Design of a Secure Electronic Cash System based on Fair Blind Signature Algorithm

Hyun-Ju Lee* · Mun-Suk Choi**

*Chungbuk National University

*Dept of Computer Science · **Radio Engineering · Chungbuk National University

E-mail : leehyn2@hanmail.net*, bidulgia@hotmail.com**

ABSTRACT

With a rapid development of Information Telecommunication technique, network communication environment has been greatly improved. People come to feel more convinient to purchase products through Internet. Accordingly, various kinds of electronic payment systems have been developed and used. In this paper, we propose an algorithm which not only can associate the broker system with an electronic cash user, but also regenerate an amount of money previously paid using technique such as Meta-Message recovery and a RSA Blind Signature based on discrete logarithm problem.

KEYWORD

Electronic Cash, Digital Signature, Fair Blind Signature, Untraceability, Discrete Logarithm Problem

Ⅰ. Introduction

With a great improvement of computer and network communication skills, e-commerce paved the way for various kinds of electronic payment systems, each of which systems should provide convenience and security simultaneously.

Electronic payment systems must guarantee a secure payment way for electronic information and on-line purchase. Electronic payment system is a very efficient way which guarantees customers, company, and merchant to have a safe, and convenient way.[1]

In this paper, for the purpose of an establishment of efficient Electronic cash system, we propose an algorithm which can regenerate the information about the oney previously paid whenever we need to check double spending, using Fair Blind Signature.

Ⅱ. Related works

1. Digital Signature and Electronic Cash System

Digital Signature is based on public cryptography scheme. A user encrypts a message with his/her private key which only the user knows. A Hash Function is a one way function. People cannot induce the original message by the output, digested message.

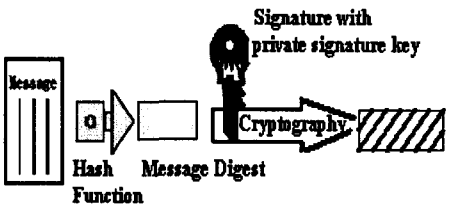

Fig 1. Digital signature

Electronic cash systems includes customers, banks which connect electronic cash to financial management networks, and merchants. Basic protocols includes four key factors.

- A withdrawal protocol : it is a protocol that pulls out electronic cash from user's account, it is done by a authenticated channel between user and banks.
- Payment protocol: it is a kind of protocol that user can pay electronic cash to the store through anonymous channel.
- Deposit protocol : it is a protocol to which stores deposit user's electronic cash information.

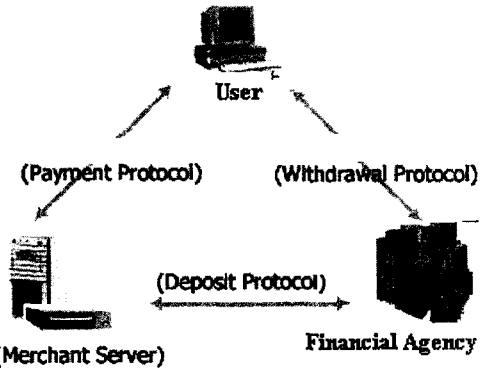

Fig 2. The model of electronic cash system

- Double-spending check protocol : it is a protocol that banks check on whether electronic cash is doubly used.

2. Basic requirement for electronic cash system

To provide safety and efficiency like real money in actual life, there are some requirement for electronic cash.[2]

- Independence : electronic cash should be transmitted by networks, not by physical conditions.
- Security : Electronic cash must not be re-used or duplicated. In online systems, it is quite easy to prevent double spending, but in Off-line systems, it is quite difficult to prevent dishonest user from using improper way.
- Untraceability : must not be traced by any other person.
- Implementation of full anonymity should be taken into serious consideration, because it might cause dropping electronic cash system efficiency, and also could be used for money laundering and tax evasion.
- Off-line transaction : it is desirable in Off-line way of trading procedure between users and stores when they use electronic cash. On-line banking system is safe, but it costs a lot and not so efficient.

III. Fair Blind Signature registration and model

1. previous registration for Fair Blind Signature

To get secrete information for fair blind signature, user should access to Publicly trusted Center which has a information to verify the user publicly, and go through previous registration steps. Registering protocol model is as follows.

2. Standler Fair Blind Signature Model

Blind Signature[3] is a protocol which provides information blinding of electronic cash, and unlinkability with signed payment. Fair Blind Signature[4] introduced by Stadler, can associate electronic cash users and brokers which are related to blind signature every time trusted party ask to. This model includes two protocols. One is a signing protocol which includes users, brokers, and trusted party. The other is a link recovery protocol.

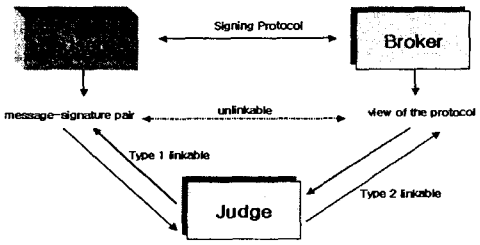

Fig 3. The model of a fair blind signature scheme

A Trusted Party provides two kinds of Fair blind Signature schemes which are received from users by the link recovery protocol. Type 1 transmits an information which guarantees the efficient authentication on message-Signature pair. Type 2 enables trusted Party to verify the sender of messages efficiently. we realize that we can detect unfair withdrawal of money by Type 1. We also provide a solution that detects double spending by using Type 2.

IV. Recovery of Electronic payment and Fair Blind RSA Signature Scheme

Fair Blind Signature introduced by Stadler cannot support recover of user's electronic cash with blind signatured electronic cash

payment. In this paper, we propose a novel Scheme which provides fairness and a solution that can regenerate an information about previously paid money, relying on Meta-Message Recovery and Blind RSA Signature which are based on Discrete Logarithm Problem proposed by Horster.[5]

1. Discrete Logarithm Problem

· $Z_p^* = \{r \in Z^p | (r,p)=1\}$: reduced residue system

· p: prime number

2. Parameter

· $c = h(\delta \cdot v_j \| \delta \cdot v_{1-j})$: hash value

· Z_q: residue system for modulo q

$v_j, v_{1-j} \in Z_q, j \in \{0,1\}$

· $payment$: spent money by electronic payment

· $y \equiv g^x \bmod p$: Public key of user

· g : Generator

3. Electronic payment recovery and Fair Blind RSA Signature

- A User sends broker $a_j \equiv g^{v_j + v_{1-j}} \bmod p$, $a_{1-j} \equiv c \cdot (g^{v_j+v_{1-j}})^{-1} \bmod p$ by v_j, v_{1-j}
- Broker calculate $c \equiv \alpha_j \cdot \alpha_{1-j} \bmod p$
- A signer generates $z_j^*, z_{1-j}^* \in Z_p$
- A broker generates parameter η_0^*, η_1^*, r_0, r_1, and transmits to user.
- The user generates $payment_j^*$.

$r_j \equiv payment^{-1}(g)^{z_j^* v_j} y^{v_{z-j}} \bmod p$,

$payment_j^* \equiv v_j^{-1} \cdot (r_j - v_{1-j}) - g^{z_j^*} \bmod q$

- The user transmits the broker r_j and $payment_j^*$.
- The broker generates

$s_j^* \equiv x \cdot (payment_j^* + g^{z_j^*}) - z_j^* \bmod q$

$\equiv x \cdot ((v_j^{-1} \cdot (r_j - v_{1-j}) - g^{z_j^*}) + g^{z_j^*}) - z_j^* \bmod q$

- The broker sends s_j^* to the user.
- The user calculates $s_j \equiv v_j \cdot s_j^* \bmod q$ for s_j^*, and gets the results of fair blind signature for

$payment \equiv g^{-s_j} y^{r_j} r_j^{-1} \bmod p$

V. Conclusion

Adopting Electronic payment system provides convinience and reduces the cost of transaction. Electronic cash needs a lower cost than credit cards, it will be expected to be widespread near future.

To meet the requirement for vitalizing domestic Electronic payment system, we should overcome the limits of cryptographic technique in which area foreign countries have played trigger role.

Reference

[1] Kazuhiko Kato, "Safe and Secure Execution Mechanism for Mobile Objects,"Moile Object Systems, Springer-Verlag, pp.201-211,1996

[2] B.Pfitzmann, "Properties of Payment Systems: General Definition Sketch and Classification," IBM Research Report, 1996.

[3] D. Chaum, "Blind Signature for Untraceable Payments," Advance in Cryptology-Crypto '82, Lecture Notes in Compture Science, Springer-Verlag, pp.199-203, 1983.

[4] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch, "Fair Blind Signature," Advances in Cryptoloty-Eurocrypt'95, Lecture Notes in Computer Science, Vol . 921, Spring-Verlag, 1995.

[5] Patrick Horster, Holger Petersen, "Meta Message Recovery and Meta Blind signature schemes based on the discrete logarithm problem and their applications," Advances in Cryptology-Asiacrypt'94, Lecture Notes in Computer Science, Springer-Verlag, 1994.