ID-based digital signature scheme on the elliptic curve cryptosystem

Yu Fang Chung^{a,*}, Kuo Hsuan Huang^a, Feipei Lai^{a,b}, Tzer Shyong Chen^c

^a Electrical Engineering Department, National Taiwan University, Taiwan

^b Computer Science and Information Engineering Department, National Taiwan University, Taiwan

^c Information Management Department, Tunghai University, Taiwan

Received 5 August 2006; received in revised form 24 December 2006; accepted 27 January 2007

Available online 3 February 2007

Abstract

The work presents a digital signature scheme on the elliptic curve cryptosystem, which is integrated with the identification scheme by Popescu [C. Popescu, An identification scheme based on the elliptic curve discrete logarithm problem, The 4th International Conference on High-Performance Computing in the Asia-Pacific Region, vol. 2 (2000) 624–625] using a one-way hash function. For making the trade-off of performance and security stand to benefit most, the proposed scheme is constructed on the elliptic curve cryptosystem. The scheme protects the signer from chosen-message attack and also identifies a forged signature.

© 2007 Elsevier B.V. All rights reserved.

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

1. Introduction

The Fiat–Shamir method of transforming identification schemes into signature schemes [1] yields efficient signature schemes, and is thus very popular. It starts with a three-move identification between a prover and a verifier. The prover who is the holder of a secret key sk sends a message cmt , known as a commitment, to the verifier. On receiving the commitment, the verifier returns a challenge ch . Then, the prover provides a response rsp . Finally, the verifier takes the prover's public key pk and the conversation $cmt||ch||rsp$ and applies a verification algorithm V to them to obtain a decision bit; the verifier accepts if $Dec = 1$. Most identification schemes are based on zero-knowledge interactive proofs [14], such as those in [1,2,3,6]. A secure digital signature scheme can be constructed using an interactive identification scheme and a hash function. When the identification scheme is converted to a signature scheme, the verifier's role is replaced by the hash function. A digital signature scheme resulting from the above paradigm has equal complexity as the starting identification scheme.

Owing to its efficiency and simple design, the Fiat–Shamir paradigm, both in theory and practice, rapidly gained popularity. The design of several digital signature schemes, including [4,17], follows this paradigm. The paradigm has also been applied in other domains to form forward and secure digital signature schemes [8] and to achieve better and exact security [15].

Different from the identification scheme of other works that used factorization problem or discrete logarithm problem as the basic concept, Popescu proposed an identification scheme [3] based on the elliptic curve discrete logarithm problem. Given the superior security and efficiency, the work applies the identification scheme proposed by Popescu [3] to develop a digital signature scheme. Such a signature scheme, involving the hash function, achieves to resist the security from the chosen-message attack and to prevent the signature from forgery.

To optimize the trade-off between performance and security, the proposed scheme is based on the elliptic curve cryptosystem (ECC). The ECC was initiated by Koblitz [11] and Miller [18], where the security was established on the discrete logarithm problem over the points on an elliptic curve, called ECDLP. The basic operations are the execution of integer points on the elliptic curve over finite fields, including addition and

* Corresponding author.

E-mail address: d92921014@ntu.edu.tw (Y.F. Chung).

multiplication. The operations associated with the ECC are more efficient than those associated with other cryptosystems, like the RSA and the DSA security solutions. Owing to the fact that the ECC has a smaller key size and faster computation, therefore it is being gradually given more importance by the academic and industrial circles. In recent years, it has been widely established among international standards, for instance, ISO 11770-3, ANSI X9.62, IEEE P1363, and FIPS 186-2, etc.

In the following, Section 2 presents the proposed ID-based digital signature scheme. Section 3 analyzes the resultant efficiency and security from the scheme. Finally, Section 4 draws the conclusions.

2. Proposed solution to digital signature scheme

In the work, the zero-knowledge based identification scheme by Popescu [3] is transformed into a digital signature scheme through conversion of one-way hash function. A one-way hash function is provided with two characteristics: the output is of a fixed length instead of the variable length of the input; also, the length of the signed message can be reduced, so that the chosen-message attack as defined by ElGamal [16] and Harn [7] can be prevented. The proposed scheme involves the one-to-one interactions to execute the system initialization phase, the key generation phase, the signature generation phase and the signature verification phase, as follows.

2.1. System initialization phase

The system initialization phase proceeds with the following commonly required parameters over the elliptic curve domain.

- (1) 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.
- (2) Two parameters $a, b \in F_q$ to define the elliptic-curve equation E over F_q : $y^2 = x^3 + ax + b \pmod{q}$ in case that $q > 3$, where $4a^3 + 27b^2 \not\equiv 0 \pmod{q}$. E should be divisible by a large prime number with regard to the security issue raised by Pohlig and Hellman [13].
- (3) 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 .
- (4) Two points B_1 and B_2 with order n in the group $E(F_q)$.
- (5) A positive integer t , which is the secure parameter, e.g. $t \geq 72$ [6].

2.2. Key generation phase

Signer U generates the individual public key, as follows.

- Step 1 Randomly select two integers (d_1, d_2) from the interval $[1, n-1]$ as the secret-key pair.
- Step 2 Compute the corresponding public key Y to (d_1, d_2) , as follows.

$$Y = d_1B_1 + d_2B_2$$

2.3. Signature generation phase

Signer U generates the signature for the message m , as follows.

- 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.

$$\begin{aligned} s_1 &= r_1 + d_1e \pmod{n} \\ s_2 &= r_2 + d_2e \pmod{n} \end{aligned}$$

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

2.4. Signature verification phase

The verifier confirms the validity of the signature for m , as follows:

- Step 1 Determine Z following $Z = s_1B_1 + s_2B_2 - eY$.
- Step 2 Determine e following $e = h(m, Z)$.
- Step 3 If the resulting e meets with the received one, then validate the signature; otherwise, reject it.

Theorem 1. *Following the applied protocol, the Z and Q is mutually convertible using the signature (s_1, s_2) , then the digital signature can be validated.*

Proof .

$$\begin{aligned} Z &= s_1B_1 + s_2B_2 - eY = [(r_1 + d_1e) \pmod{n}]B_1 \\ &\quad + [(r_2 + d_2e) \pmod{n}]B_2 - eY = r_1B_1 + d_1eB_1 \\ &\quad + r_2B_2 + d_2eB_2 - eY = (r_1B_1 + r_2B_2) + e(d_1B_1 + d_2B_2) \\ &\quad - eY = Q + eY - eY = Q \end{aligned}$$

From the above derivation, it can be proven that $h(m, Z) = h(m, Q)$. $\square$

3. Analyses of security and performance

3.1. Security considerations

The difficulties associated with the attacks are based on the solution of the elliptic curve discrete logarithm problem (ECDLP), and the security resulted from such problems is still sufficient under the reasonable computational complexity.

3.1.1. Attack 1

The case when an attacker intends to derive the secret-key pair (d_1, d_2) from the public key Y .

Table 1
Definition of given notations

Notations	Definition
T_{MUL}	Time complexity for executing the modular multiplication
T_{EXP}	Time complexity for executing the modular exponentiation
T_{ADD}	Time complexity for executing the modular exponentiation
$T_{\text{EC-MUL}}$	Time complexity for executing the multiplication of a number and an elliptic curve point
$T_{\text{EC-ADD}}$	Time complexity for executing the addition of two points in an elliptic curve

3.1.2. Security analysis 1

In the typical digital signature schemes such as ECDSA [5], a public key only corresponds to one secret key. Given the secret key d , let the public key Y be derived according to the equation $Y=dB$, and let the signature Q be derived using a random number r following the equation $Q=rB$. If Q equals to the public key Y , then the corresponding secret key is the same as r , as shown below.

$$Q = rB$$

$$Y = dB$$

That is, r equals d in the case $Q=Y$. In regard to the problem, the proposed scheme generates the public key Y using a secret-key pair (d_1, d_2) and two points B_1 and B_2 . If an attacker attempts to derive the secret-key pair (d_1, d_2) from the public key, he has to encounter the difficulty of solving the ECDLP.

3.1.3. Attack 2

The case when an attacker intends to forge an individual signature (e, s_1, s_2) for a message m .

3.1.4. Security analysis 2

To forge a valid individual signature for a message m , an attacker randomly selects a point Z to determine e following $e=h(m, Z)$. In addition to Z and e , the attacker derives the signature (s_1, s_2) by the public data B_1, B_2 and Y following $Z=s_1B_1+s_2B_2-eY$. Such solutions of unknown numbers s_1 and s_2 here also depend on the ECDLP, and it is infeasible in reasonable computational security.

3.2. Performance

Nyang and Song [6] proposed an efficient digital signature scheme, which also resulted from the identification scheme. In the scheme, the authors proved that digital signature scheme proposed by them is superior in performance to other RSA-like schemes and other well known signature schemes like Schnorr's. Therefore, we shall compare our proposed scheme to Nyang and Song's scheme for evaluation of performance.

Table 2
Conversion of various operation units to TMUL

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

Table 3
Required time complexity in unit of TMUL for ID-based digital signature schemes

Items	Scheme by Nyang and Song		Proposed scheme	
	Time complexity	Complexity in T_{MUL}	Time complexity	Complexity in T_{MUL}
Signature generation	$2T_{\text{EXP}}+1$	481	$2T_{\text{EC-MUL}}+1$	60.12
	$T_{\text{MUL}}+1$	$T_{\text{MUL}}+1$	$T_{\text{EC-ADD}}+2$	$T_{\text{MUL}}+1$
	Hashing	Hashing	$T_{\text{ADD}}+2$	Hashing
Signature verification	$2T_{\text{EXP}}+1$	481	$3T_{\text{EC-MUL}}+2$	87.24
	$T_{\text{MUL}}+1$	$T_{\text{MUL}}+1$	$T_{\text{EC-ADD}}+1$	$T_{\text{MUL}}+1$
	Hashing	Hashing	Hashing	Hashing

Table 1 defines the various notations. In Table 2, the conversion of various operation units to the time complexity for executing the modular multiplication is given based on the reference [10]. Table 3 summarizes differences between these two schemes. From the statistics in Table 3, it can be seen that be it the signature generation phase or the signature verification phase, the number of modular multiplications required by our scheme is less than that required by Nyang and Song's scheme. Therefore, our scheme can substantially raise the efficiency of signature generation and signature verification.

4. Conclusions

The security of Nyang and Song's digital signature scheme [6] is constructed on the integer factorization problem while the security of the proposed scheme is based on the difficulty of solving the elliptic curve discrete logarithm problem. According to [9], the elliptic curve discrete logarithm problem is significantly more difficult than the integer factorization problem. For the most part, the well-known RSA system [12] must use 1024 bit keys, only then can it attain computationally reasonable security; the ECC needs only 160 bit keys. So, at the same level of security, the speed of ECC is several times faster than RSA system; it can also saves on key storage space. Clearly, whether it is in terms of security or in performance, the proposed scheme is superior to Nyang and Song's signature scheme. Since implemented on the elliptic curve cryptosystem, the proposed scheme enables to reach the best trade-off between security and efficiency.

References

- [1] 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.
- [2] A.M. Allam, I.I. Ibrahim, I.A. Ali, A.E.H. Elsayy, 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.
- [3] C. Popescu, An identification scheme based on the elliptic curve discrete logarithm problem, *The 4th International Conference on High-Performance Computing in the Asia-Pacific Region*, vol. 2, 2000, pp. 624–625.
- [4] C.P. Schnorr, Efficient signature generation by smart cards, *Journal of Cryptology* 4 (3) (1991) 161–174.

- [5] 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.
- [6] D.H. Nyang, J.S. Song, Knowledge-proof based versatile smart card verification protocol, *ACM SIGCOMM Computer Communication Review* 30 (3) (July 2000) 39–44.
- [7] L. Harn, Group-oriented (t , n) threshold digital signature scheme and digital multisignature, *IEE Proceedings—Computers and Digital Techniques*, vol. 141, (5), 1994, pp. 307–313.
- [8] M. Abdalla, J.H. An, M. Bellare, C. Namprempre, From identification to signatures via the Fiat–Shamir transform: minimizing assumptions for security and forward-security, *Advances in Cryptology—Proceedings of Eurocrypt '02*, LNCS, vol. 2332, Springer, 2002, pp. 418–433.
- [9] NIST, DRAFT Special Publication 800-57, Recommendation on key management, January 2003, <http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf>.
- [10] N. Koblitz, A. Menezes, S. Vanstone, The state of elliptic curve cryptography, *Designs, Codes and Cryptography* 19 (2000) 173–193.
- [11] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* 48 (177) (1987) 203–209.
- [12] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* 21 (2) (1978) 120–126.
- [13] 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) 106–110.
- [14] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof-systems, *Proceedings of the 17th Annual ACM Symposium on Theory of computing*, 1985, pp. 291–304.
- [15] S. Micali, L. Reyzin, Improving the exact security of digital signature schemes, *Journal of Cryptology* 15 (1) (2002) 1–18.
- [16] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory* 31 (4) (1985) 469–472.
- [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] V.S. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology—Proceedings of Crypto '85*, LNCS, vol. 218, Springer, 1986, pp. 417–426.