Cryptanalysis of Chang *et al.*'s Signature Scheme with Message Recovery

Fangguo Zhang

Department of Electronics and Communication Engineering,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
isdzhfg@zsu.edu.cn

Abstract. Recently, Chang *et al.* [1] proposed a new digital signature scheme with message recovery and claimed that neither one-way hash functions nor message redundancy schemes were employed in their scheme. However, in this letter, two forgery attacks are proposed to show that Chang *et al.*'s signature scheme is not secure. To resist these attacks, the message redundancy schemes may be still used.

Keywords: *Digital signature, message recovery, message redundancy schemes, one-way hash functions, forgery attack.*

1 Introduction

Digital signature schemes allow a signer to transform any arbitrary message into a signed message, such that anyone can verify the validity of the signed message using the signer's public key, but only the signer can generate signed messages. Digital signature is very important in the modern electronic data processing systems. A digital signature scheme with message recovery [2] is useful for many applications in which small messages (*e.g.*, around 100 bits) should be signed. For example, small messages including time, date and identifiers are signed in certified email services and time stamping services. In the digital signature schemes with message recovery, the receiver can recover the original message from the received signature. The correctness of the recovered message is checked by the message redundancy scheme. Moreover, one-way hash functions and message recovery schemes are used to guard against the forgery attacks.

In [3], Shieh *et al.* proposed efficient digital multisignature schemes. The required memory of local devices is greatly reduced. Further, one-way hash functions and message redundancy schemes are not used. However, Hwang and Li indicated that the underlying signature scheme with message recovery of Shieh *et al.*'s multisignature schemes suffers from some attacks because of the absence of one-way hash functions and message redundancy schemes [4]. They claimed that message redundancy schemes are still needed to resist forgery attacks.

Recently, Chang *et al.*[1] proposed a new digital signature scheme with message recovery and claimed that their scheme preserved the properties of Shieh

et al.'s signature scheme. One major characteristic of Chang *et al.*'s scheme is to avoid using one-way hash functions and message redundancy schemes too.

However, still due to the absence of message redundancy and one-way hash functions, Chang *et al.*'s schemes suffer from the forgery attack. In this letter, we proposed two forgery attacks on Chang *et al.*'s signature scheme. To resist these attacks, the message redundancy schemes may be still used.

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

We first review Chang *et al.*'s signature scheme without using one-way hash functions and message redundancy schemes in brief using the same notation as [1].

In this scheme, there are two public system parameters p and g, where p is a large prime number and g is a primitive element in $GF(p)$. User U chooses his/her private key x, where $gcd(x, p-1) = 1$, and computes the public key $y = g^x \bmod p$. The digital signature scheme is composed of two phases: signature generation phase and verification phase.

A. **Signature Generation Phase:** Suppose that U wants to sign the message M. Then U does the following.

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

Step 2 U chooses a random number $k \in \mathbb{Z}_{p-1}^*$ and computes $r = M \cdot s \cdot g^{-k} \bmod p$.

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

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

B. **Verification Phase:** After receiving the signature (s, r, t), V performs as follows.

Step 1 V computes

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

Step 2 V checks whether $s = y^{M'} \bmod p$. If it holds, V is convinced that (s, r, t) is indeed the signature generated by U of the recovered message M'.

About the correctness and the security analysis of the scheme refer to [1].

3 Cryptanalysis of Chang *et.al.*'s Signature Scheme

In this section, we show that Chang *et al.*'s signature scheme with message recovery is not secure. Due to the absence of message redundancy and one-way hash functions, Chang *et al.*'s schemes suffer from the forgery attack. We propose two forgery attacks on Chang *et al.*'s signature scheme.

Assume that $\mathcal{A}$ is an adversary. The details of this cryptanalysis are described as follows:

Forgery Attack 1: Suppose that $\mathcal{A}$ had already a valid signature (s, r, t) generated by the signer U of the recovered message M. Now, $\mathcal{A}$ can forge another valid signature (s', r', t') as follows.

1. $\mathcal{A}$ chooses a random number $\alpha \in \mathbb{Z}_{p-1}^*$ and computes the message $m = M \cdot y^{\alpha} \bmod p$.
2. $\mathcal{A}$ sets $s' = y^m \bmod p$.
3. $\mathcal{A}$ sets $r' = r$.
4. $\mathcal{A}$ sets $t' \equiv s + t - M + \alpha - s' + m \bmod (p-1)$.

Now, we show that (s', r', t') is a valid signature of the signer U on the recovered message m.

$$\begin{aligned} & y^{s'+t'} \cdot r' \cdot g^{r'} \cdot s'^{-1} \\ \equiv\ & y^{s'+s+t-M+\alpha-s'+m} \cdot r \cdot g^{r} \cdot y^{-m} \\ \equiv\ & y^{s'+s+t-M+\alpha-s'+m-m} \cdot r \cdot g^{r} \\ \equiv\ & y^{s+t+\alpha} \cdot r \cdot g^{r} \cdot y^{-M} \\ \equiv\ & y^{\alpha} \cdot y^{s+t} \cdot r \cdot g^{r} \cdot s^{-1} \\ \equiv\ & y^{\alpha} \cdot M \pmod p \\ \equiv\ & m \end{aligned}$$

$$s' = y^m \bmod p.$$

Therefore, the forgery (s', r', t') satisfies the verification phase.

Forgery Attack 2:

Suppose that $\mathcal{A}$ had a valid signature (s, r, t) generated by the signer U of the recovered message M. Now, $\mathcal{A}$ can forge another signature:

1. Choose a random number $\alpha \in \mathbb{Z}_p^*$ and set $r' = \alpha \cdot r \bmod p$.
2. Find $\beta \in \mathbb{Z}_{p-1}^*$ such that $r + \beta \bmod (p-1) = r' \bmod (p-1)$.
3. Set $m = M \cdot \alpha \cdot g^{\beta} \bmod p$.
4. Set $s' = y^m \bmod p$.
5. Set $t' \equiv s + t - M - s' + m \bmod (p-1)$.

Now, we show that (s', r', t') is a valid signature of the signer U on the recovered message m.

$$\begin{aligned} & y^{s'+t'} \cdot r' \cdot g^{r'} \cdot s'^{-1} \\ \equiv\ & y^{s'+s+t-M-s'+m} \cdot \alpha \cdot r \cdot g^{r+\beta} \cdot y^{-m} \\ \equiv\ & y^{s'+s+t-M-s'+m-m} \cdot \alpha \cdot r \cdot g^{r+\beta} \\ \equiv\ & y^{s+t} \cdot \alpha \cdot r \cdot g^{r} \cdot g^{\beta} \cdot y^{-M} \\ \equiv\ & y^{s+t} \cdot r \cdot g^{r} \cdot s^{-1} \cdot \alpha \cdot g^{\beta} \\ \equiv\ & M \cdot \alpha \cdot g^{\beta} \pmod p \\ \equiv\ & m \end{aligned}$$

$$s' = y^m \bmod p.$$

So, V can be convinced that (s', r', t') is indeed the signature generated by U of the recovered message m.

Therefore, the adversary $\mathcal{A}$ forges the signature of the message successfully because the messages are not protected by one-way hash functions and any message redundancy schemes. The major limitation of these attacks is that the context of the message cannot be arbitrary. Due to the randomness of $\alpha \in \mathbb{Z}_p^*$, the recovered message m in our forgery is random. To overcome these attacks, an easy way is to adopt the message redundancy scheme on the recovered message M.

4 Conclusion

To reduce the computational cost, Chang *et al.* [1] proposed a new digital signature scheme with message recovery without using one-way hash functions and message redundancy schemes. However, we proposed two attacks on their signature scheme to show that the signature can be forged on an uncontrolled message. To overcome these attacks, the straightforward way is to adopt the message redundancy schemes.

References

1. C. C. Chang and Y. F. 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, 2004.
2. K. Nyberg and R.A. Rueppel, *Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem*, Proc. of Eurocrypt94, Springer-Verlag, LNCS 950, pp.182C193, 1995.
3. S.-P. Shih, C.-T. Lin, W.-B. Yang, and H.-M. Sun, *Digital multisignature schemes for authenticating delegates in mobile code systems*, IEEE Trans. Veh. Technol., vol. 49, pp. 1464C1473, July 2000.
4. S.-J. Hwang and E.-T. Li , *Cryptanalysis of Shieh-Lin-Yang-Sun signature scheme*, IEEE Commun. Lett., vol. 7, pp. 195C196, Apr. 2003.