Interdisciplinary Information Sciences Vol. 25, No. 1 (2019) 59–66

ISSN 1340-9050 print/1347-6157 online
DOI 10.4036/iis.2019.R.01

Lossy Identification Schemes from Decisional RSA

Shingo HASEGAWA* and Shuji ISOBE

Center for Information Technology in Education, Tohoku University, Sendai 980-8576, Japan

Lossy identification schemes derive tightly secure signature schemes via the Fiat–Shamir transformation. There exist several instantiations of lossy identification schemes by using several cryptographic assumptions. In this paper, we propose a new construction of the lossy identification scheme from the decisional RSA assumption which are introduced by Groth. Our lossy identification scheme has an efficient response algorithm because it requires no modular exponentiation.

KEYWORDS: signature scheme, lossy identification scheme, Fiat–Shamir transformation, decisional RSA

1. Introduction

The Fiat–Shamir transformation [7] is a general method to construct secure and efficient signature schemes from three-move identification schemes. There exist many signature schemes constructed by using this method [8, 9, 11, 14–16, 18, 20]. For the security of signatures derived by the Fiat–Shamir transformation, Abdalla, An, Bellare and C. Namprempre [1] showed that the signature scheme constructed by this method is existentially unforgeable against the chosen message attack in the random oracle model [5] if and only if the underlying identification scheme is secure against the passive impersonation attack. Moreover, they also showed that the security reduction of such signature schemes is *loose*. Namely the success probability of the reduction looses some polynomial factor because the security reduction allows the success probability of the attacker to be multiplied by the polynomial factor. This means that one must choose a large security parameter in order to ensure the security in practical.

In order to solve this problem, Abdalla, Fouque, Lyubaschevsky and Tibouchi [3] introduced the notion of the lossy identification schemes. Lossy identification schemes can be transformed into signature schemes which have a tight security reduction by the Fiat–Shamir transformation, where the tightness means that the security reduction allows no such significant loss as the polynomial factor. They proposed some instantiations of lossy identification schemes based on the short discrete logarithm assumption, the ring-LWE assumption and the subset sum assumption, respectively. Following their work, Abdalla, Ben Hamouda and Pointcheval [2] constructed lossy identification schemes from the several integer factoring-based cryptographic assumptions, such as the ϕ-hiding assumption [6], the QR assumption, the RSA assumption and the DCR assumption [19]. Hasegawa and Isobe [12] proposed a lossy identification scheme by using the subgroup decision assumption [4]. They also proposed another lossy identification scheme based on the DCR assumption by applying the construction of the subgroup decision-based scheme.

In this paper, we propose a new instantiation of lossy identification schemes. Our scheme is constructed based on the decisional RSA assumption which is introduced by Groth [10]. We consider the decisional RSA assumption over a specific type of composites which we call the DRSA composite. A DRSA composite N is a composite of the form $N = PQ$ of distinct primes P and Q, where $P = 2pp' + 1$ and $Q = 2qq' + 1$ with distinct primes p, q, p' and q'. In this case, the group $\mathbb{QR}_N$ of quadratic residues modulo N can be decomposed as $\mathbb{QR}_N = \mathbb{G}_1 \times \mathbb{G}_2$ where $\mathbb{G}_1$ and $\mathbb{G}_2$ are the unique subgroups of order $p'q'$ and pq, respectively. The decisional RSA assumption intuitively says that a uniformly random element from $\mathbb{QR}_N$ is computationally indistinguishable to the one from the subgroup $\mathbb{G}_1$. Employing the the decisional RSA assumption, Groth [10] constructed a homomorphic public key encryption, and Mei, Li, Lu and Jia [17] proposed the chosen ciphertext secure public key encryption, respectively.

Our lossy identification scheme based on the decisional RSA assumption has an efficient response algorithm as well as the DCR-based scheme by [12]. This is because our scheme needs no modular exponentiation in its response algorithm. Moreover, the size of public keys of our scheme is smaller than that of the DCR-based scheme of [12], and is as same as integer factoring-based schemes by [2]. These facts suggest that our scheme is one of the most efficient schemes among lossy identification schemes based on the integer factoring-based assumptions.

We note that a preliminary version of this paper was appeared in ISITA2014 [13]. This is a full version.

Received June 1, 2018; Accepted March 18, 2019; J-STAGE Advance published May 21, 2019
A part of this work is supported by JSPS KAKENHI Grant Number 18K11288.
*Corresponding author. E-mail: hasegawa@cite.tohoku.ac.jp

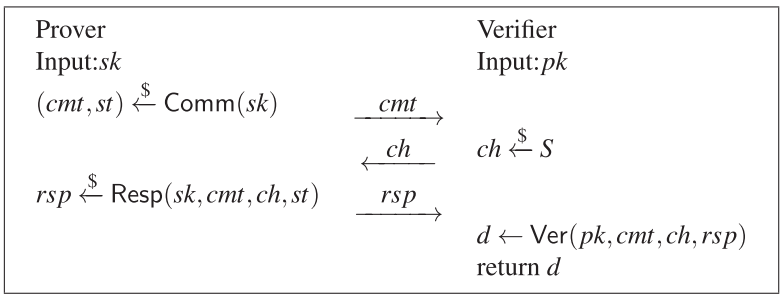

Fig. 1. Description of a lossy identification scheme ID.

2. Preliminaries

In this section, we describe definitions and notions which are used in this paper. The descriptions follow those in the literature [3, 12].

Let $\mathbb{N}$ and $\mathbb{Z}$ be the sets of natural numbers and the ring of rational integers, respectively. For any $N \in \mathbb{N}$, $\mathbb{Z}_N$ denotes the residue ring $\mathbb{Z}/N\mathbb{Z}$, and $\mathbb{Z}_N^\times$ denotes the multiplicative group of units in $\mathbb{Z}_N$, respectively. ϕ denotes Euler's phi function. For a finite set A, $|A|$ denotes the number of elements in A. Let G be a group. For an element $g \in G$, $\langle g \rangle$ denotes the cyclic subgroup generated by g. Throughout the paper, we denote by $\lambda \in \mathbb{N}$ the security parameter. A function $\varepsilon(\lambda)$ is said to be *negligible* if for any polynomial p, there exists a constant $\lambda_0 \in \mathbb{N}$ such that $\varepsilon(\lambda) < 1/p(\lambda)$ for any $\lambda \geq \lambda_0$.

We write $a \xleftarrow{\$} A$ to denote sampling an element a uniformly at random from the set A. Let $\mathcal{A}$ be a probabilistic polynomial time (PPT) Turing machine. We write $y \xleftarrow{\$} \mathcal{A}(x)$ to denote that $\mathcal{A}$ outputs y on its execution for the input x. The output y is distributed according to the internal randomness of $\mathcal{A}$.

Let X and Y be two random variables over the same finite set S. The statistical distance $\Delta(X, Y)$ between X and Y is defined by $\Delta(X, Y) = \frac{1}{2}\sum_{s \in S} |\Pr[X = s] - \Pr[Y = s]|$. Let $\mathcal{X} = \{X_\lambda\}$ and $\mathcal{Y} = \{Y_\lambda\}$ be any families of distributions indexed by the security parameter λ, where X_λ and Y_λ are random variables over a finite set S_λ. We say that $\mathcal{X}$ and $\mathcal{Y}$ are *statistically indistinguishable* if $\Delta(X_\lambda, Y_\lambda)$ is negligible in λ. Specifically, if for any sufficiently large λ, $\Delta(X_\lambda, Y_\lambda) \leq \varepsilon(\lambda)$ holds for some function ε, we say that $\mathcal{X}$ and $\mathcal{Y}$ are *statistically ε-close*. For any PPT machine $\mathcal{A}$, we define the *advantage* $\mathsf{Adv}_{\mathcal{A},\mathcal{X},\mathcal{Y}}$ of $\mathcal{A}$ in distinguishing $\mathcal{X}$ and $\mathcal{Y}$ by $\mathsf{Adv}_{\mathcal{A},\mathcal{X},\mathcal{Y}}(1^\lambda) = |\Pr[\mathcal{A}(1^\lambda, X_\lambda) = 1] - \Pr[\mathcal{A}(1^\lambda, Y_\lambda) = 1]|$. We say that $\mathcal{X}$ and $\mathcal{Y}$ are *computationally indistinguishable* if $\mathsf{Adv}_{\mathcal{A},\mathcal{X},\mathcal{Y}}$ is negligible in λ for any PPT $\mathcal{A}$. We say that $\mathcal{X}$ and $\mathcal{Y}$ are *computationally ε-close* if $\mathsf{Adv}_{\mathcal{A},\mathcal{X},\mathcal{Y}}(1^\lambda) \leq \varepsilon(\lambda)$ for any PPT $\mathcal{A}$ and for any sufficiently large λ.

2.1 Lossy identification schemes

A lossy identification scheme is a three-move protocol between two PPT machines, called the *prover* and the *verifier*. A lossy identification scheme has two key generation algorithms. The one is the normal key generation algorithm KG, which outputs a pair of a public key and a secret key on the input security parameter. Another is the lossy key generation algorithm LKG. When a public key is generated by LKG, it has no corresponding secret key. Moreover, when a prover uses a lossy key, he cannot convince the verifier with non-negligible probability. The formal definition of lossy identification schemes is given as follows.

Definition 2.1 (Lossy Identification Schemes [3]). A lossy identification scheme ID is defined by a tuple $(\mathsf{KG}, \mathsf{LKG}, \mathsf{Comm}, S, \mathsf{Resp}, \mathsf{Ver})$ such that

- KG is the normal key generation algorithm which takes a security parameter 1^λ as the input and outputs a pair (pk, sk) of a public key pk and a secret key sk.
- LKG is the lossy key generation algorithm which takes a security parameter 1^λ as the input and output a lossy public key pk.
- Comm is the prover algorithm which takes sk as the input and outputs a commitment string cmt and a state string st.
- S is the space from which the verifier chooses a challenge string ch. The length of the challenge ch is determined by λ.
- Resp is the prover algorithm which takes a tuple (sk, cmt, ch, st) as the input and outputs a response string rsp.
- Ver is the deterministic algorithm which takes a tuple (pk, cmt, ch, rsp) as the input and outputs 1 or 0 to indicate accept or reject, respectively.

The protocol ID is depicted in Fig. 1.

Note that LKG is not used in the actual execution of the protocol. LKG is used merely in the security analysis of the protocol.

$\mathsf{Tr}^{\mathsf{ID}}_{pk,sk,\lambda}()$

Generate a transcript (cmt, ch, rsp) as follows:

(1) $(cmt, st) \xleftarrow{\$} \mathsf{Comm}(sk)$;
(2) $ch \xleftarrow{\$} S$;
(3) $rsp \xleftarrow{\$} \mathsf{Resp}(sk, cmt, ch, st)$;
(4) If $\mathsf{Ver}(pk, cmt, ch, rsp) = 0$, set $(cmt, ch, rsp) \leftarrow (\perp, \perp, \perp)$.
(5) return (cmt, ch, rsp)

Fig. 2. The description of the transcript oracle.

$\mathsf{Exp}^{\mathrm{los-imp-pa}}_{\mathsf{ID},\mathcal{A}}(\lambda)$

(1) $pk \xleftarrow{\$} \mathsf{LKG}(1^\lambda)$;
(2) $(cmt, st) \xleftarrow{\$} \mathcal{A}^{\widetilde{\mathsf{Tr}}^{\mathsf{ID}}_{pk,\lambda}}(pk)$;
(3) $ch \xleftarrow{\$} S$;
(4) $rsp \xleftarrow{\$} \mathcal{A}(ch, st)$.
(5) return $\mathsf{Ver}(pk, cmt, ch, rsp)$

Fig. 3. The description of $\mathsf{Exp}^{\text{los-imp-pa}}_{\mathsf{ID},\mathcal{A}}$.

We say that a public key pk is *normal* when it is generated by KG. Otherwise when pk is generated by LKG, we say that it is *lossy*. Note that a single key pk can be generated by both KG and LKG in general.

Following [1, 3], we associate to ID, λ and each (pk, sk) generated by $\mathsf{KG}(1^\lambda)$ a randomized *transcript generation oracle* $\mathsf{Tr}^{\mathsf{ID}}_{pk,sk,\lambda}()$ that takes no input and outputs a random transcript (cmt, ch, rsp) of an "honest" execution of the protocol on (pk, sk). The description of $\mathsf{Tr}^{\mathsf{ID}}_{pk,sk,\lambda}()$ is given in Fig. 2.

Definition 2.2 ([3]). A lossy identification scheme ID is said to be $(\rho, \varepsilon_S, \varepsilon_K, \varepsilon_L)$-lossy if it satisfies the following conditions.

- ρ-completeness: For every security parameter λ and every pair of normal keys $(pk, sk) \xleftarrow{\$} \mathsf{KG}(1^\lambda)$, $\mathsf{Ver}(pk, cmt, ch, rsp) = 1$ with probability at least $\rho(\lambda)$ when $(cmt, ch, rsp) \xleftarrow{\$} \mathsf{Tr}^{\mathsf{ID}}_{pk,sk,\lambda}()$.
- ε_S-simulatability: One can assign a PPT algorithm $\widetilde{\mathsf{Tr}}^{\mathsf{ID}}_{pk,\lambda}$ to each pair (pk, λ), where pk is any normal public key which can be generated by $\mathsf{KG}(1^\lambda)$, in a way that the distributions of the honest transcript $\{\mathsf{Tr}^{\mathsf{ID}}_{pk,sk,\lambda}\}$ and of the simulated transcript $\{\widetilde{\mathsf{Tr}}^{\mathsf{ID}}_{pk,\lambda}\}$ are statistically ε_S-close, where (pk, sk) is any pair that can be generated by $\mathsf{KG}(1^\lambda)$.
- ε_K-key indistinguishability: For every security parameter λ, the two distributions $D_{0,\lambda} = \{pk \mid (pk, sk) \xleftarrow{\$} \mathsf{KG}(1^\lambda)\}$ and $D_{1,\lambda} = \{pk \mid pk \xleftarrow{\$} \mathsf{LKG}(1^\lambda)\}$ are computationally ε_K-close.
- ε_L-lossiness: Consider the experiment $\mathsf{Exp}^{\text{los-imp-pa}}_{\mathsf{ID},\mathcal{A}}$ in Fig. 3 between an adversary $\mathcal{A}$ and a hypothetical challenger. Then we say that $\mathcal{A}$ *ε_L-succeeds the passive impersonation attack with respect to lossy keys* if $\Pr[\mathsf{Exp}^{\text{los-imp-pa}}_{\mathsf{ID},\mathcal{A}}(\lambda) = 1] \geq \varepsilon_L(\lambda)$. We say that the scheme ID is ε_L-lossy if there exists no adversary $\mathcal{A}$ (that may be computationally unbounded) which ε_L-succeeds the passive impersonation attack with respect to lossy keys.

2.2 Decisional RSA assumption

We use four distinct odd primes p, q, p' and q'. We call $N = PQ$, where $P = 2pp' + 1$ and $Q = 2qq' + 1$ are primes, a DRSA composite. For a DRSA composite N, $\mathbb{QR}_N$ denotes the set of quadratic residues modulo N. Then $\mathbb{QR}_N$ is a cyclic group of order $pqp'q'$. $\mathbb{QR}_N$ has unique subgroups $\mathbb{G}_1$ of order $p'q'$ and $\mathbb{G}_2$ of order pq, respectively. By the definition of the DRSA composite, p, q, p' and q' are distinct primes. Therefore, it follows that $\mathbb{QR}_N$ can be decomposed as a direct product $\mathbb{QR}_N = \mathbb{G}_1 \times \mathbb{G}_2$.

The decisional RSA assumption in [10] is defined over $\mathbb{Z}_N^\times$ of RSA composite order. In this paper, we restrict ourselves to the case where N is a DRSA composite. The formal definition is as follows.

We first define a group generator $\mathcal{G}_{\mathsf{DRSA}}$. $\mathcal{G}_{\mathsf{DRSA}}$ takes a security parameter 1^λ as the input and outputs a tuple (p, q, p', q') such that $N = PQ$ is a DRSA composite with $P = 2pp' + 1$ and $Q = 2qq' + 1$. We assume that the bit length of each p, q, p', q' are $\ell(\lambda)$ for some polynomial $\ell(\lambda) \geq \lambda$. This requirement is needed so that both $1/pq$ and $1/p'q'$ are negligible in λ.

Definition 2.3 (Decisional RSA Assumption). Let families of distributions $\{X_{\mathsf{DRSA},\lambda}\}$ and $\{Y_{\mathsf{DRSA},\lambda}\}$ be $X_{\mathsf{DRSA},\lambda} = \{(N, y) \mid (p, q, p', q') \xleftarrow{\$} \mathcal{G}_{\mathsf{DRSA}}(1^\lambda), P = 2pp' + 1, Q = 2qq' + 1, N = PQ, y \xleftarrow{\$} \mathbb{G}_1\}$ and $Y_{\mathsf{DRSA},\lambda} = \{(N, y) \mid (p, q, p', q') \xleftarrow{\$} \mathcal{G}_{\mathsf{DRSA}}(1^\lambda), P = 2pp' + 1, Q = 2qq' + 1, N = PQ, y \xleftarrow{\$} \mathbb{QR}_N\}$. We say that the $\varepsilon_{\mathsf{DRSA}}$-decisional RSA assumption holds for $\mathcal{G}_{\mathsf{DRSA}}$ if $\{X_{\mathsf{DRSA},\lambda}\}$ and $\{Y_{\mathsf{DRSA},\lambda}\}$ are computationally $\varepsilon_{\mathsf{DRSA}}$-close.

3. Lossy Identification Schemes Based on the Decisional RSA Assumption

3.1 Basis

We propose a new lossy identification scheme based on the decisional RSA assumption. First, we introduce new families of distributions $\{\tilde{X}_{\mathsf{DRSA},\lambda}\}$ and $\{\tilde{Y}_{\mathsf{DRSA},\lambda}\}$ such that the indistinguishability between them is derived from the decisional RSA assumption.

$\tilde{X}_{\mathsf{DRSA},\lambda}$ is defined by

$$\tilde{X}_{\mathsf{DRSA},\lambda} = \{(N,g,y) \mid (p,q,p',q') \xleftarrow{\$} \mathcal{G}_{\mathsf{DRSA}}(1^\lambda),$$
$$P = 2pp'+1, Q = 2qq'+1, N = PQ, g \xleftarrow{\$} G_1, y \xleftarrow{\$} \mathbb{G}_1\} \tag{3.1}$$

where G_1 is the set of all generators of $\mathbb{G}_1$. $\tilde{Y}_{\mathsf{DRSA},\lambda}$ is defined by

$$\tilde{Y}_{\mathsf{DRSA},\lambda} = \{(N,g,y) \mid (p,q,p',q') \xleftarrow{\$} \mathcal{G}_{\mathsf{DRSA}}(1^\lambda),$$
$$P = 2pp'+1, Q = 2qq'+1, N = PQ, g \xleftarrow{\$} G_1, y \xleftarrow{\$} \mathbb{QR}_N \setminus \mathbb{G}_1\}. \tag{3.2}$$

Note that a generator of $\mathbb{G}_1$ can be uniformly sampled efficiently with overwhelming probability [10]. Namely, the uniform sampling of a generator fails with some negligible probability η. The decisional RSA assumption implies the indistinguishability between $\tilde{X}_{\mathsf{DRSA},\lambda}$ and $\tilde{Y}_{\mathsf{DRSA},\lambda}$ as shown in the following lemma.

Lemma 3.1. *Let $\eta'(\lambda) = 1/(2^{2\lambda-2}(1-\eta(\lambda)))$. Assume that the $\varepsilon_{\mathsf{DRSA}}$-decisional RSA assumption holds for $\mathcal{G}_{\mathsf{DRSA}}$. Then the families of distributions $\{\tilde{X}_{\mathsf{DRSA},\lambda}\}$ and $\{\tilde{Y}_{\mathsf{DRSA},\lambda}\}$ defined as above are computationally $\varepsilon'_{\mathsf{DRSA}}$-close for $\mathcal{G}_{\mathsf{DRSA}}$, where $\varepsilon'_{\mathsf{DRSA}}(\lambda) = \varepsilon_{\mathsf{DRSA}}(\lambda)/(1-\eta(\lambda)) + \eta'(\lambda)$.*

Proof. We first recall that $N = PQ = (2pp'+1)(2qq'+1)$, $|\mathbb{Z}_N^\times| = \phi(N) = 4pqp'q'$, $|\mathbb{QR}_N| = |\mathbb{Z}_N^\times|/4 = pqp'q'$ and $|\mathbb{G}_1| = p'q'$. Since (P,Q) is generated by $\mathcal{G}_{\mathsf{DRSA}}(1^\lambda)$, it follows that $2^{\ell-1} \le p,q,p',q' \le 2^\ell - 1$ and hence $2^{2\ell-1} < P, Q < 2^{2\ell+1}$, where $\ell = \ell(\lambda)$.

Let $Y'_{\mathsf{DRSA},\lambda} = \{(N,y) \mid (p,q,p',q') \xleftarrow{\$} \mathcal{G}_{\mathsf{DRSA}}(1^\lambda), P = 2pp'+1, Q = 2qq'+1, N = PQ, y \xleftarrow{\$} \mathbb{QR}_N \setminus \mathbb{G}_1\}$. We first show that the distribution $\{Y'_{\mathsf{DRSA},\lambda}\}$ is computationally close to $\{X_{\mathsf{DRSA},\lambda}\}$ under the DRSA assumption by the following technical claim.

Claim 3.2. If the $\varepsilon_{\mathsf{DRSA}}$-decisional RSA assumption holds for $\mathcal{G}_{\mathsf{DRSA}}$, then $\{X_{\mathsf{DRSA},\lambda}\}$ and $\{Y'_{\mathsf{DRSA},\lambda}\}$ are computationally ε'-close where $\varepsilon'(\lambda) = \varepsilon_{\mathsf{DRSA}}(\lambda) + 1/2^{2\lambda-2}$.

Proof. Let U be the uniform distribution over $\mathbb{QR}_N$ and let U' be the uniform distribution over $\mathbb{QR}_N \setminus \mathbb{G}_1$. Then, the statistical distance $\Delta(U,U')$ between U and U' over $\mathbb{QR}_N$ is

$$\begin{aligned}
2\Delta(U,U') &= \sum_{x \in \mathbb{QR}_N} |\Pr[U=x] - \Pr[U'=x]| \\
&= \sum_{x \in \mathbb{G}_1} |\Pr[U=x] - \Pr[U'=x]| + \sum_{x \in \mathbb{QR}_N \setminus \mathbb{G}_1} |\Pr[U=x] - \Pr[U'=x]| \\
&= \sum_{x \in \mathbb{G}_1} \left| \frac{1}{|\mathbb{QR}_N|} - 0 \right| + \sum_{x \in \mathbb{QR}_N \setminus \mathbb{G}_1} \left| \frac{1}{|\mathbb{QR}_N|} - \frac{1}{|\mathbb{QR}_N \setminus \mathbb{G}_1|} \right| \\
&= |\mathbb{G}_1| \cdot \frac{1}{|\mathbb{QR}_N|} + 1 - \frac{|\mathbb{QR}_N \setminus \mathbb{G}_1|}{|\mathbb{QR}_N|} \\
&= p'q' \frac{1}{pqp'q'} + 1 - \frac{pqp'q' - p'q'}{pqp'q'} \\
&= \frac{2}{pq},
\end{aligned}$$

and hence $\Delta(U,U') = 1/pq$.

Since $2^{\ell-1} \le p,q$, it holds that $2^{2\ell-2} \le pq$. Then we have $\Delta(U,U') = 1/pq \le 1/2^{2\ell-2} \le 1/2^{2\lambda-2}$. This implies that the statistical distance between $\{Y_{\mathsf{DRSA},\lambda}\}$ and $\{Y'_{\mathsf{DRSA},\lambda}\}$ is bounded by $1/2^{2\lambda-2}$. Then $\{X_{\mathsf{DRSA},\lambda}\}$ and $\{Y'_{\mathsf{DRSA},\lambda}\}$ are computationally ε'-close for $\varepsilon'(\lambda) = \varepsilon_{\mathsf{DRSA}}(\lambda) + 1/2^{2\lambda-2}$ by the triangle inequality. □

We now return to the proof of Lemma 3.1. We prove the lemma by contraposition. Assume that $\{\tilde{X}_{\mathsf{DRSA},\lambda}\}$ and $\{\tilde{Y}_{\mathsf{DRSA},\lambda}\}$ are not computationally $\varepsilon'_{\mathsf{DRSA}}$-close. Then there exists a PPT adversary $\mathcal{A}$ such that

$$\mathsf{Adv}_{\mathcal{A},\{\tilde{X}_{\mathsf{DRSA},\lambda}\},\{\tilde{Y}_{\mathsf{DRSA},\lambda}\}}(1^\lambda) = |\Pr[\mathcal{A}(\tilde{X}_{\mathsf{DRSA},\lambda}) = 1] - \Pr[\mathcal{A}(\tilde{Y}_{\mathsf{DRSA},\lambda}) = 1]| > \varepsilon'_{\mathsf{DRSA}}(\lambda),$$

for infinitely many λ.

We shall construct a PPT adversary $\mathcal{B}$ such that

$$\mathsf{Adv}_{\mathcal{B},\{X_{\mathsf{DRSA},\lambda}\},\{Y'_{\mathsf{DRSA},\lambda}\}}(1^\lambda) = |\Pr[\mathcal{B}(X_{\mathsf{DRSA},\lambda}) = 1] - \Pr[\mathcal{B}(Y'_{\mathsf{DRSA},\lambda}) = 1]| > \varepsilon'(\lambda) = \varepsilon_{\mathsf{DRSA}}(\lambda) + \frac{1}{2^{2\lambda-2}}$$

for all those λ in order to claim that $\{X_{\mathsf{DRSA},\lambda}\}$ and $\{Y'_{\mathsf{DRSA},\lambda}\}$ are not computationally ε'-close. By Claim 3.2, this shows that $\varepsilon_{\mathsf{DRSA}}$-decisional RSA assumption for $\mathcal{G}_{\mathsf{DRSA}}$ fails.

Let (N,y) be a tuple drawn according to $X_{\mathsf{DRSA},\lambda}$ or $Y'_{\mathsf{DRSA},\lambda}$. On input (N,y), $\mathcal{B}$ behaves as follows:

Step 1. Choose a generator $g \xleftarrow{\$} G_1$.

Step 2. Invoke $\mathcal{A}$ on the input (N,g,y) and outputs the output of $\mathcal{A}$.

We show the correctness of $\mathcal{B}$. In **Step 1**, a generator g of $\mathbb{G}_1$ can be sampled uniformly at random from G_1 with the

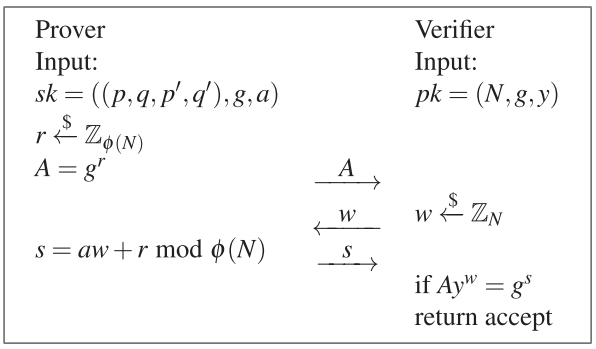

Fig. 4. Description of the lossy identification scheme $\mathsf{ID}_{\mathsf{DRSA}}$.

probability $1 - \eta(\lambda)$. In **Step 2**, the tuple (N, g, y) distributes according to $\tilde{X}_{\mathsf{DRSA},\lambda}$ if and only if the tuple (N, y) distributes according to $X_{\mathsf{DRSA},\lambda}$, and (N, g, y) distributes according to $\tilde{Y}_{\mathsf{DRSA},\lambda}$ if and only if the tuple (N, y) distributes according to $Y_{\mathsf{DRSA},\lambda}$ respectively, provided that g is actually a generator of $\mathbb{G}_1$. Thus we have

$$\begin{aligned}\mathsf{Adv}_{\mathcal{B},\{X_{\mathsf{DRSA},\lambda}\},\{Y'_{\mathsf{DRSA},\lambda}\}}(1^\lambda) &= |\Pr[\mathcal{B}(X_{\mathsf{DRSA},\lambda}) = 1] - \Pr[\mathcal{B}(Y'_{\mathsf{DRSA},\lambda}) = 1]| \\ &\geq |\Pr[\mathcal{A}(\tilde{X}_{\mathsf{DRSA},\lambda}) = 1] - \Pr[\mathcal{A}(\tilde{Y}_{\mathsf{DRSA},\lambda}) = 1]| \cdot \Pr[\text{g is a generator of } \mathbb{G}_1] \\ &> \varepsilon'_{\mathsf{DRSA}}(\lambda) \cdot (1 - \eta(\lambda)) = \varepsilon'(\lambda).\end{aligned}$$

□

3.2 Protocol

We now construct a lossy identification scheme $\mathsf{ID}_{\mathsf{DRSA}} = (\mathsf{KG}, \mathsf{LKG}, \mathsf{Comm}, S, \mathsf{Resp}, \mathsf{Ver})$ as follows. Comm and Ver are performed over the group $\mathbb{Z}_N^\times$. On the other hand, Resp is performed over the ring $\mathbb{Z}_{\phi(N)}$.

- KG takes a security parameter 1^λ as the input. KG generates $(p, q, p', q') \xleftarrow{\$} \mathcal{G}_{\mathsf{DRSA}}(1^\lambda)$, and chooses a generator $g \xleftarrow{\$} G_1$ of $\mathbb{G}_1$ and $a \xleftarrow{\$} \mathbb{Z}_{\phi(N)}$. KG sets $N = (2pp' + 1)(2qq' + 1)$ and $y = g^a$, and outputs $pk = (N, g, y)$ and $sk = ((p, q, p', q'), g, a)$.
- LKG takes a security parameter 1^λ as the input. LKG generates $(p, q, p', q') \xleftarrow{\$} \mathcal{G}_{\mathsf{DRSA}}(1^\lambda)$, and chooses a generator $g \xleftarrow{\$} G_1$ of $\mathbb{G}_1$, a generator f of $\mathbb{G}_2$, $a \xleftarrow{\$} \mathbb{Z}_{\phi(N)}$ and $b \xleftarrow{\$} \mathbb{Z}_{pq}^\times$. LKG sets $N = (2pp' + 1)(2qq' + 1)$ and $y = g^a f^b$, and outputs $pk = (N, g, y)$.
- Comm takes a tuple $((p, q, p', q'), g)$ as the input. Comm picks a random string $r \xleftarrow{\$} \mathbb{Z}_{\phi(N)}$ and sets $A = g^r$. Comm outputs the commitment string $cmt = A$ and the state string $st = r$.
- The space S of the verifier's challenges is $\mathbb{Z}_N$. The challenge string ch is $w \xleftarrow{\$} \mathbb{Z}_N$.
- Resp takes a tuple (a, w, r) as the input and computes $s = aw + r \bmod \phi(N)$. Resp outputs the response string $rsp = s$.
- Ver takes a tuple $((N, g, y), A, w, s)$ as the input and outputs 1 if $Ay^w = g^s$ holds, or outputs 0 if otherwise.

The protocol $\mathsf{ID}_{\mathsf{DRSA}}$ is depicted in Fig. 4.

3.3 Lossy properties of $\mathsf{ID}_{\mathsf{DRSA}}$

We evaluate the parameters $(\rho, \varepsilon_S, \varepsilon_K, \varepsilon_L)$ described in Definition 2.2 for $\mathsf{ID}_{\mathsf{DRSA}}$. For a tuple (p, q, p', q') generated by $\mathcal{G}_{\mathsf{DRSA}}$, we set $N = (2pp' + 1)(2qq' + 1)$, $n = pq$ and $n' = p'q'$. For any natural number k, let U_k denote the uniform distribution over $\mathbb{Z}_k$, U'_k denote the uniform distribution over $\mathbb{Z}_k \setminus \{0\}$, and let $U_k^\times$ denote the uniform distribution over $\mathbb{Z}_k^\times$, respectively. We have the following lemmas.

Lemma 3.3. *There exist negligible functions δ_1 and δ_2 such that for any (p, q, p', q') generated by $\mathcal{G}_{\mathsf{DRSA}}$,*
(1) $(N - \phi(N))/N < \delta_1(\lambda)$,
(2) $(pq - \phi(pq))/pq < \delta_2(\lambda)$,
(3) $1/pq + 1/N < \delta_1(\lambda)$,
for all sufficiently large λ.

Proof. (1) We have $\phi(N) = (P - 1)(Q - 1) = 4pqp'q'$ and $N = (2pp' + 1)(2qq' + 1) > 4pqp'q'$. We may assume without loss of generality that $p < q < p' < q'$. Then,

$$\begin{aligned}\frac{N - \phi(N)}{N} &= \frac{(2pp' + 1)(2qq' + 1) - 4pqp'q'}{(2pp' + 1)(2qq' + 1)} < \frac{2(pp' + qq') + 1}{4pqp'q'} \\ &= \frac{1}{2qq'} + \frac{1}{2pp'} + \frac{1}{4pqp'q'} < \frac{1}{2p^2} + \frac{1}{2p^2} + \frac{1}{4p^4}\end{aligned}$$

$$= \frac{1}{p^2} + \frac{1}{4p^4} \leq \frac{2}{p^2}. \tag{3.3}$$

Since $2^{\ell(\lambda)-1} \leq p$, we have $2/p^2 \leq 1/2^{2\ell(\lambda)-1}$. Thus by letting $\delta_1(\lambda) = 1/2^{2\ell(\lambda)-1}$, we have $(N - \phi(N))/N < \delta_1(\lambda)$.
(2) As in (1), we may assume without loss of generality that $p < q$. Then,

$$\frac{pq - \phi(pq)}{pq} = \frac{pq - (p-1)(q-1)}{pq} = \frac{p+q-1}{pq}$$
$$< \frac{p+q}{pq} = \frac{1}{q} + \frac{1}{p} < \frac{2}{p}. \tag{3.4}$$

Since $2^{\ell(\lambda)-1} \leq p$, we have $(pq - \phi(pq))/pq < \delta_2(\lambda)$, by letting $\delta_2(\lambda) = 1/2^{\ell(\lambda)-2}$.
(3) As in (1), we may assume without loss of generality that $p < q$. Since $N > pq$, we have

$$\frac{1}{pq} + \frac{1}{N} < \frac{2}{pq} < \frac{2}{p^2}. \tag{3.5}$$

Thus we have $1/pq + 1/N < \delta_1(\lambda)$. □

We now use the following convention. Let S and T be sets with $S \subseteq T$ and D be a distribution over S. Then we naturally regard D as a distribution over T in a way that $\Pr[D = x] = 0$ for any $x \in T \setminus S$. For any natural numbers $k_1 < k_2$, we regard $\mathbb{Z}_{k_1} = \{0, 1, \ldots, k_1 - 1\}$ as a subset of $\mathbb{Z}_{k_2} = \{0, 1, \ldots, k_2 - 1\}$.

Lemma 3.4. *Let δ_1 and δ_2 be as given in Lemma 3.3. For sufficiently large λ,*
(1) *$\Delta(U_{\phi(N)}, U_N) < \delta_1(\lambda)$, where $U_{\phi(N)}$ and U_N are regarded as distributions over $\mathbb{Z}_N$,*
(2) *$\Delta(U'_{pq}, U^{\times}_{pq}) < \delta_2(\lambda)$, where U'_{pq} and $U^{\times}_{pq}$ are regarded as distributions over $\mathbb{Z}_{pq} \setminus \{0\}$.*

Proof. For any natural numbers $k_1 < k_2$, it holds that $\Delta(U_{k_1}, U_{k_2}) = 1 - k_1/k_2$, where U_{k_1} and U_{k_2} are regarded as distributions over $\mathbb{Z}_{k_2}$ [12, Lemma 3(2)].
(1) By letting $k_1 = \phi(N)$ and $k_2 = N$, we have

$$\Delta(U_{\phi(N)}, U_N) = 1 - \frac{\phi(N)}{N} = \frac{N - \phi(N)}{N} < \delta_1(\lambda).$$

(2) It holds that $\Delta(U'_{pq}, U^{\times}_{pq}) = \Delta(U_{pq-1}, U_{\phi(pq)})$. Thus, by letting $k_1 = \phi(pq)$ and $k_2 = pq - 1$, we have

$$\Delta(U'_{pq}, U^{\times}_{pq}) = 1 - \frac{\phi(pq)}{pq-1} < 1 - \frac{\phi(pq)}{pq} = \frac{pq - \phi(pq)}{pq} < \delta_2(\lambda).$$

□

Theorem 3.5. *Assume that the $\varepsilon_{\mathsf{DRSA}}$-decisional RSA assumption holds for $\mathcal{G}_{\mathsf{DRSA}}$. Then the protocol $\mathsf{ID}_{\mathsf{DRSA}}$ is $(1, 2\delta_1, \varepsilon'_{\mathsf{DRSA}} + \delta_2, \delta_1)$-lossy, where $\varepsilon'_{\mathsf{DRSA}}$ is as in Lemma 3.1, and δ_1 and δ_2 are the negligible functions in Lemma 3.3.*

Proof. 1-completeness: 1-completeness immediately follows from the construction of $\mathsf{ID}_{\mathsf{DRSA}}$.
$2\delta_1$-simulatability: We construct a transcript simulator $\widetilde{\mathsf{Tr}}^{\mathsf{ID}_{\mathsf{DRSA}}}_{pk,\lambda}()$. Let $pk = (N, g, y)$ be generated by $\mathsf{KG}(1^\lambda)$. Then $\widetilde{\mathsf{Tr}}^{\mathsf{ID}_{\mathsf{DRSA}}}_{pk,\lambda}()$ picks $w, s \xleftarrow{\$} \mathbb{Z}_N$ and outputs (A, w, s), where $A = g^s y^{-w}$. Clearly, $\mathsf{Ver}(pk, A, w, s) = 1$ for this tuple (A, w, s).

Let Δ be the statistical distance between the distribution of the genuine transcript (A, w, s) generated by $\mathsf{Tr}^{\mathsf{ID}_{\mathsf{DRSA}}}_{pk,sk,\lambda}()$ and the one of the simulated transcript generated by $\widetilde{\mathsf{Tr}}^{\mathsf{ID}_{\mathsf{DRSA}}}_{pk,\lambda}()$. We note that s is regarded as a random variable over $\mathbb{Z}_N$, although s is distributed over $\mathbb{Z}_{\phi(N)}$ in the genuine transcript.

We shall show that $\Delta \leq 2\delta_1$. We denote by Δ_A the statistical distance between the distribution of A in the genuine transcript and the one in the simulated transcript. Δ_w and Δ_s are similarily defined, respectively. Then we have $\Delta \leq \Delta_A + \Delta_w + \Delta_s$ by the triangle inequality. Since w is uniformly distributed over $\mathbb{Z}_N$ in both of the genuine and simulated transcripts, we have $\Delta_w = 0$. In the genuine transcript, $s = aw + r \bmod \phi(N)$ is uniformly distributed over $\mathbb{Z}_{\phi(N)}$ since $r \xleftarrow{\$} \mathbb{Z}_{\phi(N)}$. On the other hand, s in the simulated transcript is uniformly distributed over $\mathbb{Z}_N$. Then, Lemma 3.4(1) implies that $\Delta_s = \Delta(U_{\phi(N)}, U_N) < \delta_1$. We next evaluate Δ_A. In the genuine transcript, $A = g^r$ is uniformly distributed over the subgroup $\mathbb{G}_1 = \langle g \rangle$ since $r \xleftarrow{\$} \mathbb{Z}_{\phi(N)}$ and the order $p'q'$ of $\mathbb{G}_1$ divides $\phi(N) = 4pqp'q'$. Consider the distribution of A in the simulated transcript. We have $A = g^s y^{-w} = g^s (g^a)^{-w} = g^{s-aw}$. Since s and w are drawn from $\mathbb{Z}_N$ uniformly and independently at random, $c = s - aw \bmod N$ is uniformly distributed over $\mathbb{Z}_N$. Therefore, the distribution of the simulated A is identical to the distribution of g^c with $c \xleftarrow{\$} \mathbb{Z}_N$. Hence we have $\Delta_A = \Delta(U_{\phi(N)}, U_N)$, and Lemma 3.4(1) implies that $\Delta_A < \delta_1$. Thus we have $\Delta \leq \Delta_A + \Delta_w + \Delta_s < 2\delta_1$.
$(\varepsilon'_{\mathsf{DRSA}} + \delta_2)$-key indistinguishability: We first evaluate the distribution of normal keys. The distribution of public keys generated by $\mathsf{KG}(1^\lambda)$ and $\tilde{X}_{\mathsf{DRSA},\lambda}$ are identical by their definitions.

We next consider the distribution of lossy keys. We show that the distribution of lossy keys and $\tilde{Y}_{\mathsf{DRSA},\lambda}$ are statistically δ_2-close. Since $\mathbb{QR}_N = \mathbb{G}_1 \times \mathbb{G}_2$ with $\mathbb{G}_1 = \langle g \rangle$ and $\mathbb{G}_2 = \langle f \rangle$, $|\mathbb{G}_1| = p'q'$ and $|\mathbb{G}_2| = pq$, any element $x \in \mathbb{QR}_N$ is uniquely expressed as $x = g^a f^b$ with $a \in \mathbb{Z}_{p'q'}$ and $b \in \mathbb{Z}_{pq}$. Thus we have that $x \in \mathbb{G}_1$ if and only if $b = 0$. Now, for the lossy key, $y = g^a f^b$ with $b \xleftarrow{\$} \mathbb{Z}^{\times}_{pq}$. Therefore, the statistical distance $\Delta(U'_{pq}, U^{\times}_{pq})$ equals the statistical

distance between the distribution of lossy keys and $\tilde{Y}_{\mathsf{DRSA},\lambda}$. By Lemma 3.4(2), we have $\Delta(U'_{pq}, U^{\times}_{pq}) < \delta_2$. Namely, the distribution of lossy keys and $\tilde{Y}_{\mathsf{DRSA},\lambda}$ are statistically δ_2-close.

Combining these facts with Lemma 3.1, The statistical distance between the distribution of KG and the one of LKG is $(\varepsilon'_{\mathsf{DRSA}} + \delta_2)$-close. This implies $(\varepsilon'_{\mathsf{DRSA}} + \delta_2)$-key indistinguishability.

δ_1-lossiness: Let $\mathcal{A}$ be any passive impersonation adversary, and let $\mathsf{Succ}_{\mathcal{A}}(\lambda)$ denote the event that the experiment $\mathsf{Exp}^{\text{los-imp-pa}}_{\mathsf{ID}_{\mathsf{DRSA}},\mathcal{A}}(\lambda)$ returns 1. We shall prove that $\delta_3(\lambda) \geq \Pr[\mathsf{Succ}_{\mathcal{A}}(\lambda)]$.

Let $pk = (N, g, y)$ be any lossy public key generated by LKG on the input 1^{λ}. Then $y = g^a f^b$, where $a \in \mathbb{Z}_{\phi(N)}$ and $b \in \mathbb{Z}^{\times}_{pq}$.

We evaluate the probability $\Pr[\mathsf{Succ}_{\mathcal{A}}]$ that the event $\mathsf{Succ}_{\mathcal{A}}$ occurs by estimating the number of the verifier's challenges for which $\mathcal{A}$ can produce a correct response. Since $\langle f \rangle = \mathbb{G}_2$, f is of order $|\mathbb{G}_2| = pq$. If the verifier's challenge $w \in \mathbb{Z}_N$ is a multiple of pq, then we have $f^w = 1$ and hence $y^w = g^{aw} f^{bw} = g^{aw} \in \mathbb{G}_1$. Namely, if the challenge w is a multiple of pq, the lossy key pk acts as normal keys. This means that there exists such a "bad" challenge w in $\mathbb{Z}_N$ with the period pq. Thus we may consider the distribution of y^w with $w \xleftarrow{\$} \mathbb{Z}_{pq}$ instead of with $w \xleftarrow{\$} \mathbb{Z}_N$.

We show that there exist overwhelmingly many challenge strings in $\mathbb{Z}_{pq}$ such that $\mathcal{A}$ cannot produce a correct response for the challenge, even if $\mathcal{A}$ is computationally unbounded and $\mathcal{A}$ can arbitrarily determine his commitment string. We use the following lemma.

Lemma 3.6. *Let $pk = (N, g, y)$ be any lossy public key, where $y = g^a f^b$ with $a \in \mathbb{Z}_{\phi(N)}$ and $b \in \mathbb{Z}^{\times}_{pq}$. Then for any commitment value $A \in \mathbb{QR}_N$ (not necessarily $A \in \mathbb{G}_1$), there exists at most one challenge value $w \in \mathbb{Z}_{pq}$ such that there exists a response $s \in \mathbb{Z}_{pq}$ satisfying $\mathsf{Ver}(pk, A, w, s) = 1$.*

Proof. Assume that $w_1, w_2 \in \mathbb{Z}_{pq}$ are challenges such that $\mathsf{Ver}(pk, A, w_1, s_1) = 1$ and $\mathsf{Ver}(pk, A, w_2, s_2) = 1$ for some $s_1, s_2 \in \mathbb{Z}_{pq}$. Then we have that

$$A = g^{s_1} y^{-w_1} = g^{s_2} y^{-w_2}. \tag{3.6}$$

Since $y = g^a f^b$, it follows from Eq. (3.6) that

$$g^{(s_1 - s_2)} = y^{w_1 - w_2} = g^{a(w_1 - w_2)} f^{b(w_1 - w_2)},$$

and hence

$$f^{b(w_1 - w_2)} = g^{(s_1 - s_2)} \cdot g^{a(w_2 - w_1)}. \tag{3.7}$$

Since $g \in \mathbb{G}_1$ and $f \in \mathbb{G}_2$, the element in Eq. (3.7) is in $\mathbb{G}_1 \cap \mathbb{G}_2 = \{1\}$. b is chosen from $\mathbb{Z}^{\times}_{pq}$. Thus $f^{b(w_1 - w_2)} = 1$ implies $w_1 - w_2 \equiv 0 \pmod{pq}$. We have $w_1 = w_2$ from $w_1, w_2 \in \mathbb{Z}_{pq}$. □

By Lemma 3.6, there is at most one challenge in $\mathbb{Z}_{pq}$ for which $\mathcal{A}$ can produce a correct response s regardless of the choice of the commitment A even if $\mathcal{A}$ is computationally unbounded. Therefore, we have

$$\Pr[\mathsf{Succ}_{\mathcal{A}}(\lambda)] \leq \lceil (N/pq) \rceil / N \leq 1/pq + 1/N < \delta_1(\lambda) \tag{3.8}$$

for any fixed $y = g^a f^b$. □

4. Concluding Remarks

In this paper, we have proposed a new construction of lossy identification scheme based on the decisional RSA assumption. Our decisional RSA-based scheme $\mathsf{ID}_{\mathsf{DRSA}}$ has the efficient response algorithm Resp as well as the DCR-based scheme $\mathsf{ID}_{\mathsf{DCR}}$ in [12], because Resp executes one modular addition and one modular multiplication but no modular exponentiation. Note that other lossy identification schemes based on integer factoring-based assumptions in [2] need modular exponentiation in their response algorithms. Moreover, the size of public keys of $\mathsf{ID}_{\mathsf{DRSA}}$ is smaller than $\mathsf{ID}_{\mathsf{DCR}}$, and as same as integer factoring-based schemes by [2]. This is because $\mathsf{ID}_{\mathsf{DRSA}}$ runs over the group $\mathbb{Z}^{\times}_N$ while $\mathsf{ID}_{\mathsf{DCR}}$ runs over the group $\mathbb{Z}^{\times}_{N^2}$. These facts means that $\mathsf{ID}_{\mathsf{DRSA}}$ is one of the most efficient scheme among lossy identification schemes based on integer factoring-based assumptions.

REFERENCES

[1] Abdalla, M., An, J. H., Bellare, M., and Namprempre, C., "From identification to signatures via the Fiat–Shamir transform: Minimizing assumptions for security and forward-security," *LNCS*, **2332**: 418–433 (2002).

[2] Abdalla, M., Ben Hamouda, F., and Pointcheval, D., "Tighter reductions for forward-secure signature schemes," *LNCS*, **7778**: 292–311 (2013).

[3] Abdalla, M., Fouque, P. A., Lyubashevsky, V., and Tibouchi, M., "Tightly-secure signatures from lossy identification schemes," *LNCS*, **7237**: 572–590 (2012).

[4] Boneh, D., Goh, E. J., and Nissim, K., "Evaluating 2-DNF formulas on ciphertexts," *LNCS*, **3378**: 325–341 (2005).

[5] Bellare, M., and Rogaway, P., "Random oracles are practical: A paradigm for designing efficient protocols," *ACM CCS 1993*, 62–73 (1993).

[6] Cachin, C., Micali, S., and Stadker, M., "Computationally private information retrieval with polylogarithmic communication," *LNCS*, **1592**: 402–414 (1999).
[7] Fiat, A., and Shamir, A., "How to prove yourself: Practical solutions to identification and signature problems," *LNCS*, **263**: 186–194 (1987).
[8] Girault, M., Poupard, G., and Stern, J., "On the fly authentication and signature schemes based on groups of unknown order," *Journal of Cryptology*, **19**: 463–487 (2006).
[9] Goh, E. J., Jarecki, S., Katz, J., and Wang, N., "Efficient signature schemes with tight reductions to the Diffie-Hellman problems," *Journal of Cryptology*, **20**: 493–514 (2007).
[10] Groth, J., "Cryptography in subgroups of $\mathbb{Z}_n^\times$," *LNCS*, **3378**: 50–65 (2005).
[11] Guillou, L. C., and Quisquater, J. J., "A "Paradoxical" identity-based signature scheme resulting from zero-knowledge," *LNCS*, **403**: 216–231 (1990).
[12] Hasegawa, S., and Isobe, S., A lossy identification scheme using the subgroup decision assumption," *IEICE Trans. Fundamentals, Special Section on Discrete Mathematics and Its Applications*, **97-A**: 1296–1306 (2014).
[13] Hasegawa, S., and Isobe, S., "Lossy identification schemes from decision RSA," *ISITA2014*, 143–147 (2014).
[14] Katz, J., and Wang, N., "Efficiency improvements for signature schemes with tight security reductions," *ACM CCS 2003*, 155–164 (2003).
[15] Lyubashevsky, V., "Fiat–Shamir with aborts: Applications to lattice and factoring-based signatures," *LNCS*, **5912**: 598–616 (2009).
[16] Lyubashevsky, V., "Lattice signatures without trapdoors," *LNCS*, **7237**: 738–755 (2012).
[17] Mei, Q., Li, B., Lu, X., and Jia, D., "Chosen ciphertext secure encryption under factoring assumption revisited," *LNCS*, **6571**: 210–227 (2011).
[18] Micali, S., and Reyzin, L., "Improving the exact security of digital signature schemes," *Journal of Cryptology*, **15**: 1–18 (2002).
[19] Paillier, P., "Public-key cryptosystems based on composite degree residuosity classes," *LNCS*, **1592**: 223–238 (1999).
[20] Schnorr, C. P., "Efficient identification and signatures for smart cards," *LNCS*, **434**: 688–689 (1990).