A Digital Signature Scheme with message recovery and without one-way hash function

Sujata Mohanty
Dept. of Computer Science and Engineering
National Institute of Technology
Rourkela, India
sujata.nitrkl@gmail.com

Banshidhar Majhi
Dept. of Computer Science and Engineering
National Institute of Technology
Rourkela, India
bmajhi@nitrkl.ac.in

Abstract— A digital signature scheme allows one to sign an electronic message and later the produced signature can be validated by the owner of the message or by any verifier. Most of the existing digital signature schemes were developed based on the use of hash function and massage redundancy to resist against forgery attack. In this paper we propose a signature scheme with message recovery and without using one way hash function which is secure and practical. The proposed scheme is shown to be secure against the parameter reduction attack and forgery attack. Security of the scheme is based on the complexity of solving the discrete logarithm problem and integer factorization. The proposed scheme does not use message redundancy and is suitable to provide signature on long messages.

***Keywords*- digital signature, message recovery, one way hash function, forgery attack, parameter reduction attack.**

I. INTRODUCTION

Digital signatures play an important role in our modern electronic society. Digital signature schemes based on asymmetric key cryptography may cause existential forgery. One way hash function such as SHA-1, which takes a variable length input and produces a fixed length output, is a usual method to prevent the existential forgery. Also signature schemes based on discrete logarithm problem do not automatically provide message recovery feature. In the ElGamal based signature schemes, the message and its signature should be sent to the verifier separately. To resist forgery attack, the original message should be first hashed by the one way hash function like SHA-1 and then the hashed result are used to deliver the digital signature [2]. So far, how to build a digital signature scheme without one-way hash functions and message redundancy is still a challenging problem [7]. However, a lot of researches are made in these areas [1, 2, 5, 6, 7].

In message recovery mode, the receiver can recover the original message from the received message [4]. It has the advantage of smaller communication overhead as the message need not be sent along with its signature and also less computational cost. We propose a signature scheme having message recovery feature without using one way hash function. The proposed scheme is an improvement over Kang et al.'s scheme as it is more secure and practical. We have used safe primes for key generation process [3], which makes the proposed scheme secure.

The rest of the work is organized as follows. In Section 2, a review of Kang et al.'s scheme is given. The proposed scheme is presented in Section 3. Security analysis of the proposed scheme is discussed in Section 4. Then in Section 5, efficiency analysis of the proposed scheme with Kang et al's scheme is presented. Finally, we conclude this paper in Section 6.

II. A REVIEW OF KANG'S SCHEME

The initialization phase of Kang et al.'s scheme is described as follows. Let p is a large prime and g is a primitive element in Z_p. The signer has private key x, where $x < (p-1)$ and gcd $(x, p-1)=1$. The public key of the signer is Y, where $Y= g^x \bmod p$. To generate a signature for message $m \in Z_p$, the signer proceeds as follows.

A. Signature generation phase

The signer generates the signature as per the following steps.

1. he signer computes s as
   $$s=Y^m \pmod p \quad (1)$$
2. The signer selects a random number k in [1, p-1] and computes r as
   $$r=s+m\, g^{-k} \quad (2)$$
3. The signer computes t from the following expression.
   $$s+t \equiv x^{-1} (k- r) \bmod (p- 1) \quad (3)$$
4. The signer sends the signature (r, s, t) of message m to the receiver or verifier.

B. Signature verification phase

After receiving the signature(r, s, t), the verifier performs the following operations.

1. Computes m´ as

978-0-7695-4058-0/10 $26.00 © 2010 IEEE
DOI 10.1109/ACE.2010.89

$$m' \equiv (r\text{-}s)\ Y^{s+t}\ g^{r} \pmod p \quad (4)$$

2. Checks the authenticity of the signature by verifying (5).
$$s = Y^{m'} \pmod p \quad (5)$$
If it holds, then the signature (r, s, t) is indeed the valid signature generated by the signer of the recovered message m.

Kang et al.'s scheme is resistant against parameter reduction attack as shown below.

Let $t' = t + s$ and $r' = r - s$. Equation 4 may be written as

$$m' \equiv (r - s)\ Y^{t'}\ g^{r} \pmod p$$
$$m' \equiv r'\ Y^{t'}\ g^{r'+s} \pmod p$$

Transformation is not able to reduce parameters; hence it is resistant to parameter reduction attack. Also this scheme is resistant to forgery attack.

We have analyzed that in the signature generation phase, as shown in (1), is computed in a way that seems to be not preferable for long messages. This is because if the message is a too lengthy document to be signed, then the computation of s will be very much complex. Also Kang et al. have used only simple prime numbers p and q instead of using safe primes. So this scheme is not secure enough to be applied in practical area.

The proposed signature scheme is much secure as it used the safe prime concept. Also it adds an improvement to Kang et al's scheme, which makes it suitable for large messages and efficient enough to be applicable in real life.

III. THE PROPOSED SIGNATURE SCHEME

The proposed signature scheme consists of three phases, namely, setup, signature generation phase and signature verification phase. A brief description of each phase is given below.

A. *Setup*

The parameters are generated as follows.

1. A trusted center chooses an integer n as the product of two primes p and q such that, $p=2fp'+1$and $q=2fq'+1$, where f, p′ and q′ are distinct primes. Then it chooses an integer g of order f both modulo p and q, i.e., $g^t \pmod n = 1$. Then it chooses an integer e which is coprime with both (p-1) and (q-1) and computes d such that $ed \equiv 1 \bmod \varphi(n)$.
2. Finally the trusted center sends d and f to the signer securely and publishes g, n and e as its public data.
3. The signer chooses its private key $x \in Z_f$ and Publishes its public key Y, where $Y = g^x \pmod n$

B. *Signature generation phase*

To sign a message m, the signer performs the following operations.

1. Computes s as
$$s \equiv Y^{d} \pmod n \quad (6)$$
2. Selects two random numbers k and u both in Z_f and computes r as
$$r = s + m\ g^{(u-k)} \pmod n \quad (7)$$
3. The signer computes **t** from the following expression
$$s + t \equiv x^{-1}\ (k - r - u) \bmod (n-1) \quad (8)$$
4. The signer then sends the triplet (r, s, t) to the receiver as the signature of the message m.

C. *Signature verification phase*

After receiving the signature(r, s, t), the verifier checks the authenticity of the signature by the performing the following operations.

1. Checks the authenticity of the signature by computing the following expression.
$$s^{e} \equiv Y \pmod n \quad (9)$$
If it holds, then the signature (r, s, t) is considered as a valid one generated by the signer of the recovered message m′.
2. It recovers the message m′as
$$m' \equiv (r - s)\ Y^{s+t}\ g^{r} \bmod (n-1) \quad (10)$$
It is verified that (r, s, t) is a valid signature of the message m as shown below.
$$\begin{aligned} m' &\equiv (r - s)\ Y^{s+t}\ g^{r} \bmod (n-1) \\ &= m\ g^{(u-k)}\ g^{x(s+t)\ t}\ g^{r} \bmod (n-1) \\ &= m\ g^{(u-k)}\ g^{x(\,x^{-1}(k-u-r))}\ g^{r} \bmod (n-1) \\ &= m\ g^{(u-k)}\ g^{(k-u-r)}\ g^{r} \bmod (n-1) \\ &= m \end{aligned}$$

The operations of the proposed signature scheme are listed in Table 1.

IV. SECURITY ANALYSIS OF OUR SCHEME

First, it is shown that how the proposed scheme resists the attacks to recover the secret key of the signer. Then the proof that it can withstand the parameter reduction attack and forgery attack without using one way hash function is discussed. Finally, the security of the signature scheme is discussed.

TABLE 1: The proposed signature scheme

Signature
1. $s \equiv Y^{d} \pmod n$
2. $r = s + m\ g^{(u-k)} \pmod n$
3. computes t from $s + t \equiv x^{-1}\ (k - r - u) \bmod (n-1)$
Verification
1. Checks whether $s^{e} \equiv Y \pmod n$
2. Recovers the message m′ as $m' \equiv (r - s)\ Y^{s+t}\ g^{r} \bmod (n-1)$

A. *Attacks to recover private key of signer*

1. It is almost impossible to recover u and k from (7), as it is equivalent to compute discrete logarithm problem over Z_f and also (u – k) appears in the exponent.
2. It is impossible to solve x from (8), since it has 3 unknown parameters k, u and x.

B. *Attacks for parameter reduction*

The message recovery equation (10) can be written as

$$m' \equiv (r - s)\, Y^{t'} g^{r} \bmod (n-1)$$
$$\equiv r'\, Y^{t'} g^{r'+s} \bmod (n-1) \qquad (11)$$

where, r=(r-s) and t′=(t+s). The parameters in (10) can not be reduced by the parameter reduction attack. Hence the proposed scheme is resistant against parameter reduction attack.

C. *forgeryAttack*

Given the message m, a forger has to solve both (6) and (11) in order to get the triplet (r, s, t). Given s, it is a discrete logarithm problem to solve (6) for d. Also the value of d is very difficult to obtain as it is generated using safe primes. Even if both r and s are known, it is difficult to solve for u and k in (7). Hence our scheme is more secure as compared to Kang et al's scheme.

D. *Suitable for long messages*

In this scheme s is computed as $s \equiv Y^d \pmod n$ instead of $s=Y^m \pmod p$ as in Kang et al.'s scheme. In Kang et al.'s scheme, message m is the exponent of the public key Y of signer. If the message is very large, computing s becomes very difficult and impractical. Here we modified (1) by making d as the exponent of Y. As d is computed by using safe primes discussed in Section 3, it is almost infeasible to obtain by an intruder. The proposed signature scheme can be applicable to large messages, hence practical. Our signature scheme has same transmission overhead as that of Kang et al.'s scheme.

E. *Security*

The value of d used to derive s in (6) is computed in the setup phase using safe primes. Any intruder wish to get d must have to obtain p and q. In the proposed scheme p and q are choosen as a function of very large primes, namely, p′ and f. Hence the solving for p and q lies in the complexity of solving integer factorization problem. Also, to get r and s, the intruder has to solve for two unknown variables, namely, u and k, whose complexity lies in solving the discrete logarithm problem. Hence, the proposed signature scheme is more secure than Kang's scheme.

V. EFFICIENCY ANALYSIS

The proposed scheme has not used message redundancy property unlike Kang's scheme. Although message redundancy helps to avoid forgery attack, it is suitable for signature generation on small messages. Signature schemes which provide message redundancy are normally not suitable for long messages. The proposed signature scheme does not support message redundancy, thereby suitable for long messages. A comparative analysis of various properties of both schemes is listed in Table 2

TABLE 2: Comparison of various properties

Features	Kang's scheme	Proposed scheme
security	less	more
Message recovery	supports	supports
Message redundancy	supports	Does not
Suitable for long message	no	yes

VI. CONCLUSION

The proposed signature scheme can withstand parameter reduction attack, forgery attack and can recover message from the signature itself. There is no message redundancy feature used in this scheme, but still it resists forgery attack. The scheme supports message recovery feature, as message is recovered from the signature and there is no need to send message along with the signature. It is also proved in Section 4 that the proposed scheme is more secure due to the use of randomization and key generation using safe primes. It is also suitable for signing large documents. Hence the proposed signature scheme can be applicable in areas like e-banking, e-bidding and e-commerce.

REFERENCES

[1]. L. Kang, X. H. Tang, "A New Digital Signature Scheme without one way hash function and message redundancy", 2005 IEEE.

[2]. C.C. Chang and YF. Chang, "Signing a Digital Signature without using one-way Hash Functions and Message Redundancy Schemes," IEEE Commun. Lett., vol. 8, no. 8, pp. 485-487, Aug. 2004.

[3]. T. ElGamal, "A Public Key Crytosystem and a Sgnature Scheme based on Discrete Logarithm," IEEE Trans. Inform. Theory, vol. IT-31, no. 4, pp. 469-472, 1985.

[4]. X.T. Fu, C.X. Xu and G.Z. Xiao, "Forgery Attacks on Chang et al.'s Signature Scheme with Message Recovery," Cryptology ePrint Archive, Report 2004/236, 2004. http://eprint.iacr.org/.

[5]. S.P. Shieh, C.T. Lin, W.B. Yang, and H.M. Sun, "Digital Multi-signature Schemes for Authenticating Delegates in Mobile Code Systems", IEEE Trans. Veh. Technol., vol. 49, July 2000, pp. 1464-1473.

[6]. J Liu, J Li, " Cryptanalysis and Improvement on a Digital Signature Scheme without using one way hash and Message Redundancy", International Conference on Information Security and Assurance,vol 7,2008

[7]. F.G. Zhang, "Cryptanalysis of Chang et al:'s Signature Scheme with Message Recovery," Cryptology ePrint Archive, Report 2004/213, 2004.