Practical E-Payment Scheme

Mohammad Al-Fayoumi[1], Sattar Aboud[2] and Mustafa Al-Fayoumi[3]

[1] Information Systems, Abdulaziz University
Jedda, KSA

[2] Information Technology Advisor, Iraqi Council of Representative
Bagdad, Iraq

[3] Computer Information Systems, Al-Zaytoonah University of Jordan
Amman, Jordan

Abstract

E-payment is now one of the most central research areas in e-commerce, mainly regarding online and offline payment scenarios. Customers are generally passive in e-commerce transaction. Relied on a blind signature, this paper introduces an e-payment protocol, in which customers have more initiative, and can terminate the transaction before possible cheats, its security is enhanced. Moreover, the cost of workers and communications falls down considerably while the cost of trusted authority and protecting information is increased. As there is no trusted authority in the proposed scheme, network overcrowding and conspiracy problems can be avoided. Furthermore, the protocol satisfies fairness and non-repudiation. This helps merchant and bank to speed up the financial transaction process and to give user instant services at any time. Also, in this paper, we will discuss an important e-payment protocol namely pay-word scheme and examine its advantages and limitations, which encourages the authors to improve the scheme that keeps all characteristics intact without compromise of the security robustness. The suggested protocol employs the idea of blind signature with the thought of hash chain. We will compare the proposed protocol with pay-word protocol and demonstrate that the proposed protocol offers more security and efficiency, which makes the protocol workable for real world services.

Keywords: *E-payment protocol, public key cryptography, blind signature scheme, e-commerce.*

1. Introduction

With the increasing impact of intangible merchandise in worldwide economies and their immediate delivery at small cost, traditional payment systems tend to be more costly than the modern one. Online processing can be of considerable value compared with the manual one. However, there are two methods of running e-payment systems.

Online payment: in which vendor checks the payment sent by purchaser with a bank before serving the purchaser.

Offline payment: in which over spending must be detected, and consequently, no online link to the bank is needed.

The e-payment schemes [1] can be sub-divided into two groups according to the online assumptions.

- Payments by transaction method: in which single payment does not need previous arrangements between purchaser and vendor.
- Payments by account method: in which purchaser and vendor should have a system account with bank and certain type of agreement between both before carrying out the real payment transaction.

The payment by transaction can further be divided into two subgroups.

- The credit card payment transaction: is tailored for a large charge payment of some hundreds or even thousands of dollars. In contrast, net money transaction is usually of low value payment with difficult transaction cost and online features, similar to the thought of the e-payment transaction. The drawback of the credit card payment transaction is the fee of transactions, particularly from the perspective of the vendor who has to pay some invoices to the clearing house according to the contract agreement with them. This certainly will have direct impact on the cost policy and the interest between the possible users.
- The e-payment by small value transactions on service: This is acquiring certain interest from the area of research. A number of important services of e-payment are e-publishing and multimedia service. In these services, due to the small transaction amount, the merchant acquires

relatively shopping mall revenue from every transaction.

As a result, expensive calculations such as digital signature should be limited in order to reduce the investments in software applications. In recent years, e-payments [2, 3] offering a relatively key improvement in the online revenue malls. The foundation of e-payments is to take benefit of the high level of viewers by presenting content for a low price. Other alternative of this thought is to rating fractions of cents for equally fractional contents sums. The main features in e-payment protocol are less charges of payment amount and high occurrence of transactions on the e-commerce system.

2. E-Payment Scheme Requirements

The e-payment protocol encompasses three participants which are as follows:

User: The user (customer) purchases e-currency from the bank employing actual money by e-payment. The user can then utilize e-currency to carry out e-payment to buy goods.

Merchant: The merchant is the data storage which provides user with both services and information.

Bank: The bank is the trusted authority. It mediates between user and merchant in order to ease the duties they carry out. In general, the bank acts like a broker offering the e-coins for the e-payments.

While using e-currency, a shared set of characteristics for an e-payment protocol is:

Anonymity: e-cash must not supply any user with information; it means that it must be anonymous e-currency transaction.

Divisibility: e-cash can be sub-divided since the notes have a basic piece.

Transference: e-cash can be transferred to a trusted authority by providing the suitable amount of currency.

Over spending detection: e-cash must be used for only once.

The e-payments are stored and then converted to digital type. This will cause new difficulties during developing secure e-payment protocol. The payment is simply duplicated against the conventional physical paying methods. As the digital payment is characterized as simple sequences of bits, nothing in them stops them copying. When a security of the payment protocol is reliant on the method the payments are hidden from the unknown. Every individual that can have access to payments may utilize them numerous times. We notice that getting anonymous cash transaction is an essential issue, and at the same time giving efficiency is another matter. In this paper, we study a merchant pay-word protocol [4],that gives anonymity characteristic using the idea of blind signature scheme and hash chain. We then proposed a blind signature scheme that will be used in the protocol for reaching better efficiency without conceding its security characteristics. Therefore, before discussing the rest of this paper, we will list the notation used as follows.

U :	User
M :	Merchant
B :	Bank
p :	Prime number
m :	Message
d :	Private Key
g :	A generator of multiplicative group
e :	Expiry information for redemption
h :	Secure hash function

3. Related Works

In 1988 Chaum, Fiat and Naor proposed their protocol entitled untraceable electronic cash [5] which relies on a single use token method. The user creates blinded e-bank currency note and passes it to the bank to be signed using bank public key. The bank signs the currency note, subtracts the value from the user account, and returns the signed currency note back to the user. The user removes the blind thing and utilizes it to buy goods from the super market. The super market checks the authenticity of the bank currency note using the bank public key and passes it to the bank where it is verified contrary to a list of currency note already used. The amount is deposited into the supermarket account, the deposit approved, and the supermarket in turn emits the merchandise. In 1995, Glassman, Manasse, Abadi, Gauthier and Sobalvarro present their protocol entitled "The Millicent protocol for inexpensive electronic commerce"[6] which is a decentralized e-payment protocol, and it allows payments as low as 1/10 of a cent. It employs a type of e-coins. It is introduced to make the cost of committing a fraud more than the cost of the real transaction. It utilizes asymmetric encryption techniques for all information transactions. Millicent is a lightweight and secure scheme for e-commerce through the internet. It is developed to support buying goods charging less than a cent. It is relied on decentralized validation of e-currency at the seller server without any further communication, costly encryption, or off-line processing. Also, in 1997, Rivest suggested his protocol entitled "Electronic lottery tickets as e-payments" [7]. In this protocol there is a possibility to reduce the number of messages engaged with every transaction. Also, the lottery ticket scheme is relied on the assumption that financial agents are risk-neutral and will be satisfied with fair wagers. In 1998, Foo and Boyd proposed another protocol called "A payment scheme using vouchers" [8].

The e-vouchers can be moveable but the direct exchange between purchasers and vendors is impossible. As a result, a financial agent is needed and this will raise the transactions charges of exchange. However, during the last decade several new e-payment protocols [9, 10] have been suggested. In this section, we will discuss pay-word protocol which is an efficient and flexible protocol [4].

4. The Pay-Word Protocol

In 2001, Rivest and Shamir [4] introduced the pay-word protocol, which is a credit-typed protocol. The protocol employs RSA public key cryptography [11] and the idea of hash chain [12]. In the pay-word protocol, if a registered user U requests the merchant M for a service, he should generate a pay-word chain that works as cash made due to merchant M . The merchant M then must check if the user U is authorized and the pay-word cash chain of the protocol is created by the user U .

Afterward, the merchant M gathers user pay-word and redeems the payment from the bank B . The pay-word protocol decreases the number of on-line connections between bank B and merchant M , since the merchant M does not need to pay for each buy. The pay-word chain creation with size n and can be stated as $x_i = h(x_i + 1)$, such that $i = n-1, n-2, ..., 0$. If creating the pay-word, the user U chooses an arbitrary number x_n , named a seed, and then x_n is hashed iteratively in reverse order until the root of the chain x_0 is created. Throughout shopping, the user U in order from x_1 to x_n releases pay-word, and the merchant M checks it simply by hash process.

Pay-word is a merchant M certain payment protocol, namely the pay-word chain is spent only to a specific merchant M . If a user U contacts a new merchant M for ordering service, besides making a new chain, the user U should pass a commitment to merchant M . The commitment includes the identity of the merchant M , the certificate published by the bank B , the root of an unused chain, the present date and other information. To implement continuous transactions, the user U pays pay-word within the chain which belongs to the merchant M . Following a suitable time, the merchant M will contact with the bank B to order redemption. For every chain, the merchant M passes the newest pay-word he received and the user U commitment to the bank B ; so, hashing from newest pay-word to the root of the chain can validate the rightness of transactions. When the validating is correct, the bank B debits user U account with the used size of the chain and credits merchant M account with the same amount. We show the transaction operation of the pay-word protocol in Figure 1.

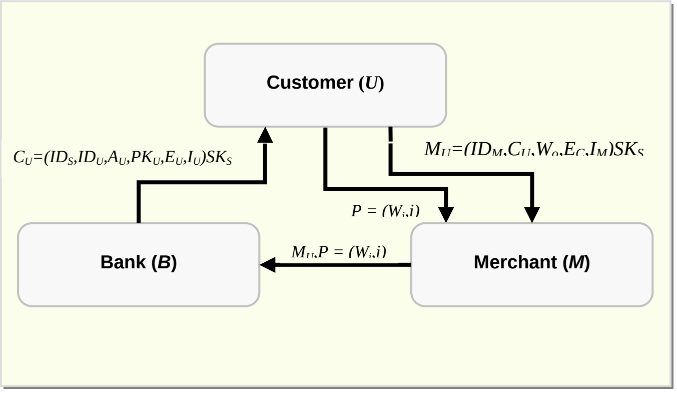
Customer (U)
C_U=(ID_S,ID_U,A_U,PK_U,E_U,I_U)SK_S
M_U=(ID_M,C_U,W_0,E_C,I_M)SK_S
P = (W_i,i)
Bank (B)
M_U,P = (W_i,i)
Merchant (M)

Fig. 1 Transaction operation of the pay-word protocol.

Remarks: pay-word is developed as a credit-based scheme. It takes benefit of hash chain to ensure time efficiency, and reaches non-denial for every payment belonging to the same chain by just one signature. After receiving a certificate, a user is authorized to transact with a merchant in a specified amount without online communication with the bank, provides the user more flexibility. However, the scheme suffers from the following limitations.

- First, the pay-word is a merchant specific payment scheme, so users have to preserve set of specific information of chains corresponding to distinct merchants.
- Second, the user has to carry out hash chain processes as many as the number of merchants every time he needs to perform business with.
- Third the user has to keep all the different pay-words of every merchant and the last index used for the transactions.
- Fourth, the user could make payments exceeding his authorized credit limit.

5. The Proposed Protocol

This paper is introduced an efficient protocol, and make a simple comparison between the proposed protocol and the above described pay-word protocol. Also, gauging the efficiency and security of the protocol will take place in section 6. However, any such protocol should contain at least four schemes, registration scheme, blind signature scheme, transaction scheme, and redemption scheme. The proposed protocol adopts the same procedures of the pay-word scheme except the blind signature scheme. Thus, in this section, we will introduce a new blind signature scheme using discrete logarithm problem [13]. We will show this improvement makes the pay-word protocol more efficient and keeps all other characteristics balanced.

5.1 Blind Scheme

The user gives a withdrawal request to the bank before his order for some service from merchant. The steps of the scheme are as follows:

Step 1: Bank

1.1. Generate an arbitrarily prime number p

1.2. Select a generator g of the multiplicative of group Z_p^*

1.3. Pick the private key d such that $1 < d < p-2$

1.4. Finds the public key $y = g^d \bmod p$

1.5. Determine the public key (p, g, y) and private key (d)

1.6. Pick a random number $z < p-2$

1.7. Send z to the user

Step 2: User

2.1. Pick a random integers v and u

2.2. Finds $f = v^y * h(m)(u^2+1) \bmod p$

2.3. Send (e, f) to the bank, where e represents an upper limit of cash that the user can use.

2.4. Pick an arbitrary integer c

2.5. Finds $k = v * c \bmod p$

2.6. Pass $a = (k)^y * (u-z) \bmod p$ to the bank

Step 3: Bank

3.1. Finds $a^{-1} \bmod p$

3.2. Finds $j = h(e)^d * (f(z^2+1) * a^{-2})^{2*d} \bmod p$

3.3. Pass (a^{-1}, j) to the user

Step 4: User

4.1. Finds

$$w = (u*z+1)*a^{-1}*(k)^y = (u*z+1)(u-z)^{-1} \bmod p$$

4.2. Finds $x = j * v^2 * (c)^4 \bmod p$

The parameter (e, w, x) is the signature on message m. However, one entity can verify this signature by checking whether $x^y \equiv (j*v^2*(c)^4)^y \bmod p$

5.2 Example

Step 1: Bank

1.1. Suppose $p = 113$

1.2. Assume a generator $g = 2$

1.3. Suppose the private key $d = 11$

1.4. Find the public key $y = g^d \bmod p = 2^{11} \bmod 113 = 14$

1.5. Determine the public key $(p = 113, g = 2, y = 14)$ and private key $(d = 11)$

1.6. Suppose $z = 7$

1.7. Send $z = 7$ to the user

Step 2: User

2.1. Assume $v = 10$ and $u = 17$

2.2. Find $f = v^y * h(m)(u^2+1) \bmod p$

$$= 10^{14} * h(8)(17^2+1) \bmod 113$$
$$= 10^{14} * h(8)(290) \bmod 113$$
$$= 41$$

2.3. Send $(e = 6, f = 41)$ to the bank. Where e represents an upper limit of cash that the user can use.

2.4. Suppose $c = 15$

2.5. Finds $k = v * c = 10 * 15 \bmod 113 = 37$

2.6. Finds $a = (k)^y * (u-z) \bmod p$

$$= 37^{14} * (17-7) \bmod 113$$
$$= 12$$

2.7. Pass $a = 12$ to the bank

Step 3: Bank

3.1. Find $a^{-1} \bmod p$

$$12^{-1} \bmod 113$$
$$12 * 66 \bmod 113 = 1$$

3.2. Finds $j = h(e)^d * (f(z^2+1) * a^{-2})^{2*d} \bmod p$

$$= h(6)^{11} * (41(7^2+1) * 12^{-2})^{2*11} \bmod 113$$
$$= h(6)^{11} * (41 * 50 * 62)^{22} \bmod 113$$
$$= h(362797056) * (127100)^{22} \bmod 113$$
$$= 19$$

3.3. Pass $(a^{-1}, j) = (66, 19)$ to the user

Step 4: User

4.1. Finds

$$w = (u*z+1)*a^{-1}*(k)^y = (u*z+1)(u-z)^{-1} \bmod p$$
$$= (17*7+1)*66*(37)^{14} = (17*7+1)(17-7)^{-1} \bmod 113$$
$$= 12 = (17*7+1)(10)^{-1} \bmod 113$$
$$= 12 = (120)(34) \bmod 113$$
$$= 12 = 12$$

4.2. Finds $x = j * v^2 * (c)^4 \bmod p$

$$= 19*10^2*(15)^4 \bmod 113$$
$$= 19 * 100 * 50625 \bmod 113$$
$$= 92$$

The parameter $(e = 6, w = 12, x = 92)$ is the signature on message m. However, one entity can verify this signature by checking whether $x^y \equiv (j*v^2*(c)^4)^y \bmod p$

$$92^{14} \equiv (19*10^2*15^4)^{14} \bmod 113$$
$$18 \equiv (19*100*50625)^{14} \bmod 113$$
$$18 \equiv 18$$

5.3 Forgery Detection

The user U gets the bank B signature on m prior to any transaction. But, in order to process an accurate redemption, the merchant M should have information of the payment transaction. It is almost unfeasible for any entity to forge the user U payment without knowing the private key d. Thus, the opponent cannot forge signature. But to successfully achieve the verification of the formula $x^y \equiv (j*v^2*(c)^4)^y \bmod p$, an opponent has to calculate x where $x = j*v^2*(c)^4 \bmod p$ provided the results of $h(e)$, $h(m)$ and w. However, it is computationally intractable to obtain the value of d without solving the discrete logarithm that is hard to solve such a problem. Thus, the opponent is unable to forge the signature.

5.4 Efficiency

In the e-payment protocol, the profit acquired by a merchant is little in every transaction. It is unwise to check the transaction employing a complicated technique that leads the average cost of the protocol more than the profit. On the other hand, large calculation in e-payment is not wise. In order to gauge efficiency of the proposed protocol, we compare the enhanced blind scheme with the pay-word scheme [4]. The time complexity of the remaining scheme stays the same in both protocols. We employ the following notation to gauge the efficiency of the schemes.

T_h: Calculation time for hash function operation

T_a: Calculation time for addition in modular multiplication

T_m: Calculation time for multiplication modular exponentiation

Table 1: Computations of efficacy in blinding scheme

Protocol Name	***Blinding Scheme***
The pay-word protocol	$5*T_h + 9*T_a + 5*T_m$
Proposed protocol	$4*T_h + 8*T_a + 4*T_m$

Actually, the modular exponentiation is a costly operation in comparison with addition or hash function operations. As a result it is simple to observe from Table 1 that the proposed protocol is more efficient than the pay-word protocol. Furthermore, when any entity computes and obtains small public key y, then the proposed protocol becomes more efficient. This makes public key operations quicker while the secret key operations remaining unchanged. In this case, when an entity uses the short public key attack, he cannot succeed with this try since every signature is being randomized by certain random numbers. So, the proposed protocol decreases expensive exponential operation and has better time efficiency.

6. Conclusion

In this paper, we described the characteristics of e-payment protocol and evaluated one of the most important e-payment protocols that relied on a hash chain. The hash chain typed scheme gives anonymity security characteristic besides other security features of e-payment protocol. The use of the blind signature scheme and hash function makes the protocol more efficient and guarantees the payment untraceable. Though, we notice that the blind scheme of the protocol takes significantly more computing time and we present an alternate blind scheme using the discrete logarithm that gives more efficiency than the existed protocol. The research accomplished in this paper has vast future prospects and can be extended towards a substantial protocol using hash function so that the modular exponentiation and costly operation can be avoided and also security depth can be reached.

References

[1] A.Tiwari, S. Sanyal, A. Abraham, J. Knapskog, and S. Sanyal, "A Multi-factor Security Protocol for Wireless Payment-Secure Web Authentication Using Mobile Devices", IADIS International Conference Applied Computing, 2007, pp.160-167.

[2] S. van, A. Odlyzko, and R. Rivest, T. Jones and D. Scot, "Does anyone really need micropayments", proceeding of the International Conference of Financial Cryptography, LNCS 2742, Springer, 2003, pp. 69-76.

[3] L. Jun, L. Jianxin, and Z. Xiaomin, "A System Model and Protocol for Mobile Payment", Proceedings of the IEEE International Conference one-Business Engineering (ICEBE'05), 2005.

[4] R. Rivest, and A. Shamir, "Pay-word and MicroMint: Two simple micropayment schemes", International Journal of Network Security, Vol. 2, No. 2, 2001, pp. 81-90.

[5] D. Chaum, Fiat, and M. Naor, "Untraceable electronic cash", Proceeding Advances in Cryptology, LNCS 403, Springer, 1988, pp. 319-327.

[6] M. Hwang, and P. Sung, "A study of micro-payment based on one-way hash chain", International Journal of Network Security, Vol. 2, No. 2, 2006, pp 81-90.

[7] R. Rivest, "Electronic lottery tickets as micropayments", Proceeding of the International Conference of Financial Cryptography, LNCS 1318, Springer, 1997, pp. 307–314.

[8] E. Foo, and C. Boyd, "A payment scheme using vouchers", Proceeding of the International Conference of Financial Cryptography, LNCS 1465, Springer, 1998, pp. 103-121.

[9] M. Baddeley, "Using e-cash in the new economy: An economic analysis of micro-payment systems", Journal of Electronic Commerce Research, Vol. 5, No. 4, 2004.

[10] J. Tellez, and J.Sierra, "Anonymous Payment in a Client Centric Model for Digital Ecosystem", IEEE DEST, 2007, pp. 422-427,

[11] R.Rivest, A. Shamir, and L. Adleman, "A Method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.

[12] D.Stinson, Cryptography: Theory and Practice, CRT Press, 2006.

[13] M. Al-Fayoumi, and S.J. Aboud, "Blind Decryption and Privacy Protection", American Journal of Applied Sciences, Science Publications Vol.2, No. 4, 2005, pp. 873-876.

Mohammad Al-Fayoumi received his B.S. degree in 1974. In 1977, he earned his Master degree in mathematics, and a postgraduate diploma in computer science was received in 1979. A Ph.D. was received in 1982 in the area of computing science. The last two degrees were awarded from Bucharest University; he joined the Yarmouk University, 1982 in Jordan, as an assistant professor and a head of computer science department. In 1986 he moved to collage of business studies in Kuwait and then moved back to Jordan in Applied Science University as associate professor and a head of computer science department. In 2005 he moved to the Middle East University for Graduate Studies in Jordan as an associate professor and a dean of information technology faculty, he promoted to a professor rank in August, 2008. Currently, he is a professor and advisor of graduate studies at the King Abdulaziz University, Saudi Arabia. His research interests include areas of information security, computer simulation, systems development, e-commerce, e-learning and internet security and algorithm analyzes and design. He has supervised many PhD's and master’s degrees research thesis and projects of diverse areas. He has published more than 40 research papers in a multitude of international journals and conferences, in addition to a nine books in the area of computer sciences.

Sattar J. Aboud received his B.S. degree in 1976. In 1982, he earned his Master degree. A Ph.D. was received in 1988. The last two degrees in the area of computing science and were awarded from U.K. In 1990, he joined the institute of technical foundation, in Iraq as an assistant professor and a head of computer system department. In 1993 he moved to Arab University College for science and technology in Iraq as an associate professor and a dean deputy. In 1995 he joined the Philadelphia University in Jordan as an associate professor and a chairman of computer science and information system department. In 2004 he moved to the Amman Arab University for graduate studies, graduate college for computing studies as a professor. Then he moved to the department of computer information systems at the Middle East University for graduate studies, Amman-Jordan as a professor. Currently, he is a advisor of information technology of the Iraqi Council of Representatives His research interests include areas like public key cryptography, digital signatures, identification and authentication, software piracy, networks security, data base security, e-commerce and e-learning security and algorithm analyzes and design. He has supervised many PhD's and master’s degrees research thesis and projects of diverse areas. He has published more than 70 research papers in a multitude of international journals and conferences.

Mustafa A. Al-Fayoumi received the B.S. degree in computer science from Yarmouk University, Irbid, Jordan, in 1988. He received the M.S. degree in computer science from the University of Jordan, Amman, Jordan, in 2003. In 2009, he received a Ph.D. degree in computer science from the Faculty of Science and Technology at Anglia Ruskin University, UK. In 2009, he joined the Al-Zaytoonah University of Jordan, in Jordan, as an assistant professor. His research interests include areas like computer Security, cryptography, identification and authentication, Wireless and mobile Networks security, e-application security, simulation and modeling, algorithm analyzes and design, information retrieval and any other topics related to them. He has published about 10 research papers an international journals and conferences.