INFORMATICA, 2009, Vol. 20, No. 4, 579–590

An Anonymous Mobile Payment System Based on Bilinear Pairings

Constantin POPESCU
Department of Mathematics and Computer Science, University of Oradea
Universitatii 1, Oradea, Romania
e-mail: cpopescu@uoradea.ro

Received: April 2007; accepted: April 2008

Abstract. Many electronic cash systems have been proposed with the proliferation of the Internet and the activation of electronic commerce. E-cash enables the exchange of digital coins with value assured by the bank's signature and with concealed user identity. In an electronic cash system, a user can withdraw coins from the bank and then spends each coin anonymously and unlinkably. In this paper, we design an efficient anonymous mobile payment system based on bilinear pairings, in which the anonymity of coins is revocable by a trustee in case of dispute. The message transfer from the customer to the merchant occurs only once during the payment protocol. Also, the amount of communication between customer and merchant is about 800 bits. Therefore, our mobile payment system can be used in the wireless networks with the limited bandwidth. The security of the new system is under the computational Diffie–Hellman problem in the random oracle model.

Keywords: cryptography, electronic cash system, bilinear pairings.

1. Introduction

A variety of on-line businesses are rapidly emerging over the Internet, which is believed to be one of the most efficient and convenient ways to provide all electronic services. An efficient and secure electronic cash system plays an important role to support these businesses safely as a trustful payment over the Internet. Real money using traditional means of payment has potential security problems such as counterfeiting and forgeability. E-cash also exhibits similar drawbacks, but properly-designed e-cash system can provide more secure and flexible service for non-face-to-face exchange of digital goods than real money. After Chaum (1983) introduced the anonymity of an e-cash using blind signature, numerous researches have been done in the field of e-cash system. Whether the bank is required to be on-line or not in the processing of an electronic transaction, Chaum *et al.* (1990) suggested an anonymous on-line e-cash system and Chaum *et al.* (1989) proposed an anonymous off-line e-cash system, which satisfies double-spending prevention with the cut-and-choose method. The e-cash systems by Okamoto and Ohta (1982, 1992) satisfy the divisibility and transferability in addition. Their schemes overcome some limitations of previous e-cash systems and provide more efficient features than real money. Brands (1993) proposed an efficient e-cash system with single-term method which is

more efficient compared with the cut-and-choose method. Brands' scheme has been used as a basic model by other researchers. However, Solms and Naccache (1992) raised the issue of perfect crime by abusing the anonymity of the e-cash system. Recently, Wang *et al.* (2005) have proposed an off-line payment scheme providing scalable anonymity. Besides the basic participants, a third party, the named Anonymity Provider agent, is involved in the scheme. The Anonymity Provider agent helps the consumer to get the required anonymity, but is not involved in the purchase process. The Anonymity Provider agent gives a certificate to the consumer when he/she needs a high level of anonymity. The authors claim that their scheme can prevent a consumer from spending a coin more than once, since after a double-spending the identity of the consumer is revealed. Camenisch *et al.* (2005) proposed an off-line e-cash scheme where a user can withdraw a wallet containing 2^l coins each of which she can spend unlinkably. Their e-cash scheme provides traceable and divisible e-coins without a trusted third party. That is, once a user has double spent one of the 2^l coins in her wallet, all her spendings of these coins can be traced. The e-cash scheme in Camenisch *et al.* (2005) is secure in the random oracle model. The revocable e-cash system (Popescu, 2004, 2006; Popescu and Oros, 2004) and (Lee *et al.*, 2002) (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.

Since the mobile device first introduced in the world, there has been rapid development of new functions, improvement of services and the enhancement of the computing power of mobile devices make M-commerce more profitable and promising. The main problem is that mobile payments face with a number of problems from not only performance but also security points of view.

Two approaches have been done to the mobile payment systems up to date: by mobile agent (Romao and Da Silva, 1998, 2001; Wang *et al.*, 1999) and by mobile device (Paybox, 2001; Mobilix, 2002). The schemes in Romao and Da Silva (1998, 2001), Wang *et al.* (1999), employing mobile agent technique has accommodated SET protocol (SET, 1997) in which several public key computations are followed for payment. On behalf of a customer, the mobile agent performs all processes necessary in SET protocol (SET, 1997) with the customer's confidential data. The authors in Paybox (2001) and Mobilix (2002), use the mobile device as an authentication tool to confirm customer's payment information and approval by sending secret short key over the air. Also, Ham *et al.* (2002) proposed a mobile payment system which does not provide: the anonymity of the customers, security against tracing a honest customer by the bank and security against money laundering.

In this paper, we present an efficient anonymous mobile payment system based on bilinear pairings. In order to construct our electronic cash system, we use the group signature of X. Chen *et al.* (2006) and the group blind signature of Zhong and He (2006). We note that only the connection between the customer and the merchant is set up through the wireless channel. Comparing with e-cash system proposed by Ham *et al.* (2002), our mobile payment system provide the anonymity of the customers and security against tracing

a honest customer by the bank and money laundering. The overall efficiency is improved in our electronic cash system compared to Lee *et al.*'s (2002) system, Camenisch *et al.*'s (2005) and Wang *et al.*'s (2005) e-cash system in terms of the storage space.

The remainder of this paper is organized as follows. In the next section, we review the properties of bilinear pairings and the model of the mobile payment system necessary in the subsequent design of our mobile payment system. Then, we present our mobile payment system 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. Preliminaries

In this section, we review some cryptographic assumptions and introduces the building blocks necessary in the subsequent design of our mobile payment system.

2.1. *Bilinear Pairings*

In this section we review the properties of bilinear pairings necessary in the subsequent design of the proposed system. Let G_1 be a cyclic additive group generated by P of order a prime q, 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 pairings is a map e: $G_1 \times G_1 \rightarrow G_2$ with the following properties:

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

Let G_1 a cyclic additive group generated by P, of order q. 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 to compute abP for $a, b \in Z_q^*$.
3. Decisional Diffie–Hellman Problem (DDHP). Given P, aP, bP, cP decide weather $c \equiv ab \bmod q$ for $a, b, c \in Z_q^*$.

We call G_1 a gap Diffie–Hellman group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP or DLP with non-negligible probability. Such a group can be found in supersingular elliptic curve of hyperelliptic curve over finite fields and the bilinear parings can be derived from Weil or Tate parings. For more details, see Boneh and Franklin (2001), Hess (2002).

2.2. *Anonymous Mobile Payment System Model*

Our mobile payment system consists of five protocols: Setup, Customer Join, Withdrawal, Payment, Deposit and Tracing. Note that Withdrawal, Deposit and Tracing protocols are

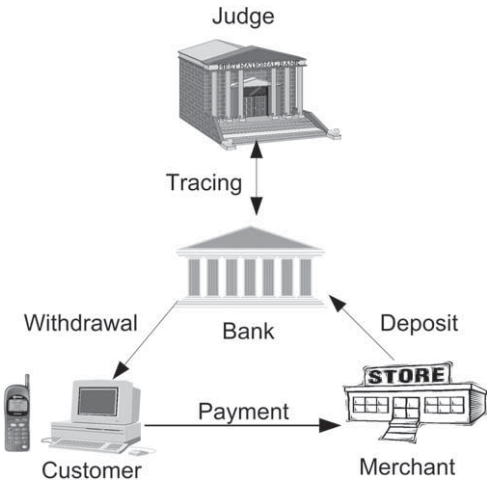

Fig. 1. Mobile payment system model.

performed over a secure wired channel and only Payment protocol is done through the mobile networks. The customer has a mobile device like a mobile phone and the merchant provides corresponding mobile services. When the customer and the merchant interacts with the bank, private information such as account information or password and even money itself are transferred into the other end. The other two connections, between the customer and the bank, and between the merchant and the bank, are assumed to be established through the secure wired channel by using the SSL protocol (SSL, 1996). The model of our mobile payment system is presented in Fig. 1.

3. The Proposed Mobile Payment System

The system is modelled by 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. All customers who open a bank account form a group and a trusted party is the group manager. When a customer, wants to withdraw an electronic coin c from his account, the bank applies a group blind signature protocol to c and decreases appropriate amount from the customer's account. Everyone including the merchant can verify the validity of group blind signature with the public key of the group. In our mobile payment system, we use the group signature of X. Chen *et al.* (2006) and the group blind signature of Zhong and He (2006).

3.1. *The Setup Protocol*

The setup protocol is performed by the group manager. 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 pairings is a map e: $G_1 \times G_1 \to G_2$. We define two ideal hash functions H_1: $\{0,1\}^* \times G_1 \to Z_q$, H_2: $\{0,1\}^* \times G_1 \to G_1$.

The group manager chooses a random number $s \in Z_q^*$ and sets $P_{\text{pub}} = sP$. The group manager keeps s as his master-key and publishes group public key $Y = \{G_1, G_2, e, q, P, P_{\text{pub}}, H_1, H_2\}$.

3.2. *The Customer Join Protocol*

Any customer who wants to join the group has to interact with the group manager and obtains membership certificate to generate the group signature:

1. The customer submits his/her identity information ID to the group manager. Also, chooses a random number $r \in Z_q^*$ as his long-term private key and sends rP 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, and sends S_{ID} to the customer. The symbol $||$ denotes the concatenation of two strings.
3. The customer randomly chooses $x_i \in Z_q^*$, $i = \overline{1,k}$. He then sends rx_iP, x_iP, rP, ID, S_{ID} to the group manager.
4. If $S_{ID} = sH_2(ID||T, rP)$ and $e(rx_iP, P) = e(rP, x_iP)$, the group manager sends $S_i = sH_2(T, rx_iP),\ i = \overline{1,k}$ to the customer.
5. The customer's member certificates are (S_i, rx_iP) and his private signing keys are $rx_i,\ i = \overline{1,k}$.
6. The group manager adds rx_iP, x_iP, rP and ID to the customer list.

3.3. *The Withdrawal Protocol*

The withdrawal protocol involves the customer and the bank. When a legitimate customer wants to withdraw a coin c from his account, the bank applies the following group blind signature protocol to sign the coin c:

1. The bank chooses a random $a \in Z_q^*$ and computes $U = aH_2(T, rx_iP)$. The bank sends U to the customer.
2. The customer chooses a random $b \in Z_q^*$ and computes $U' = U + bP$ and $H_2(c, U')$. The customer sends U' and $H_2(c, U')$ to the bank.
3. The bank computes $V = aH_2(c, U')$ and sends it to the customer.
4. The customer computes $V' = V + bP$ and $h' = H_1(c, U' + V')$ then sends h' and S_i to the bank.
5. The bank computes $W = (a + h')S_i$ and sends it to the customer.
6. The customer computes $W' = W + bP_{\text{pub}}$.
7. The resulting group blind signature of the coin c is (U', V', W', T, rx_iP).

The bank cannot link the blind coin with the identity of the customer. The customer gets the coin c from his account.

3.4. *The Payment Protocol*

The payment protocol involves the customer and the merchant. Our mobile payment system is off-line because during payment the merchant does not communicate with the bank.

1. The customer chooses a random $z \in Z_q^*$ and computes

$$U_1 = zH_2(T, rx_iP). \tag{1}$$

2. The customer computes:

$$U_2 = rx_iH_2(c, U_1), \tag{2}$$
$$h = H_1(c, U_1 + U_2), \tag{3}$$
$$U_3 = (z + h)S_i. \tag{4}$$

3. The customer sends the signature $(U_1, U_2, U_3, T, rx_iP)$ of the coin c to the merchant.
4. The merchant verifies the signature $(U_1, U_2, U_3, T, rx_iP)$ of the coin c as follows:
   (a) Computes $H_2(T, rx_iP)$, $H_2(c, U_1)$ and $h = H_1(c, U_1 + U_2)$.
   (b) Tests if the following equations hold:

$$e(U_3, P) = e\big(U_1 + hH_2(T, rx_iP), P_{\text{pub}}\big). \tag{5}$$

If Eq. (5) fail, the merchant terminates the transaction.

3.5. *The Deposit Protocol*

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

1. The merchant sends to the bank the signature $(U_1, U_2, U_3, T, rx_iP)$ of the coin c.
2. The bank verifies the validity of the signature $(U_1, U_2, U_3, T, rx_iP)$ using the same operations as the merchant (see Step 4 from Subsection 3.4).
3. If the signature $(U_1, U_2, U_3, T, rx_iP)$ of the coin c is valid and the coin c was not deposited before, the bank accepts the coin c and then the merchant sends the goods to the customer.

If the same coin c was deposited before, double spending is found and the bank requests the group manager that the identity of the dishonest customer to be revealed.

3.6. *The Tracing Protocol*

The bank can legally trace the customer of a paid coin with the help of the group manager. The group manager can easily identify the customer from the following equations:

$$e(rx_iP, P) = e(x_iP, rP), \tag{6}$$

$$e(S_{ID}, P) = e\big(H_2(ID||T, rP), P_{\text{pub}}\big). \tag{7}$$

The group manager search through the group customer list to get the identity of the customer.

4. Security and Efficiency Analysis

In this section we discuss some aspects of security and efficiency of our mobile electronic cash system. The following theorem prove the anonymity of our system.

Theorem 1. *Assuming that the group signature scheme and the group blind signature scheme are computationally secure our electronic cash system is secure against tracing a honest customer by the bank.*

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 only by the group manager. For a honest customer, the group blind signature will be used when he withdraws the coin c from the bank, so that the bank know nothing about the coin c and cannot trace the e-cash from the deposit protocol. Since x_i is randomly chosen, then rx_iP reveals no information about the customer's identity to anyone except the group manager. Also, since the group blind signature (U', V', W', T, rx_iP) 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: if the group signature scheme and the group blind signature scheme are secure against forgery attacks and the hash function H_2 is collision-resistant, the mobile e-cash system is secure against forgery of the coin c.*

Proof. Since the group blind signature is secure against existential forgery, this allows only the legal bank to generate the signature for the coin c. As the hash function has the feature of collision free, the customer cannot find a value $c' \neq c$ with $H_2(c', U') = H_2(c, U')$. Thus, the system satisfies unforgeability of coins.

Theorem 3. *Security under the assumption of computational Diffie–Hellman problem: our mobile electronic cash system is secure under the assumption of computational Diffie–Hellman problem in the random oracle model.*

Proof. Consider the following game: the adversary A forges a valid tuple $(ID, S_{ID}, rP, S, rx_iP)$ with non-negligible probability ρ through the following process. First, the adversary A queries the hash function H_2 adaptively, then outputs a tuple $(ID, S_{ID}, rP, S, rx_iP)$ in which ID, rP and rx_iP were not queried. If the tuple $(ID, S_{ID}, rP, S, rx_iP)$ is valid, it must satisfy the Eq. (7):

$$e(S_{ID}, P) = e\big(H_2(ID||T, rP), P_{\text{pub}}\big).$$

Let $H_2(ID||T, rP) = aP$ and $P_{\text{pub}} = bP$. Then, by running the adversary, we solved Computational Diffie–Hellman Problem in G_1 for $S_{ID} = abP$ or $S = abP$ with non-negligible probability ρ.

Theorem 4. *Security against money laundering: assuming that the group signature scheme and the group blind signature scheme are computationally secure, the mobile e-cash system is secure against money laundering.*

Proof. Since the group manager knows the relation between customer's identification and his secret key, money laundering is prevented. When money laundering happens, the group manager reveals the identity of dishonest customer using the tracing protocol.

We discuss the performance of our system in terms of computation and communication which are main interests in the mobile payment systems. We suppose that the bank and the merchant have enough powerful computational resources to execute several modular multiplications. We only take into consideration on the customer's computational capability during the payment protocol. Since the withdrawal protocol is carried out through the wired channel and the customer can use a personal computer for withdrawal, several modular multiplications to obtain a blind coin c is not expensive. As the main computational overheads, we consider modular multiplications (denote by MM – see Table 1).

We compare the e-cash systems proposed by Wang *et al.* (2005), Camenisch *et al.* (2005), Lee *et al.* (2002), Ham *et al.* (2002) with our mobile e-cash system (see Table 1). Suppose that the size of q is 160 bits and the hash functions H, H_1 and H_2 of 160 bits for five systems. In our mobile payment system, during the payment protocol, the customer stores and sends to the merchant only a group signature about 800 bits long. The signature in the system of Ham *et al.* is about 520 bits. The messages σ_c and $(c_u, U_1, U_2, U_3, T, rx_uP)$ in the payment protocol is 1144 bits in Lee *et al.*'s system and the message (m, e, u, v, t_1) in the payment protocol of Wang *et al.* is 1282 bits. In the payment protocol of Camenisch *et al.* (2005), a customer needs to compute 7 multi-base exponentiations to build the commitments and 11 multi-base exponentiations to carry out the proof (approximative 18432 bits).

The advantage of the proposed e-cash system is that the overall efficiency is improved in our electronic cash system compared to Lee *et al.*'s (2002) system, Camenisch *et al.*'s (2005) e-cash scheme and Wang *et al.*'s (2005) e-cash system in terms of the storage space. However, the authors in De Santis *et al.* (2008) show that in Wang *et al.*'s (2005)

Table 1
Comparison of the mobile payment systems

	Ham	Wang	Lee	Camenisch	Our
Hash functions	160 bits	160 bits	160 bits	160 bits	160 bits
Modulus q	160 bits	160 bits	160 bits	160 bits	160 bits
Sig. in Payment Protocol	520 bits	1282 bits	1144 bits	18432 bits	800 bits
Binary length of computation	12 MM	15 MM	22 MM	26 MM	9 MM
Divisibility	YES	NO	NO	YES	NO
Off-line communication	YES	YES	YES	YES	YES
TTP requirement	NO	YES	YES	NO	YES
Anonymity	NO	YES	YES	YES	YES
Unlinkability	NO	NO	NO	YES	YES
Double spending prevention	NO	NO	YES	YES	YES

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 particular, they show how a cheater, using only public information, can construct a faked proof of ownership of the coin without running any risk of being discovered. Also, the system of Ham *et al.* (2002) is not provably secure against tracing a honest customer by the bank and money laundering. Furthermore, their system does not provide the anonymity of the customers. But, our mobile electronic cash system is resistant against tracing a honest customer by the bank and money laundering. Also, the proposed mobile payment system provide the anonymity of the customers.

5. Conclusions

In this paper we proposed an anonymous mobile payment system based on bilinear pairings. The security of the new system is under the computational Diffie–Hellman problem in the random oracle model. The overall efficiency is improved in our electronic cash system compared to the e-cash systems proposed in Lee *et al.* (2002), Ham *et al.* (2002), Camenish *et al.* (2005), and Wang *et al.* (2005). Also, our mobile payment system provide security against tracing a honest customer by the bank, money laundering and the anonymity of the customers. The amount of communication between customer and merchant is about 800 bits. So, the proposed mobile payment system can be used in the wireless networks with the limited bandwidth due to the low communication between the customer and the merchant.

References

Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairings. In: *Advances in Cryptology-Crypto 2001*, *Lecture Notes in Computer Science*, Vol. 2139, pp. 213–229.

Brands, S. (1993). Untraceable off-line cash in wallets with observers. *Lecture Notes in Computer Science*, 773, 302–318.

Camenisch, J., Hohenberger, S., Lysyanskaya, A. (2005). Compact e-cash. In: *Advances in Cryptology-EuroCrypt 2005*. pp. 302–321.

Chaum, D. (1983). Blind signature for untraceable payments. In: *Proceedings of Eurocrypt'82*, Plenum Press. pp. 199–203.

Chaum, D., den Boer, B., van Heyst, E., Mjolsnes, S., Steenbeek, A. (1989). Effcient offline electronic checks. In: *Advances in Cryptology-Crypto 1989*. pp. 294–301.

Chaum, D., Fiat, A., Naor, M. (1990). Untraceable electronic cash. *Lecture Notes in Computer Science*, 319–327.

Chen, X., Zhang, F., Kim, K. (2006). A new ID-based group signature scheme from bilinear pairings. *Journal of Electronics*, 23, 892–900.

De Santis, A., Ferrara, A., Masucci, B. (2008). An attack on a payment scheme. *Information Sciences*, 178(5), 1418–1421.

Ham, W., Choi, H., Xie, Y., Lee, M., Kim, K. (2002). Secure one-way mobile payment system keeping low computation in mobile devices. In: *Proceedings of WISA*. pp. 287–301.

Hess, F. (2002). Efficient identity based signature schemes based on pairings. In: *Proceedings of the 9th Workshop on Selected Areas in Cryptography-SAC 2002*, *Lecture Notes in Computer Science*, 2595, 310–324.

Lee, M., Ahn, G., Kim, J., Park, J., Lee, B., Kim, K., Lee, H. (2002). Design and implementation of an efficient fair off-line e-cash system based on elliptic curve discrete logarithm problem. *Journal of Communications and Networks*, 4, 81–89.

Lee, T., Yip, Y., Tsang, C., Ng, K. (2001). An agent-based micropayment system for e-commerce. *Lecture Notes in Artificial Intelligence*, 2033, 247–263.

MobiliX (2002). Available at: `http://mobilix.org`.

Okamoto, T., Ohta, K. (1989). Disposable zero-knowledge authentications and their applications to untraceable electronic cash. In: *Advances in Cryptology-Crypto 1989*. pp. 481–496.

Okamota, T., Ohta, K. (1992). Universal electronic cash. *Lecture Notes in Computer Science*, 324–337.

Paybox.net (2001). Available at: `http://www.paybox.net`.

Popescu, C. (2004). An off-line electronic cash system with revokable anonymity. In: *Proceedings of IEEE Mediterranean Electrotechnical Conference*, Dubrovnik, Croatia. pp. 125–130.

Popescu, C. (2006). An electronic cash system based on group blind signatures. *Informatica*, 17(4), 551–564.

Popescu, C., Oros, H. (2004). A fair off-line electronic cash system with anonymity revoking trustee. In: *Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics*, Thessaloniki, Greece. pp. 409–416.

Romao, A., Da Silva, M.M. (1998). An agent-based secure Internet payment system for mobile computing. *Lecture Notes in Computer Science*, 1402, 80–93.

Romao, A., Da Silva, M.M. (2001). Secure mobile agent digital signatures with proxy certificates. *Lecture Notes in Artificial Intelligence*, 2033, 206–218.

SET (1997). *The SET Standard Book 1 Business Description*. Available at: `http://www.setco.org/`.

SSL (1996). *Netscape Communications. The SSL Protocol*. Version 3.0. Available at: `http://wp.netscape.com/eng/ssl3/ssl-toc.html`

von Solms, B., Naccache, D. (1992). On blind signatures and perfect crimes. *Computers and Security*, 11(6), 581–583.

Wang, X.F., Lan, K.Y., Yi, X. (1999). Secure agent-meditated mobile payment. *Lecture Notes in Artificial Intelligence*, 1599, 162–173.

Wang, H., Cao, J., Zhang, Y. (2005). A flexible payment scheme and its role-based access control. *IEEE Transactions Knowledge Data Engeneering*, 17, 425–436.

Zhong, J., He, D. (2006). A new type of group blind signature scheme based on bilinear parings. In: *Cryptology ePrint Archive*, Report 2006/439. Available at: `http://eprint.iacr.org/`.

C. Popescu received the PhD degree in computer science (cryptography) at the Babes-Bolyai University, Cluj Napoca, Romania. Since 2005 he is a professor at the Department of Mathematics and Computer Science, University of Oradea, Romania. His research interests include cryptography, network security, group signatures, security protocols and electronic payment systems.

Anoniminė mobili mokėjimo sistema paremta bitiesiniu porinimu

Constantin POPESCU

Daugelis elektroninių pinigų sistemų buvo pasiūlyta norint paskatinti internetinę elektroninę komerciją. E-pinigai, kuriuos išduoda bankas, patvirtindamas juos savo parašu, leidžia atlikti monetų skaitmeniniame pavidale cirkuliaciją. Tuo tarpu tokioje monetoje yra neatskleidžiama vartotojo tapatybė. Vartotojas gali paimti e-pinigų iš banko ir išleisti kiekvieną monetą anonimiškai ir nesusiejant ją su savo tapatybe.

Šiame straipsnyje mes sukūrėme gana efektyvią, anoniminę mobilaus mokėjimo sistemą, paremtą bitiesiniu porinimu, kurioje monetų anonimiškumas yra atskleidžiamas tuo atveju, jei yra sukčiavimas, tam pasitelkiant trečią patikimą šalį. Pranešimas tarp vartotojo ir pardavėjo siunčiamas tik vieną kartą, vykdant mokėjimo protokolą. Perduodamas informacijos kiekis tarp vartotojo ir pardavėjo yra apie 800 bitų. Todėl mūsų mobili mokėjimo sistema patogi naudoti belaidžiuose tinkluose su ribota pralaidumo juosta. Šios sistemos saugumas paremtas skaičiuotina Diffie–Hellman'o problema atsitiktinio oraklo modelyje.