Remark on the Threshold RSA Signature Scheme

Chuan-Ming Li, Tzonelih Hwang, Narn-Yih Lee
Institute of Information Engineering
National Cheng-Kung University
Tainan, Taiwan, R.O.C.

Abstract

Shared generation of secure signatures, called the threshold signatures, was introduced by Desmedt and Frankel in 1991. A threshold signature scheme is not only a threshold scheme, but also a signature scheme. Therefore, it should possess the properties of both threshold scheme and digital signature scheme. In this paper, we investigate conspiracy attacks on the Desmedt and Frankel's threshold RSA signature scheme. We also discuss the requirements of secure threshold signature scheme.

1 Introduction

A digital signature is some information which is dependent on the message and on data known only to the signer. Thus, a secure signature scheme should be able to protect a signature from being forged by the receiver or another person, and the sender cannot deny having signed the message.

The signer of the conventional digital signature schemes is usually a single user. However, the responsibility of signing messages needs to be shared from time to time. For example, a company may require that any policy decision must be signed by k directors before it is issued. It may also be a company's policy that checks should be signed by k individuals rather than by one person. Shared generation of secure signatures, called the *threshold signatures*, are used to solve these problems [1].

It is very important that a (k, l) threshold signature scheme is not only a threshold scheme in the sense that less than k users cannot generate a valid signature, but also a signature scheme such that the signature of a particular set of k users should not be forged by another set of k users. In general, there are several requirements that (k, l) threshold signatures should satisfy:

1. Similar to the (k, l) threshold secret sharing scheme, the group secret key K can be divided into l different "*secretshares*", K_1 K_2, ..., K_l, such that

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 413-419, 1994.

(a) the group signature can be easily produced with knowledge of any k secret shares ($k \leq l$);

(b) with knowledge of any $k-1$ or fewer secret shares, it is impossible to generate a group signature;

(c) the group secret key cannot be derived from the released group signature and all partial signatures; and

(d) it is impossible to derive any secret share from the released group signature and all partial signatures.

2. It is better that the size of the group signature is equivalent to the size of an individual signature.

3. The group signature can be verified by any outsider and the verification process should be as simple as possible.

4. The signing group holds the responsibility to the signed message. That is, each signer in this group cannot deny having signed the message.

5. The partial signatures and the group signature cannot be forged by malicious users.

In 1991, Desmedt and Frankel [1] proposed the first (k,l) threshold digital signature scheme based on the RSA assumption. In this paper we shall show that if k or more shareholders conspire, then the system secret of their scheme will be revealed with a high probability. Once the system secret is revealed by these shareholders, they can impersonate another set of shareholders to sign messages without holding the responsibility to the signatures, and a malicious group of k signers can deny having signed a message though in fact they have signed the message. However, this paper does not weaken the security of the threshold signature scheme in the sense that our remarks do not give more power to $k-1$ or less shareholders than estimated before.

The structure of this paper is as follows. In Section 2, we review the Desmedt et al.'s threshold RSA signature scheme. In Section 3, we shall show how $k+1$ users can conspire to derive the system's secret with a high probability. Then, we show that the system secret can also be revealed by the conspiracy of k users. Finally, we conclude this paper in Section 5.

2 Desmedt et al.'s Threshold RSA Signature Scheme

Let $n = pq$ where p, q are large primes. For p and q to be safe primes, let $p = 2p' + 1$ and $q = 2q' + 1$ where p', q' are primes [2][3]. Define $\lambda(n) = 2p'q'$ (λ is the Carmichael function, i.e., the exponent of $Z_n^*(\cdot)$.) The secret key is d which was chosen at random such that $\gcd(d, \lambda(n)) = 1$ (so d is odd) and the public key is e such that $de \equiv 1 \mod \lambda(n)$. All shareholders in the Desmedt et

al.'s scheme form a set A ($|A| = l$) such that any subset B ($|B| = k$) in A can collectively generate a signature for a message.

Basically, the Desmedt et al.'s threshold RSA signature scheme is based on interpolation polynomials over the integers. As in the Lagrange interpolation scheme of [4], let $f(x)$ be a polynomial of degree $k-1$ such that $f(0) = d - 1$. In the scheme, there is a share distribution center (SDC) which would choose $p, q, d, f(x)$ and distribute to each shareholder i a public integer x_i and a secret share K_i:

$$K_i = \frac{f(x_i)/2}{\left(\prod_{\substack{j \in A \\ j \neq i}} (x_i - x_j)\right)/2} \pmod{p'q'}, \tag{1}$$

where all the x_i's are odd and all $f(x_i)$'s are even.

To create a signature S_m of a message m, each shareholder $i \in B$ will generate a modified share $a_{i,B}$:

$$a_{i,B} = K_i \cdot \left(\prod_{\substack{j \in A \\ j \notin B}} (x_i - x_j) \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j)\right) \tag{2}$$

and will calculate the partial result $s_{m,i,B} \equiv m^{a_{i,B}} \bmod n$. Since $f(0) = d - 1$ and

$$f(x) = \sum_{i \in B} K_i \prod_{\substack{j \in A \\ j \notin B}} (x_i - x_j) \prod_{\substack{j \in B \\ j \neq i}} (x - x_j) \pmod{\lambda(n)},$$

we can have that

$$\sum_{i \in B} a_{i,B} \equiv d - 1 \mod \lambda(n). \tag{3}$$

Each $i \in B$ sends the partial result $s_{m,i,B}$ to a Combiner C. To create the signature S_m, C calculates

$$S_m \equiv m \cdot \prod_{i \in B} s_{m,i,B} \equiv m \cdot m^{d-1} \equiv m^d \bmod n. \tag{4}$$

The receiver of the S_m can check the correctness of S_m by verifying

$$m \stackrel{?}{\equiv} (S_m)^e \bmod n, \quad \text{where } e \text{ is the public key.}$$

The following example is used to illustrate Desmedt et al.'s threshold RSA signature scheme.

Example 1 : We assume that there are five shareholders in the system and any two of them can generate the signature S_m for a message m, i.e., $|A| = l = 5$, $|B| = k = 2$. First of all, the SDC chooses

$$\begin{aligned} p &= 2p' + 1 = 2 \cdot 23 + 1 = 47, \\ q &= 2q' + 1 = 2 \cdot 29 + 1 = 59, \\ d &= 221, \\ f(x) &= 6 \cdot x^{k-1} + (d-1) = 6 \cdot x + 220, \\ \text{and } x_1 &= 3,\ x_2 = 7,\ x_3 = 13,\ x_4 = 17,\ x_5 = 19. \end{aligned}$$

Thus,

$$\begin{aligned} n &= pq = 47 \cdot 59 = 2773\ , \\ \lambda(n) &= 2p'q' = 2 \cdot 23 \cdot 29 = 1334\ , \\ p'q' &= 23 \cdot 29 = 667\ , \\ e &= 833, \text{where } de \equiv 1 \mod \lambda(n)\ , \\ \text{and } f(x_1) &= 238,\ f(x_2) = 262,\ f(x_3) = 298,\ f(x_4) = 322,\ f(x_5) = 334. \end{aligned}$$

By using Eq. (1), the SDC can calculate the secret share K_1 as follows:

$$\begin{aligned} K_1 &= \frac{f(x_1)/2}{(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)/2} \bmod p'q' \\ &= \frac{238/2}{-4 \cdot -10 \cdot -14 \cdot -16/2} \pmod{667} = 197. \end{aligned}$$

Similarly, the SDC calculates $K_2 = 219$, $K_3 = 179$, $K_4 = 575$ and $K_5 = 219$. Then, the SDC sends x_i and K_i to the Shareholder i. We assume that the Shareholder 1 and the Shareholder 4, i.e., $B = \{1, 4\}$, would like to generate a signature S_m for a message m. The Shareholder 1 uses Eq. (2) to generate the modified share $a_{1,B}$,

$$\begin{aligned} a_{1,B} &= K_1 \cdot (x_1 - x_2)(x_1 - x_3)(x_1 - x_5)(0 - x_4) \\ &= 197 \cdot -4 \cdot -10 \cdot -16 \cdot -17 = 2143360, \end{aligned}$$

and sends the partial result $s_{m,1,B}$,

$$s_{m,1,B} \equiv m^{a_{1,B}} \bmod n = m^{2143360} \bmod 2773$$

to the Combiner C. Similarly, The Shareholder 4 also calculates the modified share $a_{4,B} = 138000$ and sends the partial result

$$s_{m,4,B} = m^{138000} \bmod 2773$$

to C. Finally, the C creates the signature as:

$$S_m \equiv m \cdot s_{m,1,B} \cdot s_{m,4,B} = m^{2281361} \equiv m^{221} \bmod 2773.$$

The signature receiver can check

$$m \stackrel{?}{\equiv} (S_m)^e \bmod n, \stackrel{?}{\equiv} (S_m)^{833} \bmod 2773,$$

to verify whether the signature S_m is correct or not.

3 Conspiracy Attack by k+1 Users

It is clear that $k-1$ or less shareholders cannot generate a valid signature, and once a signature is generated by k shareholders, no one can perform an impersonation or substitution attack. However, we are going to show that arbitrary set of $k+1$ shareholders can conspire to compute the system's secret $\lambda(n)$ or $p'q'$ with a high probability. This attack refers to the observation of Davida et al. in [5].
Let

$$\begin{aligned} w_1 &\equiv y \mod \lambda(n), \\ w_2 &\equiv y \mod \lambda(n), \\ w_3 &\equiv y \mod \lambda(n). \end{aligned}$$

If all the values of w_1, w_2, and w_3 are known, then one can have

$$\begin{aligned} w_3 - w_2 &= z \cdot \lambda(n), \\ w_2 - w_1 &= z' \cdot \lambda(n), \\ &\quad \text{for some integers } z \text{ and } z'. \end{aligned}$$

Therefore, $\lambda(n)$ will be revealed with a high probability by finding the greatest common divisor (GCD) of $(w_3 - w_2)$ and $(w_2 - w_1)$.

According to the combination theorem, there are $k+1$ possible ways to choose any k shareholders from $k+1$ shareholders. Each choice forms a subset, B_j, of k users. If $k+1$ (*i.e.*, $k \geq 2$) shareholders act in collusion in the Desmedt et al.'s scheme, then they may compute w_j, where $w_j = \sum_{i \in B_j} a_{i,B_j}$, $1 \leq j \leq k+1$. By the Davida et al.'s observation, we have

$$\begin{aligned} w_1 &\equiv (d-1) \mod 2p'q', \\ w_2 &\equiv (d-1) \mod 2p'q', \\ w_3 &\equiv (d-1) \mod 2p'q'. \\ &\cdots \end{aligned}$$

Thus, the system secret $2p'q'$ or $p'q'$ will be revealed with a high probability by finding the GCD of $(w_3 - w_2)$ and $(w_2 - w_1)$. Once the system secret is revealed by these $k+1$ shareholders, they are able to compute all of the secret shares. Then, these malicious shareholders can impersonate other shareholders to sign messages without holding the responsibility to the signatures. The following example is used to illustrate this attack.

Example 2 : Let us consider the Example 1 again. We assume that the Shareholders 1, 3 and 4 conspire to compute the system secret $p'q'$. They constitute three subsets $B_{(1)} = \{1,3\}$, $B_{(2)} = \{1,4\}$, $B_{(3)} = \{3,4\}$ and compute $\sum a_{i,B}$, for each subset.

$$\begin{aligned}
\sum_{i \in B_{(1)}} a_{i,B_{(1)}} &= a_{1,B_{(1)}} + a_{3,B_{(1)}} \\
&= 2294656 + -77328 = 2217328, \qquad \text{(a)} \\
\sum_{i \in B_{(2)}} a_{i,B_{(2)}} &= a_{1,B_{(2)}} + a_{4,B_{(2)}} \\
&= 2143360 + 138000 = 2281360, \qquad \text{(b)} \\
\sum_{i \in B_{(3)}} a_{i,B_{(3)}} &= a_{3,B_{(3)}} + a_{4,B_{(3)}} \\
&= 1095480 + 2093000 = 3188480, \qquad \text{(c)}
\end{aligned}$$

Then, they compute :

$$\begin{aligned}
\text{(c) - (b)} &= 907120 = z \cdot \lambda(n) = z \cdot 2p'q', \qquad \text{(e)} \\
\text{(b) - (a)} &= 60432 = z' \cdot \lambda(n) = z' \cdot 2p'q', \qquad \text{(f)} \\
&\qquad \text{for some integer } z \text{ and } z'.
\end{aligned}$$

Because p' and q' are odd primes, the product of $p' \cdot q'$ must be an odd number. By removing the factor 2 in (e) and (f) (i.e., $(e) = 11339$ and $(f) = 2001$), they will obtain

$$GCD(11339, 2001) = 667 = p' \cdot q'$$

Thus, $\lambda(n) = 2p'q' = 1334$.

4 Conspiracy Attack by k Users

In this section, we will show that if only k shareholders act in collusion, they can also compute the system secret with a high probability. The attack is described as follows.

As the conspiracy attack by $k+1$ shareholders, any subset B of k malicious shareholders can have

$$w = \sum_{i \in B} a_{i,B} \equiv (d-1) \mod \lambda(n), \qquad (5)$$

Multipling Eq. (5) by the public key e, we can have

$$\begin{aligned}
e \cdot w &\equiv e \cdot (d-1) \mod \lambda(n), \\
e \cdot w &\equiv ed - e \mod \lambda(n),
\end{aligned}$$

Because $ed \equiv 1 \mod \lambda(n)$, we can compute

$$\begin{aligned} e \cdot w &\equiv 1 - e \mod \lambda(n), \\ e \cdot w + e - 1 &\equiv 0 \equiv z \cdot \lambda(n) \mod \lambda(n), \\ &\text{for some integer } z. \end{aligned} \tag{6}$$

The result of Eq. (6) is a multiple of $\lambda(n)$. Therefore, n can be factored in polynomial time by [6].

5 Conclusions

In this paper, we have showed that the system secret of Desmedt et al.'s threshold RSA signature scheme can be revealed with a high probability by the conspiracy of $k+1$ or k shareholders. It will be very challenging to devise a threshold signature scheme that satisfies the requirements proposed in this paper.

Acknowledgement

The authors wish to thank G. R. Blakley, Y. Desmedt, Y. Frankel, M. Yung and G. I. Davida for their valuable suggestions to this paper at Crypto '93. Dr. Y. Desmedt pointed out that the system secret can also be revealed by the conspiracy of k users as shown in Section 4. This paper is supported by the National Science Council of R. O. C. under the contract NSC 82 - 0408 - E - 006 - 026.

Reference

[1] Y. Desmedt and Y. Frankel: "Shared Generation of Authenticators and Signatures", Advances in Cryptology - Cryto '91, Proceedings, pp.457-469, Springer Verlag, 1991.

[2] B. Blakley and G. R. Blakley: "Security of Number Theoretic Public Key Cryptosystems Against Random Attack", Cryptologia, 1978. In three parts: Part 1: 2(4), pp.305-321, Oct 1978; Part 2: 3(1), pp.29-42, Jan 1979; Part 3: 3(2), pp.105-118, Apr 1979;

[3] G. R. Blakley and I. Borosh: "RSA Public Key Cryptosystems Do Not Always Conceal Messages", Computers & Mathematics with Applications, 5(3): 169-178, 1979.

[4] A. Shamir: "How to share a secret", Commun. ACM, 22:612-613, 1979.

[5] G. I. Davida, D. L. Wells, and J. B. Kam: "A Database Encryption System with Subkeys", ACM Trans. Database System, 6, (2), pp.312-328, 1981.

[6] Gary L. Miller: "Riemann's hypothesis and tests for primality", J. Computer Systems Sci., 13, pp.300-317, 1976.