A Modified Digital Signature Schemes based on Integer Factorization and Discrete Logarithms

A.B.Nimbalkar [1], Dr.C.G.Desai [2]

Abstract—

A digital signature is a cryptographic method for verifying the identity of an individual. It can be a process, computer system, or any other entity, in much the same way as a handwritten signature verifies the identity of a person. Digital signatures use the properties of public-key cryptography to produce pieces of information that verify the origin of the data. Several digital schemes have been proposed as on date based on factorization, discrete logarithm and elliptical curve. However, the Swati Verma and Birendra Kumar Sharma [8] digital signature scheme which combines factorization and discrete logarithm together making it difficult for solving two hard problems from the hackers point of view. This paper presents the modified scheme of Digital Signature and analyzes them from different perceptions.
.

Index Terms-Cryptography, Integer Factoring, Discrete Logarithm, Digital Signature.

I INTRODUCTION

1. The security of most the digital signature algorithms are based on the difficulty of solving some hard theoretical problems. Digital signature algorithms are based on the concept of public key cryptography given by Diffie and Hellman [1]. Since then many public key cryptosystems are introduced, which are based on either prime factorization (FAC) or Discrete Logarithm (DL) problems [2].Although the schemes based on one of the above cryptosystem appears secure today, they may be unsecure in future. The security of the digital signatures can be enhanced by using factorization (FAC) or Discret Logarithm (DL) problems, which are most commonly hard problems those can be used but not NP-complete. L. Harn [4] in 1995 showed that one can break the He-Kiesler[5] algorithm if one has the ability to solve the prime factorization.

Lee and Hwang [6] showed that if one has the ability to solve the discrete logarithms, one can break the He-Kiesler algorithm. Shimin Wei [7] showed that any attacker can forge the signature of He-Kiesler algorithm without solving any hard problem in 2002. Now, we modify the Shimin Wei and Swati Verma [8] signature scheme based on factorization and discrete logarithm problem both with different parameters and using a collision-free one-way hash function in this paper.

[1] *Mr aakahs Nimbalkar is associated with A.M.College, Hadapsar, Pune 411028, Maharashtra. India*
[2] *Dr C G Desai is Peofessorand Head of the deptt in MIT Aurangabad Maharashtra. India.*

2. Shimin Wei Scheme [7]:

Let p be a large prime such that p-1 has two large prime factors p_1 and q_1. Let $n = p_1q_1$ and let g be a primitive element of Galois field GF(q). User A has a secret key x $(1 < x < n)$ such that gcd (x, p-1) = 1.

The corresponding public key $y = g^{x^2} \bmod p$. To sign a message m, A does the following

(1) Randomly chooses an integer t $(1 < t < n)$ such that gcd (t, p-1) = 1,

(2) Computes $r_1 = g^{t^2} \bmod p$ and makes $r_2 = g^{t^{-2}} \bmod p$ and makes sure that r1 ≠1.

(3) Find s such that $mt^{-1} = xr_1 + ts^2 (\bmod (p-1))$

(4) Send sig (m) = (r_1, r_2, s) as the signature.

To verify that (r_1, r_2, s) is a valid signature of m, one checks the identity

$$r_1^{s^4} \cdot r_2^{m^2} = y^{r^2} \cdot g^{2ms^2}$$

3. Swati Verma and Birendra Kumar Sharma scheme based on Integer Factorization and Discrete Logarithm based Algorithm.[8]

3.1 INITIALZATION

Let's select the following parameters:

p: a large prime p = 4p1 q1+ 1, where p1 = $2p_2$ + 1, q1 = $2q_2$ + 1, and p1, q1, p_2, q_2 are all primes and let n = p1.q1.

g: an primitive element of Galois field GF(q).

h (.) : a collision-free one-way hash function.

Further, the user chooses a private key X□ Zn such that gcd(X, n) = 1 and computes a corresponding public key which is certified by the certificate authority.

$$y = g^{x^2} \bmod p \quad \text{--(1)}$$

2.2 DIGITAL SIGNATURE GENERATION

To sign a message M, the signee carries out the following steps.

1. Randomly select an integer T□ Zn such that gcd (T, n) = 1,
2. Computes $r_1 = g^{r^2} \bmod p$ --(2)

And makes $r_2 = g^{r^{-2}} \bmod p$ --(3)

3. Find s such that $h(r_1, r_2, m)T^{-1} = x_{r_1} + Ts^2 \bmod n$ --(4)

Where h is a collision-free one-way hash function defined by the system

4. (r1, r2, s) is a signature of message M.

The signee then sends (r1, r2, s) to the verifier.

3.3 DIGITAL SIGNATURE VERIFICATION

On receiving the digital signature (r1 r2 s) the verifier can confirm the validity of the digital signature by the following equation,

$$r^{s^4} \cdot r_2^{h(r_1 \cdot r_2 \cdot m)^2} = y^{r^2} \cdot g^{2h(r_1 \cdot r_2 \cdot m)s^2} \quad \text{-- (5)}$$

If the equation holds, then (r1, r2, s) is a valid signature of message M.

4 A modified scheme based on Shimin Wei's Scheme[7] with Cube .

p be a large prime such that p-1 has two large prime factors p_1 and q_1. Let $n = p_1q_1$ and let g be a primitive element of Galois field GF(q). User A has a secret key x $(1 < x < n)$ such that gcd (x, p-1) = 1. The corresponding public key $y = g^{x^2} \bmod p$. To sign a message m, A does the following .

(1) Randomly chooses an integer t $(1 < t < n)$ such that gcd (t, p-1) = 1,

(2) Computes $r_1 = g^{t^2} \bmod p$ and makes $r_1 = g^{t^{-2}} \bmod p$ and makes sure that r_1 ≠1.

(3) Find s such that $mt^{-1} = xr_1 + ts^3 (\bmod (p-1))$
(1)

(4) Send sig (m) = (r_1, r_2, s) as the signature.

To verify that (r_1, r_2, s) is a valid signature of m, one checks the identity

$$r_1^{s^6} \cdot r_2^{m^2} \equiv y^{r^2} \cdot g^{2ms^3} (\bmod p) \quad (2)$$

We can be proved, since Eq.(2) can be derived as follows by Eq.(1) we have

$$(mt^{-1} - ts^3) = xr_1 \left(\mathrm{mod}\left(p-1\right)\right)$$

Squaring both the sides

$$(mt^{-1} - ts^3)^2 = x^2 r_1^2 \left(\mathrm{mod}\left(p-1\right)\right)$$

$$m^2 t^{-2} + t^2 s^6 - 2ms^3 = x^2 r_1^2 \left(\mathrm{mod}\left(p-1\right)\right)$$

$$m^2 t^{-2} + t^2 s^6 = x^2 r_1^2 + 2ms^3 \left(\mathrm{mod}\left(p-1\right)\right)$$

$$g^{m^2 t^{-2}} . g^{t^2 s^6} = g^{x^2 r_1^2} . g^{2ms^3} \left(\mathrm{mod}\left(p-1\right)\right)$$

$$(g^{t^{-2}})^{m^2} (g^{t^2})^{s^6} = y^{r_1^2} . g^{2ms^3} \left(\mathrm{mod}\left(p-1\right)\right)$$

$$r_1^{s^6} \cdot r_2^{m^2} \equiv y^{r^2} \cdot g^{2ms^3} (\mathrm{mod}\, p)$$

The verifier can authenticate the message M because the verifier can be convinced that the message was really signed by the signee.

5. A modified scheme based on Swati Ver -ma Scheme with Cube.

Let there exist a center which initializes the system and manages the public directory. Let, the center select the following parameters :

* p: a large prime $p = 4p_1 q_1 + 1$, where $p_1 = 2p^2 + 1$, $q_1 = 2q_2 + 1$, and p_1, q_1, p_2, q_2 are all primes and let $n = p_1.q_1$.
* g: an primitive element of Galois field GF(q),
* h (.) : a collision-free one-way hash function.

Further, the user chooses a private key X ϵ Z_n such that gcd(X, n) = 1 and computes a corresponding public key which is certified by the certificate authority as

$$y = g^{x^2} \bmod p \quad (1)$$

To sign a message M, the signee carries out the following steps.

1. Randomly select an integer T ϵ Z_n such that gcd (T, n) = 1,

2. Computes $r_1 = g^{T^2} \bmod p$ (2)

and makes $r_2 = g^{T^{-2}} \bmod p$ (3)

3. Find s such that

$$h(r_1, r_2, m)T^{-1} = xr_1 + Ts^3 (\mathrm{mod}\, n) \quad (4)$$

Where h is a collision-free one-way hash function defined by the system.

4. (r_1, r_2, s) is a signature of message M. The signee then sends (r_1, r_2, s) to the verifier.

5. Digital Signature Verification

On receiving the digital signature (r_1, r_2, s) the verifier can confirm the validity of the digital signature by the following equation.

$$r_1^{s^6} \cdot r_2^{h(r_1 \cdot r_2 \cdot m)^2} = y^{r_1^2} \cdot g^{2h(r_1 \cdot r_2 \cdot m)s^3} \quad (5)$$

If the equation holds, then (r_1, r_2, s) is a valid signature of message M.

If the signee follows the above digital signature scheme protocol, the verifier always accepts the digital signature.

It can be proved that Eq.(5) cab be defined from Eq.(4) as follows.

$$xr_1 = h(r_1, r_2, m)T^{-1} - Ts^3 \quad (6)$$

Squaring both the sides of above equation

$$x^2 r_1^2 = [h(r_1, r_2, m)^2 T^{-2} + T^2 s^6 - 2h(r_1, r_2, m)s^3]$$

$$x^2 r_1^2 + 2h(r_1, r_2, m)s^3 = [h(r_1, r_2, m)^2 T^{-2} + T^2 s^6]$$

Hence by Eq.(2) and Eq.(3) we have

$$r_1^{s^6} \cdot r_2^{h(r_1 \cdot r_2 \cdot m)^2} = g^{T^2 s^6} g^{T^{-2} h(r_1 \cdot r_2 \cdot m)^2}$$
$$= g^{T^{-2} h(r_1 \cdot r_2 \cdot m)^2 + T^2 S^6}$$
$$= g^{x^2 r_1^2 + 2h(r_1 \cdot r_2 \cdot m)s^3}$$
$$= y^{r_1^2} g^{2h(r_1 \cdot r_2 \cdot m)s^3} (\mathrm{mod}\, p)$$

With the knowledge of the signee's public key y and the signature (r_1, r_2, s) of message M, the verifier can authenticate the message M because the verifier can be convinced that the message was really signed by the signee. Otherwise, the signature (r_1, r_2, s) is invalid.

6. Conclusion

In this paper, we modify the digital signature schemes whose security is based on factorization (FAC), discrete logarithm problem (DLP) and collision free hash function. To enhance the security of both schemes we use cube ,so that it gives better security.

7. References :

[1] Diffie W. and Hellman M.E, "New directions in cryptography", *IEEE Transactions on Information Theory*, 22, 644- 654, (1976).

[2] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. Information Theory, IEEE Transactions on,31(4):469- 472, 2002.

[3] Harn L., "Public-key cryptosystem design based on factoring and discrete logarithms", *IEE Proceedings: Computers and Digital Techniques,* 141, 193-195, (1994).

[4] L. Harn. Comment: Enhancing the security of El Gamal's signature scheme. IEE Proceedings-Computers and Dig-ital Techniques, 142:376, 1995.

[5] He J. and Kiesler T., "Enhancing the security of El-Gamal's signature schemes", *IEE Proc. Comput. Digital Technol.* 141, 249-252, (1994).

[6] N.Y. Lee and T. Hwang. The security of He and Kiesler'ssignature schemes. In Computers and Digital Techniques,IEE Proceedings-, volume 142, pages 370-372. IET, 2002.

[7] S. Wei. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms. Progress on Cryptography, pages 107-111, 2004

[8] 'A New Signature Scheme Based on Factoring and Discrete Logarithm Problems' Swati Verma*, Birendra Kumar Sharma, International Journal of Information & Network Security (IJINS) Vol.1, No.3, August 2012, pp. 158~162.