NANYANG TECHNOLOGICAL UNIVERSITY

ELECTRONIC CASH ANALYSIS ON FAIR TRACEABILITY, DOUBLE SPENDING PREVENTION AND MODEL SIMPLIFICATION

HOU XIAOSONG

SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING

2006

Electronic Cash Analysis on Fair Traceability, Double Spending Prevention and Model Simplification

Hou Xiaosong

School of Electrical and Electronic Engineering

A thesis submitted to the Nanyang Technological University
in fulfilment of the requirement for the degree of
Master of Engineering

2006

Acknowledgements

First of all, I would like to express my sincere gratitude to my former supervisor, Dr. Tan Chik How, who guided me into the field of secure electronic commerce. His broad horizon and critical thinking made me learn a great deal during his teaching in NTU.

My special thanks to Dr. Habib Mir M. Hossein, my supervisor during thesis revision. He is always positive, encouraging and friendly, and gives me a lot of invaluable advice. In addition, as a part-time student with inflexible working hours, I would like to express my gratitude for his extra efforts and accommodation of the meeting time. Thank you, Dr. Habib.

The ICIS InfoComm Research Lab is a nurturing and stimulating environment. I would like to acknowledge the help and support of everyone in the lab who made my research work more fun and my life more pleasant.

Last but not least, my love to my parents for everything.

Summary

Our society is deeply engaged in a vast technologic revolution currently; a paper-based society is transforming to an electronic world. With proliferation and widespread use of electronic commerce over the ever-growing Internet, electronic payment systems are gaining increasing importance in our current digital society.

However, security and privacy are crucial challenges in this area: existing electronic payment systems have a major problem that they cannot handle security and privacy at the same time. These systems are secure at the cost of customers' privacy. Electronic cash solves this problem; it is an electronic payment system which enables secure payment transactions without revealing customers' identity.

This thesis starts with an overview of the concepts related to electronic payment, especially electronic cash, discussing its transactions and state-of-the-art techniques. Then, after an overview of electronic cash, we will analyze several electronic cash schemes against potential attacks.

In this thesis, I will propose *O-Cash*, the fair traceable electronic cash in wallet with observers, which supports coin tracing and owner tracing as well as self-deanonymization. This scheme achieves prior restraint of double-spending using observers, detection of double-spender's identity using cryptographic methods in case observers are broken, and fair tracing in case crimes take place.

Then, I will further propose a new electronic cash model *SignCash*, where electronic coins are generated by customers instead of banks. This model offers unique tradeoff between credit card systems and conventional off-line electronic cash systems, and provides anonymity to customers and higher security level than credit card systems. In addition, it enables customers to generate electronic coins which are authorized by the bank, and is more convenient for customers to use.

Last but not least, I will compare the proposed electronic cash system with VisaCash and eNETS, and discuss the implementation aspects.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Payment Systems

In general, all payment systems can be classified into two categories, namely, token-based systems (such as paper cash, pre-paid phone cards, subway tokens, etc.) and account-based systems (such as credit cards, telephone accounts, bank accounts, etc.). The distinguishing feature between these two categories is that token-based systems provide anonymity while account-based systems do not.

1.1.1 Token Based Payment Systems

Paper cash is an example of token-based systems, and is the most frequently and widely used payment method today. One of the advantages of paper cash is that it provides anonymity, that is, the identity of the

paper cash user will not be disclosed before and after payment. However, among the many drawbacks of paper cash, the most prominent one is that both parties engaged in a transaction must be face to face. With the widespread use of interconnected computer networks and electronic communications, the potential for electronic transactions between geographically distant parties is ever increasing. This creates the needs for new payment methods, which would be compatible with electronic communications.

1.1.2 Account Based Payment Systems

On the other hand, account-based systems do not provide privacy to customers. The banks can easily observe who pays what amount of money to whom, when and where. This enables intrusive profiling of the customers' spending habits and other personal characteristic information by drawing on mathematical techniques such as data mining. If this personal information is in the wrong hands, it may be used by advertisers to send junk mails, by criminals to select their targets, or by political aggressors to track down their opponents.

1.2 Electronic Cash

Driven by inherent weakness in traditional paper-based payment systems, the extraordinary growth of electronic commerce is stimulating the great demand for electronic payment between networked shops and customers.

Unlike most electronic payment systems which are account based, electronic cash [1, 2, 3, 4] is token based. It enables the exchange of electronic coins with the monetary value assured by the bank's blind signatures and with concealed identity of the customers.

1.2.1 Electronic Cash Features

A robust and desirable electronic cash system should have at least the following basic features:

- **Unforgeability.** Only authorized entity may issue electronic cash, which should not be forged by malicious attackers.
- **Anonymity.** The identity of the electronic cash owner should not be revealed during payment and after payment. On the other hand, a shop's customers profile should not be able to be disclosed. That is, an electronic cash system should provide both the shop and the consumer with the same amount of anonymity as paper cash today.
- **Double-spending detection.** Any attempt to spend the same

electronic coin more than once should be detected.

- **Off-line verification.** The shop is able to verify the validity of the electronic coins without involvement of the bank. This is necessary because payments sometimes have to occur even when there are limitations on the bandwidth of the communication line during the transaction, or no payment network available at all.

- **Non-repudiation.** After a valid payment transaction has been correctly completed, the electronic cash system should be able to prevent a customer from falsely claiming that the transaction was invalid. Non-repudiation offers the shops protection from someone receiving goods or services without paying for them.

1.2.2 Electronic Cash Transactions

Electronic cash systems usually involve at least three parties: customer, shop and bank. The basic scheme consists of three basic phases (as shown in Figure 1.1): withdrawal phase, payment phase and deposit phase.

1. **Withdrawal phase**, in which the bank mints electronic coins for the customer: when a customer wants to withdraw some electronic coins from the bank, his/her computing device (such as an electronic wallet) engages in an transactions with the computing devices of the bank. At the end of the withdrawal phase, the

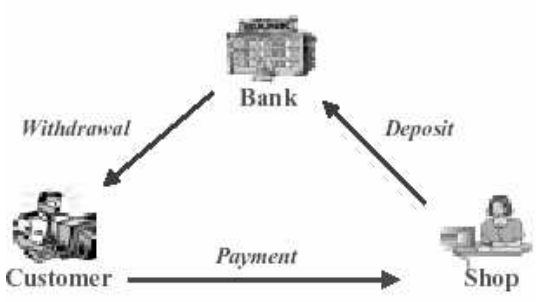

Figure 1.1: Basic Transactions of Electronic Cash

customer's computing device will obtain and store the requested amount of electronic cash.

2. **Payment phase**, in which the customer transfers the electronic cash to the shop in exchange for goods or services: to spend an electronic coin at the shop, the customer interfaces his/her computing device to that of the shop. At the end of payment phase, the available electronic cash amount from the customer's device is adjusted. In order to deposit these electronic coins, the shop will also obtain and store the customer's electronic coins with some other related payment information from the customer.

3. **Deposit phase**, which is carried out between the shop and the bank: after the bank checks and verifies the validity of electronic cash, it will credits the shop's account with the amount stated in the electronic coin.

1.3 Objective and Scope of the Research

The objective of the research is to analyze the previously proposed electronic cash systems against potential attacks, understand the open problems of current electronic cash schemes, and develop new electronic cash protocols aiming to solve the following 3 open problems of electronic cash:

- **Double Spending Prevention:** In the current digital world, nothing is easier than making multiple copies of such number strings. Therefore, prevention of double-spending is a very important research area of off-line electronic cash.

- **Fair Traceability:** A strong reason why unconditional privacy has to give way to fair tracing (revocable privacy) is that unconditional privacy may lead to 'perfect crimes' [5], such as money laundering and blackmailing, from which criminals can easily get away without leaving any trace. Therefore, fair traceability has been designed to solve these problems. Here, fair traceability means illegal tracing (without the permission from the judge or the customer) is inhibited, wile legal tracing (with the permission from the judge or the customer) is possible.

- **Model Simplification:** All previously proposed electronic cash

systems include a generally complicated process of withdrawal phase between the customer and the bank. Since the customer and the bank have to generate each electronic coin to be used, this withdrawal phase is tedious for the customers, who may like to eliminate this phase if possible. In this thesis, I will try to propose a new electronic cash model by eliminating the traditional withdrawal phase.

1.4 Contributions of the Author

The contribution of this thesis is as follows:

- A detailed review and analysis of existing electronic cash schemes against potential attacks.
- The proposal of an electronic cash protocols (*O-Cash*), which addresses the open problems of double spending prevention and fair traceability. This proposal achieves prior restraint of double-spending, detection of double-spenders' identity in case the observer is broken, and supports coin tracing and owner tracing as well as self-deanonymization in case crimes take place.
- The proposal of a new fair traceable electronic cash model and an instance of its application (*SignCash*), which addresses the open problem of model simplification. This scheme enables customers

to generate electronic coins on behalf of the bank, and offers more convenience to customers.

1.5 Organization of the Thesis

The organization of the rest of the chapters in this thesis is as follows: Chapter 2 surveys several important electronic payment systems in practice, which serve as the background information for the analysis of electronic cash. Chapter 3 provides a review of different types of electronic cash schemes, and discuss the some of the important techniques for electronic cash. Chapter 4 presents the proposal of an electronic cash system in wallet with observers that supports coin tracing, owner tracing as well as self-deanonymization. Chapter 5 provides a proposal of a new fair traceable electronic cash model and an instance of its application. Last but not least, in chapter 6, I compare the proposed electronic cash system with two existing electronic payment systems (VisaCash and eNETS), and discuss the implementation aspects of *O-Cash*.

Chapter 2

Survey of Electronic Payment Systems and Technologies

To date, there have been many electronic payment systems and technologies, aiming to realize different functions of traditional payment systems. In this chapter, I provide an overview of electronic payment in practice.

2.1 Electronic Payment Systems

2.1.1 Credit Card

Credit Card is currently the most popular electronic payment method on the Internet. The main reasons of its popularity are convenience, ease of use and omnipresence etc. However, the credit card system is not an

ideal payment method from security and privacy point of view [6].

- **No anonymity was offered to customers:** Despite the convenience of keeping a full record of customers' payment history in order to solve payment disputes, the fact that all purchases are traceable allows the bank to know their customers' whereabouts, spending patterns and personal preferences etc.

- **High costs and inability to allow small value payments:** Each credit card payment has a fixed cost plus a variable cost of 2-20% depending on the negotiated contract with the shop. For example, as a result of these high fees, credit card payments of less than 20 Singapore Dollars are not accepted in most shops in Singapore.

- **Security problems for customers:** One of the biggest problems with credit card payments is that all the users' private information is exposed to the shops. Customers have to disclose their credit card details to the shops, and trust that the shops will not misuse their credit card information. This is quite contradictory to the fact that credit card details are actually the secrets on which the whole payment system is based. In addition, even if the shops are trustworthy and honest, there are still potential threats that hackers could hack into shops' web servers and obtain huge lists of credit card informa-

tion for criminal purposes. As a result, credit card holders have to check each payment item on the monthly statement, and make sure they are not falsely charged. Even after the finding of fraudulent charges, the reimbursement process is generally time-consuming and troublesome. Therefore, in credit card systems, costumers are 'unfairly' penalized for the credit card model's own inappropriate system design.

To improve the security of credit card system, SET (Secure Electronic Transaction) was developed to provide authentication and payment data confidentiality for credit card users and shops. This solution is independent of the transport mechanism, and can be used on the world wide web as well as through emails. The core security features of SET are as follows:

1. SET participants can be authenticated by utilization of digital certificate. In this way, shops can be assured that the transactions are engaged with registered and legitimate credit card users.

2. The payment information is kept confidential by the credit card company, that is, credit card details are sent to the shops in encrypted form, and can only be decrypted by the credit card company.

3. Dual signatures are used to link the order message with the payment details in order to protect the integrity of the entire transaction. It also keeps the customer's account details secret from the shop and the purchase details secret from the bank.

SET is technically superior to credit card system over SSL/TLS. However, it has not been widely implemented because of its overall complexity and redundancy in the message exchange. Moreover, like most electronic payment schemes, SET dose not cater for the customers' anonymity.

In summary, although credit card is currently the most popular electronic payment method, many potential customers are deterred by privacy and security reasons, such as concerns of transmitting their credit card details over the Internet, fear of misuse of their card details by fraudulent shops, or fear that their personal information could be compromised or sold to other parties. Therefore, it is necessary to introduce alternative electronic payment methods that enable customers to complete their payment transactions on the Internet more securely and conveniently.

2.1.2 Store Value Card

Store Value Card is originally designed for circumstances in which the customer is present at the point of sale or service. This is a form of prepaid cash tokens that are stored in smart card chips, such as VisaCash

of Visa Inc. and CashCard of NETS Pte Ltd.

For example, NETS CashCard [7] is one of the most widely used electronic payment methods in Singapore. It is commonly used for libraries and shops, as well as electronic road pricing (ERP) payments and car park fees.

Store value cards have the following attributes:

- **Strength: Off-line Verification.** Store value card system verification is distributed, that it, it does not need central authority to perform realtime online verification. The smart cards act like branch offices of a business. They have the ability to transfer money in and out without getting permission from the central office. This is an attractive and important feature where telecommunications facilities are expensive or unavailable.

- **Strength: Low Costs.** Off-line verification can significantly reduce the transaction costs of central administration. Therefore, compared with credit cards, the advantage of store value cards is that they are more suitable for small-value payment, and are more easily obtainable due to no requirement on credits. In addition, the material costs of store value cards have been declining in recent years (as low as 1 USD).

- **Weakness: Potential Security Issue.** Store value cards are

based on smart card chip, which is a tamper-resistant unit but not tamper-proof. Therefore, it is subject to a physical attack on the card itself. This sort of attack may even be carried out by the owner of the card, in order to obtain an increased monetary value. Physical attacks can reverse-engineer the smart card and determine the secret keys, as demonstrated in the papers of Anderson and Kuhn [8], Boneh, DeMillo, and Lipton [9]. They showed that the secret key of the smart cards can be discovered after the smart cards are forced to make several simple processing errors. For example, the attacker can subject the smart card to alpha particles, which are known to flip bits from time to time. Actually, any method that can cause voltages inside the card to fluctuate will cause the smart card to make mistakes, which may be used by attackers to break the smart card.

In practice, there have been many stories where great loss was reported due to the security problems of smart cards. For example, in May 1996, two Japanese Cash Card companies reported that they sustained losses of USD 588 million, due to counterfeit cards.

In summary, although store value cards have the strength of low costs, anonymity and off-line verification, total reliance on the physical robustness of smart card is unacceptable in many applications, especially high-

value electronic payment transactions.

2.1.3 Electronic Banking

This term is used for a variety of electronic payment services whereby a customer uses an electronic device at home or workplace to initiate payment to a payee. In addition to Internet technology, electronic banking can be performed using the telephone and Interactive Voice Response (IVR). This allows customers to conduct their financial transactions from any touch-tone telephone anytime and anywhere. Through e-banking, customers can check account balance, pay bills, make payments and stop a cheque payment, etc.

For example, eNETS is a suite of Internet and mobile payment services offered by NETS Pte Ltd, giving customers greater convenience in making online and mobile payments.

- **Strength: Customer Range.** eNETS web services incorporate multiple electronic payment solutions of credit cards, direct debit and virtual accounts into one package. Customers with any kind of account can register for eNETS services.

- **Strength: User Friendliness.** It is very easy to use eNETS, where customers can complete the electronic payment in just 3 steps. In addition, when making payment at online shops, cus-

tomers can use eNETS to automatically fill in the payment form.

- **Weakness: No Anonymity.** eNETS is based on the account based payment systems, such as credit cards, internet banking accounts and eNETS virtual accounts. As shown in Chapter 1.1, account based systems do not offer anonymity to the customers.

- **Weakness: No Off-line Verification.** For all eNETS payment transactions, online verification with the central server is required, which greatly increases the transaction costs. In addition, online verification is subject to network congestion and potential breakdown.

2.2 E-wallet Technology

Recently, entrepreneurs and researchers alike are breaking through the initial online payment barriers of electronic commerce, through the development of various electronic payment systems and technologies, one of which is e-wallet (also known as digital wallet or electronic wallet).

2.2.1 E-wallet Functions

The basic functions of e-wallet are as follows:

- **Online Shopping Assistance:** With e-wallet, customers can in-

put all of their purchasing information (such as credit card, shipping address and contact number etc) once, and then make 'one-click' payment at various web sites that accept e-wallet. This provides customers relief from repetitive typing and tedious task of filling out each individual web site's purchase form. By clicking the 'pay' button, customers can initiate an electronic payment via a secure electronic transaction.

- **Identification and Authentication:** E-wallet will utilize PIN (personal identification number) to identify the customers, and to decrypt messages and generate digital signatures. It will also check the validity of digital certificates received from online shops. In this way, customers as well as shops will benefit from these functions by receiving better protection against fraud.

2.2.2 ECML – Electronic Commerce Modelling Language

To standardize e-wallet technologies and applications, Visa, MasterCard and American Express, with the support from IBM, Microsoft and Sun etc, developed and implemented ECML (Electronic Commerce Modelling Language). This language provides a set of hierarchical payment oriented data structures which enable electronic wallet to supply needed payment

data in a uniform manner to multiple online shops. In terms of security, ECML works with any web security software and any security standard, including SSL, and Visa and MasterCard's own version of SET.

2.2.3 E-wallet Architecture

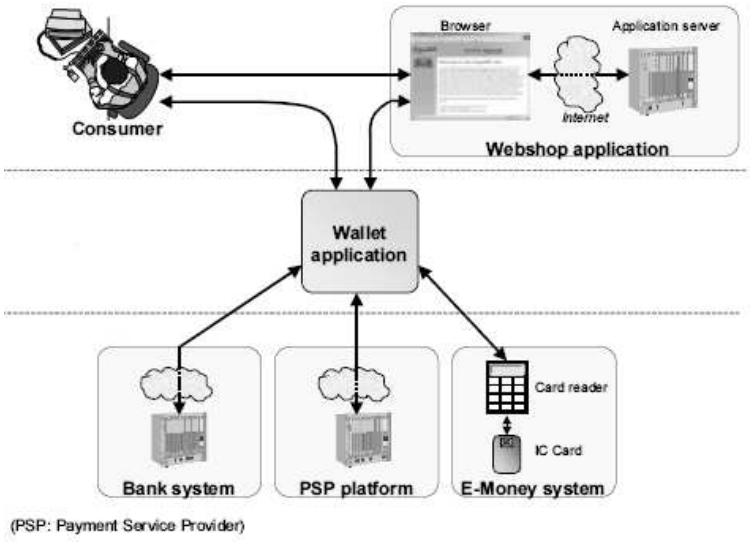

Figure 2.1: E-wallet Architecture

The architecture of e-wallet is shown in Figure 2.1 [10]. Basically, e-wallet is a mediator between customers and core payment schemes, and this technology facilitates electronic payment.

There are two types of e-wallet:

- Client-based e-wallet, which stores customers' encrypted personal information on their local devices, such as computer, PDA (personal digital assistant) or mobile phone.

- Server-based e-wallet, which stores customers' personal information in servers of Payment Service Providers (PSP) or Banks.

2.2.4 E-wallet Examples

I will show one example from each type of e-wallet: Ilium e-wallet for client-based e-wallet and Yahoo e-wallet for server-based e-wallet.

Ilium E-wallet

Ilium E-wallet [11] (as shown in figure 2.2) is a kind of client-based e-wallet, which safely stores the confidential payment information on the customer's Windows PC, Windows Mobile-based Pocket PC or Smartphone. It protects the locally stored e-wallet information by requiring a password before displaying any encrypted categories.

When making payment, the customer need to enter the password to activate the e-wallet first, then he/she can just let the e-wallet automatically fill in the online payment form and complete the payment transactions, by clicking on the 'pay' button.

Yahoo E-wallet

Yahoo E-wallet [12] is a service offered by Yahoo that stores customers' credit card, billing, and shipping information in Yahoo's servers. Customers only need to sign in with the Yahoo ID, in order to enjoy

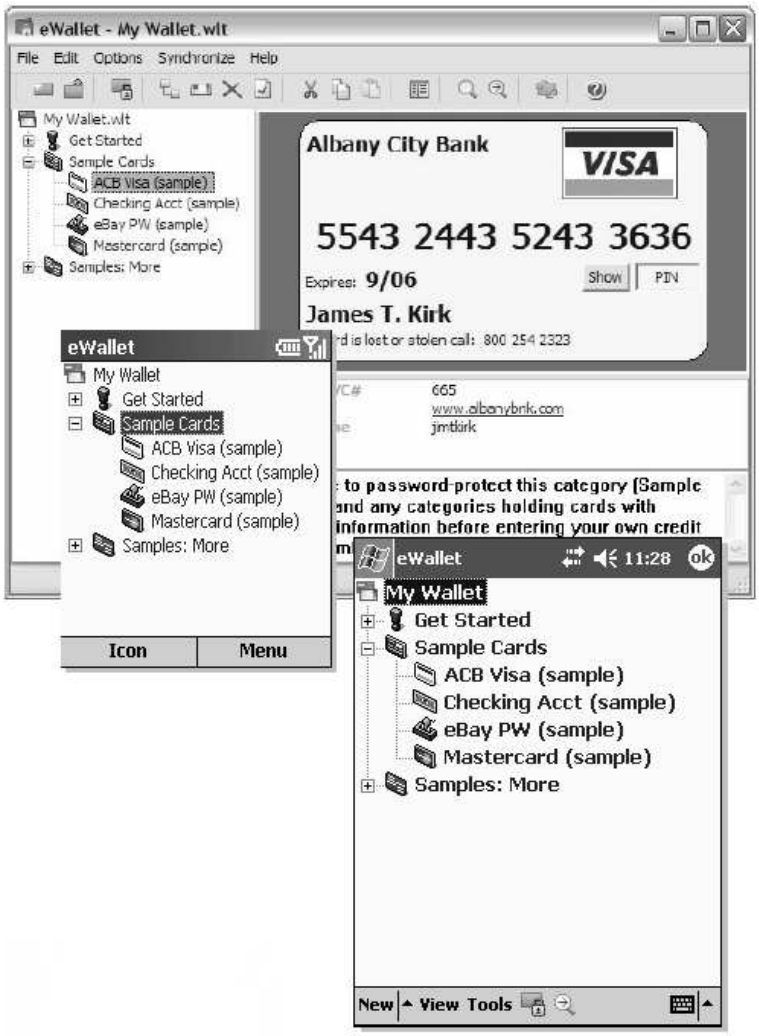

Figure 2.2: Client-based E-wallet Sample: Ilium

the service of a fast and easy checkout mechanism that remembers their credit card and shipping address information for shopping in online shop sites.

2.3 Summary of Electronic Payment

Among all the current and proposed electronic payment systems, electronic cash is generally considered as one of the most ideal electronic payment systems. However, the research in electronic cash is one of the most challenging and difficult electronic payment areas. There are several open problems that are yet to be satisfactorily resolved, such as prevention of double-spending in off-line schemes and efficient mechanisms of fair tracing fraudulent or criminal transactions etc. Therefore, a large number of researchers all over the world have shown great interests in the research of electronic cash.

Chapter 3

Literature Review of Electronic Cash

3.1 Introduction

In 1983, Chaum introduced the first anonymous electronic payment system named electronic cash [2]. As electronic cash is just a string of bits, and unlike paper cash whose security is based on the difficulty of physical forgery, electronic cash is easy to replicate and double-spend. To solve this problem, Chaum proposed that the bank should maintain a list of the already spent electronic coins and check whether each deposited coin had been spent before. This means that the bank has to be online for each payment to make sure the electronic cash is not double-spent.

3.1.1 Online vs. Off-line

In practice, forcing the bank to be online at each payment is unacceptable in many situations, because:

- Payments need to be done without connecting to the bank in some cases.
- There may be millions or even billions of payment transactions done at the same time. Therefore, checking every payment online and requiring real-time verification may lead to bank's network congestion.
- In case of the bank's system or network breakdown, no payment can be carried out at all.
- Online electronic payment systems are usually lack of atomicity [13]: network failures during a transaction will result in loss of the electronic cash involved. An ideal electronic payment system should be fair and robust in the sense that network failures, for example, do not result in incomplete transactions.
- Another problem of online electronic payment is scalability [14]: as all electronic coins that have been spent have to be recorded, the bank's database will grow over time, increasing cost and time to detect double-spending.

To overcome these limitations, electronic cash schemes need to bypass the online requirement.

Even, Goldreich and Yacobi [15] proposed an off-line electronic cash scheme based on tamper-resistant units. However, tamper-resistant units are not tamper-proof, therefore, reliance solely on the tamper-resistance of these devices is subject to attacks as described in [8, 9]. Also, because the customer has no control over the messages sent from the tamper-resistant unit [15], this unit can secretly send the customer's private information to other parties during payment transactions; in this way, the customer's privacy is compromised.

In 1989, Chaum, Fiat and Naor proposed the first off-line anonymous electronic cash scheme [16]. Unlike online electronic cash schemes which prevent double-spending by checking each electronic coin against an on-line central database, off-line electronic cash schemes cannot offer prior prevention of double-spending – they can only 'detect' double-spending using secret sharing mechanism [17].

3.1.2 Secret Sharing Mechanism

As we know, double-spending is a serious threat for off-line electronic cash schemes.

To prevent double-spending, most of the off-line electronic cash schemes

use secret sharing mechanism introduced by Blakley [18] and Shamir [17] independently.

The motivation for secret sharing is secure key management. In many situations, there is only one secret key that provides access to the confidential and important files. If the secret key is lost for some reasons, then all those important files will become inaccessible. The basic idea of secret sharing is to divide the secret key into pieces and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the secret key. The general model for secret sharing is called a 'k-out-of-n' scheme or '(k, n)-threshold' scheme. In this scheme, there is one dealer and n participants. The dealer divides the secret into n pieces and gives each participant a piece of the secret, such that any k parts can be put together to recover the secret, but less than k pieces are not able to reveal any information about the secret.

When applying secret sharing scheme to double-spending prevention, the customer gives a share of his/her identity code to the shop at each payment in response to a random challenge. If the customer spends the same electronic coin twice, he/she has to give two different shares, which will allow the bank to recover the customer's identity eventually.

With the concept of secret sharing, 'cut-and-choose' method is introduced in the first off-line untraceable electronic cash scheme [16]. In the withdrawal phase of the scheme, the customer sends to the bank $2n$

(where n is the security parameter) candidates; then the bank randomly 'cut-and-chooses' n candidates, which are named as 'terms'. The customer 'opens' inner structures of those chosen candidates to show their correctness. After verifying that those chosen candidates are all correctly structured, the bank will be sure with overwhelming probability ($> 1 - \frac{1}{2^n}$) that the rest of the candidates are also correctly structured, then the bank blindly signs them. At payment, the customer is required to provide a share of his/her identity code in response to a random challenge from the shop. The shop can verify the correctness of this response. In the deposit phase, if two distinct shares of the identity code are collected by the bank, then the identity of the double-spender is revealed.

This scheme [16] has the advantage that it does not require tamper-resistant hardware but still provides the cryptographic tracing of double-spenders. Detection after the fact may be enough to discourage double-spending in most cases, but it does not solve the problem. If someone is able to obtain an account under a false identity, or is going to disappear after double-spending a huge amount of money, they could successfully cheat the system. Therefore, in many situations, it is already too late to detect double-spending after it takes place, which has caused a great deal of loss to the electronic cash system. Indeed, an ideal off-line system must be able to actually inhibits double-spending before it takes place. (In chapter 4, I will discuss the open problem of double spending prevention

in more details.)

In terms of efficiency, although 'cut-and-choose' method successfully enables the first design of off-line electronic cash schemes, this method is by its very nature inefficient. In order to get a high enough probability of cheating detection, the electronic cash based on 'cut-and-choose' must consist of many terms, half of which are thrown away. Therefore, new techniques were proposed to achieve double-spending detection without using 'cut-and-choose' method.

3.2 Single Term Electronic Cash

3.2.1 Ferguson's Scheme

Ferguson [19] proposed the first 'single-term' electronic cash scheme based on RSA, instead of using the 'cut-and-choose' method.

In this scheme, each electronic coin is represented as three numbers, A, B and C.

$$A = ag_a^{f(a)}$$

$$B = bg_b^{f(h_b^b)}$$

$$C = cg_c^{f(h_c^c)}$$

where $g_a, g_b, g_c \in Z_n^*$ are public known numbers, h_b, h_c are public know elements of order n, and $f()$ is a one way hash function.

In the withdrawal phase, the customer gets two RSA signatures from the bank: $(C^U A)^{1/v}$ and $(C^k B)^{1/v}$, where $(v, 1/v)$ is the bank's public/secret key pair, U is the customer's identity code and k is a random number which is unique for each electronic coin. During the payment phase, in order to spend the electronic coin (A, B, C), the customer has to prove to the shop that he/she has the bank's signature on (A, B, C). In response to the shop's randomly chosen challenge d, the customer sends $r = Ud + k \bmod v$, which is the share of his/her identity, and the signature $(C^r A^d B)^{1/v}$, which can be computed by $[(C^U A)^{1/v}]^d (C^k B)^{1/v}$. The shop can easily verify the validity of these two responses. If the customer double-spends the electronic coin, he/she has to reveal two responses $r = Ud + k$ and $r' = Ud' + k$, which allow the bank to determine the double-spender's identity code $U = (r - r')/(d - d')$.

Analysis of the Scheme

This scheme is subject to an attack in the withdrawal phase. The attackers can obtain the bank's signature on two electronic coins as

$$[(C^{U_1} A)^{1/v}, (C^{k_1} B)^{1/v}], [(C^{U_2} A)^{1/v}, (C^{k_2} B)^{1/v}]$$

where U_1, U_2 are the identity codes of two customers, and k_1, k_2 are two randomly chosen numbers. Now, using these two signature pairs, the attackers can spend two electronic coins three times without revealing the identity codes in the following way:

$$[(C^{U_1}A)^{1/v}, (C^{k_1}B)^{1/v}], [(C^{U_2}A)^{1/v}, (C^{k_2}B)^{1/v}], [(C^{U_2}A)^{1/v}, (C^{k_1}B)^{1/v}]$$

At the end the deposit phase, the bank will get $U_1d_1 + k_1, U_2d_2 + k_2, U_2d_3 + k_1, d_1, d_2, d_3$. There are four unknown parameters k_1, k_2, U_1 and U_2, but only three equations, therefore, it is inadequate for the bank to compute the identity codes of the double-spenders.

In order to solve this problem, there must be a mechanism to ensure that A, B, C are not the same for any distinctive electronic coins. Therefore, an enhanced scheme proposed that bank should take part in the construction of A, B, C and make sure customers do not have so much freedom to construct A, B, C in order to abuse the system. At the same time, the anonymity of the customers are not compromised, because it is the customer who computes A, B, C from the their blinded versions signed by the bank. The proposal details of the enhanced scheme can be found in [20].

The efficiency of the single term electronic cash scheme [19] is much higher than those 'cut-and-choose' based schemes, as proved by the au-

thor. However, it is still not satisfactory. To withdraw an electronic coin, the customer needs to use 6 blind factors and perform over 20 exponential computations [21].

In addition, because the bank knows the customer's identity code U in the withdrawal phase, it can frame any particular customer, that is, the bank can successfully claim the customer is guilty of double-spending, but the customer has no way to obtain proof to defend himself/herself.

3.2.2 Varadharajan-Nguyen-Mu's Scheme

This V-N-M off-line electronic cash scheme [21] improved the efficiency of Ferguson's scheme by making some of the parameters used in the protocol to be reusable, and removes the customer's risk of the bank's framing by hiding the customer's identity. The scheme [21] works as follows:

The bank chooses a large RSA modulus n, which is the product of two large primes p and q, and a public/secret key pair $(v, 1/v)$, where v is a large prime number. The bank also publishes a suitable one-way hash function $h(\cdot)$. Let w_a, w_b, w_c and w_d be secret numbers which are randomly chosen by the bank; The bank computes $A = g^{w_a} \bmod n, B = g^{w_b} \bmod n, C = g^{w_c} \bmod n$ and $D = g^{w_d} \bmod n$ as bank's public information, where g is a generator selected from the multiplicative group Z_n^*.

Both the bank and the customer can compute a, b as follows:

$$a = I^{w_a} B = g^{w_a U} B = A^U B \bmod n,$$

$$b = I^{w_b} C = g^{w_b U} C = B^U C \bmod n,$$

where U is the customer's secret identity code and $I = g^U \bmod n$ is the customer's account number.

In the withdrawal phase, the customer and the bank preform the protocol as follows:

Customer		Bank
$g_Y = g^{U/y} \bmod n$		
$g_y = g^{1/y} \bmod n$		
$D_k = D^{1/k} \bmod n$		
	$\xrightarrow{g_Y, g_y, D_k}$	
The customer use zero-knowledge proof to prove that he knows y, k		
		$s_1' = [a g_Y^{w_b} g_y^{w_c}]^{1/v} \bmod n$
		$s_2' = [B D_k]^{1/v} \bmod n$
	$\xleftarrow{s_1', s_2'}$	
$s_1 = s_1'^y = (a^y b)^{1/v} \bmod n$		
$s_2 = s_2'^k = (B^k D)^{1/v} \bmod n$		

$r \in Z$

$m_1 = a^y b \bmod n$

$m_2 = B^k D \bmod n$

$m = h(Uy \bmod v \| m_1 \| m_2) \bmod n$

$m' = r^3 m \bmod n$

$\xrightarrow{m'}$

$s' = m'^{1/3} \bmod n$

$\xleftarrow{s'}$

$s = s'/r = m^{1/3} \bmod n$

The payment protocol is described in the following diagram:

Customer		Shop
		$d \in_R Z_v$
	$\xleftarrow{d}$	
$\alpha = Uy \bmod v$		
$\beta = (U+y)d + k \bmod v$		
	$\xrightarrow{\alpha,\beta,s,s_1,s_2}$	
		Check
		$s^3 \stackrel{?}{=} h(\alpha \| s_1^v \| s_2^v) \bmod n$
		$(s_1^d s_2)^v \stackrel{?}{=} A^{\alpha d} B^\beta C^d D \bmod n$

Analysis of the Scheme

In the deposit phase, double-spending detection is described as follows: the bank will obtain two different responses from the double-spender $\beta = (U + y)x + k$ and $\beta_0 = (U + y)x_0 + k$ for two different challenges x and x_0 provided by the shops. This will immediately allow the bank to determine $U + y = \frac{\beta - \beta_0}{x - x_0}$. As the bank also has $\alpha = Uy$, [21] claims that the bank can calculate the double-spender's secret identity code U using the following equation:

$$\begin{aligned} \alpha &= Uy \\ &= U(\frac{\beta - \beta_0}{x - x_0} - U) \\ &= \frac{\beta - \beta_0}{x - x_0}U - U^2 \end{aligned}$$

However, [21] does not provide proof that the above quadratic equation will definitely have solutions. In the case of no solutions for the quadratic equation, customers can easily double-spend electronic coins without being detected later on.

In addition, it is the customer who secretly chooses U to construct g^U as his/her identity code in the registration phase, and who computes $g_Y = g^{U/y} \bmod n$ in the withdrawal phase. However, if the customer uses different U in these two phases, the bank will not be able to link

the double-spent electronic coins to the identity of the double-spender. Therefore, to prevent this attack, a zero-knowledge proof [22] must be built in the withdrawal phase to make sure the customer is using the same U in these two phases.

3.3 Fair Traceable Electronic Cash

3.3.1 Concept of Auditable Fair Tracing

Kügler and Vogt proposed the idea of auditable tracing [23, 24, 25] that ensures detection of illegal tracing in the audit phase. They pointed out that those schemes that requires a trusted third party will incur additional costs and that misbehaviors of the trusted third party will compromise the privacy of the customers. Therefore, they suggested that fair tracing should be carried out by the bank only without any help of trusted third parties. They called their withdrawal-based scheme as *optimistic* fair tracing, which means that the decision of whether the coins should be traceable or not must be made in the withdrawal phase. This protocol cannot prevent illegal tracing beforehand, but can detect it afterwards by the traced customer. Any tracing without the judge or customer's permission is considered illegal and will be prosecuted.

3.3.2 Kügler-Vogt's Scheme

The basic idea of scheme [23] is to embed two tags in every coin: one tag contains the marking information for coin tracing (marking tag), while the second tag contains the identity of the withdrawer for owner tracing (identity tag). The customer cannot distinguish these two tags, but the bank can make the difference using the index tag. At payment the bank will ask the customer to reveal one of these two tags. The bank will accept this coin, only when the returned tag is correct. The following is a brief overview of the electronic cash scheme [23]:

Setup of the Scheme

Let $G =< g >$ be a group of order q and $g \in G$.

For the Schnorr blind signature scheme [26], $x \in_R Z_q^*$ is the blind signature private key of the bank; $y = g^x$ is the blind signature public key of the bank.

For ElGamal encryption scheme [27], there are three key pairs ($j = 0, 1, 2$): $x_j \in_R Z_q^*$ are the private encryption keys of the bank; $y_j = g^{x_j}$ and $y'_j = y^{x_j}$ are the public encryption keys of the bank.

The bank randomly chooses the default mark $M = M_{default}$ and two points (P_0, P_1), which will be the content of the index tag.

The function C_i chooses the i-th element from $(A_0, A_1, \ldots, A_i, \ldots, A_n)$.

Withdrawal Phase

Bank	Customer
$r \in_R Z_q^*$	
$i \in_R \{0, 1\}$	
If customer is not traced:	
$M = M_{default}$	
If customer is traced:	
$M = M_{session}$	
	$(\alpha, \gamma) \in_R (Z_q^*)^2$
	$(j = 0, 1, 2)$
	$\delta = g^\alpha y^\gamma$
	$\delta_j = y_j^\alpha y_j'^\gamma$
	m:serial number
$a = g^r$	
$t_0 = y_0^r \cdot P_i$	
$t_1 = y_1^r \cdot C_i(M, M_{session})$	
$t_2 = y_2^r \cdot C_i(M_{session}, M)$	
$\xrightarrow{a, t_0, t_1, t_2}$	
	$a' = a \cdot \delta$
	$t_0' = t_0 \cdot \delta_0$

$$t_1' = t_1 \cdot \delta_1$$

$$t_2' = t_2 \cdot \delta_2$$

$$c' = H(m, a')$$

$$c = c' - \gamma \bmod q$$

$$\xleftarrow{c}$$

$$s = r - cx \bmod q$$

$$\xrightarrow{s}$$

$$s' = s + \alpha \bmod q$$

$$a' \stackrel{?}{=} g^{s'} y^{c'}$$

coin: (m, c', s')

tags: (t_0', t_1', t_2')

At the end of the withdrawal phase, the customer will obtain (m, c', s') as the electronic coin, and (t_0', t_1', t_2') as the tags for checking of any illegal tracing.

- The index tag (t_0') contains the pointer P_i, where $i \in_R \{0, 1\}$ is chosen randomly.
- The left tag (t_1') contains the mark $C_i(M, M_{session})$, where $M = M_{default}$ for untraced customers and $M = M_{session}$ otherwise.
- The right tag (t_2') contains the mark $C_i(M_{session}, M)$ with M defined as above.

A *mark* either refers to the identity of the withdrawer or contains no information at all. The mark that contains no information is called the default mark and a coin with such a mark is called unmarked.

- If the shop was traced, the identity tag of the customer is revealed.
- Otherwise, the revealed tag is the marking tag:
  - If the marking tag contains the default mark, the coin was not traced.
  - Otherwise, the identity of customer is revealed.

Payment and Deposit Phase

Bank	Shop	Customer
		$coin : (m, c', s')$
		$tags : (t'_0, t'_1, t'_2)$
	$\xleftarrow{C, t'_0}$	
$\xleftarrow{C, t'_0}$		

$a' = g^{s'} y^{c'}$

$c' \stackrel{?}{=} H(m, a')$

$P = t'_0 / a'^{x_0}$

Set i so that $P = P_i$

If shop is traced, then $d = 1 - i$; **otherwise** $d = i$

The bank signed its decision as:

$D = Sign(shop, d, C, t'_0)$

$\xrightarrow{d,D}$

$\xrightarrow{d,D}$

Check Signature D

$\xleftarrow{t'_{1+d}}$

$\xleftarrow{t'_{1+d}}$

$M = t'_{1+d}/a'^{x_{1+d}}$

If shop is not traced:

look up mark M for coin tracing, if $M \neq M_{default}$

If shop is traced:

look up mark M for owner tracing

Tags and Marks in Auditable Tracing

At the beginning of the audit phase of each generation of electronic coins, the bank publishes the key that can enable customers to open all the tags: left, right and index tags. Each spent coin can be checked whether its revealed tag was the identity tag or the marking tag.

If the revealed tag was the identity tag, the customer will know that he/she has been traced. In order to make sure he/she has not been illegally traced, the customer will need to check whether this tracing has been permitted by the judge. Therefore, illegal tracing can be detected

by the customer in the audit phase.

In normal cases where there are no tracing, the customer should not have revealed the identity tag during payment transactions. What the customer have revealed should be only the index tag and a marking tag containing the default mark. If the customer can make sure he/she has not revealed the tag containing his/her identity information during payment transactions, he/she will know the payment is unconditionally anonymous.

In addition, the tags are protected from being fiddled and tampered by unauthorized persons, even involved persons, such as any customer who want to falsely claim that he/she has been illegally recognized and traced.

- Before the payment: During withdrawal phase, the bank and the customer directly participate in the protocol, where all ElGamal encrypted tags share the same commitment α with the Schnorr signature. Theses tags (t_0, t_1, t_2) are originally prepared by the bank with its digital signature, and later blinded to t'_0, t'_1, t'_2 with the customer's own information. This prevents the bank from recognizing the customers by these tags. At the end of the withdrawal phase, these tags are kept by the customer in his/her secure electronic device, which also prevents the tags from being fiddled and

tampered via access control of the electronic device.

- During the payment, only the customer and the bank will be engaged in an online verification protocol via a secure communication channel. They will not want fiddle the tags, because the payment will not be successful if the tags have been changed.

- After the payment: If the customer wants to falsely claim that he/she has been traced via proof from fiddled tags, he/she simply cannot do that because those correct tags have been recorded in the bank system. In addition, based on the security of Schnorr blind signature, which has been proven to be secure in generic model and random oracle [26], it is hard for anyone to forge or modify any tags without the secret key from the bank. Therefore, this kind of attack which aims to fiddle and tamper the tags only succeeds with negligible probability.

In this scheme [23], at the beginning of audit phase, the bank publishes the private decryption keys x_0, x_1, x_2 and the marks $M_{default}, P_0, P_1$. For every coin, the decryption keys enable the customer to extract the content of each tag. Comparing the content of the index tag with P_0 and P_1 determines which tag is the identity tag and which is the marking tag. Thus, the customer will know whether illegal tracing has been applied by the bank.

Analysis of the Scheme

This scheme is novel and efficient. However, auditable tracing cannot prevent illegal tracing, it can only detect illegal tracing 'after the fact'. This may be unacceptable in many situations. Secondly, the introduction of the additional audit period causes additional troubles for customers, who have to verify each coin's tracing possibility. Thirdly, in the audit phase, the bank has to publish all marking keys and unique undeniable signature key x. Since marking has to be authorized by a judge, and the bank has to save all marking keys and get certifications from the judge. This will introduce additional costs and complexity to the system. Last but not least, there exists a problem that may compromise the anonymity of the customer. Since no mechanism controls the bank's behavior in the audit phase, the bank can publish P_0 as P_1 and publish P_1 as P_0. Therefore, for a whole generation of coins, the bank can secretly trace every electronic coin, but all customers will think that they have not revealed their identity tags and they are not traced.

In order to make the scheme withstand this kind of attack as mentioned in the previous paragraph, a mechanism must be built in to prevent the bank from publishing P_0 and P_1 without any control. A way to repair the scheme is to make the bank publish the commitment of the relationship of P_0 and P_1, say P_0/P_1, at the beginning of this generation

of electronic coins. By doing so, the scheme forces the bank to publish P_0 and P_1 in the right order in the audit phase, which prevents the bank's above mention misbehavior.

3.4 Divisible Electronic Cash

Divisible electronic cash system is a system where customers can divide the withdrawn coins into sub-coins of smaller value and make payments many times as long as the total value of the spent sub-coins does not exceed the value of the withdrawn coin.

Binary tree, as shown in figure 3.1 [28], is the basic building block for divisible electronic cash. Each electronic coin of worth $w = 2^l$ is associated with a tree of $(l + 1)$ levels and w leaves.

Each node of the binary tree represents a certain denomination. The root node has the value w, and any other node's value can be computed by halving the value of the node's parent.

Under the following two rules, customers can choose appropriate nodes to make exact payments:

1. **Route node rule:** When a node is used, all descendant nodes and all ancestor nodes of this node cannot be used.

2. **Same node rule:** No node can be used more than once.

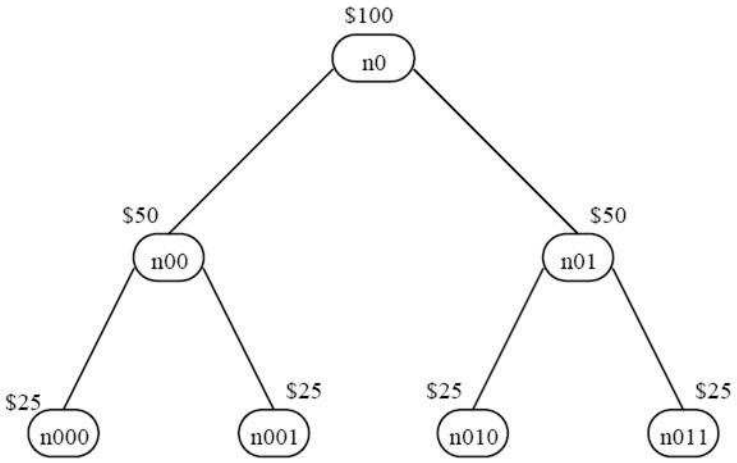

Figure 3.1: Sample Binary Tree

Some divisible electronic cash systems [29, 30, 28] have been proposed. However, in most divisible electronic cash systems [30, 28], sub-coins are linkable, that is, anyone can decide whether two payments are made by the same payer. Nakanishi and Sugiyama [29] proposed a divisible electronic cash system that provided unlinkability. In this system, no one except the payer and the trusted third party can determine whether two payments are made by the same customer, unless the payments cause over-spending, however, this system uses 'cut-and-choose' method, thus the efficiency of this system is affected to some extent.

3.5 Micro-payment

Micro-payment systems have received growing attention recently, mainly due to the fact that these schemes exhibit the potential of being embed-

ded in numerous Internet based applications. As a special type of electronic payments, micro-payment systems allow a customer to transfer to a shop or service provider a sequence of small amount payments over the computer network in exchange for goods or services, such as web browsing, where payment can be automatically achieved upon mouse click of a link of certain web sites.

3.5.1 Hash Function

Hash function is one of the most frequently used cryptographic techniques for micro-payment.

The basic operation of hash functions [31] is to map an element of larger domains to an element of smaller domains. This property is conventionally utilized in many non-cryptographic computer applications like storage allocation to improve performance. For cryptographic applications, hash functions have more important aspects, which make them playing a fundamental role in modern cryptography.

The purpose of hash functions is to provide data integrity and message authentication. For these usage, hash functions $H(\cdot)$ should satisfy the following requirements:

- **Compression.** Given an input x of arbitrary m-bit length, $H(x)$ maps to an output y of fixed bit length of n, where $m > n$.

- **One-wayness.** If $y = H(x)$ is given, it is hard to compute x.
- **Collision-freeness.** It is hard to find a pair (x, x_0) satisfying $H(x) = H(x_0)$, where $x \neq x_0$.
- **Efficiency.** Given an input x, $H(x)$ is easy to compute.

3.5.2 Hash Chain

A hash chain [32] is a variant of hash functions. It is a list of values that is constructed by recursively applying a one-way hash function to a secret random value. It has recently been widely employed to develop many practical cryptographic solutions, such as authentication [33], auction [34], as well as micro-payment [32].

The generation of hash chain is done as follows:

$$\text{Seed} : c_0$$

$$\text{1st round} : c_1 = H(c_0)$$

$$\text{2nd round} : c_2 = H(c_1) = H(H(c_0))$$

$$\ldots$$

$$\text{n-th round} : c_n = H(H^{n-1}(c_0))$$

Here c_0 is the root value of the hash chain. Because of one-wayness of hash functions, for $i = n-1, n-2, \ldots, 1$, by knowing c_i, c_{i-1} cannot be computed by those who do not know the secret random value. Therefore, if a customer knows c_{i-1} regarding c_i, which is from the same hash chain,

he/she must be the one who created the hash chain. For example, the i-th payment (for $i = 1, 2, \ldots, n$) consists of the pair (w_i, i), which can be verified using w_{i-1}, which is obtained from the $(i-1)$-th payment.

3.5.3 Micro-payment Schemes based on Hash Chain

In our view, the costs of micro-payment, such as computation costs, communication costs and key management costs, should be kept as low as possible in order for the service providers to make profit from the low value transactions. In literature, most of the micro-payment schemes share the same structure with the one-way hash chain described above. The PayWord scheme [32] is an example of micro-payment which is based on a simple one-way hash chain.

There are also attempts to develop a more efficient structure which is different from a simple one-way hash chain. PayTree [35] and UOBT (unbalanced one-way binary tree) [36] are two of those good attempts. The major difference between UOBT and PayTree is that UOBT achieves shop specific micro-payments in similar way as the conventional one-way hash chain structure. In a scheme based on UOBT, a secret random value is chosen as the root. This secret value is used to construct a tree from the root towards the lower levels in an unbalanced binary tree, such that given a child node, no parent node can be derived from the child

node.

3.6 Summary of Electronic Cash

This chapter provides an overview of the important techniques of electronic cash, discussed the various types of electronic cash, and reviewed several electronic cash schemes against some potential attacks.

As we know, in the research of electronic cash, there are issues that are yet to be satisfactorily solved, such as fair traceability, double-spending prevention of off-line schemes and simplification of the electronic cash model. Therefore, the next two chapters are focused on the design of new electronic cash systems that address these open problems.

Chapter 4

Fair Traceable Electronic Cash in Wallet with Observers: *O-Cash*

4.1 Introduction

In this chapter, I propose the scheme *O-Cash* to address the open problems of fair traceability and double spending prevention.

4.1.1 Fair Traceability

Recently, many researches have been conducted in the area of fair traceability [37, 25, 38, 39], where illegal tracing (without the permission from

the judge or the customer) is inhibited, wile legal tracing (with the permission from the judge or the customer) is allowed.

Types of Fair Tracing

Since the introduction of fair traceable electronic cash schemes [38, 37], there have been three kinds of electronic cash fair tracing mechanisms used in different scenarios:

- **Coin tracing:** The bank embeds a special piece of information into the withdrawn coins of a blackmailed or suspicious customer in the withdrawal phase, so that the bank will recognize these electronic coins when they are deposited. This type of tracing can be used in the case of blackmailing and bank robbery. In the blackmailing scenario, the blackmailed customer is forced to withdraw electronic coins for the criminal, the customer wants coin tracing to take place, so he/she could secretly inform the bank or trusted third party to apply coin tracing, so that these coins can be recognized when they are spent. In the bank-robbery scenario, the criminal forces the bank to withdraw coins for him/her. Although the robber doesn't want coin tracing to take place, the bank could just apply coin tracing secretly and catch the suspicious customer when he/she spends these electronic coins.

- **Owner tracing:** The electronic coins deposited by a suspicious person are deanonymized so that the identity of their withdrawer is revealed. This type of tracing is applied in the deposit phase, and can for instance be used in the investigation of money laundry.

- **Self-deanonymization:** Pfitzmann and Sadeghi [40] proposed another important approach of fair tracing – self-deanonymization mechanism. In this proposal, instead of the trusted third party, it is rather the customer who executes the revealing of the required information to trace the electronic coins without compromising any of his/her secret key. This feature is very important in the scenario of kidnapping, since in the case of kidnapping, the criminal has physical control over the customer so that the customer has no means to inform the trusted third party to apply fair tracing. Therefore, self-deanonymization provides mechanisms to cope with this scenario.

Brickell, Gemmell and Kravitz [38] developed a trustee-based electronic cash scheme that can be used to prevent 'perfect crimes'[5]. Only with the cooperation of several publicly appointed trusted third parties, the authority can trace a customer's spending history, determining the amount and the payee of the payment transaction. Meanwhile, Stadler, Piveteau and Camenisch [37] (as shown in figure 4.1) invented fair blind

signature schemes that can be used to prevent money laundering. In this scheme, a new type of blind signature called fair blind signature was proposed. Such schemes have the additional property that a trusted third party can deliver information, allowing the signer to link his/her blind signature to the signed message, that is, the signer is able to recognize his/her blind signature with the information provided by the trusted third party.

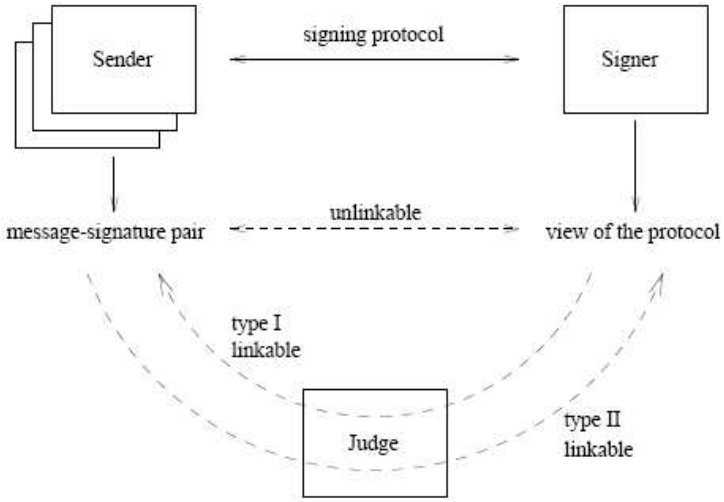

Figure 4.1: Fair Blind Signatures with Trusted Third Party

To date, most of the fair traceable electronic cash systems [38, 39, 37] rely on trusted third parties.

Methods of Fair Tracing

To date, there have been two kinds of fair tracing methods, that is, trusted third party approach [37] and auditable tracing approach [23]. A

comparison of these two approaches is listed in table 4.1.

Comparison Items	**Trusted Third Party (TTP) Approach**	**Auditable Tracing Approach**
Prevention of Illegal Tracing	Always prevents illegal tracing if TTP does not misbehave	Cannot prevent illegal tracing; detect illegal tracing after the fact
Additional Cost	Cost for TTP	Cost of the additional audit phase
Customers' Participation	When crimes take place, the customer can initiate tracing	In the audit phase, the customer has to check whether he/she has been illegally traced.
Coins' Life Cycle	Permanent	Each generation of electronic coins has an audit phase, after which the unspent coins of this generation will be invalid
Efficiency	Additional computation only for the fair traced coins	Additional computation for all the electronic coins

Table 4.1: Comparison Between TTP Approach and Auditable Tracing Approach

4.1.2 Double-spending Prevention

In the research of electronic cash, prevention of double-spending is a very important area. To date, there have been three methods to achieve this:

1. **Prevention-before-the-fact** of online electronic cash schemes (for instance, [2]): the bank checks each electronic coin with an online central database during each payment transaction, in order to verify whether the electronic coin has been spent before.

2. **Detection-after-the-fact** of off-line electronic cash schemes (for instance, [16]): when the customer wants to spend the electronic coin which is blindly signed by the bank, he/she has to answer a random numeric challenge about each electronic coin to be spent. If two or more responses regarding the same electronic coin are given by the customer, the bank will be able to detect the identity of the double-spender eventually.

3. **Prior restraint of double-spending** using tamper-resistant hardware, such as a smart card chip (for instance, [15]): the chip keeps a list of all electronic coins. If someone attempts to copy the already spent electronic coins and try to spend them again, the chip will detect this attempt and will not allow the transaction.

In literature, most of the known off-line electronic cash schemes only use method 2 to gain their security [41, 25, 42, 4]. However, in off-line electronic cash schemes, prior restraint of double-spending is as important as detection of double-spenders after the fact. Therefore, instead of just using method 3, I utilize both method 2 and method 3 to gain enhanced security for *O-Cash*, via wallet with observers.

Wallet with Observers

In [22], Chaum proposed the idea of wallet databases with observers, which involve stationing a tamper-resistant device in the customer's electronic wallet. This scheme offers prior restraint of double-spending by disabling an electronic coin once it is spent. Later, Cramer and Pedersen [43] defined additional requirements in such a way that the customer's privacy is unconditionally protected even if the observer is later analyzed by others.

Brands proposed a very efficient electronic cash scheme with observers [44]. Unlike most off-line electronic cash schemes, where the customer alone can create a valid response to a challenge from the shop, Brands' scheme requires the cooperation of the customer and the observer in order to create a valid response to a challenge during a payment transaction. In this way, the spending of electronic coins can be controlled by the observer.

In *Financial Cryptography*, a fair off-line electronic cash system with extensions to wallet with observers was proposed [45]. However, this scheme is not able to provide self-deanonymization, which is very important in the scenario of kidnapping.

4.2 Building Blocks

In this section, the basic building block of the proposed scheme *O-Cash* is given. This building block is derived from zero-knowledge proofs of a piece of information, and is denoted by 'ZKP' for short.

4.2.1 Zero-Knowledge Proof of Equality of Discrete Logarithms

In [22], Chaum and Pedersen proposed the zero-knowledge proof of equality of discrete logarithms, which is the building block for many electronic cash schemes, including the proposed *O-Cash* in this chapter. Therefore, I will discuss this proof as follows:

In the zero-knowledge proof, let $g_1, g_2 \in_R G_q$ be generators of order q, $y_1 = g_1^a$, $y_2 = g_2^a$. The prover and the verifier performs the zero-knowledge proof

$$ZKP\{(a) : y_1 = g_1^a \ \wedge \ y_2 = g_2^a\}$$

which proves that the prover knows the discrete logarithm of y_1 to the base g_1 and the discrete logarithm of y_2 to the base g_2 and they are equal.

The prover and the verifier perform the following zero-knowledge proof:

Prover		Verifier
$r \in_R Z_q$		
$w_1 = g_1^r$		
$w_2 = g_2^r$		
	$\xrightarrow{w_1, w_2}$	
		$u \in_R Z_q$
	$\xleftarrow{u}$	
$s = r - ua \bmod q$		
	$\xrightarrow{s}$	
		Check
		$w_1 \stackrel{?}{=} y_1^u g_1^s$
		$w_2 \stackrel{?}{=} y_2^u g_2^s$

1. The prover randomly chooses $r \in Z_q$, and computes two numbers w_1 and w_2 as $w_1 = g_1^r$ and $w_2 = g_2^r$.

2. The prover sends w_1 and w_2 to the verifier.

3. The verifier randomly chooses $u \in Z_q$, and sends u to the prover.

4. After computing $s = r - ua \bmod q$, the prover sends s to the verifier.

5. The verifier will check the following two equations: $w_1 \stackrel{?}{=} y_1^u g_1^s$ and $w_2 \stackrel{?}{=} y_2^u g_2^s$. If these two equations hold, then the verifier will know that the prover knows the discrete logarithm of y_1 to the base g_1

and the discrete logarithm of y_2 to the base g_2 and they are equal, but the verifier will not know the exact value of the the discrete logarithm.

4.3 Protocols of *O-Cash*

There are four entities in the *O-Cash* model:

- The *bank* maintains the customer accounts, issues observers and helps the customers to withdraw electronic cash.
- The *customer* has to embed the bank-issued observer into his/her trusted computing device in order to make electronic cash payments. The observer and the computing device together form an *electronic wallet*.
- The *electronic wallet* consists of a tamper-resistant observer [22], such as smart card chip that the customer cannot modify, and a software-only computing device, trusted by the customer. The computing device can be a PDA for making payment at the point of sale (POS) or a computer for making payment online. The customer has full control over his/her computing device, but has no internal access to the observer. All information that inflows or outflows the observer must pass through the computing device, allowing the

customer to ensure that there is no unauthorized communication between the observer and other parties. Meanwhile, the computing device cannot complete a transaction without the cooperation of the observer. This gives the observer the power to prevent the customer from making payments that it does not allow, such as spending the same electronic coin more than once. Note that, even if the tamper-resistant protection is unexpectedly defeated somehow, this scheme can still provide cryptographic security to detect and identify the double-spenders, through blind signatures.

- The *shop* verifies the payment from the customer and deposit the collected electronic coins to the bank.

Utilizing the techniques of wallet with observers [44] and fair tracing through trusted third party [42], the proposed fair traceable electronic cash scheme in wallet with observers is as follows:

4.3.1 Setup

The Parameters of the Bank. The bank chooses two one-way hash functions $H(\cdot)$ and $H_0(\cdot)$. $H(\cdot)$ is used for the construction and verification of the digital signatures of the bank, while $H_0(\cdot)$ is used by the shop to compute challenges in the payment protocol. Then the bank defines G_q, which is a subgroup of order q in Z_p^*, where p and q are two large prime

numbers such that $q|p-1$. The bank also publishes (g, g_1, g_2, g_3), which are generators selected from G_q. Let $x \in Z_q^*$ be the secret key of the bank and the corresponding public key of the bank is $h = g^x \bmod p$.

The Parameters of the Trusted Third Party. The secret key of the trusted third party is τ and the public key of the trusted third party is $(h_{T_1} = g_1^\tau \bmod p,\ h_{T_2} = g_2^\tau \bmod p)$.

4.3.2 Account Opening

To open an account, the customer first selects a secret number $u_1 \in Z_q$ at random, and computes $g_1^{u_1} \bmod p$. Then, the customer sends $g_1^{u_1} \bmod p$ to the bank as his/her identity information and keeps u_1 as the secret identity code, which is unknown to the bank unless the customer double-spends the same electronic coin.

The bank provides the customer with an observer, embedded in its memory a randomly chosen number $\alpha_1 \in Z_q^*$, which is encrypted and kept unknown to the customer. The bank computes $A_\alpha = g_1^{\alpha_1} \bmod p$, $I = A_\alpha g_1^{u_1} \bmod p$ and $z = (Ig_2)^x \bmod p$, then it transmits A_α and z to the customer, who will store these numbers in his/her electronic wallet.

4.3.3 Withdrawal Protocol

When a customer wants to withdraw an electronic coin, he/she first identifies himself/herself to the bank, and the following withdrawal protocol is performed:

Observer		Customer		Bank
	$\xrightarrow{h_{T_1}^{\alpha_1}}$			
		$s \in_R Z_q^*$		
		$E = h_{T_1}^{\alpha_1 s} h_{T_1}^{u_1 s} h_{T_2}^{s}$		
		$D = I g_2 g_3^{s^{-1}}$		
			$\xrightarrow{D,E}$	
		$T = D^s$		
				$w \in_R Z_q$
				$a = g^w$
				$b = (I g_2)^w$
$\alpha_2 \in_R Z_q$				
$B_\alpha = g_1^{\alpha_2}$				
	$\xrightarrow{B_\alpha}$			
			$\xleftarrow{a,b}$	
		$x_1, x_2, e \in_R Z_q$		
		$A = (I g_2)^s$		
		$z' = z^s$		

$$B_1 = g_1^{x_1} A_\alpha^{se} B_\alpha$$

$$B_2 = g_2^{x_2}$$

$$u, v \in_R Z_q$$

$$a' = a^u g^v$$

$$b' = b^{su} A^v$$

$$c' = H(A, B_1, B_2, z', a', b')$$

$$c = c'/u \bmod q$$

$$\xrightarrow{c}$$

$$r = cx + w \bmod q$$

$$\xleftarrow{r}$$

$$g^r \stackrel{?}{=} h^c a$$

$$(Ig_2)^r \stackrel{?}{=} z^c b$$

$$r' = ru + v \bmod q$$

1. The observer in the customer's electronic wallet computes $h_{T_1}^{\alpha_1}$ and sends this value to the customer. The customer chooses a random number $s \in Z_q^*$ and computes $D = Ig_2 g_3^{s^{-1}}$ and $E = h_{T_1}^{\alpha_1 s} h_{T_1}^{u_1 s} h_{T_2}^{s}$, then the customer sends D and E to the bank.

2. The customer computes $T = D^s$, which will be used for verification and self-deanonymization later.

3. The observer generates a random number $\alpha_2 \in Z_q$, and sends the number $B_\alpha = g_1^{\alpha_2}$ to the customer. Meanwhile, the bank generates

a random number $w \in Z_q$, and sends $a = g^w$, $b = (Ig_2)^w$ to the customer.

4. The customer generates three random numbers $x_1, x_2, e \in Z_q$, and computes $A = (Ig_2)^s$, $z' = z^s$, $B_1 = g_1^{x_1} A_\alpha^{se} B_\alpha$ and $B_2 = g_2^{x_2}$. In addition, he/she randomly generates two secret numbers $u, v \in Z_q$, and computes $a' = a^u g^v$ and $b' = b^{su} A^v$. After the computation of $c' = H(A, B_1, B_2, z', a', b')$, the customer sends the challenge $c = c'/u \bmod q$ to the bank.

5. The bank sends back the response $r = cx + w \bmod q$ to the customer, and deducts the value of the withdrawn electronic coin from the customer's bank account.

6. The customer checks the equations $g^r = h^c a \bmod p$ and $(Ig_2)^r = z^c b \bmod p$. If the equations hold, then the customer computes $r' = ru + v \bmod q$.

At the end of the withdrawal protocol, the customer obtains the electronic coin in the form of $(A, B_1, B_2, z', a', b', r', T)$, and keep the secret information (u_1, s, x_1, x_2) for the payment phase of the electronic coin.

Proposition 1. *If the customer and the bank follow the withdrawal protocol correctly, then the following two equations hold:* $g^{r'} = h^{H(A,B_1,B_2,z',a',b')} a'$ *and* $A^{r'} = z'^{H(A,B_1,B_2,z',a',b')} b'$, *which are used in the payment protocol to*

verify the validity of the electronic coin.

Proof.

The first equation follows from

$$\begin{aligned} g^{r'} &= g^{ru+v} \\ &= g^{cxu+wu+v} \\ &= h^{c'}a^{u}g^{v} \\ &= h^{H(A,B_1,B_2,z',a',b')}a' \end{aligned}$$

and the second from

$$\begin{aligned} A^{r'} &= (Ig_2)^{sr'} \\ &= (Ig_2)^{s(ru+v)} \\ &= (Ig_2)^{s(cxu++wu+v)} \\ &= z'^{cu}(Ig_2)^{suw+vs} \\ &= z'^{H(A,B_1,B_2,z',a',b')}b' \end{aligned}$$

4.3.4 Payment Protocol

When the customer wants to make a payment at the shop, the following protocol is performed:

Observer	Customer	Shop
		$\xrightarrow{A,B_1,B_2}$
		$A \neq 1$
		$d = H_0(A, B_1, B_2, I_s, date/time)$
		$\xleftarrow{d}$
	$d' = s(d + e) \bmod q$	
	$\xleftarrow{d}$	
α_2 still in memory?		
$r_\alpha = d'\alpha_1 + \alpha_2 \bmod q$		
	$\xrightarrow{r_\alpha}$	
		$g_1^{r_\alpha} \stackrel{?}{=} A_\alpha^{d'} B_\alpha$
		$\rho \in_R Z_q$
		$r_1 = r_\alpha + d(u_1 s) + x_1 \bmod q$
		$r_2 = ds + x_2 \bmod q$
		$D_1 = A_\alpha g_1^{u_1} h_{T_1}^{\rho}$
		$D_2 = g_1^{\rho}$
		$a_1 = I^s = A_\alpha^s g_1^{u_1 s}$
		$a_2 = g_2^s$
		$\xrightarrow{r_1,r_2,a_1,a_2,D_1,D_2,(A,B_1,B_2,z',a',b',r',T)}$
		Check
		$g^{r'} \stackrel{?}{=} h^c a'$

$$A^{r'} \stackrel{?}{=} z'^{c} b'$$

$$g_1^{r_1} \stackrel{?}{=} a_1^d B_1$$

$$g_2^{r_2} \stackrel{?}{=} a_2^d B_2$$

$$g_1^{r_1} g_2^{r_2} \stackrel{?}{=} A^d B_1 B_2$$

$$T \stackrel{?}{=} a_1 a_2 g_3$$

$$Customer \Rightarrow Shop : ZKP\{(\rho) : D_1 = A_\alpha g_1^{u_1} h_{T_1}^{\rho} \parallel D_2 = g_1^{\rho}\}$$

1. The customer sends A, B_1, B_2 to the shop.

2. If $A \neq 1$, the shop computes $d = H_0(A, B_1, B_2, I_s, date/time)$, where I_s is the unique identity number of the shop. Then, the shop sends the challenge to the customer.

3. The customer computes $d' = s(d + e) \bmod q$ and sends it to the observer.

4. If α_2 is still in memory, then the observer computes the response $r_\alpha = d'\alpha_1 + \alpha_2 \bmod q$ and sends it to the customer. (If α_2 has already been erased, then the observer knows that the customer is trying to double-spend the current electronic coin, so the observer locks up.) Then the observer erases α_2 from its memory.

5. The customer verifies the equation $g_1^{r_\alpha} = A_\alpha^{d'} B_\alpha$. If it holds, he/she randomly chooses a number $\rho \in Z_q$, and computes the following: $r_1 = r_\alpha + d(u_1 s) + x_1 \bmod q$, $r_2 = ds + x_2 \bmod q$, $D_1 = A_\alpha g_1^{u_1} h_{T_1}^{\rho}$,

$D_2 = g_1^{\rho}$, $a_1 = I^s = A_{\alpha}^s g_1^{u_1 s}$ and $a_2 = g_2^s$. Then the customer sends the above computed numbers and the electronic coin in the form of $(A, B_1, B_2, z', a', b', r', T)$ to the shop for verification.

6. The shop checks the following equations: $g^{r'} = h^c a'$, $A^{r'} = z'^c b'$, $g_1^{r_1} = a_1^d B_1$, $g_2^{r_2} = a_2^d B_2$, $g_1^{r_1} g_2^{r_2} = A^d B_1 B_2$ and $T = a_1 a_2 g_3$.

7. The customer needs to prove to the shop that he/she knows the representation of $D_1 = A_{\alpha} g_1^{u_1} h_{T_1}^{\rho}$ and $D_2 = g_1^{\rho}$, and that they are correctly computed using zero-knowledge proof.

8. If the above stated verifications hold, the shop accepts the electronic coin as a valid payment.

4.3.5 Deposit Protocol

At any suitable time, the shop sends the payment transcripts of collected electronic coins to the bank. The bank verifies the transcript, and accepts the coin if everything is done correctly.

4.3.6 Fair Tracing

In *O-Cash*, the fair tracing mechanism is built in to prevent the following crimes.

Scenario 1 – Blackmailing: In this scenario, the blackmailer contacts the victim customer anonymously and threatens him/her to withdraw

electronic coins that are chosen and blinded by the blackmailer. The blackmailer can only communicates with the victim, but cannot observe the victim customer's communication with the bank. Therefore, when the victim customer withdraws the electronic coin, he/she wants to secretly add a mark to the coins, so that the blackmailer will be caught when he/she spends the marked electronic coins.

Solution of Scenario 1 – Coin tracing can help the victim customer to achieve his/her objectives. It is initialized by the customer via adding a mark to the coin, but executed by the bank via remailing the mark to the shop. In the withdrawal phase, the bank gives the trusted third party the value, then the trusted third party computes

$$E^{1/\tau} g_3 = (h_{T_1}^{\alpha_1 s} h_{T_1}^{u_1 s} h_{T_2}^{s})^{1/\tau} g_3 = g_1^{\alpha_1 s u_1 s} g_2^{s} g_3 = a_1 a_2 g_3 = T$$

This value can be put on a blacklist and will be recognized when the electronic coin is spent.

Scenario 2 – Kidnapping: The kidnapper has physical control over the kidnapped victim customer, therefore, the victim customer has no means to inform the bank or the trusted third party to execute the fair tracing. In order to protect his/her interests in this scenario, the victim customer has to initiate and execute fair tracing all by himself/herself.

Solution of Scenario 2 – Self Deanonymization is embedded to achieve this objective. It is the customer who executes the revealing of the required information to trace the electronic coins. In order to make this happen, in the withdrawal protocol, the customer sends the bank $T = D^s$, which is part of the payment view of the electronic coin. In this way, the bank can link the identity of the withdrawer with the electronic coin which has the parameter T. In this way, the victim customer can distinguish these coins, so that the kidnapper will be caught when spending these coins.

Scenario 3 – Money Laundry: In this scenario, the suspicious spender tries to make use of the dirty money obtained illegally. By linking the payment view and withdrawal view of the electronic coins, the authority can find clues and proof to investigate the illegal spender. In this scenario, the legitime customer does not want his/her withdrawn electronic coins to be misused when falling into the wrong hands, therefore the customer will add the correct mark to his/her withdrawn coins, in order to facilitate owner tracing. However, compared with coin tracing, owner tracing is not helpful in preventing many types of fraud [46], because the discriminators are based on the purchase rather than anything directly related to the coin.

Solution of Scenario 3 – Owner tracing is achieved as follows.

Given the value D_1 and D_2 gathered in the payment phase, the trusted third party computes

$$D_1/D_2^{\tau} = A_{\alpha} g_1^{u_1} h_{T_1}^{\rho} / g_1^{\tau\rho} = A_{\alpha} g_1^{u_1} = I$$

This reveals the identity of the coin owner.

4.4 Security Analysis

4.4.1 Anonymity

Under the discrete logarithm assumption (details are described in Appendix C.2) , if the customer does not double-spend an electronic coin, it is computationally infeasible for the bank to compute u_1, which is the secret identity code of the customer. In addition, the bank cannot make use of the tracing mechanism without the help of the trusted third party. This is because the bank cannot compute the discrete logarithms $log_{g_1} h_{T_1}$ and $log_{g_2} h_{T_2}$.

4.4.2 Unforgeability

Because only the bank knows the secret key x. Under the discrete logarithm assumption, it is computationally infeasible to forge the blind signature of the bank using adaptive chosen-message attack (details are

described in Appendix C.4). Therefore, no one other than the bank can mint valid electronic coins.

4.4.3 Prior restraint of double-spending

If the tamper-resistance of the observer is not broken, the customer is not able to double-spend an electronic coin, because the observer has to participate in the withdrawal and payment protocols. The customer does not know $\log_{g_1} A_\alpha$ and $\log_{g_1} I$, but the scheme need to perform Schnorr identification protocol, proving these knowledge, which is only known to the observer. Therefore, without the observer's cooperation, the customer cannot make any payment. In addition, α_2 is a one-time parameter, and this mechanism ensures that each coin can be spent only once.

4.4.4 Detection of double-spending

In case the tamper-resistance of the observer is broken by an attacker, the proposed scheme can still detect the identity of the double-spender. If an electronic coin is spent twice, the customer has to response two different challenges from the shop, therefore, the bank get two response pairs (r_1, r_2) and (r_1', r_2'). By computing $(r_1 - r_1')/(r_2 - r_2')$ the bank can

get the customer's secret information u_1 as follows:

$$\frac{r_1 - r_1'}{r_2 - r_2'} = \frac{(r_\alpha + d(u_1 s) + x_1) - (r_\alpha + d'(u_1 s) + x_1)}{ds + x_2 - d's + x_2} = \frac{(d - d')(u_1 s)}{(d - d')s} = u_1.$$

Then, the bank can know the identity of the double-spender by searching the identity code in the bank's account databases.

4.5 Summary of *O-Cash*

In this chapter, I propose *O-Cash*, an electronic cash scheme in wallet with observers that provides coin tracing and owner tracing as well as self-deanonymization. This scheme addressed the areas of double-spending prevention and fair traceability. In the next chapter, I focus on the discussion of a new model of fair electronic cash and its applications, which addresses the area of model simplification.

Chapter 5

A New Fair Traceable Electronic Cash Model Based On Separable Group Signature: *SignCash*

5.1 Introduction

In this chapter, I propose the scheme *SignCash* to address the open problems of model simplification via separable group signature.

5.1.1 Group Signature

Group signatures were introduced by Chaum and Heijst [47] in 1991. This type of digital signatures allows the registered group members to produce digital signatures on behalf of the whole group; anyone can verify the digital signatures but he/she does not know the identity of the signer. The group manager has some secret information, which can be used to discover the identity of the signer. Group digital signatures can be used in many applications. For example, a CEO of a company wants some individual employees to validate price lists, press releases, or digital contracts on behalf of the entire company. In this scenario, the CEO can set up a group signature scheme, and act as the group manager. Then the designated employees can act as group members to sign various documents on behalf of the entire company. By using this approach, the company will conceal its internal structure, and the verifiers would only have to know the company's public key to verify the signatures on the documents. Moreover, only the CEO, who is the group manager, can determine which employee has signed which document.

The definition and properties of group signatures are as follows:

Definition: Group signature schemes are digital signature schemes consisted of the following four procedures:

- *Setup:* A protocol between the designated group manager and the

group members. The output of this step is a membership certificate and a secret key for each group member, the group public key and the secret key of the group manager. New members can join the group without affecting the group public key.

- *Sign*: A signature generation algorithm that on input a group public key, a membership certificate, a membership secret and a message m, outputs the group signature m_s of m.

- *Verify:* An algorithm that takes as input the group public key, the signature m_s, the message m, and outputs *true* or *false* to indicate the correctness of the group signature.

- *Open:* An algorithm that takes as input the message m, the signature m_s, the group manager's secret key, and returns the identity of the signer.

A secure group signature must fulfill the following security requirements:

- *Correctness:* Signatures correctly produced by a group member using the signature generation algorithm must be accepted by the verification algorithm.

- *Conditional Anonymity:* Anyone can easily check that a signature was produced by certain group member of the group, but only the group manager can determine which member has produced the

signature. That is, given a valid signature, it is hard to find the identity of the signer without knowing the group manager's secret key.

- *Unforgeability:* Only the group members are able to generate signatures on behalf of the group, that is, only group members can issue signatures that are verifiable by the group public key.

- *Non-framing:* No one, even the group manager and group members collude, is able to generate signatures on behalf of other group members.

- *Exculpability:* Since framing is not possible for group signatures, the group member cannot repudiate his/her signatures later on. The group manager can always determine the identity of the group member who has issued a group signature. In addition, the group manager can also prove this without compromising that particular group member's anonymity in previous or future messages he/she may sign.

- *Unlinkability:* Deciding whether two different valid signatures were generated by the same group member is hard for anyone except the group manager. This unlinkability feature makes group signatures attractive for electronic cash applications.

5.1.2 Group Signature Applications in Electronic Cash Systems

In literature, there have been several proposals of electronic cash systems based on group signature schemes [48, 49, 4, 50]

Traore [50] proposed the first privacy-protecting off-line electronic cash scheme based on group signatures. Later, Qiu, Chen and Gu [4] designed another system that combines a group signature scheme and a blind signature scheme. However, Canard and Traore [48] and Choi, Zhang and Kim [49] suggested that Qiu's system does not provide anonymity, which is an important and basic requirement for the design of electronic cash schemes. Recently, Canard and Traore proposed another group signature based electronic cash schemes [48], where each coin obtained by the customer is actually a membership certificate issued by the bank.

However, all previously proposed electronic cash schemes have a relatively complicated process of withdrawal phase between the customer and the bank. As the customer and the bank have to generate each electronic coin to be used, this withdrawal phase is tedious for the customers, who may like to eliminate this phase if possible.

5.2 Separable Group Signature Applications in *SignCash*

The concept of 'separability' was introduced in [51] to overcome the security problems caused by dependency between keys of different parties. In the light of this concept, Camenisch and Michels proposed the separable group signature schemes [52]. In this model, there are two independent group managers: the membership manager is responsible for key generation and group member registration; while the revocation manager can reveal the identity of a group signature's originator.

5.2.1 Entities in *SignCash*

There are four entities in *SignCash* representing different roles of the group signature schemes:

- The *bank* is the group membership manager, which maintains the accounts of all customers and registers new customers.
- The *customer*, which is the group member, can make payment by signing the transaction message using his/her private membership key and certificate.
- The *shop* can verify the generated electronic coins in the form of group signatures using the group public key published by the bank.

- The *clearing house*, which serves as the group revocation manager, clears the payment transactions between the shop and the customer.

5.2.2 Simplified Transaction Model in *SignCash*

The above mentioned four entities represent different roles in *SignCash* model. In order to achieve electronic cash payment and deposit, different transactions are executed among these roles:

- **Account Opening Transaction.** The bank is the financial organization issuing valid electronic payment instruments. It registers new *SignCash* customers and maintains the accounts of all customers. After the account opening transaction, the bank will update its customer database with the customer's identity information and the account number, while the customer will obtain a valid membership certificate and a secret key. In addition, the customer will get the license and password to install and activate *electronic wallet* on his/her computer, mobile phone or PDA etc.

- **Payment Transaction.** During the payment transaction, the shop prepares the payment message for the customer to sign. This payment message contains all the transaction information, such as date, time, shop ID, currency and amount of the payment. With

electronic wallet, the customer can make payment by signing the transaction message using his/her private key. With the group public key published by the bank, the shop can check the validity of the customer's payment signature. Since only registered customer can generate electronic coins with his/her own private key and cannot repudiate the signed electronic coins later, therefore, if the signature is verified as correct, the shop can be assured that it will be accredited after this payment transaction is cleared in the deposit phase. In addition, because of the security requirements of group signature schemes, the customer can be assured that no one will be able to forge a new valid signature in his/her name.

- **Deposit Transaction.** The shop deposits the collected electronic coins periodically to the clearing house. The clearing house, which serves as the group revocation manager, verifies the validity of the deposited electronic coins, and sends the bank periodic summaries of settlement of each account based on the monetary value stated by the deposited electronic coins. For auditing and security purposes, the clearing house is required to keep all the records of transactions and settlement for a certain period of time. If the customers or the shops found any discrepancy between the bank statement and the actual payment or deposit, they can request the clearing house to

prove the correctness of the settlement reports based on the signed payment message.

- **Tracing Transaction.** The bank knows the linkage between the account number and the customer identity, and the clearing house knows the linkage between the account number and the payment history, therefore, if and only if a tracing order is issued from the judge, the clearing house can cooperate with the bank to execute fair tracing. Without judge's permission, the collusion between the bank and the clearing house to trace any payment will be considered as illegal and will be prosecuted.

Unlike traditional electronic cash schemes which usually include a complicated withdrawal phase, the proposed new electronic cash model *SignCash* enables the customer to generate electronic coins by themselves. Therefore, withdrawal phase can be eliminated from the simplified new model.

5.3 Building Blocks

In this section, the basic building block of the proposed scheme *SignCash* is given. This building block is derived from zero-knowledge proofs of a piece of information, and is denoted by 'ZKP' for short.

5.3.1 Zero-Knowledge Proof of a Discrete Logarithms in an Interval

In [53], Jan and Markus presented the zero-knowledge proof of a discrete logarithms lies in an Interval.

In this proof, $\varepsilon > 1$ is a security parameter and $l_1 < l_g$ and l_2 denote lengths. A pair $(c, s) \in \{0,1\}^k \times \{-2^{l_2+k}, ..., 2^{\varepsilon(l_2+k)}\}$ satisfying $c = H(g||y||g^{s-c2^{l_1}}y^c||m)$ is a signature of a message $m \in \{0,1\}^*$ with respect to a public key $y \in G$.

Such a signature is the zero-knowledge proof and can be computed as follows in an integer $x \in \{2^{l_1}, ..., 2^{l_1} + 2^{l_2}\}$ is known such as $y = g^x$ holds:

1. Choose $r \in_R \{0,1\}^{\varepsilon(l_2+k)}$, and compute $t = g^r$.
2. $c = H(g||y||t||m)$.
3. $s = r - c(x - 2^{l_1})$ (in Z)

This zero-knowledge proof is denoted as

$$ZKP\{(\alpha) : y = g^\alpha \ \wedge \ (2^{l_1} - 2^{\varepsilon(l_2+k)+1} < \alpha < 2^{l_1} + 2^{\varepsilon(l_2+k)+1})\}(m)$$

5.4 Protocols of *SignCash*

In this section, I will elaborate the protocols of an instance of the application of *SignCash* model, based on the group signatures [53]. The

protocol details are as follows:

5.4.1 Setup

The Parameters of the Bank

First of all, the security parameters l_g, l_0, l_1 and l_2 are set (for example, $l_g = l_0 = 1200$, $l_1 = 860$ and $l_2 = 600$), in order to meet the security requirements of the electronic payment scheme.

Served as the group membership manager, the bank chooses a group $G =< g >$ and two random elements z,$h \in G$ with the same large order (around $2^{l_g/2}$), and publishes g, G, z, h. Then, the bank chooses two large random prime numbers p and q (around $2^{l_g/2}$) of the form $p = 2p' + 1$ and $q = 2q' + 1$ where p' and q' are prime numbers as well. The bank publishes $n = pq$ and keeps p and q secret, then defines a subgroup of Z_n^* and chooses two numbers z, h from this subgroup.

The Parameters of the Clearing House

The secret key of the clearing house is x and the public key of the clearing house is $y = g^x$. Then a collision free one-way hash function $H(\cdot)$ is published.

5.4.2 Account Opening

To open an account, the customer first has to identify himself to the bank by means of official documents like a driving license or passport. The customer uses his/her electronic wallet to choose a random prime numbers $e \in_R \{2^{l_1}, ..., 2^{l_1} + 2^{l_2} - 1\}$ and $e_n \in_R \{2^{l_0-1}, ..., 2^{l_0} - 1\}$, then he/she computes $e_m = ee_n$ and $z_m = z^{e_n}$. The customer commits to e_m and z_m by signing them, and sends e_m and z_m and their commitments to the bank. The bank computes $u = {z_m}^{1/e_m}$ and sends u to the customer, who checks that $z = u^e$. The bank stores (u, e_m, z_m) and the customer's identity in the bank's customer database. The customer will get license to install *electronic wallet*, and keep (u, e) as his/her membership key.

5.4.3 Payment Protocol

When the customer wants to make a payment at the shop, he/she signs the transaction message (including the Shop ID, the amount and currency of the payment etc) using his/her electronic wallet embedded with the secret key, in order to demonstrate that he/she agrees the signed payment to this shop. The shop verifies the newly generated electronic coins in the form of group signature using the public key from the bank, and accepts this payment if the verification is successful. The following payment protocol is performed for the signature generation and verification:

shop Customer

$m = H(ShopID, Date, Time, Amount, Currency)$

$\xrightarrow{m}$

$a = g^w.$

$b = uy^w$

$d = g^e h^w$

$t_1 = b^{r_1}(1/y)^{r_2}$

$t_2 = a^{r_1}(1/g)^{r_2}$

$t_3 = g^{r_3}$

$t_4 = g^{r_1} h^{r_3}$

$c = H(g\|h\|y\|z\|a\|b\|d\|t_1\|t_2\|t_3\|t_4\|m)$

$s_1 = r_1 - c(e - 2^{l_1})$

$s_2 = r_2 - cew$

$s_3 = r_3 - cw$

$\xleftarrow{(c,s_1,s_2,s_3,a,b,d)}$

Check

$c = H(g\|h\|y\|z\|a\|b\|d\|z^c b^{s_1 - c2^{l_1}}/y^{s_2}\|a^{s_1 - c2^{l_1}}/g^{s_2}\|a^c g^{s_3}\ \|d^c g^{s_1 - c2^{l_1}} h^{s_3}\|m)$

Check

$ZKP\{(e, w) : d = g^e h^w \ \wedge \ (2^{l_1} - 2^{\varepsilon(l_2+k)+1} < e < 2^{l_1} + 2^{\varepsilon(l_2+k)+1})\}(m)$

1. The shop first generates a transaction message of payment for the customer to sign: $m = H(ShopID, Date, Time, Amount, Currency)$.

2. The customer chooses an integer w and computes $a = g^w$, $b = uy^w$ and $d = g^e h^w$.

3. Then the customer chooses r_1, r_2 and r_3, and computes $t_1 = b^{r_1}(1/y)^{r_2}$, $t_2 = a^{r_1}(1/g)^{r_2}, t_3 = g^{r_3}$, $t_4 = g^{r_1}h^{r_3}$. After computation of $c = H(g\|h\|y\|z\|a\|b\|d\|t_1\|t_2\|t_3\|t_4\|m)$, the customer also computes $s_1 = r_1 - c(e - 2^{l_1})$, $s_2 = r_2 - cew$ and $s_3 = r_3 - cw$.

4. The generated electronic coin is $(c, s_1, s_2, s_3, a, b, d, z)$, then the customer sends his/her electronic coin to the shop.

5. The shop verifies the signature using the equation

$$c = H(g\|h\|y\|z\|a\|b\|d\|z^c b^{s_1 - c2^{l_1}}/y^{s_2}\|a^{s_1 - c2^{l_1}}/g^{s_2}\|a^c g^{s_3}$$
$$\|d^c g^{s_1 - c2^{l_1}} h^{s_3}\|m).$$

6. The shop also needs to verify that e has sufficient length (at least 2^{l_1} bits). This is achieved by a zero-knowledge proof of a discrete logarithms lies in an interval.

7. The shop accepts the signature on the transaction message as a valid payment signature if the above stated equation holds.

5.4.4 Deposit Protocol

At any suitable time, the shop sends the transcript of each electronic payment to the clearing house. The clearing house verifies the signa-

ture on the transaction message. Then the clearing house computes the identity code $u = b/a^x$, where a and b are from the deposited electronic coins and x is the clearing house's secret key. The clearing house will clear all the payment transactions of each deposited electronic coin, and periodically sends the summarized report to the bank. This report contains the amount to be deducted or credited for each identity code of the customers and ID of the shops. Since the bank knows the relationship between identity code and the customer's real identity, so the bank deducts the correct amount of money from each customer's account and credits the correct amount to each shop.

5.4.5 Fair Tracing

Unlike the previous fair tracing mechanisms (ie. trusted third party tracing and auditable tracing), the fair tracing mechanism of *SignCash* is achieved via the cooperation of the bank and the clearing house. In case crimes take place, the judge will issue a tracing order, then the clearing house and the bank can cooperate to trace the given customer's payment history, because the customers' identities and the payment transaction messages are linked in this situation.

5.5 Security Analysis

5.5.1 Anonymity

Deciding whether an electronic coin originates from a certain customer requires to decide whether $log_g a$ equals to $log_y(b/b')$. However, under the Diffie-Hellman decision assumption [54], it is infeasible. Therefore, it is hard to find out the customer's identity who signed a payment transaction message without the clearing house's secret key.

5.5.2 Unlinkability

To decide whether two coins $(c, s_1, s_2, s_3, a, b, d)$ and $(c', s_1', s_2', s_3', a', b', d')$ are from the same customer requires to decide whether $log_y(a/a') = log_y(b/b') = log_y(d/d')$. However, under the Diffie-Hellman decision assumption, it is computationally hard.

5.5.3 Non-framing

Since it is hard to compute the discrete logarithm of z to the base u, which is only known to the customer, therefore, it is hard to sign in the name of the non-involved customers, even if the bank, the clearing house and some customers collude.

Chapter 6

Comparison and Implementation of O-Cash

6.1 Introduction

In this chapter, I will compare *O-Cash* with the electronic payment systems in practice, namely, Visa Cash and eNETS (details are provided in Appendix D). Then, an overview of the implementation approach, tools and validation is provided.

6.2 Comparison of Visa Cash, eNETS and *O-Cash*

Electronic payment systems may be assessed and compared from the following dimensions: the technical aspect, the economic aspect and the social aspect [55].

6.2.1 Comparison From Technical Aspect

- **Security.** Above all, security is an utmost factor of technical aspect. It means only authorized entity may participate in the payment transactions, in order to prevent malicious misrepresentation, false transactions and fake payment.

- **Privacy.** An ideal electronic payment system should be able to provide both the shop and the costumer with anonymity in payment transactions.

- **Off-line Payment.** The shop is able to verify the validity of the electronic payment without involvement of the bank. This is necessary because payments sometimes have to occur even when there are limitations on the bandwidth of the communication line during the transaction, or no payment network available at all. Off-line verification also significantly reduces the transaction costs of elec-

tronic payment.

Item	Visa Cash	eNETS	O-Cash
Security	Based on the tamper resistance of smart card	Based on PIN verification online	Double Security: smart card with PIN, and secrete key of blind signature for payment transactions
Privacy	Yes: token based payment, where owners of smart card chips can remain anonymous	No: account based payment, where revealing customers' account number is a must	Yes: token based system, where the owner of the wallet and the signer of blind signatures can remain anonymous
Off-line Payment	Yes: smart card reader can verify the payment without connecting to issuing bank	No: customers' account need to be online processed at the central bank for balance maintenance	Yes: shops can off-line verify the customer's blind signature with the bank's public key

Table 6.1: Comparison from Technical Aspect

6.2.2 Comparison From Economic Aspect

- **Transaction Costs.** This refers to the costs incurred by the payer and payee during payment transactions. Transaction costs include not only direct costs, such as online verification, but also indirect costs, such as fixed costs to setup the payment system.

- **User Range.** This refers to the range of the customers who are

able to access the electronic payment systems, without other pre-requisite.

- **Financial Risk.** Customers are generally concerned about the financial risk of the payment systems, for example, in the case of card loss or online transaction security.

Item	**Visa Cash**	**eNETS**	**O-Cash**
Transaction Costs	Transaction costs are low, but there are fixed costs of smart card readers	Transaction costs are high, due to online verification of each transaction with the central bank	Transaction costs are low, but there are fixed costs of e-wallet with observer
User Range	Good: any customer can buy the visa cash cards, even those without bank or credit card account	Good: any customer who have a bank, credit card or eNETS virtual account	Fair: limited to those who have a bank account
Financial Risk	High: Customers cannot get back the loss, if the card is lost or stolen	Fair: Customer are subject to loss if their PIN is stolen by malicious fake web sites or hackers	Low: PIN is required to activate the e-wallet, and secret key is needed to enter locally in their e-wallet

Table 6.2: Comparison from Economic Aspect

6.2.3 Comparison From Social Aspect

In addition to satisfying the needs from both technical and economic aspects, successful electronic payments systems also needs to address the

requirements from social aspects.

- **Crime Resistent.** An ideal should be robust enough to resist crimes or even deter criminal attempts.
- **User Friendliness.** Simplify and ease to use is a important factor when customers choose electronic payment systems.
- **Mobility.** Customers do not always have access to computers and networks, therefore, a good electronic payment system with good mobility should be able to be accessed anywhere.

Item	**Visa Cash**	**eNETS**	**O-Cash**
Crime Resistent	Low: subject to cloning of smart cards	Fair: subject to attacks from hackers on the central bank's servers	Good: Double security from PIN and secret key.
User Friendliness	Good	Good	Fair: Due to more security requirements, there are relatively more steps in order to make a payment
Mobility	Good	Fair: need computer and network access	Good

Table 6.3: Comparison from Social Aspect

6.3 Implementation Aspects of *O-Cash*

In this section, I provide an overview of O-Cash from the implementation aspect.

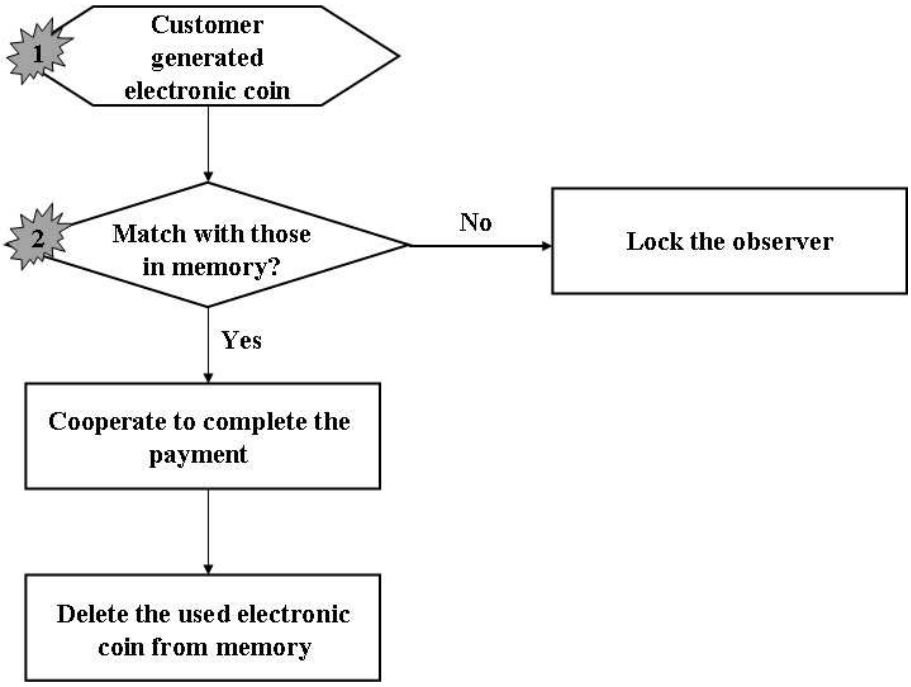

Figure 6.1: Process Flow of O-Cash

Figure 6.1 shows the high level process flow of O-Cash, where two proven techniques are to be built into the O-Cash implementation.

1. A blind signature scheme is utilized to build each electronic cash system since the invention of electronic cash. Therefore, the validity of the blind signature is of critical importance to the implementation validation of electronic cash systems.

2. Electronic wallets with observers provide added security to elec-

tronic cash systems. Smart card technology is proven to be tamper resistent and has been used in stored value cards with increasing popularity.

These two techniques are very important to the validation of O-Cash implementation.

6.3.1 Blind Signature: Implementation Approach and Concept

When it comes to the design and validation of electronic cash systems, it is fundamental to validate the used blind signature scheme, which is the backbone of electronic cash systems.

The following two requirements of blind signatures provides the customers with anonymity, which are the distinguishing feature of electronic cash systems.

- **Blindness**: After the signature generation protocol, the signer has no or only publishable information about the message content, and the resulting signature.

- **Unlinkabilty**: Given some message-signature pairs, the verifiers and the signer are not able to identify whether they are generated by the same signer. Unlinkability is a stronger requirement than anonymity.

Construction and Validation Blind Signature

In the following, a scheme for obtaining Blind Schnorr Signature [56] will be discussed; many electronic cash systems use this scheme as building blocks.

Let G be a finite cyclic group of prime order q with a generator g such that computing discrete logarithms is infeasible. x is the signer's secret key, $y = g^x$ is the signer's public key, and $H(\cdot)$ is a collision-resistant one-way hash function that maps $\{0,1\}^*$ to Z_q.

Requester		Signer
		$r \in_R Z_q^*$
		$t' = g^r$
	$\xleftarrow{t'}$	
$\alpha, \beta \in_R Z_q$		
$t = t' g^\alpha y^\beta$		
$c = H(m \Vert t)$		
$c' = c - \beta \bmod q$		
	$\xrightarrow{c'}$	
		$s' = r - c'x \bmod n$
	$\xleftarrow{s'}$	
$s = s' + \alpha \bmod q$		

$$c \stackrel{?}{=} H(m \| g^s y^c)$$

At the end of the blind Schnorr signature scheme, the requester will have (c, s) as the blind signature on m. The following verification holds:

$$H(m \| g^s y^c) = H(m \| g^{s'+\alpha} y^{c'+\beta}) = H(m \| g^{r-c'x+\alpha+c'x} y^{\beta}) = H(m \| t' g^{\alpha} y^{\beta}) = c$$

Because the signer does not know the message m and the signature (c, s), he/she cannot recognize either the signed message or the signature later, so 'blindness' is achieved in this way.

To validate the blind Schnorr signature scheme, we will need to check the two requirements as described before, namely, blindness and unlinkability [56].

6.3.2 E-wallet with Observers: Implementation Tools and Infrastructure

The *E-wallet with Observers* [22] consists of two parts:

1. A bank issued tamper-resistant observer, such as smart card chip that the customer cannot modify.

2. A software-only computing device, trusted by the customer. The computing device can be a PDA for making payment at the point of sale (POS) or a computer for making payment online.

The observer and the computing device together form an electronic wallet. The customer has full control over his/her computing device, but has no internal access to the observer. All information that inflows or outflows the observer must pass through the computing device, allowing the customer to ensure that there is no unauthorized communication between the observer and other parties. Meanwhile, the computing device cannot complete a transaction without the cooperation of the observer. This gives the observer the power to prevent the customer from making payments that it does not allow, such as spending the same electronic coin more than once. Note that, even if the tamper-resistant protection is unexpectedly defeated somehow, this scheme can still provide cryptographic security to detect and identify the double-spenders.

O-Cash is designed to be able to implement on the following infrastructure:

- **Internet and computer based**. The next wave of electronic payment schemes integrating privacy protection, non-repudiation is based on the Internet revolution. The examples of e-commerce services, such as Amazon, eBay and Dell, demonstrate the impact of Internet setting on the old trade model. Direct PC and other equipment purchasing is yet another novel business model that the Internet enables. The direct access to customers and reduction of

supply chains are expected to further enhance the economic value of the Internet. Therefore, electronic payments on the web are of prime importance, and *O-Cash* is designed to have this capability of enabling payment through computer with smart card reader.

- **Mobile Device based**. M-Commerce, which refers to the use of portable wireless devices for payment transactions, has been proposed previously. The main idea is to simplify the processing of regular payments on customers' side. In *O-Cash*, customers can install electronic wallet on their mobile phone or PDA, and can make payment at any point of sale (POS). The portable electronic wallet device have a trustworthy display and keypad to control payment transactions, as well as SIM cards for data protection and active certificates for distributed trust. An additional advantage of the mobile device based O-Cash is that contact-less interfaces could be used, such as radio or infrared.

Chapter 7

Conclusions

Throughout this thesis, the main objectives are focused on the following three open problems of electronic cash.

- **Double Spending Prevention:** How to prevent anyone from spending the same electronic coin twice?
- **Fair Traceability:** How to enable legal tracing and inhibit illegal tracing?
- **Model Simplification:** Is there any way to simplify the electronic cash model?

O-Cash, an electronic cash scheme in wallet with observers, has been proposed to address the open problems of double-spending prevention and fair traceability. To achieve double spending prevention, *O-Cash*

offers prior restraint of double-spending via tamper resistent hardware and detection of double-spenders' identity via cryptographic protocols. To address fair traceability, *O-Cash* supports coin tracing and owner tracing as well as self-deanonymization in case crimes take place.

SignCash, a new fair traceable customer generated electronic cash model, has been proposed to simplify the traditional electronic cash model. To achieve model simplification, *SignCash* enables customers to generate electronic coins on behalf of the bank, therefore, withdrawal phase can be eliminated in the new model.

For the area of electronic cash, there are other open problems, which may be good topics for future research:

- **Divisibility.** An electronic cash scheme that enables the divisibility allows an electronic coin to be divided into subdivisions. Each subdivision is worth any desired value and all values of the subdivisions must be added up to the original value.

- **Transferability.** The ability to transfer paper cash is very important in our daily life, so in desirable systems, electronic cash should be able to be transferred from customer to customer.

Publications

[1] X. Hou and C. H. Tan, Fair Traceable Off-line Electronic Cash In Wallet With Observers, *International Conference on Advanced Communication Technology – ICACT'2004*, Pages 595-599, IEEE Communication Society Press, 2004

[2] X. Hou and C. H. Tan, A New Electronic Cash Model, *International Conference on Information Technology: Coding and Computing – ITCC'2005*, Pages 374–379, IEEE Computer Society Press, 2005

Bibliography

[1] T. Cao, D. Lin, and R. Xue. A Randomized RSA-based Partially Blind Signature Scheme For Electronic Cash, *Computers & Security*, Volume 24, Pages 44–49, 2005.

[2] D. Chaum. Blind Signatures For Untraceable Payments, *Advances in Cryptology – CRYPTO'1982*, Pages 199–203, Plenum Press, 1983.

[3] C. Popescu. An Off-line Electronic Cash System With Revokable Anonymity, *IEEE Mediterranean Electrotechnical Conference – IEEE MELECON'2004*, Volume 2, Pages 763–767, 2004.

[4] W. Qiu, K. Chen, and D. Gu. A New Off-line Privacy Protection E-Cash System With Revokable Anonymity, *Information Security Conference – ISC'2002*, Lecture Notes in Computer Science, Pages 177–190, Springer-Verlag, 2002.

[5] S. Solms and D. Naccache. On Blind Signatures And Perfect Crimes, *Computers and Security*, Volume 11, No.6, Pages 581–583, 1992.

[6] M. Jakobsson, D. MRaihi, Y. Tsiounis, and M. Yung. Electronic Payments: Where Do We Go from Here?, *CQRE'1999*, Pages 43–63, 1999.

[7] http://www.nets.com.sg/.

[8] R. Anderson and M. Kuhn. Low Cost Attacks On Tamper Resistant Devices, *International Workshop on Security Protocols – IWSP'1997*, Lecture Notes in Computer Science, Volume 1361, Pages 125–136, Springer-Verlag, 1997.

[9] D. Boneh, R. A. DeMillo, and R. J. Lipton. On The Importance Of Checking Cryptographic Protocols For Faults, *Advances in Crytology – EUROCRYPT'1997*, Lecture Notes in Computer Science, Volume 1233, Pages 37–51, Springer-Verlag, 1997.

[10] S. Hille and P. Stappen. Electronic Payment Put In Context, http://gigaabp.telin.nl, GigaABP, 2002.

[11] http://www.iliumsoft.com/.

[12] http://wallet.yahoo.com/.

[13] D. Tygar. Atomicity in Electronic Commerce, *Fifteenth Annual ACM Symposium on Principles of Distributed Computing*, Pages 8–26, 1996.

[14] G. Medvinsky and C. Neuman. NetCash: A Design For Practical Electronic Currency On The Internet, *1st ACM Conference on Computer and Communication Security*, Pages 102–106, 1993.

[15] S. Even, O. Goldreich, and Y. Yacobi. Electronic Wallet, *Advances in Cryptology – CRYPTO'1983*, Pages 383–386, 1984.

[16] D. Chaum, A. Fiat, and M. Naor. Untraceable Electronic Cash, *Advances in Cryptology – CRYPTO'1988*, Lecture Notes in Computer Science, Volume 403, Pages 319–327, Springer-Verlag, 1990.

[17] A. Shamir. How To Share A Secret, *Communications of the ACM*, Pages 612–613, 1979.

[18] G. R. Blakley. Safeguarding Cryptographic Keys, *Proceedings of AFIPS National Computer Conference*, Volume 48, Pages 313–317, 1979.

[19] N. Ferguson. Single Term Off-line Coins, *CWI technical report CS-R9318*, 1993.

[20] N. Ferguson. Single Term Off-line Coins, *Advances in Cryptology – EUROCRYPT'1993*, Lecture Notes in Computer Science, Volume 765, Pages 318–328, Springer-Verlag, 1994.

[21] V. Varadharajan, K. Q. Nguyen, and Y. Mu. On The Design Of Efficient RSA-based Off-line Electronic Cash Schemes, *Theoretical Computer Science*, Volume 226, No.1–2, Pages 173–184, 1999.

[22] D. Chaum and T. P. Pedersen. Wallet Databases With Observers, *Advances in Cryptology – CRYPTO'92*, Lecture Notes in Computer Science, Volume 740, Pages 89–105, Springer-Verlag, 1993.

[23] D. Kügler and H. Vogt. Auditable Tracing With Unconditional Anonymity, *International Workshop on Information Security Application – WISA'2001*, Pages 151–163, 2001.

[24] D. Kügler and H. Vogt. Fair Tracing Without Trustees, *Financial Cryptography – FC'2001*, Pages 136–148, 2001.

[25] D. Kügler and H. Vogt. Off-line Payments With Auditable Tracing, *Financial Cryptography – FC'2002*, Lecture Notes in Computer Science, Volume 2357, Pages 269–281, Springer-Verlag, 2002.

[26] C. P. Schnorr. Security Of Blind Discrete Log Signatures Against Interactive Attacks, *International Conference On Information and Communications Security – ICICS'2001*, Lecture Notes in Computer Science, Volume 2229, Pages 1–12, 2001.

[27] T. ElGamal. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Theory*, Volume IT-31, No.4, Pages 469–472, 1984.

[28] T. Okamoto and K. Ohta. Universal Electronic Cash, *Advances in Cryptology – CRYPTO'1991*, Lecture Notes in Computer Science, Volume 576, Pages 324–337, Springer-Verlag, 1992.

[29] T. Nakanishi and Y. Sugiyama. Unlinkable Divisible Electronic Cash, *Proceedings of 3rd International Workshop on Information Security – ISW'2000*, Lecture Notes in Computer Science, Volume 1975, Pages 121–134, Springer-Verlag, 2000.

[30] T. Okamoto. Active Certificates: A New Paradigm In Digital Certificate Management, *Advances in Cryptology – CRYPTO'1995*, Lecture Notes in Computer Science, Volume 963, Pages 438–451, Springer-Verlag, 1995.

[31] I. B. Damgard. Collision Free Hash Functions And Public Key Signature Schemes, *Advances in Cryptology – EUROCRYPT'1987*, Lecture Notes in Computer Science, Volume 304, Pages 203–216, Springer-Verlag, 1988.

[32] R. L. Rivest and A. Shamir. PayWord And MicroMint: Two Simple Micropayment Schemes, *CRYPTOBYTES*, Volume 2, No.1, Pages

7–11, 1996.

[33] L. Lamport. Password Authentication With Insecure Communications, *Communications of ACM*, Volume 24, No.11, Pages 770–772, 1981.

[34] K. Suzuki, K. Kobayashi, and H. Morita. Efficient Sealed-bid Auction Using Hash Chain, *International Conference on Information Security and Cryptology – ICISC'2000*, Lecture Notes in Computer Science, Volume 2015, Pages 183–191, Springer-Verlag, 2000.

[35] C. S. Jutla and M. Yung. PayTree: Amortized Signature For Flexible Micro-payments, *Second USENIX Association Workshop on Electronic Commerce*, Pages 213–221, 1996.

[36] S. M. Yen, L. T. Ho, and C. Y. Huang. Internet Micropayment Based On Unbalanced one-way binary tree, *International Workshop on Cryptographic Techniques and E-Commerce – CRYPTEC'1999*, Pages 155–162, 1999.

[37] J. Camenisch, J. Piveteau, and M. Stadler. Fair Blind Signatures, *Advances in Cryptology – EUROCRYPT'1995*, Lecture Notes in Computer Science, Volume 921, Pages 209–219, Springer-Verlag, 1995.

[38] E. Brickell, P. Gemmell, and D. Kravitz. Trustee-based Tracing Extensions To Anonymous Cash And The Making Of Anonymous Change, *Proceedings of the Sixth Annual ACM-SIAM Symposium on Discrete Algorithms – SODA'1995*, Pages 457–466, 1995.

[39] J. Camenisch, U. Maurer, and M. Stadler. Digital Payment Systems With Passive Anonymity-Revoking Trustees, *Journal of Computer Security*, Volume 5, No.1, Pages 69–89, 1997.

[40] B. Pfitzmann and A. R. Sadeghi. Self-escrowed Cash Against User Blackmailing, *Financial Cryptography – FC'2000*, Lecture Notes in Computer Science, Volume 1962, Pages 42–52, Springer-Verlag, 2000.

[41] S. Canard and J. Traore. On Fair E-cash Systems Based On Group Signature Schemes, *The Eighth Australasian Conference on Information Security and Privacy – ACISP'2003*, Lecture Notes in Computer Science, Volume 2727, Pages 237–248, Springer-Verlag, 2003.

[42] Y. Mu, K. Q. Nguyen, and V. Varadharajan. A Fair Electronic Cash Scheme, *International Symposium on Electronic Commerce – ISEC'2001*, Pages 20–32, 2001.

[43] R. J. F. Cramer and T. P. Pedersen. Improved Privacy In Wallets With Observers, *Advances in Cryptology – EUROCRYPT'1993*,

Lecture Notes in Computer Science, Volume 765, Pages 329–343, Springer-Verlag, 1994.

[44] S. Brands. Untraceable Off-line Cash In Wallet With Observers, *Advances in Cryptology – CRYPTO'1993*, Lecture Notes in Computer Science, Volume 773, Pages 302–318, Springer-Verlag, 1994.

[45] A. Solages and J. Traore. An Efficient Fair Offline Electronic Cash System With Extensions To Checks And Wallets With Observers, *Financial Cryptography – FC'1998*, Lecture Notes in Computer Science, Volume 1465, Pages 275–295, Springer-Verlag, 1998.

[46] G. I. Davida, Y. Frankel, Y. Tsiounis, and M. Yung. Anonymity Control In E-Cash Systems, *Financial Cryptography – FC'1997*, Lecture Notes in Computer Science, Volume 1318, Pages 1–16, Springer-Verlag, 1997.

[47] D. Chaum and E. van Heijst. Group Signatures, *Advances in Cryptology – EUROCRYPT'1991*, Springer-Verlag, Pages 257–265, 1991.

[48] S. Canard and J. Traore. On Fair E-cash Systems Based on Group Signature Schemes, *Proceedings of Australasian Conference on Information Security and Privacy – ACISP'2003*, Pages 237–248, 2003.

[49] H Choi, F. Zhang, and K. Kim. Electronic Cash System Based On Group Signatures With Revokable Anonymity, *Proceedings of Workshop of Korea Information Security Institute*, Pages 29–34, 2003.

[50] J. Traore. Group Signatures And Their Relevance To Privacy Protecting Offline Electronic Cash Systems, *Proceedings of Australasian Conference on Information Security and Privacy – ACISP'1999*, Pages 228–243, 1999.

[51] J. Kilian and E. Petrank. Identity Escrow, *Advances in Cryptology – CRYPTO'1998*, Lecture Notes in Computer Science, Volume 1642, Pages 169–185, Springer-Verlag, 1998.

[52] J. Camenisch and M. Michels. Separability And Efficiency For Generic Group Signature Schemes, *Advances in Cryptology – CRYPTO'1999*, Pages 106–121, 1999.

[53] J. Camenisch and M. Michels. A Group Signature Scheme Based On An RSA-Variant, *Advances in Cryptology – ASIACRYPT'1998*, Lecture Notes in Computer Science, Volume 1514, Pages 160–174, Springer-Verlag, 1998.

[54] W. Diffie and M. Hellman. New Directions In Cryptography, *IEEE Transactions on Information Theory*, Volume IT-22, No.6, Pages 644–654, 1976.

[55] Z. Y. Lee, H. C. Yu, and P. J. Ku. An Analysis And Comparison Of Different Types Of Electronic Payment Systems, *Portland International Conference on Management of Engineering and Technology – PICMET'2001*, Volume 2, Pages 38–45, 2001.

[56] T. Okamoto. Provably Secure And Practical Identification Schemes And Corresponding Signature Schemes, *Advances in Cryptology – CRYPTO'1992*, Lecture Notes in Computer Science, Volume 740, Pages 31–53, Springer-Verlag, 1992.

[57] R. L. Rivest, A. Shamir, and L. M. Adleman. A Method For Obtaining Digital Signatures And Public-key Cryptosystems, *Communications of the ACM*, Volume 21, No.2, Pages 120–126, 1978.

[58] Y. Tsiounis. Efficient Electronic Cash: New Notions And Techniques, Ph.D Thesis, College of Computer Science, Northeastern University, Boston, MA, USA, 1997.

[59] KPMG Consulting. Problem Gambling – ATM/EFTPOS Functions And Capabilities, A Report Provided to Australian Government, 2005.

Appendix A

Symbols and Notations

- p, q: large primes such that $q|p-1$.
- Z_p: for any prime p, the set of non-negative integers smaller than p.
- Z_p^*: a multiplicative group of integers modulo p.
- G_q: a subgroup of Z_p^* of order q where the discrete logarithm problem is hard.
- g: a generator of G_q.
- $r \in_R$ [a, b]: an integer r, which is chosen randomly from $[a, b]$.
- a^{-1}: the multiplicative inverse of $a \in Z_p^*$.
- $\|$: the concatenation of two strings.

Appendix B

Glossary and Abbreviations

- **Algorithm:** A set of steps, instructions, mathematical routine or computational rules specifying the procedures to perform a task, in order to solve a particular problem.

- **Acquirer:** An institution that provides a shop with facilities to accept card payments, accounts to the shops for the proceeds and settles the resulting obligations with card issuers. In the example of credit card systems, an acquirer is a Visa/Master Card affiliated entity that is in charge of processing credit card transactions.

- **Certification Authority:** Also known as CA. A trusted third-party entity that directly issues, renews, or revokes digital certificates. The role of the CA in this process is to guarantee that the two parties exchanging information are really who they claim to

be. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. In order for others to verifies the applicant's identity, the CA makes its own public key readily available to the public.

- **Clearing:** The processing of financial transactions between the acquirer and issuer for reconciliation, billing and statement use. For example, the clearing of credit card system is the precess to facilitate posting of a cardholder's account and reconciliation of a merchant's settlement position.

- **Clearing House:** An agency or separate corporation that facilitates the clearing and settlement of checks or payment items.

- **Cryptography:** The mathematical science and technology used to secure the confidentiality by converting it into a secret code, called cipher text, by an encryption algorithm. The cipher text can be reconverted to the original data, called plain text, only by someone holding the proper decryption algorithm and secret key.

- **Database:** A collection of inter-related data which may only be accessed by authorized users. It is composed of fields (single piece of info), records (complete set of fields), and tables (list of records) together with a set of operations for searching, sorting, recombin-

ing, and other functions

- **Electronic Commerce:** Also known as e-commerce. The conduct of business transactions in an electronic manner, usually over the Internet. More specifically, e-commerce refers to the integration of email, Electronic Funds Transfer (EFT), Electronic Data Interchange (EDI), and other techniques into a comprehensive electronic-based system.

- **Electronic Data Interchange:** Also known as EDI. This term refers to the exchange of computer readable data in a standardized form (e.g., purchase orders, confirmations, invoices, bills of lading) between business partners.

- **Electronic Funds Transfer:** Also known as EFT. A transfer of funds between accounts by electronic means rather than conventional paper-based payment methods. EFT includes Fedwire, Automated Clearing House (ACH) transfers, On-line Payment and Collection (OPAC) system, etc

- **Electronic Letter of Credit:** Also known as eLOC. An instrument certified by an authorized official that authorizes the recipient to request an electronic draw down (or advance) of funds.

- **Electronic Wallet:** Software, integrated circuit card or super

smart card that enables a customer to conduct online payment transactions. An e-wallet can hold a customer's digital certificates to identify the customer, shipping information to speed payment transactions, and electronic cash that has been withdrawn.

- **Encryption:** The use of cryptographic algorithms to encode readable data (plain text) into a sequence of characters (cipher text), in order to hide its content from everyone except its intended viewer.

- **Interactive Voice Response:** Also known as IVR. The systems that provide pre-recorded information over telephone, in response to user input in the form of DTMF (Dual Tone Multiple Frequency) signaling.

- **Mobile Commerce:** Also known as M-Commerce. This term refers to the business transactions that are made or facilitated using mobile devices.

- **Micro-payment:** A small amount of payment, perhaps even less than a penny, which would be uneconomical to process through traditional payment media. With micropayments, however, e-commerce merchants can sell products for far lower prices, such as charging small fees for downloading documents or charging per click for online advertising. Micropayment systems are still largely experimen-

tal and not widely available.

- **Non-repudiation:** A cryptographic situation in which someone who digitally signs a document using his/her digital signature, ensuring document integrity and authenticity, cannot later claim that he/she did not originate the document, or that the document was altered after he/she signed it. Non-repudiation protects both the sender and the recipient of the document from false claims that the document was either not sent, or not received.

- **Personal Digital Assistant:** Also known as PDA. A compact, mobile hand-held device for information storage/retrieval, computing and networking. PDA is typically operated via a touch screen stylus rather than a keyboard, and is often used for keeping calendars and address book information.

- **Personal Identification Number:** Also known as PIN. A private series of numbers that a customer used in order to prove the customer's identity.

- **Point of Sale:** Also known as POS. This term generally refers to the site where a payment transaction occurs.

- **RSA:** A public-key cryptographic system that was invented by Ron Rivest, Adi Shamir, and Leonard Adleman.

- **Session key:** A temporary key that is only valid for a short period.
- **Secure Electronic Transaction:** Also known as SET. The SET specification is an open technical standard and protocol developed by Visa and MasterCard. It is used to protect the security of credit card transactions conducted over the Internet.
- **Secure Socket Layer:** Also known as SSL. A standard developed by Netscape so that encrypted information can be read only by the intended recipient.
- **Secure Hypertext Transfer Protocol:** Also known as S-HTTP or HTTPS. This is a web protocol that supports sending data securely over the World Wide Web. It is often used in conjunction with Secure Sockets Layer (SSL).

Appendix C

Cryptographic Background

C.1 Introduction

The goal of this chapter is to encompass the notions and functions necessary for the understanding of electronic cash, which necessitates an overview of modern cryptography, mainly due to the complexity of electronic cash schemes.

In 1976, Diffie and Hellman's original paper 'New Directions in Cryptography' [54] marked the beginning of modern cryptography. They proposed cryptography based on intractable problems, which are hard for attackers to solve. Modern cryptography is inherently linked to these intractable problems, so I will introduces two most frequently used intractable problems in section C.2: the discrete logarithm problem and factorization problem. In section C.3 and C.4, I will discuss the impor-

tant applications of intractable problems, namely, one-way functions and digital signatures, which are very important to the design and analysis of electronic cash.

C.2 Intractable Problems

As most of the electronic cash schemes, including the schemes discussed in this thesis, are based on discrete logarithm assumption and/or factorization assumption, I will briefly describe these concepts in this section.

C.2.1 Discrete Logarithm Related Assumptions

For any prime p, the set of non-negative integers smaller than p is denoted by Z_p and the multiplicative group is denoted by Z_p^*.

The *inverse modulo p of an element* $a \in Z_p^*$ (denoted by a^{-1}) is the unique number in Z_p^*, that satisfies $a \cdot a^{-1} = 1 \bmod p$.

For any element $a \in Z_p^*$, *the order of a modulo p* is the smallest non-negative integer μ such that $a^{\mu} = 1 \bmod p$.

This order always divides $p-1$. Consequently, it always holds that $a^{p-1} = 1 \bmod p$. Let g be an element of order $p-1$ in Z_p^*, which is referred to as a *generator of the group* Z_p^*.

Assumption 2-1 (Discrete Logarithm Assumption): Finding the exponent $x \in Z_{p-1}$ of $h \in Z_p^*$ with respect to $g \in Z_p^* \backslash \{1\}$, such that

$g^x = h \bmod p$, is the Discrete Logarithm Problem (DLP). The Discrete Logarithm Assumption (DLA) states that it is hard to solve DLP.

Let q be a large prime factor dividing $p-1$. The unique subgroup of Z_p^* of order q is denoted by G_q.

Definition 2-1 (Representation Problem): Let $k \geq 2$. A generator-tuple of length k is a k-tuple $(g_1, g_2, \cdots, g_k)$ with $g_i \in G_q \backslash \{1\}$ and $g_i \neq g_j$ if $i \neq j \in \{1, \ldots, k\}$. For any $h \in G_q$, a representation of h with respect to a generator-tuple $(g_1, \ldots, g_k)$ is a tuple $(a_1, \ldots, a_k)$, with $a_i \in Z_q$ for all $1 \leq i \leq k$, such that $\prod_{i=1}^{k} g_i^{a_i} = h$.

Proposition 2-1 (Representation Assumption): Assuming that it is hard to compute discrete logarithm in G_q, given a number $h \in G_q$ and a randomly chosen generator-tuple $(g_1, \ldots, g_k)$, it is hard to find a representation of h based on $(g_1, \ldots, g_k)$.

Note: For $h = 1$, there is a trivial representation (0,0,...,0). For $h \neq 1$, it is believed to be hard to solve the representation problem, in which the hardness of finding a representation for random elements is generally based on the hardness of computing discrete logarithms in G_q [44].

C.2.2 Factoring Related Assumptions

Assumption 2-2 (Factoring Assumption): Given a sufficiently large $n = p \cdot q$, where p and q are large enough primes, it is hard to find p and q.

The RSA problem is closely related to the hardness of factoring a large integer. The RSA signature scheme, which was introduced by Rivest, Shamir and Adleman [57], is based on the intractability of the RSA problem.

Assumption 2-3 (RSA Assumption): Given a sufficiently large n which is the product of two distinct primes p and q, a positive odd integer e such that $\gcd(e, \text{lcm}(p-1,q-1))=1$. For an integer c, finding an integer m such that $m^e = c \bmod n$ is the RSA Problem. The RSA Assumption states that it is hard to find the e^{th} roots modulo n.

The RSA problem can be easily solved if the factorization of n is known. But without knowing the factorization of n, it is believed that RSA schemes achieve very high security. Therefore, many electronic cash schemes use RSA schemes for the construction of electronic coins.

C.3 One-Way Functions

Definition 2-2 (One-Way Function): A one-way function is a function $f: A \rightarrow B$ such that for each $x \in A$ there exists a polynomial-time algorithm to compute $f(x)$. But for given $y \in B$, it is hard to find $x \in A$ such that $y = f(x)$.

The functions based on Discrete Logarithm Assumptions and Factoring Assumptions are usually considered to be one-way functions, for example:

- $f_1 : Z_q \rightarrow G_q, f_1(x) = g^x \bmod p$;
- $f_2 : Z_n^* \rightarrow Z_n^*, f_2 = x^e \bmod n$.

One-way functions are also very important tools for the construction of electronic cash schemes.

C.4 Digital Signatures

One important application of public key cryptography is digital signatures. A digital signature of a message is a string of bits dependent on some secret information (known only to the signer) and on the content of the message being signed. The functions of digital signatures and traditional hand-written signatures have the following similarities:

- **Authentication:** a digital signature guarantees that the signer is the originator of the document;
- **Unforgeability:** only legitimate signers can sign a document and no others could produce a valid signature in the name of the legitimate signer;
- **Non-reusability:** a digital signature cannot be reused for another different document;
- **Unalterability:** after the document is signed, it cannot be altered;
- **Non-repudiation:** no signer can repudiate his/her signature later.

Definition 2-3 (Digital Signature Scheme): a digital signature scheme is a public key cryptosystem that consists of the following items:

- A key generation algorithm KG, which generates a secret key/public key pair (pk, sk) for the signer;
- A signature algorithm S, which is a protocol for producing a digital signature. With input (sk, M), the signature algorithm produces s, which is called the signature of the message M.
- Verification algorithm V, which is a method allowing the recipient to verify a signature. With input (pk, M, s), the output of the verification algorithm yields either *true* or *false*.

The security of a digital signature scheme has different levels depending on how much information an adversary can obtain. In terms of attacks, there are several types, which include [58]:

- *Known plaintext attack*, in which the adversary is given a set of signatures and the respective messages.
- *Chosen plaintext attack*, in which the adversary has a chance to request the signatures on some messages of his/her choice at one time.
- *Adaptive chosen plaintext attack*, in which the adversary has chances to request the signatures on some messages of his/her choice at any time, in any sequence. The choice of latter messages may be based on the analysis result of previous messages.

In terms of forgery, there are several levels of success:

- *Existential forgery*: the adversary succeeds in forging the signature of at least one message, which may not be of his/her choice or even meaningful.
- *Selective forgery*: the adversary succeeds in forging the signature of only some messages of his/her choice.
- *Universal forgery*: the adversary is able to forge the signature of

any message without the secret key of the target digital signature scheme.

- *Total break*: the adversary finds out the secret key of the target digital signature scheme.

RSA Digital Signatures

Many electronic cash systems discussed in this thesis are based on the RSA public key cryptosystem. Therefore, I will discuss the scheme of RSA Digital Signatures as follows:

Each RSA participant picks his/her own RSA key pairs at random. The public key consists of a modulus $n = pq$ of prescribed size, where p and q are two randomly generated primes of equal size, and an exponent e, which is co-prime with $\phi(n) = (p-1)(q-1)$. The private key d is the multiplicative inverse of e modulo $\phi(n)$, that is, the unique number d satisfying $de \equiv 1 \bmod n$, which is denoted by $1/e$.

To sign a message $m \in Z_n^*$, where the signer has private key d and public key (e, n), the signer computes the signature $s = m^d \bmod n$. To verify the correctness of the digital signature, the requester checks whether $s^e \equiv m \bmod n$. For a correct RSA digital signature, this equation must hold since the equation of $m^{de} \equiv m \bmod n$ holds due to $m^{\phi(n)} \equiv 1 \bmod n$ for all $m \in Z_n^*$. Actually, it can be proven that $m^{de} \equiv m \bmod n$ for all $m \in Z_n^*$.

When applying RSA scheme to the design of electronic cash systems, the actual message should be transformed into a related message by applying a one-way hash and/or redundancy-adding function $f(\cdot)$ to it and then signing the result of $f(m)$. The reason is because RSA digital signatures can be existentially forged (e.g. select an arbitrary s and take $m = s^e \bmod n$, then s is a valid RSA signature on the message m).

C.5 Blind Signatures

Blind digital signatures, also known as blind signatures, play a critical role in the design and analysis of electronic cash. Actually, blind signatures [2] were introduced by Chaum to design the first electronic cash systems.

The function of blind signatures is to allow a verifier to obtain digital signatures from a signer without the signer knowing the message to be signed.

Blind signatures are important techniques for the withdrawal phase of anonymous electronic cash schemes, and ensure the validity of electronic coins in the payment and deposit phase, while on the other hand ensure the untraceability of blindly signed electronic coins and the anonymity of customers.

The process to get a blind signature is as follows: instead of providing

the signer with the actual message M, the requester sends the signer a blinded version M_0 of the message M. The transformation has to be such that the signer will not be able to know M after seeing and signing M_0. In addition, there must exist an inverse transformation, which on input the signature S_0 of M_0 will output a valid signature S on the original message M.

Appendix D

Existing Electronic Payment Systems

D.1 VisaCash

D.1.1 Introduction

Visa Inc. has developed its own cash-like system called Visa Cash Card. It is basically a stored value card designed for those who may have difficulty in obtaining a credit card and do not want to build their credit. Its system is based on a small smart card with an embedded microprocessor that stores electronic cash. This card is loaded with electronic cash via specialized ATM machines or over the counter, and then the stored electronic cash can later be spent by inserting the card into the retailer's

card-reader. In this way, electronic cash is transferred from the card to another entity, which may either be another card or a shop's computer system.

D.1.2 Smart Card: The Basis of Visa Cash

As the security of Vias Cash system is based on smart card. In order to evaluate Visa Cash Card, it is important to understand the features and properties of smart card. In this section, I will discuss the basic information of smart card and its applications.

Smart Card Definition

A smart card is a plastic card containing an embedded microprocessor that stores information and applications. The microprocessor is an integrated circuit computer chip, which is a thin piece of semiconductor material that has been chemically processed to perform complex operations, coupled with a smart card reader. In practice, smart cards can be used for payment with electronic cash stored inside, and can be recharged via a smart card writing device.

Smart Card Capacity and Platform

Smart cards vary in the amount of memory that they contain, which affects the number and types of applications that can be run [59].

- 32K smart cards allow the same card to be used for multiple applications.
- 64K or 128K cards are available for high-capacity applications.
- Gemplus has produced a prototype card with 256MB of flash memory.

There are three main smart card platforms [59] as shown in table D.1.

Vendor	**Platform Name**	**Primary Use**
Mondex	Multos	Financial smart card applications
Microsoft	Windows for Smart Cards	Network security applications
Sun Microsystems	Java Card	GSM and m-commerce applications

Table D.1: Smart Card Platform

Smart Card Growth

Smart cards have become an important electronic payment solution around the globe, and its popularity is increasing in emerging applications. In shipment terms, the most mature smart card market is the Europe, Middle East and Africa (EMEA) region, which accounts for over 50% of card shipments. However, based on the information from *Datamonitor* as shown in figure D.1, EMEA's relative importance is decreasing as Asia-Pacific catches up.

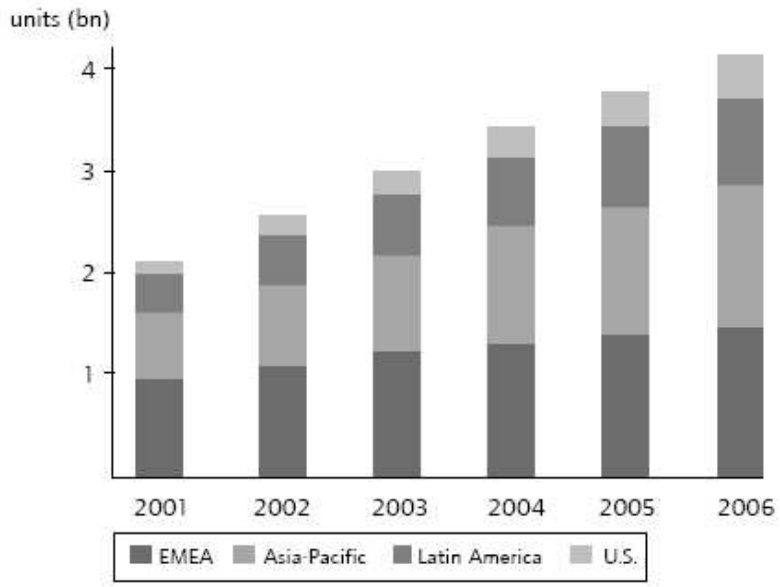

Figure D.1: Smart Card Market Growth

Smart Card Applications

The two core functions of smart cards are described as below:

1. Data storage, management and transport: a smart card, although small in size, can currently store up to 100 times as much data as a traditional magnetic stripe card. This is particularly useful in areas where a significant amount of data storage is needed. For example, smart cards carrying medical records and test results, for example, have been pilot implemented in Australia. Another example is GSM mobile phone cards and stored value cards which are widely used as a type of electronic wallets.

2. User identification: special mechanisms for identifying the user are

offered by the smart card, so that security and privacy are ensured. Usually the identification mechanism is based on a user name and a PIN. But other mechanisms are also available or are under testing, for example biometrics, such as fingerprint scanning, are used in conjunction with smart identity cards.

D.2 eNETS

D.2.1 Introduction

Network for Electronic Transfers Singapore Pte Ltd, also known as NETS, is an electronic payment platform, formed in 1985 by a consortium of local banks in Singapore – Development Bank of Singapore (DBS), Overseas Chinese Banking Corporation (OCBC) and United Overseas Bank (UOB) etc. NETS aims to establish infrastructure, systems and services to facilitate electronic payment services. The company starts operations by offering an island-wide EFTPOS network in Singapore. Over the years, NETS has evolved to a multi-service organization, providing a comprehensive range of electronic payment services. Today, NETS services are available at more than 12,500 merchants and across 30,000 points of access, including retail outlets, educational institutions, government establishments and car parks (source: www.nets.com.sg).

D.2.2 EFTPOS: The Basis of NETS

EFTPOS is the abbreviation for electronic funds transfer at point of sale. The development of electronic payment in Singapore was boosted by the introduction of the EFTPOS service offered by NETS since 1986. EFTPOS is a debit card system allowing ATM card holders to use their ATM cards to make electronic payment at point of sale (POS) through Electronic Fund Transfer (EFT) from their accounts. In addition, the reverse flow (CashBack) service was introduced in 2001 to allow consumers to withdraw cash at selected retail stores through EFTPOS terminals. This service is currently provided free to the ATM card holders of five major local banks in Singapore.

EFTPOS transactions acquired on NETS terminals are online routed to NETS for processing, before the transactions are approved. The routing arrangements have two methods as follows:

- For debit cards issued in Singapore, NETS dispatches the transaction for authorization to the issuing bank. The issuing bank will:

    1. Verifies the PIN.
    2. Checks whether there are sufficient funds are available in the customer's account.
    3. Verifies that the transaction is not fraudulent,

4. Debits the customer's account

5. Informs the shop and customer of the successful transaction

- For credit cards, such as Amex, NETS routes the transaction to the card processor determined by the credit company. The card processor, on behalf of the issuing bank, will check the payment limit, verify that the transaction is not fraudulent and authorize the payment.

The process of making eNETS payment over the Internet [7] is as follows:

1. Click the button 'eNETS' of the web site.

2. Choose the amount and method of payment (e.g. credit card, direct debit or internet banking accounts etc).

3. eNETS will automatically fill in the payment form and complete the payment.