Fair Electronic Exchange Based on Fingerprint Biometrics

Harkeerat Bedi, University of Tennessee at Chattanooga, USA
Li Yang, University of Tennessee at Chattanooga, USA

ABSTRACT

Fair exchange between two parties can be defined as an instance of exchange such that either both parties obtain what they expected or neither one does. Protocols that facilitate such transactions are known as “fair exchange protocols”. We analyze one such protocol by Micali that demonstrates fair contract signing, where two parties exchange their commitments over an already negotiated contract. In this journal we show that Micali’s protocol is not completely fair and demonstrate the possibilities for one party cheating by obtaining the other party’s commitment and not offer theirs. A revised version of this protocol by Bao provides superior fairness by handling the above mentioned weakness but fails to handle the possibility of a replay attack. Our proposed protocol improves upon Bao’s protocol by addressing the weakness that leads to a replay attack. We also demonstrate a software implementation of our system which provides fair contract signing along with properties like user authentication achieved through the use of a fingerprint based authentication system and features like confidentiality, data-integrity and non-repudiation through implementation of hybrid cryptography and digital signatures algorithms based on Elliptic Curve Cryptography.

Keywords: Biometrics, Contract Signing, ECDSA, ECIES, Elliptic Curve Cryptography, Fair Exchange, Minutiae Based Fingerprint Authentication System, Optimistic Protocols

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 which 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 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 traditional methods of trade. Even though commerce of this type offers qualities like speed and convenience, properties like fairness and security are equally essential. 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 this form 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 where exchange of goods and services is performed such that both 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 its part of the exchange, means for providing fairness should be available. This 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 Alice sends a message to 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.

b. **Electronic contract signing (ECS):** Where both Alice and Bob wish to sign a contract that has been already 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. However, various multi-party contract signing protocols 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).

In the ideal case, where both Alice and Bob are guaranteed to be honest and the communication channel is secure and provides resilience, fair exchange can be achieved trivially without the aid of any external fairness provider. The above described scenarios can thus be carried out as follows:

**Fair Certified E-Mail:**

- **Step 1:** Alice sends her message to Bob.
- **Step 2:** Bob sends his receipt for the message to Alice. Receipt may be the digital signature of Bob on the message which will also provides non repudiation.

**Fair Electric Contract Signing:**

It is assumed that both parties have negotiated the contract before hand.

- **Step 1:** Alice sends her digital signature on the contract to Bob.
- **Step 2:** Bob sends his digital signature on the contract to Alice.

**Fair Online Payment System:**

- **Step 1:** Alice sells goods or services online by sending it to Bob.
Related Content

Assurance for Temporal Compatibility Using Contracts
[www.irma-international.org/chapter/assurance-temporal-compatibility-using-contracts/20665/](www.irma-international.org/chapter/assurance-temporal-compatibility-using-contracts/20665/)

Software Security Engineering: Toward Unifying Software Engineering and Security Engineering
[www.irma-international.org/chapter/software-security-engineering/23135/](www.irma-international.org/chapter/software-security-engineering/23135/)

Cybercafé Management Software
[www.irma-international.org/chapter/cybercafe-management-software/28533/](www.irma-international.org/chapter/cybercafe-management-software/28533/)

Computational Complexity Analysis for a Class of Symmetric Cryptosystems Using Simple Arithmetic Operations and Memory Access Time
[www.irma-international.org/article/computational-complexity-analysis-class-symmetric/78530/](www.irma-international.org/article/computational-complexity-analysis-class-symmetric/78530/)

On the Security of Self-Certified Public Keys
[www.irma-international.org/article/security-self-certified-public-keys/55379/](www.irma-international.org/article/security-self-certified-public-keys/55379/)