Applied Mathematical Sciences, Vol. 6, 2012, no. 28, 1363 - 1369

New ID-Based Digital Signature Scheme on Factoring and Discrete Logarithms

Nedal Tahat, Zead Mustafa and A. K. Alomari

Department of Mathematics, Faculty of Sciences
The Hashemite University, Zarqa 13133, Jordan
nedal@hu.edu.jo , zmagablh@hu.edu.jo, abdomari2008@yahoo.com

Abstract

The past years have seen many attempts to construct identity based signature schemes on a single hard problem, like factoring or discrete logarithms. But in the near future, those systems will no longer be secure if the solution of factoring or discrete logarithms problems is discovered. In this paper, we propose a new identification based signature scheme on factoring (FAC) problem and discrete logarithms (DL) problems. Having concatenated FAC and DL hard problems, the presented scheme has solid structure and will hopelessly leave the eavesdropper baffled. The performance analysis has been given to describe the proposed scheme in terms of security level. In addition, the scheme protects the signer from chosen-message attack and also identifies a forged signature. At the moment, no malicious attacks are capable of ‘‘breaking” this scheme in a reasonable amount of time obviously. We also show that the performance of the scheme requires only minimal operation both in signing and verifying logarithms and is resistant to attack.

Keywords: Digital signature scheme; Identification scheme; Factoring; Discrete logarithm; Chosen-message attack

1 Introduction

A signature scheme is a method for signing a message stored in electronic form. As such, a signed message can be transmitted over a computer network. In 1984, Shamir [19] introduced the concept of ID-based cryptosystems, in which the private key of an entity was generated from his identity information and a master key of a trusted third party called a private key generator. The first ID-based signature (IBS) scheme was proposed by Shamir [3]. Later, many ID-based signature schemes were presented in [4, 7, 10, 11]. Most identification schemes are based on zeroknowledge

interactive proofs [12], such as those in [1,2,5,6]. 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. Popescu proposed an identification scheme [5] based on the elliptic curve discrete logarithm problem. Given the superior security and efficiency, the work applies the identification scheme proposed by Popescu [5] 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. However, all developed identification based signature schemes in the literature are based on single hard problems, like factoring, discrete logarithm, or elliptic curve discrete logarithm problem such as [4, 7, 10, 11, 14]. In the future, if one finds a solution of one of these problems, the related identification based signature schemes will be no longer secure. Thus, in this study we proposed a secure identification based signature scheme on discrete logarithms and factoring problem.
In the following, section 2 presented the proposed ID-based digital signature scheme. Section 3 analyzes the resultant security and efficiency from the new scheme and finally, Section 4 gives our conclusions.

2 Proposed solution to digital signature scheme

Using a one-way hash function, the identification scheme developed by Popescu [5], based on zero-knowledge, can be transformed into a digital multi-signature scheme. 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 E1Gamal [13] and Harn [8], can be resisted. 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 defined multiplicative groups.

- $h(.)$ cryptographic hash function whose output is a *t*-bit length. If a security parameter t has a large value, the speed becomes slow. For the identification scheme, t = 20 is enough for the most applications, $t = 45$ for national security applications. For the digital signature, $t \geq 72$ is enough [6].
- p is a large prime and n is a factor of $p - 1$ that is the product of two safe prime $\bar{p}$ and $\bar{q}$ i.e, $n = \bar{p}\bar{q}$
- $\varphi(n) = (\bar{p} - 1)(\bar{q} - 1)$ is a phi-Euler function.
- Generate integer g of the multiplicative group Z_p^* with order n in the group Z_p^*
- $\gcd(a, b)$ is the greatest common divisor of a and b.

2.2 Key generation phase

Signer $\mathcal{S}$ generates the individual public keys, as follows

1) Picks randomly $e \in Z^*_{\varphi(n)}$ and calculates secret key $d \equiv e^{-1} \pmod{(n)}$)

.

2) Randomly select two integers x from the interval $[1, n-1]$ as the secret keys.
3) Compute the corresponding public key y to x, as follows

$$y \equiv g^x (\text{mod } p)$$

Thus the public and secret keys of the system are respectively given by (y, e) and (d, x)

2.3 Signature generation phase

Signer $\mathcal{S}$ generates the signature for the message *m*, as follows.

1) Randomly select number $k \in Z^*_n$ and computes

$$L \equiv g^k \text{ (mod } p)$$
$$Q \equiv L^L \pmod{p}$$

2) Convert the message *m* and the value Q into one integer w using has-function operation.

$$w = h(m, Q) \in \{0, \dots, 2^t - 1\}$$

3) Generate the signature s as follows.

$$s = (w^e\, x + k\, L)^d \text{ (mod } n)$$

Send (w, s) to the verifier.

2.4 Signature verification phase

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

1) Determine R following

$$R \equiv g^{s^e}\, y^{-w^e} \pmod{p}$$

2) Determine w following

$$w \equiv h(m, R) \tag{1}$$

If the resulting w meets with the received one, then validate the signature; otherwise, reject it.

Theorem 1: *Followings the applied protocol, the R and Q is mutually convertible using the signature s , then the digital signature can be validated.*

Proof: The equation (1) in Signature verification phase is true for valid signatures since

$$
\begin{aligned}
R \equiv g^{s^e}\, y^{-w^e} \equiv\ & g^{((w^e x + kL)^d)^e} (g^x)^{-w^e} \\
& \equiv g^{w^e x}\, g^{kL} g^{-w^e x} \\
& \equiv (g^k)^L \pmod{p} \\
& \equiv L^L \\
& \equiv Q
\end{aligned}
$$

From the above derivation, it can be proven that $h(m, R) = h(m, Q) = w$.

3 Security and Performance Analyses

In this section, we discuss some security properties of our ID-based signature scheme; also we show the performances analysis of our scheme.

3.1 Security considerations

Now we shall show some possible attacks by which an adversary (Adv) may try to take down the new developed identification scheme. The difficulties associated with the attacks are based on the solution of the DL and FAC problems. For every attack, we define the attack and give reason why this attack would be failed.

3.1.1 Attack 1

Adv wishes to obtain secret keys $(x,\ d)$ using all information that available from the system. In this case, Adv needs to solve $y \equiv g^x \pmod{p}$ and $d \equiv e^{-1} \pmod{\varphi(n)}$ which are clearly infeasible because the difficulty of solving DL and FAC.

3.1.2 Attack 2

The case when an adversary (Adv) intends to forge an individual signature (w, s) for message m. To forge a valid individual signature for a message m, an attacker randomly selects a point R to determine w following $w \equiv h(m, R)$. In addition to R and w, the Adv derive signature s by the public data g, y and e following $R \equiv g^{s^e}\, y^{-w^e} \pmod{p}$. Such solutions of unknown numbers s here also depend on the DLP and FAC , and it is infeasible in reasonable computational security. Assume now DL is breakable. Then the Adv knows s^e but still does not now s because he learns nothing about d . Now assume that FAC is breakable. The he knows d but does not know s^e (DL).

3.1.3 Attack 3

It is assumed that Adv is able to solve DLP. In this case, Adv knows x and can generate or calculate the number s but in signing generating. Unfortunately, he does not know d hence cannot compute the number s because the difficulty of breaking FAC. Thus fails to produce the signature (w, s) .

3.1.4 Attack 4

It is assumed that Adv is able to solve FAC. Thus, he knows the prime factorization of n. In this case, Adv knows d. However, he cannot compute s since no information is available for x. Thus fails to produce the signature (w, s) .

3.2 Performances

The performance of our scheme is described in terms of number of keys, computational complexity and communication costs. We use the following notations to analyze the performance of our scheme.

- T_{mul} Time complexity for executing the modular multiplication
- T_{exp} Time complexity for executing the modular exponentiation
- T_{inv} Time complexity for executing the modular inverse computation
- T_h Time complexity for performing hash function

We ignore the negligible time performing for modular addition. The performance of our proposed signature scheme is summarized as follows: The number of secret keys (SK) and public keys (PK) of the scheme are respectively given by SK = 2 and PK = 2. The computational complexity for the key generation, signing generation and verification is given by the following Table 1 and the last column converts various operation units to T_{mul} where $T_{exp} \approx 240T_{mul}$ given by Koblitz, Menezes and Vanstone [9]

Table 1
Time complexity in unit of T_{mul} for our scheme

Items	Time complexity	Complexity in T_{mul}
Key generation	$T_{exp} + T_{inv}$	$240T_{mul} + T_{inv}$
Signature generation	$4T_{exp} + T_{mul} + T_h$	$961T_{mul} + T_h$
Signature verification	$4T_{exp} + T_{mul} + T_h$	$961T_{mul} + T_h$

The communication costs or size of parameters of the scheme (both signature generation and verification) is $|n| + 3|p|$ where $|a| +$ denotes the bit-length of a. Nyang and song [6] proposed an efficient digital signature scheme, which also result from the identification scheme. In the scheme, the authors proved that signature scheme proposed by the superior in performance to other RSA-like scheme and other well known signature sckeme Schnorr's. In Nyang and song [6] scheme needs $481T_{mul} + T_h$ in both signature message and in its verifying signature. Note that the efficiency of ours scheme no less frequently on the efficiency of scheme by Nyang and song. The little increase in the time complexity in our scheme compared with scheme by Nyang and song is contributed by use of two hard problems but yet the scheme provides longer security than schemes based on a single problem.

4 Conclusion

In this study, we have proposed a new ID-based signature scheme based on two hard problems; factoring and discrete logarithms. The scheme offers a longer/higher level of security than that scheme based on a single hard problem. Furthermore, the proposed scheme requires only $961T_{mul} + T_h$ and $961\ T_{mul} + T_h$ respectively for both signature generation and verification. We considered some possible attacks and demonstrated that the proposed scheme would be secure against those attacks.

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 and A. E. H. Elsawy. Efficient zeroknowledg 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] A. Shamir. Identity-based cryptosystems and signature schemes, In: *Blakely, G.R. Chaum, D. (eds.) CRYPTO 1984. LNCS*, vol. 196, pp. 47–53. Springer, Heidelberg (1985).

[4] C. J. Cha, H. J. Cheon. An identity-based signature from gap diffie-hellman groups. In: *Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 18–30. Springer, Heidelberg* (2002).

[5] 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.

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

[7] F. Hess. Efficient identity based signature schemes based on pairings. In: *Nyberg, K., Heys, H.M.* (eds.) SAC 2002. LNCS, vol. 2595, pp. 310–324. Springer, Heidelberg (2003)

[8] L. Harn. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. *IEE Proceedings-Computers and Digital Techniques*, vol. 141(5), (1994), 307- 313.

[9] M. N. Koblitz and S. Vanstone. The state of elliptic curve cryptography. *Design, Codes and Cryptography* 19, (2000), 173-193.

[10] P. G. Kenneth. ID-based signatures from pairings on elliptic curves. *Cryptology Print Archive, Report* 2002/004 (2002), http://eprint.iacr.org/

[11] R. Sakai, K. Ohgishi and M. Kasahara,.: Cryptosystems based on pairing. In: *SCIS 2000, Okinawa, Japan* (2000).

[12] S. Goldwasser, S. Micali and C. Rackoff, The knowledge complexity of interactive proof-systems, *Proceedings of the 17th Annual ACM Symposium on Theory of computing*, (1985), pp. 291–304.

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

[14] Y. Chung, K. Huang, and T. Chen. ID-based digital signature scheme on the elliptic curve cryptosytem. *Computer Standards and Interface* 29 (2007), 601-604.

Received: September, 2011