Institute of Advanced Engineering and Science

International Journal of Information & Network Security (IJINS)
Vol.1, No.3, August 2012, pp. 158~162
ISSN: 2089-3299

A New Signature Scheme Based on Factoring and Discrete Logarithm Problems

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

Article Info

Article history:

Received 06 th June, 2012
Revised 12 th July, 2012
Accepted, 25 th July2012

Keyword:

Cryptography
Digital Signature
Discrete Logarithm Problem
Factoring
Security

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 modified the He-Kiesler signature scheme. In this paper, we 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 our opinion, our scheme is more secure than the earlier one.

Corresponding Author:

Swati Verma
School of Studies in Mathematics,
Pt. Ravishankar Shukla University Raipur (C.G.), India.
Email: swativerma15@gmail.com

1. INTRODUCTION

It is well known that Diffie and Hellman [1] gave the concept of public key cryptography. Since then, several public key cryptosystems based on a hard mathematical problem either factoring or discrete logarithms 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 is based on the same mathematical problems which are used to design public key cryptosystems. Hence, security of the digital signatures [2, 5, 8, 11, 12, 13, 14] depends upon the hardness of either factoring and discrete logarithm. However, most of these are found to be insecure [4, 7, 9, 10].

In a paper, Harn [3] and He-Kiesler [6] proposed digital signatures which were based on factoring and discrete logarithm problem both. Same year, Lee and Hwang [10] have shown that having ability to solve the discrete logarithm problem only, one can break He-Kiesler scheme. Although, Shimin Wei [15] have proposed an improvement over He-Kiesler scheme [6]. Now, we propose a new digital signature scheme by improving the Shimin Wei [15] 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.

2. OVERVIEW

2.1 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 $n = p_1 q_1$ 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

(1) Randomly chooses an integer t_1 $(1 < t < n)$ such that $\gcd(t_1; p-1) = 1$, and calculates $t = t_1^2 \bmod (p-1)$
(2) Computes $c = x_1 t_1 \bmod (p-1)$
(3) Computes $r = g^{t^2} \bmod p$ and makes sure that $r_1 \neq 1$,
(4) Finds s such that $m = xr + ts \bmod (p-1)$
(5) 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

$$g^{m^2} \equiv z^{r^2} r^{s^2} g^{2rsc^2} \bmod p .$$

2.2 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

(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 $r_1 \neq 1$.

(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

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

3. THE NEW DIGITAL SIGNATURE SCHEME

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

3.1 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 $n = p_1.q_1.$

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

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

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

$$y = g^{X^2} \bmod p \qquad (1)$$

3.2 Digital Signature Generation

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

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

$$r_1 = g^{T^2} \bmod p \tag{2}$$

and makes

$$r_2 = g^{T^{-2}} \bmod p \tag{3}$$

3. Find s such that

$$h(r_1, r_2, m)T^{-1} = Xr_1 + Ts^2 \bmod n. \tag{4}$$

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.

3.3 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

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

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

Theorem 3.1 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) we have

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

Squaring both sides in the above equation

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

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

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

The above 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.

4. SECURITY ANALYSIS OF THE PROPOSED SCHEME

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 difficult 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 integer fixed 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.

5. CONCLUSION

In this paper, we proposed a 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.

ACKNOWLEDGEMENTS

The author wishes to thank the anonymous referees for their very useful comments and suggestions.

REFERENCES

[1] Diffie W. and Hellman M.E, “New directions in cryptography”, *IEEE Transactions on Information Theory*, 22, 644-654, (1976).
[2] ElGamal T., “A public-key cryptosystem and a signature scheme based on discrete logarithms”, *IEEE Transactions on Information Theory IT-31*, 469-472, (1985).
[3] Harn L., “Public-key cryptosystem design based on factoring and discrete logarithms”, *IEE Proceedings: Computers and Digital Techniques*, 141, 193-195, (1994).
[4] Harn L., “Comment: enhancing the security of ElGamal's signature schemes”, *IEE Proc. Comput. Digital Technol*. 142, 376, (1995).
[5] He W.H, “Digital signature schemes based on factoring and discrete logarithms”, *Electron. Lett.* 37 (4), 220-222, (2001).
[6] He J. and Kiesler T., “Enhancing the security of ElGamal's signature schemes”, *IEE Proc. Comput. Digital Technol.* 141, 249-252, (1994).
[7] Hung M.S, “Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms”, *in Proceedings of the National Computer Symposium*, Taipei, Taiwan,December, pp.F043-F045, (2001).
[8] Laih C.S. and Kuo W.C, “New signature schemes based on factoring and discrete logarithms”, *IEICE Trans. Fund*, E80-A,(1), pp.46-53, (1997).
[9] Lee N.Y, “Security of Shaos signature schemes based on factoring and discrete logarithms”, *IEE Proc.-Computers and Digital Techniques*, 146, (2), pp. 119-121, (1999).
[10] Lee N.Y. and Hwang T, “The Security of He and Kiesler's signature schemes”, *IEE Proc. Comput. Digital Technol.* 142, pp. 370-372, (1995).
[11] Lee N.Y. and Hwang T, “Modified Harn signature scheme based on factoring and discrete logarithms”, *IEE Proc. Comp. Digital Tech*.,143 (3), pp. 196-198, (1996).
[12] Li J. and Xiao G., “Remarks on new signature scheme based on two hard problems”, *Elec. Lett.*, 34 (25), 2401, (1998).
[13] Rivest R. L. et al, “A method for obtaining digital signatures and public key cryptosystems”, *Commun. ACM*, 21, 120-126, (1978).
[14] Shao Z., “Signature schemes based on factoring and discrete logarithms”, *IEE Proc. Comput. Digital Technol.* 145, 33-36, (1998).
[15] Wei S., “A New Digital signature schemes based on factoring and discrete logarithms”, *Progress on Cryptography The Springer International Series in Engineering and Computer Science,* Vol 769, 107-111, (2004).

BIOGRAPHY OF AUTHORS

Swati Verma received the B.Sc. and M.Sc. degree in Mathematics form Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 2005 and 2007. She joined School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India for her research work. She is a life member of Cryptology Research Society of India (CRSI). Her area of interest is Public Key Cryptography and Digital Signature.

Birendra Kumar Sharma Professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical Society and the Ramanujan Mathematical Society.