A Secure, Anonymous and Scalable Digital Cash System

Feng Xue

School of Computer Science
McGill University, Montreal
August 1999

A thesis submitted to the
Faculty of Graduate Studies and Research
In partial fulfillment of the requirements for the degree of
Master of Science

Table of Contents

List of Figures and Tables

Résumé

Les signatures *à l'aveugle* réalisent l'anonymat dans les systèmes de paiements électroniques. Cependant, une fois déployées dans les systèmes d'argent numérique tels que « *eCash »*, les signatures *à l'aveugle* engendrent des inconvénients tels que la mauvaise résistance aux changements d'échelle et l'anonymat non garanti. Dans ce mémoire, nous proposons de combiner les signatures numériques à un autre mécanisme appelé « *Money-exchange* » existant dans « *NetCash »* pour élaborer un nouveau système de paiement électronique. Dans le nouveau système, deux formes d'argent numérique sont introduites : les billets numériques et la monnaie numérique. Nous avons étendu le mécanisme « *Money-exchange* » pour permettre l'échange d'argent d'une forme à une autre. Du côté de l'émetteur d'argent numérique, au moins deux bases de données sont maintenues pour détecter le double paiement. Ce nouveau système d'argent numérique est très sécuritaire du fait qu'il utilise deux algorithmes de cryptage symétrique et asymétrique. La combinaison des signatures *à l'aveugle* avec notre extension du mécanisme « *Money-exchange* » offre un anonymat complet et inconditionnel. Cette combinaison permet aussi une meilleure résistance aux changements d'échelle du système par rapport au nombre de clients à servir.

Abstract

Blind signatures make anonymity a reality in digital cash systems. However, when deployed in digital cash systems such as *eCash*, blind signatures raise such drawbacks as bad scalability and unfair anonymity. In this thesis, efforts have been done to combine digital signatures and a mechanism called "money-exchange" found in *NetCash* to build a new digital cash system. In the new system, two forms of digital cash are introduced: digital notes and digital coins. "Money-exchange" is extended to permit cash exchange from one form to the other. At the side of the digital cash issuer, at least two databases are maintained to detect double-spending. The new digital cash system is secure due to its deployment of both symmetric and asymmetric encryption algorithms. The combination of blind signatures and the extended money-exchange mechanism offers unconditional and fair anonymity, and it makes the system more scalable with the regards to the number of clients served.

Acknowledgements

First of all, I wish to give my thanks to my thesis supervisors Professor Petre Dini and Professor Claude Crépeau for their guidance, advice, and encouragement throughout the research. This thesis benefits from their careful reading and constructive criticism.

I truly thank CRIM for supplying me a wonderful researching environment and the generous financial supports.

I also wish to thank the School of Computer Science for the graduate courses and the research environment. Thanks to our graduate secretary Franca Cianci for her wonderful works.

Finally, I am especially grateful for the supports and encouragements from my wife Tiao during the graduate studies and research.

Introduction

A secure, anonymous and scalable digital payment system is critical to persuade people into e-commerce activities. Since 1980s, many digital payment systems, mechanisms and protocols have been proposed, and among them, some are being evaluated or even have been commercially deployed. There are many forms of electronic payment systems just as there are many forms of traditional payment instruments. Generally, they fall into three categories: secure credit card system, credit-debit system, and digital cash system. Each one has its advantages as well as disadvantages. For example, the secure credit card system is the easiest one to implement, and it is the most similar to the current conventional bank payment systems. However, clients' privacy such as purchase habits is exposed to the financial institutions. Therefore, it does not offer anonymity. Currently, it is widely accepted that digital cash systems stand for the future of digital payment systems, because they offer anonymity to individuals.

The fundament of digital cash systems for offering anonymity is blind signature. Blind signature extends RSA digital signature algorithm in such a way that a message is concealed from the signer when it is being signed. When blind signatures are deployed in digital cash systems, they give a client a way to hide the identities of digital cash when they are withdrawn from a bank. Thus, the spending pattern of the client with the bank-blindly-signed digital cash is undetectable to others. *eCash* is such a digital cash system which makes full use of blind signature mechanism. However, it has been pointed out that blind signatures also produce some shortcomings. First, the scalability of the system is quite unsatisfactory due to the deployed mechanism of detecting double spent digital cash, and the bad performance of the mechanism is due to the deployment of blind signatures. Second, anonymity offered is not fair. Only payers are unconditionally anonymous, while payees are not.

There is another presented digital cash system, *NetCash*, which offer anonymity through a mechanism called money exchange. Although the provided anonymity is not unconditional, it is fair to both payers and payees and the performance of its double-spending detection mechanism is better than that of *eCash*. It is imaginable that combining blind signature and cash exchange could be a practical solution for building a better digital cash system.

The main purpose of this thesis is to present the attempts of building this new system. The contents of the paper are divided into five chapters. Chapter 1 introduces the current states of e-commerce and discusses cryptographic techniques. Chapter 2 addresses variant digital payment systems. Chapter 3 delves into two digital cash systems *eCash* and *NetCash*, with emphasis on blind signatures and money exchange mechanisms, respectively. In Chapter 4, the attempts of combining *eCash* and *NetCash* are presented in details. In Chapter 5, a partial implementation of the presented system is included. Finally, conclusions of the thesis and future works are given.