signature schemes suffer from a drawback that these signature sizes are quite large in practice. Note that a strongly unforgeable signature scheme (in the sense of Definition 2 in [14]) is also a strong one-time signature scheme (Definition 3 in [14]). However, by using a strongly unforgeable signature scheme such as [4, 22, 7, 15, 6] instead of the one-time signature, these constructions also need at least six signature parameters.

In this paper, we propose a strongly unforgeable IBS scheme without random oracles, with five signature parameters. The security of the scheme relies on the difficulty to solve three problems related to the Diffie–Hellman (DH) problem, and a one-way isomorphism that no PPT adversary can find the inverse one. The signature size of our scheme is smaller than that of other schemes based on varieties of the DH problem or the discrete logarithm problem.[5] One of the reasons why the number of parameters can be reduced from six to five is that our scheme is directly constructed without applying [10, 2, 11] or [14].

The paper is organized in the following way. In Section 2, we prepare for the construction of our scheme, 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 strong unforgeability in Section 4, and discuss efficiency in Section 5. We provide conclusions in Section 6.

[5] Currently, the most practical strongly unforgeable signature schemes [12, 9] without random oracles are constructed based on the Strong RSA assumption. It is known that each component in the parameters of the signature and the public key generated by these schemes needs to be at least 1024-bits in size. On the other hand, it is sufficient to be 160-bits in size for signature schemes constructed based on the discrete logarithm problem (including varieties of the DH problem) over elliptic curves. In this paper, we only consider such schemes.

2 Preliminaries

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

2.1 One-Way Isomorphism and Bilinear Map

The following definitions are due to [18, 5]. 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 $\mathbb{G}_2$;
- $f\colon \mathbb{G}_2 \to \mathbb{G}_1$ 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 Co-Diffie–Hellman Problem

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

$$(g_1, g_2, g_2^x, g_2^y)$$

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

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

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

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.

2.3 ID-based Signature Schemes

The definition of the IBS scheme in this section is due to [17]. 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, and is performed by the PKG.

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`.

The parameters in Sign and Verify are used in a different order later on. These four 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 Strong Unforgeability

The definition of the strong unforgeability in this section is due to [4, 6, 17]. In particular, Paterson–Schuldt [17] defined the unforgeability and the strong unforgeability. However, their construction of the IBS scheme satisfied only the unforgeability.

Strong unforgeability 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 private key d_i corresponding to the public key ID_i issued by $\mathcal{A}$. 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 first running Extract to obtain the private key d_i of ID_i, and then running Sign to generate a signature $\sigma_{i,j}$ of $(\mathrm{ID}_i, M_{i,j})$, and sending $\sigma_{i,j}$ to $\mathcal{A}$.

Output: Finally $\mathcal{A}$ outputs $(\mathrm{ID}_*, M_*, \sigma_*)$. If σ_* is a valid signature of (ID_*, M_*) according to Verify, $\mathrm{ID}_* \notin \{\mathrm{ID}_i\}$ for Extract Queries and $(\mathrm{ID}_*, M_*, \sigma_*) \notin \{(\mathrm{ID}_i, M_{i,j}, \sigma_{i,j})\}$ for Signature Queries, 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 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 unforgeable, 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

$$\Pr\left[\mathcal{A}\left(g_1, g_2, g_1^x, g_2^{r_i}, g_2^{x+1/r_i} \middle| \ i = 1, \ldots, q\right) = \left(g_1^{r_*}, g_2^{x+1/r_*}\right) \middle| \begin{array}{l} r_* \in \mathbb{Z}_p^* , \\ r_* \notin \{r_1, \ldots, r_q\} \end{array}\right] \geq \varepsilon \ ,$$

where the probability is over the choice $g_1 \in_\mathrm{R} \mathbb{G}_1,\ g_2 \in_\mathrm{R} \mathbb{G}_2$, $x, r_1, \ldots, r_q \in_\mathrm{R} \mathbb{Z}_p^*$, 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

$$\Pr\Big[\mathcal{A}\left(g_1, g_2, g_1^x, g_2^{1/x}, g_2^{r_i}, g_2^{xr_i}, g_2^{x+1/r_i} \,\Big|\, i = 1, \ldots, q\right) \\ = \left(g_2^{r_*}, g_2^{xr_*}, g_2^{x+1/r_*}\right) \Big| \begin{array}{l} r_* \in \mathbb{Z}_p^* \ , \\ r_* \notin \{r_1, \ldots, r_q\} \end{array} \Big] \geq \varepsilon \ ,$$

where the probability is over the choice $g_1 \in_{\mathrm{R}} \mathbb{G}_1,\ g_2 \in_{\mathrm{R}} \mathbb{G}_2,\ x, r_1, \ldots, r_q \in_{\mathrm{R}} \mathbb{Z}_p^*$, 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.

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 [18], on multiplicative cyclic groups constructed on non-supersingular elliptic curves. Security of our scheme is essentially based on the co-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 strong unforgeability 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 `master-key` is MK and the public parameter are

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

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: Given `params`, (ID, M) and $\sigma = (\sigma_1, \ldots \sigma_5)$, verify

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

If the equalities hold the result is `valid`; otherwise the result is `invalid`.

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 1. *Suppose that the* (t_0, ε_0)*-co-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 unforgeable, 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* $\mathbb{G}_2$*.*

An outline of our proof is as follows. Suppose that there exists an adversary, $\mathcal{A}$, who 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 unforgeable 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 co-DH assumption and the Assumption III.

Proof. Suppose that there exists an adversary, $\mathcal{A}$, who $(q_\mathrm{e}, q_\mathrm{s}, t, \varepsilon)$-breaks our IBS scheme. 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.

4.1 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

$$(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, f, g_1, g_2, g_1^{\alpha}, u', U, v', V)$$

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, $\mathcal{U} := \mathcal{U}_\mathrm{e} \cup \mathcal{U}_\mathrm{s}$, 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

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

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

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

(4.1-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:

$$
\begin{aligned}
(d_{i,1}, d_{i,2}) &:= \left((g_2^{s_i})^{X_i}, g_2^{\alpha + 1/s_i} \right) & (2)\\
&= \left(g_2^{\overline{s_i}}, g_2^{\alpha} \cdot \left(g_2^{X_i} \right)^{1/\overline{s_i}} \right) \\
&= \left(g_2^{\overline{s_i}}, g_2^{\alpha} \cdot \left(u' \prod_{k=1}^{n_1} u_k^{\mathrm{id}_{i,k}} \right)^{1/\overline{s_i}} \right) & (3)
\end{aligned}
$$

and sends it to $\mathcal{A}$. Here $\overline{s_i} := s_i X_i \bmod p$ ($i \in \mathcal{U}_{\mathrm{e}}$). (Notice that, by eliminating all $s_i \in_{\mathrm{R}} \mathbb{Z}_p^*$ in (2), we can regard all $\overline{s_i} \in_{\mathrm{R}} \mathbb{Z}_p^*$ as random numbers in (3).)

– **Signature Queries:** The adversary $\mathcal{A}$ adaptively issues Signature Queries $(\mathrm{ID}_i, M_{i,j})$ $\left(i \in \mathcal{U}_{\mathrm{s}}, j \in \mathcal{M}_{\mathrm{s}}^i\right)$. Assume that X_i is from (1) for $i \in \mathcal{U}_{\mathrm{s}}$ and

$$
Y_{i,j} := y' + \sum_{k=1}^{n_2} m_{i,j,k}\ y_k\ , \tag{4}
$$

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

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

(4.1-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 $(\mathrm{ID}_i, M_{i,j})$:

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

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

Output: The adversary $\mathcal{A}$ outputs $(\mathrm{ID}_*, M_*, \sigma_*)$ such that $\sigma_* = (\sigma_{*,1}, \ldots, \sigma_{*,5}) \in \mathbb{G}_2^5$ is a valid signature of (ID_*, M_*), $\mathrm{ID}_* \notin \{\mathrm{ID}_i \mid i \in \mathcal{U}_\mathrm{e}\}$ and $(\mathrm{ID}_*, M_*, \sigma_*) \notin \left\{(\mathrm{ID}_i, M_{i,j}, \sigma_{i,j}) \mid i \in \mathcal{U}_\mathrm{s}, j \in \mathcal{M}_\mathrm{s}^i\right\}$.

Artificial Abort: Assume that

$$X_* := x' + \sum_{k=1}^{n_1} \mathrm{id}_{*,k}\ x_k\ ,$$

$$Y_* := y' + \sum_{k=1}^{n_2} m_{*,k}\ y_k\ , \tag{5}$$

where $\mathrm{ID}_* := (\mathrm{id}_{*,1}, \ldots, \mathrm{id}_{*,n_1}) \in \{0,1\}^{n_1}$ and $M_* := (m_{*,1}, \ldots, m_{*,n_2}) \in \{0,1\}^{n_2}$. If $\mathrm{ID}_* \neq \mathrm{ID}_i$ 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 $i \in \mathcal{U}_\mathrm{s}$ and $j \in \mathcal{M}_\mathrm{s}^i$, then $\mathcal{B}$ aborts this game.

4.2 Analysis

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

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

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

Since σ_* is `valid`, we assume that

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

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

(4.2-1) 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.

(4.2-2) Otherwise (i.e. $X_* \not\equiv 0 \pmod{p}$).
(4.2-2.1) Suppose that $\mathrm{ID}_* \notin \{\mathrm{ID}_i \mid i \in \mathcal{U}_\mathrm{e}\}$ (which is an assumption of the strong unforgeability) and $(\mathrm{ID}_*, \overline{s_*}) \notin \{(\mathrm{ID}_i, \overline{s_i}) \mid i \in \mathcal{U}_\mathrm{s}\}$. Then, it is sufficient to consider

$$\begin{aligned}\Pr\Big[&\mathcal{A}\Big(g_1, g_2, g_1^{\alpha}, g_2^{x'}, g_2^{x_1}, \ldots, g_2^{x_{n_1}}, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}},\\ &g_2^{X_i}, g_2^{Y_{i,j}}, g_2^{\overline{s_i}}, g_2^{\overline{r_{i,j}}}, g_2^{\overline{s_i}\ \overline{r_{i,j}}}, g_2^{\alpha+X_i/\overline{s_i}}, g_2^{\overline{s_i}+Y_{i,j}/\overline{r_{i,j}}} \Big|\ i \in \mathcal{U}_\mathrm{s}, j \in \mathcal{M}_\mathrm{s}^i\Big)\\ &= \Big(g_2^{X_*}, g_2^{Y_*}, g_1^{\overline{s_*}}, g_2^{\overline{r_*}}, g_2^{\overline{s_*}\ \overline{r_*}}, g_2^{\alpha+X_*/\overline{s_*}}, g_2^{\overline{s_*}+Y_*/\overline{r_*}}\Big)\Big]\ ,\end{aligned} \tag{6}$$

in the case that $\mathcal{A}$ knows all $g_2^{\overline{s_i}}$ $(= d_{i,1})$. This means that $\mathcal{U} = \mathcal{U}_\mathrm{e} = \mathcal{U}_\mathrm{s}$. Suppose that the probability (6) $\geq \varepsilon'$ for some $\varepsilon' \leq \varepsilon$.

Then the probability (6) can be reduced to a contradiction of either the co-DH assumption or Assumption II. A more elaborate proof is proposed in Appendix A.
(4.2-2.2) 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

$$\begin{aligned}\Pr\Big[&\mathcal{A}\Big(g_1, g_2, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{l,j}}, g_1^{\overline{s_l}}, g_2^{1/\overline{s_l}}, g_2^{\overline{r_{l,j}}}, g_2^{\overline{s_l}\ \overline{r_{l,j}}}, g_2^{\overline{s_l}+Y_{l,j}/\overline{r_{l,j}}} \Big|\ j \in \mathcal{M}_\mathrm{s}^l\Big)\\ &= \Big(g_2^{Y_*}, g_2^{\overline{r_*}}, g_2^{\overline{s_l}\ \overline{r_*}}, g_2^{\overline{s_l}+Y_*/\overline{r_*}}\Big)\Big]\end{aligned} \tag{7}$$

in the case that $\mathcal{A}$ knows $x', x_1, \ldots, x_{n_1}$ and g_2^{α}. Suppose that the probability (7) $\geq \varepsilon''$ for $\varepsilon' + \varepsilon'' = \varepsilon$.

Then the probability (7) can be reduced to a contradiction of either the co-DH assumption or Assumption III. A more elaborate proof is proposed in Appendix B.

A proof of the limited range of values $(q_\mathrm{e}, q_\mathrm{s}, t, \varepsilon)$ is proposed in Appendix C. Therefore, we proved Theorem 1. □

5 Efficiency

In this section, we consider efficiency of strongly unforgeable IBS schemes without random oracles.

Huang–Wong–Zhao [14] proposed a general method to transform unforgeable IBS schemes into strongly unforgeable ones by attaching strong one-time signatures. Table 1 shows efficiency of IBS schemes from the Huang–Wong–Zhao [14]. For $(x_\mathrm{r}, y_\mathrm{r})$ of the row in the table, x_r represents the number of signature

Table 1. Efficiency of IBS schemes from the transformation in Huang–Wong–Zhao [14]

Strong one-time signatures / Unforgeable IBS schemes	[4] (4; 1)	[22] (4; 2)	[7] (5; 4)	[15] (4; 2)	[6] (4; 2)
Paterson–Schuldt [17] (3, 3)	7/4	7/5	8/7	7/5	7/5

Table 2. Efficiency of IBS schemes from the transformation in [10, 2, 11]

Signature schemes $\mathcal{S}'$ / Certificates (signature) schemes $\mathcal{S}$	[4] (4; 1)	[22] (4; 2)	[7] (5; 4)	[15] (4; 2)	[6] (4; 2)
Boneh–Boyen [4] (2, 1)	6/2	6/3	7/5	6/3	6/3
Zhang–Chen–Susilo–Mu [22] (2, 2)	6/3	6/4	7/6	6/4	6/4
Camenisch–Lysyanskaya ver.A [7] (3, 4)	7/5	7/6	8/8	7/6	7/6
Okamoto [15] (3, 2)	7/3	7/4	8/6	7/4	7/4
Boneh–Shen–Waters [6] (3, 2)	7/3	7/4	8/6	7/4	7/4

parameters and y_{r} that of the bilinear maps. For $(x_{\mathrm{c}}; y_{\mathrm{c}})$ of the column, x_{c} the number of signature parameters and public keys, and y_{c} that of the bilinear maps. For $x_{\mathrm{t}}/y_{\mathrm{t}}$ in the table, x_{t} $(= x_{\mathrm{c}} + x_{\mathrm{r}})$ the number of signature parameters for each strongly unforgeable IBS scheme; and y_{t} $(= y_{\mathrm{c}} + y_{\mathrm{r}})$ that of the bilinear maps. Notice that we count the number of the signature parameters to be small. However, these constructions need at least six signature parameters.

Also, it is known that strongly unforgeable IBS schemes can be constructed with the approach of attaching certificates to strongly unforgeable (non-ID-based) signatures. Table 2 shows efficiency of IBS schemes from this construction in [10, 2, 11]. Here, $(x_{\mathrm{r}}, y_{\mathrm{r}})$ of the row, $(x_{\mathrm{c}}; y_{\mathrm{c}})$ of the column and $x_{\mathrm{t}}/y_{\mathrm{t}}$ in this table mean the numbers such as in Table 1.

All these constructions need at least six signature parameters. In our scheme of Section 3.2, it is sufficient to be five. On the other hand, our scheme is inefficient since the bilinear map is used six times during one iteration of verification in the scheme.

6 Conclusions

In this paper, we proposed a strongly unforgeable IBS scheme without random oracles, with five signature parameters, based on three problems related to the DH problem and a one-way isomorphism. However, our scheme is inefficient since the bilinear map (the pairing) is used six times during one iteration of verification in the scheme. Our next step is to propose more efficient schemes with the same security (or we have a possibility that the six times have not been a problem by a future study of the computation process rate of the bilinear map).

References

1. F. Bao, R. H. Deng, and H. Zhu. Variations of Diffie–Hellman problem. In *ICICS* 2003*, LNCS* 2836, pages 301–312. Springer-Verlag, 2003.
2. M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. In *EUROCRYPT* 2004*, LNCS* 3027, pages 268–286. Springer-Verlag, 2004.
3. D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In *EUROCRYPT* 2004*, LNCS* 3027, pages 223–238. Springer-Verlag, 2004.
4. D. Boneh and X. Boyen. Short signatures without random oracles. In *EUROCRYPT* 2004*, LNCS* 3027, pages 56–73. Springer-Verlag, 2004.
5. D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In *CRYPTO* 2001*, LNCS* 2139, pages 213–229. Springer-Verlag, 2001.
6. D. Boneh, E. Shen, and B. Waters. Strongly unforgeable signatures based on computational Diffie–Hellman. In *Public Key Cryptography* 2006*, LNCS* 3958, pages 229–240. Springer-Verlag, 2006.
7. J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *CRYPTO* 2004*, LNCS* 3152, pages 56–72. Springer-Verlag, 2004.
8. J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie–Hellman groups. In *Public Key Cryptography* 2003*, LNCS* 2567, pages 18–30. Springer-Verlag, 2003.
9. R. Cramer and V. Shoup. Signature schemes based on the strong RSA assumption. In *ACM Conference on Computer and Communications Security*, pages 46–51, 1999.
10. Y. Dodis, J. Katz, S. Xu, and M. Yung. Strong key-insulated signature schemes. In *Public Key Cryptography* 2002*, LNCS* 2567, pages 130–144. Springer-Verlag, 2003.
11. D. Galindo, J. Herranz, and E. Kiltz. On the generic construction of identity-based signatures with additional properties. In *ASIACRYPT* 2006*, LNCS* 4284, pages 178–193. Springer-Verlag, 2006.
12. R. Gennaro, S. Halevi, and T. Rabin. Secure hash-and-sign signatures without the random oracle. In *EUROCRYPT* 1999*, LNCS* 1592, pages 123–139. Springer-Verlag, 1999.
13. F. Hess. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptography (SAC* 2002*), LNCS* 2595, pages 310–324. Springer-Verlag, 2002.
14. Q. Huang, D. S. Wong, and Y. Zhao. Generic transformation to strongly unforgeable signatures. In *ACNS* 2007*, LNCS* 4521, pages 1–17. Springer-Verlag, 2007.
15. T. Okamoto. Efficient blind and partially blind signatures without random oracles. In *TCC* 2006*, LNCS* 3876, pages 80–99. Springer-Verlag, 2006.
16. K. G. Paterson. ID-based signatures from pairings on elliptic curves. Cryptology ePrint Archive, Report 2002/004, 2002. `http://eprint.iacr.org/`.
17. K. G. Paterson and J. C. N. Schuldt. Efficient identity-based signatures secure in the standard model. In *ACISP* 2006*, LNCS* 4058, pages 207–222. Springer-Verlag, 2006.
18. T. Saito, F. Hoshino, S. Uchiyama, and T. Kobayashi. Candidate one-way functions on non-supersingular elliptic curves. *IEICE Transactions*, 89-A(1):144–150, 2006.
19. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *SCIS* 2000, Okinawa, Japan, 2000.

20. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO' 84, LNCS* 196, pages 47–53. Springer-Verlag, 1984.
21. B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT* 2005*, LNCS* 3027, pages 114–127. Springer-Verlag, 2005.
22. F. Zhang, X. Chen, W. Susilo, and Y. Mu. A new signature scheme without random oracles from bilinear pairings. In *VIETCRYPT* 2006*, LNCS* 4341, pages 67–80. Springer-Verlag, 2006.

A A Continuation of the proof from (4.2-2.1)

(A-2.1.1) Assume that there exists a number $l \in \mathcal{U}$ such that $s_* = s_l$. In (6), if $\mathcal{A}$ knows all $\overline{s_i}, \overline{r_{i,j}}$ $(i \in \mathcal{U}_{\mathrm{s}}, j \in \mathcal{M}_{\mathrm{s}}^i)$ 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 (6). Also, since $X_*/\overline{s_*} \equiv X_l/\overline{s_l} \pmod p$, we replace the third component 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 components. Thus $\mathcal{A}$ has an advantage of ε' in solving

$$\mathcal{A}\left(g_1, g_2, g_2^{x'}, g_2^{x_1}, \ldots, g_2^{x_{n_1}}, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{X_i}, g_2^{Y_{i,j}} \,\middle|\, i \in \mathcal{U}_{\mathrm{s}}, j \in \mathcal{M}_{\mathrm{s}}^i\right) = g_1^{X_*/X_l} \quad (8)$$

where the problem is over the choice $g_2 \in_{\mathrm{R}} \mathbb{G}_2$, $x', x_1, \ldots, x_{n_1}, y', y_1, \ldots, y_{n_2} \in_{\mathrm{R}} \mathbb{Z}_p^*$, X_i $(i \in \mathcal{U})$ in (1), X_* in (5), $Y_{i,j}$ $(i \in \mathcal{U}_{\mathrm{s}}, j \in \mathcal{M}_{\mathrm{s}}^i)$ in (4), Y_* in (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 $g_2^{X_l}, g_2^{x_1}, \ldots, g_2^{x_{n_1}}$ (or u', U), $\mathrm{ID}_i (i \in \mathcal{U}), \mathrm{ID}_*$, and eliminates these parameters from (8). Also, since $g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{i,j}} (i \in \mathcal{U}_{\mathrm{s}}, j \in \mathcal{M}_{\mathrm{s}}^i)$ are unrelated to the output $g_1^{X_*/X_l}$, 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 (8), $\mathcal{A}$ has an advantage of ε' in solving

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

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 $x' \in_{\mathrm{R}} \mathbb{Z}_p^*$ 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

$$\mathcal{A}\left(g_1, g_2, g_2^{y}, g_2^{h}\right) = g_1^{y/h} \ ,$$

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

$$\mathcal{A}\left(g_1, g_2, g_2^{y}, g_2^{h}\right) = g_1^{yh} \ .$$

where the problem 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 co-DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$ with a non-negligible probability.

(A-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 (6). Also, considering the pair

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

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 (6). These mean that the probability (6) can be deformed to a contradiction of Assumption II.

B A Continuation of the proof from (4.2-2.2)

(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 $k \in \mathcal{M}_{\rm s}^l$ such that $r_* = r_{l,k}$. In (7), if $\mathcal{A}$ knows the all $\overline{r_{l,j}}$ $(j \in \mathcal{M}_{\rm s}^l)$ and $\overline{s_l} \in \mathbb{Z}_p^*$, then we can eliminate

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

from (7). Also, since $Y_*/\overline{r_*} \equiv Y_{l,k}/\overline{r_{l,k}} \pmod p$, we replace the second component 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 components. Thus $\mathcal{A}$ has an advantage of ε'' in solving

$$\mathcal{A}\left(g_1, g_2, g_2^{y'}, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{l,j}} \middle| \ j \in \mathcal{M}_{\rm s}^l \right) = \left(g_2^{Y_*}, g_2^{Y_*/Y_{l,k}} \right) , \qquad (9)$$

where the problem is over the choice $g_2 \in_{\rm R} \mathbb{G}_2$, $y', y_1, \ldots, y_{n_2} \in_{\rm R} \mathbb{Z}_p^*$, $Y_{l,j} (j \in \mathcal{M}_{\rm s}^l)$ in (4), Y_* in (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 (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 (9), $\mathcal{A}$ has an advantage of ε'' in solving

$$\mathcal{A}\left(g_1, g_2, g_2^{y_1}, \ldots, g_2^{y_{n_2}}, g_2^{Y_{l,k}} \right) = g_2^{K_{l,k,*}/Y_{l,k}} .$$

Such as (A-2.1.1), this means that $\mathcal{A}$ solves the co-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 (7) can be deformed to a contradiction of Assumption III.

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

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

(B-2.2.2.1) Assume that $c \neq |\mathcal{M}_\mathrm{s}^l|$ 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 co-DH problem in $(\mathbb{G}_2, \mathbb{G}_1)$ with a non-negligible probability.

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

C The Limited Range of Values $(q_\mathrm{e}, q_\mathrm{s}, t, \varepsilon)$

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

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

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

$$\begin{aligned}
&\Pr\left[\bigcap_{i\in\mathcal{U}}\left(X_i \overset{(p)}{\not\equiv} 0 \cap X_* \overset{(p)}{\not\equiv} X_i\right) \cap \bigcap_{j\in\mathcal{M}_\mathrm{s}^l}\left(Y_{l,j} \overset{(p)}{\not\equiv} 0 \cap Y_* \overset{(p)}{\not\equiv} Y_{l,j}\right),\ \mathcal{A}\ (q_\mathrm{e}, q_\mathrm{s}, t, \varepsilon)\text{-breaks } \mathcal{S}\right] \\
&\quad\geq \varepsilon\left(1 - \frac{2(q_\mathrm{e} + q_\mathrm{s})}{p}\right) \qquad (10)
\end{aligned}$$

in the proposed scheme $\mathcal{S}$. From (4.2-1) and (4.2-2), the probability

$$\Pr\Big[\mathcal{B}\left(g_1, g_2, g_1^{\alpha}, g_2^{r_i}, g_2^{\alpha+1/r_i}\Big|\ i \in \mathcal{U}\right) = \left(g_1^{r_*}, g_2^{\alpha+1/r_*}\right) \cup\ \mathcal{A}\left(g_1, g_2, g_2^{x}, g_2^{y}\right) = g_1^{xy}$$
$$\cup\ \mathcal{A}\Big(g_1, g_2, g_1^{s_l}, g_2^{1/s_l}, g_2^{r_{l,j}}, g_2^{s_l r_{l,j}}, g_2^{s_l+1/r_{l,j}}\Big|\ j \in \mathcal{M}_{\mathrm{s}}^{l}\Big) = \left(g_2^{r_*}, g_2^{s_l r_*}, g_2^{s_l+1/r_*}\right)\Big]$$
$$(\geq \varepsilon = \varepsilon' + \varepsilon'')$$

is at least the probability of the left-hand side of (10). Since

$$\Pr\left[A_1 \cup A_2\right] = \Pr[A_1] + \Pr[A_2] - \Pr\left[A_1 \cap A_2\right]$$

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

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

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

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