Computers and Electrical Engineering 36 (2010) 1035–1045

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Fair exchange protocol of Schnorr signatures with semi-trusted adjudicator ☆

Zuhua Shao *

Zhejiang University of Science and Technology, No. 318, LiuHe Road, Hangzhou, Zhejiang 310023, PR China

ARTICLE INFO

Article history:
Received 29 October 2008
Received in revised form 12 March 2010
Accepted 25 March 2010
Available online 22 April 2010

Keywords:
Fair exchange protocol
Schnorr signatures
Discrete logarithm
Random oracle model

ABSTRACT

In this paper, we propose an optimistic fair exchange protocol of Schnorr signatures with a semi-trusted adjudicator. In this protocol, we enforce the adjudicator accountability in the protocol to relax excessive reliance on the trust of the adjudicator, so that the adjudicator only needs to be trusted by the signer. We present a security model and then show that the protocol is strong EUF–CMA secure under the standard Discrete Logarithm (DL) assumption in the random oracle model. Finally, we compare the performance of the fair exchange protocol of Schnorr signatures.

1. Introduction

With the phenomenal growth of the Internet, more and more business are conducted via the Internet. Because of the unsafe factors, whenever a message is sent over the Internet, there is no assurance that it would be delivered to the intended recipient. Even if the message has been delivered, the recipient might claim otherwise. The problem of fair exchanging has become one of the most fundamental problems in electronic transactions and digital rights management, in which fairness is a relevant security property. For example, a signer is willing to sign some document, such as a commerce contract, e-cash, or a certified mail receipt, but if and only if a verifier fulfills some obligation, such as delivering some goods, or disclosing some information. On the other hand, the verifier is not willing to fulfill his obligation unless he is sure to get the signature from the signer. This circularity needs a mechanism to allow two mutually distrustful parties to exchange digital items over open computer networks in a fair way, so that no party involved in the protocol can take a significant advantage over the other, even if the protocol is halted for some reason.

Fair exchange protocols for digital items have been extensively studied in cryptography. There were essentially two different approaches to solving this problem in previous literatures.

Early approach to solving the fair exchange problem is based on computational fairness [1,2]. It is assumed that both parties involved have equal computational power. They take turns to exchange their commitments/secrets "little-by-little". If one party stops prematurely, both parties have about the same fraction of the peer's secrecy, which means that they can complete the construction off-linely by investing about the same amount of computing. Though this approach does not require the intervention of any third party, its assumption is unrealistic in most real applications, and proposed exchange protocols are highly interactive with much message flows.

☆ Reviews processed and proposed for publication to the Editor-in-Chief by Associate Editor Dr. Malek.

* Tel.: +86 571 85171332; fax: +86 571 85121214.
E-mail address: zhshao_98@yahoo.com

0045-7906/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2010.03.005

In 2004, Chen et al. [3] introduced a somewhat weaker concept, called concurrent signatures. Without the help of any third party, two parties could interact and produce two signatures, respectively. However, both signatures are ambiguous with respect to the identity of the signers until an extra piece of information (the keystone) is released by one party. At that time, both signatures become binding to their true signers concurrently. Chen et al. explained many applications in which concurrent signatures suffice.

As Even and Yacobi [4] proved, full fairness is impossible in a deterministic two-party contract signing protocol. The concurrence signature protocol cannot be an exception. In fact, the party who controls the keystone has a degree of advantage over the other. The former controls the timing of the keystone releasing and whether the keystone is released. The former even might privately show the other's signature together with the unreleased keystone to outsiders.

An alternative approach resorts to a neutral Trusted Third Party TTP as an adjudicator, who can be called upon to handle disputes between the involved parties. According to its involvement degree in the protocol, there are mainly three types of TTP: in-line, on-line and off-line [5]. Among them, fair exchange protocols with an off-line trusted third party are preferable as they offer a more cost-effective use of a trusted third party. The TTP is invoked only in the case of a network failure or either party's misbehaves. In the great majority of cases, the protocol can run without any intervention of the TTP since the two participants are honest and the network is well functioning. Hence, such protocols are called optimistic.

Asokan et al. [6] were the first to formally study the problem of optimistic fair exchanges. They presented several provably secure protocols based on the concept of verifiably encrypted signatures, i.e., a way of encrypting a signature under a designated public key and subsequently proving that the resulting ciphertext indeed contains such a signature. Since then, several optimistic fair exchange protocols based on verifiably encrypted signatures have been proposed to achieve more efficiency [7–12]. Most of them are proved secure with or without random oracles. However, all these schemes involve expensive and highly interactive zero-knowledge proofs in the exchange phase.

The first non-interactive verifiably encrypted signature scheme was constructed by Boneh et al. [13]. Though this scheme requires special elliptic curve groups with a bilinear map and relies on a form of the computational Diffie–Hellman assumption for such groups, it is provably secure in the random oracle model [14] and is the most efficient fair exchange protocol at that time. Later, Zhang et al. [15] proposed a new verifiably encrypted signature scheme from bilinear pairings and further showed that it is more efficient than the previous protocols of this kind. However, the security proofs of both of verifiably encrypted signature schemes use a weaker security model, in which the key pair of the adjudicator was chosen by the simulator instead of the signature forger. In the real world, the adjudicator is a potential adversary as Dodis and Reyzin stated [16]. Shao [17] showed that a malicious adjudicator is able to forge verifiably encrypted signatures of Boneh et al. in a rogue-key attack, which would be accepted in many environments. Later, Lu et al. [18] proposed a verifiably encrypted signature scheme, derived from a novel application of the Waters's signature scheme [19]. They showed that their scheme was secure without random oracles in the same security model as that of Boneh et al.'s scheme. Some recent papers without random oracles published in the literature continued to rely on the same security model [20–22].

A different paradigm for building optimistic fair exchange protocols of signatures for was proposed by Park et al. [23]. They introduced a connection between fair exchange protocols and sequential two-party multisignature schemes and provided a novel method of constructing fair exchange protocols by distributing the computation of RSA. Their approach avoids the design of verifiably encrypted signature schemes at the cost of having cosigner store a piece of prime signer's secret key. However, Dodis and Reyzin [16] broke Park et al.'s scheme by pointing out that an honest-but-curious adjudicator can easily derive the private key of the signer after the end of registration phase. Moreover, they proposed a new primitive, called verifiably committed signatures, for constructing fair exchange protocols, and presented a committed signature scheme based on GDH signatures [24]. Later, some fair exchange protocols based on RSA signatures were proposed independently by following Park et al.'s approach [25–27]. However, in some protocols, the exchanged signature is two-signature rather than the ordinary signature in verifiably encrypted signature schemes, which would reduce the efficiency of the fair exchange protocols based on them. Other protocol uses an interactive zero-knowledge proof to verify partial signatures.

However, the fairness of signature exchange protocols with TTP, no matter whether based on verifiably encrypted signatures or on verifiably committed signatures, relies on the neutrality of the trusted third party. If he colludes with one party, the other would be duped. For example, in a fair exchange protocol based on verifiably encrypted signatures, the signer computes a signature, and then encrypts it under the public key of a designated third party. Although the encrypted signature is undeniable, encrypting means that the signer would not release the signature unless the verifier fulfills his obligation. On the other hand, *the third party does not commit any thing at all*, though he is able to decrypt the encrypted signature. He could either refuse to extract the signature even though the verifier fulfills his obligation or extract the signature presumptuously without seeing the fulfilling obligation.

Therefore, both the signer and the verifier must negotiate to choose a common trusted third party as an adjudicator before exchanging, the function of which is beyond those required of a normal Certification Authority. This excessive reliance on the trust of the TTP has become a major practical hindrance to fair exchange protocols getting widely deployed, since it is difficult for mutually distrustful parties to seek unity of thinking on the honesty of a third party over the open Internet, particularly for those parties in different countries with unbalanced information.

To cope with the subtle problem for the trust in the TTP in fair exchange protocols, recently, Shao introduced a new paradigm for building fair exchange protocols of signatures [17,28]. The idea is to enforce the trusted third party TTP account-