

AN APPROACH TO ONLINE ANONYMOUS
ELECTRONIC CASH

by

Li Ying

A thesis submitted in partial fulfillment of the
requirements for the degree of

Master of Science in Software Engineering

Faculty of Science and Technology
University of Macau

2011



Approved by _____
Supervisor

Date _____

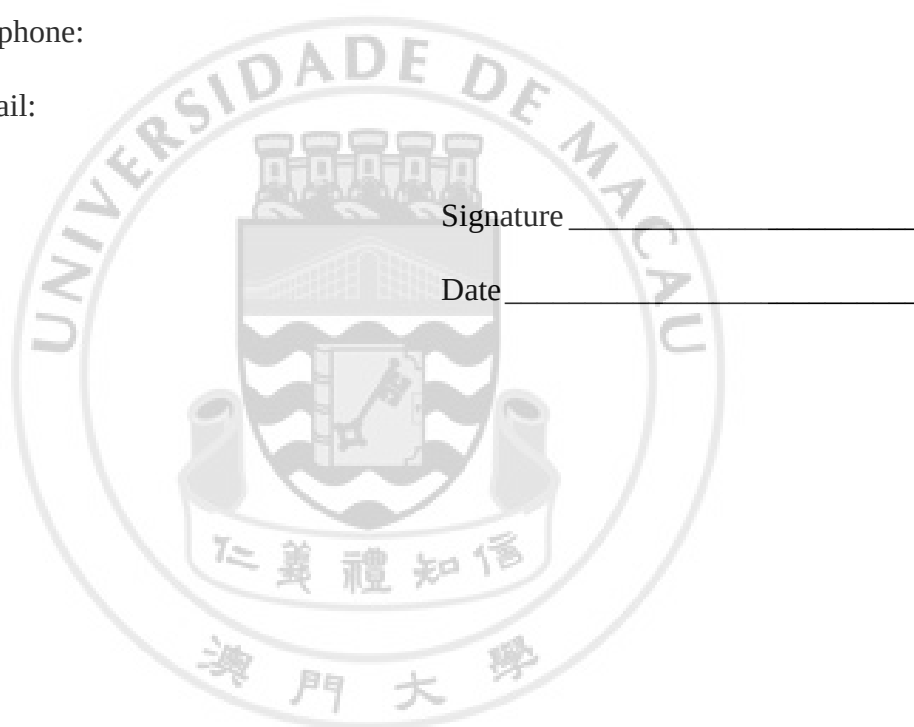
In presenting this thesis in partial fulfillment of the requirements for a Master's degree at the University of Macau, I agree that the Library and the Faculty of Science and Technology shall make its copies freely available for inspection. However, reproduction of this thesis for any purposes or by any means shall not be allowed without my written permission. Authorization is sought by contacting the author at

Address:

Telephone:

Fax:

E-mail:



University of Macau

Abstract

AN APPROACH TO ONLINE ANONYMOUS
ELECTRONIC CASH

by Li Ying

Thesis Supervisor: Prof. Guo Jing-Zhi
Department of Computer and Information Science
Master of Science in Software Engineering

Electronic cash (E-cash) has been the focus of financial cryptographers since the 1980's. Many researches began to pay close attention to the application and promotion of online electronic cash, which refers to a token or character strings issued by a bank. And they are stored and transferred between wallets of banks, merchants and customers etc. on the computer. The electronic cash system utilizes digital data for representing e-cash. However, transferability is an important issue. In some current online E-cash solutions, a user is permitted to spend the cash accepted from the issuing bank to a specific merchant. This type of system appears to be as inconvenient as depositing the e-cash into the bank after every payment for redemption. That is to say, e-cash in many existing schemes can not be used repeatedly.

This work will try to propose a novel Common Electronic Cash (CoeCash) Mechanism, which is workable e-cash payment in Internet. Moreover, it will try to implement four components of the system including the pseudonym center, CoeCash wallet system, CoeCash issuing center and CoeCash verification center.

Keywords: Electronic cash, Electronic payment systems, Anonymous control, Authentication

TABLE OF CONTENTS

List of figures	iv
List of TABLES	vi
Glossary	vii
LIST of Abbreviations	viii
Chapter 1: Introduction	1
Background	1
Research Questions and Motivation	3
Objectives	3
Organization of the Thesis	4
Chapter 2: Literature Review	6
Distinction between Various E-cash Concepts	6
Existing Electronic Cash Payment Systems	7
Typical Models and Protocols	7
Advantages of Online and Offline E-cash Systems	8
Limitations of Some E-cash Systems	9
Related Technologies Used in this Thesis	11
Hash	11
Public Key Infrastructure (PKI)	11
Digital Signature	12
Double Signature and Blind Signature	13
Elliptic Curve Asymmetric Algorithm	14
Summary	16
Chapter 3: Common Electronic Cash Mechanism	17
Overview of CoeCash Mechanism	17
The General Idea of Coecash	17
Framework of CoeCash Mechanism	18
CoeCash Issuing Protocol	19
CoeCash Withdrawal Protocol	23
CoeCash Payment and Deposit Protocols	24

CoeCash Transaction Computing	25
Summary	26
Chapter 4: CoeCash Prototype	27
Architecture of CoeCash Prototypical System	27
Implementation of CoeCash Prototypical System	28
CoeCash Pseudonym Center	28
CoeCash Wallet System	33
Flow diagram Implementation of the CoeCash Wallet System	34
The Storage Methods in the Wallet	35
Data architecture and mechanism of the Wallet (User)	36
The Main Implementation Framework of the Wallet Client	37
Transport between Wallets Software	38
CoeCash Issuing Center	38
Data architecture and mechanism of the Cashbox(Bank)	39
Using the Webservice technique to implement the issuing interface	40
Sample codes to implement the issuing interface	42
Data Encryption and Certification	44
CoeCash Verification Center (TTP)	46
Summary	50
Chapter 5: Experiments on CoeCash Prototype	51
Experimental Setup	51
Experimental Results	52
Summary	55
Chapter 6: Conclusions and Future Work	56
Bibliography	57
APPENDIX A: Key Code Fragments	60
APPENDIX B: Experimental Setting of Test Computers	67
APPENDIX C: Statistical Results of Test Computers	68
APPENDIX D: Control Code of Remote Agent Software	69
Personal Information	72
Education	72

Scholarships and Awards Listed in Dean's honor list in the second semester in 2005-2006	72
--	----

