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

RÈsumÈ äääääääääääääääääääääääääääääää. vi

Abstract ääääääääääääääääääääääääääääää... vii

Acknowledgements ääääääääääääääääääääääääää. viii

Introduction ääääääääääääääääääääääääääääää ix

Chapter 1. E-commerce and cryptographic techniques äääääääää. 1
1.1 E-commerce and digital payment systems ...ääääääääää.. 1
1.2 Cryptography äääääää.ääääääääääääääääää. 2
1.2.1 Security attacks ...ääääääää.äääääääääää 2
1.2.2 Security services ..ääääääääääääääääää 3
1.2.3 Cryptographic techniques äääääääääääääää 4
1.2.3.1 Encryption and decryption ääääääääää... 4
1.2.3.2 Digital signatures äääää..äääääääää 10
1.2.3.3 Certificates and certification authorities ...ääää 14
1.2.3.4 RSA äääääääääääääääääää.. 15

Chapter 2. Digital payment systems ääääää.ääääääääääää 17
2.1 Secure credit card systems ääääääääääääääääää.. 17
2.1.1 iKP ä...ääääääääääääääääääääää 17
2.1.2 Other systems in this category ...äääääääääää.. 19
2.2 Credit-debit systems ääääääääää.ääääääääää.. 20
2.3 Digital cash systems ääääääääää.äääääääääää.. 21
2.3.1 Properties of digital cash systems äääääääääää 22
2.3.2 Double-spending ääääääääääääääääää.. 26
2.3.3 Digital cash proposals ääääääääääää...äää... 27

Chapter 3. eCash and NetCash ..äääääääääääääääääää... 29
3.1 eCash ääääääääääääääääääääääääää.. 29
3.1.1 Blind signature ääääääääääääääääää. 30
3.1.2 Cryptography basis for blind signature ääääääää... 30
3.1.3 Withdrawal of eCash coins ääääääääääääää.. 31
3.1.4 Payments with eCash coins äääääääääääää. 33
3.1.5 Deposit of eCash coins äääääääääääääää 34
3.1.6 Discussion äääääääääääääääääää 34
3.2 NetCash ääääääääääääääääääääääää.. 35
3.2.1 Withdrawal of NetCash Coins ääääääääääää. 35

3.2.2 Money-exchange ääääääääääääääääää. 36
3.2.3 Payments with NetCash Coins ääääääääääää 36
3.2.4 Deposit of NetCash Coins äääääääääääää... 37
3.2.5 Discussion ääääääääääääääääääää 37
3.3 Conclusion ääääääääääääääääääääää.. 40

Chapter 4. Combination of eCash and NetCash ääääääääääää.. 41
4.1 Combine eCash and NetCash ääääääääääääääää. 41
4.1.1 Digital coin and digital note äääääääääääää 41
4.1.2 Entities and protocols ääääääääääääääää.. 42
4.1.3 Server side mechanisms for double spending detectionää.. 43
4.1.4 Digital cash withdrawal ääääääääääääää... 44
4.1.5 Digital cash exchange äääääääääääääää.. 46
4.1.5.1 Exchange note for coins äääääääääää... 46
4.1.5.2 Exchange coins for coins ääääääääää.. 48
4.1.6 Digital cash payment äääääääääääääää... 48
4.1.7 Digital cash deposit ääääääääääääääää. 50
4.1.8 Discussion ääääääääääääääääääää 51
4.1.8.1 Multi-party security ääääääääääää.. 51
4.1.8.2 Unconditional Anonymity ääääääääää 52
4.1.8.3 Enhanced scalability ääääääääääää. 53
4.2 Extending the system ääääääääääääääääää.. 54
4.2.1 Enhance scalability ääääääääääääääää.. 55
4.2.2 Extend cash exchange mechanism ääääääääää.. 58
4.2.2.1 Offer payees unconditional anonymity äääää. 59
4.2.2.2 Offer ≥Divisibility≤ for digital cashääääää.. 60

Chapter 5. Implementation ääääääääääääääääääääää 62
5.1 Introduction ääääääääääääääääääääääää 62
5.2 System requirements and architecture äääääääääääää 62
5.3 Implementation tool ääääääääääääääääääää 64
5.4 What have been done ääääääääääääääääääää.. 64
5.5 Implement blind signature ääääääääääääääääää.. 66
5.5.1 Generate public/private key pairs äääääääääää 68
5.5.2 Blind the serial number äääääääääääääää 69
5.5.3 Sign a blinded serial number ääääääääääää... 70
5.5.4 Unblind and verify the bankπs signature ääääääää.. 70
5.6 Implement the server-client communication äääää.äääää. 71
5.7 Implement database access ääääääääääääääää. 73
5.8 Implement graphic user interface (GUI) ääääääääääää 76

Conclusion and future works ääääääääääääääääääää. 78
Reference ääääääääääääääääääääääääääää. 79
Appendix: Source codes of the implementation ..ääääääääääää. 82

List of Figures and Tables

Figure 1 ≠ Encryption and decryption ääääääääääääääääää 5
Figure 2 ≠ Encryption and decryption with symmetric algorithms ...ääää.ä... 7
Figure 3 ≠ Encryption and decryption with asymmetric algorithms ...äääää... 9
Figure 4 ≠ Digital signatures with public-key algorithms .ääääääääää. 14
Figure 5 ≠ Entities and protocols in typical digital cash payment systems ääää 22
Figure 6 ≠ Entities and protocols in the new digital cash system äääääää.. 43
Figure 7 ≠ Server-side databases for detecting double-spending äääääää... 44
Figure 8 ≠ One new database is added for enhancing the system scalability .ää... 56
Figure 9 ≠ Exchange a note for a new note ääääääääääääääää 59
Figure 10 ≠ Exchange coins for a note äääääääääääääääää... 60
Figure 11 ≠ System architecture ääääääääääääääääääää. 63
Figure 12 ≠ Class diagram in package ca.crim.dcash (UML) äääääääää 65
Figure 13 ≠ Classes in package ca.crim.dcash with details (UML) ääääää... 67
Figure 14 ≠ GUI: Configuration ääääääääääääääääääää. 76
Figure 15 ≠ GUI: Denominations äääääääääääääääääää... 77
Figure 16 ≠ GUI: Withdraw äääääääääääääääääääää... 77

Table 1 ≠ Comparing *eCash* and *NetCash* ääääääääääääää.ää 40
Table 2 ≠ Table *Denomination* in the database *Bank* ääääääääääää. 74
Table 3 ≠ Table *Notes* in the database *Client* äääääääääääääää. 76

RÈsumÈ

Les signatures ‡ *lπaveugle* rÈalisent lπanonymat dans les systËmes de paiements Èlectroniques. Cependant, une fois dÈployÈes dans les systËmes d'argent numÈrique tels que ´†*eCash*†ª, les signatures ‡ *lπaveugle* engendrent des inconvÈnients tels que la mauvaise rÈsistance aux changements dπÈchelle et l'anonymat non garanti. Dans ce mÈmoire, nous proposons de combiner les signatures numÈriques ‡ un autre mÈcanisme appelÈ ´ *Money-exchange* ª existant dans ´†*NetCash*†ª pour Èlaborer un nouveau systËme de paiement Èlectronique. Dans le nouveau systËme, deux formes d'argent numÈrique sont introduites : les billets numÈriques et la monnaie numÈrique. Nous avons Ètendu le mÈcanisme ´ *Money-exchange* ª†pour permettre l'Èchange d'argent d'une forme ‡ une autre. Du cÙtÈ de l'Èmetteur d'argent numÈrique, au moins deux bases de donnÈes sont maintenues pour dÈtecter le double paiement. Ce nouveau systËme d'argent numÈrique est trËs sÈcuritaire du fait quπil utilise deux algorithmes de cryptage symÈtrique et asymÈtrique. La combinaison des signatures ‡ *lπaveugle* avec notre extension du mÈcanisme ´ *Money-exchange* ª offre un anonymat complet et inconditionnel. Cette combinaison permet aussi une meilleure rÈsistance aux changements dπÈchelle du systËme par rapport au nombre de clients ‡ 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 CrÈpeau 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, clientsπ 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.