WUJNS
Wuhan University Journal of Natural Sciences

Vol.11 No.1 2006 155-159

Article ID: 1007-1202(2006)01-0155-05

# A Fair E-Cash Payment Scheme Based on Credit

□ **WANG Shao-bin, HONG Fan, CUI Guo-hua**

College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China

**Abstract**: A new fair e-cash payment scheme based on credit is present in this paper. In the scheme, an overdraft credit certificate is issued to user by bank. Using the overdraft credit certificate, user can produce e-cash himself to pay in exchanges. Merchant can verify the e-cash received from user. Bank can make a fair dispute resolution when there is a dissension between user and merchant. It can avoid the problem of partition e-cash for changes, prevent from reusing e-cash and faking e-cash. It fits justice, anonymity, non-deny and impartiality.

**Key words**: overdraft credit; off-line payment; e-cash; impartiality; justice

**CLC number**: TN 918

**Received date**: 2005-04-22

**Foundation item**: Supported by the National High Technology Development 863 Program of China under Grant (863-301-1-3)

**Biography**: WANG Shao-bin(1972-), male, Ph.D., research direetion: information security and electronic commerce. E-mail: wsbhust@tom.com

## 0 Introduction

The concept of electronic cash scheme was first introduced by Chaum[1] in 1983. From then on, there are a lot of improvements in e-cash research. Untraceable electronic cash was first presented by Chaum, Fiat and Naor[2]. Single-term off-line coins were first introduced independently by Brands[3,4], Ferguson[5] and Franklin[6,7]. Presently, most of realized e-cash in electronic payment system is based on the single-term off-line coins scheme. During the lifecycle, e-cash usually pass through three processes: take e-cash process, payment process and deposit process. It deals with user, bank and merchant. The circulation of e-cash is depicted as Fig. 1.

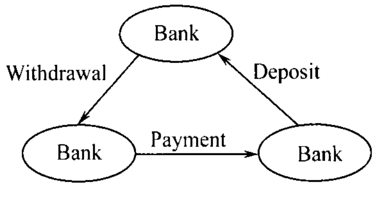

**Fig. 1 Circulation of e-cash**

There are some important problems including in e-cash researching. Such as the problem of partition e-cash to give changes, prevent from reusing e-cash and faking e-cash, keep justice, anonymity, non-deny and impartiality, storage and lose, efficiency and so on.

A new fair e-cash payment model based on credit is present in this paper. In the model, an overdraft credit certificate is issued to user by bank. User can produce e-cash himself to pay when needed. Merchant can verify the e-cash received from user. Bank can make a fair dispute resolution when there is a dissension between user and merchant. It can avoid the problem of partition e-cash to give changes, prevent from reusing e-cash and faking e-cash. It fulfills justice, anonymity, non-deny and impartiality.

## 1 Background

Presently, most of banks can issue an overdraft credit card to user in real life. User can use the card to pay freely in a limited number. The bank can automatic provide a loan to user. User can deposit the money to bank for his overdraft in a limit time. For example, a golden card issued by ICBC (Industrial and Commercial Bank of China), user can use this card to pay freely in \$5 000. ICBC can automatic provide a loan to user. We can use the same model to pay in Internet electronic commerce. First, user can apply to be an overdraft credit consumer in a bank. The bank issues an overdraft credit certificate to user after evaluating the user's credit. The overdraft credit certificate proved that this consumer can produce a valid e-cash for paying in the limited number. When buying in the limited credit number, consumer produces e-cash himself and pays to merchant. After verifying the overdraft credit certificate and e-cash, the merchant send the merchandise to consumer. Merchant can deposit the e-cash to bank in a limited time. Figure 2 shows the e-cash payment schemes based on overdraft credit. The details are described in next section.

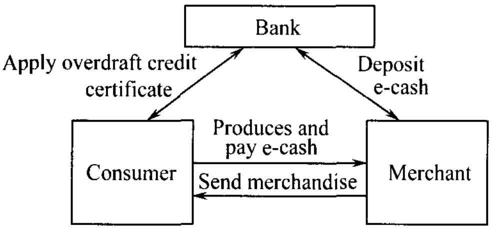

**Fig. 2 An e-cash payment schemes**

There are some virtues if we design the model as Fig. 2. Firstly, it can avoid the problem of partition e-cash to give changes, prevent from reusing e-cash and faking e-cash. Secondly, it fits justice, anonymity, non-deny and impartiality. In the third, because the exchange process does not need the bank, it can depress the bottleneck of exchange. Finally, as the e-cash is produced by user, it avoids the storage and lose problem.

## 2 Fair E-cash Payment Protocols

Fair e-cash payment scheme is composed of two parts: bank system and exchange system. Bank system includes national bank and the other branch banks. National bank issues certification for the other branch banks. Branch bank sets up account and issues overdraft credit certificate for consumer. It can be thought as a set up process. If needed, branch bank can make a fair dispute resolution when there is a dissension between user and merchant. Exchange system includes payment process, deposit process and dispute resolution process. The basic scheme is given in Fig. 3.

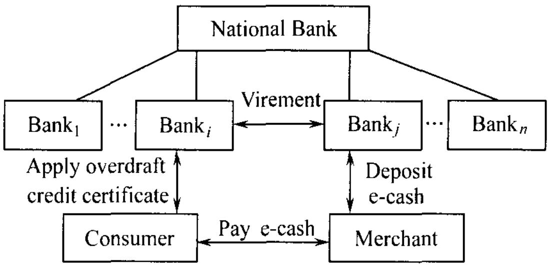

**Fig. 3 The basic fair e-cash payment scheme**

Next, we describe the four processes: set up process, exchange process, deposit process and dispute resolution process.

### 2.1 Setup Process

Set up process is composed of bank system set up and consumer register in bank.

Bank system set up: National bank issues certification for the other branch banks. It is used to prove the branch bank's validity. Supposed $(x_B, y_B)$ are the secret key and public key of national bank, $(x_B, y_B)$ are the secret key and public key of branch bank $i$. $\mathrm{CA}_{B_i} = E_{x_B}(y_{B_i})$ is the certification of branch bank $i$ issued by national bank. We ignore the other information in the certification. $E_{x_B}(\cdot)$ is an encryption function using $x_B$. National bank bring $(x_B, y_B)$ himself and publish public key. Branch bank $i$ produce $(x_{B_i}, y_{B_i})$ too, but it should be verified by nation bank and get certification $\mathrm{CA}_{B_i} = E_{x_B}(y_{B_i})$ from nation bank.

Consumer register in bank: Consumer can register to be an overdraft credit user in a familiar branch bank. The detail protocols are as follows:

Consumer submits his correlative datum to bank $i$ and apply for an overdraft credit certificate. After checking the consumer's credit file, bank $i$ setup an accounts for the consumer. Then consumer proves his cipher arithmetic using in e-cash and send the correlative key to bank $i$. If the cipher arithmetic has passed the checking, bank $i$ awards the overdraft credit certificate to consumer. The protocols are shown in Fig. 4.

This is an interactive protocol between consumer C and bank $i$. We use the double signature scheme presented

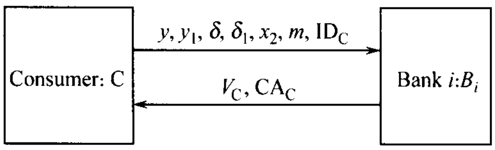

**Fig. 4 Consumer register protocols**

in Ref. [8]. Consumer first generates two mutual keys (private key, public key): $(x, y)$, $(x_1, y_1)$, and the arbitration key $x_2$, then contacts bank $i$ to get the public key $y$ certified. $(x, y)$ are used to produce e-cash named as $\delta$. $\mathrm{ID_C}$ is consumer's unique identity. $(x_1, y_1)$ are used to produce consumer's commitment for the exchange named as ($\delta_1$. This value $\delta_1$ has no intrinsic value, but serves as consumer's commitment to the exchange. The arbitration key $x_2$ is used by bank to make a fair dispute resolution when there is a dissension between user and merchant. After verifying the construction of arithmetic, bank $i$ issues a signed certificate $\mathrm{CA_C}$ and an overdraft credit voucher $V_C$ to consumer. The voucher $V_C$ is a signed statement for $\delta_1$ from bank $i$ that assures the following: ① $y_1$ is Consumer's valid commitment public key, and ② The algebraic relations between the keys have been verified, and, as a result, bank $i$ can generate an e-cash (multi-signature) from the corresponding consumer's commitment signature. ③ The largest value of an e-cash produced by consumer each time is limited in scopes. It stipulates the largest value of an e-cash which consumer can overdraft based on credit. The registration protocol describes as follows:

1) Consumer generates $\rho$, $q$, $g$, $x$, $x_1$, $x_2 = x_1 - x$, $y = g^x$ and $y_1 = g^{x_1}$, and opens $\rho, q, g$. The parameters $\rho$, $q$ and $g$ are the same of DSA signature scheme. And then, consumer computers e-cash (denote as $\delta$) and a commitment (denote as $\delta_1$) for a supposed random exchange information $m$.

$\delta = (r, s): r = mg^{-k} \bmod \rho, r' = r \bmod q, s = k - r'x \bmod \rho$, $k \in_R Z_p^*$.

$\delta_1 = (r_1, s_1): r_1 = mg^{-k} \bmod \rho$, $r_1' = r_1 \bmod q$, $s_1 = k - r_1' x_1 \bmod \rho$.

Consumer sends ($\rho$, $q$, $g$, $y$, $y_1$, $\delta$, $\delta_1$, $x_2$, $\mathrm{ID_C}$) to bank $i$.

2) After received the message from consumer, bank $i$ first verify $\delta$ and $\delta_1$, then construct $\delta$ using $x_2$ and $\delta_1$. Bank $i$ verify the e-cash $\delta$ is checking:

$m \overset{?}{=} g^s y^{r'} r \bmod \rho$,

And verify the commitment $\delta_1$ is checking:

$m \overset{?}{=} g^{s_1} y_1^{r_1'} r_1 \bmod \rho$.

Construct $\delta$ using $x_2$ and $\delta_1$ is as follow: First, bank $i$ verifies $\delta_1$: $(r_1, s_1)$. If it is true, then construct an e-cash $\delta^*$: $(r^*, s^*)$, let $r^*$ and $s^*$ satisfy the follow relation:

$r^* = r_1$, $r_1^{*\prime} = r_1 \bmod \mathrm{q}$, $s^* = s_1 + r_1^{*\prime} x_2 \bmod \rho$.

Finally, check $\delta^*: (r^*, s^*) = \delta: (r, s)$.

If everything is in order, bank $i$ authorize consumer's construction of arithmetic scheme, send $V_C$ and $C_{\mathrm{CA}}$ to consumer.

$\mathrm{CA}_C = (E_{x_{B_i}}(y) \parallel \mathrm{CA}_{B_i})$, $\mathrm{CA}_{B_i} = E_{x_B}(y_{B_i})$ is a certification of bank $i$ from nation bank. $E_{x_{B_i}}(y)$ is a signature of branch bank $i$. $y$ is a public key used to verify the e-cash produced by consumer.

$V_C = \mathrm{sig}_{B_i}(y_1 \parallel N \parallel E_\Psi(x_2 \parallel \mathrm{ID_C}))$ is a signature of branch bank $i$. $y_1$ is a public key used to verify the commitment to the exchange issued by consumer. $N$ stipulates the largest value of an e-cash which consumer can overdraft based on credit. If the number of consumers is large, it requires bank $i$ to securely store a correspondingly large number of secret arbitration key $x_2$ (one for each consumer). This can be avoided by using the following technique: Bank $i$ concatenate $x_2$ and consumer's unique identification, $\mathrm{ID_C}$, to form $(x_2 \parallel \mathrm{ID_C})$, and then encrypt this value via some symmetric-key encryption algorithm $E_\Psi$, where $\Psi$ denotes the secret key. Bank $i$ then creates a signature of the concatenated value of $y$ and $E_\Psi(x_2 \parallel \mathrm{ID_A})$. That is, $\mathrm{sig}_{B_i}(y \parallel E_\Psi(x_2 \parallel \mathrm{ID_C})$, where $\mathrm{sig}_{Bi}(\cdot)$ denotes a signature algorithm of bank $i$. This value is used as the voucher $V_C$: $V_C = \mathrm{sig}_{B_i}(y_1 \parallel \mathrm{N} \parallel \cdot E_\Psi(x_2 \parallel \mathrm{ID_C}))$. Now, Bank $i$ can extract $x_2$ from $V\mathrm{c}$ (using $\Psi$), and only needs to securely store $\Psi$.

By the end of which either one of the parties aborts, or consumer learns $(x, y)$, $(x_1, y_1)$, $x_2$, $V_C$, $C_{\mathrm{CA}}$, bank $i$ learns his secret arbitration key $x_2$, and $y$, $y_1$, $x_2$, $V_C$, $C_{\mathrm{CA}}$.

### 2.2 Exchange Process

This is an interactive protocol between consumer and merchant. We assume that national bank's public key $y_B$ is open. Consumer initiates the protocol with merchant. We assume that consumer and merchant have gone through a negotiation process to agree on the purchase information $m$ (which might contain consumer's unique identity, merchant's unique account number, price of the merchandise, description of the merchandise, and date of transaction) prior to the start of the exchange protocol. This process may be as simple as consumer choosing fixed-priced goods from merchant's website. Note that consumer's digital signature on $m$ (which is $\delta$) acts as e-cash. In addition, consumer and merchant agree on a session key using some key-agreement protocol (e. g. , Diffie-Hellman key agreement). The session key is used to encrypt the digital merchandise to deter eavesdropping. Figure 5 shows the messages exchanged between consumer and merchant in the exchange protocol when both parties act honestly.

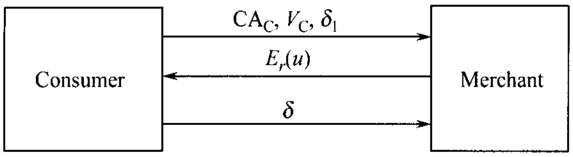

**Fig. 5  The exchange protocol**

1) Consumer select a random number $k$, and compute $\delta_1(r_1, s_1)$:

$r_1 = mg^{-k} \bmod \rho, r_1' = r_1 \bmod q$, $s_1 = k - r_1'x \bmod \rho$.

Consumer sends $\delta_1$, $C_{CA}$ and $V_C$ to merchant.

2) Merchant verifies $CA_C$, $V_C$ and $\delta_1$.

In order to verify $CA_C = (E_{x_{B_i}}(y) \| CA_{B_i})$, firstly, merchant verifies $CA_{B_i}$ using national bank open public key $y_B$, then obtain the public key $y_{B_i}$ of bank $i$ from $CA_{B_i}$, and use $y_{B_i}$ to verify $E_{x_{B_i}}(y)$. Finally, merchant obtains the consumer's public key $y$ from $E_{x_{B_i}}(y)$.

Merchant can verify $V_C = \text{sig}_{B_i}(y_1 \| N \| E_\Psi(x_2 \| \text{ID}_C))$ using $y_{B_i}$, obtain the public key $y_1$ and $N$ from $V_C$. $N$ stipulates the largest value of an e-cash which consumer can overdraft based on credit.

Merchant can verify the commitment $\delta_1$ is checking $m \overset{?}{=} g^{s_1} y_1^{r_1'} r_1 \bmod \rho$ using $y_1$, and check whether the sum of accounts is out of $N$.

If everything is in order, merchant encrypts the digital merchandise $u$ with some symmetric encryption algorithm $E_r(\cdot)$, where $r$ is the secret encryption key (i. e. , the session key). The encrypted merchandise $E_r(u)$ is sent to consumer. However, if any one of the items received from consumer is invalid, merchant does not send the merchandise, and stops the protocol.

3) Consumer decrypts and verifies the merchandise. If consumer is satisfied with the merchandise, he computes the e-cash $\delta(r, s)$: $r = mg^{-k} \bmod \rho$, $r' = r \bmod q$, $s = k - r'x \bmod \rho$, $k \in_R Z_p^*$, and send it to merchant. Otherwise, consumer stops the protocol.

4) Merchant verifies $\delta$ using $y$:

Check: $m \overset{?}{=} g^s y^{r'} r \bmod \rho$.

If it is valid, merchant ends the protocol. Otherwise, merchant initiates the dispute resolution protocol.

## 2.3 Deposit Process

Merchant deposit e-cash process showing in Fig. 6.

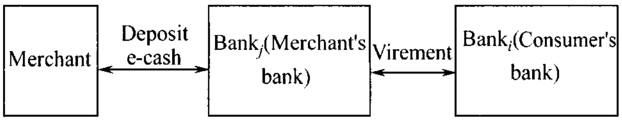

**Fig. 6  Merchant deposit e-cash process**

Merchant sends the e-cash and $CA_C = (E_{x_{B_i}}(y) \| CA_{B_i})$ to bank $j$ (merchant's bank).

Bank $j$ verifies $CA_{B_i}$ using $y_B$, verifies $E_{x_{B_i}}(y)$ using $y_{B_i}$, verifies e-cash $\delta$ using $y$. If the $\delta$ has not been deposit, bank $j$ deposit it for merchant in her accounts. In each e-cash, there are unique random number and period of validity. The bank can check the unique random number and period of validity to avoid the e-cash be redeposited by merchant.

If the e-cash is validity, bank $j$ request bank $i$ to transfer financing from consumer's accounts. Bank $i$ automatic provide a loan to consumer.

## 2.4 Dispute Resolution Process

If merchant does not receive the e-cash $\delta$, or if $\delta$ is invalid, he initiates a dispute resolution protocol by contacting bank $i$. We assume that reliable channels exist between the parties. The following steps describe the dispute resolution protocol.

1) Merchant encrypts the session key $r$ using $y_{B_i}$ as $E_{y_{B_i}}(r)$, and $E_{y_{B_i}}(\cdot)$ is an asymmetric encryption algorithm. Merchant then sends $V_C$, $CA_C$, $\delta_1$, $m$, $E_r(u)$ and $E_{y_{B_i}}(r)$ to bank $i$.

2) Bank $i$ decrypts $E_{y_{B_i}}(r)$ using his private key $x_{B_i}$, and uses $r$ to recover $u$. Next, he extracts all the system parameters and keys from $CA_C$ and $V_C$, and then verifies $\delta_1$ using those values. If everything is in order, bank $i$ generates the e-cash $\delta(r, s)$ using $\delta_1$ and his secret arbitration key $x_2$ as follow: $r = r_1$, $r_1' = r_1 \bmod q$, $s = s_1 + r_1'x_2 \bmod \rho$.

The multi-signature $\delta$ is sent to merchant, and the (encrypted) merchandise is forwarded to consumer. Otherwise, if any of the items received from merchant is invalid, bank $i$ halts the dispute resolution protocol without sending anything to either party.

# 3 Analysis

Security against the registration follows unconditionally. In our scheme, consumer has $\rho$, $q$, $g$, $x$, $x_1$, $x_2$, $y$, $y_1$, $V_C$ and $CA_C$, bank $i$ has $\rho$, $q$, $g$, $x_2$, $y$ and $y_1$. Indeed, if bank $i$ accepted the values ($\rho$, $q$, $g$, $y$, $y_1$, $\delta$,

$\delta_1$, $x_2$, $\mathrm{ID_C}$) in the registration, it means that $m=g^s y^{r'} r \bmod \rho$, $m=g^{s_1} y_1^{r_1'} r_1 \bmod \rho$ and $s=s_1+r_1' x_2 \bmod \rho$ is valid. Also, any valid commitment signature $\delta_1=(r_1, s_1)$ satisfies $r_1=mg^{-k} \bmod \rho$, $r_1'=r_1 \bmod q$, $s_1=k-r_1'x \bmod \rho$. Therefore the resolved e-cash signature $\delta=(r, s)$: $r=r_1 \bmod q$, $s=s_1+r_1'x_2 \bmod \rho$ satisfies $x_2=x_1-x$, and thus must pass the usual verification algorithm. Bank $i$ can't obtain $(x, x_1)$ in the registration. So, the registration is security.

Security against the exchange follows unconditionally. In the exchange process, consumer sends merchant ($\mathrm{CA_C}$, $V_C$, $\delta_1$, $\delta_2$), merchant can't obtain ($x$, $x_1$, $x_2$). Besides, consumer uses a random number $k$ in every signature. The $k$ has no effect to merchant and bank $i$ for verifying. Merchant has no other way to produce the signature $\delta$ and $\delta_1$. If merchant does not receive the multi-signature $\delta$ (in step 3 of exchange protocol), or if $\delta$ is invalid (in step 4), he can obtain (from bank $i$ by initiating the dispute resolution protocol. If consumer does not receive the merchandise (in step 2 of exchange protocol), she lost nothing. Because the value $\delta_1$ sent to merchant in step 1 has no intrinsic value, but serves as consumer's commitment to the exchange. So, we can see during the exchange process, there is no party losing benefits.

As mentioned above, we can draw a conclusion that our scheme is secure. The scheme can avoid the problem of partition e-cash to give changes. In our scheme, the e-cash is produced by consumer according to the exchange, it does not need to give changes.

The scheme can prevent from reusing e-cash and faking e-cash. There is no need for consumer to reuse e-cash, for the e-cash is produced by him, and there is no value for him to reuse it. Merchant can not re-deposit the e-cash. In each e-cash, there are unique random number and period of validity. The bank can check the unique random number and period of validity to avoid the e-cash be re-deposited by merchant. Nobody can fake the e-cash. For the consumer, he can not fake an e-cash, because he can not fake another legal private key to produce e-cash, and there is benefit for him to do it. For the other parties, they can not fake an e-cash, because they can not obtain consumer's private key.

The scheme fulfills non-deny. There are signatures in exchange information, merchant has consumer's commitment, e-cash produced by consumer himself and no others can fake it, so the consumer can not deny. The scheme fulfills impartiality. As mentioned above, we can see during the exchange process, there is no party losing benefit even if one party quit in any time. So it is impartiality. The scheme fits anonymity. The consumer's identity is encrypted by bank. So, the consumer is anonymity to merchant. For consumer there no need to know the merchant's identity, so, merchant may keep anonymity to consumer.

The scheme fits justice. If needed, (for example, the law request), bank can release the consumer's anonymity from e-cash produced by consumer.

The efficiency and other aspect of the scheme: there is not concerned with bank in the exchange process and e-cash produce process. This can depress the bottleneck of exchange. Finally, as the e-cash is produced by user, it avoids the storage and lose problem.

The shortage of the scheme: the bank should evaluate consumer's credit and define an equal overdraft credit certificate. There is a certain risk for bank.

## References

[1] Chaum D. Blind Signatures for Untraceable Payments. In: Chaum D, Rivest R L, Sherman A T Eds. *Advances in Cryptology-CRYPTO'82*. Santa Barbara, New York: Plenum Press,1983. 199-203.

[2] Chaum D, Fiat A, Naor M. Untraceable Electronic Cash (Extended Abstract). In: Goldwasser S Ed. *Advances in Cryptology-CRYPTO'88 Proceedings*. Santa Barbara, New York: Springer-Verlag Press,1988. 319-327.

[3] Brands S. An Efficient Off-line Electronic Cash System Based on the Representation Problem. Technical Report CS-R9323, Amsterdam: CWI (Centre for Mathematics and Computer Science), 1993.

[4] Brands S. Untraceable off-line electronic cash in wallet with observers. In: Feigenbaum J Ed. *Advances in Cryptology-CRYPTO'93*. New York: Springer-Verlag Press,1994. 302-318.

[5] Ferguson N. Single term off-line coins. In: Brickell F ed. *Advances in Cryptology- EUROCRYPT'93*. Berlin: Springer-Verlag Press, 1994. 318-328.

[6] Franklin M, Yung M. *Towards Provably Secure Efficient Electronic Cash*. Report CUCS-018-92, New York: Columbia University, Department of Computer Science, 1992.

[7] Matthew,Franklin K, Yung M. Secure and Efficient Off-line Digital Money. In: Carlsson S, Lingas A, Karlsson R G Eds. *Automata,Languages and Programming*. Lund,Sweden: Springer-Verlag Press,1993. 265-276.

[8] Shaobin W, Fan H, Xian Z. Optimistic Fair-Exchange Protocols Based on DSA Signatures. In: Alamitos L Ed. *Proceedings-*2004 *IEEE International Conference on Services Computing, Shanghai*. Newzealand: IEEE Computer Society Press, 2004. 498-501.

□