AN EFFICIENT DIGITAL SIGNATURE SCHEME WITH MESSAGE RECOVERY

MANOJ KUMAR CHANDE[a1] **AND ANITA SINGH**[b]

[a]Department of Mathematics, Shri Shankaracharya Institute of Professional Management and Technology, Raipur, Chhattisgarh, India
[b]Department of Mathematics, Rungata Engineering College, Raipur, India

ABSTRACT

The existing digital signature schemes with message recovery were developed without using one way hash function, most of them are either insecure or less efficient for practical use. Chang et al. proposed a new digital signature scheme, and claimed the scheme without using any hash function can resist forgery attacks. However, many attacks on Chang et al.'s scheme were presented. Kang et al. also gave an effective improvement to resist these forgery attacks. Liu and Li gives improvement over kang's signature scheme by shorten the signature. They maintain the same level of security, but provide the signature scheme having more efficiency in computation and communication. In this paper, an attempt to be made to improve signature scheme given by Liu and Li. To reduce the computation load in signature generation as well as in signature verification phase, the arbitrary message m, is not used as an exponent like in the other signature scheme with message recovery, this will result the signatures generated are short in length. Security of the proposed signature scheme is based on the difficulty of solving the discrete logarithm problem (DLP). Our improvement maintain the security level of Liu and Li scheme and makes it more efficient regarding computation as well as security. The proposed scheme does not use message redundancy and is suitable to provide signature on long messages.

KEYWORDS: Discrete Logarithm Problem, Multi-signature, Message Recovery, Proxy Signature, Self- certified Key.

Digital signatures play the key role in the modern day data processing systems. In the available literature most of the proposed signature schemes were based on well-known public key systems such as Rivest, Shamir and Adleman (RSA) [1], and ElGamal [2] systems. In 1995, Nyberg and Rueppel [3], [4], presented signature schemes, which provides the property to recover messages. In this kind of signature scheme the signer O , send a signature for a message to a verifier V . After receiving the signature, the verifier V can recover and verify the message from the signature. The security of their signature scheme based on the DLP.

In the year 2000, Shieh et al. [5], proposed a three parameters signature scheme without using one-way hash functions and message redundancy schemes. later in 2003, Hwang and Li [6], found a forgery attack on it. In 2004, Chang et al. [7], proposed a new digital signature scheme with the property of message recovery. He claimed that his scheme don't involve any hash function or padding any redundancy and still it can resist forgery attacks. However, there are many researcher attacks on Chang et al.'s scheme.

In the same year 2004, Fu et al. [8], presented a forgery attack in which the forger can forge signature of original signer for a specific message without getting any valid signature. In the year 2005, Zhang [9], gives two forgery attacks on, Chang et al. [7] and shows that the signature can be forged on an uncontrolled message. Chein [10], also shown that the signature scheme given in Chang et al. is not secure. Kang and Tang [11], gives the parameter reduction attack on Shieh [5], and Chang [7], signature scheme. Based on their analysis, they propose a new digital signature scheme which is robust under the known forgery attacks.

In the year 2008, Liu and Li [12], proposed two signature schemes and claim that they are as secure as Kang et al.'s scheme. However, the signature generated in their scheme is much shorter than Kang et al.'s scheme. The computation load is less and communication efficiency is being improved.

REVIEW OF LIU AND LI SCHEME WITH MESSAGE RECOVERY

In this section we review Liu and Li [12], gives a signature scheme with message recovery. Liu and Li gave an improvement over kang's signature scheme to shorten the signed signature. Our improvement keeps the security of Liu and Li scheme. In the proposed signature scheme the message to be signed is not used as an exponent to generate one of the parameter s of signature. This improvement provides the signature scheme more efficiency for practical applications.

(i) Parameter Generation: Consider p and q large primes such that $q \mid p-1$. Let $g \in Z_p^*$, be a primitive element of order q .Let x is the private key of the signer O , where $x < p-1$ and $\gcd(x, p-1) = 1$.The corresponding public key is $y = g^x \bmod p$.

(ii) Signature Generation:

(a) Signer O computes

$$s = y^m \bmod q$$

(b) Randomly select $k \in [1, q]$ and computes

[1] Corresponding author

$$r = m \cdot g^{-k} \bmod p \qquad (1)$$

$$t = x^{-1}(k - r \cdot s) \bmod q \qquad (2)$$

Signer O , sends the signature (r, s, t) to the verifier.

(iii) Signature Verification:

To verify the signature received, verifier V computes

(a) $m'' = y^{t} \cdot r \cdot g^{r \cdot s} \bmod p$

(c) Verifier V checks $s = y^{m''} \bmod p$

if this holds, then the verifier accepts the signature (r, s, t) as a valid one.

THE PROPOSED SIGNATURE SCHEME WITH MESSAGE RECOVERY

The proposed signature scheme has the following phases:

(i) Parameter Generation:

(a) A trusted centre (TA), selects an integer N , as a product of two primes p and q . The two primes p and q are such that $p = 2 \cdot k \cdot \tilde{p} + 1$ and $q = 2 \cdot k \cdot \tilde{q} + 1$, where k , $\tilde{p}$ and $\tilde{q}$ are distinct large primes. Then TA chooses an integer g of order k . Then TA selects e , which is co prime to both $p - 1$ and $q - 1$ and compute corresponding value d , such that $e \cdot d \equiv 1 \bmod \phi(N) \cdot$

(d) TA sends d and k to the original signer. Then TA made g , N and e public.

(e) The signer O , select his/her private key $x \in Z_k$ and make $y = g^{k} \bmod N$ public.

(ii) Signature Generation:

To generate the signature the signer O , do the following computation

(a) First compute $s = y^{d} \bmod N$, (3)

(b) The signer O , selects two random numbers $\alpha, \beta \in Z_k$ and compute

$$r = m \cdot s \cdot g^{\alpha - k} \qquad (4)$$

(f) The signer O compute t as

$$t = x^{-1} \cdot (k - r \cdot s - \alpha) \qquad (5)$$

(c) The signer O , sends (r, s, t) as signature of the message to the receiver R .

(iii) Signature Verification:

(a) To verify the signature received, verifier V computes

$$m'' = y^{t} \cdot r \cdot g^{r \cdot s} \cdot s^{-1} \qquad (6)$$

(b) The verifier V , authenticate the signature by calculating

$$s^{e} = y \bmod N \qquad (7)$$

If its true then the signature (r, s, t) is a valid signature. Its validity as shown below:

$$m'' = y^{t} \cdot r \cdot g^{r \cdot s} \cdot s^{-1}$$

$$= g^{k - r \cdot s - \alpha} \cdot m \cdot s \cdot g^{\alpha - k} \cdot g^{r \cdot s} \cdot s^{-1}$$

$$= m \, .$$

SECURITY ANALYSIS OF THE PROPOSED SIGNATURE SCHEME

In this section we analyze the security of our proposed signature scheme. The changes or improvement are made in parameter and signature generation phases.

(a) The prime numbers used are not only the random primes but they are safely calculated large primes, so they give more security to signature scheme.

(b) It is difficult to recover α and k from equation (4), because in process of recovery of k , the attacker has to encounter discrete logarithm problem. It is also not feasible for anyone to find x from equation (5), since there are two unknowns k and x .

(c) To obtain (r, s, t) and make forgery, a forger has to encounter DLP to solve equations (3) and (7). Knowledge of s , is not have any advantage, because again if someone looking to recover d from equation (3), he/she has to face DLP. Hence the proposed signature scheme with message recovery has a higher level security as compared to Liu and Li scheme.

(d) To compute s , d is used instead of m and the computation has being done for mod N in place of mod q as in Liu et al.'s scheme. In Liu and Li [12], scheme the message m is used as an exponent to the public key y of the signer. If the message m is very large, then the computation of s becomes difficult. So using d as an exponent, it helps to the proposed scheme to be applicable for large messages.

(e) The private parameter d is used to compute s in the equation (3), is generated with safe prime number. Suppose some adversary looking to get d , than he/she must have to obtain the primes p and q. In the parameter generation phase p and q are chosen as a functions of very large primes, namely, $\tilde{p}$ and $\tilde{q}$. Hence to solve for p and q is infeasible because of the intractability of integer factorization problem (IFP). To know r and s, the attacker has to solve for two unknown variables, namely, α and k, which is very complex due to intractability of DLP.

CONCLUSION

The proposed signature is secure cryptographically as shown in security analysis and applicable for large messages.

REFERENCES

R.L. Rivest, A. Shamir, and L. Adelman, “A method for obtaining digital signature and public key cryptosystem”, Communications of ACM, vol. 21, no. 2, pp. 120-126, 1978.

T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory vol. 30, no. 4, pp. 469-472, 1985.

K. Nyberg, and R. A. Rueppel, “A new signature scheme based on the DSA giving message recovery”, in Proceedings of the First ACM Conference on Computer and Communication Security, pp. 58-61, 1993.

K. Nyberg, and R. A. Rueppel, “Message recovery for signature schemes based on the discrete logarithm problem”, in Eurocrypt'94, LNCS 950, pp. 182-193, 1995.

S. P. Shieh, C. T. Lin, W. B. Yang and H. M. Sun, “Digital multisignature schemes for authenticating delegates in mobile code systems”, IEEE Transaction on Vehicular Technology, vol. 49, pp. 1464-1473, July 2000.

S. J. Hwang and E. T. Li, “Cryptanalysis of Shieh-Lin-Yang-Sun signature scheme”, IEEE Commun. Lett., vol. 7, pp. 195-196, Apr. 2003.

C. C. Chang and Y. F. Chang, “Signing a digital signature without using one-way hash functions and message redundancy schemes”, IEEE Communication Letters, vol. 8, pp. 485-487, 2004.

X. T. Fu, C. X. Xu and G. Z. Xiao, “Forgery Attacks on Chang et al.'s signature scheme with message recovery”, http://eprint.iacr.org/2004/236, 2004.

F. G. Zhang, Cryptanalysis of Chang et al.'s Signature Scheme with Message Recovery, IEEE Communication Letters, vol. 9, pp. 358-359, 2005.

H. Y. Chien, “Forgery Attacks on Digital Signature Schemes without using One-way Hash and Message Redundancy”, IEEE Communication Letters, vol. 10, pp. 324-325, 2006.

L. Kang and X. H. Tang, “Digital signature scheme without hash functions and message redundancy”, Journal on Communications (In Chinese), vol. 27, no. 5, pp. 18-20, 2006.

Jie Liu and Jianhua Li, “Cryptanalysis and Improvement on a Digital Signature Scheme Without Using One-way Hash and Message Redundancy”, International conference on Information Security and Assurance, 2008, IEEE, pp. 266-269, 2008.