University of Wollongong

Research Online

Faculty of Engineering and Information
Sciences - Papers: Part A

Faculty of Engineering and Information
Sciences

1-1-2014

Revisiting optimistic fair exchange based on ring signatures

Yang Wang

University of Wollongong, yw990@uowmail.edu.au

Man Ho Au

University of Wollongong, aau@uow.edu.au

Willy Susilo

University of Wollongong, wsusilo@uow.edu.au

Follow this and additional works at: <https://ro.uow.edu.au/eispapers>

Part of the [Engineering Commons](#), and the [Science and Technology Studies Commons](#)

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Revisiting optimistic fair exchange based on ring signatures

Abstract

Optimistic fair exchange (OFE) is a kind of protocol that solves the fair exchange problem with the help of a trusted third party, usually referred to as an arbitrator. Participation of the arbitrator is required only when there is a dispute amongst the exchanging parties. Thus, the majority of the executions of the exchange does not involve the arbitrator and hence the term optimistic. The passive nature of the arbitrator makes optimistic fair exchange a desirable tool in applications such as contract signing and electronic commerce. The highest level of security of optimistic fair exchange in the literature is the multi-user security in the chosen-key model, proposed by Huang, Yang, Wong and Susilo in CT-RSA 2008. They showed that an efficient optimistic fair exchange scheme secure in this sense can be constructed generically from a conventional digital signature and a two-party ring signature. In particular, the underlying ring signature is required to be unforgeable under an adaptive attack, against a static adversary in the 2-user setting. In this paper we propose a new security model for two-party ring signatures called unforgeability against restricted adaptive attacks and demonstrate that our new model is strictly weaker than the model of unforgeable under an adaptive attack, against a static adversary in the 2-user setting. We make an observation that two-party ring signatures secure in this weaker model will suffice to guarantee the security of the resulting OFE scheme following the aforementioned generic construction. Based on this observation, more efficient OFE schemes secure in the standard model can be constructed. Specifically, we prove that the wellknown Bender, Katz and Morselli's 2-user ring signature is secure in our weakened model. Based on this two-party ring signature, we construct an OFE secure in the chosen-key model offering multi-user security in the standard model under the Computational Diffie-Hellman assumption. The assumption is arguably weaker than those used in all existing constructions, which rely on the random oracle model, decisional assumptions or the Strong Diffie-Hellman assumptions. It is also worth noting that our scheme is the most efficient one in the standard model, and offers comparable efficiency against those secure under the random oracle model.

Keywords

fair, exchange, ring, optimistic, signatures, revisiting

Disciplines

Engineering | Science and Technology Studies

Publication Details

Wang, Y., Au, M. Ho Allen. & Susilo, W. (2014). Revisiting optimistic fair exchange based on ring signatures. *IEEE Transactions on Information Forensics and Security*, 9 (11), 1883-1892.

Revisiting Optimistic Fair Exchange based on Ring Signatures

Yang Wang, Man Ho Au, *Member, IEEE* and Willy Susilo^{*¶}, *Senior member, IEEE*

Abstract—Optimistic fair exchange (OFE) is a kind of protocol that solves the fair exchange problem with the help of a trusted third party, usually referred to as an arbitrator. Participation of the arbitrator is required only when there is a dispute amongst the exchanging parties. Thus, the majority of the executions of the exchange does not involve the arbitrator and hence the term *optimistic*. The passive nature of the arbitrator makes optimistic fair exchange a desirable tool in applications such as contract signing and electronic commerce. The highest level of security of optimistic fair exchange in the literature is the multi-user security in the chosen-key model, proposed by Huang, Yang, Wong and Susilo in CT-RSA 2008. They showed that an efficient optimistic fair exchange scheme secure in this sense can be constructed generically from a conventional digital signature and a two-party ring signature. In particular, the underlying ring signature is required to be *unforgeable under an adaptive attack, against a static adversary in the 2-user setting*.

In this paper we propose a new security model for two-party ring signatures called *unforgeability against restricted adaptive attacks* and demonstrate that our new model is strictly weaker than the model of *unforgeable under an adaptive attack, against a static adversary in the 2-user setting*. We make an observation that two-party ring signatures secure in this weaker model will suffice to guarantee the security of the resulting OFE scheme following the aforementioned generic construction. Based on this observation, more efficient OFE schemes secure in the standard model can be constructed. Specifically, we prove that the well-known Bender, Katz and Morselli's 2-user ring signature is secure in our weakened model. Based on this two-party ring signature, we construct an OFE secure in the chosen-key model offering multi-user security in the standard model under the Computational Diffie-Hellman assumption. The assumption is arguably weaker than those used in all existing constructions, which rely on the random oracle model, decisional assumptions or the Strong Diffie-Hellman assumptions. It is also worth noting that our scheme is the most efficient one in the standard model, and offers comparable efficiency against those secure under the random oracle model.

Keywords: optimistic fair exchange, generic construction, two party ring signatures, restricted adaptive attacks

I. INTRODUCTION

NOWADAYS more business is conducted over the Internet, and electronic commerce grows rapidly. Thus fair exchange, i.e., how to make mutually distrustful participants exchange digital items over open networks in a fair way,

attracts a lot of interest from the research community. An exchange is said to be fair if at the end of the exchange process, either each participant receives the other's digital item, or neither participant does.

Traditionally, many digital items such as electronic checks and electronic airline tickets are implemented as digital signatures. Thus, in a fair exchange protocol, it is normally assumed that at least one of the digital items being exchanged is a signature on some message.

Optimistic fair exchange (OFE), introduced by Asokan, Schunter and Waidner [1] in 1997, is a kind of protocol to solve the fair exchange problem. An optimistic fair exchange protocol comprises signers, verifiers, and a trusted third party named "arbitrator". In such a protocol, Alice the signer first delivers a partial signature to Bob the verifier. A valid partial signature serves as a partial commitment from Alice about the exchange to take place and assures Bob that he will receive Alice's full signature at the end of the protocol. The assurance follows from the fact that the arbitrator is capable of converting the partial signature into a full one. After verifying the validity of the partial signature, Bob fulfills his obligation by delivering his digital item to Alice, after which Alice should send her full signature to complete the exchange. Note that under normal circumstances, the arbitrator does not need to be involved at all. In the case Alice refuses to send her full signature or there is a network failure, Bob shows the evidence of fulfilling his obligation and asks the arbitrator to make a resolution, in which the arbitrator converts the partial signature into a full one and sends it back to Bob.

As a useful tool in applications such as electronic commerce, optimistic fair exchange has been extensively researched [2]–[12] since its introduction. Traditionally, two popular approaches for constructing non-interactive optimistic fair exchange schemes are adopted, namely, *verifiably encrypted signatures*-based constructions [7], [8], [10], [13]–[15] and *sequential two-party multisignatures*-based constructions [4]. Most proposed OFE schemes are proven secure in the random oracle model [16], in which a hash function is treated as a random function and all users have oracle access to this random function. A proof in the random oracle model is heuristic, because such a proof may not guarantee the security when the random oracle is replaced by a concrete hash function [17].

Formally defining the security model for optimistic fair exchange turns out to be a gradual process. Security of early optimistic fair exchange protocols is studied in the single-user setting, in which an adversary is only allowed to issue the resolution queries with respect to the challenge signer.

^{*}This work was supported by ARC Future Fellowship FT0991397.

Y. Wang is with Cyberspace Security College, PLA Information Engineering University, Zhengzhou, Henan 450002, China. M. H. Au is with Hong Kong Polytechnic University, Hong Kong. and W. Susilo is with School of Computer Science and Software Engineering, University of Wollongong, Australia. E-mail: (yw990@uowmail.edu.au, csallen@comp.polyu.edu.hk, wsusilo@uow.edu.au). This work was conducted when Y. Wang and M. H. Au were with University of Wollongong.

[¶]Corresponding Author: W. Susilo. Tel: +61-2-42215535.

Due to the reality that many signers may share the same arbitrator, in 2007, Dodis, Lee and Yum [18] considered optimistic fair exchange in the multi-user setting and registered-key model [19], where an adversary is allowed to make the resolution queries with respect to any correctly generated public keys. This naturally captures the case that dishonest users may collude to cheat another user. Dodis, Lee and Yum showed that the single-user security of optimistic fair exchange does not guarantee multi-user security [18].

In 2008, Huang, Yang, Wong and Susilo [20] studied the security of optimistic fair exchange in the multi-user setting and *chosen-key model*, where an adversary can make the resolution queries even with respect to adversarially chosen public keys which may not be generated correctly. More specifically, the registered-key model assumes the authenticity of public keys and each user in the system should demonstrate its knowledge of the corresponding secret key in the public key registration stage and thus disallow various kinds of key substitution attack. However, the chosen-key model allows a user to select arbitrary public keys without the need to demonstrate its knowledge of the corresponding secret key. The chosen-key model is more practical, as in the public key infrastructure a user is not required to show its knowledge of the secret key when applying a certificate of its public key from a certification authority. They demonstrated, through an example, that an optimistic fair exchange scheme provably secure in the registered-key model may not be secure in the chosen-key model.

Since the multi-user setting and chosen-key model guarantees strong security, it would be desirable if an optimistic fair exchange scheme were secure under this model. Before the proposal of this model, previous OFE schemes based on verifiably encrypted signatures are known to be secure only in the single user setting or in the registered-key model. Huang, Yang, Wong and Susilo [20] showed that the popular paradigm of building OFE schemes from verifiably encrypted signatures can still yield schemes secure in the multi-user setting and chosen-key model if the encryption of the signature is secure against chosen ciphertext attack and that the proof of correctness is one-time simulation-sound. They argue that in the standard model, these two requirements are expensive to achieve and thus the resulting scheme from this paradigm is not efficient.

They proposed a new construction paradigm of OFE. Their construction is based on conventional signatures [21] and ring signatures [22]. They showed that the ring signature did not need to satisfy the highest level of existential unforgeability considered in [23], namely *unforgeability with respect to insider corruption*. Instead, *unforgeability under an adaptive attack, against a static adversary* [24] in the 2-user setting will suffice. Since there already exist a number of efficient conventional signatures and ring signatures that are secure without random oracles, efficient OFE schemes whose security does not rely on random oracles can be built by following Huang et al.'s generic construction. In fact, they also demonstrated the flexibility of their generic construction and discussed three efficient OFE instantiations without random oracles.

A. Our contributions

Our contributions comprise three aspects. Firstly, we propose a new security model for 2-user ring signatures, which is named “unforgeability against restricted adaptive attacks”, and compare it with the existing model *unforgeability under an adaptive attack, against a static adversary in the 2-user setting*. We separate these two models by presenting a concrete ring signature scheme, and show that our new model is strictly weaker. This means that any ring signature that is *unforgeable under an adaptive attack, against a static adversary* will also be unforgeable in our new model, but the converse may not be true.

Next, we revisit Huang et al.'s generic construction of OFE schemes from conventional signatures and ring signatures, and prove that a ring signature secure in our new model would suffice to guarantee the resulting OFE scheme's security in the multi-user setting and chosen-key model, rather than the previous understanding that the ring signature should be *unforgeable under an adaptive attack, against a static adversary*. This observation can provide us with alternatives for the ring signatures to be adopted in the OFE construction.

Finally, to demonstrate the impact of our observation, we offer a concrete OFE instantiation based on a ring signature scheme that is only secure in our weaker model, i.e., *unforgeability against restricted adaptive attacks*. This concrete OFE instantiation is *the most efficient* OFE scheme secure in the standard model in terms of signature size, generation as well as verification. Also, our OFE instantiation relies on a weak assumption, namely, the computational Diffie-Hellman assumption.

II. PRELIMINARIES

A. Complexity Assumption

We review a well-established complexity assumption, the computational Diffie-Hellman Assumption [25].

Definition 1: (Computational Diffie-Hellman Assumption). Let G be a cyclic group with generator g of prime order $p \geq 2^k$, where k is a security parameter. Given $(g, A = g^a, B = g^b)$ where a, b are uniformly chosen at random from $\mathbb{Z}_p$, we say that the computational Diffie-Hellman (CDH) assumption holds for G if for every probabilistic polynomial time (PPT) adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ in computing g^{ab} ,

$$\text{Adv}_{\mathcal{A}}(k) = \Pr[\mathcal{A}(g, A, B) = g^{ab}]$$

is negligible in k .

B. Digital signatures

SYNTAX. A signature scheme Sig comprises three efficient algorithms: $\text{SIG} = (\text{KG}, \text{Sig}, \text{Ver})$. The key generation algorithm KG takes as input a security parameter 1^k and outputs a signing key sk and a verification key vk . The signing algorithm Sig takes as input a signing key sk and a message m from the associated message space $\mathcal{M}$, and outputs a signature $\sigma \leftarrow \text{Sig}(sk, m)$. The verification algorithm Ver takes as input a message m , a signature σ and a verification key pk and outputs either $\top$ indicating valid or $\perp$ indicating invalid.

We require that $\text{Ver}(m, \text{Sig}(sk, m), vk) = \top$, for any $m \in \mathcal{M}$.

SECURITY. We consider a standard security notion for signature schemes: *existential unforgeability under adaptive chosen message attacks* [21], denoted by UF-CMA. Intuitively, this notion requires that an adversary is not able to generate a signature on a new message under the challenge public key. We define the adversary $\mathcal{A}$'s advantage $\text{Adv}_{\text{SIG}, \mathcal{A}}^{\text{UF-CMA}}(k)$ as

$$\Pr \left[\text{SIG.Ver}(m, \sigma, vk) = \top \mid \begin{array}{l} (sk, vk) \leftarrow \text{SIG.KG}(1^k), \\ (m, \sigma) \leftarrow \mathcal{A}^{O_{\text{Sig}}(\cdot)}(vk), \\ m \notin \text{Query}(\mathcal{A}, O_{\text{Sig}}(\cdot)) \end{array} \right],$$

where $\mathcal{A}$ is allowed to make a sequence of queries to the signing oracle $O_{\text{Sig}}(\cdot)$, and $\text{Query}(\mathcal{A}, O_{\text{Sig}}(\cdot))$ is the set of queries made by $\mathcal{A}$ to oracle $O_{\text{Sig}}(\cdot)$. SIG is said to be UF-CMA-secure, if the advantage function $\text{Adv}_{\text{SIG}, \mathcal{A}}^{\text{UF-CMA}}(k)$ is negligible in k for any PPT adversary $\mathcal{A}$.

In this paper, we follow the terminology used in [20] and refer to the signature schemes reviewed above as conventional signature schemes to distinguish them from ring signature schemes. Besides, we denote the signatures generated by a conventional signature scheme as conventional signatures.

C. Ring signatures

SYNTAX. A ring signature scheme RS comprises three efficient algorithms: $\text{RS} = (\text{KG}, \text{Sig}, \text{Ver})$. The key generation algorithm KG takes as input a security parameter 1^k and outputs a public verification key pk and a private signing key sk . The signing algorithm Sig takes as input a signing key sk , a message m from the associated message space $\mathcal{M}$ and a set of public keys $R := \{pk_i\}_{i=1}^l$ such that $pk \in R$ where (sk, pk) is a key pair outputted by $\text{KG}(1^k)$, and outputs a ring signature $\sigma \leftarrow \text{Sig}(sk, m, R)$. The verification algorithm Ver takes as input a message m , a ring signature σ and a list of public keys $R := \{pk_i\}_{i=1}^l$, and outputs $\top$ or $\perp$ for accept or reject. We require that $\text{Ver}(m, \text{Sig}(sk, m, R), R) = \top$, for any $m \in \mathcal{M}$.

A 2-user ring signature scheme is a specific case of the above that only supports rings R for which $|R| = 2$.

SECURITY. Two security properties that a ring signature scheme should satisfy are *anonymity* and *unforgeability*. Intuitively, anonymity requires that no one should be able to determine which number of a ring has actually generated the signature, and unforgeability requires that no one should be able to generate a ring signature if none of the ring members' private keys is known.

In Huang et al's construction of OFE, a fundamental level of anonymity, the *basic anonymity* [23], is sufficient. We review it here.

- 1) Key pairs $\{pk_i, sk_i\}_{i=1}^{n(k)}$ are generated by $\text{RS.KG}(1^k)$, and the set of public keys $R := \{pk_i\}_{i=1}^{n(k)}$ is given to an adversary $\mathcal{A}$.
- 2) $\mathcal{A}$ is provided with a ring signing oracle $O_{\text{Sig}}(\cdot, \cdot, \cdot)$, where $O_{\text{Sig}}(s, m, S)$ outputs $\text{RS.Sig}(sk_s, m, S)$, and we require that $S \subset R$ and $pk_s \in S$.

- 3) $\mathcal{A}$ submits (m^*, i_0, i_1, R^*) where $R^* \subset R$, $pk_{i_0}, pk_{i_1} \in R^*$. A random bit b is chosen and $\mathcal{A}$ is given the challenge ring signature $\sigma^* \leftarrow \text{RS.Sig}(sk_{i_b}, m^*, R^*)$.
- 4) $\mathcal{A}$ outputs a bit b' and succeeds if $b' = b$.

A ring signature scheme is said to achieve *basic anonymity* if no adversary wins the above experiment with probability non-negligibly greater than $1/2$.

For the security level of unforgeability, they consider the model *unforgeability under an adaptive attack, against a static adversary in the 2-user setting* [24]. It is defined as follows.

$$(sk_0, pk_0) \leftarrow \text{RS.KG}(1^k)$$

$$(sk_1, pk_1) \leftarrow \text{RS.KG}(1^k)$$

$$R := \{pk_0, pk_1\}$$

$$(m, \sigma) \leftarrow \mathcal{A}^{O_{\text{RS.Sig}}(R)}$$

$$\text{success of } \mathcal{A} := \left[\bigwedge \begin{array}{l} \text{RS.Ver}(m, \sigma, R) = \top \\ (\cdot, m, R) \notin \text{Query}(\mathcal{A}, O_{\text{RS.Sig}}) \end{array} \right]$$

where $\mathcal{A}$ is a PPT adversary, $O_{\text{RS.Sig}}$ is the ring signing oracle which takes as input an index $i \in \{0, 1\}$, a message m , a 2-user ring S where $pk_i \in S$, and outputs a ring signature σ on message m under the ring S using the signing key sk_i , and $\text{Query}(\mathcal{A}, O_{\text{RS.Sig}})$ is the set of ring signature queries issued by $\mathcal{A}$. A ring signature scheme is said to be (*existentially*) *unforgeable under an adaptive attack, against a static adversary in the 2-user setting* if no adversary wins the experiment with non-negligible probability.

III. A NEW MODEL FOR 2-USER RING SIGNATURES

We now define a new security model named “unforgeability against restricted adaptive attacks” for 2-user ring signatures, and then show it is strictly weaker than the model Huang et al. considered in [20] and reviewed above. Consider the following experiment.

$$(sk_0, pk_0) \leftarrow \text{RS.KG}(1^k)$$

$$(sk_1, pk_1) \leftarrow \text{RS.KG}(1^k)$$

$$R := \{pk_0, pk_1\}$$

$$(m, \sigma) \leftarrow \mathcal{A}^{O'_{\text{RS.Sig}}(R)}$$

$$\text{success of } \mathcal{A} := \left[\bigwedge \begin{array}{l} \text{RS.Ver}(m, \sigma, R) = \top \\ (m, \{\cdot, pk_1\}) \notin \text{Query}(\mathcal{A}, O'_{\text{RS.Sig}}) \end{array} \right]$$

where $\mathcal{A}$ is a PPT adversary, $O'_{\text{RS.Sig}}$ is the ring signing oracle which takes as input a message m , a 2-user ring S where $pk_1 \in S$, and outputs a ring signature σ on message m under the ring S using the signing key sk_1 , and $\text{Query}(\mathcal{A}, O_{\text{RS.Sig}})$ is the set of ring signature queries issued by $\mathcal{A}$. By “restricted adaptive”, we mean that the adversary can adaptively choose a public key pk where $pk \neq pk_1$ and makes queries to the ring signing oracle with respect to the ring $\{pk, pk_1\}$, but the adversary is prohibited from making queries with respect to the ring $\{pk, pk_0\}$. Besides, the adversary is not allowed to make a query on the challenge message with respect to any ring (however, in the model considered by Huang et al., the adversary can make queries on the challenge message with respect to any 2-user ring S such that $S \neq R$ and $S \cap R \neq \emptyset$). A ring signature scheme is said to be (*existentially*) *unforgeable against restricted adaptive attacks* if there is no adversary wins the experiment with non-negligible probability.

A. Separating Adaptive Model from Restricted Adaptive Model

In the following, we give a concrete example for showing that a 2-user ring signature scheme secure in our restricted adaptive model may not be secure in the adaptive model considered by Huang et al. The instantiation is a simple modification of Bender, Katz and Morselli's 2-user ring signature scheme [23]. More specifically, in Bender, Katz and Morselli's 2-user ring signature scheme, each user chooses his own Waters hash generators [26]. In our example, all users share the same Waters hash generators. The modified 2-user ring signature scheme $RS = (KG, \text{Sig}, \text{Ver})$ is as follows.

Let G be a multiplicative cyclic group of prime order p , g be a generator of G , and $e : G \times G \rightarrow G_T$ be a bilinear pairing where G_T is a multiplicative group of order p . Let further $u', u_1, u_2, \dots, u_n \leftarrow G$ be the Waters hash generators that are uniformly and independently chosen at random from G . Let $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ be a collision-resistant hash function. We assume the public parameter $(G, g, p, e, H, u', u_1, \dots, u_n)$ is shared by all users.

RS.KG : Choose a random exponent $\alpha \in \mathbb{Z}_p$; set $pk = g^\alpha$ and $sk = \alpha$.

RS.Sig(sk, M, R) : To sign a message $M \in \{0, 1\}^*$ with respect to the ring $R = \{pk, pk'\}$ where $sk = \alpha$ is the corresponding secret key of pk , proceed as follows: compute $(m_1, \dots, m_n) \leftarrow H(M)$, where $m_i \in \{0, 1\}$ for $i = 1$ to n , and choose random $r \leftarrow \mathbb{Z}_p$. The ring signature σ is set as

$$S_1 = (pk')^\alpha \cdot (u' \prod_{j=1}^n u_j^{m_j})^r, \text{ and } S_2 = g^r.$$

RS.Ver(M, σ, R) : To verify the signature (S_1, S_2) on message M with respect to the ring $R = \{pk, pk'\}$, compute $(m_1, \dots, m_n) \leftarrow H(M)$ and check whether

$$e(pk, pk') = e(S_1, g) \cdot e(S_2^{-1}, u' \prod_{j=1}^n u_j^{m_j}).$$

Bender, Katz and Morselli [23] proved that their ring signature scheme is unconditionally anonymous against full key exposure, the highest level of anonymity considered in [23]. They also showed that their ring signature scheme is unforgeable against chosen-subring attacks, in which the adversary is not allowed to making signing queries with respect to a ring containing adversarially-generated public keys.

On the other hand, the same scheme is known to be insecure in the adaptive model as shown in [27]. The adaptive attack described in [27] is also applicable to the modified version presented above. Indeed, to generate a signature on message $M \in \{0, 1\}^*$ with respect to the ring $R = \{pk, pk'\}$ where $sk = \alpha$ is the corresponding secret key of pk , an adversary randomly chooses $s \in \mathbb{Z}_p$, sets a public key $\bar{pk} = (pk')^s$, and asks the signing oracle to generate a signature on message M with respect to the ring $R' = \{pk, \bar{pk}\}$. Let $(m_1, \dots, m_n) \leftarrow H(M)$, the signature with respect to the ring R' will be

$$S_1 = \bar{pk}^\alpha \cdot (u' \prod_{j=1}^n u_j^{m_j})^r, \text{ and } S_2 = g^r.$$

Therefore $(S_1^{1/s}, S_2^{1/s})$ will be a ring signature with respect to the ring R on message M .

It is easy to see that the above instantiation of ring signature scheme is unconditionally anonymous against full key exposure, as the only value $(pk')^\alpha$ (where $pk = g^\alpha$) is needed to sign, and either of the two users can compute this value.

Next, we show that the above instantiation of ring signature scheme is in fact secure in our unforgeability model, i.e., unforgeable under a restricted adaptive attack.

Theorem 1: The 2-user ring signature scheme above is unforgeable against restricted adaptive attacks if the CDH assumption holds in G .

Proof. Suppose an adversary $\mathcal{A}$ breaks the unforgeability under a restricted adaptive attack. We show how to construct an algorithm $\mathcal{B}$ that produces a solution for a CDH instance. This will contradict with the CDH assumption. Let the CDH instance be $(G, p, g, A = g^a, B = g^b)$. Let q be the number of different messages contained in the queries $\mathcal{A}$ has made to the ring signing oracles.

At the start, the simulator sets an integer, $l = 4q$, and chooses uniformly at random an integer, k^* between 0 and n . It then chooses an n -length vector, $\vec{x} = (x_i)$, where the elements of $\vec{x}$ are chosen uniformly at random between 0 and $l - 1$ and a value, x' , chosen uniformly at random between 0 and $l - 1$. Besides, the simulator chooses a random $y' \in \mathbb{Z}_p$ and an n -length vector, $\vec{y} = (y_i)$, where the elements of $\vec{y}$ are chosen at random in $\mathbb{Z}_p$. The simulator keeps these values private. Let $e : G \times G \rightarrow G_T$ be a bilinear pairing where G_T is a multiplicative group of order p and $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ be a collision-resistant hash function. The simulator sets $pk_0 = A$ and $pk_1 = B$ and assigns the Waters hash generators parameters $u' = B^{p-k^*m+x'}g^{y'}$ and $u_i = B^{x_i}g^{y_i}$. The simulator forwards pk_0, pk_1 and the public parameters $(G, p, e, H, u', u_1, \dots, u_n)$ to the adversary. From the view of the adversary, the distribution of the simulated public parameters is identical to the real construction.

For ease of analysis we define the following functions where $\tilde{M}$ is the set of indices i such that $m_i = 1$ when $H(M) = (m_1, \dots, m_n)$:

$$F(M) = (p - mk^*) + x' + \sum_{i \in \tilde{M}} x_i, \text{ and } J(M) = y' + \sum_{i \in \tilde{M}} y_i.$$

Thus we have the equation

$$u' \prod_{i \in \tilde{M}} u_i = B^{F(M)} g^{J(M)}.$$

We also define a binary function $K(M)$ as

$$K(M) = \begin{cases} 0, & \text{if } x' + \sum_{i \in \tilde{M}} x_i \equiv 0 \pmod{l} \\ 1, & \text{otherwise.} \end{cases}$$

When the adversary issues a signing query on message M with respect to a ring $\{g_1, pk_1\}$ where g_1 could be pk_0 or could be adversarially-generated by the adversary, the simulator checks whether $K(M) = 0$. If so, the simulator aborts. Otherwise, the simulator chooses a random $r \in \mathbb{Z}_p$, and computes the signature as

$$S_1 = g_1^{\frac{-J(M)}{F(M)}} (u' \prod_{i \in \tilde{M}} u_i)^r, \text{ } S_2 = g_1^{\frac{-1}{F(M)}} g^r.$$

Let $\tilde{r} = r - \frac{\alpha}{F(M)}$ and $g_1 = g^\alpha$. Then we have

$$\begin{aligned}
S_1 &= g_1^{\frac{-J(M)}{F(M)}} (u' \prod_{i \in \tilde{M}} u_i)^r \\
&= g_1^{\frac{-J(M)}{F(M)}} (B^{F(M)} g^{J(M)})^r \\
&= B^\alpha (B^{F(M)} g^{J(M)})^{-\frac{\alpha}{F(M)}} (B^{F(M)} g^{J(M)})^r \\
&= B^\alpha (u' \prod_{i \in \tilde{M}} u_i)^{r - \frac{\alpha}{F(M)}} \\
&= B^\alpha (u' \prod_{i \in \tilde{M}} u_i)^{\tilde{r}}
\end{aligned}$$

Additionally, we have

$$S_2 = g_1^{\frac{-1}{F(M)}} g^r = g^{r - \frac{\alpha}{F(M)}} = g^{\tilde{r}}.$$

The simulator will be able to perform this computation if and only if $F(M) \neq 0 \pmod p$. Finally the adversary outputs a signature (S_1^*, S_2^*) on a message M^* with respect to the target ring $\{pk_0, pk_1\}$. Due to the collision-resistant property of the hash function, $H(M^*) \neq H(M)$ for any message M that had been submitted to the signing query before. Let $\tilde{M}^*$ be the set of indices i such that $m_i^* = 1$ where $H(M^*) = (m_1^*, \dots, m_n^*)$. If $x' + \sum_{i \in \tilde{M}^*} x_i = k^*l$, then we have

$$\begin{aligned}
e\left(\frac{S_1^*}{(S_2^*)^{y + \sum_{i \in \tilde{M}^*} y_i}}, g\right) &= \frac{e(A, B) e(S_2^*, u' \prod_{j=1}^n u_j^{m_j^*})}{e((S_2^*)^{y + \sum_{i \in \tilde{M}^*} y_i}, g)} \\
&= e(A, B).
\end{aligned}$$

Therefore the simulator can solve the CDH problem by computing g^{ab} as

$$g^{ab} = \frac{S_1^*}{(S_2^*)^{y + \sum_{i \in \tilde{M}^*} y_i}}.$$

Similar to [26], the probability that the simulator does not abort when simulating the signing oracle and the equation $x' + \sum_{i \in \tilde{M}^*} x_i = k^*l$ holds is at least $\lambda = \frac{1}{8(n+1)q}$, which is non-negligible. This completes the proof. $\square$

B. Separating Restricted Adaptive Model from Chosen-Subring Model

For completeness, we also study the relations between our restricted adaptive model and existing ring signature models. Specifically, we further show that, for 2-user ring signatures satisfying *basic anonymity*, our model is strictly stronger than the existing model *unforgeability against chosen-subring attacks* [23] reviewed below.

Let $RS = (KG, \text{Sig}, \text{Ver})$ be a ring signature scheme. The model *unforgeability against chosen-subring attacks in 2-user setting* is defined by the following experiment:

- 1) Key pairs $\{pk_i, sk_i\}_{i=1}^{n(k)}$ are generated by $RS.KG(1^k)$ where $n(\cdot)$ is a polynomial, and the set of public keys $R := \{pk_i\}_{i=1}^{n(k)}$ is given to an adversary $\mathcal{A}$.
- 2) $\mathcal{A}$ is provided with a ring signing oracle $\text{OSign}(\cdot, \cdot, \cdot)$, where $\text{OSign}(s, m, S)$ outputs $RS.\text{Sig}(sk_s, m, S)$, and we require that $|S| = 2$, $S \subset R$ and $pk_s \in S$.
- 3) $\mathcal{A}$ outputs (m^*, R^*, σ^*) where $|R^*| = 2$, and succeeds if $R^* \subset R$, $RS.\text{Ver}(m^*, \sigma^*, R^*) = \top$, and $\mathcal{A}$ had not queried $(\cdot, m^*, R^*)$ to the ring signing oracle.

A ring signature scheme is said to be (*existentially*) *unforgeable against chosen-subring attacks in the 2-user setting* if there is no adversary wins the above experiment with non-negligible probability.

We emphasize that, for a ring signature satisfying basic anonymity, by a hybrid argument, the above model is in fact equivalent to a model in which $\mathcal{A}$ is only given the set of two public keys $R := \{pk_1, pk_2\}$, all the ring signing queries should be queried with respect to the challenge ring R , and the final forgery of a ring signature should be with respect to the same ring R .

On the one hand, it is not hard to see that if a ring signature is unforgeable against chosen-subring attacks in the 2-user setting, it is unforgeable in the model when $n(k) = 2$, as the adversary in the experiment of unforgeable against chosen-subring attacks is provided with more resources.

On the other hand, we show below existence of an adversary $\mathcal{A}$ that succeeds in the experiment of unforgeable against chosen-subring attacks implies existence of an adversary $\mathcal{A}'$ that succeeds in the experiment when $n(k) = 2$. Recall that $\mathcal{A}'$ is given $R := \{pk_1, pk_2\}$ and its goal is to output a ring signature with respect to the challenge ring R . $\mathcal{A}'$ generates key pairs $\{pk_i, sk_i\}_{i=3}^{n(k)}$ by running $RS.KG(1^k)$ respectively where $n(\cdot)$ is a polynomial. $\mathcal{A}'$ forwards $R' := \{pk_i\}_{i=1}^{n(k)}$ to the adversary $\mathcal{A}$ and answers $\mathcal{A}$'s queries. Remember that $\mathcal{A}$ makes signing queries with respect to tuples (s, m, S) where $|S| = 2$, $S \subset R'$ and $pk_s \in S$. If $S = R$, $\mathcal{A}'$ submits the query (s, m, R) to its own oracle and forwards the reply to $\mathcal{A}$. If $s \notin \{1, 2\}$, $\mathcal{A}'$ can generate a ring signature σ using the secret key sk_s and forwards σ to $\mathcal{A}$. If $S = \{pk_s, pk_j\} \neq R$ but $s \in \{1, 2\}$, $\mathcal{A}'$ generates a ring signature σ using the secret key sk_j and forwards σ to $\mathcal{A}$. Guaranteed by the basic anonymity property of ring signatures, the replies simulated by $\mathcal{A}'$ are indistinguishable from the real ones. Finally $\mathcal{A}$ outputs a ring signature tuple (m^*, R^*, σ^*) where $|R^*| = 2$. Since the key pairs $R' := \{pk_i\}_{i=1}^{n(k)}$ have the same distribution, with non-negligible probability it will be the case $R^* = R$. That is to say, the adversary $\mathcal{A}'$ can succeed with non-negligible probability by outputting (m^*, σ^*) .

For 2-user ring signatures with basic anonymity, the argument that unforgeability against restricted adaptive attacks is a stronger model than unforgeability against chosen-subring attacks follows from the following two claims.

Claim 1: If a 2-user ring signature scheme achieves basic anonymity and is unforgeable against restricted adaptive attacks, then it is unforgeable against chosen-subring attacks.

Proof of the claim is straightforward, since, guaranteed by the basic anonymity property, any ring signature queries in the chosen-subring model with respect to the signing key sk_0 can be simulated by the adversary in the restricted adaptive model by generating a ring signature using secret key sk_1 . $\square$

Claim 2: If there exists a 2-user ring signature scheme which achieves basic anonymity and is unforgeable against chosen-subring attacks, then there exists a scheme which achieves basic anonymity, but is not unforgeable against restricted adaptive attacks.

Proof. Let $RS = (KG, \text{Sig}, \text{Ver})$ be a ring signature scheme satisfying the conditions stated in the claim. Construct the following scheme RS' from RS as follows.

- $KG'(1^k)$: Randomly pick a bit $b \in \{0, 1\}$ and run $(sk, pk) \leftarrow KG(1^k)$. Output $pk' = b || pk$ and $sk' = sk$.
- $\text{Sig}'(sk_d, m, S)$: On input a message m , a 2-user set $S := \{b_0 || pk_0, b_1 || pk_1\}$, and a secret key sk_d which is the corresponding secret key of $b_d || pk_d$ where $d \in \{0, 1\}$, if $b_0 = b_1$, it outputs $\sigma \leftarrow \text{Sig}(sk_d, m, \bar{S})$ where $\bar{S} := \{pk_0, pk_1\}$; otherwise, it outputs $\sigma \leftarrow \text{Sig}(sk_d, \bar{m}, \bar{S})$, where $\bar{m}$ is the complementary message of m , i.e. $\bar{m}$ and m are of the same bit-length but each i -th bit of them are different.
- $\text{Ver}'(m, \sigma, S)$: On input a message m , a ring signature σ , and a 2-user set $S := \{b_0 || pk_0, b_1 || pk_1\}$, if $b_0 = b_1$, it outputs $\text{Ver}(m, \sigma, \bar{S})$ where $\bar{S} := \{pk_0, pk_1\}$; otherwise, it outputs $\text{Ver}(\bar{m}, \sigma, \bar{S})$ where $\bar{m}$ is the complementary message of m .

Clearly, the above scheme RS' still achieves basic anonymity. It is also not difficult to see that it remains unforgeable against chosen-subring attacks. However, it is not unforgeable against restricted adaptive attacks, since given a challenge ring $R := \{b_0 || pk_0, b_1 || pk_1\}$, the adversary can always asks a query on message m with respect to a ring $R' := \{b'_0 || pk_0, b_1 || pk_1\}$ where $b'_0 = 1 - b_0$. In this case, the adversary can easily forge a ring signature on message $\bar{m}$ with respect to the challenge ring R where message $\bar{m}$ is the complementary message of m . $\square$

Based on the above analysis, the security guaranteed by our restricted adaptive model lies between of the securities guaranteed by *unforgeability against chosen-subring attacks* and *unforgeability under an adaptive attack, against a static adversary*.

IV. REVIEW OF OPTIMISTIC FAIR EXCHANGE

In this section, we review the definition of optimistic fair exchange, and Huang et al.'s generic construction of OFE schemes based on conventional signatures and ring signatures.

Definition 2: A non-interactive optimistic fair exchange scheme involves the users (signers and verifiers) and the arbitrator, and is formalized by the following (probabilistic) polynomial-time algorithms:

- $\text{Setup}^{\text{TTP}}$: On input 1^k , the algorithm generates a secret key ASK , and a public key APK for the arbitrator.
- $\text{Setup}^{\text{User}}$: On input 1^k and (optionally) APK , it outputs a secret key SK and a public key PK . For a user U_i , we use (SK_i, PK_i) to denote the user's key pair.
- Sig and Ver : These are similar to conventional signing and verification algorithms of an ordinary digital signature scheme. $\text{Sig}(m, SK_i, APK)$, outputs a full signature¹ σ of U_i 's on message m , while $\text{Ver}(m, \sigma, PK_i, APK)$ outputs $\top$ or $\perp$, indicating σ is a valid full signature of U_i 's on m or not.

¹In OFE, full signatures are the signatures that the exchanging parties intend to exchange and they represent the digital services the parties provide. We use this terminology to distinguish them from signatures generated by ordinary signature schemes.

- PSig and PVer : These are partial signing and verification algorithms respectively. $\text{PSig}(m, SK_i, APK)$ outputs a partial signature σ_P , while $\text{PVer}(m, \sigma_P, PK_i, APK)$ outputs $\top$ or $\perp$.
- Res : This is the resolution algorithm run by the arbitrator. $\text{Res}(m, \sigma_P, ASK, PK_i)$ outputs a full signature σ , or $\perp$ indicating the failure of resolving a partial signature.

Correctness property states that

- $\text{Ver}(m, \text{Sig}(m, SK_i, APK), PK_i, APK) = \top$, $\text{PVer}(m, \text{PSig}(m, SK_i, APK), PK_i, APK) = \top$, and $\text{Ver}(m, \text{Res}(m, \text{PSig}(m, SK_i, APK), ASK, PK_i), PK_i, APK) = \top$.

Resolution ambiguity property states that any “resolved signature” $\text{Res}(m, \text{PSig}(m, SK_i, APK), ASK, PK_i)$ is computationally indistinguishable from an “actual signature” $\text{Sig}(m, SK_i, APK)$.

A. Security in Multi-User setting and Chosen-key Model

The security of an optimistic fair exchange scheme comprises three aspects: security against signers, security against verifiers, and security against the arbitrator. Below we review the security in the multi-user setting and chosen-key model proposed in [20]. Note that in the following experiments, the adversary can make queries to the resolution oracle with respect to adversarially chosen public keys without knowing the corresponding secret keys.

SECURITY AGAINST SIGNERS. We require that the probability that any PPT adversary $\mathcal{A}$ succeeds in the following experiment is negligible in k .

$$\begin{aligned} \text{Setup}^{\text{TTP}}(1^k) &\rightarrow (ASK, APK) \\ (m, \sigma_P, PK^*) &\leftarrow \mathcal{A}^{O_{\text{Res}}}(APK) \\ \sigma &\leftarrow \text{Res}(m, \sigma_P, ASK, PK^*) \\ \text{success of } \mathcal{A} &:= \left[\bigwedge \begin{array}{l} \text{PVer}(m, \sigma_P, PK^*, APK) = \top \\ \text{Ver}(m, \sigma, PK^*, APK) = \perp \end{array} \right] \end{aligned}$$

where the resolution oracle O_{Res} takes as input a valid partial signature σ_P on message m under the public key PK_i (i.e. (m, σ_P, PK_i) such that $\text{PVer}(m, \sigma_P, PK_i, APK) = \top$), and outputs a full signature σ on m under PK_i . In other words, the signer should not be able to produce a valid partial signature such that it cannot be converted to a full signature by the honest arbitrator.

SECURITY AGAINST VERIFIERS. We require that the probability that any PPT adversary $\mathcal{A}$ succeeds in the following experiment is negligible in k .

$$\begin{aligned} \text{Setup}^{\text{TTP}}(1^k) &\rightarrow (ASK, APK) \\ \text{Setup}^{\text{User}}(1^k) &\rightarrow (SK, PK) \\ (m, \sigma) &\leftarrow \mathcal{A}^{O_{\text{PSig}}, O_{\text{Res}}}(PK, APK) \\ \text{success of } \mathcal{A} &:= \left[\bigwedge \begin{array}{l} \text{Ver}(m, \sigma, PK, APK) = \top \\ (m, \cdot, PK) \notin \text{Query}(\mathcal{A}, O_{\text{Res}}) \end{array} \right] \end{aligned}$$

where oracle O_{Res} is described in the experiment of security against signers, $\text{Query}(\mathcal{A}, O_{\text{Res}})$ is the set of queries made by $\mathcal{A}$ to oracle O_{Res} , and the partial signing oracle O_{PSig} takes as input a message m and outputs a partial signature σ_P on m .

under the challenge public key PK. In other words, the verifier himself should not be able to convert a partial signature σ_P into a full signature. Note that there is no need to provide $\mathcal{A}$ with the signing oracle, since it can be simulated by O_{PSig} and O_{Res} .

SECURITY AGAINST THE ARBITRATOR. We require that the probability that any PPT adversary $\mathcal{A}$ succeeds in the following experiment is negligible in k .

$$\begin{aligned} \text{Setup}^{\text{User}}(1^k) &\rightarrow (\text{SK}, \text{PK}) \\ (\text{ST}, \text{APK}) &\leftarrow \mathcal{A}(\text{PK}) \\ (m, \sigma) &\leftarrow \mathcal{A}^{O_{\text{PSig}}}(\text{ST}, \text{APK}, \text{PK}) \\ \text{success of } \mathcal{A} &:= \left[\begin{array}{l} \wedge \text{Ver}(m, \sigma, \text{PK}, \text{APK}) = \top \\ m \notin \text{Query}(\mathcal{A}, O_{\text{PSig}}) \end{array} \right] \end{aligned}$$

where ST is $\mathcal{A}$'s state information, which might not be the corresponding private key of APK (may contain some random coins used in the arbitrator's key pair generation process), oracle O_{PSig} is described in the previous experiment, and $\text{Query}(\mathcal{A}, O_{\text{PSig}})$ is the set of queries made by $\mathcal{A}$ to oracle O_{PSig} . In other words, the arbitrator should not be able to produce a full signature on behalf of the signer, unless the signer has generated a partial one.

Note that all the previous OFE security models do not consider the security notion of strong-unforgeability which further guarantees that an adversary cannot produce a new signature on some message that has been signed before. While strong-unforgeability is more desirable as it guarantees higher security, the standard notion of unforgeability appears to be sufficient for a number of applications of OFE. For instance, in the scenario of contract signing, a number of the signer's signatures on the same contract only mean that the signer has committed herself to the contract, and a single signature of the signer's would be sufficient to show this. Thus in this work we follow the tradition of OFE and focus on unforgeability, which makes the presentation more general.

We also make the remark that in order to guarantee fairness for the signer, the verifier has to make a proof that he has fulfilled his own obligation to the signer when he submits a resolution request to the arbitrator. Similar to previous papers [4], [18], how this is done is not formally considered in Huang et al.'s chosen-key model as this is application-specific. As suggested in [13], this issue can normally be addressed in practice by including an enforcing resolution policy γ inside the message, which states that in the resolution process the verifier has to send its own digital item (signature for instance) to the arbitrator. After the resolution, the arbitrator will send the verifier's digital item to the signer to ensure both parties will gain the other's digital item.

B. Generic Construction based on ring signatures

Huang et al. [20] showed that optimistic fair exchange schemes secure in the multi-user setting and chosen-key model could be constructed based on conventional signatures and ring signatures. We briefly review some intuitions of the construction here.

Let $\text{SIG} = (\text{KG}, \text{Sig}, \text{Ver})$ be a conventional signature scheme, and $\text{RS} = (\text{KG}, \text{Sig}, \text{Ver})$ be a ring signature scheme. Each signer has a key pair for SIG and a key pair for RS. The arbitrator has only a key pair for RS. A partial signature in the OFE scheme will be a conventional signature generated using SIG, and a full signature is the partial signature together with a ring signature generated using RS with the ring members being the signer and the arbitrator. To resolve a partial signature, the arbitrator simply uses its secret key to produce a ring signature.

Below are the details of Huang et al.'s generic construction of OFE.

- **Setup^{TPP}:** The arbitrator runs $(ask, apk) \leftarrow \text{RS.KG}(1^k)$ and sets $(\text{ASK}, \text{APK}) := (ask, apk)$.
- **Setup^{User}:** Each user U_i runs $(\hat{sk}_i, \hat{pk}_i) \leftarrow \text{SIG.KG}(1^k)$ and $(\bar{sk}_i, \bar{pk}_i) \leftarrow \text{RS.KG}(1^k)$, respectively. For a user U_i , we set $(\text{SK}_i, \text{PK}_i) := ((\hat{sk}_i, \bar{sk}_i), (\hat{pk}_i, \bar{pk}_i))$.
- **Sig:** The signer U_i first produces a conventional signature σ' on message m as the partial signature, i.e. $\sigma' \leftarrow \text{SIG.Sig}(\hat{sk}_i, m)$, and then generates a ring signature on m and its public key PK_i , i.e., $\sigma^{\text{RS}} \leftarrow \text{RS.Sig}(\bar{sk}_i, m || \text{PK}_i, R)^2$ where $R := \{\bar{pk}_i, apk\}$. The full signature is then set as $\sigma := (\sigma', \sigma^{\text{RS}})$.
- **Ver:** On input a message m and a signature σ with respect to signer U_i 's public key PK_i , where $\sigma = (\sigma', \sigma^{\text{RS}})$, the verifier checks the validity of σ' and σ^{RS} by running $\text{SIG.Ver}(m, \sigma', \hat{pk}_i)$ and $\text{RS.Ver}(m || \text{PK}_i, \sigma^{\text{RS}}, R)$ respectively, where $R := \{\bar{pk}_i, apk\}$. If both output $\top$, it returns $\top$ indicating accept; otherwise, it returns $\perp$ indicating reject.
- **PSig:** The signer U_i computes a conventional signature σ' on message m , i.e. $\sigma' \leftarrow \text{SIG.Sig}(\hat{sk}_i, m)$, and returns σ' as the partial signature.
- **PVer:** On input a message m and a partial signature σ' with respect to signer U_i 's public key PK_i , the verifier returns $\text{SIG.Ver}(m, \sigma', \hat{pk}_i)$.
- **Res:** On input a message m and a partial signature σ' with respect to a user U_i 's public key PK_i , the arbitrator first checks the validity of σ' by running $\text{SIG.Ver}(m, \sigma', \hat{pk}_i)$. If σ' is invalid, it returns $\perp$; otherwise, it computes $\sigma^{\text{RS}} \leftarrow \text{RS.Sig}(ask, m || \text{PK}_i, R)$, where $R := \{\bar{pk}_i, apk\}$. The arbitrator returns $\sigma := (\sigma', \sigma^{\text{RS}})$.

Note that even though the partial signature σ' itself is a valid conventional signature, we cannot view it as the full signature of the signer. The signer's full commitment to a message consists of a conventional signature σ' together with a ring signature σ^{RS} while the ring comprises the signer and the arbitrator. Correctness of the construction follows from that of SIG and RS, and resolution ambiguity property follows from the anonymity requirement of RS.

²In Huang et al.'s construction, the ring signature is computed on m, σ' and PK_i , i.e., $\sigma^{\text{RS}} \leftarrow \text{RS.Sig}(\bar{sk}_i, m || \sigma' || \text{PK}_i, R)$. We will later show that the security of the generic construction is still preserved even if we sign on $m || \text{PK}_i$ rather than $m || \sigma' || \text{PK}_i$.

V. SECURITY OF THE GENERIC CONSTRUCTION

In [20], Huang et al. have proved that the above generic construction of OFE is secure in the multi-user setting and chosen-key model, provided that SIG is existentially unforgeable against adaptive chosen message attacks and RS is a secure ring signature scheme that has basic anonymity and existential unforgeability under an adaptive attack, against a static adversary in the 2-user setting.

Here we will show that the construction is still secure if we adopt a ring signature scheme that is secure in our weaker model, i.e., unforgeable against restricted adaptive attacks.

Theorem 2: The generic construction of the optimistic fair exchange scheme is secure in the multi-user setting and chosen-key model, if SIG is existentially unforgeable against chosen message attacks and RS is a secure ring signature scheme that is existential unforgeable against restricted adaptive attacks.

Proof. Theorem 2 follows from the following lemmas. $\square$

Lemma 1: The generic construction of the optimistic fair exchange scheme 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 $m||PK_i$ using its own secret key, under the ring $R := \{\hat{pk}_i, apk\}$. Therefore, no adversary can win the game. $\square$

Lemma 2: The generic construction of the optimistic fair exchange scheme is secure against verifiers if RS is unforgeable against restricted adaptive attacks.

Proof. Suppose that an adversary $\mathcal{A}$ breaks the security against verifiers. We show how to construct an algorithm $\mathcal{B}$ that breaks the unforgeability against restricted adaptive attacks.

Given two public keys pk_0 and pk_1 , which are challenge public keys, $\mathcal{B}$ randomly generates a key pair $(\hat{sk}, \hat{pk})$ of SIG by running $(\hat{sk}, \hat{pk}) \leftarrow \text{SIG.KG}(1^k)$, and sets $APK := pk_1$ and $PK := (pk, pk_0)$. It then runs $\mathcal{A}$ as a subroutine with input (PK, APK) .

When $\mathcal{A}$ makes a partial signing query m to oracle O_{PSig} , $\mathcal{B}$ computes and returns $\text{SIG.Sig}(\hat{sk}, m)$ to $\mathcal{A}$. When $\mathcal{A}$ makes a resolution query (m, σ', PK'_i) where $PK'_i := (\hat{pk}'_i, \bar{pk}'_i)$ to oracle O_{Res} , $\mathcal{B}$ checks whether $\text{PVer}(m, \sigma', PK'_i, APK) = \top$. If not, $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ submits $(m||PK'_i, \{\bar{pk}'_i, pk_1\})$ to its own ring signing oracle. Let the reply be σ^{RS} , $\mathcal{B}$ forwards (σ', σ^{RS}) to $\mathcal{A}$.

The simulation is perfect. Finally, $\mathcal{A}$ outputs its forgery $(\tilde{m}, \tilde{\sigma})$, where $\tilde{\sigma} = (\tilde{\sigma}', \tilde{\sigma}^{RS})$. Thus we have $\text{RS.Ver}(\tilde{m}||PK, \tilde{\sigma}^{RS}, R) = \top$ where $R := \{pk_0, pk_1\}$. Since $(\tilde{m}, \cdot, PK) \notin \text{Query}(\mathcal{A}, O_{\text{Res}})$, $\mathcal{B}$ has never issued a query $(\tilde{m}||PK, \{\cdot, pk_1\})$ to its own ring signing oracle. Therefore $\tilde{\sigma}^{RS}$ is a valid ring signature on a new message $\tilde{m}||PK$ under the ring $\{pk_0, pk_1\}$. $\mathcal{B}$ can simply output $(\tilde{m}||PK, \tilde{\sigma}^{RS})$ and break the existential unforgeability against restricted adaptive attacks. $\square$

Lemma 3: The generic construction of the optimistic fair exchange scheme is secure against the arbitrator if SIG is unforgeable under adaptive chosen message attacks.

Proof. Since this proof only relies on the property of the conventional signature scheme SIG, the proof is the same as that in [20]. Here we will just omit it. $\square$

VI. A NEW EFFICIENT OFE SCHEME

In the following, we provide an OFE instantiation to demonstrate the significance of the generic construction when adopting a ring signature scheme that is unforgeable against restricted adaptive attacks. We will use Water's signature scheme [26] as SIG and the modified Bender-Katz-Morselli ring signature (in Section III-A) as RS.

Global Setup : On input 1^k where k is a security parameter, the setup algorithm generates a multiplicative cyclic group G of prime order p and a bilinear pairing $e : G \times G \rightarrow G_T$ where G_T is a multiplicative group of order p . Let g be a generator of G . Let $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ be a collision-resistant hash function. The setup algorithm picks independently and uniformly at random Waters hash generators $u', u_1, \dots, u_n \leftarrow G$. The public parameters shared by all users are set as $(G, p, e, H, u', u_1, \dots, u_n)$.

After the global setup is finished, the algorithms in OFE can be executed as follows.

Setup^{TTP}: The TTP chooses exponents $y \leftarrow \mathbb{Z}_p$ and sets $Y = g^y$. **APK** is set as Y . **ASK** is set as y .

Setup^{User}: User U_i randomly and independently chooses two exponents $x_i, x'_i \leftarrow \mathbb{Z}_p$, a generator $g_i \leftarrow G$, a set of Waters hash generators $u'_i, u_{i,1}, u_{i,2}, \dots, u_{i,n} \leftarrow G$ and parses $\text{SK}_i = (x_i, x'_i)$. It computes $X_i = g^{x_i}$, $X'_i = g_i^{x'_i}$ and sets $\text{PK}_i = (X_i, X'_i, g_i, u'_i, u_{i,1}, u_{i,2}, \dots, u_{i,n})$.

PSig($M, \text{SK}_i, \text{APK}$): It computes $(m_1, \dots, m_n) \leftarrow H(M)$, chooses $r \leftarrow \mathbb{Z}_p$, and computes

$$S_1 = g_i^{x_i} \cdot (u'_i \prod_{j=1}^n u_{i,j}^{m_j})^r, \text{ and } S_2 = g_i^r.$$

The partial signature is set as $\sigma_P = (S_1, S_2)$.

PVer($M, \sigma_P, \text{PK}_i, \text{APK}$): It verifies

$$e(g_i, X_i) = e(S_1, g) \cdot e(S_2^{-1}, u'_i \prod_{j=1}^n u_{i,j}^{m_j}).$$

If so, returns $\top$; otherwise it returns $\perp$.

Sig($M, \text{SK}_i, \text{APK}$): It computes $\sigma_P \leftarrow \text{PSig}(M, \text{SK}_i, \text{APK})$ and $(m'_1, \dots, m'_n) \leftarrow H(M||\text{PK}_i)$. It then chooses $r' \leftarrow \mathbb{Z}_p$ and computes

$$S'_1 = \text{APK}^{x'_i} \cdot (u' \prod_{j=1}^n u_j^{m'_j})^{r'}, \text{ and } S'_2 = g^{r'}.$$

The full signature is set as $\sigma = (\sigma_P, S'_1, S'_2)$.

Ver($M, \sigma_P, \text{PK}_i, \text{APK}$): It verifies whether $\text{PVer}(M, \sigma_P, \text{PK}_i, \text{APK}) = \top$ and whether

$$e(\text{APK}, X'_i) = e(S'_1, g) \cdot e(S'^{-1}_2, u' \prod_{j=1}^n u_j^{m'_j}).$$

If both hold, it returns $\top$; otherwise, it returns $\perp$.

Res($M, \sigma_P, \text{ASK}, \text{PK}_i$): It first verifies whether σ_P is a valid partial signature by running $\text{PVer}(M, \sigma_P, \text{PK}_i, \text{APK})$. If σ_P is

invalid, it returns $\perp$. Otherwise, it computes $(m'_1, \dots, m'_n) \leftarrow H(M || PK_i)$, chooses $r' \leftarrow \mathbb{Z}_p$, computes

$$S'_1 = (X'_i)^y \cdot (u' \prod_{j=1}^n u_j^{m'_j})^{r'}, \text{ and } S'_2 = g^{r'},$$

and returns $\sigma = (\sigma_P, S'_1, S'_2)$.

Since the securities of both Waters' signature scheme and that of the modified Bender-Katz-Morselli ring signature are based on the computational Diffie-Hellman assumption, our instantiation is secure under the computational Diffie-Hellman assumption [25], a well-established assumption on which many cryptographic primitives are based.

A. Comparison

There are only three efficient OFE schemes that are known to be secure in the multi-user setting and chosen-key model without random oracles. They are the three instantiations proposed by Huang et al. based on their generic construction. **Instantiation** $\mathcal{I}_1$ uses Waters' signature scheme [26] as SIG and Shacham-Waters's ring signature scheme [27] as RS. The security is based on sub-group decision assumption [27], [28] and computational Diffie-Hellman assumption [25]. **Instantiation** $\mathcal{I}_2$ employs Boneh-Boyen's weakly secure signature scheme [29] plus a one-time signature scheme as SIG, and Chandran-Groth-Sahai ring signature scheme [30] as RS. The security follows from a stronger assumption, i.e., strong Diffie-Hellman assumption [29], [30].

In these two instantiations, each user has two key pairs, one for the conventional signature and the other one for ring signature. To make the instantiations more practical and efficient, it may be more desirable to combine the two key pairs into one. Thus in **Instantiation** $\mathcal{I}_3$, Boyen's ring signature [24] (or, say, his mesh signature) is employed. In Boyen's ring signature scheme, each user owns a single key pair, and the adversary can ask not only ring signature queries, but also atomic (or conventional) signature queries. The security is based on Poly Strong Diffie-Hellman assumption introduced by Boyen [24], which is a stronger variant of the Strong Diffie-Hellman assumption.

Compared with the three instantiations suggested by Huang et al., our instantiation has the advantage of relying on simpler assumption.

As a side note, the most efficient scheme in the random oracle model is based on the verifiably-encrypted signature [15] and secure in the single-user setting under the CDH assumption. Next we compare the performance of our instantiation with Huang et al.'s three instantiations and the most efficient OFE scheme in the random oracle model (we call it BGLS scheme). Since pairing and exponentiation operations take more time than multiplication operations do, we will simply ignore the costs of multiplication computations and hash evaluations. Besides, the calculations that can be done off-line are not counted in the evaluation of the performances of the schemes. Let "E" denote an exponentiation operation, and "P" denote a pairing operation. By "OFE.Sig elements", "OFE.Sig costs" and "OFE.Ver costs", we mean the number of group elements of a full signature, the cost of generating

Schemes:	OFE.Sig elements	OFE.Sig costs	OFE.Ver costs
$\mathcal{I}_1$	8	7E	8P
$\mathcal{I}_2$	10	12E	9P
$\mathcal{I}_3$	8	10E	8E + 4P
BGLS	1	1E	2P
Ours	4	4E	4P

TABLE I
PERFORMANCE COMPARISON

a full signature, and the cost of verifying a full signature, respectively. The table I summarizes the performances of Huang et al.'s instantiations, BGLS scheme, and our instantiation. From the table, it is clear that, compared with Huang et al.'s instantiations, our instantiation saves almost 50% or even more of the costs in both generating a full signature and verifying a full signature. Besides, the number of group elements of the full signature in our instantiation is only half of those in Huang et al.'s instantiations. It should also be noted that **Instantiation** $\mathcal{I}_1$ requires the use of composite order groups equipped with a bilinear map, which is known to be less efficient compared with prime-order groups equipped with bilinear map.

For the generation and verification of a partial signature of BGLS scheme, the cost are 3 exponentiations and 3 pairing operations, respectively. The partial signature size of BGLS scheme is 2 group elements. On the contrary, the costs for generating and verifying a partial signature of our scheme are 2 exponentiations and 2 pairing operations, respectively. The partial signature size of our scheme is 2 group elements. It is fair to say our construction performs comparably to the most efficient scheme secure in the random oracle model.

VII. CONCLUSION

It is well-known that efficient optimistic fair exchange schemes without random oracles can be built from conventional signatures and ring signatures. To guarantee the resulting OFE scheme's security in the multi-user setting and chosen-key model, it was previously believed that the ring signature scheme should be unforgeable under an adaptive attack, against a static adversary in the 2-user setting. In this paper, we proposed a new weaker model for ring signatures named "unforgeability against restricted adaptive attacks", and proved that a 2-User ring signature secure in our weaker model was sufficient to guarantee the resulting OFE scheme's security. This observation makes it feasible to construct more efficient OFE schemes whose security relies on a weaker assumption.

REFERENCES

- [1] N. Asokan, M. Schunter, and M. Waidner, "Optimistic protocols for fair exchange," in *Proc. 4th ACM Conference on Computer and Communications Security*, 1997, pp. 8–17.
- [2] O. Markowitch and S. Saeednia, "Optimistic fair exchange with transparent signature recovery," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, P. F. Syverson, Ed., vol. 2339. Springer, 2001, pp. 329–340.
- [3] S. Micali, "Simple and fast optimistic protocols for fair electronic exchange," in *Proceedings of the twenty-second annual symposium on Principles of distributed computing*, ser. PODC '03. New York, NY, USA: ACM, 2003, pp. 12–19. [Online]. Available: <http://doi.acm.org/10.1145/872035.872038>

- [4] Y. Dodis and L. Reyzin, "Breaking and repairing optimistic fair exchange from podc 2003," in *Proceedings of the 3rd ACM workshop on Digital rights management*, ser. DRM '03. New York, NY, USA: ACM, 2003, pp. 47–54. [Online]. Available: <http://doi.acm.org/10.1145/947380.947387>
- [5] G. Wang, "An abuse-free fair contract signing protocol based on the rsa signature," in *Proceedings of the 14th international conference on World Wide Web*, ser. WWW '05. New York, NY, USA: ACM, 2005, pp. 412–421. [Online]. Available: <http://doi.acm.org/10.1145/1060745.1060807>
- [6] P. D. Ezhilchelvan and S. K. Shrivastava, "A family of trusted third party based fair-exchange protocols," *IEEE Trans. Dependable Secur. Comput.*, vol. 2, pp. 273–286, October 2005. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1100865.1100969>
- [7] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters, "Sequential aggregate signatures and multisignatures without random oracles," in *EUROCRYPT, 2006*. Springer, 2006, pp. 465–485.
- [8] J. Zhang and J. Mao, "A novel verifiably encrypted signature scheme without random oracle," in *Proceedings of the 3rd international conference on Information security practice and experience*, ser. ISPEC'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 65–78. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1759508.1759518>
- [9] Y. Okada, Y. Manabe, and T. Okamoto, "An optimistic fair exchange protocol and its security in the universal composability framework," *Int. J. Appl. Cryptol.*, vol. 1, pp. 70–77, February 2008. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1356045.1356051>
- [10] M. Rückert and D. Schröder, "Security of verifiably encrypted signatures and a construction without random oracles," in *Proceedings of the 3rd International Conference Palo Alto on Pairing-Based Cryptography*, ser. Pairing '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 17–34.
- [11] S. Heidavand and J. L. Villar, "Fair and abuse-free contract signing protocol from boneh-boyen signature," in *Proceedings of the 7th European conference on Public key infrastructures, services and applications*, ser. EuroPKI'10. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 125–140. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2035155.2035168>
- [12] Q. Huang, D. S. Wong, and W. Susilo, "Group-oriented fair exchange of signatures," *Inf. Sci.*, vol. 181, pp. 3267–3283, August 2011. [Online]. Available: <http://dx.doi.org/10.1016/j.ins.2011.03.024>
- [13] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," *Advances in Cryptology-Eurocrypt 1998, Lecture Notes in Computer Science 1403*, pp. 591 – 606, 1998.
- [14] J. Camenisch and I. Damgård, "Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes," in *Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ser. ASIACRYPT '00. London, UK: Springer-Verlag, 2000, pp. 331–345. [Online]. Available: <http://dl.acm.org/citation.cfm?id=647096.716992>
- [15] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," *Advances in cryptology - Eurocrypt 2003, Lecture Notes in Computer Science*, vol. 2656, pp. 416–432, 2003.
- [16] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *ACM Conference on Computer and Communications Security*, D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, and V. Ashby, Eds. ACM, 1993, pp. 62–73.
- [17] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited (preliminary version)," in *STOC*, J. S. Vitter, Ed. ACM, 1998, pp. 209–218.
- [18] Y. Dodis, P. J. Lee, and D. H. Yum, "Optimistic fair exchange in a multi-user setting," in *Proceedings of the 10th international conference on Practice and theory in public-key cryptography*, ser. PKC'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 118–133. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1760564.1760577>
- [19] B. Barak, R. Canetti, J. B. Nielsen, and R. Pass, "Universally composable protocols with relaxed set-up assumptions," in *FOCS'04*, 2004, pp. 186–195.
- [20] Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Efficient optimistic fair exchange secure in the multi-user setting and chosen-key model without random oracles," in *Proceedings of the 2008 The Cryptographers' Track at the RSA conference on Topics in cryptology*, ser. CT-RSA'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 106–120. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1791688.1791698>
- [21] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, 1988.
- [22] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *ASIACRYPT*, ser. Lecture Notes in Computer Science, C. Boyd, Ed., vol. 2248. Springer, 2001, pp. 552–565.
- [23] A. Bender, J. Katz, and R. Morselli, "Ring signatures: Stronger definitions, and constructions without random oracles," *J. Cryptology*, vol. 22, no. 1, pp. 114–138, 2009.
- [24] X. Boyen, "Mesh signatures," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, M. Naor, Ed., vol. 4515. Springer, 2007, pp. 210–227.
- [25] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [26] B. Waters, "Efficient identity-based encryption without random oracles," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, R. Cramer, Ed., vol. 3494. Springer, 2005, pp. 114–127.
- [27] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in *Public Key Cryptography*, ser. Lecture Notes in Computer Science, T. Okamoto and X. Wang, Eds., vol. 4450. Springer, 2007, pp. 166–180.
- [28] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in *TCC*, ser. Lecture Notes in Computer Science, J. Kilian, Ed., vol. 3378. Springer, 2005, pp. 325–341.
- [29] D. Boneh and X. Boyen, "Short signatures without random oracles," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds., vol. 3027. Springer, 2004, pp. 56–73.
- [30] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sub-linear size without random oracles," in *ICALP*, ser. Lecture Notes in Computer Science, L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki, Eds., vol. 4596. Springer, 2007, pp. 423–434.

Yang Wang received his Ph.D. degree from the University of Wollongong, Wollongong (UOW) in 2014. He is now a lecturer in Cyberspace Security College, PLA Information Engineering University, Zhengzhou, Henan 450002, China. His research interests include applied cryptography, fair exchange and security analysis of protocols.

Man Ho Au (M12) received his PhD from the University of Wollongong (UOW) in 2009. Currently, he is an assistant professor at the Department of Computing, Hong Kong Polytechnic University (PolyU). Before joining PolyU in July 2014, he was a lecturer in UOW. He works in the area of information security. In particular, his research interests include applying public-key cryptographic techniques to systems with security and privacy concerns. He has published over 70 referred journal and conference papers.

Willy Susilo (SM01) received his PhD degree from the University of Wollongong (UOW) in 2001. He is a Professor and the Director of Centre for Computer and Information Security Research, University of Wollongong. He held the prestigious ARC Future Fellow awarded by the Australian Research Council. His main research interests include cryptography and information security. His main contribution is in the area of digital signature schemes. He has published over 300 refereed journal and conference papers.