Information Sciences 325 (2015) 300–315

Contents lists available at ScienceDirect

Information Sciences

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

How to protect privacy in Optimistic Fair Exchange of digital signatures☆

Qiong Huang[a,*], Duncan S. Wong[b], Willy Susilo[c]

[a] College of Mathematics and Informatics, South China Agricultural University, 483 Wushan Road, Guangzhou 510642, China
[b] Department of Computer Science, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, China
[c] School of Computer Science and Software Engineering, University of Wollongong, Northfields Avenue, Wollongong, Australia

ARTICLE INFO

Article history:
Received 19 July 2014
Revised 9 January 2015
Accepted 8 July 2015
Available online 17 July 2015

Keywords:
Optimistic Fair Exchange
Signature
Ambiguity
Privacy preserving

ABSTRACT

How to sign an electronic contract online between two parties (say Alice and Bob) in a fair manner is an interesting problem, and has been extensively studied for a long time. Optimistic Fair Exchange (OFE) is an efficient solution to it, in which a semi-trusted third party, named the *arbitrator*, is responsible for resolving any dispute that may arise during an exchange between Alice and Bob. Recently, several variants of OFE, such as Ambiguous OFE (AOFE) and Perfect AOFE (PAOFE), have been introduced to protect the privacy of Alice and Bob. These primitives prevent any outsider from telling which parties are involved in an exchange of digital signatures *before* the exchange completes. However, in PAOFE, AOFE and all the existing works on OFE, the arbitrator can always learn the signer's full signature *at* (or even *before*) the end of resolution, which is undesirable in some important applications, for example, signing a contract between two parties which do not want others to find out even when there is a dispute that needs resolution by the arbitrator.

In this work, we introduce a new notion called *Privacy-Preserving Optimistic Fair Exchange* (P^2OFE) for protecting the privacy of users, in which other than Alice and Bob, no one else including the arbitrator, can collect any evidence about an exchange between them even after the resolution of a dispute. We formally define P^2OFE and present the corresponding security models and propose a concrete and efficient construction of P^2OFE. We also discuss about several extensions about implementation. Our scheme is proved to be secure under the given security models based on the Strong Diffie–Helllman and Decision Linear assumptions without relying on the random oracle heuristic.

© 2015 Elsevier Inc. All rights reserved.

1. Introduction

The fair exchange problem is about constructing a protocol for two parties, Alice and Bob, that allow them to exchange items in an all-or-nothing (fair) manner, that is, after the protocol, either both parties obtain the other's item or none of them does. There are two major approaches to do fair exchange. The first one is to have the parties release their secrets 'gradually', e.g. bit by

☆ A preliminary version of this work appears in the proceedings of CT-RSA 2014 [23]. This work is supported by National Natural Science Foundation of China (Nos. 61472146, 61103232), Guandong Natural Science Foundation (No. S2013010011859), and Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2014A030306021). D. S. Wong is supported by a grant from the RGC of the HKSAR, China (Project no. CityU 121512). W. Susilo is supported by ARC Future Fellowship FT0991397.

* Corresponding author. Tel.: +86 20 85285389.
E-mail addresses: csqhuang-c@my.cityu.edu.hk (Q. Huang), duncan@cityu.edu.hk (D.S. Wong), wsusilo@uow.edu.au (W. Susilo).

http://dx.doi.org/10.1016/j.ins.2015.07.032
0020-0255/© 2015 Elsevier Inc. All rights reserved.

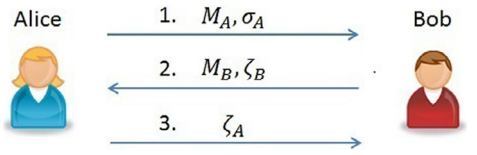

Fig. 1. OFE: normal execution.

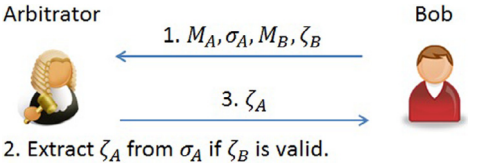

Fig. 2. OFE: resolution.

bit, in multiple rounds. Besides, it is assumed that both of them have comparable computation power. Thus, this approach may not be appropriate for practical use.

Another approach is *Optimistic Fair Exchange* (OFE), the notion of which was introduced by Asokan et al. [1] and later extended to support the exchange of digital signatures [2]. In OFE there is a third party called *arbitrator*, which is semi-trusted by the two parties. It is usually offline and gets involved only when there is a dispute. Alice prepares an 'encapsulated' version of her signature, called *partial signature* and denoted by σ_A, and sends it to Bob. After confirming the validity of σ_A, Bob returns his *full signature* ζ_B to Alice. In the third move, Alice tells Bob how to 'decapsulate' σ_A or directly sends her full signature ζ_A to Bob if she believes ζ_B is valid. Fig. 1 shows a normal execution of OFE. If Alice refuses or fails to return ζ_A, Bob resorts to the arbitrator for resolving σ_A. After checking the fulfillment of Bob's obligation, the arbitrator extracts ζ_A from σ_A, and sends it to Bob. Fig. 2 shows the resolution process.

Due to the simple and elegant framework, and the low level of trust on the third party, OFE has many useful applications. One of them is to sign contracts between two online parties. For example, Alice wants to buy a software from Bob's online shop. She generates a partial signature on a message "Bob can withdraw $100 from my bank account". Bob then gives Alice his full signature on message "Alice can get a copy of Windows 10 from my shop". If everything goes well, Alice gets the software and Bob gets the money from Alice's bank account. In case Bob does not get the full signature of Alice, Bob asks the arbitrator for resolving Alice's partial signature to a full one.

On the privacy of OFE and its variants: In conventional OFE, Alice's partial signature σ_A already reveals her intention to exchange with Bob, from which Bob may take advantage. This is unfair to Alice. In [16,25], the notion of *Ambiguous* Optimistic Fair Exchange (AOFE)[1] was introduced to remove the unfairness. In AOFE, Bob is endowed with the ability of producing partial signatures computationally indistinguishable from those of Alice. Recently, Wang et al. [38] proposed an enhanced version of AOFE, named *Perfect* AOFE (PAOFE), in which a partial signature leaks no information about the actual signer or the intended verifier. This is useful for applications where the involved parties of an exchange wish to further protect their privacy of whether they are indeed involved in an exchange. For instance, Alice and Bob sign a business contract (e.g. a procurement deal) online. Revealing who is involved in the process may be potentially harmful to (the image of) Alice and/or Bob. Using PAOFE, no one including the arbitrator can tell who and what exchange has taken place from the transcript of a normal execution.

Although the privacy is ensured in a normal execution of PAOFE, this is not the case if a dispute occurs and a resolution is solicited. At the end of resolution in (P)(A)OFE, the arbitrator gets the full signature ζ_A of Alice. Hence, the arbitrator could confirm if a particular party, say Alice, was involved in an exchange. Whereas there are applications in which the parties do not want anyone including the arbitrator to confirm and especially, convince others about their involvement in an exchange. Even in the example above, revealing and confirming who was involved in the business contract to the arbitrator during a dispute may potentially hurt (the image of) Alice and/or Bob. We stress here that revealing the contract (i.e. the message) itself (*without the signatures*) does not entail any concern on revealing, or letting outsiders or the arbitrator to confirm the involvement of a particular party in an exchange. This is because such a contract/message can be made up by anyone. Only the signed contract can be used to confirm a party's involvement. In this scenario, PAOFE would not help because the arbitrator learns the final signature ζ_A at the end of the resolution and hence can confirm the involvement of Alice. The arbitrator can even convince others about Alice's involvement by making use of ζ_A.

Our contributions: In this paper we contribute to the study of fair exchange in the following aspects:

1. We introduce the notion of *Privacy-Preserving* OFE (P^2OFE). It differs from PAOFE mainly in that P^2OFE explicitly requires that even the arbitrator cannot learn the signer's full signature. The resolution in P^2OFE is a protocol between the verifier and the arbitrator, and consists of two algorithms, Res^A and Res^V. Briefly, after receiving a partial signature σ for resolution,

[1] It is named *abuse-free contract signing* in [16] and *ambiguous optimistic fair exchange* in [25]. Hereafter we call it ambiguous Optimistic Fair Exchange (AOFE), for the sake of the ease of presentation.

Download English Version:

https://daneshyari.com/en/article/6857618

Download Persian Version:

https://daneshyari.com/article/6857618

Daneshyari.com