Forgery Attacks on Chang *et al.*'s signature scheme with message recovery [*]

FU Xiaotong, XU Chunxiang and XIAO Guozhen

(Key Laboratory of the CNIS of the Ministry of Education, Xidian Univ., Xi'an, China)

Abstract It is found that Chang *et al.*'s signature scheme with message recovery is not as secure as they claimed, in fact. In this letter, two forgery attacks is proposed to show that the signature can be forged on any uncontrolled messages. To overcome these attacks, the one-way hash functions and the message redundancy schemes may be still used.

Key words: Digital signature, message recovery, cryptanalysis, forgery attack

1 Introduction

Digital signatures become more and more important than before in the modern electronic data processing systems. In the digital signature scheme with message recovery, a legal receiver can recover the original message from the received signatures. The correctness of the recovered messages are usually checked by the message redundancy scheme. Furthermore, one-way hash function and message recovery scheme are used to resist the forgery attacks.

Recently, to reduce the computational cost, C.C.Chang and Y.F.Chang[1] proposed a new digital signature scheme with message recovery without using one-way hash function and message redundancy scheme. However, due to the absence of one-way hash and message redundancy, Chang *et al.*'s scheme suffer from the forgery attack. We propose two forgery attacks to show that attackers who have a valid signature can forge signatures that can be verified validly on any uncontrolled messages. To resist these attacks, the one-way hash functions and the message redundancy schemes may be still used.

The rest of the paper is as following: In the second section, we briefly review Chang *et al.*'s signature scheme. In the third section, two forgery attacks is proposed that can successfully forge signatures. Our conclusion is the last section.

2 Review of Chang *et al.*'s Signature Scheme

We first review Chang *et al.*'s signaturew scheme without using one-way hash function and message redundancy scheme in brief. The scheme consists of two phases: signature-generation phase and verification

[*] This work was supported in part by the Natural Science Foundation of China (60073051)(90104005).

phase. Through our paper, we use the same notation as in [1].

p : a large prime number

g : a primitive element in Z_p.

(x, y): user U's private and public key pair.

where $gcd(x, p-1) = 1$, and $y = g^x \bmod p$.

M: the message to be signed

V: the verifier.

Signature-Generation Phase:

Suppose user U wants to sign the message M. Then U dose the following steps.

Step 1 U computes $s = y^M \bmod p$.

Step 2 U chooses a random number k in $[1, p-1]$,
computes $r = M \cdot s \cdot g^{-k} \bmod p$.

Step 3 U computes t, where $s + t = x^{-1} \cdot (k - r)(\bmod(p-1))$.

step 4 U sends the signature (r, s, t) of M to the verifier V.

Verification Phase:

After receiving the signature (r, s, t), V performs as following.

Step 1 V computes:

$$\begin{aligned} M' &= y^{s+t} \cdot r \cdot g^r \cdot s^{-1} \\ &= g^{x(s+t)} M \cdot s \cdot g^{-k} \cdot g^r \cdot s^{-1} \\ &= g^{k-r} \cdot M \cdot g^{-k+r} (\text{mod} p) \end{aligned}$$

step 2 V checks whether $s = y^{M'} \bmod p$.

If it holds, V is convinced that (r, s, t) is indeed the signature generated by U of the recovered message M'.

3 Forgery Attacks on Chang *et al.*'s Signature Scheme

In this section, we propose two forgery attacks to show that Chang *et al.*'s signature scheme is not secure. Assume A is an attacker and suppose that A already had a valid signature (r, s, t) generated by the legal signer U of the message M. Then, A can forge valid signature (r', s', t') as following two forgery attacks.

Forgery Attack 1

ARandomly chooses $r' \in Z_p^*$,

AComputes:

$$\begin{aligned} m &= r' \cdot g^{r'} \bmod p \\ s' &= y^m \bmod p \\ t' &= (m - s') \bmod (p-1) \end{aligned}$$

(r', s', t') is a forged signature of message m.

And (r', s', t') is a valid signature of message m, because:

$$\begin{aligned} m' &= y^{s'+t'} r' g^{r'} (s')^{-1} \\ &= y^m r' g^{r'} y^{-m} \\ &= r' g^{r'} \\ &= m \bmod p \end{aligned}$$

Thus, $y^{m'} = y^m = s \bmod p$. (r', s', t') is a valid signature of message m.

Forgery Attack 2

ARandomly chooses $R \in Z_p^*$, and Computes:

$$\begin{aligned} r' &= r \cdot R \bmod p \\ m &= MRsg^{r(R-1)} \bmod p \\ s' &= y^m \bmod p \\ t' &= (s + t + m) - s' \bmod (p-1) \end{aligned}$$

(r', s', t') is a valid signature of message m because:

$$\begin{aligned} m' &= y^{s'+t'} r' g^{r'} (s')^{-1} \\ &= y^{s+t+m} rRg^{r+R} y^{-m} \\ &= (y^{s+t} rg^r s^{-1}) \cdot (g^{-r} s) \cdot (Rg^{rR}) \\ &= MRsg^{r(R-1)} \\ &= m \bmod p \end{aligned}$$

Thus, $y^{m'} = y^m = s \bmod p$. (r', s', t') is a valid signature of message m.

4 Conclusion

Two forgery attacks are proposed to show that Chang *et al.*'s signature scheme without using one-way hash function and message redundancy scheme is not as secure as thy claimed, the signature can be forged on any uncontrolled messages. To overcome these attacks, the one-way hash functions and the message redundancy schemes may be still used.

References

[1] C.C.Chang and Y.F.Chang, *Signing a digital signature without using one-way hash function and message redundancy schemes*, IEEE Commun. Lett., vol.8, NO.8, pp.485-487, 2004.

[2] S.-J.Hwang and E.-T. Li, *Cryptanalysis of Shieh-Lin-Yang-Sun signature schme*, IEEE Commun. Lett., vol.7, NO.?, pp.195-196, 2003.

[3] F.G.Zhang, *Cryptanalysis of Chang et al.'s siganture scheme with message recovery*, availlable at http://eprint.iacr.org.

[4] IEICE