Meta-He Digital Signatures Based on Factoring and Discrete Logarithms

SHUN-FU PON, ERL-HUEI LU and YA-CHENG LU
Department of Electrical Engineering
Chang Gung University
259 Wen-Hwa 1st Road, Kwei-San, Tao-Yuan
TAIWAN, R.O.C.

Abstract: - This study investigates all variations of the He's digital signature scheme based on factoring and discrete logarithms. In contrast to three modular exponentiation computation, the optimal two schemes of generalized He's signature verification reveals that only two modular exponentiation is needed for signature verification.

Key-Words: - Digital signature, Batch verify, Computation complexity.

1 Introduction

The first digital signature scheme was proposed in 1978 by RSA [1]. RSA's security assumption was based on the complexities of factoring (FAC) a large composite integer n=p*q, where p and q are two distinct large primes. ElGamal [2] proposed an alternative digital signature scheme in 1985, with a security assumption based on solving the discrete logarithm (DL) problem. These two digital signature schemes have been adopted as worldwide standards and applied in many different cryptographic applications [3].

The FAC or DL signature scheme may however be insecure if the security assumption does not exist in the future. To enhance security assumption, Harn [4] first proposed a digital signature scheme based on FAC and DL simultaneously that achieved the same moduli size as the FAC and DL assumptions. Lee [5] noted that unfortunately "hackers" could forge the signatures with high probabilities if they solve the DL problem. Lee [5] proposed a modified scheme with enhanced security that promised the degree of security originally claimed. These two schemes [4,5] however, unlike the ElGamal [2] have the same modulus, requiring more keys for each user to distribute and store. To improve upon this shortcoming, He [6] proposed another scheme to enhance the original ElGamal signature scheme security. Harn [7], Lee [8] and Tiersma [9] have shown however that He's scheme is not secure if the DL problem is solved. Shao [10] proposed two signature schemes in 1998 with a security assumption based on FAC and DL simultaneously, though Li [11] and Lee [12] subsequently showed that Shao's scheme was not as secure as claimed.

To overcome the weakness of Shao's scheme, He [13] proposed a signature scheme that achieved the previously described advantages, notably: (1) It is based on two hard problems; (2) uses the same modulus; and (3) only requires one pair of public and private keys. This study investigates all variations of He's signature scheme, in which security is based on FAC and DL. The optimal two variations investigated need only two modular exponentiation for signature verification. This paper is organized as follows: Section 2 reviews the original He's signature scheme, Section 3 describes the design of generalized He's signature schemes. Conclusions are made in Section 4.

2 Review of He's Signature Scheme [13]

Initialization: The system selects a large prime $P = 4p_1 \cdot q_1 + 1$ and an element g with order $p_1 \cdot q_1$ in Z_P, where $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and p_1, q_1, p_2, q_2 are all primes. For convenience, let $R = p_1 \cdot q_1$ for later use. After the public parameters P, g and R are selected, each user

selects a private key $x \in Z_R$ such that $\gcd((x + x^{-1}), R) = 1$ and computes the corresponding public key

$$y = g^{(x+x^{-1})^2} \bmod P. \quad (1)$$

Signature generation: To sign a message m, the following steps are performed:

1. Randomly select an integer $t \in Z_R$ such that $\gcd((t + t^{-1}), R) = 1$ and compute

$$r_1 = g^{(t+t^{-1})^2} \bmod P, \quad (2)$$

and

$$r_2 = g^{(t+t^{-1})^{-2}} \bmod P. \quad (3)$$

2. Find s satisfying

$$(x + x^{-1}) = s \cdot (t + t^{-1}) + f(r_1, r_2, m) \cdot (t + t^{-1})^{-1} \bmod R \quad (4)$$

where f is a one-way hash function defined by the system.

3. Send (r_1, r_2, s) associated with m to the verifier.

Signature verification: The verifier can check the signature's authenticity by verifying the following congruent equality:

$$y \overset{?}{=} r_1^{s^2} r_2^{f^2(r_1,r_2,m)} g^{2s \cdot f(r_1,r_2,m)} \bmod P. \quad (5)$$

3 Meta-He Digital Signature Schemes

This section develops a complete list of 8 He-type digital signature schemes. The symbols m, P, g, R, x, y, t, r_1 and r_2 are reused as described in Section 2. All public and private keys are generated using the same conditions and equations of the He's signature scheme. Three symbols are set as follows:

$$\tilde{x} = x + x^{-1} \bmod R, \quad (6)$$

$$\tilde{t} = t + t^{-1} \bmod R, \quad (7)$$

$$H = f(r_1, r_2, m), \quad (8)$$

where f is a one-way hash function. The generalized signature generating equation for all variations of the He's signature scheme are represented without loss of generality, as

$$a\tilde{x} = b\tilde{t} + c\tilde{t}^{-1} \bmod R, \quad (9)$$

where (a, b, c) are three parameters from (m, s), or a mathematical combination. The parameter a for example, can be m, s, or ms.

The form of the generalized signature generating equation is now examined, and some restrictions on (a, b, c) based on security considerations are examined.

(1) We must treat $\tilde{x}$, $\tilde{t}$ and $\tilde{t}^{-1}$ as three different terms in eqn. 9 to ensure that the corresponding verification equation can be found; the verifier will otherwise not know the three secret numbers for signature verification. For example, if the signature equation is $s\tilde{x}\tilde{t} = H\tilde{t} \bmod R$, then the verification equation can be $r_1^{s^2\tilde{x}^2} = r_2^{H^2} \bmod P$ or $y^{s^2\tilde{t}^2} = r_2^{H^2} \bmod P$.

(2) The signer claims that (r_1, r_2, s) with m is a valid signature, so that s and H should be included in the signature equation and can be used in parameters (a, b, c).

(3) Eqn.9 always contains five parameters: two parameters are public information and three parameters are secret numbers. We can be sure that the number of secret parameters will always be larger than the number of equations available to the attacker, and so the generalized signature equation is secure, like the original He's scheme [13].

According to the above discussion, if the difference between the signed symbols + and - in eqn.9 is ignored, all the possible variations of He's digital signature schemes in Table 1 can be designed and listed.

Table 1. Generalized He-type signature schemes

Signature equation (mod R)	Signature verification (mod P)	Comment
(1) $s \cdot \tilde{x} = H \cdot \tilde{t} + \tilde{t}^{-1}$	$y^{s^2} = r_1^{H^2} r_2 g^{2H}$	
(2) $s \cdot \tilde{x} = \tilde{t} + H \cdot \tilde{t}^{-1}$	$y^{s^2} = r_1 r_2^{H^2} g^{2H}$	
(3) $H \cdot \tilde{x} = s \cdot \tilde{t} + \tilde{t}^{-1}$	$y^{H^2} = r_1^{s^2} r_2 g^{2s}$	
(4) $\tilde{x} = s \cdot \tilde{t} + H \cdot \tilde{t}^{-1}$	$y = r_1^{s^2} r_2^{H^2} g^{2s \cdot H}$	He's scheme

(5) $H \cdot \tilde{x} = \tilde{t} + s \cdot \tilde{t}^{-1}$	$y^{H^2} = r_1 r_2^{s^2} g^{2s}$	
(6) $\tilde{x} = H \cdot \tilde{t} + s \cdot \tilde{t}^{-1}$	$y = r_1^{H^2} r_2^{s^2} g^{2s \cdot H}$	
(7) $\tilde{x} = s \cdot H \cdot \tilde{t} + \tilde{t}^{-1}$	$y = r_1^{s^2 H^2} r_2 g^{2s \cdot H}$	Optimal scheme
(8) $\tilde{x} = \tilde{t} + s \cdot H \cdot \tilde{t}^{-1}$	$y = r_1 r_2^{s^2 H^2} g^{2s \cdot H}$	Optimal scheme

There are obviously eight types of signature variations with a security assumption based simultaneously on FAC and DL. Signature scheme 4 is the original He's scheme.

In addition to security considerations, especially in cryptographic devices like smart cards, computational complexity is another important factor. The number of bit operations for modular multiplication, modular squaring, or modular inversion in Z_P is $O((\lg P)^2)$. In contrast to the modular exponentiation $O((\lg P)^3)$, the complexity $O((\lg P)^2)$ can be ignored. Signature scheme 7 and 8 is therefore the optimal scheme since their signature verification equations need two modular exponentiations.

4 Conclusions

Eight variations of He's digital signature scheme has been investigated, and all achieve the following advantages: (1) based on FAC and DL assumptions simultaneously; (2) use same modulus; (3) require only one pair of public and private keys. This paper's proposed two optimal schemes show that two modular exponentiations are enough for signature verification.

References:

[1] R.L. Rivest, A. Shamir and L. Adelman, A method for obtaining digital signatures and public-key cryptosystem, *Commun. ACM*, Vol. 21, No. 2, 1978, pp. 120-126.

[2] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inf. Theory*, IT-31, No. 2, 1985, pp. 469-472.

[3] B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1996.

[4] L. Harn, Public-key cryptosystem design based on factoring and discrete logarithms, *IEE Proc., Comput. Digit. Tech*., Vol. 141, No. 3, 1994, pp. 193-195.

[5] N.Y. Lee and T. Hwang, Modified Harn signature scheme based on factoring and discrete logarithms, *IEE Proc., Comput. Digit. Tech*., Vol. 143, No. 3, 1996, pp. 196-198.

[6] J. He and T. Kiesler, Enhancing the security of ElGamal's signature schemes, *IEE Proc., Comput. Digit. Tech*., Vol. 141, No. 4, 1994, pp. 193-195.

[7] L. Harn, Comment: Enhancing the security of ElGamal's signature schemes, *IEE Proc., Comput. Digit. Tech*., Vol. 142, No. 5, 1995, p. 376.

[8] N.Y. Lee and T. Hwang, The Security of He and Kiesler's signature schemes, *IEE Proc., Comput. Digit. Tech*., Vol. 142, No. 5, 1995, pp. 370-372.

[9] H.J. Tiersma, Enhancing the security of ElGamal's signature schemes, *IEE Proc., Comput. Digit. Tech*., Vol. 144, No. 1, 1997, pp. 47-48.

[10]Z. Shao, Signature schemes based on factoring and discrete logarithms, *IEE Proc., Comput. Digit. Tech*., Vol. 145, No. 1, 1998, pp. 33-36.

[11]J. Li and G. Xiao, Remarks on new signature scheme based on two hard problems, *Electron. Lett.*, Vol. 34, No. 25, 1998, p. 2401.

[12] N.Y. Lee, Security of Shao's signature schemes based on factoring and discrete logarithms, *IEE Proc., Comput. Digit. Tech*., Vol. 146, No. 2, 1999, pp. 119-121.

[13] W.H. He, Digital signature scheme based on factoring and discrete logarithms, *Electron. Lett.*, Vol. 37, No. 4, 2001, pp. 220-222.