An attack on Horng's identification scheme based on Shamir's modified RSA

C. J. Mitchell, S.-L. Ng

Mathematics Department, Royal Holloway, University of London,

Egham, Surrey TW20 0EX, United Kingdom

Abstract

In [1], Horng proposed an identification scheme based on Shamir's modified RSA ([2]). We show that the scheme is vulnerable to active attacks which enable the attacker to obtain the factorisation of the public key.

In [1], Horng proposed an identification scheme based on Shamir's "RSA for paranoids" [2]. This modified RSA cryptosystem is as follows. Let Alice choose two large primes p and q with $p << q$. Let $n = pq$ and $\phi(n) = (p-1)(q-1)$. Let e be the public exponent and d the secret exponent, where $ed \equiv 1 \bmod \phi(n)$, and let d' be an integer, $0 < d' < p-1$, with $d' \equiv d \bmod (p-1)$. Alice's public key pair is then (e, n) while her secret key pair is (d', p). For a plaintext m with $m < p$, the corresponding ciphertext is $c \equiv m^e \bmod n$. To decrypt, Alice simply computes $m \equiv c^{d'} \bmod p$. The advantage of this modified RSA is that Alice only needs to perform operations modulo p, while the other prime q can be chosen to be large enough to prevent general factorisation attacks.

Horng's identification scheme [1] is based on Shamir's modified RSA. Let n, p, q, e, d and d' be as above, and let $|x|$ denote the bit length of the integer x. Alice makes public e, n, $|p|$ and a large prime r with $r < p$. Alice identifies herself to Bob using the following protocol:

1. Alice sends her public key (e, n) and its certificate to Bob and Bob verifies the correctness of the public key.

2. Bob chooses an integer $R < p$ at random with $(R, r) = 1$ and sends $U \equiv R^e \bmod n$ to Alice.

3. Alice computes $V \equiv U^{d'} \bmod p$, chooses a randomly with $1 \leq a \leq r$, and sends $W = V + ar$ to Bob.

4. Bob computes $R' \equiv W \bmod r$ and accepts Alice's identity if $R' = R \bmod r$.

We show that this identification scheme is vulnerable to an active attack which results in Bob learning the value of p. The attack is outlined below:

1. Bob chooses $R \simeq p$, with $|R| = |p|$.

2. Bob sends $U \equiv R^e \bmod n$ to Alice.

3. Alice replies with W as above.

4. Bob then computes $R' \equiv W \bmod r$.

   If $R' = R \bmod r$ then $R < p$.

   If $R' \neq R \bmod r$ then $R \geq p$.

After each run of the protocol Bob knows whether p is greater or lesser than his choice of R. This enables him to conduct a binary search for p. This attack works because of the following:

If $R < p$ then the protocol is run correctly and Bob obtains $R' = R \bmod r$.

Let $R \geq p$. Then $V = U^{d'} \bmod p = R''$ and $R'' = R \bmod p$ with $R'' < R$. So $R'' = R - sp$ for some integer $s > 0$, and $W = V + ar = R'' + ar = R - sp + ar$. Now Bob computes $R' \equiv W \bmod r = (R - sp + ar) \bmod r \equiv (R - sp) \bmod r = R'$, and $R' = R \bmod r$ if and only if $r|sp$, if and only if $r|s$ since p is prime. Now, if $|R| = |p| = k$, then

$2^{k-1} \leq R, p < 2^k$. If $s \geq 2$ then $sp \geq 2^k$ and $R - sp < 0$ which we can't have. So $s = 1$ and r does not divide s. Hence if $R \geq p$ then $R' \neq R \bmod p$.

References

[1] G. Horng, "Identification scheme based on Shamir's 'RSA for paranoids' ", *Electronics Letters*, Vol.35, No. 22, 1999, pp 1941–1942.

[2] A. Shamir, "RSA for paranoids", *CryptoBytes (The Technical Newsletter of RSA Laboratories)*, Vol. 1, 1995, pp 1–4.