Theoretical Computer Science 562 (2015) 177–193

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Ambiguous optimistic fair exchange: Definition and constructions ☆

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

[a] College of 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 Special Administrative Region, China
[c] School of Computer Science and Software Engineering, University of Wollongong, Northfields Avenue, Wollongong, Australia

ARTICLE INFO

Article history:
Received 2 June 2013
Received in revised form 15 July 2014
Accepted 23 September 2014
Available online 30 September 2014
Communicated by G. Ausiello

Keywords:
Optimistic fair exchange
Ambiguity
Signature
NIZK proof
Standard model

ABSTRACT

Optimistic fair exchange (OFE) is a protocol for solving the problem of exchanging items or services in a fair manner between two parties, a signer and a verifier, with the help of an arbitrator which is called in only when a dispute happens between the two parties. In almost all the previous work on OFE, after obtaining a partial signature from the signer, the verifier can present it to others and show that the signer has indeed committed itself to something corresponding to the partial signature *even* prior to the completion of the transaction. In some scenarios, this capability given to the verifier may be harmful to the signer. In this paper, we propose the notion of *ambiguous optimistic fair exchange* (AOFE), which is a variant of OFE and requires additionally that the verifier cannot convince anybody about the authorship of a partial signature generated by the signer. We present a formal security model for AOFE in the multi-user setting and chosen-key model, and propose a generic construction of AOFE that is provably secure under our model. Furthermore, we propose an efficient instantiation of the generic construction, security of which is based on Strong Diffie–Hellman assumption and Decision Linear assumption without random oracles.

1. Introduction

Optimistic Fair Exchange (OFE) allows two parties to fairly exchange information in such a way that at the end of a protocol run, either both parties have obtained the complete information from one another or none of them has obtained anything from the counter party. In an OFE, there is a third party, called Arbitrator, which is only called in when a dispute occurred between the two parties. OFE is a useful tool in practice, for example, it can be used for performing contract signing, fair negotiation and similar applications on the Internet. Since its introduction [1], there have been many OFE schemes proposed [2,16,3,11,33,14,29,32,38,4,34,15,21,35]. For all recently proposed schemes, an OFE protocol for signature

☆ A preliminary version of this paper appeared in ASIACRYPT 2008 [20]. This is a vastly extended version. This work is supported by the National Natural Science Foundation of China (Nos. 61103232, 61472146), the Guangdong Natural Science Foundation (No. S2013010011859) and the Research Fund for the Doctoral Program of Higher Education of China (No. 20114404120027). 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.
E-mail addresses: csqhuang-c@my.cityu.edu.hk (Q. Huang), gyang@uow.edu.au (G. Yang), duncan@cityu.edu.hk (D.S. Wong), wsusilo@uow.edu.au (W. Susilo).

http://dx.doi.org/10.1016/j.tcs.2014.09.043
0304-3975/

typically consists of three message flows. The initiator of OFE, Alice, first sends a *partial signature* σ_P to a responder, Bob, where σ_P is considered as Alice's partial commitment to her full signature which will be sent to Bob. But beforehand, Bob should send his full signature back to Alice first in the second message flow. After receiving Bob's full signature, Alice then sends her full signature to Bob in the third message flow. If Bob refuses to send his full signature to Alice in the second message flow, σ_P should have no use to Bob, so that Alice has no concern about giving away σ_P. However, after Bob has sent his full signature to Alice while Alice refuses to send her full signature in the third message flow, then Bob can ask the Arbitrator to retrieve Alice's full signature from σ_P by sending both σ_P and Bob's full signature to the Arbitrator. To the best of our knowledge, among almost all the known OFE schemes, there is one common property about Alice's partial signature σ_P which has neither been captured in any of the security models for OFE nor been considered as a requirement for OFE. The property is that once σ_P is given out, at least one of the following statements is true.

1. Everyone can verify that Alice generates σ_P, because σ_P, similar to a standard digital signature, has the non-repudiation property with respect to Alice's public key;
2. Bob can show to anybody that Alice is the signer of σ_P.

For example, in [15,21], the partial signature of Alice is a standard signature, which can only be generated by Alice. In many other OFE schemes, Alice's signature is encrypted under the arbitrator's public key, and then a non-interactive proof is generated to show that the ciphertext indeed contains a signature of Alice. This is known as *verifiably encrypted signature*. However, regarding the validity and non-repudiation of a signature, as pointed out by Boyd and Foo [10], this raises the question of whether a non-interactive proof that a signature is encrypted is really having any difference from a signature itself, as the proof is already sufficient to convince any third party that the signer has committed to the message.

This property may cause no concern in some applications, for example, in those where only the full signature is deemed to have some actual value to the receiving party. However, it may be undesirable in some other applications. Since σ_P is publicly verifiable and non-repudiative, σ_P has evidently shown Alice's commitment to the corresponding message. This may incur some unfair situation, to the advantage of Bob, if Bob does not send out his full signature. In contract signing applications, this could be undesirable because σ_P can already be considered as Alice's undeniable commitment to a contract in court while there is no evidence showing that Bob has committed to anything. For example, Alice wants to sign with Bob a contract of procuring Bob's company. After sending out her partial signature, Alice has no way to regret and cannot withdraw the procurement if Bob persists. However, Bob can pause the contract signing, and use Alice's partial signature to bargain for better offers with others. He then carries out a new OFE protocol with the one offering the best price to sign the contract. Bob can play the same trick iteratively until that no one can give an even better offer.

For making OFE be applicable to more applications and practical scenarios, in this paper, we propose to enhance the security requirements of OFE and construct a new OFE scheme which does not have the problems mentioned above. One may also think of this as an effort to make OFE more admissible as a viable fair exchange tool for real applications. We will build an OFE scheme which not only satisfies all the existing security requirements of OFE (with respect to the strongest security model available [21]), but in addition to that, will also have σ_P be not self-authenticating and unable for Bob to demonstrate to others that Alice has committed herself to something. We call this enhanced notion of OFE as *Ambiguous Optimistic Fair Exchange* (AOFE). It inherits all the formalized properties of OFE [15,21] and has a new property introduced: *signer ambiguity*. It requires that a partial signature σ_P generated by Alice or Bob should look alike and be indistinguishable even to Alice and Bob.

1.1. Related works

There have been many OFE schemes proposed in the past [2,3,11,33,14,29,32,38,4,34,15,21]. In the following, we review some recent ones by starting from 2003 when Park, Chong and Siegel [33] proposed an OFE based on sequential two-party multi-signature. It was later broken and repaired by Dodis and Reyzin [14]. The scheme is *setup-driven* [39,40], which requires all users to register their keys with the arbitrator prior to conducting any transaction. In [32], Micali proposed another scheme based on a CCA2 secure public key encryption with the property of *recoverable randomness* (i.e., both plaintext and randomness used for generating the ciphertext can be retrieved during decryption). Later, Bao et al. [4] showed that the scheme is not fair, where a dishonest party, Bob, can obtain the full commitment of another party, Alice, without letting Alice get his obligation. They also proposed a fix to defend against the attack.

In PKC 2007, Dodis, Lee and Yum [15] considered OFE in a *multi-user* setting. Prior to their work, almost all previous results considered the single-user setting only which consists of a single signer and a single verifier (along with an arbitrator). The more practical multi-user setting considers a system to have multiple signers and verifiers (along with the arbitrator), so that a dishonest party can collude with other parties in an attempt of cheating. Dodis et al. [15] showed that security of OFE in the single-user setting does not necessarily imply the security in the multi-user setting. They also proposed a formal definition of OFE in the multi-user setting, and proposed a generic construction, which is *setup-free* (i.e. no key registration is required between users and the arbitrator) and can be built in the random oracle model [5] if there exist one-way functions, or in the standard model if there exist trapdoor one-way permutations.

In CT-RSA 2008, Huang, Yang, Wong and Susilo [21] considered OFE in the multi-user setting and *chosen-key* model, in which the adversary is allowed to choose public keys arbitrarily without showing its knowledge of the corresponding private keys. Prior to their work, the security of all previous OFE schemes (including the one in [15]) are proven in a