AN ATTACK ON A SIGNATURE SCHEME PROPOSED BY OKAMOTO AND SHIRAISHI*

Ernest F. Brickell
Bell Communications Research
Morristown, NJ 07960

and

John M. DeLaurentis
Sandia National Laboratories
Albuquerque, NM 87185

Abstract

Recently Okamoto and Shiraishi proposed a public key authentication system [1]. The security of the scheme is based on the difficulty of solving quadratic inequalities. This new system is interesting since the amount of computing needed for the proposed scheme is significantly less than that needed for an RSA encryption.

This report is an investigation into the security of the proposed digital signature scheme. We demonstrate that if the system is used as it is presented, an opponent could sign messages without factoring the modulus. Further, we suggest a modification which may not have the same flaw as the proposed scheme.

Introduction

Prior to the publication of this authentication system, Ong, Schnorr, and Shamir presented a public key signature scheme [2] which was based on the difficulty of solving a quadratic equation over the ring of integers modulo n (here n is the product of two large rational primes). Pollard produced a random polynomial time algorithm [3] which would allow an opponent to sign messages without knowing the secret key. In an attempt to overcome the weakness pointed out by

* This work performed at Sandia National Laboratories supported by the U. S. Dept. of Energy under contract No. DE-AC04-76DP00789.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 28-32, 1986.

Pollard, a new version of the signature scheme was introduced [4]. This variant was based on the difficulty of solving a polynomial equation over the quadratic integers. It has been shown that the new system is also insecure [5]. In fact, breaking the latest scheme can be "reduced" to the problem of solving the original quadratic equation.

The digital signature scheme proposed by Okamoto and Shiraishi is similar to the ones proposed by Ong, Schnorr, and Shamir in that it is based on the difficulty of solving a quadratic expression. More precisely, the signature s is considered to be valid for the message m if and only if

$$(*) \qquad h(m) \leq s^2 \pmod n \leq h(m) + \delta \quad , \qquad \delta = O(n^{2/3})$$

and s is not "small in absolute value"; that is, $\gamma \leq s \leq n-\gamma$, for a suitably chosen γ. Here $h(\cdot)$ is a "one-way" function and the modulus n has the form $n = p^2q$, for large primes p,q. In this paper we will use the expression $x \pmod n$ to denote the least nonnegative integer congruent to x mod n. The idea behind the authentication scheme is to force an opponent to compute an approximate square root for h(m).

Cryptanalysis of the Basic Scheme

We show that an opponent can sign messages without knowing the factorization of n by using the following procedure: Choose x such that for some positive integers k, ℓ and nonnegative integer c we have

$$2kx = \ell n + c$$

where $k = O(n^{1/12})$ and $c = O(n^{1/6})$. (For example, let $x = \lceil \ell/2k \rceil$, $k = O(n^{1/12})$, $c = O(n^{1/6})$.) Next we calculate

$$y = (h(m) - x^2) \bmod n \quad ,$$

$$z = (k^{-2}y) \bmod n \quad ,$$

$$z = \lceil \sqrt{z} \rceil = \sqrt{z} + \varepsilon \quad ,$$

here $\lceil w \rceil$ is the least integer which is greater than or equal to w. Finally we set

$$s = x + ka \quad .$$

We sign the message m with s. To verify that s satisfies condition (*) notice that

$$\begin{aligned} s^2 \pmod n &\equiv (x^2 + 2kxa + k^2a^2) \bmod n \\ &\equiv (x^2 + ca + k^2(z + 2\sqrt{z}\,\varepsilon + \varepsilon^2)) \bmod n \\ &\equiv (x^2 + ca + y + 2k^2\sqrt{z}\,\varepsilon + k^2\varepsilon^2) \bmod n \\ &\equiv (h(m) + ca + 2k^2\sqrt{z}\,\varepsilon + k^2\varepsilon^2) \bmod n \\ &= h(m) + \delta \end{aligned}$$

where $\delta = O(n^{2/3})$ as desired.

This ensures that the signature s would be accepted as authentic.

Cryptoanalysis of the Lower Bits Method

Okamoto and Shiraishi proposed another signature scheme which they call the lower bits method. In addition to the modulus $n = p^2q$ and the one-way function h, they add ε to the public key where ε is an integer and $\varepsilon = O(n^{1/3})$. s is considered a valid signature of m if and only if for $s' = (s^2 - h(m)) \bmod n$ and s' the least nonnegative residue, either

$$s' \equiv 0 \bmod \varepsilon$$

or

$$(n - s') \equiv 0 \bmod \varepsilon \quad ,$$

and s is again not "small in absolute value."

An opponent can forge messages if he can take square roots mod ε, which he can do if he knows the factorization of ε. To forge a signature to m, pick x such that for some positive integers k, ℓ and nonnegative integer c

$$2kx = \ell n + c$$

where $k^2\varepsilon^2 + c\varepsilon < n$. Next calculate

$$x' = h(m) - x^2 \bmod n$$

and a such that $0 \leq a < \varepsilon$ and

$$k^2a^2 + ca \equiv x' \bmod \varepsilon \quad .$$

Let $s = x + ka$. Then

$$\begin{aligned} s^2 - h(m) &\equiv x^2 + 2kxa + k^2a^2 - h(m) \bmod n \\ &\equiv x^2 - h(m) + k^2a^2 + ca \bmod n \\ &\equiv x^2 - h(m) + f\varepsilon + x' \bmod n \\ &\equiv f\varepsilon \bmod n \quad . \end{aligned}$$

Since

$$0 \leq h^2a^2 + ca,\ x' < n$$

then

$$-n < f\varepsilon < n \quad .$$

Hence if $s' = s^2 - h(m) \bmod n$ (i.e., s' is the least nonnegative residue), then either

$$s' = f\varepsilon \qquad (\text{if} \quad f > 0)$$

or

$$n - s' = -f\varepsilon \qquad (\text{if} \quad f < 0) \quad .$$

A Secure (?) Modification

Suppose that instead of signing messages with approximate square roots, the designer chose to sign messages with k^{th} roots, i.e., s is a signature for m whenever $s^k \equiv h(m) \pmod n$, $k > 4$. To be more precise, the signature s is considered valid if the following inequality holds

$$(**) \qquad h(m) \leq s^k \pmod n \leq h(m) + \delta \quad , \qquad \delta = O(n^{2/3}) \quad .$$

The legitimate user can sign messages in nearly the same fashion as in the original scheme. Pick a random $x \in z^*_{pq}$ (z^*_{pq} is the multiplicative group modulo pq). Compute s as follows

$$s = x + ypq$$

where

$$y = w(kx^{k-1})^{-1} \pmod{p}$$

and

$$w = \lceil (h(m) - x^k \pmod{n})/(pq) \rceil \quad .$$

It can be shown that s satisfies (**). We do not know if the modified scheme possesses the same flaw as the original system. However, in view of the demonstrated weakness of the Okamoto-Shiraishi quadratic inequality scheme and the unsuccessful attempts made by Ong, Schnorr and Shamir, the security of the modified system is highly questionable.

References

[1] T. Okamoto, A. Shiraishi, "A Fast Signature Scheme Based on Quadratic Inequalities," Proc. of the 1985 Symposium on Security and Privacy, April 1985, Oakland, CA.

[2] H. Ong, C. P. Schnorr, and A. Shamir, "An Efficient Signature Scheme Based on Quadratic Equations," Proc. 16th ACM Symp. Theor. Computing (1984), 208-216.

[3] J. M. Pollard, "Solution of $x^2 - ky^2 \equiv m \pmod{n}$," Private communication with C. P. Schnorr, June 29, 1984.

[4] H. Ong, C. P. Schnorr, and A. Shamir, "Efficient Signature Schemes Based on Polynomial Equations," to appear in Crypto'84, Lecture Notes in Computer Science, Springer-Verlag, NY (1984).

[5] D. Estes, L. Adleman, K. Kompella, K. McCurley, G. Miller, "Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields," to appear.