Future Generation Computer Systems 62 (2016) 29–39

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Provably secure robust optimistic fair exchange of distributed signatures

Yujue Wang [a,g], Qianhong Wu [b,e], Duncan S. Wong [c], Bo Qin [d,e,*], Jian Mao [b,h], Yong Ding [f]

[a] School of Information Systems, Singapore Management University, Singapore
[b] School of Electronic and Information Engineering, Beihang University, Beijing, China
[c] Department of Computer Science, City University of Hong Kong, Hong Kong, China
[d] Key Laboratory of Data Engineering and Knowledge Engineering, Ministry of Education, School of Information, Renmin University of China, Beijing, China
[e] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China
[f] School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, China
[g] State Key Laboratory of Integrated Services Networks, Xidian University, Xian, China
[h] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China

HIGHLIGHTS

- We model optimistic fair exchange between two groups.
- We define security in optimistic fair exchange of distributed signatures (OFEDS).
- OFEDS supports most generic access structure.
- The first OFEDS scheme is presented with robustness and non-interactive properties.
- Our scheme is proven secure under standard assumption.

ARTICLE INFO

Article history:
Received 22 October 2014
Received in revised form
17 February 2016
Accepted 16 March 2016
Available online 25 March 2016

Keywords:
Optimistic fair exchange
Distributed signature
Secret sharing
Monotone span program
Verifiably encrypted signatures

ABSTRACT

We introduce the concept of optimistic fair exchange of distributed signatures (OFEDS) which allows two groups of parties to fairly exchange digital signatures. Specifically, an authorized set of parties from each group can jointly take part in the protocol on behalf of the affiliated group to fulfill obligation, and a semi-trusted arbitrator will intervene in the protocol only when there are disputes between two sides. Our OFEDS extends the functionality of optimistic fair exchange of threshold signatures to a more generic case. We formalize the security model of OFEDS, in which besides the standard security requirements for existing optimistic fair exchange protocols, robustness is incorporated so that OFEDS can be successfully performed even when there exist some dishonest signers. We propose a non-interactive construction of OFEDS based on the well-established Computational Diffie–Hellman (CDH) assumption. Our proposal shows that there exists CDH-based OFEDS for any general monotone access structure. Theoretical and experimental analyses demonstrate our OFEDS construction has reasonable efficiency for real applications.

1. Introduction

Optimistic fair exchange (OFE) [1] allows two parties to exchange electronic items (e.g., electronic contracts) in a fair manner, i.e., either both parties obtain their expected items or neither party can do. A standard OFE protocol involves three parties, namely, party A, party B and an arbitrator. Among them, the arbitrator is semi-trusted and is intended to help A and B for resolving disputes during the item exchange process. In practice, the arbitrator is usually keeping offline unless either party A or B is cheated. The OFE protocol is carried out in three regular moves and two standby moves. Specifically, the party A first generates a *partial signature* which may be a verifiable encryption [2] of her *full signature* and gives it to B, who validates the received item and sends back

[*] Correspondence to: School of Information, Renmin University of China, No. 59, Zhongguanchun Avenue, Haidian District, 100872, Beijing, China. Tel.: +86 10 6251 2492.
E-mail address: bo.qin@ruc.edu.cn (B. Qin).

http://dx.doi.org/10.1016/j.future.2016.03.012
0167-739X/© 2016 Published by Elsevier B.V.

Table 1
Comparison of OFE schemes in multi-user setting.

Scheme	Functionality
Dodis, Lee and Yum [36]	OFE between *two individuals* with *one arbitrator*
Huang et al. [37]	OFE between *two individuals* with *one arbitrator*
Huang et al. [38]	OFE between *two individuals* with *one arbitrator*
Küpçü and Lysyanskaya [39]	OFE between *two individuals* with *multiple arbitrators*
Huang, Wong and Susilo [4]	OFE between *two parties* on behalf of *respective groups*
Qu et al. [5]	OFE between *two parties* on behalf of *respective rings*
Wang et al. [6]	OFE between *two authorized sets* more than a *threshold*
This paper	OFE between *two authorized sets* of *generic form*

his full signature to A when the validation result is true. If A accepts B's full signature and further provides her full signature to B, then these two parties have successfully exchanged their digital items, i.e., full signatures. Otherwise, if A refuses to fulfill her responsibility after receiving B's valid item, then B can ask the arbitrator for resolution by running standby moves. Note that OFE is different from oblivious transfer (OT) protocol [3], where OT allows users to exchange *secret* information in a fair manner.

Since its introduction, OFE has been received considerable attentions, of which several protocols were proposed in multi-user settings, e.g., [4–6]. However, all the existing OFE protocols cannot effectively support the applications in a more complicated scenario as follows. For example, a group of manufactories trying to sign a contract with a group of selling companies so that they can unify prices to avoid over competition. The authorized subset (e.g., several qualified representatives) is capable to sign it on behalf of the affiliated group, while none of the unauthorized ones can do so. In fact, here, the authorized sets constitute a *monotone access structure* which is similar to that in secret sharing schemes [7–9] and distributed signature schemes [10–14], which capture the threshold ones as special cases. Threshold primitives [15–18] can only support regular access policies, i.e., a set is authorized if it comprises at least a quorum of parties. Therefore, even the OFE protocol of threshold signatures [6] cannot apply to this generic setting. Note that the most related protocols, i.e., OFE protocols of group/ring signatures [4,5], just allow a single member from different groups to fairly exchange their digital items on behalf of respective groups. These types of protocols also cannot be applied to such complicated scenarios. This motivates the work in this paper.

1.1. Our contribution

We observe a gap in existing OFE models and instantiated protocols (as shown in Table 1). Specifically, to the best of our knowledge, there are no studies in the public literatures which work on fairly exchanging distributed signatures with regard to general monotone access structures. The monotone access structure has the desirable expressiveness to define the authorized set, and hence, is flexible and versatile in practice. Therefore, motivated by the above scenario, we extend the existing OFE concept to a multi-user setting in which both groups A and B consist of multiple users, and the corresponding authorized subsets of A and B can perform the role of these groups for fairly exchanging digital items. Particularly, we are interested in providing a universal solution to such applications.

First, we introduce the notion of *optimistic fair exchange of distributed signatures* (OFEDS) and present a formal definition. We also formalize the security model of OFEDS which includes the security requirements of standard OFE protocols, such as ambiguity and security against signers, verifier and arbitrator, respectively. The difference lies in that these security requirements are defined on a group of parties, rather than a single party (see Section 3.2 for details). Furthermore, a security requirement called *robustness* is incorporated so that distributed signatures can be successfully exchanged in a fair way even if there are some malicious users (signers).

Second, we present a non-interactive CDH-based OFEDS construction with better expressiveness, where the generic access structure is modeled by *monotone span program* (MSP). It is shown that the proposed OFEDS protocol meets all the security requirements that defined in the security model. Since the facts that every monotone access structure can be realized by a *linear secret sharing scheme* (LSSS) and LSSS has been proved equivalent to MSP [7], our construction can apply to any monotone access structures. Therefore, our construction covers the existing threshold-oriented OFE protocols as a special case.

Third, we thoroughly analyze our OFEDS construction from both theoretical and experimental perspectives. Only the user-key-generation algorithm has linear computation costs with the cardinality of the signer set. The efficiencies of partial-/full-signature-reconstruction algorithms are related to the signer number in an authorized set. All the other algorithms have constant computations. Therefore, the performance analyses show that the proposed OFEDS protocol is practical to support real applications.

Compared to the preliminary version [19], the contribution of this full paper lies in that the majority of Section 1 is revised, and moreover, the formal security model of OFEDS as well as the security proofs of our construction in the random oracle model are presented. The performance evaluations and analyses of our OFEDS construction are also the new results of this paper.

1.2. Related work

OFE for exchanging items between two parties in a *fair* way was first proposed by Asokan, Schunter and Waidner [1], where the arbitrator is needed only in case of depute occurrence. *Fairness* is an important and desirable property in many real-world applications and has received plenty of research attentions. For example, fairness in e-payments [20] guarantees the involved parties could get either their bought goods or payments with the help of online/offline bank. Fairness is also a fundamental requirement for players when carrying out online contests [21] like e-auctions and e-games, in the sense that all of unfair competitions should be prevented from the system.

To prevent the verifier (i.e., party B) from abusing the received partial signature from party A, Huang et al. [22] introduced *ambiguous* OFE which enhances the security at the signer side. In [23], Huang, Wong and Susilo presented an interactive ambiguous OFE based on the designated confirmer signature such that when generating the partial signature, the signer should interact with the verifier. Furthermore, Wang et al. [24] managed to enhance the security at both sides of A and B, that is, the communication transcripts will leak nothing with regard to the involved parties. To this end, they introduced the concept of *perfect ambiguous* OFE. Recently, Huang et al. [25] investigated *privacy-preserving* OFE with more rigorous security in the sense that even the arbitrator cannot learn the resolved signatures, which further enhances the