Chapter 17
A Resilient Fair Electronic Contract Signing Protocol

Harkeerat Bedi
University of Memphis, USA

Li Yang
University of Tennessee at Chattanooga, USA

ABSTRACT

Fair exchange between parties can be defined as an instance of exchange such that either all parties involved in the exchange obtain what they expected or neither one does. The authors examine a protocol by Micali that provides fair contract signing, where two parties exchange their commitments over a pre-negotiated contract in a fair manner. They show that Micali’s protocol is not entirely fair and demonstrate the possibilities for one party cheating the other by obtaining the other party’s commitment and not offering theirs. A revised version of this protocol by Bao which provides superior fairness by handling some of the weaknesses is also discussed. However, both these protocols fail to handle the possibilities of a replay attack. Their prior work improves upon these protocols by addressing the weakness that leads to a replay attack. This journal extends their prior work on fair electronic exchange by handling a type of attack which was not handled earlier and provides a brief survey of the recent work related to the field of fair electronic exchange. They also discuss the application of cryptography to our protocol which includes implementation of hybrid cryptography and digital signature algorithms based on elliptic curves to achieve features like confidentiality, data-integrity and non-repudiation.

INTRODUCTION

Commerce has come a long way since the beginning of our civilization. The ability to exchange goods and services for items of equivalent value has been widely exercised. Based on the kind of items exchanged between two parties, it can either be classified as a barter system where goods and services are exchanged for other goods and services, or the act of selling and buying where goods and services are sold or bought between parties in exchange for money.

The notion of fair exchange can be expressed as the ability to exchange goods or services for
other goods or services in a fair manner where both the parties obtain what they expected. Being a fundamental concept, this can be implemented in various scenarios that may include exchanges based on barter system or buying and selling of goods.

With the advent of computers and the Internet, new means of performing commerce have been invented. E-commerce is one such solution where good and services are bought and sold between interested parties using computers over a network. With the rapid growth of the Internet, the magnitude of commerce performed online has also increased significantly. This increase is primarily because commerce conducted online is convenient and fast when compared to the traditional methods of trade. Even though commerce of this type offers benefits like speed and convenience, without properties like fairness and security, such services become less useful as they significantly increase the risk of failure. E-commerce cannot flourish or even sustain if it is not able to provide fairness and security. Therefore the concept of fair exchange plays a vital role in shaping such forms of commerce. When carried out online using computers and the Internet, such fair exchange is known as fair electronic exchange.

FAIR ELECTRONIC EXCHANGE

Fair electronic exchange can be demonstrated as e-commerce that takes place between two parties who are online and where exchange of goods and services is performed such that both either parties obtain what they expected or they obtain nothing at all. After an exchange is performed or aborted prematurely, none of the parties should have an unfair advantage over the other. If cheating takes place, where one party refuses to present their part of the exchange, other means for providing fairness should be available. These may include use of additional entities like a human judge or electronic ones that can comprehend the situation and act accordingly to provide fairness. Protocols that provide such facilities are termed as fair exchange protocols. Such protocols can be used for the following purposes:

a. Certified E-Mail (CEM), where a user named Alice sends a message to a user named Bob and gets a receipt from him in return. Providing the quality of fairness would include Alice getting the receipt only when Bob gets the message or Bob getting the message only when Alice gets the receipt. Associated protocols include (Zhou & Gollmann, 1996; Kremer & Markowitch, 2001; Ateniese & Nita-Rotaru, 2002; Imamoto & Sakurai, 2002)

b. Electronic Contract Signing (ECS), where both Alice and Bob wish to sign a contract that has already been negotiated. This would involve Alice sending her commitment (digital signature) on the contract to Bob and him sending his commitment (digital signature) on the same in return. Providing fairness would involve Alice receiving Bob’s commitment only when her commitment is received by Bob and vice versa. This example demonstrates contract signing between two parties. Protocols that provide such functionality include (Ben-Or, Goldreich, Micali, & Rivest, 1990; Damgard, 1995; Bao, Deng, & Mao, 1998; Asokan, Shoup, & Waidner, 1998; Ateniese, 1999; Garay, Jakobsson, & MacKenzie, 1999; Micali, 2003; Bao, Wang, Zhou & Zhu, 2004). However, various multi-party contract signing protocols also exist and have also been proposed in (Baum-Waidner, 2001; Ferrer-Gomila, Payeras-Capella, Huguet-Rotger, 2001; Garay & MacKenzie, 1999;

c. Online payment systems (OPS), where Alice is the seller and Bob is the buyer and payment is given in return of the item of value (Cox, Tygar & Sirbu, 1995). Similar e-payment schemes in electronic commerce include