Universal Forgeability of Wang-Wu-Wang Key-Insulated Signature Scheme

Zhengjun Cao

Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Science,

Chinese Academy of Sciences, Beijing, P.R. China. 100080 zjcamss@hotmail.com

(Graduate School of Chinese Academy of Sciences)

Abstract Wang et al. recently proposed a new perfect and strong key-insulated signature scheme in [1]. We find that the scheme is universally forgeable. In the paper we present a simple and direct attack on it.

Keywords key-insulated signature scheme, universal forgeability.

1 Introduction

Dodis Y. et al. have investigated key-insulated public key cryptosystems in 2002.[2] About half year later, they presented another technical report[3] on it, entitled Key-insulated Signature Schemes. Loosely speaking, key-insulated signature is more secure than classical signature. Of course, we should observe that designing key-insulated signature scheme is more difficult than classical signature scheme. As far as more details of key-insulated signature, one can refer to [3].

Recently, Wang et al. proposed a new perfect and strong key-insulated signature scheme.[1] Although the authors claimed that the key-updated algorithm, signing algorithm and verifying algorithm are more efficient than those algorithms in [3], we find that the new scheme is universally forgeable. In the paper we show its universal forgeability by a simple and direct attack.

The organization of the paper is as follows: Section 2 reviews Wang-Wu-Wang key-insulated signature scheme. In section 3 we give a simple and direct attack on it. Some conclusion remarks will be given in section 4.

2 Wang-Wu-Wang key-insulated signature scheme

Setup

$n = p_1 p_2$: a product of two secure primes p_1, p_2.

S_{id}: the identity of signer.

$Nonce$: random number for once.

$H(\cdot)$: $\{0,1\}^* \longrightarrow \{0,1\}^l$ collision-free hash function, l is the binary length of n.

User picks a polynomial $f(x) = \sum_{i=0}^{N} b_i x^i$ satisfying $f(j+1) = f(j)^2 \ mod \ n$, and a polynomial $a(x) = \sum_{i=0}^{N} a_i x^i$. Denote $F(x) := (\sum_{i=0}^{N}(a_i + b_i)x^i)^2 \ (:= c^2(x))$, take $\sum_{i=0}^{N} a_i x^i$ as master key SK^*, $f(0)$ as initial key SK_0. The user's public key is $(n, F(1), \cdots, F(N))$. In period j, the signing key is $SK_j = c(j) = \sum_{i=0}^{N} a_i j^i + f^2(j-1)$.

Algorithm It consists of five algorithms: $(Gen, Upd^*, Upd, Sign, Verify)$.

$\underline{Gen(1^k, N)}$

$$f(0) \longleftarrow_R Z_n$$

for $i = 1, \cdots, N$

$$f(i) = f^2(i-1)$$

$$f(x) = \sum_{i=0}^{N} f(i) \prod_{j \neq i, j=0}^{N} \frac{x - x_j}{x_j - x_i} = \sum_{i=0}^{N} b_i x^i$$

for $i = 0, 1, \cdots, N$

$$\begin{aligned} F(x) &= [\sum_{i=0}^{N}(a_i + b_i)x^i]^2 = c^2(x) \\ SK^* &= \sum_{i=0}^{N} a_i x^i = a(x) \\ SK_0 &= f(0) \\ PK &= (n, F(1), \cdots, F(N)) \end{aligned}$$

Return (PK, SK^*, SK_0)

$\underline{Upd^*(j, a(x)):}$ return $SK_j' = a(j)$

$\underline{Upd(j, f(0), a(j)) :}$ return $SK_j = a(j) + f^{2^j}(0)$

$\underline{Sign(j, SK_j, M) :}$ M is the message to sign; SK_j is the secret key for period j

For each signature:

$$\begin{aligned} r &\longleftarrow_R Z_n^* \\ s &= H(M \parallel S_{id} \parallel j \parallel Nonce \parallel r^2 \ mod \ n) \\ d &= r/SK_j^s \ mod \ n \end{aligned}$$

Return $(j, M, S_{id}, Nonce, s, d)$

$\underline{Verify(PK, j, M, S_{id}, Nonce, s, d)}$

M is the signed message, PK is the public key, (s, d) is the signature of M in period j, S_{id} is the signer's identification, $Nonce$ is a one time random number.

If

$$s = H(M \parallel S_{id} \parallel j \parallel Nonce \parallel d^2 F^s(j) \ mod \ n)$$

return 1, otherwise return 0.

3 Universal forgeability

The authors claim that the security of the signature scheme is based on factoring problem, but we find it is false. In the section we present a simple and direct attack on it, only according to the verifying phase. As far as the possible faults in the whole description of algorithm (see [1]) and other possible attacks, we do care nought for them.

The forgery procedure: Given an arbitrary message M, period j, the identification S_{id} of the signer, a one time random number $Nonce$ and the public parameter $F(j)$, the attacker executes the following procedure:

Step 1: Pick $\lambda \in_R Z_n$

Step 2: Compute

$$s = H(M \parallel S_{id} \parallel j \parallel Nonce \parallel F^{\lambda}(j) \ mod \ n)$$

Step 3: Check whether $\lambda - s$ is a even or odd. If it is an odd, goto step 1.

Step 4: Compute $d = F^{\frac{\lambda - s}{2}}(j) \ \ mod \ n$, output $(j, M, S_{id}, Nonce, s, d)$.

Correctness: By the verifying phase, It only needs to verify

$$d^2 F^s(j) = (F^{\frac{\lambda - s}{2}}(j))^2 F^s(j) = F^{\lambda}(j) \ \ (mod \ n)$$

In fact, the challenge in the scheme is very easy to shun.

4 Conclusion

In the paper, we analyze Wang-Wu-Wang key-insulated signature scheme. Our results show that the scheme is universally forgeable. As far as other attacks on it, we do care nought for them. But we hold that the attack is more simple and direct. All in all, the scheme is fragile.

References

[1] Jilin Wang, Qianhong Wu, Yumin Wang. A new Perfect and strong key-insulated signature scheme. ChinaCrypt'2004, pp.233-239.

[2] Dodis Y., Katz J., Xu S., et al.. Key-insulated public key cryptosystems. EuroCrypt'2002. http://citeseer.nj.nec.com/dodis02keyinsulated.html

[3] Dodis Y., Katz J., Xu S., et al.. Strongkey-insulated signature schemes. DIMICS Technical Report 2002-25, November 2002. http://citeseer.nj.nec.com/dodis02strong.html