Applied Mathematical Sciences, Vol. 7, 2013, no. 73, 3615 - 3624
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2013.32121

ID-Based Signature Scheme

Using Elliptic Curve Cryptosystem

E. S. Ismail

School of Mathematical Sciences, Faculty of Science and Technology
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia
esbi@ukm.my

W. S. Wan-Daud

Institut Matematik Kejuruteraan, Universiti Malaysia Perlis
Jalan Serawak, 02000 Kuala Perlis, Perlis, Malaysia
wsuhana@unimap.edu.my

Abstract

Chung, Huang, Lai and Chen proposed an ID-based signature scheme on the elliptic curve cryptosystem. Their scheme is secure but requires $60.12T_{MUL} + 1T_H$ for signature generation and $87.24T_{MUL} + 1T_H$ for signature verification. In this article, we propose an improvement of their signature scheme with three results: The improved scheme reduces about 50% and 33% of time complexity respectively for both signature generation and signature

verification. The new scheme requires only one pair of secret and public keys but Chung et al.'s scheme needs two secret keys. The communication cost of the new scheme is only half of Chung et al.'s scheme.

Mathematics Subject Classification: 94A60

Keywords: Cryptography; Digital signature scheme; Identification scheme; Elliptic curve cryptosystem; Chosen-message attack

1 Introduction

Most developed digital signature schemes [1-5] are based on two number-theoretic problems namely factoring (FAC) [6] or discrete logarithms (DL) [7] problems. Although these schemes are secure, they are very slow and inefficient. To overcome this problem, elliptic curve cryptography [8-9] is proposed in which they utilized the hard problem called elliptic curve discrete logarithm (ECDL). The schemes based on ECDL provide smaller key size and faster computation, and therefore rapidly gained popularity [10-11]. On the other hand, Fiat and Shamir [12] successfully introduced a method of transforming identification schemes (ID) [13-15] into efficient signature schemes, such as those in [16-17]. To maximize the trade-off between security and efficiency performance, one should construct signature schemes on elliptic curve cryptosystem as proposed by Chung, Huang, Lai and Chen (CHCL) [18]. The CHLC's scheme is secure and requires complexity time $60.12T_{MUL} + 1T_H$ for signature generation and $87.24T_{MUL} + 1T_H$ for signature verification. In this article, we improve the CHLC's scheme and it turns out that the improved scheme is also secure, and needs smaller complexity time for both its signature generation and signature verification. The new scheme requires only one pair of secret and public keys but Chung et al.'s scheme needs two secret keys. The communication cost of the new scheme is only half of Chung et al.'s scheme.

The organization of this article is as follows. Section 2 presents the original CHCL's scheme. Section 3 proposes the improved signature scheme and in Section 4, we analyze the resultant efficiency and security from the scheme. Section 5 gives our conclusion.

2 Review of CHLC's scheme

We will review briefly the CHLC's scheme [18] in the following section.

The implementation of the developed scheme involves the system initialization phase, the key generation phase, the signature generation phase and the signature verification phase, as follows. In the system initialization phase, the following commonly required parameters over the elliptic curve domain are generated to initialize the scheme.

a. A field size q, where either $q = p$ in case that p is an odd prime (the common practice), or $q = 2^m$ in case that q is a prime power.
b. Two parameters $a, b \in F_q$ to define the elliptic curve equation E over F_q: $y^2 \equiv x^3 + ax + b \pmod p$ in case that $q > 3$, where $4a^3 + 27b^2 \neq 0 \pmod q$. E should be divisible by a large prime number with regard to the security issue raised by Pohlig and Hellman [19].
c. A finite point $B = (x_b, y_b)$ whose order is a large prime number in $E(F_q)$, where $B \neq O$ (O denotes infinity) such that the order of B is n.
d. Two points B_1 and B_2 with order n in the group $E(F_q)$.
e. A positive integer t, which is the secure parameter, say $t \geq 72$ [19].

In key generation phase, the signer U generates his public key by randomly selects two integers (d_1, d_2) from the interval $[1, n-1]$ as the secret key pair and computes the corresponding public key Y to (d_1, d_2), as $Y = d_1B_1 + d_2B_2$.

To create a signature for a message m, the signer executes the following steps:

Step 1 Randomly select two numbers (r_1, r_2) from $[1, n-1]$ to compute Q over $E(F_q)$.

$$Q = r_1B_1 + r_2B_2$$

Step 2 Convert the message m and the value Q into one integer e using hash-function operation.

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

Step 3 Generate the signature (s_1, s_2), as follows.

$$s_1 \equiv r_1 + d_1e \pmod n, \text{ and}$$
$$s_2 \equiv r_2 + d_2e \pmod n$$

Step 4 Send (s_1, s_2) to the verifier.

After receiving the signature (s_1, s_2), the verifier calculates $Z = s_1B_1 + s_2B_2 - eY$ and $\overline{e} = h(m, Z)$. The verifier validates the signature if $\overline{e} = e$, otherwise rejects it.

3 The improved signature scheme

The system parameters of the proposed scheme are the same as those of CHLC's scheme as described previously. In key generation phase, the signer U generates his public key by randomly select an integer d from the interval $[1, n-1]$ as the secret key and compute the corresponding public key Y to d, as $Y = dB_2$.

To create a signature for a message m, the signer executes the following steps:

Step 1 Randomly select a number r from $[1, n-1]$ to compute Q over $E(F_q)$.

$$Q = B_1 + rB_2$$

Step 2 Convert the message m and the value Q into one integer e using hash-function operation.

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

Step 3 Generate the signature, s as follows.

$$s \equiv r + de (\mathrm{mod}\, n)$$

Step 4 Send (s, e) to the verifier.

After receiving the signature (s, e), the verifier calculates $Z = sB_2 + B_1 - eY$ and $\overline{e} = h(m, Z)$. The verifier validates the signature if $\overline{e} = e$, otherwise reject it.

4 Security analysis and performance evaluation

4.1 Correctness

The correctness of the scheme is shown as below:

Theorem 1. If the above signature generation runs smoothly, then the verifier can validate the received signature, (s, e).

Proof: Note that

$$Z = sB_2 + B_1 - eY = (r + de)B_2 + B_1 - eY = rB_2 + B_1 + deB_2 - eY = Q + eY - eY = Q.$$

4.2 Security considerations

The security analysis of our improved signature scheme is similar to that of CHLC's scheme. The difficulties associated with the attacks are based on the solution of the elliptic curve discrete logarithm problem (ECDL), and the security resulted from such problems is still sufficient under that reasonable computational complexity. Some possible attacks by which an adversary (Adv) may try to take down the improved scheme will be analyzed as follows.

4.2.1 Attack 1

The case when the Adv intends to derive the secret key d from the public key, $Y = dB_2$. Further, say that $Q = Y$, then $B_1 + rB_2 = dB_2$. Note that $r = d$ if and only if $B_1 = O$. Thus if the Adv attempts to derive the secret key, d, he has to encounter the difficulty of solving the ECDL problem.

If the signer chooses a same integer, r, to sign two different messages m_1 and m_2 then the Adv learns that

$s_1 \equiv r + de_1 (\mathrm{mod}\, n)$ and $s_2 \equiv r + de_2 (\mathrm{mod}\, n)$

where $e_1 = h(m_1, Q)$ and $e_2 = h(m_2, Q)$. If this happen, then the Adv may obtain the secret key d by computing $d \equiv (s_1 - s_2)(e_1 - e_2)^{-1} (\mathrm{mod}\, n)$.

4.2.2 Attack 2

The case when the Adv wishes to forge an individual signature (s, e) for a message, m. To forge a valid signature for a message m, the Adv first randomly selects a point Z and calculate $e = h(m, Z)$. Next the Adv tries to obtain s from the following equation

$Z = sB_2 + B_1 - eY$

where B_1, B_2 and Y are public data. The method of finding a number s, is also depend on ECDL problem thus it is infeasible in reasonable computational security.

4.3 Performance evaluation

We compare the improved scheme and CHLC's scheme in terms of the number of keys (secret key, SK and public key, PK), computational complexity in both signature generation and signature verification and communication cost for each scheme. To describe the computational complexity, we need Table 1 which defines the various notations and Table 2 that shows the conversion of various operation units to the time complexity for executing the modular multiplication [20].

Table 1: Definition of given notations

Notations	Definition
$\boldsymbol{T_{MUL}}$	Time complexity for executing the modular multiplication
$\boldsymbol{T_{EXP}}$	Time complexity for executing the modular exponentiation
$\boldsymbol{T_{ADD}}$	Time complexity for executing the modular addition
$\boldsymbol{T_{EC-MUL}}$	Time complexity for executing the elliptic curve multiplication
$\boldsymbol{T_{EC-ADD}}$	Time complexity for executing the elliptic curve addition
$\boldsymbol{T_H}$	Time complexity for executing the hash-function

Table 2: Conversion of various operations units to T_{MUL}

$T_{EXP} \approx 240T_{MUL}$	$T_{EC-MUL} \approx 29T_{MUL}$	$T_{EC-ADD} \approx 0.12T_{MUL}$	T_{ADD} is negligible

The following Table 3 summarizes differences between the two schemes. From the statistics in Table 3, it easily can be seen that in both signature generation and signature verification, the number of modular multiplications required by our scheme is 50% and 33% less than that required in CHLC's scheme.

Table 3: Comparison between CHLC's scheme and the improved scheme

Items	Time Complexity of CHLC's scheme	Complexity in $\boldsymbol{T_{MUL}}$ of CHLC's scheme	Time Complexity of our scheme	Complexity in $\boldsymbol{T_{MUL}}$ of our scheme
Signature generation	$2T_{EC-MUL} + T_{EC-ADD} + 2T_{ADD} + 2T_{MUL} + T_H$	$60.12T_{MUL} + T_H$	$T_{EC-MUL} + T_{EC-ADD} + T_{ADD} + T_{MUL} + T_H$	$30.12\,T_{MUL} + T_H$
Signature verification	$3T_{EC-MUL} + 2T_{EC-ADD} + T_H$	$87.24\,T_{MUL} + T_H$	$2T_{EC-MUL} + 2T_{EC-ADD} + T_H$	$58.24\,T_{MUL} + T_H$
Number of keys	PK = 1, SK = 2		PK = 1, SK = 1	
Communication cost	$\boldsymbol{6\lvert n\rvert}$		$\boldsymbol{3\lvert n\rvert}$	

We also can estimate the speedup of the improved scheme in comparison with CHLC's scheme by neglecting the time complexity of the hash-function. Note that, the minimum requirement of time complexity for any ECDL problem-like signature scheme is given by $1T_{EC-MUL} + 1T_{EC-ADD} + T_H$ or equivalent to $29.12T_{MUL}$ in both for signature generation and signature verification. If a digital signature scheme needs $29.12T_{MUL}$ for both signature generation and signature verification, we say that signature scheme performs 100% efficiency. To estimate our scheme, we use the following formulas:

$$\text{Speedup} = 100\% - \left(\frac{\text{Time complexity of our scheme (in } T_{MUL}) \; - 29.12T_{MUL}}{\text{Time complexity of our scheme (in } T_{MUL})}\right) \times 100\%.$$

This formula compares any scheme with scheme 100% efficiency. The speedup of signature generation and verification phases for CHCL's and our schemes can be calculated as below:

For CHCL's scheme, we have

a. (Signature Generation) $\text{Speedup} = 100\% - \left(\frac{60.12-29.12}{60.12}\right) \times 100\% = 48.44\%$
b. (Signature Verification) $\text{Speedup} = 100\% - \left(\frac{87.24-29.12}{87.24}\right) \times 100\% = 33.38\%.$

For the improved scheme, we have

a. (Signature Generation) $\text{Speedup} = 100\% - \left(\frac{30.12-29.12}{30.12}\right) \times 100\% = 96.68\%$
b. (Signature Verification) $\text{Speedup} = 100\% - \left(\frac{58.24-29.12}{58.24}\right) \times 100\% = 50\%.$

Therefore, in comparison to the method in CHLC's scheme, the signature generation and signature verification phases of our method performs 96.68% and 50% efficiency respectively. The CHCL's scheme performs only 48.44% and 33.38% efficiency respectively for signature generation and signature verification. From Table 3 and the above estimation, it is clear that our scheme improves and raises greatly the efficiency of signature generation and signature verification.

5 Conclusions

In this article, we have proposed an improved ID-based digital signature scheme on elliptic curve cryptosystem. The security of our improved scheme is equivalent to those of CHLC's scheme based on the hardness of solving elliptic curve discrete logarithm problem. We have also demonstrated that, our scheme required less number of modular multiplications than that of CHLC's scheme. We too managed to reduce the number of keys and communication cost compared to CHLC's scheme. Finally, we conclude that our scheme improved by 96.68% and 50% respectively in both signature generation and signature verification than CHLC's scheme.

Acknowledgement: We acknowledge the financial support received from Universiti Kebangsaan Malaysia under the Research Grant UKM-DLP-2011-028.

References

[1] E. S. Ismail, N. M. F. Tahat and R. R. Ahmad. A new digital signature scheme based on factoring and discrete logarithms. *Journal of Mathematics and Statistics*, 4(4), 2008, pp: 222-225.

[2] N. M. F. Tahat, S. M. A. Shatnawi and E. S. Ismail. 2008. A New Partially Blind Signature Based on Factoring and Discrete Logarithms. *Journal of Mathematics and Statistics*, 4(2), 2008, pp:124-129.

[3] E. S. Ismail, Y. A. Hasan, A new version of El-Gamal signature scheme. *Sains Malaysiana* 35(2), 2006, pp. 69-72.

[4] K. Rabah, Elliptic curve elgamal encryption and signature schemes. *Inform. Technol. J*., 4(3), 2005, pp. 299-306.

[5] S. F. Tzeng, M. S. Hwang, Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem, *Comput. Standards and Interfaces* 26(2), 2004, pp. 61-71.

[6] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signature and public-key cryptosystem. *Communication of the ACM*, 21(2), 1978, pp. 120-126.

[7] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory*, IT-31(4), 1985, pp. 469-472.

[8] N. Koblizt, Elliptic curve cryptosystem, *Mathematics of Computation* 48(177), 1987, pp. 203-209.

[9] V. S. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology-Proceedings of Crypto'85*, LNCS, vol. 218, Springer, 1986, pp. 417-426.

[10] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), *International Journal of Information Security*, vol. 1, (1), Springer, 2001, pp. 36-63.

[11] W. J. Caelli, E. P. Dawson, S. A. Rea, Elliptic curve cryptography and digital signatures, *Computer & Security* 18(1), 1999, pp. 47-66.

[12] A. Fiat, A. Shamir, How to prove yourself: practical solutions to identification and signature problems, *Advances in Cryptology-Proceedings of Crypto'86*, LNCS, vol. 263, Springer, 1987, pp. 186-194.

[13] C. Popescu, An identification scheme based on the elliptic curve discrete logarithm, *The 4th International Conference on High-Performance Computing in the Asia-Pacific Region*, vol. 2, 2000, pp. 624-625.

[14] D. H. Nyang, J. S. Song, Knowledge-proof based versatile smart card verification protocol, *AMC SIGCOMM Computer Communication Review*, 30(3), 2000, pp. 39-44.

[15] A. M. Allam, I. I. Ibrahim, I. A. Ali, A. E. H. Elsawy, Efficient zero-knowledge identification scheme with secret key exchange, *Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems*, vol. 1, 2003, pp. 516-519.

[16] C. P. Schnorr, Efficient signature generation by smart cards, *Journal of Cryptology* 4(3), 1999, pp. 161-174.

[17] T. Okamoto, Provably secure and practical identification schemes and corresponding signature schemes, *Advances in Cryptology-Proceedings of Crypto'92*, LNCS, vol. 740, Springer, 1992, pp. 31-53.

[18] Y. F. Chung, K. H. Huang, F. Lai, T. S. Chen, ID-based digital signature scheme on the elliptic curve cryptosystem, *Computer Standards and Interfaces* 29, 2007, pp. 601-604.

[19] S. C. Pohlig, M. E. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, *IEEE Transactions on Information Theory* 24(1), 1978, pp. 106-110.

[20] N. Koblizt, A. Menezes, S. Vanstone, The state of elliptic curve cryptography, *Design, Codes and Cryptography* 19, 2000, pp. 173-193.