Optimistic Fair Exchange of Digital Signatures*

N. Asokan† Victor Shoup‡ Michael Waidner‡

October 1, 1999

Abstract

We present a new protocol that allows two players to exchange digital signatures over the Internet in a fair way, so that either each player gets the other's signature, or neither player does. The obvious application is where the signatures represent items of value, for example, an electronic check or airline ticket. The protocol can also be adapted to exchange encrypted data. It relies on a trusted third party, but is "optimistic," in that the third party is only needed in cases where one player crashes or attempts to cheat. A key feature of our protocol is that a player can always force a timely and fair termination, without the cooperation of the other player, even in a completely asynchronous network. A specialization of our protocol can be used for contract signing; this specialization is not only more efficient, but also has the important property that the third party can be held *accountable* for its actions: if it ever cheats, this can be detected and proven.

*This is an extensively revised and expanded version of an extended abstract in *Eurocrypt '99*, and of IBM Research Report RZ 2973 (Dec. 17, 1997).

†Nokia Research Center, Kelsinki; work done while at IBM Research, Zürich Research Laboratory

‡IBM Research, Zürich Research Laboratory, CH-8803 Rüschlikon; e-mail: {sho,wmi}@zurich.ibm.com

1 Introduction

As more business is conducted over the Internet, the *fair exchange problem* assumes increasing importance. For example, suppose player A is willing to give an electronic check to player B in exchange for an electronic airline ticket. The problem is this: how can A and B exchange these items so that either each player gets the other's item, or neither player does.

Both electronic checks and electronic airline tickets are implemented as digital signatures. Presumably, many other items to be exchanged over the Internet will be so implemented. Therefore, it seems fruitful to focus our attention on the fair exchange of digital signatures.

Of course, one could use an on-line trusted third party in every transaction to act as a mediator: each player sends his item to the third party, who upon verifying the correctness of both items, forwards the item to the other player. This is a rather straightforward solution; variations are discussed in the papers [CTS95, DGLW96, FR97].

In this paper, we present a new protocol for fair exchange that takes a different approach. Our protocol uses a trusted third party, but only in a very limited fashion: the third party is only needed in cases where one player attempts to cheat or simply crashes; therefore, in the vast majority of transactions, the third party will not need to be involved at all. Following [ASW97], we call our protocol *optimistic*; in addition to [ASW97], optimistic protocols for several variants of the fair exchange problem are discussed in [BDM98, BP90, Mic97].

Compared to a protocol using an on-line third party, the optimistic approach greatly reduces the load on the third party, which in turn reduces the cost and insecurity involved in replicating the service in order to maintain availability. It also makes it more feasible to implement the trusted third party service as a distributed, fault-tolerant system, eliminating the single point of failure.

Our new protocol can be used to exchange commonly used digital signatures, including RSA [RSA78], DSS [Kra93], Schnorr [Sch91], Fiat-Shamir [FS87], GQ [GQ90], and Ong-Schnorr [OS91] signatures, as well as the payment transcripts used in Brands' [Bra93] off-line, anonymous cash scheme. Moreover, the protocol can also be adapted to exchange digital content, such as music or stock quotes, and to the related problem of certified e-mail.

Our protocol also enjoys the following properties:

(1) It works in an asynchronous communication model: there is no need for synchronized clocks, and one player cannot force the other to wait for any length of time—a fair and timely termination can always be forced by contacting the third party.

(2) To use it, one need not modify the signature scheme or message format *at all*. Thus, it will inter-operate with existing or proposed schemes for electronic checks, coins, tickets, receipts, etc., without *any* modification to these schemes.

(3) The protocol does not require the players to "pre-register," or otherwise interact in advance with the trusted third party.

(4) It is practical. A typical exchange requires only a few rounds of interaction, transmission of a few KBytes of data, and a couple thousand modular multiplications.

(5) The protocol can be proved secure (modulo standard intractability assumptions) in the random hash function model [BR93], where a hash function is treated *as if* it were a "black box" that contains a random function.

(6) The two players need not sacrifice their privacy in making use of the trusted third party.

We wish to emphasize the importance of property (1). Previous optimistic protocols for fair exchange could easily leave one player "hanging" for a long time, without knowing if the exchange was going to complete, and without being able to do anything about it. Not only can this be a great inconvenience, it can also lead to a real loss in the case of time-sensitive data like stock quotes. In our protocol, this cannot happen so long as the third party is available. Clearly identifying this problem and providing an effective solution is probably the most important contribution of this paper.

We stress the practical importance of property (2): it allows a general-purpose fair exchange service to be deployed without the cooperation of the institutions responsible for the items being exchanged (banks, airlines, etc.). Indeed, it seems quite unrealistic to expect these institutions to redesign their schemes and all of the relevant software to accommodate a fair exchange protocol if this has not already been designed for. Our protocol can accommodate any common signature scheme without modification. Previous optimistic protocols for fair exchange do not allow for this: these protocols either require that the item being exchanged have a special structure to facilitate the exchange protocol, or they partially sacrifice fairness, with one player ending up with just an affidavit from the third party that the other player owes him something. In our protocol, the two players get the real thing—not a substitute or affidavit.

We also point out that in practice, the most common threat to a fair exchange is not malicious behavior by a player, but simply the possibility that one player crashes in the middle of the exchange. Our protocol deals equally well with both types of threats.

In addition to the above general protocol for fair exchange of digital signatures, we give a specialized version of this protocol for contract signing. Here, we allow ourselves the additional flexibility of defining the form of a