An MSS Based on the Elliptic Curve Cryptosystem

Hemlal Sahu and Birendra Kumar Sharma
(Corresponding author: Hemlal Sahu)

School of Studies in Mathematics,
Pt. Ravishankar Shukla University Raipur (C.G.), 492010 India
(Email: {hemlalsahu; sharmabk07}@gmail.com)
(Received Feb. 11, 2009; revised and accepted Apr. 21, 2009)

Abstract

In 2004, a multi-signature scheme (MSS) based on the elliptic curve cryptosystem is given by Chen et al. [1]. Later, Liu and Liu [6] showed that if one of the users always sends his data in the last during each steps of the key generation and multi-signature generation phase then MSS becomes insecure. In this paper we propose a scheme which prevents the system from such insecurity. Also, in the proposed scheme, we provide security with more efficiency by considering only one point of elliptic curve in the place of two points considered in MSS.

Keywords: Digital multi-signature scheme, elliptic curve cryptosystem (ECC), elliptic curve discrete logarithm problem

1 Introduction

A digital signature is an electronic analogue of hand written signature. That is, a digital signature allows the receiver of a message to convince any third party that the message in fact originated from the sender. Digital signatures play important role in our modern electronic society since they have the properties of integrity and authentication. The integrity property ensures that the received message is not modified and the authentication property ensures that the sender is not impersonated. In well-known conventional digital signature such as Diffie-Hellman system [2], RSA system [7] and ElGamal system [3], a single signer is sufficient to produce a valid signature and anyone else can verify the validity of signature. Itakura and Nakamura [5] proposed the first multi-signature scheme in which multiple signers can co-operate to sign the same message and any verifier can verify the validity of the multi-signature. Public-key identification schemes prevent online systems or electronic cash from unauthorized access and unauthorized transfer. Such a signature scheme involving the hash function can resist the chosen-message attack and prevent the signature from being forged. The ECC is constructed from integer points on the elliptic curve in finite fields, whose basic operations include addition and multiplication under the ECC Is-ill. The operations associated with ECC are more efficient than those associated with other cryptosystems, including the RSA [7] and the DSA [3]. Besides, the ECC is applied herein to research digital signatures and is developed to promote the security and execution efficiency of a cryptosystem. A one-way hash function is designed herein with two characteristics: the output is of a fixed length, unlike the input, which is of variable length; also the length of the signed message can be reduced by applying the hash function, so that the chosen-message attack, as defined by ElGamal [3] and Harn [4], can be resisted.

2 System Initialization Phase

The preparatory procedure for initializing the system is selecting the following commonly required parameters over the elliptic curve domain.

1) A field size q, which is selected such that, $q = p$ if p is an odd prime; otherwise, $q = 2^m$, as q is a prime power.

2) Two parameters a, $b \epsilon F_q$ that define the equation of elliptic curve E over F_q ($y^2 = x^3 + ax + b \pmod q$ in the case $q > 3$, where $4a^3 + 27b^2 \neq 0 \pmod q$).

3) A finite point B whose order is a large prime number n in $E(F_q)$, where $B \neq O$ (O denotes infinity).

4) A positive integer t, which is the secure parameter, e.g., $t \geq 72$.

3 Key Generation Phase

All members of the group U_i $(1 \leq i \leq N)$ generate the keys, as follows.

Step 1. Person U_1 randomly select an integers p_1 from the interval [1, n/N], and specify p_1 as private key, and send $Y_1 = p_1 B$ to U_2.

Step 2. Person U_2 randomly selects an integer p_2 from the interval [1, n/N], and specify p_2 as private key, and send $Y_2 = p_2 Y_1 = p_2\ (p_1 B)$ to U_3.

Step 3. Continuing above process person UN randomly select an integers p_N from the interval [1, n/N], and specify p_N as private key and generate

$$Y_N \quad = \quad p_N Y_{N-1} = p_N \ldots p_2 p_1 B.$$

Step 4. $Y = p_N \ldots p_2 p_1 B$ is a group public key.

4 Multi-signature Generation Phase

Let m be the message that requires the multi signature of all the group members. To cooperatively generate the multi-signature, each signer in the group U_i $(1 \leq i \leq N)$ performs the following steps.

Step 1. Person U_N randomly select an integers q_N from the interval [1, n/N], and send $Q_N = q_N B$ to U_{N-1}.

Step 2. Person U_{N-1} randomly selects an integer q_{N-1} from the interval [1, n/N], and send $Q_{N-1} = q_{N-1} Q_N = q_{N-1}(q_N B)$ to U_{N-2}.

Step 3. Continuing above process person U_1 randomly select an integers q_1 from the interval [1, n/N], and generate

$$Q_1 = q_1 Q_2 = q_1 \ldots q_{N-1} q_N B.$$

Step 4. Taking $Q = q_1 \ldots q_{N-1} q_N B$.

Step 5. Combine m and Q into a single integer e using the following one way hash function

$$e \quad = \quad h(m, Q) \epsilon [1, 2^t].$$

Step 6. We also compute R and T as follows: U_1 sends $p_1 B$ and $q_1 B$ to U_2, U_2 sends $q_2 p_1 B$ and $p_2 q_1 B$ to U_3. Continuing above process, U_{N-1} sends $q_{N-1} \ldots p_1 B$ and $p_{N-1} \ldots p_2 q_1 B$ to U_N, and U_N computes $q_N q_{N-1} \ldots p_1 B$ and $p_N\ p_N - 1 \ldots p_2 q_1 B$.

$$Taking R \quad = \quad q_N q_{N-1} \ldots p_1 B$$

and

$$T \quad = \quad p_N p_{N-1} \ldots p_2 q_1 B.$$

Step 7. Compute $s_i' s$ according to the equation: U_1 computes

$$s_1 \quad = \quad (q_1 + p_1 e) \bmod n.$$

U_1 sends s_1 to U_2, and U_2 computes

$$s_2 \quad = \quad [(q_2 q_1 + q_2 p_1 e) + (p_2 q_1 + p_2 p_1 e)] \bmod n$$

with the help of p_2 and q_2. Similarly U_3 computes s_3. After $N-1$ steps U_N will compute

$$\begin{aligned} s_N \quad = \quad & [(q_N \ldots q_2 q_1 + q_N \ldots q_2 p_1 e) \\ & + (p_N \ldots p_2 q_1 + p_N \ldots p_2 p_1 e)] \bmod n. \end{aligned}$$

Step 8. Taking $s = [(q_N \ldots q_2 q_1 + q_N \ldots q_2 p_1 e) + (p_N \ldots p_2 q_1 + p_N \ldots p_2 p_1 e)] \bmod n$.

Step 9. Send the message m with the multi-signature (e, s) to the verifier.

5 Multi-signature Verification Phase

The verifier validates the received multi-signature (e, s), as follows.

Step 1. Compute Z using Y, R, T and (e, s) according to the equation,

$$Z \quad = \quad sB - eY - eR - T.$$

Step 2. Verify the accuracy of the following multi signature verification equation

$$e \quad = \quad h(m, Z).$$

If certifiable, accept the validity of the received multi-signature; otherwise, reject it.

Theorem 1. *The multi-signature is considered to be valid if the signer and the verifier conform to the applied protocols.*

Proof.

$$\begin{aligned} Z \quad = \quad & sB - eR - T - eY \\ = \quad & ((q_N \ldots q_2 q_1 + q_N \ldots q_2 p_1 e) + \\ & (p_N \ldots p_2 q_1 + p_N \ldots p_2 p_1 e))B - eR - T - eY \\ = \quad & qN \ldots q_2 q_1 B + q_N \ldots q_2 p_1 eB + \\ & p_N \ldots p_2 q_1 B + p_N \ldots p_2 p_1 eB - eR - T - eY \\ = \quad & Q + eR + T + eY - eR - T - eY \\ = \quad & Q. \end{aligned}$$

□

6 Security Analysis

The security with elliptic curve based discrete logarithm is more reliable in public key cryptosystems as compare to others. This is the reason why we have proposed signature scheme with elliptic curve based discrete logarithm problem. Below, we explain how several possible attacks are not possible in our proposed scheme.

Attack 1. Liu and Liu [6] showed that if one of the users always sends his data in the last of each steps during the multi-signature generation phase then the scheme given by Chen et al. [1] becomes insecure. In our scheme, key generation phase and multi-signature generation are done in two different ways i.e. if one person starts to generate key then in multi-signature generation phase his number will come in the last. Thus, our system is more secure against this attack.

Attack 2. In our scheme, key generation phase entirely depends on elliptic curve based discrete logarithm problem and the schemes with such problem are known as more reliable. This makes our scheme more secure and reliable for any possible attack. Moreover, in multi-signature scheme [1], each user has to generate the key independently whereas in our scheme, for each user key generation depends on preceding one.

Attack 3. Similarly, the first part of multi-signature key generation procedure is also based on elliptic curve discrete logarithm problem hence makes it more reliable and secure.

Attack 4. The second part of Multi-signature key generation is to find the value of s. Since it involves addition and product of integers with respect to modulo n. So we can say that finding this key is intractable. Also our system involves two additional parameters R and T not considered in scheme [1] makes the scheme more secure.

7 Efficiency Analysis

1) In our scheme, we consider only one point for key generation phase and for the first part of Multi-signature key generation phase. This makes our scheme more efficient as compare to the scheme given by Chen et al. [1] wherein two points are considered for that purpose.

2) The computational efficiency is increased for the second part of multi-signature key generation phase in our scheme by computing s only. However, in the scheme given by Chen et al. [1] double computation i.e. computation of s_1 and s_2 is required.

References

[1] T. S. Chen, K. H. Huang, and Y. F. Chung, "Digital multi-signature scheme based on the elliptic curve cryptosystem," *J. Computer Science and Technology*, vol. 19, no. 4, pp. 570, 2004.

[2] W. Diffie and M. Hellman, "New Directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[3] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, no. 4, pp. 469-472, 1985.

[4] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEEE Proceedings Computers and Digital Techniques*, vol. 141 no. 5, pp. 307-313, 1994.

[5] K. Itakura and K. Nakamura, "A public key cryptosystem suitable for digital multisignatures," *NEC Research and Development*, vol. 71, pp. 1-8, 1983.

[6] D. Liu, P. Lio, and Y. Q. Dai, "Attack on digital multi-signature scheme based on the elliptic curve cryptosystem," *Journal of Computer Science and Technology*, vol. 22, no. 1, pp. 92-94, 2007.

[7] L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications ACM*, vol. 21, no. 2, pp. 120-126, 1978.

Hemlal Sahu was born in India in 1980. He hold a degree of B.Sc and M.Sc in Mathematics from Pandit Ravishankar Shukla University Raipur, Chhattisgarh (India). He is currently a research scholar of School of Studies in Mathematics, Pandit Ravishankar Shukla University Raipur. His scientific interests lie in the fields of elliptic curve based public key cryptosystems. He is a life member of Cryptology Research Society of India.

Birendra Kumar Sharma Professor & Head, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical society and the Ramanujan Mathematical Society.