Theoretical Computer Science 527 (2014) 83–96

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Attribute-based optimistic fair exchange: How to restrict brokers with policies

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

Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Australia

ARTICLE INFO

Article history:
Received 24 June 2013
Received in revised form 27 November 2013
Accepted 28 January 2014
Communicated by X. Deng

Keywords:
Optimistic fair exchange
Attribute-based encryption
Policy
Standard model

ABSTRACT

Optimistic fair exchange (OFE) is a kind of protocols for solving the fair exchange problem between two participants with the help of an arbitrator that only needs to be involved when dispute occurs. As far as we are concerned, all previous work on OFE does not take into account user's attributes such as nationality and age. We identify that in some applications, the attributes could play an important role in the exchange to take place, and OFE may not be suitable to these scenarios. We introduce a new notion named *attribute-based optimistic fair exchange* (ABOFE) to solve the fair exchange problem in the attribute-based setting. We formalise the notion of ABOFE and present a security model in the multi-user setting under the chosen-key attack. We also present a generic construction of ABOFE from existing cryptographic primitives and prove that our proposal is secure with respect to our definition in the standard model. An instantiation in the standard model is discussed.

1. Introduction

The brokerage business model has been used since the pre-Internet era, where the intermediary buys from the supplier (or producer) and owns the goods first, and then sells it. This model plays a very important role in the online business nowadays, as it enables fast and secure transactions without relying on a single merchant's connection. Brokers have been known to be active in business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) or peer-to-peer (P2P) markets. Although this model is known to be very useful and practical, some issues have happened since the broker may incorporate some certain strategies to increase his/her sales, and it may damage even the supplier.

Consider the following real life case study. A broker B buys games from the game developer G and sells these games to its customer. Since B is considered as a broker, the price that has been set to B is certainly lower than the retail price of the game itself. In order to maximise its sales, B is happy to make its margin to be very low, and this way B will gain popularity among the customers and attract more buyers. In particular, this is certainly possible if B purchases the games from different countries, since usually the price for each country will be different, due to the sales tax applied. This action is certainly damaging the market and G will not be able to sell that particular game with the retail price to the customers as they would have preferred to acquire it from B instead. This issue can be solved by placing required policies for the brokers. First of all, each broker must be licensed in order to sell the games. The license is limited to the country of residence. The

* Corresponding author.
E-mail addresses: yw990@uowmail.uow.edu.au (Y. Wang), aau@uow.edu.au (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.2014.01.029
0304-3975/

game will be playable, if and only if, the required CD key sold by the broker matches with the country where the game will be played. To give an example, someone resides in the US will purchase a CD key from the broker. First of all, he/she needs to be sure that the broker is a licensed retailer for US. Once the CD key is issued by the broker, this CD key is only usable if it is used in the US and not in other countries. Another scenario involves limitation of the age restriction towards the game itself. For instance, consider the game "God of War" that is restricted to people over 18 years old. A US online reseller sells the activation key (or CD key) for this game. This price is lower than the price of the same game available in Canada. There are two issues need to be solved here. First, the buyer needs to be ensured that the reseller is a genuine reseller, and the reseller needs to be sure that the buyer is at least 18 years old. Subsequently, the activation key sold can only be used in the US and not elsewhere. Hence, the buyer from Canada will not be able to make use of this particular activation key.

Our Approach In this paper, we intend to present a cryptographic primitive that aims to solve the above scenario. We make use of the notion of optimistic fair exchange (OFE) and enhance this notion to enable policies for both parties, namely the seller and the buyer (or the signer and the verifier, resp.). A trivial solution for enabling the above scenario would be that prior to involving an OFE protocol, each participant will simply present an evidence, for instance a copy of the identity card or license, to the other participant, hence confirming that they satisfy the requirements. Nevertheless, this solution compromises the privacy of the users, and therefore it is not ideal. Furthermore, providing such kind of evidence over the network securely is rather challenging as well.

1.1. Optimistic fair exchange

Optimistic fair exchange (OFE), first introduced by Asokan, Schunter and Waidner [1], is a kind of protocols aiming to guarantee fairness for two parties Alice and Bob exchanging digital items. A trusted third party named "arbitrator" is needed in OFE, but involves only when there is a dispute between exchanging parties. Since a large number of digital items such as electronic checks and electronic airline tickets are implemented as digital signatures, the optimistic fair exchange of digital signatures constitutes an important part of any business transaction.

In a typical execution of optimistic fair exchange of digital signatures, Alice first sends a partial signature to Bob. Bob verifies the validity of Alice's partial signature, and sends its full signature to Alice, after which Alice sends her full signature back to Bob and completes the exchange. In the case there is a network failure or Alice attempts to cheat by refusing to send her own full signature, the arbitrator will convert Alice's partial signature into a full one and send it back to Bob. It is implicitly assumed that Bob should offer his own full signature when asking the arbitrator for help, and the arbitrator will send Bob's full signature to Alice later. Thus at the end of this exchange, either both Alice and Bob gain the other's full signature, or neither does. Thus the exchange is fair.

As a useful tool in applications such as contract signing and electronic commerce, OFE has been extensively researched [2–8] since its introduction. Several primitives are useful for the construction of OFE, including verifiably encrypted signatures [9–15], and sequentially two-party multisignatures [16]. It was further showed that OFE can be constructed from OR signature [17], and from conventional signatures and ring signatures [18].

In an orthogonal dimension, formal OFE security models [17,18] are proposed. While most optimistic fair exchange protocols are studied in the *certified-key* model (also known as the *registered-key* model [19]) in which the adversary is only allowed to make queries with respect to the registered public keys, the security of optimistic fair exchange in the multi-user setting and *chosen-key model* [18], where the adversary can choose its public key arbitrarily probably without knowing the corresponding private keys, is more desirable.

1.2. Our contribution

In this paper, motivated by idea of attribute-based encryption (ABE) [20] and ciphertext policy attribute-based encryption (CPABE) [21], we introduce the notion of *attribute-based optimistic fair exchange* (ABOFE), which can be viewed as an extension of OFE, as a practical cryptographic solution to the aforementioned scenario.

In ABOFE, each user satisfying a set of attributes is assigned a credential by the credential centre. This allows the signer Alice to generate a credential-protected package in such a way that only verifiers that possess appropriate credentials can convert it into a full signature, which naturally guarantees that the verifier should satisfy some particular set of attributes.

We propose the syntax and also define a security model for ABOFE in the multi-user setting under chosen-key attack. Our model captures the existing security requirements for OFE, namely, security against signers, security against verifiers and security against the arbitrator. As suggested by the respective names, they intend to cover the scenarios when the named party is dishonest.

Finally, we propose a generic construction of ABOFE from the two well established cryptographic primitives, OFE and CP-ABE, and provide the security proof of our proposal in the proposed model. Our generic construction works in the standard model and does not involve any extra assumptions. The efficiency of an instantiation about the generation construction is also discussed.