Blind Signature Scheme Based on Elliptic Curve Cryptography

Chwei-Shyong Tsai[‡] Min-Shiang Hwang[†] Pei-Chen Sung[§]

Department of Management Information System, National Chung Hsing University[†]
250 Kuo Kuang Road., Taichung, Taiwan 402, R.O.C.
Email: mshwang@nchu.edu.tw
Fax: 886-4-22857173
Department of Information Management, National Taichung Institute of Technology[‡]
129 Sec. 3, San-min Rd., Taichung, Taiwan 404, R.O.C.
Department of Information Management, Chaoyang University of Technology[§]
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.

Abstract

Blind signatures are important techniques and are widely used in many e-commerce services, such as electronic voting and electronic cash system. In this article, we present a blind signature scheme based on elliptic curves cryptography and prove that it satisfies the requirements of blindness, unforgeability and untraceability.

Keywords: Blind signature, cryptosystem, digital signature, elliptic curves cryptography.

Introduction

Blind signature is a kind of digital signatures. Unlike a normal digital signature scheme, in a blind signature scheme, a signer signs a message without knowing what the message contains. That is, the message is blinded by a requester. After receiving the signed message from the signer, the requester can derives the valid signature for the message from the signer. Anyone can verify the blind signature using the public key of the signer. If the message and its signature are published, the signer can verify the signature, but he/she cannot link the message-signature pair [4]. Because of these two properties: blindness and untraceability, blind signatures are widely used in many e-commerce services, (e.g. electronic voting schemes and electronic payment systems).

The concept of the first blind signature scheme was introduced by Chaum [2]. This scheme was based on the factoring logarithm and the security depended on the RSA assumption. Camenisch et al. presented the blind signature based on the discrete logarithm problem [1]. In order to improve the efficiency of the blind signature, Fan et al. proposed a new scheme with a security which depended on the difficulty of solving the square roots of quadratic residues [3]. In this article, we present a new blind signature scheme based on elliptic curve cryptography (ECC) [5, 6, 7, 10]. The security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP) and was proven to provide greater efficiency than the factorization and discrete logarithm systems used by Vanstone [11].

In the next section, we shall present an improved scheme based on ECC. In Section 3, the discussions will reveal that our scheme can achieve the requirements of blindness, unforgeability and untraceability. Finally, concluding remarks will be given in the last section.

The Proposed Scheme

In this section, we propose a new blind signature which is based on ECC. Notations in this article are listed as follows.

X_s: private key of the signer
Q_s: public key of the signer
k: randomly chosen number by the signer
u, v: randomly chosen number by the requester
m: message which the requester wants to blind
$H(\cdot)$: a collision-free hash function
P: a generator point in ECC

The procedure of the proposed scheme is shown in Figure1.

Step 1. The requester gets R' from the signer. That is, $R'=kP$.

Step2. The requester calculates $R= uR'+vP$, $e= H(R||m)$, and sends $e'= \frac{e}{u}$ to the signer.

Step 3. The signer calculates $S'= X_s e' + k$ and sends it to the requester.

Step 4. Upon receiving S', the requester calculates $S= S'u+ v$ and checks the following equation:

$$SP= eQ_s + R \qquad (1)$$

If this verification is successful, then the requester gets a valid signature.

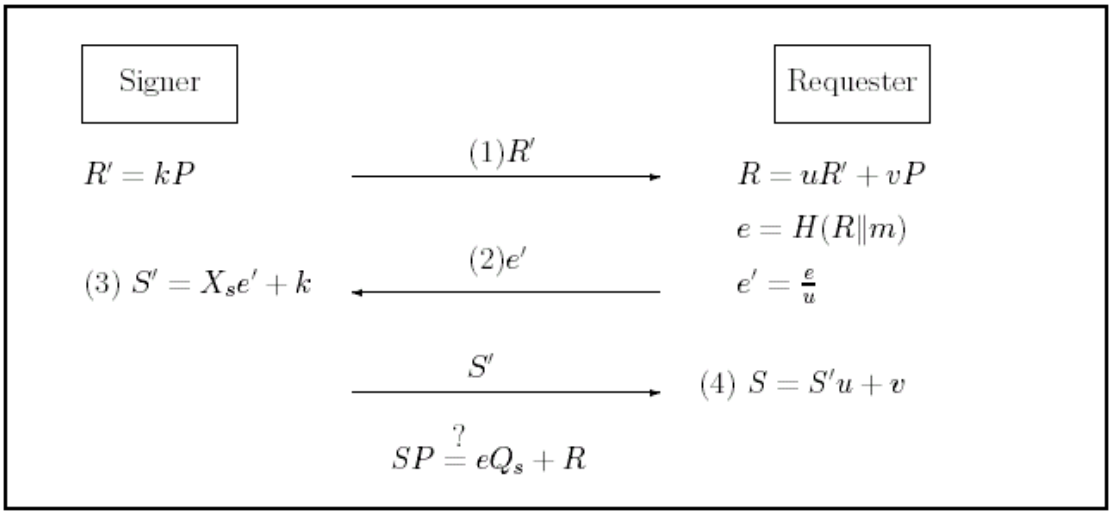

Figure 1: The proposed scheme

We give an e-Payment application to indicate the effective of the proposed scheme. If a user (U) wants to withdraw a coin (E-cash) from the bank (B). The procedures of using the proposed scheme are as follows:

1. U sends a request to B for withdrawing of E-coin, m.
2. B chooses a random number k, computes R' $(=kP)$, and sends R' to U. After receiving R', U computes R $(=uR'+vP)$ and e $(=H(R||m))$, using secret random value u and v. Then, U calculates the blinded value e' $(e'=e/u)$ and sends it to B.
3. B uses his/her private key to generate a blind signature S' $(=X_b e'+k)$ for e' and

sends it to *U*. Here X_b is *B*'s private key.

4. U un-blinds *B*'s signature *S'* by using *u* and *v* (i.e., $S = S'u + v$), and verifies *S* by checking the equations: $SP = eQ_b + R$, where Q_b is a public-key of the bank. If the equation holds, *U* obtains a valid E-cash.

Next, *U* stores the E-cash S to a diskette or smart card. When the user U wants to purchase merchandise over Internet, he/she sends the E-cash to the merchant. The merchant verifies the E-cash whether legal one or not by checking the equations: $SP = eQ_b + R$. If the equation holds, the merchant obtains a valid E-cash.

Security Analysis

In this section, we will show that our scheme preserves all the characteristic of a blind signature.

- **Blindness:**

  The signer signs a message without knowing its contents. Blindness is the first important property in a blind signature. In our scheme, the requester calculates $R = uR' + vP$, and generates e' which is a concatenation of R and m with a hash function $H(\cdot)$. Then, he/she sends them to the signer. Hence, the signer cannot know the message m.

- **Unforgeability:**

  No one can forge (m, R, S) because the elliptic curve discrete logarithm problem is difficult to solve. We assume three situations as follows.

  Situation 1: If someone tried to fake R_1, m_1, he/she cannot obtain S_1. Because $S_1P = e_1Q_s + R_1$ and S_1 is unknown. It is an elliptic curve discrete logarithm problem and difficult to solve.

  Situation 2: If someone gets S_1, m_1, he/she cannot obtain R_1. Because $S_1P = e_1Q_s + R_1$, R_1 is unknown, and $e_1 = H(R_1||m_1)$. It is also an elliptic curve discrete logarithm problem and difficult to solve.

  Situation 3: If someone tries to fake R_1 and S_1, he/she cannot obtain m_1. Because $S_1P = e_1Q_s + R_1$, he/she cannot get e_1 without m_1. It is an elliptic curve discrete logarithm problem and is difficult to solve.

- **Untraceability**

  If anyone obtains the valid signature, he/she cannot link this signature to the

message. In our scheme, if the signer keep a record set (k_i, R'_i, e'_i, S'_i), where $i= 1, 2, \ldots, n$, he/she cannot trace the blind signature. We expand this as follows.

When the requester reveals n records (m_i, R_i, S_i) to the public, the signer will compute the values e_i and u', and obtain S_i and R_i, where $e_i = H(R_i \| m_i)$, and $u' = \frac{e_i}{e'_i}$. However, the signer cannot trace the blind signature by detecting whether each R_i and R_{i+1} have the same relation. Therefore, the signer cannot trace the blind signature.

Conclusion

The main advantage of ECC is more efficient, including storage efficiencies, bandwidth savings and computational efficiencies, than those of existing public key schemes with the same criterion of security and data [11]. Therefore, the proposed scheme can apply to the applications which are constrained by bandwidth, processing capacity, power availability, or storages. Such as, wireless transactions, hand-held computer or PDA, and smartcard applications. Smartcards have restricted computational power and memory, but they are ideal for protecting secret data (private keys, token, E-cash, or sensitive operations) [8, 9]. Therefore, we can combine the proposed scheme with smartcards to apply in e-Payment application.

In this article, we have proposed a blind signature scheme based on the elliptic curve discrete logarithm problem. ECC had been proven to provide more efficiency. Our scheme preserves all the characteristic of a blind signature. Our scheme can be applied to electronic commerce applications, such as e-voting or e-payment.

References

[1] J. Camenisch, J. Piveteau, and M. Stadler, “Blind signatures based on discrete logarithm problem," in Advances in Cryptology, EUROCRYPT'94, pp. 428{432, Lecture Notes in Computer Science, 950, 1994.

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

[3] C. I. Fan and C. L. Lei, “Efficient blind signature scheme based on quadratic rsidues," IEE Electronic Letters, pp. 811-813, 1996.

[4] M. S. Hwang, C. C. Lee, Y. C. Lai, "An untraceable blind signature scheme",

IEICE Transactions on Foundations, vol. E86-A, no. 7, pp. 1902-1906, 2003.

[5] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", Computer Standards & Interfaces, vol. 26, no. 2, pp. 73-84, 2004.

[6] Neal Koblitz, “Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203-209, 1987.

[7] V. Miller, ”Use of elliptic curves in cryptography," in Advances in Cryptology, CRYPTO'85, pp. 417-426, 1986.

[8] J. J. Shen, C. W. Lin, M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards", Computers & Security, Vol. 22, no. 7, pp. 591-595, 2003.

[9] J. J. Shen, C. W. Lin, M. S. Hwang, "A modified remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 49, no. 2, pp. 414-416, 2003.

[10] S. F. Tzeng and M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", Computer Standards & Interfaces, vol. 26, no. 2, pp. 61-71, 2004.

[11] Scott A. Vanstone, “Elliptic curve cryptosystem- the answer to strong, fast public-key cryptography or securing constrained environments," Information Security Technical Report, vol. 2, no. 2, pp. 78-87, 1997.

Chwei-Shyong Tsai was born in Changhua, Taiwan, Republic of China, on September 3, 1962. He received the B.S. degree in Applied Mathematics in 1984 from National Chung Hsing University, Taichung, Taiwan. He received the M.S. degree in Computer Science and Electronic Engineer in 1986 from National Center University, Chungli, Taiwan. He received the Ph.D. degree in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. Since August 2002, he has been an associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. His research interests include image authentication, information hiding, and cryptography.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC.). He received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 90 articles on the above research fields in international journals.

Pei-Chen Sung received the B.C. degree in Finance from Chaoyang University of Technology, Taichung, Taiwan, Republic of Chain (ROC). She is currently pursuing her M.S. degree in Information Management from Chaoyang University of Technology ,Taichung, Taiwan, ROC. Her current research interests include micropayment and digital signature.