A Secure and Efficient Off-line Electronic Transaction Protocol

Constantin Popescu
Department of Mathematics and Computer Science, University of Oradea
Oradea 410087, Romania
cpopescu@uoradea.ro

Abstract: In this paper we propose a secure and efficient off-line electronic transaction protocol based on an ID-based public key encryption system and group signature schemes, which is constructed from bilinear pairings. The anonymity of the customer is revocable by a trustee in case of dispute. Because the amount of communication in the payment protocol is about 1280 bits, our off-line electronic transaction protocol can be used in the wireless networks with the limited bandwidth or the limited-storage environment such as smart card.

Keywords: Cryptography, protocol, electronic cash system, bilinear pairings, group signatures.

1. Introduction

Recently, a variety of on-line businesses are rapidly emerging over the Internet, which are considered to be some of the most efficient and convenient ways to provide all electronic services. An efficient and secure electronic transaction protocol plays an important role to support these businesses safely as a trustful payment over the Internet.

Since Chaum proposed untraceable electronic cash systems based on blind signatures in 1982 [1], various extended systems have been proposed, which provide functionalities such as anonymity, double spending prevention, unforgeability, untraceability and efficiency [2], [3], [4], [5], [6]. Off-line electronic cash systems were first introduced in [7] and then developed further in [8], [9], [10], [11], [12], [13]. In these cases the bank's involvement in the payment transaction between a customer and a merchant was eliminated. Customers withdraw electronic coins from the bank and use them to pay a merchant (a shop). The merchant subsequently deposits the coins back to the bank. Most off-line electronic cash systems use a restricted form of blind signatures to implement anonymity. The revocable e-cash system [14], [15] (or fair payment system) in which anonymity can be revoked when needed, becomes one of the active research areas of preventing such misuses. In the revocable e-cash scheme, the identification of an illegal user can be traced by the cooperation of a trustee and a bank.

Along with countermeasures [14], [16] against the blackmailing and money laundering, many schemes in [15], [17], [18] have been proposed to resist against the abuse of anonymity. The scheme suggested by Camenisch et al. [19] requires the trustee to take part in the initialization phase but does not provide a prevention against extortion and blindfolding attacks. Some schemes were suggested to prevent these attacks. Fujisaki and Okamoto's scheme [17] and Jakobsson and Yung's scheme [18] are said to be not efficient in the sense that the users need to communicate with a trustee in every payment phase. Recently, Wang, Cao and Zhang [20] proposed an off-line payment scheme in which the anonymity of consumers is scalable. Consumers can get the required anonymity without showing their identities to any third party. However, the authors in [21] show that in Wang, Cao and Zhang's scheme, given a valid coin and without knowing any secret information, everyone is able to spend the coin as many times as he wants.

In this paper we propose a secure off-line electronic transaction protocol based on an ID-based public key encryption system and group signature schemes. In order to construct our electronic cash system, we use the group signature of X. Chen, F. Zhang, K. Kim [22] and the blind signature of Schnorr [23]. The proposed off-line electronic cash system is provable secure. Its security is based on the ID-based public key encryption system [24], which is constructed from bilinear pairings. We discuss some aspects of security of our off-line electronic cash system, such as: the anonymity of the customer and the security against the forgery of the coin. Because the amount of communication in the payment protocol is about 1280 bits, our off-line electronic

transaction protocol can be used in the wireless networks with the limited bandwidth or in the Internet environment (payments using smart cards).

The rest of this paper is organized as follows. In the next section we review the properties of bilinear pairings and group signatures. Then we present our off-line electronic transaction protocol in section 3. Furthermore, we discuss some aspects of security and efficiency in section 4. Finally, section 5 concludes the work of this paper.

2. Cryptographic Tools

In this section we review bilinear pairings, the ID-based public key systems and the properties of a group signature scheme which will be used in the subsequent design of our off-line electronic transaction protocol.

2.1 Bilinear pairings

Let G_1 be a cyclic additive group generated by P of prime order q and G_2 be a cyclic multiplicative group of the same order q. Let $a,b \in Z_q^*$. We assume that the discrete logarithm problems in both G_1 and G_2 are hard. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: $e(aP,bQ) = e(P,Q)^{ab}$, for all $P,Q \in G_1$ and $a,b \in Z_q^*$.
2. Non-degenerate: There exist $P,Q \in G_1$ such that $e(P,Q) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(P,Q)$ for all $P,Q \in G_1$.

We first introduce the following problems in G_1:

1. Discrete Logarithm Problem (DLP): given 2 elements P, Q find an integer $r \in Z_q^*$ such that $Q = rP$.
2. Computational Diffie-Hellman Problem (CDHP): Given P, aP, bP, compute abP for $a,b \in Z_q^*$.
3. Decisional Diffie-Hellman Problem (DDHP): Given P, aP, bP, cP, decide whether $c \equiv ab \bmod q$ for $a,b,c \in Z_q^*$.

We call G_1 a gap Diffie-Hellman group if the Decisional Diffie-Hellman Problem can be solved in polynomial time but there is no polynomial time algorithm to solve the Computational Diffie-Hellman Problem or Discrete Logarithm Problem with non-negligible probability. Such a group can be found in supersingular elliptic curves of hyperelliptic curves defined over finite fields and the bilinear pairings can be derived from Weil or Tate pairings. For more details, see [25], [26].

2.2 ID-based public key setting from bilinear pairings

The ID-based public key systems, introduced by Shamir [24], allow some public information of the user such as name, address and email etc., rather than an arbitrary string to be used as his public key. The private key of the user is calculated by Private Key Generator (PKG) and sent to the user via a secure channel. ID-based public key setting from bilinear pairings can be implemented as follows [27], [22]:

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$. Define two cryptographic hash functions $h_1: \{0,1\}^* \to Z_q$, $h_2: \{0,1\}^* \to G_1$.

1. Setup Procedure: PKG chooses a random number $s \in Z_q^*$ and sets $P_{pub} = sP$. The center publishes systems parameters $\{G_1, G_2, e, q, P, P_{pub}, h_1, h_2\}$ and keeps s as the private master-key.
2. Extract Procedure: A user submits his/her identity information ID to PKG. PKG computes the user's public key as $Q_{ID} = h_2(ID)$, and returns $S_{ID} = sh_2(ID)$ to the user as his/her private key.

2.3 Group signatures

Group signature schemes are a relatively recent cryptographic concept introduced by Chaum and van Heyst [28] in 1991. An application of a group signature scheme is the electronic cash as it was pointed out in [29]. In this case, several banks issue coins, but it is impossible for shops to find out which

bank issued a coin that is obtained from a customer. The central bank plays the role of the group manager and all other banks issuing coins are group members.

A group signature scheme is comprised of the following procedures:

1. **Setup**: an algorithm that generates the group public key and a group secret key for the group manager.
2. **Join**: a protocol between the group manager and a potential member that generates the user's secret key and public key.
3. **Sign**: a protocol between a group member and a user which, on input the message m from the user and the signer's secret key, the membership certificate and membership key, produces a signature on the message m.
4. **Verify**: an algorithm which, on input the group public key and the group signature for the message, decides the validity of the signature.
5. **Open**: an algorithm which, given a signed message and a group secret key, returns the identity of the signer together with a proof of this fact.

A group signature scheme [30] allows the members of a group to sign messages on behalf of the group such that the following properties hold:

1. Correctness: Signatures produced by a group member using the sign procedure must be accepted by the verify procedure.
2. Unforgeability: Only group members are able to sign messages on behalf of the group.
3. Anonymity: Given a signature, identifying the actual signer is computationally hard for everyone but the group manager.
4. Unlinkability: Deciding whether two different signatures were computed by the same group member is computationally hard.
5. Traceability: The group manager can always establish the identity of the member who issued a valid signature.
6. No framing: Even if the group manager and some of the group members collude, they cannot sign on behalf of non-involved group members.
7. Coalition-resistance: A colluding subset of group members cannot generate a valid signature that the group manager cannot link to one of the colluding group members.

3. Proposed Off-line Protocol

The proposed protocol consists of four types of participants: customers, merchants, banks and trusted parties. The customers honestly withdraw money from the bank and pay money to the merchant. The merchants get money from customers and deposit it in the bank. The banks manage customer accounts, issue and redeem money. The bank can legally trace a dishonest customer with the help of the trusted parties. An e-cash system is anonymous if the bank in collaboration with the merchant cannot trace the coin to the customer. The system is off-line if during payment the merchant does not communicate with the bank.

In our off-line electronic transaction protocol, all customers who open a bank account form a group and a Private Key Generator (trusted party) is the group manager. We assume that in our electronic cash system, the group manager is a trusted party like the country's Central Bank (e.g. the US Treasury). When a customer wants to withdraw an electronic coin from his account, the bank applies a blind signature protocol [23] to this coin and decreases appropriate amount from the customer's account. Everyone including the merchant can verify the validity of the blind signature. The withdrawals are made by the bank by applying the blind signature of Schnorr [23] to a coin randomly selected by a customer and the payments are made by the customer by applying the group signature of Chen, Zhang, Kim [22] to the random coin. We use a group signature scheme in our protocol for the following reasons. First, we need the traceability of a group signature scheme in the tracing protocol. The group manager can trace the identity of the customer who makes a double spending and sends it to the bank. Second, in our registration protocol, we use the Join procedure of a group signature scheme, that is, any customer who wants to withdraw a coin from the bank has to interact with the group manager and obtains a membership certificate.

3.1 System setup

Let G_1 be a Gap Diffie-Hellman group generated by P, whose order is a prime q, G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$. We define three cryptographic secure hash functions $H_1: \{0,1\}^* \times G_1 \to Z_q$, $H_2: \{0,1\}^* \times G_1 \to G_1, H_3: \{0,1\}^* \to Z_q$. We remark that H_1, H_2 and H_3 have distinct ranges. For the case of H_2 the range is a Gap Diffie-Hellman group G_1. The process for selecting the parameters and generating G_1, G_2, q, e, P is given in [25].

The Group Manager:
To setup his parameters, the group manager performs the following:

1. Chooses a random number $s \in Z_q^*$ and sets $P_{pub} = sP$.
2. Keeps s as his master-key.
3. Publishes the group public key $Y = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$.

The Bank:
To setup his parameters, the bank performs the following:

1. Selects a random secret x_b from the interval $[1, q-1]$.
2. Calculates the point $P_b = x_b P$
3. The public key of the bank is P_b.
4. The corresponding secret key is x_b.

3.2 The registration protocol

Any customer who wants to withdraw a coin from the bank has to interact with the group manager and obtains a membership certificate. We assume that communication between the customer and the group manager is secure, i.e., private and authentic.

1. The customer submits his/her identity information ID to the group manager. The customer also chooses a random number $r \in Z_q^*$ as his long-term private key, computes rP and sends it to the group manager.
2. The group manager computes $S_{ID} = sH_2(ID \| T, rP)$, where T is the life of the customer's long-term private key r. (Since the value of T can be used by the bank as a convert channel to track this customer, the group manager, say, can fix an expiring date to be used by all cash issued during 2010). The group manager sends S_{ID} and T to the customer.
3. The customer randomly chooses $x_u \in Z_q^*$ and computes $P_u = x_u P$ and $rx_u P$. He then sends P_u and $rx_u P$ to the group manager.
4. The group manager checks if $e(rx_u P, P) = e(rP, x_u P)$, and then sends $S = sH_2(T, rx_u P)$ to the customer.
5. The customer's member certificate is $(S, rx_u P)$ and his private signing key is rx_u.
6. The group manager adds $rx_u P$, $x_u P$, rP and ID to the customer list.

3.3 The withdrawal protocol

The withdrawal protocol allows a customer to withdraw e-coins from the bank. After having open a bank account, the customer withdraws an e-coin from his account by using blind signature. Therefore, the bank cannot link the e-coin to the identity of the customer but can debit to the account correctly. The withdrawal protocol involves the customer and the bank in which the customer withdraws an electronic coin from the bank. First, the customer proves his identity to the bank and then the bank uses blind Schnorr signature [23] to sign the e-coin. Also, we assume that communication between the customer and the bank is secure, i.e., private and authentic [31], [32].

The customer must perform the following protocol with the bank:

1. The customer sets his electronic cash requirement: $m = H_3(\text{withdrawalrequire} \| ID)$, where ID is the identity of the customer. Then, the customer chooses a random value $k_u \in [1, q-1]$ and signs the message m using the elliptic curve signature scheme of Schnorr [33]:

$$r_u = H_1(k_u P, m) \quad (1)$$

$$s_u = k_u - r_u x_u \bmod q. \quad (2)$$

The customer sends m, P_u and the signature (r_u, s_u) to the bank.
2. The bank checks that the following equality holds:

$r_u = H_1(s_u P + r_u P_u, m).$ (3)

3. Then, the bank uses blind Schnorr signature [23] to sign the e-coin: selects $k' \in [1, q-1]$, computes the point $R = k'P$ and sends R to the customer.
4. The customer establishes a random coin c, randomly selects $\alpha, \beta \in [1, q-1]$, computes $R_b = R + \alpha P + \beta P_b, c_b = H_1(c \| \alpha, R_b)$ and blinds the e-coin by computing $c' = c_b - \beta \bmod q$. The customer sends the value c' to the bank.
5. The bank computes: $s' = k' - c' x_b \bmod q$ and forwards s' to the customer.
6. The customer computes $s_b = s' + \alpha \bmod q$. The pair (c_b, s_b) is a valid e-coin signature issued by the bank.
7. The customer verifies the blind signature (c_b, s_b) of the coin c, issued by the bank, by checking that the following equation holds:

$s_b P + c_b P_b = R_b$ (4)

8. The blind signature of the coin c is the pair (c_b, s_b).

The customer gets the coin c from his account.

3.4 The payment protocol

In the proposed off-line transaction protocol, during payment the merchant does not communicate with the bank. The payment protocol involves the customer and the merchant and should be done through a secure channel (i.e., data privacy and integrity). After withdrawing e-coins, the customer can pay for what the merchant provided. Then the merchant verifies the validity of the received e-coins.

In order to sign the coin c, the customer uses the group signature scheme of Chen, Zhang, Kim [22]:

1. The merchant sends challenge $c_m = H_3(ID_m \| time)$ to the customer, where ID_m is the merchant's identity and *time* is the recorded time of the transaction.
2. The customer chooses a random $z \in Z_q^*$ and computes

$U_1 = zH_2(T, rx_u P)$ (5)

3. The customer computes:

$c_u = H_3(c \| c_b \| s_b \| c_m)$ (6)

$U_2 = rx_u H_2(c_u, U_1)$ (7)

$h = H_1(c_u, U_1 + U_2)$ (8)

$U_3 = (z + h)S$ (9)

4. The customer sends c, c_b, s_b and the signature $\sigma = (c_u, U_1, U_2, U_3, T, rx_u P)$ of the coin c to the merchant.
5. The merchant verifies the signature $(c_u, U_1, U_2, U_3, T, rx_u P)$ of the coin c as follows:
   a) Computes $H_2(T, rx_u P)$, $H_2(c_u, U_1)$ and $h = H_1(c_u, U_1 + U_2)$
   b) Tests if the following equations hold:

$e(U_3, P) = e(U_1 + hH_2(T, rx_u P), P_{pub})$ (10)

$e(U_2, P) = e(H_2(c_u, U_1), rx_u P)$ (11)

$c_u = H_3(c \| c_b \| s_b \| c_m)$ (12)

If the equations (10), (11) and (12) fail, then the merchant terminates the transaction.

The merchant needs to verify if $c_u = H_3(c \| c_b \| s_b \| c_m)$ because the old signature $(c_u, U_1, U_2, U_3, T, rx_u P)$ of used coin still can pass verification of (10) and (11). The merchant needs to check the linkage of the new coin and its signature.

3.5 The deposit protocol

The deposit protocol permits the merchant to deposit the received e-coins to the bank. When receiving the deposited requirement from the merchant, the bank first verifies the validity of received e-coins and then credits the account of the merchant.

In the on-line e-cash system this protocol is part of the payment protocol as executed by the merchant. In our system, the deposit protocol is executed at a later moment, preferably in batch mode. The bank holds a record of spent cash to prevent double spending of e-cash. The bank cannot link deposited coins to a customer without collaboration from the group manager.

The deposit protocol involves the merchant and the bank as follows:

1. The merchant sends c, c_u, c_b, s_b and c_m to the bank.
2. The bank verifies the signature as given in the equation (6).
3. After verification succeeds, the bank checks if c obtained from the merchant exists in its database. If the coin c is in the database of the bank, then the bank finds the signature σ' for the deposited

coin in its database and sends it to the merchant (detection of double spending).

4. If the merchant receives σ' from the bank, he/she checks whether $\sigma' = \sigma$. If $\sigma' = \sigma$, then the merchant rejects performing protocol (double spending). Otherwise, the merchant sends $U_1, U_2, U_3, T, rx_u P$ and *time* to the bank.
5. The bank verifies the validity of the signature $\sigma = (c_u, U_1, U_2, U_3, T, rx_u P)$ using the equations (10) and (11).
6. If the signature $(c_u, U_1, U_2, U_3, T, rx_u P)$ of the coin c is valid, then the bank accepts the coin c. Then, the bank will deposit the cash to the merchant's account and the merchant sends the goods to the customer. The bank stores c and $(c_u, U_1, U_2, U_3, T, rx_u P)$ in its database.
7. If the bank finds out that c and $(c_u, U_1, U_2, U_3, T, rx_u P)$ has been stored before but different *time* and c_m, then the coin c has been double spending. The bank performs the tracing protocol and detects the identity of the double spender with the help of the group manager.

3.6 The tracing protocol

The bank can legally trace the customer of a paid coin with the help of the group manager. The tracing protocol involves the bank and the group manager as follows:

1. The bank sends the signature $(c_u, U_1, U_2, U_3, T, rx_u P)$ of the coin c to the group manager.
2. The group manager verifies the signature $(c_u, U_1, U_2, U_3, T, rx_u P)$ using the equations (10) and (11).
3. The group manager can easily identify the customer from $rx_u P$. The group manager can provide a proof that it is indeed the customer's signature from the following equations:

$$e(rx_u P, P) = e(x_u P, rP) \quad (13)$$

$$e(S_{ID}, P) = e(H_2(ID \| T, rP), P_{pub}) \quad (14)$$

4. The group manager searches through the group customer list to get the identity of the customer and sends it to the bank.

Also, the group manager cannot misattribute a signature to frame the customer unless he can compute bP given P, aP and rP which satisfies:

$$a \equiv rb \bmod q \quad (15)$$

The authors in [22] define this problem the Reversion of Computation Diffie-Hellman Problem. They prove that the Reversion of Computation Diffie-Hellman Problem is equivalent to Computational Diffie-Hellman Problem in G_1.

4. Security and Efficiency Analysis

In this section we discuss some aspects of security and efficiency of our off-line electronic transaction protocol. The following theorem proves the anonymity of our system.

Theorem 1 Our off-line electronic transaction protocol achieves anonymity w.r.t. the bank, i.e., it is infeasible for the bank to trace a customer without the cooperation of the group manager.

Proof: The identity of a honest customer is anonymous and cannot be linked with the e-cash. However, the customer who makes a double spending will be traced by the bank with the help of the group manager using the tracing protocol. In this case, the group manager searches through the group customer list to get the identity of the customer and sends it to the bank. For an honest customer, the Schnorr blind signature will be used when he withdraws the coin c from the bank, so that the bank cannot link a coin to the honest owner of the coin without the group manager's help. Since x_u is randomly chosen, then $rx_u P$ reveals no information about the customer's identity to anyone except the group manager. Also, since $c_u = H_3(c \| c_b \| s_b)$ and the blind signature (c_b, s_b) of the coin c cannot give any information for the coin c, the bank cannot link the blind coin with the identity of the customer.

Theorem 2 Security against forgery of the coin c: The proposed off-line transaction protocol is secure against forgery of the coin c.

Proof: Since the Schnorr's blind signature is secure against existential forgery [23], this allows only the legal bank to generate the signature for the coin c. As the hash function H_1 has the feature of collision free (The hash function is called collision free if it is infeasible

to generate two distinct inputs with matching outputs), the customer cannot find a value $c'' \neq c$ with $H_1(c'' \| \alpha, R_b) = H_1(c \| \alpha, R_b)$. Thus, the proposed off-line transaction protocol satisfies unforgeability of coins.

and merchant is about 1280 bits, the proposed off-line transaction protocol can be used in the wireless networks with the limited bandwidth or in the limited-storage environment such as the smart card.

Table 1. Comparison of the transaction protocols - Storage space

	Our protocol	Au [2]	Canard [3]
Withdrawal Protocol	1120 bits	8160 bits	6420 bits
Payment Protocol	1280 bits	5188 bits	30740 bits
Deposit Protocol	1440 bits	5164 bits	27648 bits

Table 2. Comparison of the transaction protocols - Computation cost

		Our protocol	Au [2]	Canard [3]
Withdrawal Protocol	multi-EXP	7	2156	5
	Pairing	0	22	0
Payment Protocol	multi-EXP	1	800	1673
	Pairing	4	14	0
Deposit Protocol	multi-EXP	0	10	14
	Pairing	4	0	0

We evaluate the storage space and computational time of the costly operations. Table 1 and Table 2 summarize the storage space and computation cost respectively, of different protocols of our system and the schemes in [2] and [3]. The overall efficiency is improved in our electronic transaction protocol compared to Au et al.'s system [2] and Canard et al.'s system [3] in terms of the storage space and the computation cost. Our protocol has a point P of 160 bits and q of 160 bits. For a moderate value $L = 10$ and $t = 40$, the payment protocol in [3] requires 1673 multi-based exponentiations and a total bandwidth of 30740 bits. The payment protocol in [2] requires 800 multi-based exponentiations, 14 pairings and a total bandwidth of 5188 bits. In contrast, the payment protocol in our system requires 1 multi-based exponentiation, 4 pairings and a total bandwidth of 1280 bits.

5. Conclusions

In this paper we presented a secure and efficient off-line electronic transaction protocol based on a ID-based public key encryption system and group signature schemes. In order to construct our off-line electronic transaction protocol, we used the group signature of Chen, Zhang, Kim and the blind signature of Schnorr. Because the amount of communication between customer

REFERENCES

1. CHAUM D., **Blind Signature for Untraceable Payments**, Proc. of Eurocrypt'82, Plenum Press, 1983, pp. 199-203.
2. AU M., W. SUSILO, Y. MU, **Practical Anonymous Divisible e-Cash from Bounded Accumulators**, Proc. of Fin. Cryptography and Data Security, 2008.
3. CANARD S., GOUGET A., **Divisible e-Cash Systems Can Be Truly Anonymous**, Proceedings of Eurocrypt 2007, pp. 482-497.
4. FUN C., **Ownership-attached Unblinding of Blind Signatures for Untraceable Electronic Cash**, Information Science, 2006, pp. 263-284.
5. KU C., C. TSAO, Y. LIN, C. CHEN, **An Escrow Electronic Cash System with Limited Traceability**, Information Science, 2004, pp. 17-30.
6. TROLIN M., **A Universally Composable Scheme for Electronic Cash**, Proc. of Indocrypt, 2005, pp. 347-360.
7. CHAUM D., FIAT A., NAOR M., **Untraceable Electronic Cash**, Proc. of the Crypto'88, 1990, pp. 319-327.
8. FRANKLIN M., YUNG M., **Secure and Efficient Off-line Digital Money**, Proc. of the 20th Intl. Colloq., Languages and Programming, 1993, pp. 265-276.

9. LEE M., G. AHN, J. KIM, J. PARK, B. LEE, K. KIM, H. LEE, **Design and Implementation of an Efficient Fair Off-line e-Cash System Based on Elliptic Curve Discrete Logarithm Problem**, Journ. of Comm. and Networks 4, 2002, pp. 81-89.
10. OKAMOTO T., K. OHTA, **Universal Electronic Cash**, Proc. of the 11th Ann. Intl. Cryptology Conf. on Advances in Cryptology, 1992, pp. 324-337.
11. OKAMOTO T., **An Efficient Divisible Electronic Cash Scheme**, Proc. of Crypto'95, pp. 302-318.
12. POPESCU C., **A Fair Off-line Electronic Cash System Based on Elliptic Curve Discrete Logarithm Problem,** Studies in Informatics and Control, Vol. 14(4), 2005, pp. 291-298.
13. POPESCU C, **An Electronic Cash System Based on Group Blind Signatures**, Informatica 17(2006), pp. 551-564.
14. BRICKELL E., P. GEMMELL, D. KRAVITZ, **Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Exchange**, Proc. of 6th Ann. ACM-SIAM Symp. on Discrete Algorithms, 1995, pp. 457-466.
15. CAMENISCH J., M. PIVETEAU, M. STADLER, **An Efficient Fair Payment System**, Proc. of 3rd ACM Conf. on Computer and Commun. Security, ACM Press, 1996, pp. 88-94.
16. STADLER M., J. M. PIVETEAU, J. CAMENISCH, **Fair-blind Signatures**, Proc. of Eurocrypt'95, pp. 209-219.
17. FUJISAKI E., T. OKAMOTO, **Practical Escrow Cash System**, Proc. of Cambridge Workshop on Security Prot., 1997, pp. 3-48.
18. JAKOBSSON M., M. YUNG, **Revokable and Versatile e-Money**, Proc. of 3rd Ann. ACM Conf. on Computer and Commun. Security, 1996, pp. 76-87.
19. CAMENISCH J., U. MAURER, M. STADLER, **Digital Payment Systems with Passive Anonymity-Revoking Trustees**, Journal of Computer Security 5, 1997, pp. 69-90.
20. WANG H., CAO J., ZHANG Y., **A Flexible Payment Scheme and Its Role-based Access Control**, IEEE Trans. Knowledge Data Engeneering 17, 2005, pp. 425-436.
21. DE SANTIS A., A. L. FERRARA, B. MASUCCI, **An Attack on a Payment Scheme**, Information Sciences 178, 2007, pp. 1418-1421.
22. CHEN X., F. ZHANG, K. KIM, **A New ID-based Group Signature Scheme from Bilinear Pairings**, Journ. of Electronics 23, 2006, pp. 892-900.
23. POINTCHEVAL D., J. STERN, **Security Arguments for Digital Signatures and Blind Signatures**, Journ. of Cryptology 13, 2000, pp. 361-396.
24. SHAMIR A., **Identity-based cryptosystems and signature schemes**, Proc. of Crypto, 1984, pp.47-53.
25. BONEH D., M. FRANKLIN, **Identity-based Encryption from the Weil Pairings**, Proc. of Crypto 2001, pp. 213-229.
26. HESS F., **Efficient Identity Based Signature Schemes Based on Pairings**, Proc. of 9th Workshop on Selected Areas in Cryptogr., SAC 2002, pp. 310-324.
27. CHA J. C., J. H. CHEON, **An Identity-Based Signature from Gap Diffie-Hellman Group**, Proc. of PKC, Lecture Notes in Computer Science, 2003, pp. 18-30.
28. CHAUM D., E. VAN HEYST, **Group Signatures**, Proc. of Eurocrypt'91, pp. 241-246.
29. LYSYANSKAYA A., Z. RAMZAN, **Group Blind Signature: A Scalable Solution to Electronic Cash**, Proc. of Fin. Cryptogr., FC'98, pp. 184-197.
30. ATENIESE G., J. CAMENISCH, M. JOYE, G. TSUDIK, **A Practical and Provably Secure Coalition-Resistant Group Signature Scheme**, Proc. of Crypto 2000, pp. 255-270.
31. FLORIN L., M. H. ZAHARIA, D. GÂLEA, **Emergent Dynamic Routing Using Intelligent Agents in Mobile Computing**, Studies in Informatics and Control, Vol. 17(2), 2008.
32. POPESCU C., HOREA OROS, **An off-line electronic cash system with multiple banks**, Intl. Journ. of Computers, Commun. and Control, Suppl. Issue, 2006, pp. 386-392.
33. MENEZES A., **Elliptic Curve Public Key Cryptosystems**, Kluwer Academic Publishers, 1993.