American Journal of Applied Sciences 4 (8): 538-542, 2007
ISSN 1546-9239

Anonymous and Non-Repudiation E-Payment Protocol

Sattar J Aboud and Mohammed Ahmed AL-Fayoumi
Department of Computer Information System, Faculty of Information Technology
Middle East University for Graduate Studies, P.O.Box 42, Amman 11610, Jordan

Abstract: There are many proposals offer anonymous and non-repudiation e-payment protocols. But they have the drawbacks that the anonymity can be misused by fraudulent to perform a perfect crimes. Currently, the hot research concentrates on the accepting of e-payment protocols where the anonymity of the coins is cancelable via a trusted authority in the case of criminal entities. In the article we suggest an efficient protocol for e-payment scheme that offers a good level of security with appreciate to its efficiency. The proposed protocol prevents the blind office and the bank from impersonate an entity, so that the entity could not repudiate it when the entity misused a coin. Another benefit is that it is constructed from efficient cryptography schemes so that its security can simply be analyzed. The strength of this scheme is in its easiness. So, we claim that the suggested protocol is more efficient than the existing schemes, since it allows to both a blind office and a bank to impersonate an entity to find and to spend a coin without to be noticed. It might cause a repudiation difficulty where the entity can repudiate his bad activities by proposing that both the bank and the blind office acted inaccurately. Other relevant issues related to the new protocol will be discussed in the section of the security of the scheme.

Keywords: e-payment protocol, blind signature scheme, hash function, RSA scheme, Elgamal scheme.

INTRODUCTION

The idea of anonymous payment scheme was introduced in 1982[1]. In fact this anonymity might be misused by fraudulent to perform a perfect crime[2]. For instance stealing of the private keys, money laundry, and blackmailing of coins. The use of blindfolded protocols in the banks are considered as a modern threats[3]. To avoid these threats the payment schemes must offer anonymity method which accepts the tracing of coins in any of the states mentioned above by an authorized trusted authority. The first scheme that is stopping blackmailing and money laundry was suggested in[4]. However, there are some proposals[5-7] to prevent these threats. Every scheme needs the participation of the trusted authority in the opening of the bank account, and also in the withdrawal of coins. The only scheme that does not need trusted authority participation excepting the anonymity has just suggested in[8]. But, it is unable to stop extortion threats and the employ of blindfolding schemes. These threats are just prevented in the scheme of[9], which is also not efficient as it needs the trusted authority interaction in e-payment schemes. In case that one of these threats is needed, they require an on-line e-payment scheme among user, shop, and trusted authority to stop the spending of illegitimate coins. However, in any e-payment scheme there are two requirements.

1. The entity need to have anonymous e-payment service
2. The bank needs to ensure that the e-payment scheme will not be abused.

For example, when double spending is suspected; the related participant's identity must be traceable[10]. There are numerous papers are suggested employing blind signature schemes to design an e-payment protocols, which satisfies the needs of both the banks and the entities[11-13]. We propose a secure payment system that allows anonymity by trusted authority in the case of any extortion attacks. Therefore we employ a blind office as a pseudo identity escrow agency. The scheme based on the hypothesis of high trust relations[14-16] between a bank, user and blind office, since both blind office and bank can impersonate user without being noticed.

The problem with the current protocols are that a difficulty resultant from these trust relations when user can repudiate his bad activity[17] by claiming that no

Corresponding Author: Sattar J Aboud, Department of Computer Information System, Faculty of Information Technology, Middle East University for Graduate Studies, P.O.Box 42, Amman 11610, Jordan

need to trust both blind office and bank. In this situation it is hard for an unbiased judge to adjudicate between the three entities. The main benefit of the proposed protocol is to avoid blind office and bank from impersonating user, so that user could not repudiate that the entity has abused a coin. Other significant benefits of this scheme are modular, simple design that easy to understand, to apply and to analyze with concern to security needs, for the security analysis we benefits from the modular design of the propose scheme using well known public key encryption schemes. In addition, the proposed scheme is multi-purpose, as it allows the integration of multi spendable and divisible coins and supports the challenge semantics. However, the objectives of the article are:

1. To modify the existing schemes that is non-repudiation, which when it has to make judge to determine which one to abuse bank, user or blind office. This need encountered in other payment schemes[18].
2. Introduce an amendment in the current protocols to provide three characteristics of anonymity, non-repudiation and traceability.
3. To develop an efficient e-payment scheme with anonymity method that achieves prevention of any type of extortion attacks.

THE GENERAL E-PAYMENT SCHEME

In this section we will describe the general e-payment scheme which is appropriate for both the existing protocols and the suggested protocol. However, it includes five entities a user U, a blind office O, a bank B, a judge J, and a shop S. It works as follows:

- U obtains a coin C signed blindly by B.
- B keeps a relations proof among U's real identifier ID and pseudo identifier PID.
- O participated in the blind signature, holds another relations proof among PID and C.
- To spend C, U proofs to S that he has information of secret key x according to C.
- If C is misused, for example double spending, B and O will work together to construct a link among ID and C, and J will be participated in this procedure to judge.

Assume that U and B both have an exponent key type signatures denoted by (S_U, V_U) and (S_B, V_B) respectively, such that V_U is known to B and V_B is known to U, O and S. Assume also that O has an exponent public-key cryptosystem, denoted by (E_o, D_o), such that E_o is known to U and B, J could be verified all the schemes. The potential implementation for these cryptosystems is RSA scheme[19]. The coin contains three fields which are as follows:

1. The exponent key denoted by y for a public key type signature scheme. The corresponding secret signature key is represented by x.
2. The information field i having some pertinent data concerning C, for example its value and expiry dates.
3. The bank's digital signature on both y and i.

There are two different methods of counting i in bank's signature scheme. As follows:

- i could be concatenated with y via O before finding a blinded exponent key represented by y^{-}
- i could be added via bank using another signature key based on the information which is being denoted.

In fact, we need the digital signature scheme of the bank to have some feature, that is $S_B(m_1) * S_B(m_2) = S_B(m_1 * m_2)$ which keeps for RSA. Certainly this is usually not preferable property for a digital signature scheme, and for this reason the RSA must always be employed with a special redundancy function or a one-way hash function[20-22]. In the proposed scheme, we are going to employ a one-way hash function presented by $h(m)$ for the message m with S_B. We will refer to a blinding function by F, and use it as an inverse to the digital signature scheme. Thus $S_B(F(m_1)m_2) = m_1 * S_B(m_2)$, for each m_1, m_2, but when bank digital signature scheme is RSA, then F is just exponentiation employing the public verification key.

THE PROPOSED PROTOCOL

In this section we will introduce the proposed protocol which is as follows:

The General Protocol

1. The user U and B generate a shared secret s.
2. Then B signs a one way hash function of s, namely $S_B(h(s))$ which is employed to build PID by concatenating it with $E_o(s)$.

3. Also B keeps a relation proof among ID and s, which we indicate by $\{ID, s\}$. It is a digital signature on $h(s)$ employing S_U.

The Withdraw Protocol

The steps of the proposed protocol for withdrawing a coin work as follows, in which all messages exchanged between B and U are supposed to be encrypted with s when the communication channels between them are insecure.

1. U picks x randomly, calculates y and then sends $E_o(y)$ to O.
2. Both U and O generate a shared w, by employing the Diffie-Hellman scheme[23].
3. O calculates $y^- = F(w) * y$ and passes it to U.
4. U proves y^-, and then passes B a message signed employing S_u. This message is invented of s, y^-, O's name and other uses data, for instance the present time and a time stamp, to guarantee that the innovation and uniqueness of the signature is provable.
5. B holds U's signature scheme, withdraws a true coin from U's account, and then responds to U by $T = E_O(S_B(y^-))$. Then U sends T to O.
6. O recovers T to get $S_B(y^-)$, then un-blinds $S_B(y)$ to build C, and then passes C to U. Next O keeps $\{PID, C\}$, which contains a record of PID and two public key encryption values, that is the public key encryption value of T with s and the public key encryption value of $E_B(y)$ with s.

The Spending Protocol

To spend C use the following steps:

1. U sign a message which is created via S as a challenge, to prove U knows x.
2. S claims a true coin back from B later.
3. If C is double spending, B will request a tracing steps in which B and O work together to construct a link among C and ID, relied on $\{ID, s\}$ and $\{PID, C\}$

The proposed protocol has three major properties compared with the existing protocols.

1. O can not spend C, because does not know x.
2. O and U together create a arbitrary w, it guarantee that both O and U can not separately influence the value of w, and therefore both U and O cannot get more than one coin from a one blind signature.
3. B holds U's signature on y^- as a relations evidence amongst ID and y^- indicated by $\{ID, y^-\}$. It guarantees that U and B cannot discuss who published x.

For example, in the M'Raihi protocol[6] the bank can connect ID with y^-, it is yet likely for U to reject accountability for C since he has no concept concerning the relationship among y and y^- when creation a contribution to this connection since he is blinded too.

SECURITY OF THE SCHEME

For the security evaluation we gain from the modular design of proposed scheme employing well known cryptography schemes. Though, all possible threads can be shown to be avoided. The security analysis is clearly controlled as we avoided interaction between the methods as much as possible. We now plan the proofs that the novel scheme has several security characteristics. However, we assume that all entities B, U, O, J and S, do not conspire with every other one.

Theorem 1: U can not get C without the participation of bank and O.

Proof 1: to get C without bank and O be participated, U should be able to calculate $S_B(y^-)$ from y^- or from $E_O(S_B(y^-))$, each of which is supposed to be infeasible

Theorem 2: The entity who is the publisher of secret key x can only be spending a valid coin pertinent to x.

Proof 2: it is computationally infeasible to decrypt x from given y even with other allied known data, because the secret key x is known just to its publisher and is not disclosed to any other person. So, the acquaintance of x is needed to spend C, the outcomes follows.

Theorem 3: O cannot masquerade as U to B or to S.

Proof 3: To impersonate U to B, O should find U's digital signature on the y^- selected by O, which is supposed to be infeasible. To impersonate U to S for spending C, O should be acquainted with both C and x. As U is able to prove y^-, O cannot blind

U and then get bank's digital signature scheme on y^- according to his private x. So, it is infeasible for O to find C and its equivalent x.

Theorem 4: When the bank impersonate U to get and to spend C, he cannot claim that U published the coin.

Proof 4: To verify $\{ID, y^-\}$, the bank required U 's digital signature on y^- such a digital signature cannot be computed even with O 's cooperation, when U is not participated in the coin creation.

We conclude this discussion with a following consequence. When a coin with a relationship of $\{ID, C\}$ is abused, U cannot repudiate accountability for this misuse because this assumption is depending on theorems 2, 3, and 4. The real coin with a relationship of $\{ID, C\}$ holds by both B and O should be related to a secret key x in which published by U and as a result U is the only entity able to spend C.

CONCLSIONS

We introduced an efficient e-payment protocol with three characteristics of anonymity, non-repudiation and traceability. It is one of the first protocols that achieve prevention of any type of extortion threads. On account of its high security and efficiency, it can be gauged for two key applications of secure internet e-payment and efficient e-purse, where the efficiency and security requirements are completely different. In the article we described a possible repudiation difficulty in current payment protocols and suggested an alternative protocol to conquer the difficulty. The primary benefit of the new protocol is that both B and O cannot impersonate U to find and to spend C without being discovered. Thus if U misuses C, he cannot repudiate it via proposing that it is performed by both B and O. This benefit is at the user computational cost are more burdensome than for the existing protocols, since the user requires to make pre- calculations of the digital signature scheme when employing digital signature scheme for spending C.

REFRENCES

1. Chaum, D., 1983. Blind Signature for Untraceable Payments, Advances in Cryptology. Crypto'82. Plenum Press. pp: 199-203.
2. Solms, V and D. Naccache, 1992. Blind Signatures and Perfect Crimes. Intl. J. Computers & Security, Vol. (11): 581-583.
3. Liu, J., K. Wei and S. Wong, 2001. Recoverable and Untraceable E-Cash, EUROCON'2001: Trends in Communications. Intl. Conference on Information Technology, Vol. (1): 342-349.
4. Brickell, E., P. Gemmell and D. Kravitz, 1995. Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Exchange. Proceeding of 6th Intl. Conference of ACM-SIAM SODA: 457-466.
5. Camenisch, M and M. Stadler, 1996. Digital Payment Systems with Passive anonymity-revoking trustees: Computer Security-ESORICS96, Lecture Notes in Computer Security 1146. Springer-Verlag, PP: 33-34.
6. M'Raihi D, 1996. Cost Effective Payment Schemes with Piracy Regulation: Advances in Cryptology-ASIACRYPT 96, Lecture Notes in Computer Science 1163. Springer-Verlag, pp: 266-275.
7. Jacobson, M and M. Youg, 1997. Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System. Proceeding of Intl. Workshop on Financial Cryptography: 21-30.
8. Binh, D, 2007. A Fair Payment Scheme with On-line Anonymous Transfer. M.Sc Thesis. MIT, pp: 3-27.
9. Susan Hohenberger, 2006. Advances in Signatures Encryption and E-Cash from Bilinear Group. PhD Thesis. MIT, pp. 95-142.
10. Liisa, K., 2001. The Perfect Payment Architecture, Technical Document Mobley Forum, www.mobeyforum .
11. Zheng, X and D. Chen, 2003. Study of Mobile Payments System Proceedings of the IEEE Intl. Conference on E-Commerce, (CEC'03).
12. Kungpisdan, S., B. Srivnivasan and P. Le, 2004. A Secure Account-Based Mobile Payment Protocol. Proceedings of the Intl. Conference on Information Technology: Coding and Computing, (ITCC'04).
13. Yang, L and J. Li, 2006. Application Study on Public Key Cryptography in Mobile Payment, Proceeding of the 5th WSEAS Intl. Conference on Information Security and Privacy, Venice. Italy: 20-22.
14. NCSC-TG-017, 2000. A Guide to Understanding Identification and Authentication in Trusted Systems: U.S National Computer Center.

15. Abe, M and E. Fujisaki, 1996. How to Date Blind Signatures. Advances in Cryptology: ASIACRYPT '96: 244-251.
16. Micali, S., 2003. Simple and Fast Optimistic Protocols for fair e-exchange. Proceeding in Intl. Conference of 22nd Annual ACM Symposia: On Principles of Distributed Computing (PODC'03). ACM Press: 12-19.
17. Song, R and L. Korba, 2004. How to Make E-cash with Non-Repudiation and Anonymity. Proceedings of the Intl. Conference on Information Technology: Coding and Computing, (ITCC'04):167-172.
18. Wade, T and L. Washington, 2006. Introduction to Cryptography with Coding Theory: 2nd Edition, Prentice Hall, pp: 287-295.
19. Rivest, R., A. Shmir and L. Adlman, 1978. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM (21): 294-299.
20. Department of Commerce, National Institute of Standards and Technology, 1994. Digital Signature Standard. Federal Information Processing Standard Publication 186, USA.
21. Menezes, P. van Oorschot and S Vanstone, 1997. Handbook of Applied Cryptography. CRT Press, pp: 321-358.
22. Douglas Stinson, 2006. Cryptography and Practice. CRT Press, pp: 232-254.
23. Diffie W. and M.E. Hellman, 1976. New Direction in Cryptography. IEEE: Transaction of Information Theory, IT-22(6):644-654.