4-2008

Efficient optimistic fair exchange secure in the multi-user setting and chosen-key model without random oracles

Qiong HUANG

Guomin YANG
Singapore Management University, gmyang@smu.edu.sg

Duncan S. WONG

Willy SUSILO

Citation

HUANG, Qiong; YANG, Guomin; WONG, Duncan S.; and SUSILO, Willy. Efficient optimistic fair exchange secure in the multi-user setting and chosen-key model without random oracles. (2008). *Proceedings of the Cryptographers' Track at the RSA Conference 2008, San Francisco, April 8-11*. 106-120.
Available at: https://ink.library.smu.edu.sg/sis_research/7382

Efficient Optimistic Fair Exchange Secure in the Multi-user Setting and Chosen-Key Model without Random Oracles

Qiong Huang[1], Guomin Yang[1], Duncan S. Wong[1], and Willy Susilo[2]

[1] Department of Computer Science,
City University of Hong Kong, Hong Kong
[2] School of Computer Science & Software Engineering,
University of Wollongong, Australia

Abstract. Optimistic fair exchange is a kind of protocols to solve the problem of fair exchange between two parties. Almost all the previous work on this topic are provably secure only in the random oracle model. In PKC 2007, Dodis et al. considered optimistic fair exchange in a multi-user setting, and showed that the security of an optimistic fair exchange in a single-user setting may no longer be secure in a multi-user setting. Besides, they also proposed one and reviewed several previous construction paradigms and showed that they are secure in the multi-user setting. However, their proofs are either in the random oracle model, or involving a complex and very inefficient NP-reduction. Furthermore, they only considered schemes in the *certified-key model* in which each user has to show his knowledge of the private key corresponding to his public key.

In this paper, we make the following contributions. First, we consider a relaxed model called *chosen-key model* in the context of optimistic fair exchange, in which the adversary can arbitrarily choose public keys without showing the knowledge of the private keys. We separate the security of optimistic fair exchange in the *chosen-key* model from the *certified-key* model by giving a concrete counterexample. Second, we strengthen the previous *static* security model in the multi-user setting to a more practical one which allows an adversary to choose a key *adaptively*. Third, we propose an *efficient* and *generic* optimistic fair exchange scheme in the multi-user setting and *chosen-key* model. The security of our construction is proven *without random oracles*. We also propose some efficient instantiations.

1 Introduction

Optimistic fair exchange, introduced by Asokan, Schunter and Waidner [1], is a kind of protocols to solve the problems in fairly exchanging items between two parties, say Alice and Bob. In such a protocol, there is an arbitrator who is semi-trusted by Alice and Bob and involves only if one party attempts to cheat the other or simply crashes. Since the introduction, it has attracted many researchers' attention, such as [2,3,11,20,13,16,19,26,25,4,23,12] and so on.

T. Malkin (Ed.): CT-RSA 2008, LNCS 4964, pp. 106–120, 2008.

There are two popular paradigms for building optimistic fair exchange schemes. One is based on *verifiably encrypted signatures* [8], such as [2,3,11], and the other is based on *sequential two-party multisignatures*, such as [20]. Park et al.'s sequential two-party multisignature based optimistic fair exchange [20] was broken and repaired by Dodis and Reyzin [13]. However, Dodis-Reyzin schemes are *setup-driven* [27,28], which require key registration for all users with the arbitrator. In the same year, Micali proposed a fair electronic exchange protocol for contract signing with an invisible trusted party [19], using a CCA2 secure public key encryption scheme with *recoverable randomness* (i.e., the decryption algorithm can extract from the ciphertext both the plaintext and the randomness used for generating the ciphertext) and a signature scheme that is existentially unforgeable under chosen message attacks. The idea is similar to that of the verifiably encrypted signature paradigm. Later, Bao et al. [4] showed that the scheme does not satisfy the fairness requirement. A dishonest Bob can get Alice's full commitment without letting Alice get his obligation. They also provided an improvement to avoid such an attack.

To the best of our knowledge, almost all verifiably encrypted signature schemes and sequential multisignature schemes, even though efficient, are proven secure in the random oracle model only, which is only heuristic. The only schemes which are proven secure without random oracles are the verifiably encrypted signature scheme and the multisignature scheme proposed by Lu et al. [17]. Both schemes are based on Waters' signature scheme [24], and have been proven secure in the *certified-key* model [17] (or the *registered-key* model [5]), in which the adversary is required to certify that the public keys it includes in the signing oracle and in its forgery are properly generated and it knows the corresponding private keys.

Recently, Dodis et al. [12] considered optimistic fair exchange in a multi-user setting. Prior to their work, almost all previous results considered the single-user setting only, in which there are only one signer and one verifier (along with an arbitrator). A more practical setting is the multi-user setting, in which there are many signers and many verifiers (along with an arbitrator), so that a dishonest party can collude with some other parties in an attempt of cheating another party. Though the security of both encryption and signature in the single-user setting is preserved in the multi-user setting, Dodis et al. [12] showed that this is not necessarily true for optimistic fair exchange. They showed a counterexample that is secure in the single user setting but insecure in the multi-user setting. Furthermore, they proposed a formal definition of optimistic fair exchange in the multi-user setting, and presented a generic construction. Their generic construction is *setup-free* (i.e. no key registration is required between users and the arbitrator) and can be built if there exist one-way functions in the random oracle model, or if there exist trapdoor one-way permutations in the standard model. However, all the schemes presented in [12] were proven secure in the *certified-key* model only. If the adversary is allowed to choose public keys arbitrarily without requiring to show its knowledge of the corresponding private keys, these schemes may not be secure.

Our Results: Our contributions are in three-fold. First, we note that optimistic fair exchange schemes secure in the certified-key model may not be secure in the chosen-key model [18]. We separate these two models by presenting a counterexample. Namely, we present a scheme which is secure in the certified-key model but insecure in the chosen-key model. The crux of the problem is to allow the adversary in the chosen-key model to arbitrarily set public keys *without* showing its knowledge of the corresponding private keys (cf. certified-key model). Hence, the model is more realistic and it provides the adversary with more flexibility and power in attacking other honest parties in the system.

Second, we further strengthen the security model in the multi-user setting for optimistic fair exchange first proposed by Dodis et al. [12]. In particular, we notice that in [12], the model capturing the security against the arbitrator is a *static* model which requires the malicious arbitrator to fix its keys before seeing the challenging public key of the signer. We propose to strengthen it to an *adaptive* model which allows the arbitrator to set its keys with reference to the value of the challenging public key of the signer.

Third, we propose an *efficient* and *generic* construction of optimistic fair exchange in the multi-user setting and chosen-key model, and prove the security *without random oracles*. The construction is based on a conventional signature [14,24] and a ring signature [21,24,6,22,10,15], both of which can be constructed efficiently without random oracles. This also contributes a new paradigm for constructing optimistic fair exchange, besides the existing ones: the verifiably encrypted signatures based approach and the sequential two-party multisignature based one. In our generic construction, we further show that the ring signature scheme used in our construction does not need to be with the highest level of existential unforgeability considered in [6], namely *unforgeability with respect to insider corruptions*. Instead, *unforgeability against a static adversary* [10] will suffice. We also propose some efficient instantiations of our generic construction.

Organization: In the next section, we review the definition of optimistic fair exchange, and modify Dodis et al.'s security games to adapt the chosen-key model. In Sec. 3, we give a counterexample to separate the security level between the certified-key model and the chosen-key model. Our generic construction is then proposed and shown secure in the multi-user setting and under the chosen-key model in Sec. 4. Some efficient instantiations are also discussed in the section. Finally, we conclude this paper in Sec. 5.

2 Definitions and Security Model

2.1 Definitions in the Multi-user Setting and Chosen-Key Model

The definition for non-interactive optimistic fair exchange (OFE) follows the one in the multi-user setting given in [12] but having the authenticity assumption on public keys removed. This implies that we do not restrict ourselves to the *certified-key* model [17], but consider the definition under a stronger security model, called the *chosen-key* model [18]. We will give more details shortly

(Sec. 2.2) and make some additional remarks to discuss some subtleties in the definitions. Readers can refer to [12] for the detailed definition.

The *correctness* condition can be defined in a natural way. The *ambiguity* property requires that any "resolved signature" $\mathsf{Res}(m, \mathsf{PSig}(m, SK_{U_i}, APK), ASK, PK_{U_i})$ is *computationally indistinguishable* from an "actual signature" $\mathsf{Sig}(m, SK_{U_i}, APK)$.

2.2 Chosen-Key Model

Note that [12] only considers OFE in the certified-key model [17]. In such a model, it is assumed that the authenticity of public keys of users in the system can be verified and each user should show his knowledge of the corresponding private key in some *public key registration stage* for defending against key substitution attacks. Alternatively, the adversary is required to show that the public keys included in queries to the signing oracle and in its forgery are properly generated.

In this paper, we consider a stronger security model for OFE, the *chosen-key* model, which was originally introduced by Lysyanskaya et al. in the context of aggregate signature [18]. An adversary in a chosen-key model can arbitrarily set public keys *without* showing its knowledge of the corresponding private keys. The only limitations are that the adversary cannot replace the challenge user's public key and all the public keys chosen by the adversary should fall into some public key space (which is defined under some system-wide parameters and known to all parties in the system). Such relaxation gives the adversary more flexibility and power in attacking other (honest) parties in the system. Schemes secure in the certified-key model may not necessarily be secure in the chosen-key model.

For example, let us consider the Security Against Verifiers under the chosen-key model (Sec. 2.3). After receiving a partial signature from the challenge signer, the adversary may ask the arbitrator for resolving it into a full signature with respect to a *different* public key chosen maliciously by the adversary according to the challenge signer's public key and the partial signature received. Based on this attacking approach, in Sec. 3, we describe a concrete OFE scheme as an example for showing that a scheme secure in the certified-key model does not necessarily be secure in the chosen-key model.

2.3 Security Model

The security of optimistic fair exchange consists of three aspects: security against signers, security against verifiers, and security against the arbitrator. The definitions of them in the multi-user setting and chosen-key model are given as follows.

- Security against signers: Intuitively, we require that no PPT adversary A should be able to produce a partial signature with non-negligible probability, which looks good to verifiers but cannot be resolved to a full signature by the honest arbitrator. This ensures the fairness for verifiers, that is, if the signer has committed to a message, the verifier will always be able to get the full commitment of the signer. Formally, we consider the following experiment:

$$\begin{aligned} \mathsf{Setup}^{\mathsf{TTP}}(1^k) &\rightarrow (ASK, APK) \\ (m, \sigma', PK^*) &\leftarrow A^{O_{\mathsf{Res}}}(APK) \\ \sigma &\leftarrow \mathsf{Res}(m, \sigma', ASK, PK^*) \\ \text{success of } A &:= [\mathsf{PVer}(m, \sigma', PK^*, APK) = \mathsf{accept} \\ &\quad \wedge \mathsf{Ver}(m, \sigma, PK^*, APK) = \mathsf{reject}] \end{aligned}$$

where oracle O_{Res} takes as input a *valid*[1] partial signature σ' of user U_i on message m, i.e. (m, σ', PK_{U_i}), and outputs a full signature σ on m under PK_{U_i}. In this experiment, the adversary can arbitrarily choose public keys, and it may not know the corresponding private key of PK^*. The advantage of A in the experiment $\mathrm{Adv_A}(k)$ is defined to be A's success probability.

- Security against verifiers: This security notion requires that any PPT verifier B should not be able to transform a partial signature into a full signature with non-negligible probability if no help has been obtained from the signer or the arbitrator. This requirement has some similarity to the notion of *opacity* for verifiably encrypted signature [8]. Formally, we consider the following experiment:

$$\begin{aligned} \mathsf{Setup}^{\mathsf{TTP}}(1^k) &\rightarrow (ASK, APK) \\ \mathsf{Setup}^{\mathsf{User}}(1^k) &\rightarrow (SK, PK) \\ (m, \sigma) &\leftarrow B^{O_{\mathsf{PSig}}, O_{\mathsf{Res}}}(PK, APK) \\ \text{success of } B &:= [\mathsf{Ver}(m, \sigma, PK, APK) = \mathsf{accept} \\ &\quad \wedge (m, \cdot, PK) \notin \mathit{Query}(B, O_{\mathsf{Res}})] \end{aligned}$$

  where oracle O_{Res} is described in the previous experiment, the partial signing oracle O_{PSig} takes as input a message m and returns a valid partial signature σ' on m under PK, and $\mathit{Query}(B, O_{\mathsf{Res}})$ is the set of valid queries B issued to the resolution oracle O_{Res}. In the experiment, B can ask the arbitrator for resolving any partial signature with respect to any public key (adaptively chosen by B, probably without the knowledge of the corresponding private key), with the limitation described in the experiment. The advantage of B in the experiment $\mathrm{Adv_B}(k)$ is defined to be B's success probability.
- Security against the arbitrator: Intuitively, this security notion requires that any PPT arbitrator C should not be able to generate with non-negligible probability a full signature without explicitly asking the signer for generating one. This ensures the fairness for signers, that is, no one can

[1] By 'valid', we mean that σ' is a valid partial signature on m under public key PK_{U_i}, alternatively, the input (m, σ', PK_{U_i}) of O_{Res} satisfies the condition that $\mathsf{PVer}(m, \sigma', PK_{U_i}, APK) = \mathsf{accept}$.

frame the actual signer on a message with a forgery. Formally, we consider the following experiment:

$$\begin{aligned}
\mathsf{Setup}^{\mathsf{User}}(1^k) &\to (SK, PK)\\
(ASK^*, APK) &\leftarrow C(PK)\\
(m, \sigma) &\leftarrow C^{O_{\mathsf{PSig}}}(ASK^*, APK, PK)\\
\text{success of } C &:= [\mathsf{Ver}(m, \sigma, PK, APK) = \mathsf{accept}\\
&\qquad \wedge (m, \cdot) \notin \mathit{Query}(C, O_{\mathsf{PSig}})]
\end{aligned}$$

where the partial signing oracle O_{PSig} is described in the previous experiment, ASK^* is C's state information, which might not be the corresponding private key of APK, and $\mathit{Query}(C, O_{\mathsf{PSig}})$ is the set of queries C issued to the partial signing oracle O_{PSig}. The advantage of C in this experiment $\mathrm{Adv}_{\mathrm{C}}(k)$ is defined to be C's success probability.

Definition 1. *A non-interactive optimistic fair exchange scheme is said to be* secure in the multi-user setting and chosen-key model *if there is no PPT adversary that wins any of the experiments above with non-negligible advantage.*

Remark 1. (Differences From [12]) Though the experiments of Security Against Signers and Security Against Verifiers remain in the same form as those in [12], we put no requirement on that the adversary has to register a public key before using it. In other words, the adversary can freely choose public keys (from the public key space) and use them during the attack, without proving its knowledge of the corresponding private keys. In [12] on the other hand, the authenticity assumption of public keys is made in all the experiments.

On the Security Against the Arbitrator, our corresponding experiment seems to be stronger than the one considered in [12], in which the adversary has to fix APK before learning the challenge signer's public key PK. This *static* form of adversarial key generation seems to be unnecessarily weak. We propose a strengthened one which allows the adversary to *adaptively* set APK based on the value of PK generated using $\mathsf{Setup}^{\mathsf{User}}$. In this way, the security model considered in this paper will be at least as strong as that in [12]'s, if not stronger. This observation is also supported by the counterexample given in Sec. 3.

3 Separating Chosen-Key Model from Certified-Key Model

As reviewed in the introduction, OFE in the single-user setting can normally be built from verifiably encrypted signature or from sequential two-party multisignature. Dodis et al. [12] showed that secure OFE in the multi-user setting can also be built from these primitives, but only the verifiably encrypted signature based ones may support the setup-free feature [27,28]. Also note that in [12], all the security analysis were carried out in the *certified-key* model [17] and therefore, they may not remain secure in the *chosen-key* model [18]. In the following, we give a concrete example for showing that a secure OFE in the certified-key model may no longer be secure in the chosen-key model. The example is based on Lu et al.'s [17] verifiably encrypted signature scheme. Readers can refer to [17] for Lu et al.'s scheme **WVES** .

3.1 A WVES-Based OFE

Observe that Lu et al.'s **WVES** is an OFE in the *single-user* setting and the *certified-key* model , under which, **WVES.Kg** and **WVES.AKg** constitute the OFE registration protocol Setup, and **WVES.Sig**, **WVES**. **Ver**, **WVES.ESig**, **WVES.EVer** and **WVES.Adj** are corresponding to Sig, Ver, PSig, PVer and Res, respectively. In the single-user setting and certified-key model [13,12], Security Against Signers is due to the correctness of **WVES**. That is, if η is a valid verifiably encrypted signature, the adjudicator can always convert it to an ordinary signature. Security Against Verifiers is due to the opacity property [8] of **WVES**.

The Security Against the Arbitrator does not trivially follow the unforgeability of the verifiably encrypted signature scheme, since in the corresponding experiment, the malicious arbitrator knows more secret information than a public verifier does. To show its security, we build a forger $\mathcal{F}$ of Waters' signature scheme using the malicious arbitrator/adjudicator C. Given the system parameters and a public key $A = e(g, g)^{\alpha}$, $\mathcal{F}$ randomly picks $\beta \leftarrow \mathbb{Z}_p$ and sends the system parameters, A and $(\beta, v := g^{\beta})$ to C[2]. The rest of the proof goes essentially the same as that in [17], except that $\mathcal{F}$ uses its signing oracle to simulate the PSig oracle. If C outputs a valid forgery (S_1, S_2), i.e., $\mathbf{Ver}(PK, M, (S_1, S_2)) = \mathsf{accept}$, $\mathcal{F}$ simply outputs $\sigma^* := (S_1, S_2)$ on M as its forgery for Waters' signature scheme. By the validity of (S_1, S_2), we have that σ^* is also a valid forgery with respect to the challenge public key. Besides, the above scheme can easily be shown to be secure in the *multi-user* setting and the certified-key model as well.

3.2 An Attack under Chosen-Key Model

If we retain the multi-user setting but upgrade the model from certified-key model to the chosen-key model, we will see that the **WVES**-based OFE above will no longer be secure.

Let us consider the Security Against Verifiers. In the chosen-key model, the adversary (i.e. the verifier in the experiment) can first ask the challenge signer for a partial signature on some message under the challenge public key PK. Then, the adversary makes up a new public key PK' according to the partial signature and PK, and queries the challenger for resolving the partial signature with respect to PK' rather than to PK. The adversary finally tries to find out the full signature under PK from the resolved signature. In the *chosen-key* model, since the adversary can arbitrarily pick public keys without showing its

[2] Alternatively, C picks its key pair and shows its knowledge of ASK. This is due to the restriction of certified-key model. Readers can refer to [12] for detailed discussions about this.

knowledge of the corresponding private keys, such an attack approach is possible. Below is the detail of the actual attack against the **WVES**-based OFE.

(In)Security Against Verifiers: Upon receiving the challenge signer's public key $PK = e(g,g)^\alpha$ from the challenger, the adversary B queries O_{PSig} for a partial signature $\sigma' = (K_1, K_2, K_3)$ on message M. Then B generates another public key $PK' := PK \cdot e(g,g)^b$ where $b \leftarrow \mathbb{Z}_p$, and queries O_{Res} for resolving a partial signature in the form $\sigma'' = (K_1 \cdot g^b, K_2, K_3)$ under the public key PK'. Note that σ'' is a valid partial signature on M under PK'. Upon receiving the resolved signature $\sigma = (S_1, S_2)$, B outputs the full signature under the challenge public key PK as $\tilde{\sigma} = (S_1/g^b, S_2)$ and wins the game.

Therefore, **WVES**-based OFE is insecure in the multi-user setting under the *chosen-key* model. We should also emphasize that this does not contradict with the results given in [17] as their schemes were originally designed for security in the *certified-key* model only.

4 An Efficient and Generic Construction without Random Oracles

In this section, we propose an OFE proven secure in the multi-user setting and the chosen-key model, that is, under the adversarial model formalized in Sec. 2.3. Our construction is based on two primitives: conventional signature [14] and ring signature [21]. Since there exist signature schemes and ring signature schemes proven secure without random oracles, it is possible for us to construct a secure OFE without random oracle also. Refers can refer to [14] for the security definition of conventional signatures. In the following, we first briefly review the definition of ring signature.

(**Ring Signature:**) The notion of ring signature was introduced by Rivest et al. in Asiacrypt 2001 [21] and has later been widely studied [6,10,22,15].

The security of a ring signature scheme includes two parts, *anonymity* (or *ambiguity*) and *unforgeability*. The strongest computational complexity based security notions of them are *anonymity against attribution attacks/full key exposure* and *unforgeability with respect to insider corruption*, respectively [6,10]. In our construction of OFE (to be shown later), we actually do not require a ring signature scheme to equip with such a strong level of anonymity and unforgeability. Instead, *unforgeability under an adaptive attack, against a static adversary* [10] will suffice. It is defined as follows.

$$
\begin{aligned}
(sk_i, pk_i) &\leftarrow \mathsf{RS.KG}(1^k), \text{ for } i = 1, \cdots, \ell \\
R &:= \{pk_i\}_{i=1}^{\ell} \\
(R, m, \sigma) &\leftarrow A^{O_{\mathsf{RS.Sig}}}(R) \\
\text{success of } A &:= [\mathsf{RS.Ver}(m, \sigma, R) = \mathsf{accept} \wedge (\cdot, m, R) \notin \mathit{Query}(A, O_{\mathsf{RS.Sig}})]
\end{aligned}
$$

where A is a PPT adversary, $O_{\mathsf{RS.Sig}}$ is the ring signing algorithm which takes as input an index i, a message m, a list of public keys S such that $S \cap R \neq \emptyset$

and $pk_i \in R$, and outputs a ring signature σ on m under the ring S using the signing key sk_i, and $Query(A, O_{\mathsf{RS.Sig}})$ is the set of ring signing queries (of the form (i, m, S)) issued by A. The advantage of A in the experiment is defined to be its success probability. A ring signature scheme is said to be *(existentially) unforgeable under an adaptive attack, against a static adversary* (where 'static' means that the adversary should not corrupt any honest user and its forgery should be with respect to the prescribed ring R,) if there is no PPT adversary which wins the experiment with non-negligible advantage. It's readily seen that the above unforgeability is weaker than the *unforgeability with respect to insider corruption* considered in [6]. For our purpose, the number ℓ of (honestly generated) public keys is 2 and the size of the ring S in a signing query issued by A is also 2 (i.e., $\ell = 2$ and $|S| = 2$).

4.1 The Construction

Let $\mathsf{SIG} = (\mathsf{KG}, \mathsf{Sig}, \mathsf{Ver})$ be a conventional signature scheme and $\mathsf{RS} = (\mathsf{KG}, \mathsf{Sig}, \mathsf{Ver})$ a ring signature scheme. Our construction idea is as follows. The partial signature will be a conventional signature generated using SIG, and the full signature is the partial signature in conjunction with a ring signature generated under RS. The 'ring' members of the ring signature are the signer and the arbitrator. To resolve a partial signature, the arbitrator simply produces a ring signature. One of the main reasons of employing a ring signature scheme in our construction is that the unforgeability game of ring signature (that is, unforgeability under an adaptive attack, against a static adversary, as stated above) fits well in the chosen-key model for OFE. That is, the adversary can ask for a ring signature with respect to a ring which includes public keys not being certified. Below are the details of our generic construction denoted by OFE.

- $\mathsf{Setup}^{\mathsf{TTP}}$: The arbitrator runs $(ask, apk) \leftarrow \mathsf{RS.KG}(1^k)$ and sets $(ASK, APK) := (ask, apk)$.
- $\mathsf{Setup}^{\mathsf{User}}$: Each user U_i runs $(\hat{sk}_i, \hat{pk}_i) \leftarrow \mathsf{SIG.KG}(1^k)$ and $(\bar{sk}_i, \bar{pk}_i) \leftarrow \mathsf{RS.KG}(1^k)$. U_i then sets $(SK_{U_i}, PK_{U_i}) := ((\hat{sk}_i, \bar{sk}_i), (\hat{pk}_i, \bar{pk}_i))$.
- Sig: On input a message m, the signer U_i first produces a conventional signature σ' as the partial signature, i.e. $\sigma' \leftarrow \mathsf{SIG.Sig}(\hat{sk}_i, m)$, and then completes the signing process by generating a ring signature on m and σ', i.e. $\sigma^{\mathsf{RS}} \leftarrow \mathsf{RS.Sig}(\bar{sk}_i, m\|\sigma'\|PK_{U_i}, R)$ where $R := \{\bar{pk}_i, apk\}$. The full signature is then set as $\sigma := (\sigma', \sigma^{\mathsf{RS}})$.
- Ver: On input a message m and a signature σ purportedly produced by U_i, where $\sigma = (\sigma', \sigma^{\mathsf{RS}})$, the verifier checks the validity of σ' and σ^{RS} by running $\mathsf{SIG.Ver}(m, \sigma', \hat{pk}_i)$ and $\mathsf{RS.Ver}(m\|\sigma'\|PK_{U_i}, \sigma^{\mathsf{RS}}, R)$ respectively, where $R := \{\bar{pk}_i, apk\}$. If both output accept, it returns accept; otherwise, it returns reject.
- PSig: On input a message m, the signer U_i computes a conventional signature, i.e. $\sigma' \leftarrow \mathsf{SIG.Sig}(\hat{sk}_i, m)$, and returns σ' as the partial signature.
- PVer: On input a message m and a partial signature σ' purportedly produced by U_i, the verifier returns $\mathsf{SIG.Ver}(m, \sigma', \hat{pk}_i)$.

- Res: On input a message m and a partial signature σ' of user U_i, the arbitrator first checks the validity of σ' by running $\mathsf{OFE.PVer}(m, \sigma', PK_{U_i}, APK)$. If σ' is invalid, it rejects the input by outputting $\perp$; otherwise, it computes $\sigma^{\mathsf{RS}} \leftarrow \mathsf{RS.Sig}(ask, m \| \sigma' \| PK_{U_i}, R)$, where $R := \{\bar{pk}_i, apk\}$. The arbitrator returns $\sigma := (\sigma', \sigma^{\mathsf{RS}})$.

As in [12], one cannot view σ' as the full signature of the signer, even though it is itself a valid conventional signature. The signer's full commitment to a message comprises the partial signature σ' generated using SIG, along with a ring signature σ^{RS} produced by the signer or the arbitrator using RS. The *correctness* of the construction simply follows that of SIG and RS, and the *ambiguity* follows the *anonymity* requirement is satisfied due to that of the ring signature RS.

Remark 2. One may notice that Dodis et al.'s generic OFE construction [12] uses a similar idea to ours. They employ a conventional signature as the partial signature and use an additional OR-signature to complete the generation of the full signature. An OR-signature itself can be viewed as a two-user ring signature. Even though OR-signature can express much richer languages, almost all the constructions of OR-signature follow the Fiat-Shamir heuristic, thus can only be proven secure in the random oracle model, or otherwise, require to have complex NP-reduction and non-interactive witness indistinguishable proofs of knowledge involved, that could be very inefficient. By applying our idea, an efficient and generic OFE scheme without random oracles can be built, as there are already quite a number of efficient conventional signature schemes and ring signature schemes proven secure without random oracles available in the literature.

Intuitively, for our construction above, the Security Against Signers holds unconditionally; the Security Against Verifiers follows the unforgeability property of the ring signature RS, and the Security Against the Arbitrator is guaranteed by the unforgeability of SIG. Thus, we have the following theorem.

Theorem 1. *The generic construction of optimistic fair exchange scheme* OFE *above is secure in the* multi-user *setting and* chosen-key *model, provided that* SIG *is a conventional signature scheme that is existentially unforgeable against chosen message attacks and* RS *is a secure ring signature scheme that is with* basic anonymity *and* existential unforgeability under an adaptive attack, against a static adversary*.*

Proof. Theorem 1 immediately follows from the following lemmas. □

Lemma 1. *The optimistic fair exchange scheme* OFE *above is unconditionally secure against signers.*

Proof. Obviously, for any message m and any valid signature σ' on m under the verification key $\hat{pk}_i$, the arbitrator can always produce a ring signature σ^{RS} on $m \| \sigma' \| PK_{U_i}$ under the ring $R := \{\bar{pk}_i, apk\}$. Therefore, no adversary can win the game. □

Lemma 2. *The optimistic fair exchange scheme* OFE *above is secure against verifiers if* RS *is unforgeable under adaptive attacks against a static adversary.*

Proof. Suppose that B is a PPT adversary which breaks the Security Against Verifiers with probability ϵ_B. We construct a PPT algorithm $\bar{B}$ to break the existential unforgeability of RS with the same probability.

On input a security parameter 1^k and given two public keys pk_0 and pk_1, which are the (honestly generated) challenge public keys as in the unforgeability game of ring signature (See page 113), $\bar{B}$ randomly generates a key pair $(\hat{sk}, \hat{pk})$ of SIG by running $(\hat{sk}, \hat{pk}) \leftarrow \mathsf{SIG.KG}(1^k)$, flips a bit $b \leftarrow \{0,1\}$, and sets $APK := pk_b$ and $PK := (\hat{pk}, pk_{1-b})$. It then runs B on input (APK, PK), and simulates oracle O_{PSig} using the secret key $\hat{sk}$ and oracle O_{Res} using $\bar{B}$'s ring signing oracle. More in detail, to answer an PSig query of m, $\bar{B}$ computes and returns $\mathsf{SIG.Sig}(\hat{sk}, m)$ to B. To answer an Res query of (m, σ', PK_{U_i}), if σ' is a valid partial signature on m under PK_{U_i}, $\bar{B}$ queries its ring signing oracle for getting a ring signature σ^{RS} on message $m\|\sigma'\|PK_{U_i}$ under the ring $\{pk_0, pk_1\}$ using the secret key corresponding to pk_b, and then sends $(\sigma', \sigma^{\mathsf{RS}})$ back to B.

At the end of the experiment, when B outputs its forgery $(\tilde{m}, \tilde{\sigma})$, where $\tilde{\sigma} = (\tilde{\sigma}', \tilde{\sigma}^{\mathsf{RS}})$, without loss of generality, we assume that B has already got $\tilde{\sigma}'$ from a query to oracle O_{PSig}. The other case that B produced $\tilde{\sigma}'$ by itself will be covered by the Security Against the Arbitrator, which is to be shown later.

Obviously, the simulation above is perfect, and thus B wins the game with probability ϵ_B. We have that $\mathsf{OFE.Ver}(\tilde{m}, \tilde{\sigma}, PK, APK) = \mathsf{accept}$ and $(\tilde{m}, \cdot, PK) \notin Query(B, O_{\mathsf{Res}})$. The former also implies that $\mathsf{SIG.Ver}(\tilde{m},\ \tilde{\sigma}', \hat{pk}) = \mathsf{accept}$ and $\mathsf{RS.Ver}(\tilde{m}\|\tilde{\sigma}'\|PK, \sigma^{\mathsf{RS}}, (pk_0, pk_1)) = \mathsf{accept}$ hold. Since $(\tilde{m}, \cdot, PK) \notin Query(B, O_{\mathsf{Res}})$, $\bar{B}$ has never issued a query to its ring signing oracle on input $\tilde{m}\|\tilde{\sigma}'\|PK$. Therefore, $\tilde{\sigma}^{\mathsf{RS}}$ is a valid ring signature on the new message $\tilde{m}\|\tilde{\sigma}'\|PK$ under the ring $\{pk_0, pk_1\}$. We then let $\bar{B}$ output $(\tilde{m}\|\tilde{\sigma}'\|PK, \tilde{\sigma}^{\mathsf{RS}})$ and $\bar{B}$ wins its own game with probability ϵ_B. □

Lemma 3. *The optimistic fair exchange scheme* OFE *above is secure against the arbitrator if* SIG *is unforgeable under chosen-message attacks.*

Proof. Suppose that C is a PPT adversary which breaks the Security Against the Arbitrator with probability ϵ_C. We build a PPT algorithm $\bar{C}$ to break the unforgeability of the conventional signature scheme SIG with the same probability.

Given the challenge verification key pk of SIG (along with a signing oracle O_{sk}), $\bar{C}$ runs $\mathsf{RS.KG}(1^k)$ to get a key pair $(\bar{sk}, \bar{pk})$ and feeds $PK := (pk, \bar{pk})$ as input to C, which then returns an arbitrator public key APK and begins to issue queries to O_{PSig}. This oracle can perfectly be simulated by $\bar{C}$ using O_{sk}. Namely, on input a message m, $\bar{C}$ forwards it to O_{sk} and relays the oracle's answer to C as a valid partial signature. Finally, C outputs its forgery $(\tilde{m}, \tilde{\sigma})$ where $\tilde{\sigma} = (\tilde{\sigma}', \tilde{\sigma}^{\mathsf{RS}})$, such that $\mathsf{OFE.Ver}(\tilde{m}, \tilde{\sigma}, PK, APK) = \mathsf{accept}$ and $(\tilde{m}, \cdot) \notin Query(C, O_{\mathsf{PSig}})$. We then have that $\tilde{\sigma}'$ is a valid signature on $\tilde{m}$, and $\tilde{m}$ has never been issued by $\bar{C}$ to its signing oracle. We simply let $\bar{C}$ output $(\tilde{m}, \tilde{\sigma}')$. Obviously $(\tilde{m}, \tilde{\sigma}')$ is a valid forgery for SIG, and $\bar{C}$ wins the unforgeability game with advantage ϵ_C. □

4.2 Instantiations

There are quite a number of efficient conventional signature schemes and ring signature schemes without random oracles available in the literature, like [24,7], [22,15,10] and many others. Using these schemes and applying our generic construction, we can get many concrete and efficient OFE schemes proven secure without random oracles in the multi-user setting and chosen-key model. For example, we can use Waters' signature scheme [24] as SIG and Shacham-Waters' ring signature scheme [22] as RS. Note that in such an instantiation, Waters' signature scheme may work in a group of composite order [22] rather than in a group of prime order [24], so that SIG and RS can share the same set of system parameters. Besides, it is necessary to mention that there is a global setup process before any execution of the scheme. The requirement of having such a setup process stems from that of Shacham-Waters' ring signature scheme. For this instantiation, the ambiguity of the scheme is based on sub-group decision assumption [9,22], while the security against verifiers and security against the arbitrator are based on computational Diffie-Hellman assumption. The OFE.Sig algorithm of the resulting scheme requires no pairing operation, and the OFE.Ver algorithm requires four pairings. A main disadvantage of this instantiation is that the size of system parameters is large. It is determined by the output length of the underlying hash function used in Waters' signature scheme [24,22].

Alternatively, we may consider another instantiation, which enjoys much shorter system parameters but suffers from stronger underlying assumptions, i.e. strong Diffie-Hellman assumption [7,15]. In this instantiation, we employ Boneh-Boyen's weakly secure signature scheme [7] plus a one-time signature scheme as SIG[3], and Groth's ring signature scheme (in the common reference string model) [15] as RS. The reason that we use Boneh-Boyen's weakly secure signature scheme plus a one-time signature scheme as SIG is the same as the one behind the combination of Waters signature and Shacham-Waters ring signature. (SIG and RS share system parameters.) Note that for RS, we do not need to use the signature compression technique as in [15] since the ring in our case merely consists of two users. The Sig algorithm of the resulting scheme does not require any pairing operation either, while the Ver algorithm requires nine pairings.

In these two instantiations, each user has two key pairs, one for the conventional signature and the other one for ring signature, just as in the generic construction (Sec. 4.1). To make the instantiations more practical and efficient, people may wish to combine the two key pairs into one. Boyen's ring signature [10] (or, say, his mesh signature) is a good candidate for this purpose. In Boyen's ring signature scheme, the adversary can make not only ring signature queries, but also atomic (or conventional) signature queries. Boyen's scheme works in the common reference string model. The anonymity holds unconditionally, and the unforgeability is guaranteed by the *Poly Strong Diffie-Hellman* assumption introduced by Boyen [10], which is a stronger variant of the Strong Diffie-Hellman

[3] It is easy to see that a weakly secure signature scheme plus a one-time signature scheme lead to a signature scheme that is unforgeable against chosen message attacks. We skip the detailed proof here.

(SDH) assumption. In the resulting OFE scheme, the signer Alice and the arbitrator Charlie form a ring. We view an atomic signature of Alice as her partial signature, and the combination of the atomic signature and a ring signature as Alice's full commitment. We can see that, similar to the generic construction, the security against signers of this optimized instantiation also holds unconditionally. The security against verifiers will hold due to the unforgeability of Boyen's (two-user) ring signature scheme, and the security against the arbitrator follows the unforgeability of the (single-user) ring signature scheme. Any forgery of Alice's atomic signature σ' on a message m, where $\sigma' = (S, t) = (g^{\frac{1}{a+bm+ct}}, t)$ and (a, b, c) is Alice's secret key, can be trivially transformed into a forgery of the ring signature scheme under the ring consisting of Alice only, i.e. we set $s_0 := 0$ and randomly select t' from its domain, then the forgery is $(S_0, S_1, t_0, t_1) := (1, S, t', t)$. The validity of the forgery is readily seen. Though this instantiation relies on a stronger assumption, it enjoys higher efficiency and fewer system parameters. It also requires fewer pairing operations for $\mathsf{OFE.Ver}$ than that of the second instantiation, and has fewer system parameters than that of the first instantiation. The $\mathsf{OFE.Sig}$ does not require any pairing operation, and $\mathsf{OFE.Ver}$ requires only four pairings. Each user including the arbitrator needs to manage only one key pair (unlike the first two instantiations in which each user has two key pairs), and the public key consists of only three points on the elliptic curve (if we employ the *symmetric* group setting, i.e. $\mathbf{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_t$) [10].

5 Conclusion

In this paper we considered optimistic fair exchange in the multi-user setting and separated the security of optimistic fair exchange in the certified-key model from that in the *chosen-key* model. We proposed the efficient generic construction of optimistic fair exchange in the multi-user setting and chosen-key model and proved its security without random oracles. Our scheme is built from a conventional signature and a ring signature, both of which can be efficiently constructed without random oracles. We also discussed some efficient instantiations of our generic construction.

Acknowledgements

We'd like to thank the anonymous reviewers for their invaluable comments. The work was supported by grants from CityU (Project Nos. 7001959 and 7002001) and the Research Grants Council of the Hong Kong Special Administrative Region, China (RGC Ref. No. CityU 122107).

References

1. Asokan, N., Schunter, M., Waidner, M.: Optimistic protocols for fair exchange. In: CCS, pp. 7–17. ACM Press, New York (1997)
2. Asokan, N., Shoup, V., Waidner, M.: Optimistic fair exchange of digital signatures (extended abstract). In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 591–606. Springer, Heidelberg (1998)

3. Asokan, N., Shoup, V., Waidner, M.: Optimistic fair exchange of digital signatures. IEEE Journal on Selected Areas in Communication 18(4), 593–610 (2000)
4. Bao, F., Wang, G., Zhou, J., Zhu, H.: Analysis and improvement of Micali's fair contract signing protocol. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 176–187. Springer, Heidelberg (2004)
5. Barak, B., Canetti, R., Nielsen, J.B., Pass, R.: Universally composable protocols with relaxed set-up assumptions. In: FOCS 2004, pp. 186–195. IEEE Computer Society Press, Los Alamitos (2004)
6. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 60–79. Springer, Heidelberg (2006), http://eprint.iacr.org/
7. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)
8. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. In: EUROCRYPT 2003. LNCS, vol. 2656, pp. 416–432. Springer, Heidelberg (2003)
9. Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer, Heidelberg (2005)
10. Boyen, X.: Mesh signatures: How to leak a secret with unwitting and unwilling participants. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 210–227. Springer, Heidelberg (2007)
11. Camenisch, J., Damgård, I.: Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 331–345. Springer, Heidelberg (2000)
12. Dodis, Y., Lee, P.J., Yum, D.H.: Optimistic fair exchange in a multi-user setting. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 118–133. Springer, Heidelberg (2007) Also at Cryptology ePrint Archive, Report 2007/182, http://eprint.iacr.org/
13. Dodis, Y., Reyzin, L.: Breaking and repairing optimistic fair exchange from PODC 2003. In: DRM 2003, pp. 47–54. ACM Press, New York (2003)
14. Goldwasser, S., Micali, S., Rivest, R.: A digital signature scheme secure against adaptive chosen-message attack. SIAM J. Computing 17(2), 281–308 (1988)
15. Groth, J.: Ring signatures of sub-linear size without random oracles. In: Arge, L., Cachin, C., Jurdziński, T., Tarlecki, A. (eds.) ICALP 2007. LNCS, vol. 4596, pp. 423–434. Springer, Heidelberg (2007)
16. Kremer, S.: Formal Analysis of Optimistic Fair Exchange Protocols. PhD thesis, Université Libre de Bruxelles (2003)
17. Lu, S., Ostrovsky, R., Sahai, A., Shacham, H., Waters, B.: Sequential aggregate signatures and multisignatures without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 465–485. Springer, Heidelberg (2006)
18. Lysyanskaya, A., Micali, S., Reyzin, L., Shacham, H.: Sequential aggregate signatures from trapdoor permutations. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 74–90. Springer, Heidelberg (2004)
19. Micali, S.: Simple and fast optimistic protocols for fair electronic exchange. In: PODC 2003, pp. 12–19. ACM Press, New York (2003)

20. Park, J.M., Chong, E.K.P., Siegel, H.J.: Constructing fair-exchange protocols for e-commerce via distributed computation of RSA signatures. In: PODC 2003, pp. 172–181. ACM Press, New York (2003)
21. Rivest, R., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001)
22. Shacham, H., Waters, B.: Efficient ring signatures without random oracles. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 166–180. Springer, Heidelberg (2007)
23. Wang, G.: An abuse-free fair contract signing protocol based on the RSA signature. In: Proceedings of 14th International Conference on World Wide Web, WWW 2005, pp. 412–421. ACM Press, New York (2005)
24. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
25. Zhang, Z., Zhou, Y., Feng, D.: Efficient and optimistic fair exchanges based on standard RSA with provable security. Cryptology ePrint Archive, Report 2003/178 (2004), `http://eprint.iacr.org/`
26. Zhu, H.: Constructing optimistic fair exchange protocols from committed signatures. Cryptology ePrint Archive, Report 2005/012 (2003), `http://eprint.iacr.org/`
27. Zhu, H., Bao, F.: Stand-alone and setup-free verifiably committed signatures. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 159–173. Springer, Heidelberg (2006)
28. Zhu, H., Susilo, W., Mu, Y.: Multi-party stand-alone and setup-free verifiably committed signatures. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 134–149. Springer, Heidelberg (2007)