Journal of Modern Mathematics and Statistics 6 (1): 7-9, 2012
ISSN: 1994-5388

A New Signature Scheme Based on Factoring and Discrete Logarithm Problems

Swati Verma and Birendra Kumar Sharma
School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.), India

Abstract: In 1994, He and Kiesler proposed a digital signature scheme which was based on the factoring and the discrete logarithm problem both. Same year, Shimin-Wei modiffied the He-Kiesler signature scheme. In this study, researchers propose an improvement of Shimin-Wei signature scheme based on factorization and discrete logarithm problem both with different parameters and using a collision-free one-way hash function. In the opinion, the scheme is more secure than the earlier one.

Key words: Cryptography, digital signature, discrete logarithm problem, factoring, function, factorization, India

INTRODUCTION

It is well known that Diffie and Hellman (1976) gave the concept of public key cryptography. Since then several public key cryptosystems based on a hard mathematical problem either factoring or discrete logarithm have been proposed. Those cryptosystems in which said problem was easy to solve were found to be insecure. Also, the encryption in digital signature scheme are based on the same mathematical problems which are used to design public key cryptosystems. Hence, security of the digital signatures (Laih and Kuo, 1997; Li and Xiao, 1998; Lee and Hwang, 1996; Rivest *et al*., 1978; Elgamal, 1985; He, 2001; Shao, 1998) depends upon the hardness of either factoring and discrete logarithm. However, most of these are found to be insecure (Harn, 1995; Hung, 2001; Lee and Hwang, 1995; Lee, 1999).

In a study, Harn (1994) and He and Kiesler (1994) proposed digital signatures which were based on factoring and discrete logarithm problem both. Same year, Lee and Hwang (1995) have shown that having ability to solve the discrete logarithm problem only, one can break He-Kiesler scheme. Although, Wei (2004) have proposed an improvement over He and Kiesler (1994)'s scheme. Now, researchers propose a new digital signature scheme by improving the Wei (2004) signature scheme based on factorization and discrete logarithm problem both with different parameters and using a collision-free one-way hash function in this study.

BRIEF REVIEW OF HE-KIESLER'S AND SHIMIN WEI'S SIGNATURE SCHEME

He-Kiesler's scheme: 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 or an element of large order of GF (q). Note that if a common p is used by all users, the two factors of n must be kept secret from every user (actually these two factors will never be used by anyone and thus can be discarded once n is produced).

Any user A has a secret key x_1 ($1<x_1<n$) such that gcd (x_1, p - 1) = 1. From x_1 constructed the quadratic residue $x = x_1^2 \bmod (p - 1)$ and corresponding public key $y = g^{x^2} \bmod p$. To sign a message m, A does the following:

- Randomly chooses an integer t_1($1<t<n$) such that gcd (t_1; p - 1) = 1 and calculates $t = t_1^2 \bmod (p - 1)$
- Computes $c = x_1t_1 \bmod (p - 1)$
- Computes $r = g^{t^2} \bmod p$ and makes sure that $r_1 \neq 1$
- Finds s such that $m = xr + ts \bmod (p - 1)$
- Sends sig (m) = (r, s, c) as the signature

To verify that (r, s, c) is a valid signature of m, one simply checks the identity $g^{m^2} \equiv z^{r^2} r^{s^2} g^{2rsc^2} \bmod p$.

Shimin wei's scheme: 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:

- Randomly chooses an integer t ($1<t<n$) such that gcd (t, p - 1) = 1
- Computes $r_1 = g^{t^2} \bmod p$ and makes $r_1 = g^{r^2} \bmod p$ and makes sure that $r_1 \neq 1$
- Find s such that $mt^{-1} = xr_1 + ts^2 \bmod (p - 1)$
- 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:

Corresponding Author: Swati Verma, School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.), India

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

THE NEW DIGITAL SIGNATURE SCHEME

This scheme can be divided into three phases: initialization, digital signature generation and digital signature verification.

Initialization: Let there exists a center which initialize the system and manage the public directory. Let, the center selects 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 $n = p_1q_1$
- g: an primitive element of Galois field GF (q)
- h(.): a collision-free one-way hash function

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

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

Digital signature generation: To sign a message M, the signee carries out the following steps.

- Randomly select an integer $T \in Z_n$ such that gcd (T, n) = 1
- Computes

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

and makes:

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

- Find s such that (where, h is a collision-free one-way hash function defined by the system):

$$h(r_1, r_2, m)\, T^1 = Xr_1 + Ts^2 \bmod n \quad (4)$$

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

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:

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

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

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

Proof: The theorem can be proved since Eq. 5 can be derived as follows by Eq. 4, researchers have:

$$Xr_1 = h(r_1, r_2, m)\, T^{-1} - Ts^2 \quad (6)$$

Squaring both sides in Eq. 6:

$$X^2 r_1^2 = [h(r_1, r_2, m)^2\, T^{-2} + T^2 s^4 - 2h(r_1, r_2, m)\, s^2]$$
$$X^2 r_1^2 + 2h(r_1, r_2, m)s^2 = [h(r_1, r_2, m)^2\, T^{-2} + T^2 s^4]$$

Hence by Eq. 2 and 3, researchers have:

$$\begin{aligned} r_1^{s^4} r_2^{h(r_1, r_2, m)^2} &= g^{T^2 s^4}\, g^{T^{-2} h(r_1, r_2, m)^2} \\ &= g^{T^{-2} h(r_1, r_2, m)^2 + T^2 s^4} \\ &= g^{x^2 r_1^2 + 2h(r_1, r_2, m)s^2} \\ &= y^{r^2} g^{2h(r_1, r_2, m)s^2} \bmod p \end{aligned}$$

This equation is equivalent to Eq. 5. With the knowledge of the signees 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.

SECURITY ANALYSIS

Attack 1: An adversary (Adv) attempts to derive the private key X from the corresponding public key y for any user. In this case, the Adv has to recover a private key X from Eq. 1 which is polynomially equivalent to both FAC and DLP.

Attack 2: The Adv has to choose randomly a three tuple (r_1, r_2, s). This is as dificult as solving the FAC, DL problem and collision-free one-way hash function simultaneously.

Attack 3: An Adv attempts to forge a valid signature (r_1, r_2, s) for message M. In this case, the Adv tries to derive the signature (r_1, r_2, s) for a given message M by letting two integerfixed and finding the other one. Adv randomly select (r_1, r_2) or (r_1, s) or (r_2, s) and find s or r_2 or r_1, respectively such that the Eq. 5 satisfied.

CONCLUSION

Researchers proposed new digital signature scheme whose security is based on Factorization (FAC), Discrete

Logarithm Problem (DLP) and collision free hash function under a more suited parameters provides better security.

REFERENCES

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

Elgamal, T., 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31: 469-472.

Harn, L., 1994. Public-key cryptosystem design based on factoring and discrete logarithms. IEE Proc. Comput. Digital Techniques, 141: 193-195.

Harn, L., 1995. Enhancing the security of ElGamal's signature schemes. IEE Proc. Comput. Digital Technol., 142: 376-376.

He, J. and T. Kiesler, 1994. Enhancing the security of El Gamal's signature scheme. Proc. IEE. Comput. Digital Techniques, 141: 249-252.

He, W.H., 2001. Digital signature schemes based on factoring and discrete logarithms. Electron. Lett., 37: 220-222.

Hung, M.S., 2001. Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms. Proceedings of the 2001 National Computer Symposium, December 2001, Taipei, Taiwan, pp: F043-F045.

Laih, C.S. and W.C. Kuo, 1997. New signature schemes based on factoring and discrete logarithms. IEICE Trans. Fund, E80-A: 46-53.

Lee, N.Y. and T. Hwang, 1995. The security of he and Kiesler's signature schemes. IEE Proc. Comput. Digital Technol., 142: 370-372.

Lee, N.Y. and T. Hwang, 1996. Modified Harn signature scheme based on factoring and discrete logarithms. IEE Proc. Comput. Digital Technol., 143: 196-198.

Lee, N.Y., 1999. Security of shaos signature schemes based on factoring and discrete logarithms. IEE Proc. Comput. Digital Techniques, 146: 119-121.

Li, J. and G. Xiao, 1998. Remarks on new signature scheme based on two hard problems. Elect. Lett., 34: 2401-2401.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21: 120-126.

Shao, Z., 1998. Signature schemes based on factoring and discrete logarithms. IEE Proc. Comput. Digital Technol., 145: 33-36.

Wei, S., 2004. A new digital signature schemes based on factoring and discrete logarithms. Progress Cryptography, 769: 107-111.