ID-Based Optimistic Fair Exchange Scheme Based on RSA

Taek-Young Youn and Ku-Young Chang

Fairness of exchange is a significant property for secure online transactions, and a fair exchange scheme is a useful tool for ensuring the fairness of exchanges conducted over networks. In this paper, we propose an ID-based optimistic fair exchange scheme based on the RSA function, one which is designed by combining a well-known RSA-based signature scheme and the (naive) RSA function. Note that the main contribution of this paper is to give the first provably secure ID-based fair exchange scheme based on the RSA function, whose security can be proved under fully formalized security models. Our scheme has the following additional strongpoints. The scheme is setup-free; hence, there is no registration step between a user and an arbitrator. Moreover, the proposed scheme is designed in an ID-based setting; thus, it is possible to eliminate the need for certificates and avoid some related problems.

Keywords: Cryptography, ID-based cryptosystem, RSA function, fair exchange, setup-freeness.

I. Introduction

These days, certain basic social activities such as commercial transactions and business communications are more frequently conducted over networks through the use of computers. One significant security requirement for such activities is the fairness of exchange, in the sense that two communicating parties give and take items without allowing either party to gain an advantage through any wrongdoings. The fair exchange scheme is a useful tool for fair activities performed over the Internet that require such a level of security.

A simple way to implement fair exchange schemes is to adopt an arbitrator, who will then aid clients to exchange signatures in a fair manner. In such scenarios, two users may commit their signatures to an arbitrator, who then only forwards them to the intended receivers if the two signatures are valid. This simple approach is not efficient, since the arbitrator should participate in every execution of a fair exchange, even if there is no dispute between users. To overcome this shortcoming, an optimistic fair exchange scheme has been proposed by Asokan and others [1] where an arbitrator only becomes involved in the execution of an exchange if there is a dispute between the two parties. Simply, optimistic fair exchange schemes work as follows. First, each communicating party generates a partial signature and gives it to its communicating partner. When valid partial signatures are exchanged between communicating parties, each party gives additional information to its partner so that the partner can recover the full signature from the already exchanged partial signature. An arbitrator only becomes involved in the protocol when either party refuses to help its partner to obtain the required full signature. The arbitrator's role is to recover a full signature from a partial signature without the assistance of

Manuscript received Apr.15, 2013; revised Nov. 12, 2013; accepted Nov. 21, 2013.

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (Grant No. 2011-0029925).

Taek-Young Youn (taekyoung@etri.re.kr) and Ku-Young Chang (corresponding author, jang1090@etri.re.kr) are with SW·Content Research Laboratory, ETRI, Daejeon, Rep. of Korea.

either party.

Until now, numerous fair exchange schemes have been proposed based on various primitives [1]–[13], and two paradigms have been mainly used for designing fair exchange schemes. One is based on verifiably encrypted signatures [1]–[4], and the other is based on two-party multi-signatures [8]. In [5], Dodis and Reyzin introduced verifiably committed signatures [10]–[12] that generalize verifiably encrypted signatures and two-party multi-signatures. A new paradigm has been proposed based on ID-based signatures [9]. Recently, a designated confirmer signature scheme was used in the design of a fair exchange scheme [7].

Due to the convenience and simplicity of the RSA function, several fair exchange schemes based on the function itself have been proposed, but the greater part of them are insecure or inefficient. The scheme in [14] was broken by Cathalo, Libert, and Quisquater [15]. In [8], a fair exchange scheme based on two-party multi-signatures has been proposed; unfortunately, the scheme is easily breakable at the registration phase [5]. In [16], a simple fair exchange scheme based on ID-based mediated RSA has been proposed [17]. The scheme remains secure, but its security is not proved with formal language. The schemes in [5], [18], and [19] are secure, but they require costly zero-knowledge proofs. In [20], a secure ID-based fair exchange scheme based on the RSA function has been proposed, but its security is not proved under fully formalized security models. In [21]–[22], generic constructions have been proposed that permit us to easily obtain a provably secure fair exchange scheme from a set of component schemes (which are specified in each transform technique) without burdensome security analysis. In [9], an efficient fair exchange scheme has been proposed by combining an RSA signature and a well-known ID-based signature [23].

In 1984, Shamir [24] introduced the notion of identity-based public-key cryptography in an attempt to simplify key management procedures of traditional certificate-based public key infrastructure (PKI) by way of eliminating certificates. Since the first practical ID-based encryption based on bilinear pairings was proposed by Boneh and Franklin [25], a rapid development of ID-based schemes has taken place based on pairing operations [13], [26]–[29], including ID-based fair exchange schemes. Until now, most ID-based fair exchange schemes have been designed based on pairing operations [13], [26], [28]; thus, it is worthy to design ID-based fair exchange schemes without the pairing operation for a variety of primitives. Note that RSA-based schemes are widely used in practice instead of pairing-based schemes due to the convenience and simplicity of the RSA function [30]. Hence, from a practical viewpoint, it is particularly worthwhile designing RSA-based schemes. However, only a small number of schemes based on the RSA function have been proposed, for such schemes are not easy to design.

One desirable property of a fair exchange is its setup-freeness. A fair exchange scheme is called setup-free if there is no registration step between a user and the arbitrator, and a fair exchange is called setup-driven if a user should interact with the arbitrator for registration. As indicated in [21], a setup-free fair exchange is more advantageous than a setup-driven fair exchange. The first setup-free fair exchange scheme was proposed in [3], and several schemes [9]–[12], [21] have since been proposed with the property.

1. Contribution

Until now, several ID-based fair exchange schemes have been proposed, but only a few of these have been designed based on the RSA function. Some fair exchange schemes have been designed using either ID-based encryption or ID-based signatures as a component [9], [16], but they are not ID-based fair exchange schemes. Though generic construction strategies have been proposed in [21]–[22], these techniques are not intended to be used in the design of ID-based fair exchange schemes. In [20], an efficient fair exchange scheme based on the GQ-IBS scheme [23] has been proposed, but the security of the proposed scheme has not yet been verified under fully formalized security models.

In this paper, we propose an efficient ID-based optimistic fair exchange scheme based on the RSA function by combining the GQ-IBS scheme and the (naive) RSA function. We prove the security of the proposed fair exchange scheme under fully formalized security models based on the hardness of the RSA problem. The main contribution of this paper is to provide the first provably secure ID-based fair exchange scheme based on the RSA function, whose security can be proved under fully formalized security models. In [20], an ID-based fair exchange scheme based on the GQ-IBS scheme has been proposed, as in our scheme, but so far attempts to prove its security under fully formalized security models have failed. Some significant points were not considered in the security proof (given in [20]). For example, security against an adversary — who can obtain multiple valid private keys — was not considered in [20], which is one of the fundamental security requirements of ID-based schemes. Moreover, in [20], one trusted party performed two sensitive roles — that of the key-issuer and that of the arbitrator. Note that recently formalized security models separate the role of the key-issuing server (KIS) and the arbitrator since it is desirable to separate these roles for higher security. Therefore, we can say that our scheme is the first provably secure ID-based fair exchange scheme that is designed based on the RSA function and whose security can be

proved under fully formalized security models. The proposed scheme has some strongpoints. Our scheme is suitable for cryptographic engineering practices due to the simplicity of the RSA function, and the scheme is efficient in the sense that it provides almost the same performance compared with the underlying signature scheme. Moreover, the proposed scheme is designed in an ID-based setting; hence, it is possible to eliminate the need for certificates and avoid some related problems. Our scheme also achieves setup-freeness, which means that users can enjoy the fairness provided by the fair exchange scheme without the need to interact with the arbitrator for registration.

The rest of this paper is organized as follows. In section II, we review formal models of ID-based fair exchange schemes. In section III, we design an RSA-based optimistic fair exchange scheme in an ID-based setting. We prove the multi-user security of the scheme in section IV. Finally, section V concludes this paper.

II. Formal Models for ID-Based Fair Exchange Schemes

1. Formal Description

ID-based optimistic fair exchange schemes are composed with the following algorithms:

Setup$^{KIS}(k)$: This algorithm, when given the security parameter k, generates a public-private key pair (pk_k, sk_k), where sk_k is the private key corresponding to pk_k and is issued by KIS.

Setup$^{Arb}(k)$: Given the security parameter k, the algorithm generates a public-private key pair (pk_a, sk_a) for an arbitrator Arb.

Ext(pk_k, sk_k, id): The algorithm generates the private signing key sk for an identity id. The identity id is used as a public key.

Sig(id, sk, pk_k, pk_a, m): The algorithm produces a full signature σ on a message m in the message space M. This algorithm can be probabilistic.

Vfy(id, pk_k, pk_a, σ, m): The algorithm checks the validity of given signature σ. If σ is a valid signature on m, then the algorithm returns T; otherwise F.

PSig(id, sk, pk_k, pk_a, m)$: The algorithm produces a partial signature ω on a message m in M. The algorithm can be probabilistic.

PVfy(id, pk_k, pk_a, ω, m): The algorithm checks the validity of given partial signature ω on m. If ω is valid, then the algorithm returns T; otherwise F.

Open(id, pk_k, pk_a, sk_a, ω, m): Given a partial signature ω on a message m, the algorithm extracts the full signature σ from ω.

A fair exchange protocol requires two properties: correctness and ambiguity. Let ω = PSig(id, sk, pk_k, pk_a, m) be a partial signature and σ = Sig(id,sk,pk_k,pk_a,m) be a full signature of a message m of a user U whose identity is id. The correctness property requires the following conditions:

(1) PVfy(id, pk_k, pk_a, ω, m) = T,

(2) Vfy(id, pk_k, pk_a, σ, m) = T,

(3) Vfy(id, pk_k, pk_a, σ', m) = T,

where σ' = Open(id, pk_k, pk_a, sk_a, ω, m), which is a full signature opened by the algorithm Open upon receiving the partial signature ω. If Open is a deterministic algorithm, then $\sigma' = \sigma$; otherwise (that is, if Open is a probabilistic algorithm) σ' could differ from σ. The ambiguity property requires that σ' and σ are computationally indistinguishable. To measure the ambiguity, it suffices to show that any full signature can be generated by both the signing algorithm "Sig" and the opening algorithm Open.

2. Security Models

We review the security notions for ID-based fair exchange schemes introduced by Zhang and others [28] and rearrange them to give the notions as definitions. Note that the basic concept for the security notions in [28] is not changed.

A secure fair exchange scheme should be secure against malicious signers, verifiers, and an arbitrator. To be secure against malicious signers, it is a necessary requirement that a signer should not be allowed to generate a valid partial signature that cannot then be converted to a full signature. A full-partial signature pair is called unfair if the partial signature is valid but the full signature is not.

Definition 1. Security against signers.

Given an adversary algorithm, say $\mathcal{A}$, the advantage of the algorithm $\mathcal{A}$ is defined as follows:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIG}}(k) = \Pr\left[\begin{array}{l} \mathrm{PVfy}(id, pk_k, pk_a, \omega, m) = T \\ \text{and } \mathrm{Vfy}(id, pk_k, pk_a, \sigma, m) = \mathrm{F}: \\ (pk_k, sk_k) \leftarrow \mathrm{Setup}^{\mathrm{KIS}}(k), \\ (pk_a, sk_a) \leftarrow \mathrm{Setup}^{\mathrm{Arb}}(k), \\ (id, \omega, m) \leftarrow \mathcal{A}^{O_E, O_O}(I, pk_a, sk_a), \\ \sigma \leftarrow \mathrm{Open}(id, pk_k, pk_a, sk_a, \omega, m) \end{array}\right],$$

where O_E and O_O are oracles that respond to extraction and opening queries asked by $\mathcal{A}$, respectively. The set of all identities is denoted by I. The partial signature of a message m is denoted by ω, with σ being the corresponding full signature. An ID-based fair exchange is said to be secure against malicious signers if for any $\mathcal{A}$, its advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIG}}(k)$ is negligible.

For security against verifiers, it is a requirement that no one be allowed to generate a full signature from a partial signature

without asking the arbitrator to open it.

Definition 2. Security against verifiers.

The advantage of $\mathcal{A}$ in computing a full signature from a partial signature, whose full signature was not generated by an opening oracle, is defined as follows:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{VFY}}(k)=\Pr\left[\begin{array}{l}\mathrm{Vfy}(id,pk_k,pk_a,\sigma,m)=T \text{ and}\\ (m,\omega)\in L_P \text{ and } (m,\sigma)\notin L_F:\\ (pk_k,sk_k)\leftarrow \mathrm{Setup}^{\mathrm{KIS}}(k),\\ (pk_a,sk_a)\leftarrow \mathrm{Setup}^{\mathrm{Arb}}(k),\\ (id,\sigma,\omega,m)\leftarrow \mathcal{A}^{O_E,O_P,O_O}(I,pk_k,sk_a)\end{array}\right],$$

where O_E, O_P, and O_O are oracles that respond to extraction, partial signing, and opening queries asked by $\mathcal{A}$, respectively. We assume that $\mathcal{A}$ cannot obtain the private key of the target user. In other words, it is assumed that the private key of the identity *id* was not returned by oracle O_E. The set of all identities is denoted by I, the set of message/signature pairs generated by O_P is denoted by L_P, and the set of all message/signature pairs opened by O_O is denoted by L_F. An ID-based fair exchange is secure against malicious verifiers if for any $\mathcal{A}$, its advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{VFY}}(k)$ is negligible.

For security against an arbitrator, it is a requirement that no single arbitrator be allowed to generate a valid full signature whose partial signature was not generated by a partial signing oracle. Similar to the ordinary notions of unforgeability, we consider the existential unforgedability under adaptive chosen message attacks, which is regarded as a standard security notion for signature schemes.

Definition 3. Security against arbitrators.

The advantage of an adversary $\mathcal{A}$ in existentially forging a full signature whose partial signature was not generated by a partial signing oracle is defined as follows:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{ARB}}(k)=\Pr\left[\begin{array}{l}\mathrm{Vfy}(id,pk_k,pk_a,\sigma,m)=T\\ \text{and } (\omega,m)\notin L:\\ (pk_k,sk_k)\leftarrow \mathrm{Setup}^{\mathrm{KIS}}(k),\\ (pk_a,sk_a)\leftarrow \mathrm{Setup}^{\mathrm{Arb}}(k),\\ (id,\sigma,m)\leftarrow \mathcal{A}^{O_E,O_P}(I,pk_k,pk_a,sk_a)\end{array}\right],$$

where O_E and O_P are respectively oracles that respond to the extraction and partial signing queries asked by $\mathcal{A}$. We assume that the adversary $\mathcal{A}$ cannot obtain the private key of the target user. In other words, it is assumed that the private key of the identity *id* was not returned by the oracle O_E. The set of all identities is denoted by I. Let σ be the full signature of ω on the message m, and let L be the set of signature/message pairs that are generated by O_P. An ID-based fair exchange is secure against a malicious arbitrator $\mathcal{A}$ if its advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{ARB}}(k)$ is negligible.

III. ID-Based Optimistic Fair Exchange Schemes

In this section, we propose an identity-based optimistic fair exchange (ID-OFE) based on the identity-based signature proposed by Guillou and Quisquater (GQ-IBS) [23], [31] and the standard RSA function proposed by Rivest, Shamir and Adleman [32].

1. Scheme

In our scheme, we assume the existence of two trusted entities. One is the trusted KIS that issues the secret key for a user, and the other is the arbitrator Arb that lends support in resolving disputes between clients. Since KIS and Arb are trusted entities, such as a certificate authority is in a PKI, we can use their public keys without certificates as such information can be regarded as a system parameter. In what follows, we denote id_i to be the corresponding identity of user U_i.

Setup$^{\mathrm{KIS}}$. KIS chooses a safe RSA modulus $n_k = p_k q_k$ and a prime e_k such that $gcd(e_k, \phi(n_k)) = 1$, where ϕ is Euler's totient function, and computes $d_k = e_k^{-1} \bmod \phi(n_k)$. The public key is $\{n_k, e_k\}$, and the private key is d_k. The hash function I maps identity information to an element of Z_{nk}^*, and the hash function h maps a string of arbitrary length to an ℓ_h-bit string.

Setup$^{\mathrm{Arb}}$. Arb chooses a safe RSA modulus $n_a = p_a q_a$ and a prime exponent e_a that satisfies $gcd(e_a, \phi(n_a)) = 1$. It then computes $d_a = e_a^{-1} \bmod \phi(n_a)$. The public key is $\{n_a, e_a\}$, and the private key is d_a. The hash function that maps a string of arbitrary length to an element of Z_{na}^* is denoted by H.

Ext. When a user U_i requests their private key, the key-issuing server computes $I_i = I(id_i)$ and $sk_i = I_i^{dk} \bmod n_k$ and then sends sk_i to U_i in a secure way. User U_i can verify the correctness of a given private key by checking $sk_i^{ek} = I(id_i) \bmod n_k$.

PSig and Sig. To make a signature of a message m, U_i chooses three random values a (in Z_{na}^*), a^* (in $\{0, 1\}^{\ell_h}$), and r (in Z_{nk}^*) and then computes $t = r^{ek} \bmod n_k$, $a_e = H(m||a^*||t) \cdot a^{ea} \bmod n_a$, $c = h(m||a_e||t)$, and $b = r \cdot sk_i^c \bmod n_k$. Then, the partial signature and the full signature on m are (a_e, b, c) and (a, a^*, b, c), respectively. Note that two values, m and t, are used for computing a_e and c. We repeatedly use the same inputs to give a way to manage random oracles in Theorem 1. Note that in PSig and Sig, two values, (m and t), are repeatedly used for computing a_e and c to simulate random oracles in the proof of Theorem 1. In the theorem, we can correctly respond to queries on random oracles due to the fact that the same input values are used for generating different messages.

Pvfy. For a given artial signature (a_e, b, c) on m, a verifier computes $t' = b^{ek} \cdot I(id_i)^{-c} \bmod n_k$. Then, the signature is valid

only if the following condition holds: $h(m||a_e||t') = c$.

Vfy. Given a full signature (a, a^*, b, c) on a message m, a verifier computes $t'=b^{ek} \cdot I(id_i)^{-c} \bmod n_k$ and $a_e'=H(m||a^*||t') \cdot a^{ea} \bmod n_a$. The signature is then valid only if the following condition holds: $h(m||a_e'||t')= c$.

Open. When a partial signature (a_e, b, c) generated by U_i on a message m is given, the arbitrator Arb verifies the following condition: $h(m||a_e||t') = c$, where $t'=b^{ek} \cdot I(id_i)^{-c} \bmod n_k$. If the condition holds, Arb chooses a random $a^{*\prime}$ in $\{0,1\}^{\ell_h}$ and recovers a' by computing $a' = (a_e/H(m||a^{*\prime}||t'))^{da} \bmod n_a$. The opened full signature is then $(a', a^{*\prime}, b, c)$.

Note that in the opening algorithm Open the two equations $a=a'$ and $a^*=a^{*\prime}$ are not always guaranteed, which means that the opened full signature is not always the same as the full signature generated by Sig. In other words, a partial signature can be opened to more than one full signature since there are several pairs (u, v) satisfying $a_e=H(m||v||t) \cdot u^{ea} \bmod n_a$. Therefore, when a dispute occurs, the role of the arbitrator is to find a pair $(a', a^{*\prime})$ such that $a_e = H(m||a^{*\prime}||t) \cdot a'^{ea} \bmod n_a$ instead of recovering the fixed pair (a, a^*). Note that this property does not have any influence upon the security of the fair exchange scheme. Note that the scheme in [9] also has the same property and that this did not influence the security of their fair exchange scheme; a fact that has been indicated in [20]. From now on, we do not distinguish between the full signatures generated by Sig and the full signatures generated by Open.

It is easy to show that the proposed scheme achieves the required level of correctness. Let $\omega = (a_e, b, c)$ be a partial signature on a message m of a user U_i (whose identity is id_i), and let $\sigma = (a, a^*, b, c)$ be a full signature for the partial signature. Recall that, as we discussed in section II.1, a fair exchange scheme has to satisfy three conditions for correctness. The proposed scheme achieves correctness since it satisfies the following conditions:

- Condition (1), (2): The full signature σ is correctly verified since

$$t' = b^{ek} \cdot I(id_i)^{-c} = r^{ek} = t \bmod n_k$$

and

$$a_e' = H(m||a^*||t) \cdot a^{ea} = a_e \bmod n_a.$$

For the same reason, the partial signature ω is also verified correctly.

- Condition (3): A valid full signature σ is always recoverable from the partial signature since the RSA function is bijective.

As we briefly stated in section II.1, we can measure the ambiguity of a fair exchange scheme by showing that any full signature can be generated either by the signing algorithm Sig or by the opening algorithm Open. In the proposed scheme, any correctly generated partial signature (a_e, b, c), whose full signature is (a, a^*, b, c), can be transformed to a full signature by opening a' and $a^{*\prime}$ such that $a_e=H(m||a^{*\prime}||t') \cdot a'^{ea} \bmod n_a$, where $t' = b^{ek} \cdot I(id_i)^{-c} \bmod n_k$. The opening algorithm can generate a full signature that is identical to the full signature generated by the signer when the algorithm uses the same a^* (that is, $a^*=a^{*\prime}$). Therefore, the scheme achieves the ambiguity.

2. Performance

Recall that the goal of this paper is to construct an ID-based optimistic fair exchange scheme using the RSA function and that the scheme in [20] is the only known ID-based optimistic fair exchange scheme that is designed based on the RSA function. Hence, to demonstrate the strongpoints of our scheme, we compare our scheme with the previously proposed scheme in terms of security and computational complexity.

Security: The scheme in [20] is designed based on the GQ-IBS scheme, as is our scheme, but the two schemes provide different levels of security. First of all, the security proof given in [20] does not follow well-formalized security models. In particular, the security proof does not take into account an adversary capable of obtaining multiple valid private keys. Note that this security feature is one of the fundamental requirements of ID-based schemes; thus, we can say that the scheme in [20] fails to provide sufficient (provable) security. Moreover, in [20], one trusted party performs two sensitive roles — that of the key-issuing server and that of the arbitrator. For stronger security, it is desirable to separate sensitive roles. For this reason, recently formalized security models separate the role of the key-issuing server and the arbitrator. Therefore, our scheme provides stronger security features than the scheme in [20].

Computational Complexity: The computation costs of the proposed scheme and the scheme in [20] are essentially identical, with insignificant differences due to the structural similarity of the two schemes. Hence, we did not compare their efficiency. The proposed ID-OFE is practical in terms of computational complexity. For each signing and verification, we need three exponentiations. Note that the cost of partial signing is identical to the cost of full signing. We can efficiently compute one exponentiation with e_a by using short RSA exponents such as 3 and $2^{16}+1$. The size of the exponent determines the cost of exponentiation, so the cost of exponentiation with e_a is not a heavy one. Hence, the computational cost of our scheme is comparable to that of the GQ-IBS scheme. When $e_a=3$, we need two additional multiplications for signing and verification compared with the GQ-IBS scheme. The lengths of a partial signature and a full signature are $2\ell_n+\ell_h$ and $2\ell_n+2\ell_h$, respectively, where $\ell_n=|n_k|=|n_a|$. In practice, we used ℓ_n =1,024 and ℓ_h=160 for 1,024-bit RSA modulus.

Additional Useful Properties: The proposed scheme has some desirable properties, including setup-freeness and convenience in development. Since the scheme is setup-free, no interaction with an arbitrator is necessary. A user should interact with the KIS to obtain a private signing key, but the user still does not interact with the arbitrating server. Our scheme is designed by combining the RSA function and GQ signature scheme, and the GQ signature can be implemented by using the RSA function. Due to the simplicity of the RSA function, the proposed scheme is suitable for cryptographic engineering practices.

IV. Security

Prior to proving the security of the proposed ID-OFE scheme, we review the RSA problem that guarantees the security of our scheme.

Definition 4. For a given (N, E, C), the RSA problem is to find the Eth root of C under the modulus N.

In this paper, we consider the case where the public exponent E is a prime number. Note that the RSA problem is still secure even though the public exponent is a prime number.

From now on, we prove the security of the proposed ID-OFE scheme under the hardness of the RSA problem in the random oracle model. We want to emphasis that the security of our scheme is proved in the multi-user setting, where an adversary can make oracle queries for any users including the target victim user. Roughly speaking, in the security proof, oracle queries are not restricted to the target victim user; thus, the security proof is valid in the multi-user setting.

Theorem 1. The proposed ID-OFE scheme is secure under the security notions described in section II.2 if the RSA assumption holds and the advantage of an adversary who breaks the security of our scheme is bounded by $\varepsilon_{RSA}+\varepsilon(k)$, where ε_{RSA} is the maximum advantage of polynomial time adversaries who break the RSA problem and $\varepsilon(k)$ is a negligible function.

Proof. Since we prove the security of our scheme in the random oracle model, we have control over all hash function outputs. For each hash function we maintain a list that stores previous queries; thus, we can respond to a hash query in a previously asked message by retrieving stored data. □

Security against signers: Let (a_e, b, c) be a partial signature on a message m generated by a user U_i whose hashed identity is $I_i = I(id_i)$. If the given partial signature is valid, then we have the following relation:

$$h(m||a_e||t) = c,$$

where $t = b^{ek} \cdot I_i^{-c} \bmod n_k$. Since the RSA encryption is bijective, for any integer a^* in $\{0, 1\}^{\ell h}$, we can compute the element a in Z_{na} as

$$a = (a_e/H(m||a^*||t))^{da} \bmod n_a,$$

and the values a and a^* satisfy the following condition:

$$a_e = H(m||a^*||t) \cdot a^{ea} \bmod n_a.$$

Hence, (a, a^*, b, c) is a valid full signature for the given partial signature. Therefore, all valid partial signatures can be transformed to a valid full signature, so the proposed scheme is unconditionally secure against malicious signers.

Security against Verifiers: Let (N, E, C) be a given challenge to the RSA problem. Recall that the goal is to compute the Eth root of C under the modulus N. Let $\mathcal{A}$ be an algorithm that generates the full signature from a partial signature that was generated by a partial signing oracle, but which has not yet been opened by the opening oracle. To prove security against verifiers, we solve the RSA problem by using the algorithm $\mathcal{A}$. To simulate the attack environment, we choose a safe RSA moduli n_k and a prime e_k such that $gcd(\phi(n_k), e_k) = 1$, and set (n_k, e_k) and (N, E) as the public key for KIS and Arb, respectively. We denote $n_a = N$ and $e_a = E$. We know $\phi(n_k)$ — the secret key of KIS. Throughout the proof, we use a security parameter ℓ to simulate random oracles. The size of the parameters is chosen so that the distribution of $g^j \bmod n_j$ is statistically uniform over Z_{nj}^* for any generator g in Z_{nj}, i in $\{0, 1\}^{\ell}$, and j in $\{a, k\}$. We maintain four lists L_I, L_h, L_H, and L_{PSig} for the three hash functions I, h, and H and for the partial-signing queries PSig, respectively. We respond to each query asked by the algorithm $\mathcal{A}$ as follows:

Hash Query for *I*: We respond to the query for id_i by choosing a random I_i, which is then given to $\mathcal{A}$. We store (id_i, I_i) in L_I, which contains previous queries.

Hash Query for *h*: For the hash query on (m, a_e, t), we choose a random c and give it to $\mathcal{A}$ as the hash value such that $h(m||a_e||t) = c$. We store (m, a_e, t, c) in L_h.

Hash Query for *H*: We respond to a hash query on (m, a^*, t) as follows. If there is a tuple $(m, \bullet, t, \bullet, \bullet)$ in L_H, we retrieve $\{(a_e, b, c), (m, t), \delta\}$ in L_{PSig}, choose a random ζ in $\{0,1\}^{\ell}$ such that $gcd(\delta - \zeta, e_a) = 1$, compute $\gamma = C^{\zeta} \bmod n_a$, give γ to the adversary $\mathcal{A}$, and store $(m, a^*, t, \gamma, \zeta)$ in L_H. Otherwise, we choose a random γ, give it to $\mathcal{A}$, and store $(m, a^*, t, \gamma, 0)$ in L_H.

Extraction Query: For the extraction query on an identity id_i, we retrieve (id_i, I_i) from L_I, compute $sk_i = I_i^{dk} \bmod n_k$, and then give the result to $\mathcal{A}$. Recall that we did not consider the case where id_i is the identity of the target user (victim).

Partial Signing Query: To respond to a partial signing query on a message m of a user U_i, we choose five random values a^* in $\{0, 1\}^{\ell h}$, δ in $\{0, 1\}^{\ell}$, ζ in $\{0,1\}^{\ell}$, r in Z_{nk}^*, and c in $\{0, 1\}^{\ell h}$ such that $gcd(\delta - \zeta, e_a) = 1$, compute $t = r^{ek} \bmod n_k$, $b = r \cdot sk_i^c \bmod n_k$, $\gamma = C^{\zeta} \bmod n_a$, and $a_e = C^{\delta} \bmod n_a$ and set $H(m||a^*||t) = \gamma$ and $h(m||a_e||t) = c$. Since the following relation holds, (a_e, b, c) is a valid partial signature on m: $b^{ek} \cdot I_i^{-c} =$

$(r^{ek} \cdot I_i^c) \cdot I_i^{-c} = r^{ek} = t \bmod n_k$. We store $\{(a_e, b, c), (m, t), \delta\}$ in L_{PSig}. We also store $(m, a^*, t, \gamma, \zeta)$ in L_H.

Full Signing Query: When the algorithm $\mathcal{A}$ requests a full signing query on a message m of a user U_i, we compute a full signature (a, a^*, b, c) according to the description of the ID-OFE scheme. Since we know the private key of KIS, the full-signing query can be successfully simulated.

Opening Query: We respond to an opening query on a partial signature (a_e, b, c) of m as follows. First, we compute $\gamma = a_e^{ea \cdot \eta + 1} \bmod n_a$ and $a = a_e^{-\eta} \bmod n_a$ for a randomly chosen integer η in $\{0, 1\}^{\ell}$. Then, we set $H(m||a^*||t) = \gamma$ for a randomly chosen a^* in $\{0, 1\}^{\ell h}$, store $(m, a^*, t, \gamma, 0)$ in L_H, and then give (a, a^*, b, c) to the adversary as the full signature of the given partial signature. We have $H(m||a^*||t) \cdot a^{ea} = a_e^{ea \cdot \eta + 1} \cdot a_e^{-ea \cdot \eta} = a_e \bmod n_a$, so (a, a^*, b, c) is a valid full signature of the given partial signature.

Let (a, a^*, b, c) be a full signature of a partial signature (a_e, b, c) on a message m of a user U_i, which is returned by the adversary algorithm $\mathcal{A}$. The partial signature (a_e, b, c) was generated by a partial signing oracle but not opened by the opening oracle.

Since (a_e, b, c) is a valid partial signature that was generated by a partial signing oracle, we have the following: $t = b^{ek} \cdot I(id_i)^{-c} \bmod n_k$ and $h(m||a_e||t) = c$, and $\{(a_e, b, c), (m, t), \delta\}$ and $(m, a^*, t, \gamma, \zeta)$ are stored in L_{PSig} and L_H, respectively. Hence, we have

$$C^{\delta} = a_e = H(m||a^*||t) \cdot a^{ea} = C^{\zeta} \cdot a^{ea} \bmod n_a.$$

From the above equation, we have

$$\mathcal{A} = (C^{\delta} \cdot C^{-\zeta})^{da} = C^{da(\delta - \zeta)} \bmod n_a.$$

Since the two values δ and ζ satisfy $gcd(\delta - \zeta, e_a) = 1$, we can find two integers, μ and v, such that $\mu \cdot (\delta - \zeta) + v \cdot e_a = 1$ by performing the extended Euclidean algorithm. Then, using these values, we can recover the e_ath root (Eth root) of C by computing

$$a^{\mu} \cdot C^{v} = C^{da(\mu \cdot (\delta - \zeta))} \cdot C^{da \cdot v \cdot ea} = C^{da} \bmod n_a.$$

Then, we can solve the RSA problem with advantage ε if the advantage of algorithm $\mathcal{A}$ is ε; thus, $\varepsilon < \varepsilon_{RSA}$, where ε_{RSA} is the maximum advantage of polynomial time adversaries that break the RSA problem. Therefore, the ID-OFE scheme is secure against verifiers if the RSA problem is intractable.

Security against the arbitrator: To prove unforgeability, we forge a signature of the GQ-IBS scheme by using an algorithm $\mathcal{A}$ that breaks the unforgeability of the proposed ID-OFE scheme. Let (N, E) be a set of parameters for GQ-IBS given as a challenge. We set $n_k = N$ and $e_k = E$. We can access the two hash oracles O_I^{GQ} and O_h^{GQ}, an extraction oracle O_{Ext}^{GQ}, and a signing oracle O_{Sig}^{GQ}. A malicious arbitrator can open any partial signature; hence, we did not provide the opening oracle. We maintain two lists, L_H and L_{Sig}, for hash queries for H and for signing queries, respectively. We respond to $\mathcal{A}$'s queries as follows.

Hash Query for *I*: For a given hash query on an identity id_i, we make a hash query on the identity to hash oracle O_I^{GQ}. Let I_i be the answer returned by the oracle. We give I_i to $\mathcal{A}$.

Hash Query for *h*: When $\mathcal{A}$ asks a hash query on a pair (m, a_e, t), we make a hash query for (m', t) to hash oracle O_h^{GQ} where $m' = m||a_e$. Let c be the answer returned by O_h^{GQ}. We then give c to $\mathcal{A}$.

Hash Query for *H*: For a given hash query for (m, a^*, t) we choose a random γ, we then give it to algorithm $\mathcal{A}$ who then stores (m, a^*, t, γ) in L_H.

Extraction Query: For a given extraction query for an identity id_i, we make an extraction query to O_{Ext}^{GQ} for the identity. We give the answer sk_i, returned by the oracle O_{Ext}^{GQ}, to the algorithm $\mathcal{A}$. Recall that we did not consider the case where id_i is the identity of the target user (victim).

Partial/full Signing Query: When algorithm $\mathcal{A}$ makes a signing query on a message m of a user U_i, we respond to the query as follows. We choose a random value a_e in Z_{na}^* and make a singing query on $m' = m||a_e$ to the signing oracle O_{Sig}^{GQ}. Let (b, c) be the signature of m' answered by O_{Sig}^{GQ}. Then, we choose two random values, a in Z_{na}^* and a^* in $\{0, 1\}^{\ell h}$, and then compute the following:

$$t = b^{ek} \cdot I_i^{-c} \bmod n_k$$

and

$$\gamma = a_e / a^{ea} \bmod n_a.$$

We set $H(m||a^*||t) = \gamma$ and store (m, a^*, t, γ) and (m, a, a^*, b, c) in L_H and L_{Sig}, respectively. For a partial signing query, we give (a_e, b, c) to algorithm $\mathcal{A}$. For a full signing query, we give (a, a^*, b, c) to algorithm $\mathcal{A}$.

Algorithm $\mathcal{A}$ may return a signature $((a, a^*, b, c))$ on a message (m) whose partial signature was not generated by any oracle. Note that since the arbitrator can open a partial signature to a full signature, we exclude the case where the adversary obtains the full signature by opening a partial signature that was generated by an oracle. We return (b, c) as a forgery on the message m', where $t = b^{ek} \cdot I(id_i)^{-c} \bmod n_k$, $a_e = H(m||a^*||t)$, and $m' = m||a_e$. If the forged signature returned by the algorithm $\mathcal{A}$ is valid, then we have $h(m||a_e||t) = c$. Hence, (b, c) is a valid signature of the GQ-IBS scheme since the following relation holds: $h(m'||t) = c$, where $m' = m||a_e$. Therefore, the unforgeability of the ID-OFE scheme is reduced to the security of the GQ-IBS scheme. Let ε be the advantage of the algorithm $\mathcal{A}$. Then, we can break the GQ-IBS scheme with advantage ε, so $\varepsilon < \varepsilon_{GQ\text{-}IBS}$, where $\varepsilon_{GQ\text{-}IBS}$ is the maximum advantage of polynomial time adversaries that break the security of the GQ-IBS scheme. Since the security of the GQ-IBS scheme is reduced to the hardness of the RSA problem [33]–[34] we have $\varepsilon_{GQ\text{-}IBS} \approx \varepsilon_{RSA} + \varepsilon(k)$ for a negligible function $\varepsilon(k)$. Hence, $\varepsilon < \varepsilon_{RSA} + \varepsilon(k)$.

V. Conclusion

In this paper, we propose an efficient ID-based optimistic fair exchange based on the RSA function. From a theoretical point of view, the proposed scheme is the first provably secure ID-based fair exchange scheme based on the RSA function whose security can be proved under fully formalized security models. Note that the theoretical contribution is the main contribution of this paper. The proposed scheme has the following additional strongpoints. The scheme is suitable for cryptographic engineering practices due to the simplicity of the RSA function. The scheme is setup-free; therefore, the arbitrator participates in the protocol execution only if there is a dispute between the two parties. Moreover, the proposed fair exchange scheme is designed in an ID-based setting; hence, it is possible to eliminate the need for certificates and avoid some related problems.

References

[1] N. Asokan, V. Shoup, and M. Waidner, "Optimistic Fair Exchange of Digital Signatures," *EUROCRYPT LNCS,* vol. 1403, Berlin: Springer-Verlag, 1998, pp. 591–606.

[2] N. Asokan, V. Shoup, and M. Waidner, "Optimistic Fair Exchange of Digital Signatures," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 4, Apr. 2000, pp. 593–610.

[3] D. Boneh et al., "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *EUROCRYPT LNCS*, vol. 2656, Berlin: Springer-Verlag, 2003, pp. 416–432.

[4] J. Camenisch and I. Damgård, "Verifiable Encryption, Group Encryption, and Their Applications to Separable Group Signatures and Signature Sharing Schemes," *ASIACRYPT LNCS*, vol. 1976, Berlin: Springer-Verlag, 2000, pp. 331–345.

[5] Y. Dodis and L. Reyzin, "Breaking and Repairing Optimistic Fair Exchange from PODC 2003," *ACM Workshop DRM*, New York: ACM Press, 2003, pp. 47–54.

[6] X. Huang et al., "Optimistic Fair Exchange with Strong Resolution-Ambiguity," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, Aug. 2011, pp. 1491–1502.

[7] Q. Huang, D.S. Wong, and W. Susilo, "A New Construction of Designated Confirmer Signature and its Application to Optimistic Fair Exchange," *Pairing LNCS*, vol. 6487, Berlin: Springer-Verlag, 2010, pp. 41–61.

[8] J.M. Park, E.K.P. Chong, and H.J. Siegel, "Constructing Fair-Exchange Protocols for E-Commerce via Distributed Computation of RSA Signatures," *PODC*, New York: ACM Press, 2003, pp. 172–181.

[9] D.H. Yum and P.J. Lee, "Efficient Fair Exchange from Identity-Based Signature," *IEICE Trans. Fundamentals*, vol. E91-A, no. 1, Jan. 2008, pp. 119–126.

[10] H. Zhu and F. Bao, "More on Stand-Alone and Setup-Free Verifiably Committed Signatures," *ACISP LNCS*, vol. 4058, Berlin: Springer-Verlag, 2006, pp. 148–158.

[11] H. Zhu and F. Bao, "Stand-Alone and Setup-Free Verifiably Committed Signatures," *CT-RSA LNCS*, vol. 3860, Berlin: Springer-Verlag, 2006, pp. 159–173.

[12] H. Zhu, W. Susilo, and Y. Mu, "Multi-party Stand-Alone and Setup-Free Verifiably Committed Signatures," *PKC LNCS*, vol. 4450, Berlin: Springer-Verlag, 2007, pp. 134–149.

[13] L. Zhang, Q. Wu, and B. Qin, "Identity-Based Optimistic Fair Exchange in the Standard Model," *Security Commun. Netw.*, vol. 6, no. 8, Aug. 2013, pp. 1010–1020.

[14] O. Markowitch and S. Saeednia, "Optimistic Fair Exchange with Transparent Signature Recovery," *FC LNCS*, vol. 2339, Berlin: Springer-Verlag, 2002, pp. 339–350.

[15] J. Cathalo, B. Libert, and J.-J. Quisquater, "Cryptanalysis of a Verifiably Committed Signature Scheme Based on GPS and RSA," *LNCS*, vol. 3225, Berlin: Springer-Verlag, 2004, pp. 52–60.

[16] Z. Zhang and D. Feng, "Simple Fair Exchange Based Mediated-RSA and Factoring Representation," *WISA*, Jeju Island, Rep. of Korea, 2003, pp. 689–696.

[17] X. Ding and G. Tsudik, "Simple Identity-Based Cryptography with Mediated RSA," *CT-RSA LNCS*, vol. 2612, Berlin: Springer-Verlag, 2003, pp. 193–210.

[18] G. Ateniese, "Efficient Verifiable Encryption (and Fair Exchange) of Digital Signatures," *ACM Conf. Comput. Commun. Security*, 1999, pp. 138–146.

[19] G. Ateniese, "Verifiable Encryption of Digital Signatures and Applications," *ACM TISSEC*, vol. 7, no. 1, Feb. 2004, pp. 1–20.

[20] S. Saeednia, O. Markowitch, and Y. Roggeman, "Identity-Based Optimistic Fair Exchange with Transparent Signature Recovery," *CANS*, 2003. http://www.ulb.ac.be/di/scsi/markowitch/publications/dms03.pdf

[21] Y. Dodis, P.J. Lee, and D.H. Yum, "Optimistic Fair Exchange in a Multi-user Setting," *PKC LNCS*, vol. 4450, Berlin: Springer-Verlag, 2007, pp. 118–133.

[22] Q. Huang et al., "Efficient Optimistic Fair Exchange Secure in the Multi-user Setting and Chosen-Key Model without Random Oracles," *CT-RSA LNCS*, vol. 4964, Berlin: Springer-Verlag, 2008, pp. 106–120.

[23] L.C. Guillou and J.-J. Quisquater, "A Paradoxical Indentity-Based Signature Scheme Resulting from Zero-Knowledge," *CRYPTO LNCS*, vol. 403, Berlin: Springer-Verlag, 1988, pp. 216–231.

[24] A. Shamir, "Identity Based Cryptosystems and Signature Schemes," *Cryptology LNCS*, vol. 196, Berlin: Springer-Verlag, 1985, pp. 47–53.

[25] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *CRYPTO LNCS*, vol. 2139, Berlin: Springer-Verlag, 2001, pp. 213–229.

[26] C. Gu, Y. Zhu, and Y. Zhang, "An ID-Based Optimistic Fair Signature Exchange Protocol from Pairings," *CIS LNCS*, vol. 3802, Berlin: Springer-Verlag, 2005, pp. 9–16.

[27] X.-Y. Ren, Z.-H. Qi, and Y. Geng, "Provably Secure Aggregate Signcryption Scheme," *ETRI J.*, vol. 34, no. 3, June 2012, pp. 421–428.

[28] Z. Zhang et al., "Efficient ID-Based Optimistic Fair Exchange with Provable Security," *ICICS LNCS*, vol. 3783, Berlin: Springer-Verlag, 2005, pp. 14–26.

[29] L. Zhang, Q. Wu, and Y. Hu, "Hierarchical Identity-Based Encryption with Constant-Size Private Keys," *ETRI J.*, vol. 34, no. 1, Feb. 2012, pp. 142–145.

[30] S. Lim and H.-S. Lee, "A Short and Efficient Redactable Signature Based on RSA," *ETRI J.*, vol. 33, no. 4, Aug. 2011, pp. 621–628.

[31] L.C. Guillou and J.-J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing both Trasmission and Memory," *EUROCRYPT LNCS*, vol. 330, Berlin: Springer-Verlag, 1988, pp. 123–128.

[32] R.L. Rivest, A. Shamir, and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *ACM*, vol. 21, no. 2, Feb. 1978, pp.120–126.

[33] M. Bellare et al., "Security Proofs for Identity-Based Identification and Signature Schemes," *EUROCRYPT LNCS*, vol. 3027, Berlin: Springer-Verlag, 2004, pp. 268–286.

[34] Y. Dodis et al., "Strong Key-Insulated Signature Schemes," *PKC LNCS*, vol. 2567, Berlin: Springer-Verlag, 2003, pp. 130–144.

Taek-Young Youn received his PhD degree in cryptography from Korea University, Seoul, Rep. of Korea in 2009. He was working as a postdoctoral researcher at the Graduate School of Information Management and Security, Korea University, Seoul, Rep. of Korea, from September 2009 to June 2010. He is now a researcher at the Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea. His research interests include information security, public key cryptosystems, and cryptographic protocol.

Ku-Young Chang received his BS, MS and PhD degrees in mathematics from Korea University, Seoul, Rep. of Korea, in 1995, 1997, and 2000, respectively. He is currently a principal researcher in the Cryptography Research Section at ETRI, Daejeon, Rep. of Korea. His research interests include cryptography, data privacy, and architectures for computations in finite fields.