Theoretical Computer Science 562 (2015) 57–74

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Optimistic fair exchange in the enhanced chosen-key model

Yang Wang [a,c], Man Ho Au [b,c,*], Willy Susilo [c,1]

[a] Cyberspace Security College, PLA Information Engineering University, China
[b] Department of Computing, Hong Kong Polytechnic University, Hong Kong
[c] Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Australia

ARTICLE INFO

Article history:
Received 26 November 2013
Received in revised form 27 August 2014
Accepted 13 September 2014
Available online 21 September 2014
Communicated by G. Ausiello

Keywords:
Optimistic fair exchange
Chosen-key model
Enhanced model

ABSTRACT

Optimistic fair exchange (OFE) is a kind of protocol to guarantee fairness for the parties involved in an exchange with the help of an arbitrator. A fundamental work of optimistic fair exchange is to define security models capturing realistic attacks and design schemes secure in practical models. The security models are very essential to ensure that they capture practical situation, which will ensure that the protocols can be adopted in practice. The contributions of this paper are three fold. First, we observe that the existing OFE models do not capture realistic situation, where the adversary can actually observe the full signatures generated by the signer, prior to launching the actual attack. That is to say, the adversary is not provided with the signing oracle, which will produce full signatures generated by the signer. It is commonly believed that the full signatures generated by the signer can be simulated by the full signatures generated by the arbitrator. Unfortunately, we show that this perception is false. Second, we propose an enhanced model of OFE that explicitly provides the adversary with the signing oracle, which outputs the full signatures generated by the signer. We demonstrate the difference between our enhanced model and the existing chosen-key model through two concrete OFE schemes that serve as counterexamples. Finally, we revisit two existing generic constructions of optimistic fair exchange schemes, one based on verifiably encrypted signatures, and the other based on conventional signatures and ring signatures. Our result shows that the two generic approaches can still offer schemes secure in our enhanced model, which captures the real scenario that dishonest users may have access to the full signatures generated by the signer.

1. Introduction

Nowadays electronic commerce grows rapidly and assumes increasing importance. A significant issue for electronic commerce is how to exchange digital items in a fair way so that either each party receives the other's item or neither party does. Since digital items are normally not revocable, i.e. once the digital item has been sent then there is no means to revoke or cancel it, the exchange of digital items should happen simultaneously to achieve fairness for both involved parties. Unfortunately, real simultaneity in general cannot be realized, since the transmission of any data requires time. Moreover,

* Corresponding author at: Department of Computing, Hong Kong Polytechnic University, Hong Kong.
E-mail addresses: yw990@uowmail.uow.edu.au (Y. Wang), csallen@comp.polyu.edu.hk (M.H. Au), wsusilo@uow.edu.au (W. Susilo).

[1] This work is supported by ARC Future Fellowship FT0991397.

http://dx.doi.org/10.1016/j.tcs.2014.09.033
0304-3975/

the networks where the exchange takes place may be insecure and there is no assurance that the digital item will eventually be delivered to the intended recipient.

Optimistic fair exchange (OFE), first introduced by Asokan, Schunter and Waidner [1] in 1997, is a kind of protocol to solve the fair exchange problem with the help of a trusted third party named "an arbitrator". In such a protocol, the arbitrator is used in an effective manner in the sense that it only involves to solve the disputes between participants, while in the vast majority of transactions, the arbitrator does not need to be involved at all. Consider the scenario that Alice is willing to sign some statements, for instance, an electronic check, in exchange for Bob's fulfillment of some obligation (delivers some digital good, for example). By adopting an optimistic fair exchange protocol, this exchange can be summarized as a three-step process. Alice, usually called the signer, firstly sends a partial signature to Bob, usually called the verifier. The partial signature assures Bob that the arbitrator is able to convert it into a full one. Then Bob fulfills his obligation. Later, Alice should send her full signature to complete the exchange. In the case Alice refuses to do so, Bob can ask the arbitrator to make a resolution, who will convert Alice's partial signature into a full one and send it back to Bob.

In an OFE scheme, the full signatures generated by the signer and those generated by the arbitrator based on the signer's partial signature are both viewed as the signer's valid full signatures and represent the signer's commitment on some statements. However, they does not necessarily to be the same. Following the terms in [2], full signatures generated by the signer are called *actual signatures* and full signatures generated by the arbitrator are called *resolved signatures*.

1.1. Previous work and related notions

Optimistic fair exchange has a long history due to its fundamental role in electronic commerce. It is well-known that optimistic fair exchange schemes can be constructed from *verifiably encrypted signatures* [3–8] and *sequential two-party multisignatures* [9]. It has been widely accepted that optimistic fair exchange schemes should have the property called "resolution ambiguity" [9–11], namely the actual signatures generated by the signer should be at least computationally indistinguishable from the resolved signatures generated by the arbitrator. As the intervention of an arbitrator could be caused by a network failure rather than by the cheating of a signer, an optimistic fair exchange scheme with resolution ambiguity property can avoid bad publicity for the signer. In the following, we mainly review the attempts in defining security models capturing possible practical attacks for optimistic fair exchange schemes, as they are mostly relevant to this paper.

Early optimistic fair exchange protocols was studied in the single-user setting and the security model assumed only one signer and one verifier. The first formal security model was proposed in [1,3] but failed to consider the case where the arbitrator itself may be dishonest. A more generalized model in the single-user setting was suggested by Dodis and Reyzin [9] to take into account a dishonest arbitrator.

Since there are many users who may share the same arbitrator in the real world, the security model in the single-user setting does not capture the possible attacks by colluding dishonest users. In PKC 2007, Dodis, Lee and Yum [10] considered the multi-user security of optimistic fair exchange which allows dishonest users to collude to cheat another user. They separated the security of optimistic fair exchange between single-user setting and multi-user setting by showing that an optimistic fair exchange instance provably secure in the single-user setting is not secure in the multi-user setting. Independently, this was also studied by Zhu, Susilo and Mu in 2007 [12].

Since then, the security of optimistic fair exchange intuitively covers the following three aspects.

- Security against signers: the signer should not be able to generate a partial signature that cannot be converted into a full one by the honest arbitrator.
- Security against verifiers: the verifier should not be able to generate a full signature of the signer's by himself/herself.
- Security against the arbitrator: the arbitrator should not be able to generate a full signature on behalf of the signer without observing a corresponding partial one.

Most optimistic fair exchange protocols have been studied in the *certified-key* model (also known as the *registered-key* model [13]). In this model, it is assumed that the authenticity of public keys are verifiable and each user in the system should show its knowledge of the corresponding secret key in the public key registration stage to resist key substitution attacks. That is to say, in this model, the dishonest signer and the dishonest arbitrator have to show their knowledge of their corresponding secret keys, and the dishonest verifier can only make resolution queries with respect to the target signer and other public keys whose secret keys are known.

However, in the public key infrastructure, when a certification authority issues a certificate of a user's public key, the user is not required to show its knowledge of the secret key. Thus the certified-key model is not practical enough, as it relies on a stronger assumption than the normal authenticity assumption placed on the certification authority.

In CT-RSA 2008, Huang, Yang, Wong and Susilo [11] studied the security of optimistic fair exchange in the *chosen-key model*, in which the adversary can adversarially select public keys without knowing the corresponding secret key. This model provides more realistic power to the adversary in attacking the honest users. On the one hand, the adversary can choose its own public key without knowing the corresponding secret key. Specifically, in the security against the arbitrator, the dishonest arbitrator is even allowed to set its own public key after knowing the target signer's public key. In the certified-key model, however, the dishonest arbitrator has to set its key pair before seeing the target signer's public key. On the other hand, for a dishonest signer or verifier, the adversary is allowed to make resolution queries with respect to