IJICTR International Journal of Information & Communication Technology Research

Volume 8- Number 2- Spring 2016 (9-14)

A New Electronic Cash Protocol Using a Modified ElGamal and an Untraceable Signature Scheme

Ali Zaghian
Department of Mathematics
Malek-Ashtar university of Technology
Esfahan, Iran
a_zaghian@mut-es.ac.ir

Mohsen Mansouri
Department of Mathematics
Malek-Ashtar university of Technology
Esfahan, Iran
Mohsen.mlksh@gmail.com

Received: February 25, 2015- Accepted: March 2, 2016

Abstract— **In this paper, a new transaction protocol based on electronic cash using a modified ElGamal signature and a secure blind signature scheme is proposed. With the extension of untraceable electronic cash, a fair transaction protocol is designed which can maintain anonymity and double spender detection and attaches expiration date to coins so that the banking system can manage its databases more efficiently. The security of the system is based on discrete logarithm problem and factoring problem.Also our protocol has better performance than similar protocols. So the new protocol is very efficient.**

Keywords- digital signature; blind signature; ElGamal digital signature; RSA; electronic payment system; electronic voting system.

1. INTRODUCTION

Due to the ubiquity of the internet and wireless networks, the development of electronic commerce is growing up rapidly which speeds up on-line commodity circulation. Thus, safe and efficient conduct of electronic payment has become a critical problem which needs to be salved urgently. Many payment mechanisms, such as electronic cash (e-cash), credit cards, and electronic wallets, can fully protect the privacy of customers in various electronic transactions. The advent of E-commerce demands for secure communication of digital information. The widespread networks make electronic commerce more and more popular than before. Many businesses employ computers and networks to deal with the transactions of most commercial activities [1]. Along with the swift development of Internet, more and more people start to carry on commercial activities, such as securities trading, shopping, etc. The computerization of financial business and payment system indicates the development direction of finance. In a traditional transaction, a customer and a shop are face-to-face during the transaction, so that they can easily and fairly exchange the money and the goods at the same time. Compared with traditional payment schemes, electronic payment has many advantages, for example the convenience and the speediness, these advantages can be serious challenges to a schemes and their designer. Electronic commerce usually involves two distrusted parties exchanging their items, for instance an electronic check and an electronic ticket. A fair payment protocol allows two users to exchange items so that either both users get the exchanged items or neither user does. It has been proven throughout the years that this can be achieved by cryptography. Digital signature schemes are essential for E-commerce as they

allow one to authorize digital documents that are transferred across networks. A blind signature scheme [2], first introduced by Chaum, is a variant of digital signature scheme and plays an important role in many e-commerce applications. The blindness property plays a central role in applications such as electronic voting and electronic cash schemes where anonymity is of great concern. After Chaum [1] advanced the first electronic cash system in 1982, the electronic payment has gradually improved. In general, e-cash can be classified into two types, which are on-line e-cash [3-5] and off-line e-cash [6-17]. In electronic cash protocols, users must decide which type of e-cash they will use later when withdrawing. If a user withdraws an on-line e-cash, she/he cannot spend it in those shops which only accept off-line e-cash. In 2013, Baseri et al. proposed a secure untraceable off-line electronic cash system [24]. They claimed that their scheme could achieve security requirements of an e-cash system such as, untraceability, anonymity, unlinkability, double spending checking, un-forgeability, date-attachability, and prevent forging coins. They further prove the un-forgeability security feature by using the hardness of discrete logarithm problems. But, in 2016, Baoyuan Kang and Danhui Xu show that Baseri, et al., 's scheme is suffering from some faults in anonymity, expiration date and merchant frauds [25]. To improve Baseri, et al., 's scheme, they also propose a new untraceable off-line electronic cash scheme. The new scheme not only possesses the features, such as anonymity, unforgeability, unreusability, but also possesses the feature of avoiding merchant frauds. In this paper, relying on a proposed blind signature scheme in [18], a new untraceable off-line blind signature-based electronic cash scheme is proposed. It is shown that payment protocol in the proposed scheme via a new ElGamal signature scheme is introduced, detects double-spending if and only if the e-coin can only be used once. The propose scheme is compared to [19] in section 5, to show that it is better. The new scheme has features of a fair e-cash scheme, for example:

Anonymity: A user will not possess anonymity if she/he commits a crime. Therefore if a coin is spend legitimately, neither the recipient nor the bank can identify the user.

Unreusability: The digital cash cannot be copied or reused.

Unforgeability: Only a bank can produce digital coins

Off-line Payment: No communication with the central bank is needed during the transaction.

The proposed scheme attaches an expiration date to each coin. This feature can greatly reduce the size of the databases the bank has to manage. Also it is shown in Section 5.3 that if a coin is spent twice, the user's identity is revealed efficiently. The security of the scheme comes from the difficulty of the discrete logarithm problem and factoring of integers for large enough primes. Theretofore, many cash schemes have been proposed which tend to focus only on a limited subset of expected properties. In 1988, Chaum et al. proposed the first off-line e cash scheme [13] with untraceability. Then George et al. [11] defined anonymity control where a user will not possess anonymity if she/he commits a crime. In 2001, Wang and Zhang [10] used cut-and-choose methodologies to design their e-cash scheme which achieves double-spending detection and user anonymity. After 2002, many authors considered coin tracing and owner tracing in their proposed schemes [6-9, 12]. Anonymity control becomes a necessary feature in an off-line e-cash scheme. The remainder of this paper is organized as follows. Section 2 Propose a New ElGamal signature scheme. A New electronic cash scheme is provided in Section 3. Section 4 presents the performance comparisons. The security analysis is discussed in Section 5 and finally section 6 concludes the paper.

2. IMPROVEMENT OF ELGAMAL SIGNATURE SCHEME

In this section we improve the original ElGamal signature scheme with removing inverse operation from secret random number $k \in \mathbb{Z}_{p-1}^{*}$.

2.1 INITIAL PHASE

Let p be a prime number such that the discrete logarithm problem in $\mathbb{Z}_p^*$ is intractable, and let $\alpha \in \mathbb{Z}_p^*$ be a primitive element. Define:

$$K = \{(p, \alpha, a, \beta) ; \alpha^a \equiv \beta (\text{mod } p)\} \quad (2.1)$$

As the set of all possible keys. The values (p, α, β) are the public key, and α is the private key.

2.2 SIGNING PHASE:

The signer to sign message x, chooses a (secret) random number $k \in \mathbb{Z}_{p-1}^{*}$ and then implements following computations.

$$\begin{cases} sig_k(x, k) = (\gamma, \delta) \\ \gamma \equiv \alpha^k \ mod p \\ \delta \equiv [(x - a)\beta - (\gamma + k)] mod (p-1) \end{cases} \quad (2.2)$$

He/she introduces the pair (γ, δ) as signature on message x.

2.3 VERIFICATION PHASE

To verify the signature (γ, δ) on x, we observe that

$$Ver(x, (\gamma, \delta)) = true \Leftrightarrow \beta^{\gamma} \gamma^{\delta} \equiv \alpha^{x} \bmod p \quad (2.3)$$

A complete treatment of the scheme can be found in [20].

3. A NEW UNTRACEABLE OFF-LINE ELECTRONIC CASH SYSTEM

There are four participants in the scheme: a Certification Authority (CA), the Bank (B), the Customer (C) and the Merchant (M). Also this scheme executes in five separate phases: The initialization phase performed by different entities and where necessary information such as public keys are generated. The withdrawal phase performed between a bank and a customer. The payment phase performed between a customer and a merchant. The deposit phase

between a merchant and a bank and finally the exchange phase that executed by a bank.

3.1 Initial Phase

This phase executes in five subsections as follow. **3.1.1** The Certification Authority CA:

3.1.1.1 Selects a large prime p.

3.1.1.2 Selects α as square of a primitive root modp

3.1.1.3 Selects three public hash functions H_0, H_1, H_2. H_0 Takes an integer as input. H_1 Takes a 3-tuple of integers as input while H_2 inputs 5- tuple integers.

3.1.1.4 The Certification Authority Publishes $< p, \alpha, H_0, H_1, H_2 >$.

3.1.2 The Bank B:

3.1.2.1 Selects n as a factor of $p-1$, that is product of two safe prime.

3.1.2.2 Picks randomly an integer $e \in \mathbb{Z}_n^* = \{1, 2, ..., n-1\}$ such that $\gcd(e, n) = 1$.

3.1.2.3 calculates an integer d satisfying the congruence $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$.

3.1.2.4 Chooses a secret identity number $x \in \mathbb{Z}$ and computes $y = \alpha^x (\mathrm{mod}\, p)$.

3.1.2.5 Finally, publishes (e, y) as a pair of public key whereas kept (d, x) as a pair of secret key of the scheme.

3.1.3 The Customer C:

3.1.3.1 Selects its RSA parameters as $(p_C, q_C, n_C, e_C, d_C)$, where $n_C > p$.

3.1.3.2 Chooses an identity number r_C and random number c and then computes:

$$F \equiv (H_0(c \,\|\, \alpha^{r_C}), c)^e \bmod n \qquad (3.1)$$

3.1.3.3 Finally, C sends $(F, \alpha^{r_C} (\mathrm{mod}\, p))$ to B.

3.1.4 The Bank B:

3.1.4.1 Computes $F_d (\mathrm{mod}\, n)$ to obtain c and stores c and $\alpha^{r_C} (\mathrm{mod}\, p)$ along with identity information of the customer (e.g., name, address, etc.) in its database.

3.1.4.2 Chooses a random number r_B and calculates the numbers

$$\begin{cases} j = (c \,\|\, r_B) \bmod p \\ R \equiv \alpha^j (\mathrm{mod}\, p) \end{cases} \qquad (3.2)$$

3.1.4.3 Stores $< R, j, R_B >$ in its database.

3.1.4.4 Computes $R^{e_C} (\mathrm{mod}\, n_C)$ and sends that to C.

3.1.5 The Merchant M:

3.1.5.1 Chooses an identification number ID_M and registers it with the Bank

3.2 Withdrawal Protocol

Withdrawal Protocol executes in five phases between a customer and the Bank where the final purpose is gaining a five-tuple called electronic coin. Since we want produce an e-coin protecting anonymous of customer, we should use a blind signature scheme. In [18] is presented a new blind signature scheme based on factoring and discrete logarithms. This kind of scheme provides a longer or higher security than that scheme based on a single hard problem. This is due the impossibility of attackers to solve two hard problems simultaneously. We profit from this signature scheme in our withdrawal bellow:

3.2.1 The Customer C:

3.2.1.1 Uses his/her private key d_C and computes $(R^{e_c})^{d_c} = R (\mathrm{mod}\, n)$.

3.2.1.2 Then uses parameters of new ElGamal signature in section 2. I.e. chooses a (secret) random number $k \in \mathbb{Z}_{p-1}^*$ and then computes $\gamma \equiv \alpha^k (\mathrm{mod}\, p)$.

3.2.1.3 Now customer uses resulting R in the first part of previous step and computes secret parameter a. She/he selects random number a_1 and lets $a = (R \,\|\, a_1)$ and then computes $\beta = \alpha^a (\mathrm{mod}\, p)$.

3.2.1.4 She/he uses number $\hat{k}$ in initialization phase and chooses blinding factors (a_2, a_3) and then computes $D \equiv \hat{k}^{a_2} . \alpha^{a_3} (\mathrm{mod}\, p)$.

3.2.1.5 Finally checks that $\gcd(D, n) = 1$. If this is not case, C goes back to select another blinding factors, otherwise, he/she computes and sends

$$L \equiv \alpha^{-1} . H_1(\gamma, \beta, D) . \hat{k} . D^{-1} (\mathrm{mod}\, n) \qquad (3.3)$$

3.2.2 The Bank B:

3.2.2.1 Uses its private key x, and then computes and sends $\hat{s} = (Lx + \hat{k}r) \bmod n$ to the C.

3.2.3 The Customer C:

3.2.3.1 Computes and sends $s \equiv (a_2 . \hat{s} . D . \hat{k}^{-1} + a_3 D) . (\hat{s}^{-1})^e \bmod n$ to the B.

3.2.4 The Bank B:

3.2.4.1 Computes expiration date t = (date||time).

3.2.4.2 Computes $\hat{u} \equiv s^d (\mathrm{mod}\, n)$ and sends $(\hat{u}, t)$ to the C.

3.2.5 The Customer C:

3.2.5.1 Computes $u \equiv \hat{u} . \hat{s} (\mathrm{mod}\, n)$. The coin (γ, β, D, u, t) is now complete.

Finishing withdrawal protocol and producing electronic coin, the customer should pay an e-coin to the merchant and receive his/her goods. This process is executable between a customer and a merchant using a payment protocol. But the merchant should check the validity of the paid e-coin. Also the merchant should verify the presented blind signature and consider the expiration date. The details of this phase are also depicted in Fig.1.

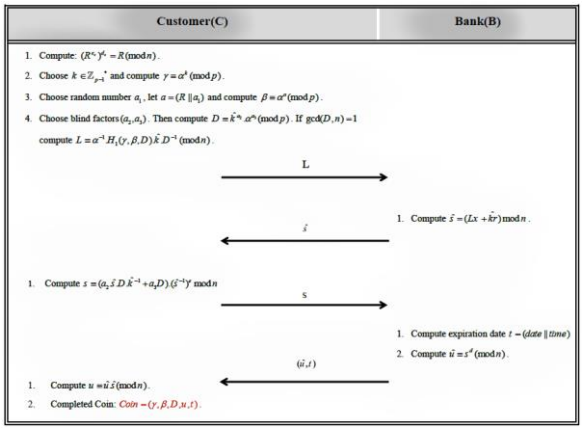

Fig.1. Withdrawal Protocol

3.3 PAYMENT PROTOCOL

This protocol performs in four steps between customer C and merchant M as follows

3.3.1 The Customer C:

3.3.1.1 Sends e-coin (γ, β, D, u, t) to the M.

3.3.2 The merchant M:

3.3.2.1 Checks the expiration date of the coin.

3.3.2.2 Using coin values and public parameters, he/she checks following equation:

$$\alpha^{u^e} \equiv y^{H_1(\gamma,\beta,D)} . D^D \pmod p \qquad (3.4)$$

If this is the case, the merchant knows the coin is valid. But, more steps are required to prevent double spending. If the coin be valid, the merchant goes to step 3.3.3.

3.3.3 The merchant M:

3.3.3.1 Computes $x = H_2(\gamma, \beta, ID_M, Date \| time)$ where date and time represent the date and time of the transaction.

3.3.3.2 Sends value x to the customer.

3.3.4 The customer C:

3.3.4.1 Utilizes new ElGamal's scheme to compute δ such that:

$$\delta \equiv [(x - a)\beta - (\gamma + k)] \bmod (p - 1) \qquad (3.5)$$

3.3.4.2 Sends value δ to the merchant.

3.3.5 The merchant M:

3.3.5.1 The merchant M accepts the coin if

$$\alpha^{x\beta} \equiv \alpha^{(\gamma+\delta)} . \beta^{\beta} . \gamma \pmod p \qquad (3.6)$$

The details of this phase are also depicted in Fig.2.

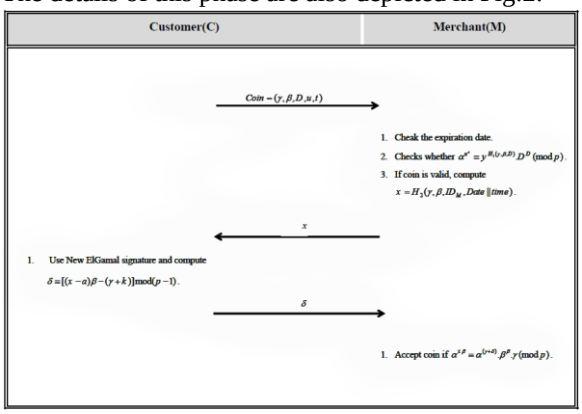

Fig.2 Payment Protocol

3.4 DEPOSIT PROTOCOL

This protocol performs in two steps between merchant M and Bank B. In this phase the merchant deposits the accepted e-coin in the bank and a fraud control procedure is carried out to detect possible cheating. The Bank maintains two tables: the Deposit Table and the Exchange Table. These tables are used in deposit and the exchange phase as well as the fraud control procedure. The content of Deposit Table summarized in Table 1. This table includes information of per coin and related in the payment protocol. In this table ID_i represents identity of i-th merchant that deposits the accepted e-coin in the bank.

Table 1. Deposit Table

Coin Information	Deposited by	Date expiration
$(\gamma_1, \beta_1, D_1, u_1, t_1, \delta_1, x_1)$	ID_1	*Date* 1
$(\gamma_2, \beta_2, D_2, u_2, t_2, \delta_2, x_2)$	ID_2	*Date* 2
●	●	●
●	●	●
●	●	●
$(\gamma_n, \beta_n, D_n, u_n, t_n, \delta_n, x_n)$	ID_n	*Date* n

3.4.1 The merchant M:

3.4.1.1 Sends e-coin (γ, β, D, u, t) and related (x, δ) to the bank.

3.4.2 The Bank B:

3.4.2.1 If the coin (γ, β, D, u, t) exits in either of the Deposit Table or the Exchange Table (This table summarized in Table 2), skips to Fraud Control procedure, because this coin already used.

3.4.2.2 If not, checks if $\alpha^{u^e} \equiv y^{H_1(\gamma,\beta,D)} . D^D \pmod p$, if so, the coin is valid and the Bank stores $(\gamma, \beta, D, u, t, \delta, x)$ into Deposit Table and transfers money to the Merchant's account. The details of this phase are also depicted in Fig.3.

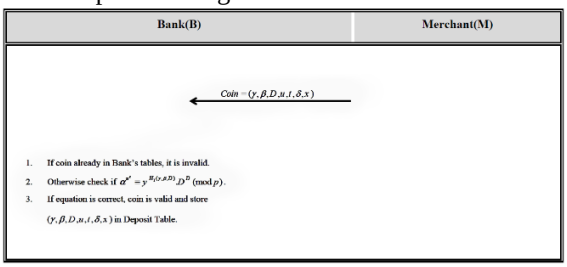

Fig.3 Deposit Protocol

3.5 EXCHANGE PROTOCOL

In this phase, the Bank exchanges only outdated coins which are not in the Deposit Table or the Exchange Table. Suppose A owner of such coins. He/She can present the coin to the Bank and receive a new coin with up- dated expiration date. The details are as follows.

Table 2. Exchange Table

Coin Information	Exchanged by	Date expiration
$(\gamma_1, \beta_1, D_1, u_1, t_1)$	ID_1	*Date* 1
$(\gamma_2, \beta_2, D_2, u_2, t_2)$	ID_2	*Date* 2
•	•	•
•	•	•
•	•	•
$(\gamma_n, \beta_n, D_n, u_n, t_n)$	ID_n	*Date n*

3.5.1 A presents his/her outdated coin together with ID to the Bank.

3.5.2 Bank which checks if A knows the corresponding r_C in subsection 3.1.3 and if the coin is valid according to 3.4 equation. Now, a new coin can be generated.

3.5.3 To generate a new coin, the withdrawal protocol runs between the user A and the Bank. The Bank then updates Exchange Table. Note that when a coin enters this table, then it is considered invalid and no further transaction on it can be performed.

Therefore, the proposed scheme attaches expiration date to coins so that the banking system can manage its databases more efficiently and reduce the size of the databases the bank has to manage.

4. Security Discussion

According to the [2] unforgeability and double-spending detection are the most important security issues pertaining to electronic cash. In this section, we consider unforgeability and double-spending.

4.1 Unforgeability of the coin

Unforgeability in the proposed protocol is hold. Unforgeability of a coin is related to the unforgeability of the bank signature and so this unforgeability is related to secrecy of the private key of Bank. Considering using the secure blind signature in the withdrawal protocol lead to producing the electronic coin and so forging this blind signature is impossible [20] and as a result produced electronic coin is unforgeable.

4.2 Double-spending detection

In this section, we prove that how the Bank can reveal the identity of customer using new ElGamal scheme if he/she spends the coin twice. Suppose in the proposed protocol, the spender spends the coin twice. Once with merchant M and another with M'. Suppose in the deposit phase, M deposits his/her coin with (x, δ). Now when M' wants to deposit his coin with (x', δ'), the bank discuses that this coin was before in his table and for revealing the identity of the spender, uses new ElGamal signature. Then as for values (x', δ'), (x, δ) he organizes an equation system for both merchant as follow:

$$\begin{cases} \delta \equiv [(x - a)\beta - (\gamma + k)] \bmod (p-1) \\ \delta' \equiv [(x' - a)\beta - (\gamma + k)] \bmod (p-1) \end{cases} \quad (4.1)$$

Bank solves this equation system with unknown parameters a, k. Therefore

$$k \equiv 2^{-1}[(x + x')\beta - (\delta + \delta') - 2\gamma] \bmod (p-1) \quad (4.2)$$

Also the Bank computes a:

$$a \equiv 2^{-1}[(x - x')\beta - (\delta - \delta')\beta^{-1}] \bmod (p-1) \quad (4.3)$$

Then a, spender private key, is been defined for the bank and so considering the first phase of withdrawal protocol as the section 3.2.1.1 and the equation $a = (R \| a_1)$, the Bank gains R. Now using section 3.1.4.2 and also having save r_B, j, R in the database of the Bank, the identification number c and all the identification information of the customer be reveal for the Bank. Therefore while double spending a coin, the spender stays anonymous, if not his/her hidden identification will be revealed.

5. Performance Comparison

In this section the performance of the proposed scheme with related schemes in terms of the frequency used hash functions, exponential and modular operation in two common phases is compared. The Table 3 shows the comparison between proposed scheme in the withdrawal phase for the customer and the bank, and payment for the merchant and the schemes Chang [21], Juang [22], Liu [23] and Eslami [19]. As it is shown in the Table 3, the new payment protocol in each three phases works better than its base protocol i.e. [19]. The customer uses modular operations twice and exponential once, whereas the number of hash operation in both protocol are equal. Also in withdrawal phase and according to the calculations done by the bank, although the number of exponential and modular in two protocol is the same, there is no hash function in the proposed scheme.

Also in this scheme number of modular and hash function in the payment phase compared to [19] is reduced. However the merchant uses equal calculations in the exponential operations.

If inverse operation is involved in these two protocols, there is no inverse operation observed in the payment phase in calculation δ for the customer, because of using the new ElGamal signature. While other operations in this phase in the both protocol is the same. It must be considered that the electronic coin produced in [19] was a (u, g, A, r, A'', t), that in the new scheme is reduced to (γ, β, D, u, t) and the frequency of the validation conditions is improved from 2 to 1. So the new protocol is very efficient.

Between the five protocols in the table 3, except Chang scheme that is online of transaction type, other schemes are offline. From the security view, the Chang and Lio schemes are based on factoring problem, but the Jang scheme is based on discrete logarithm problem and the Eslami and the new schemes are based on two difficult problems i.e. factoring problem and discrete logarithm problem.

Table 3. Performance comparison

Exponentials					Modulars					Hash functions					Operations
New	2011 Eslami	2006 Lin	2005 Juang	2003 Chang	New	2011 Eslami	2006 Lin	2005 Juang	2003 Chang	New	2011 Eslami	2006 Lin	2005 Juang	2003 Chang	Protocol / Phases
5	6	16	3	2	7	9	15	6	6	1	1	2	0	2	Withdrawal (Customer)
1	1	2	1	4	2	2	2	2	0	0	1	0	0	2	Withdrawal (Bank)
6	6	7	2	2	2	3	4	2	0	2	3	2	0	2	Payment(Merchant)

6. CONCLUSION

In this paper, a new transaction protocol based on electronic cash using a modified ElGamal signature and a secure blind signature scheme is proposed. This protocol which not only can maintain anonymity but also can find double spender of the coin by using the new ElGamal signature scheme. The security of the system is based on discrete logarithm problem and factoring problem. The electronic cash in our proposed scheme has an expiration date which enables the banking system can manage its databases more efficiently. We observe that our protocol has better performance than similar protocols. So the new protocol is very efficient.

REFERENCES

[1] W. Hua, Z. Yanchun, C. Jinli, and V. Varadharajan, "Achieving se- cure and flexible m-services through tickets", *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 33, no. 6, pp. 697-708, Nov. 2003.

[2] D. Chaum. "Blind signatures for untraceable payments". *Advances in Cryptology. CRYPTO 82*, pp. 199-203, 1982.

[3] T. Nakanishi and Y. Sugiyama, "An efficient on-line electronic cash with unlinkable exact payments", *IEICE Trans. Fund. Electron., Common. Comput. Sci*, vol. E88-A, no. 10, pp. 2769-2779, 2005.

[4] R. Song and L. Korba, "How to make e-cash with non-repudiation and anonymity", in Proc. Inf. Technol.: Coding Comput. Washington, *DC: IEEE Computer Society*, pp.167-172, 2004.

[5] J. Camenisch, A. Lysyanskaya, and M. Meyerovich "Endrosed e-cash", *in Proc. IEEE Symp. Security and Privacy. Washington, DC: IEEE Computer Society*, pp.101-115, May 2007.

[6] C. Popescu, "An off-line electronic cash system with revokable anonymity", in Proc. 12th IEEE Mediterranean Conf., Dubrovnik, *Croatia: IEEE Computer Society*, pp.763-767, May 2004.

[7] X. Hou and C. H. Tan, "Fair traceable off-line electronic cash in wallets with observers", in Proc. Adv. Commun. Technol., Phoenix Park, Korea: *IEEE Computer Society*, pp.595-599, Feb. 2004.

[8] T. Nakanishi, N. Haruna, and Y. Sugiyama, "Unlinkable electronic coupon protocol with anonymity control", *in Information Security, London, U.K.: Springer-Verlag*, pp.37-46, Feb. 2004.

[9] X. Hou and C. H. Tan, "A new electronic cash model. in Proc". Int. Conf. Inf. Technol.: Coding Comput. Washington, *DC: IEEE Computer Society*, pp.374-379, 2005.

[10] H. Wang and Y. Zhang, "Untraceable off-line electronic cash flow in e-commerce", in Proc. Austral. Comput. Sci. Conf., Los Alamitos, *CA: IEEE Computer Society*, pp.191-198, Feb. 2001.

[11] I. George, Y. Frankel, Y. Tsiounis, and M. Yung, "Anonymity control in e-cash systems, in Financial Cryptography". *London, U.K.: Springer- Verlag*, pp.1-16, 1997.

[12] W. Qiu, K. Chen, and D. Gu. "A new offline privacy protecting e- cash system with revocable anonymity", *in Information Security. London U.K.: Springer-Verlag*, pp.177-190, Oct. 2002.

[13] D. Chaum, A. Fiat, and M. Naor. "Untraceable electronic cash", *in Advances in Cryptology-CRYPTO'88*. New York: Springer-Verlag, pp. 319-327, 1990.

[14] M. Jakobsson and M. Yung. "Revokable and versatile electronic money", *in Proc. Conf. Comput. Commun. Security*, New York: ACM, pp.76-87, Mar. 1996.

[15] V. Varadharajan, K. Q. Neguyen, and Y. Mu. "On the design of efficient Rsa-based off-line electronic cash schemes", *Theor. Comput. Sci*, vol. 226, no. 1-2, pp. 173-184, Sep. 1999.

[16] Y. Hanatani, Y. Komano, K. Ohta, and N. Kunihiro. "Provably secure electronic cash based on blind multisignature scheme", *Financial Cryptography Data Security*, vol. 4107, pp. 236-250, Oct. 2006.

[17] S. Canard, A. Gouget, and J. Traore. "Improvement of efficiency in (unconditional) anonymous transferable e-cash", *Financial Cryptograph*. Data Security, vol. 5143, pp. 202-214, Aug. 2008.

[18] N. M. F. Tahat, E. S. Ismail and R. R. Ahmad. "A New Blind Signature Scheme Based On Factoring and Discrete Logarithms", *International Journal of Cryptology Research*, 1-9, 2009.

[19] Z. Eslami and M. Talebi, "A new untraceable off-line electronic cash system", *Electronic Commerce Research and Applications*, vol. 10, pp. 59-66, 2011.

[20] A. Zaghian and M. Mansouri, "A New Blind Signature Scheme Based on Improved ElGamal Signature Scheme", *International journal of information and communication technology research (IJICTR)*, Volume 4- Number 5- pp. 61-65, December 2012.

[21] C.Chang, Y.Lai, "A flexible date-attachment scheme on e-cash", *Computers and Security*, 160–166, 2003.

[22] W.Juang, "A practical anonymous off-line multi-authority payment scheme", *Electronic Commerce Research and Applications*, 240–249, 2005.

[23] K.Liu, P.Tsang, S.Wong, "Recoverable and untraceable e-cash", In Second European PKI Workshop: Research and Applications, LNCS 3545, Springer, NewYork, 206–214, 2005.

[24] Baseri, Y., B. Takhtaei, and J. Mohajeri (2013).Secure untraceable off-line electronic cash system, Scientia Iranica, 20 (3), 637–646.

[25] Baoyuan Kang and Danhui Xu, "An Untraceable Off-Line Electronic Cash Scheme without Merchant Frauds", International Journal of Hybrid Information Technology, Vol.9, No.1 (2016).

Ali Zaghian was born in Isfahan, Iran in 1959 and received his B.Sc. degree in mathematics from Isfahan university, and his M.Sc. and Ph.D. degrees respectively in mathematics and cryptography-mathematics from tarbiat moalem university, Tehran Iran, in 2008. He is currently assistant professor in Cryptography-Mathematics Department of Malek-Ashtar university of technology (MUT), Isfahan, Iran. His research interests include coding and cryptography algorithms

Mohsen Mansouri was born in Isfahan, Iran in Oct the 16th in 1982 and received his B.Sc. degree in Cryptography-Mathematics Department of Malek-Ashtar university of technology (MUT), Isfahan, Iran, in 2011. His research interests include public key cryptosystems, with a focus on elliptic curve cryptography (ECC), blind signatures and authentications protocols