

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

© Feng Xue, 1999

Table of Contents

Résumé	vi
Abstract	vii
Acknowledgements	viii
Introduction	ix
Chapter 1. E-commerce and cryptographic techniques	1
1.1 E-commerce and digital payment systems	1
1.2 Cryptography	2
1.2.1 Security attacks	2
1.2.2 Security services	3
1.2.3 Cryptographic techniques	4
1.2.3.1 Encryption and decryption	4
1.2.3.2 Digital signatures	10
1.2.3.3 Certificates and certification authorities	14
1.2.3.4 RSA	15
Chapter 2. Digital payment systems	17
2.1 Secure credit card systems	17
2.1.1 iKP	17
2.1.2 Other systems in this category	19
2.2 Credit-debit systems	20
2.3 Digital cash systems	21
2.3.1 Properties of digital cash systems	22
2.3.2 Double-spending	26
2.3.3 Digital cash proposals	27
Chapter 3. eCash and NetCash	29
3.1 eCash	29
3.1.1 Blind signature	30
3.1.2 Cryptography basis for blind signature	30
3.1.3 Withdrawal of eCash coins	31
3.1.4 Payments with eCash coins	33
3.1.5 Deposit of eCash coins	34
3.1.6 Discussion	34
3.2 NetCash	35
3.2.1 Withdrawal of NetCash Coins	35

36	3.2.2 Money-exchange
36	3.2.3 Payments with NetCash Coins
37	3.2.4 Deposit of NetCash Coins
37	3.2.5 Discussion
40	3.3 Conclusion
41	Chapter 4. Combination of eCash and NetCash
41	4.1 Combine eCash and NetCash
41	4.1.1 Digital coin and digital note
42	4.1.2 Entities and protocols
43	4.1.3 Server side mechanisms for double spending detection
44	4.1.4 Digital cash withdrawal
46	4.1.5 Digital cash exchange
46	4.1.5.1 Exchange note for coins
48	4.1.5.2 Exchange coins for coins
48	4.1.6 Digital cash payment
50	4.1.7 Digital cash deposit
51	4.1.8 Discussion
51	4.1.8.1 Multi-party security
52	4.1.8.2 Unconditional Anonymity
53	4.1.8.3 Enhanced scalability
54	4.2 Extending the system
55	4.2.1 Enhance scalability
58	4.2.2 Extend cash exchange mechanism
59	4.2.2.1 Offer payees unconditional anonymity
60	4.2.2.2 Offer “Divisibility” for digital cash
62	Chapter 5. Implementation
62	5.1 Introduction
62	5.2 System requirements and architecture
64	5.3 Implementation tool
64	5.4 What have been done
66	5.5 Implement blind signature
68	5.5.1 Generate public/private key pairs
69	5.5.2 Blind the serial number
70	5.5.3 Sign a blinded serial number
70	5.5.4 Unblind and verify the bank’s signature
71	5.6 Implement the server-client communication
73	5.7 Implement database access
76	5.8 Implement graphic user interface (GUI)
78	Conclusion and future works
79	Reference
82	Appendix: Source codes of the implementation

List of Figures and Tables

5	Figure 1 – Encryption and decryption
7	Figure 2 – Encryption and decryption with symmetric algorithms
9	Figure 3 – Encryption and decryption with asymmetric algorithms
14	Figure 4 – Digital signatures with public-key algorithms
22	Figure 5 – Entities and protocols in typical digital cash payment systems
43	Figure 6 – Entities and protocols in the new digital cash system
44	Figure 7 – Server-side databases for detecting double-spending
56	Figure 8 – One new database is added for enhancing the system scalability
59	Figure 9 – Exchange a note for a new note
60	Figure 10 – Exchange coins for a note
63	Figure 11 – System architecture
65	Figure 12 – Class diagram in package ca.crim.dcash (UML)
67	Figure 13 – Classes in package ca.crim.dcash with details (UML)
76	Figure 14 – GUI: Configuration
77	Figure 15 – GUI: Denominations
77	Figure 16 – GUI: Withdraw
40	Table 1 – Comparing <i>eCash</i> and <i>NetCash</i>
74	Table 2 – Table <i>Denomination</i> in the database <i>Bank</i>
76	Table 3 – Table <i>Notes</i> in the database <i>Client</i>

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 Ciani 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 fundamental 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.