An M^3 Public-Key Encryption Scheme

H.C. Williams*
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
CANADA R3T 2N2

1. Introduction. It is well known that the RSA public-key cryptosystem can be broken if the composite modulus can be factored. It is not known, however, whether the problem of breaking any RSA system is equivalent in difficulty to factoring the modulus. In 1979 Rabin [5] introduced a public-key cryptosystem which is as difficult to break as it is to factor a modulus $R = p_1p_2$, where p_1, p_2 are two distinct large primes. Essentially Rabin suggested that the designer of such a scheme first determine p_1 and p_2, keep them secret and make R public. Anyone wishing to send a secure message M $(0 < M < R)$ to the designer would encrypt M as K, where

$$K \equiv M^2 \pmod{R}$$

and $0 < K < R$, then transmit K to the designer.

The designer can determine M from K by solving the congruences

$$x^2 \equiv K \pmod{p_1}$$
$$(1.1)\quad y^2 \equiv K \pmod{p_2}$$

for x and y. Since $M \equiv \pm x \pmod{p_1}$ and $M \equiv \pm y \pmod{p_2}$, by using the Chinese Remainder Theorem he can deduce four different possibilities for M. If M has some kind of internal redundancy, it should be possible to select the correct M from among the four candidates.

There are two difficulties with this scheme.

(i) Although there are $O(\log p)$ probabilistic methods for solving the quadratic congruence (see §5)

$$x^2 \equiv M \pmod{p}$$

when p is a prime, the solution of (1.1) and the subsequent use of the Chinese Remainder Theorem can still be quite time consuming.

(ii) The 4:1 ambiguity in the decrypted messages can be a problem, especially if (as is often the case in transmitting keys) internal redundancy in M is to be minimized.

Indeed, Rabin only advocated his technique as a signature scheme and not as an encryption technique. He also pointed out that, if we insist that $p_1 \equiv p_2 \equiv 1 \pmod{3}$, then we can replace the $K \equiv M^2 \pmod{k}$ step by $K \equiv M^3 \pmod{R}$ and also get a scheme as difficult to break as it is to factor R. However, in this case we get a 9:1 ambiguity in the decrypted messages.

* Research supported by NSERC of Canada Grant A7649.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 358-368, 1986.

In [10] Williams showed how a scheme like Rabin's could be developed in which problems (i) and (ii) could be eliminated. This technique made use of the following theorem.

Theorem 1.1 If $p_1 \equiv p_2 \equiv -1 \pmod 4$, $R = p_1 p_2$, and the Jacobi symbol $(X/R) = 1$. For some X, then

$$X^{(p_1 - 1)(p_2 - 1)/4} \equiv \pm 1 \pmod R. \quad \square$$

Corollary. If $K \equiv X^2 \pmod R$ and $(X/R) = 1$, then,

$$K^d \equiv \pm X \pmod R,$$

where $d = ((p_1 - 1)(p_2 - 1)/4 + 1)/2$.

In this scheme the designer determines R and d and a small S such that $(S/R) = -1$. (In [10] R was calculated in such a way that $S = 2$.) He makes R and S public and keeps d secret. Anyone wishing to send a secure message M to the designer

(1) determines b_1 (= 0 or 1) such that $(M/R) = (-1)^{b_1}$;

(2) puts

$$M_0 \equiv S^{b_1} M \pmod R,$$

where $0 < M_0 < R$, and computes b_2 (= 0 or 1) such that $b_2 \equiv M_0 \pmod 2$;

(3) computes

(1.2) $$K \equiv M_0^2 \pmod R,$$

where $$0 < K < R;$$

(4) and then transmits $L = \{K, b_1, b_2\}$.

To decrypt L the designer

(1) finds $$N \equiv K^d \pmod R,$$

where $0 < N < R$;

(2) puts $N_0 = R - N$ or N, whichever is even;

(3) and computes

$$M \equiv S^{-b_1}(-1)^{b_1} N_0 \pmod R$$

where $0 < M < R$.

This scheme, like Rabin's, is as difficult to break as it is to factor R. Actually, the scheme presented here differs from that given in [10] in two respects. First, it is more general in that it allows for the utilization of an arbitrary S such that $(S/R) = -1$ instead of restricting S to 2. Also in [10] the designer could include a value of e such that $\gcd(e, \phi(R)) = 1$ in his public key $\{R, S, e\}$. This allows for the combination of the above idea with that of the RSA technique. This is easily done by replacing (1.2) above by

$$K \equiv M_0^{2e} \pmod R.$$

Of course, the designer must now evaluate his value for d by solving the

linear congruence

$$de \equiv ((p_1 - 1)(p_2 - 1)/4 + 1)/2 \pmod{\phi(R)}.$$

The use of this e values (especially if e is fairly large) will frustrate attacks like those mentioned by Lipton in [1].

The purpose of this paper is to show how this same idea can be extended to the M^3 scheme suggested by Rabin. We first point out that in order to develop our previous cryptosystem it was necessary that we

I. have the Jacobi symbol and (in order that the scheme be useable) be able to determine the symbol rapidity, i.e. in $O(\log R)$ steps;

II. have Theorem 1.1;

III. and have a method for the designer to identify the actual message which was sent (decryption steps (2) and (3)).

Our strategy for extending our idea, then, will be to extend each of I., II., and III.).

2. Arithmetic in $Q(\rho)$. Let $\mathbb{Z}$ denote the set of all rational integers and let ρ be a primitive cube root of unity, that is $\rho^2 + \rho + 1 = 0$. Let $K = Q(\rho)$ be the algebraic number field formed by adjoining ρ to the rationals Q. In this section we will review several of the well-known results concerning K and then develop a theorem analogous to Theorem 1.1.

We first denote by $\mathcal{O}_K$ the set

$$\mathcal{O}_K = \{a + b\rho \mid a,b \in \mathbb{Z}\}.$$

$\mathcal{O}_K$ is the set of all algebraic integers in K. If $\alpha \in \mathcal{O}_K$, then $\alpha = a + b\rho$ for some $a,b \in \mathbb{Z}$ and the norm of α, $N(\alpha)$, is $\alpha\bar{\alpha}$ where $\bar{\alpha} = a + b\rho^2$. Thus $N(\alpha) = a^2 - ab + b^2$.

The primes in $\mathcal{O}_K$ are given by

(i) $1 - \rho$;

(ii) p, where p is a prime in $\mathbb{Z}$ and $p \equiv -1 \pmod 3$;

(iii) $a + b\rho$, where $a \equiv -1 \pmod 3$, $3 \mid b$, and $N(a + b\rho) = p$, where p is a prime in $\mathbb{Z}$ and $p \equiv 1 \pmod 3$.

Since $\mathcal{O}_K$ is a unique factorization domain, for any $\beta \in \mathcal{O}_K$, we have

$$\beta = \eta \prod_{i=1}^{t} \pi_i^{\kappa_i}, \tag{2.1}$$

where the π_i $(i = 1,2, \ldots, t)$ are primes of $\mathcal{O}_K$ and $\eta \in \{1,-1,\rho,-\rho\}$. Also, this expression for β is unique (up to order of the π_i's).

We also have

Theorem 2.1 If $\alpha \in \mathcal{O}_K$ and π is a prime of $\mathcal{O}_K$, then

$$\alpha^{(N(\pi) - 1)/3} \equiv \rho^{\lambda} \pmod{\pi},$$

where $\lambda \in \{0,1,2\}$. □

If, with Jacobi, we define the symbol $[\alpha/\pi]$ to be the value of ρ^{λ} in Theorem 2.1, we can get an extended Jacobi symbol by defining $[\alpha/\beta]$ as

$$[\alpha/\beta] = \prod_{i=1}^{t} [\alpha/\pi_i]^{\kappa_i},$$

when β has the prime power decomposition given by (2.1).

Let $p_1 \equiv p_2 \equiv 1 \pmod 3$ be two distinct primes in $\mathbb{Z}$, $R = p_1 p_2$, and let π_1, π_2 be primes of $\mathcal{O}_K$ such that $N(\pi_1) = p_1$ and $N(\pi_2) = p_2$. Such π_1 and π_2 always exist and in Algorithm 1 of section 5 we describe an expeditious method for finding them. If $\pi_1 = a_1 + b_1\rho$ and $\pi_2 = a_2 + b_2\rho$, $(a_1, b_1, a_2, b_2 \in \mathbb{Z})$, then

$$\pi_1\pi_2 = A + B\rho,$$

where $A = a_1a_2 - b_1b_2$, $B = b_1a_2 - b_2a_1 - b_1b_2$ and $\gcd(B,R) = 1$.
Compute $C \in \mathbb{Z}$ by

$$C \equiv -AB^{-1} \pmod{R}.$$

Note that since

$$R = p_1p_2 = N(\pi_1\pi_2) = A^2 - AB + B^2,$$

we have

$$C^2 + C + 1 \equiv 0 \pmod{R} \text{ and } C^3 \equiv 1 \pmod{R};$$

indeed,

$$C \equiv \rho \pmod{\pi_1\pi_2}.$$

We can now prove a result analogous to Theorem 1.1.

Theorem 2.2 If $(p_1 - 1)(p_2 - 1)/9 \equiv -1 \pmod 3$ and $[X/\pi_1\pi_2] = 1$ for some $X \in \mathbb{Z}$, then

$$X^{(p_1 - 1)(p_2 - 1)/9} \equiv C^{\lambda} \pmod{R}$$

where $\lambda \in \{0,1,2\}$.

Proof. Let $\rho^{\kappa} = [X/\pi_1]$ $(\kappa \in \{0,1,2\})$.
Since $[X/\pi_1\pi_2] = 1$, we must have $[X/\pi_2] = \rho^{3 - \kappa}$.

Now $$\kappa(p_1 - 1)(p_2 - 1)/9 \equiv -\kappa \pmod 3;$$

hence,

$$\kappa(p_1 - 1)/3 \equiv (3 - \kappa)(p_2 - 1)/3 \pmod 3. \tag{2.2}$$

We have $$X^{(p_1 - 1)/3} \equiv \rho^{\kappa} \pmod{\pi_1}$$

and $$X^{(p_2 - 1)/3} \equiv \rho^{3 - \kappa} \pmod{\pi_2};$$

thus, if $\lambda \equiv \kappa(p_2 - 1)/3 \pmod 3$ $(\lambda \in \{0,1,2\})$, then from (2.2) we see that

$$X^{(p_1 - 1)(p_2 - 1)/9} \equiv \rho^{\lambda} \pmod{\pi_1}$$

and

$$X^{(p_1 - 1)(p_2 - 1)/9} \equiv \rho^{\lambda} \pmod{\pi_2}.$$

It follows that

$$X^{(p_1 - 1)(p_2 - 1)/9} \equiv \rho^{\lambda} \equiv C^{\lambda} \pmod{\pi_1\pi_2}.$$

and

$$X^{(p_1 - 1)(p_2 - 1)/9} \equiv C^{\lambda} \pmod{R}. \quad \square$$

Corollary. If π_1 and π_2 are defined as above, $K \equiv X^3 \pmod R$ and $[X/\pi_1\pi_2] = 1$, then

$$K^d \equiv C^{\lambda}X \pmod R,$$

where $\lambda \in \{0,1,2\}$ and $d = ((p_1 - 1)(p_2 - 1)/9 + 1)/3$.

3. The M^3 Scheme. In our M^3 scheme the designer selects two large distinct primes p_1, p_2 such that $p_1 \equiv p_2 \equiv 1 \pmod 3$ and $(p_1 - 1)(p_2 - 1)/9 \equiv -1 \pmod 3$. He then determines a_1, a_2, b_1, b_2, A, B, C, d as described in §2. He also selects (by trial) a value for $S \in \mathbb{Z}$ such that $[S/\pi_1\pi_2] = \rho$ and evaluates $S^{-1} \pmod R$. He makes his encryption key $\{A,B,S\}$ public. Since $R = A^2 - AB + B^2$, the key occupies the same amount of space as that needed by our M^2 scheme.

To encrypt a message M $(0 < M < R)$ the sender executes the following steps.

(1) Evaluate the extended Jacobi symbol $[M/A + B\rho] = \rho^{b_1}$, where $b_1 \in \{0,1,2\}$.

(2) Determine

$$M_0 \equiv MS^{2b_1}, \quad M_1 \equiv CM_0 \pmod R,$$

where $0 < M_0, M_1 < R$. Put $M_2 = R - M_0 - M_1$. Since $M_0 + M_1 + M_2 = R \equiv 1 \pmod 3$, one of M_0, M_1, M_2 is distinct modulo 3 from the other two. If this is M_i, put $b_2 = i$.

(3) Compute

(3.1) $$K \equiv M_0^3 \pmod R,$$

where $0 < K < R$.

(4) Transmit $E(M) = L = \{K, b_1, b_2\}$.

To decrypt the message L, the designer must perform the following steps.

(1) Determine

$$N \equiv K^d \pmod R,$$

where $0 < N < R$.

(2) Calculate

$$N_0 = N, \quad N_1 \equiv CN_0 \pmod R \ (0 < N_1 < R), \quad N_2 = R - N_1 - N_0.$$

Let N_j be that one of N_0, N_1, N_2 which is distinct modulo 3 from the other two.

(3) Compute

$$D(L) \equiv S^{-b_1} C^{2b_2} N_j \pmod{R},$$

where $0 < D(L) < R$.

That $D(L) = D(E(M)) = M$ follows easily from the corollary of Theorem 2.2 and the simple fact that $C^2 + C + 1 \equiv 0 \pmod{R}$. Hence $\{N_0, N_1, N_2\} = \{M_0, M_1, M_2\}$ and $N_j = M_i \equiv C^i M_0 \pmod{R}$. If, as in the case disccused in §1, we wish to add a value of e such that $\gcd(e,\phi(R)) = 1$ to the encryption key, we can do so easily by replacing (3.1) by

$$K \equiv M_0^{3e} \pmod{R}.$$

Also, d must now be a solution of the linear congruence

$$de \equiv ((p_1 - 1)(p_2 - 1)/9 + 1)/3 \pmod{\phi(R)}.$$

There is, of course, one problem here that we have not discussed and that is the method of computing $[M/A + B\rho]$ rapidly and without knowing how to factor $A + B\rho$. In §5 we describe an $O(\log R)$ algorithm for doing this.

We conclude this section by pointing out that this idea can also be used to produce signatures in much the same manner as that used in [10]; further, our encryption scheme is an example of a claw-free permutation (see Goldwasser et al. [2]).

4. Security. In this section we will show that it is as difficult to break this system as it is to factor R in $\mathbb{Z}$. This problem is equivalent in difficulty to the problem of factoring $A + B\rho$ in O_K. We first require three lemmas.

Lemma 4.1. Let $K \equiv Y^3 \pmod{R}$ for some $Y \in \mathbb{Z}$. For any $i \in \{0,1,2\}$ there exists an $X \in \mathbb{Z}$ such that

$$X^3 \equiv K \pmod{R} \text{ and } [X/\pi_1\pi_2] = \rho^i [Y/\pi_1\pi_2].$$

Proof. Let $j, k \in \{0,1,2\}$ such that

$$j - k \equiv i(p_1 - 1)/3 \pmod{3}.$$

Since

$$(p_1 - 1)(p_2 - 1)/9 \equiv -1 \pmod{3},$$

we must have

$$i \equiv j(p_1 - 1)/3 + k(p_2 - 1)/3 \pmod{3}. \tag{4.1}$$

If we use the Chinese Remainder Theorem to find X such that

$$X \equiv C^j Y \pmod{p_1}$$
$$X \equiv C^k Y \pmod{p_2},$$

then

$$X^3 \equiv Y^3 \equiv K \pmod{R}$$

and

$$\begin{aligned}[X/\pi_1\pi_2] &= [C/\pi_1]^j [C/\pi_2]^k [Y/\pi_1\pi_2] \\ &= [\rho/\pi_1]^j [\rho/\pi_2]^k [Y/\pi_1\pi_2] \\ &= \rho^i [Y/\pi_1\pi_2]\end{aligned}$$

by (4.1).

Lemma 4.2 For any $Y \in \mathbb{Z}$ such that $\gcd(Y,R) = 1$ and any $b_1, b_2 \in \{0,1,2\}$ there exists a unique $M \in \mathbb{Z}$ $(0 < M < R)$ such that for the encryption key $\{A,B,S,e\}$ we have

$$E(M) = \{K,b_1,b_2\},$$

where $K \equiv Y^3 \pmod R$ and $0 < K < R$.

Proof. Let

$$fe \equiv 1 \pmod{\phi(R)}$$

and put

$$T \equiv Y^{3f} \pmod R.$$

By Lemma 4.1 there must exist $X \in \mathbb{Z}$ such that $X^3 \equiv T \pmod R$ and $[X/\pi_1\pi_2] = 1$. Define $X_i \equiv C^iX \pmod R$, where $0 < X_i < R$, $i = 0,1,2$, and let X_j be that one of X_0,X_1,X_2 which is distinct modulo 3 from the other two. Set

$$k \equiv 2(b_2 - j) \pmod 3,\ k \in \{0,1,2\}$$

and put

$$M \equiv S^{-2b_1}C^kX \pmod R,$$

where $0 < M < R$.

Now

$$[M/\pi_1\pi_2] = [S/\pi_1\pi_2]^{-2b_1} = \rho^{b_1}$$

$$([C/\pi_1\pi_2] = \rho^{(p_1 - 1) + (p_2 - 1)/3} = 1)$$

also,

$$M_i \equiv C^iS^{2b_1}M \equiv C^hX \pmod R,$$

where $h = 2(b_2 - j) + i$ and $0 < M_i < R$. Hence, we get $\{M_0,M_1,M_2\} = \{X_0,X_1,X_2\}$ and when $i = b_2$, then

$$M_i \equiv C^jX \pmod R.$$

It follows that $M_i = X_j$ and M_i is distinct modulo 3 from the other two M_m values when $i = b_2$. Also

$$M_0^{3e} \equiv X^{3e} \equiv T^e \equiv Y^{3ef} \equiv Y^3 \equiv K \pmod R.$$

Hence $E(M) = \{K,b_1,b_2\}$. Since $D(E(M)) = M$, M must also be unique. □

Lemma 4.3 If $X, Y \in \mathbb{Z}$, $X^3 \equiv Y^3 \pmod R$, and $[X/\pi_1\pi_2] \neq [Y/\pi_1\pi_2]$, then $\gcd(X - C^iY,R) = p_1$ for some $i \in \{0,1,2\}$.

Proof. Since $X^3 \equiv Y^3 \pmod R$, we have

$$(X - Y)(X - CY)(X - C^2Y) \equiv 0 \pmod{p_1p_2}.$$

If $p_1p_2 \mid X - C^iY$, then

$$[X/\pi_1\pi_2] = [C^iY/\pi_1\pi_2]_2 = [Y/\pi_1\pi_2],$$

which is not so. Thus, there must exist some $X - C^iY$ with $i \in \{0,1,2\}$ such that $p_1 \mid X - C^iY$ and $p_2 \nmid X - C^iY$. It follows that $\gcd(X - C^iY,R) = p_1$. □

Now suppose that we have some algorithm F which we will decrypt $1/k$ of all messages. If an arbitrary Y is selected such that $[Y/\pi_1\pi_2] \neq 1$ and $\gcd(Y,R) = 1$ (Note that S is a possible value of Y.), then put $K \equiv Y^3 \pmod R$

with $0 < K < R$ and select any $b_1, b_2 \in \{0,1,2\}$. By Lemma 4.2 there exists a unique M such that

$$E(M) = \{K, b_1, b_2\}.$$

After k trials at a value for Y we would expect that F would determine the corresponding M from $\{K, b_1, b_2\}$. Putting $M_0 \equiv MS^{2b_1} \pmod R$ and $X \equiv M_0^e \pmod R$, we have

$$X^3 \equiv Y^3 \pmod R$$

and

$$1 = [X/\pi_1\pi_2] \neq [Y/\pi_1\pi_2].$$

It follows from Lemma 4.3 that with knowledge of M and Y, we can easily factor R.

It might be felt that, in revealing the values of A and B, the designer in some way aids his opponent to factor $R = A^2 - AB + B^2$. For example, if his opponent were able to find G,H such that $G \neq \pm A, \pm B, \pm(A - B)$ and $R = G^2 - GH + H^2$, then he could factor R by using his knowledge of A,B,G,H. We point out, however, that if we are given C such that $C^2 + C + 1 \equiv 0 \pmod R$, then $(2C + 1)^2 \equiv -3 \pmod R$ and it can be shown that by using Algorithm 1 we can compute A and B such that

$$R = A^2 + AB + B^2$$

in $O(\log R)$ operations. Thus, knowledge of C is equivalent to the knowledge of A and B. Now $C^3 \equiv 1 \pmod R$ and if we could find X such that $X^3 \equiv 1 \pmod R$ and $[X/\pi_1\pi_2] \neq 1$, we could factor K. But this is really no different from taking an arbitrary Y, determining $K \equiv Y^3 \pmod R$ and then finding some X such that $X^3 \equiv K$ and $[X/\pi_1\pi_2] \neq [Y/\pi_1\pi_2]$, a problem equivalent in difficulty to factoring R. That is, unless there is something special sbout a value of $K = 1$, knowledge of C seems, for the problem of factoring R, to give no more information than the knowledge of an arbitrary Y.

We should, nevertheless, emphasize here that the method of showing the equivalence of breaking our system to the problem of factoring R is constructive; that is, this encryption technique is vulnerable to a known cipher text attack, if such an attack can be mounted. We refer the reader to the relevant comments in [10] concerning this.

The problem of extending our method further to an M^r encryption scheme, where r is a prime and $p_1 \equiv p_2 \equiv 1 \pmod r$ is rather difficult. In the first place, it is necessary to be able to further extend the Jacobi symbol and be able to evaluate it in $O(\log R)$ time. This would mean, as far as is known today, that the cyclotomic extension of the rationals $K_r = Q(\rho)$, where ρ is a primitive r^{th} root of unity, must be Euclidean. As K_r can be Euclidean only when the class number of K_r is 1, this means that r could only be 2, 3, 5, 7, 11, 13, 17, 19. Of these it is known that if $r = 2, 3, 5, 7, 11$, then K_r is Euclidean. The other values 13, 17, 19 have not

been investigated (see Lenstra [4]). While it may, in principle, be possible to extend the algorithms in §5 to the cases of $4 = 5, 7, 11$, the details would be very onerous and the corresponding computations would be concomitantly slowed. Possibly, the case of $r = 5$ might be worthwhile investigating.

5. Algorithms. In this section we describe two algorithms. The first of these is a method of determining a and b, given m and x such that $x^2 \equiv -3 \pmod m$, for which

$$m = a^2 - ab + b^2.$$

If m is a prime we can find x in $O(\log m)$ operations by using either the algorithm described by Lehmer [3] or that of Shanks [7]. This often requires that we know in advance a quadratic non-residue of m. There is no $O(\log m)$ deterministic way known for doing this, but in practice one finds such a non-residue by trial very easily. An $O(\log m)$ deterministic method for finding x when m is prime has been given recently by Schoof [6], but as Schoof himself says, no one would ever use this very complicated technique.

The algorithm we present here is a simple adaptation of the method described by Wilker [8] to solve $u^2 + 5v^2 = m$. There is no loss of generality in assuming m is not a perfect square and $m \equiv 1 \pmod 3$.

Algorithm 1. (Find s,t such that $m = s^2 + 3t^2$ when $m \equiv 1 \pmod 3$.)

(1) Use the Euclidean algorithm to find $r_0, r_1, r_2, \ldots$, where

$$\begin{aligned} x &= q_0 m + r_0 && 0 < r_0 < m \\ m &= q_1 r_0 + r_1 && 0 < r_1 < r_0 \\ r_0 &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\ &\text{- - - - - - -} && \text{- - - - - -} \end{aligned}$$

If $r_0^2 < m$, then $m = r_0^2 + 3$ and we are done. If $r_0^2 > m$, then find r_n such that

$$r_{n-1}^2 > m \quad \text{and} \quad r_n^2 < m.$$

Only $O(\log m)$ operations are needed to do this.

(2) Put $s = \pm r_n$. When $3 \mid r_{n-1}$ and $r_{n-1}^2 < 9m$, put $t = +r_{n-1}/3$; otherwise, put $t = \pm(r_n - k)$, where

$$k \equiv ((3r_n\varepsilon_{n-1} - \varepsilon_n\varepsilon_{n-1}r_n - 2r_{n-1})/6 \pmod{r_n}.$$

Here $0 < k < r_n$, $r_i \equiv \varepsilon_i \pmod 3$, and $|\varepsilon_i| \le 1$.

We have $m = s^2 + 3t^2 = (s + t)^2 - 2t(s + t) + 4t^2$.

If m is a prime p and we want a prime $\pi = a + b\omega$ such that $N(\pi) = p$, then we select the sign of s such that $a = s + t \equiv -1 \pmod 3$ and put $b = -2t$ when $3 \mid t$. If $3 \nmid t$, we select the sign of t such that $a = 2t \equiv -1 \pmod 3$ and put $b = s + t$.

The next algorithm we present is one which can be used to evaluate the extended Jacobi symbol $[\alpha/\beta]$ without requiring the factorization of β. This algorithm was undoubtedly known to Jacobi and is given in Williams and Holte [9]. We assume that $\alpha = A + B\rho$, $\beta = C + D\rho$. Here the symbols A,B,C,D do not have the meanings assigned to them previously but merely denote rational integers such that $3 \nmid D$ and $3 \mid D$.

Algorithm 2. (Determine g and γ such that $[\alpha/\beta] = \rho^g[\beta/\gamma]$ and $N(\gamma) < N(\beta)$).

(1) Find $E = A - xC + yD$, $F = B - yC - xD + yD$, where

$$x = Ne\{(AC + BD - AD)/N(\beta)\},$$

$$y = Ne\{(BC - AD)/N(\beta)\},$$

$N(\beta) = C^2 - CD + D^2$, $Ne\{\alpha\}$ denotes the nearest integer to α.

(2) If $E \equiv -F \pmod 3$, divide $E + F\rho$ by $1 - \rho$ k times until $(E + F\rho)/(1 - \rho)^k = \overline{E} + \overline{F}\rho$ and $\overline{E} \not\equiv -\overline{F} \pmod 3$. This process is facilitated by making use of the observation that if $E = -F + 3Q$, then

$$(E + F\rho)/(1 - \rho) = 2Q - F + Q\rho.$$

(3) If $3 \mid \overline{F}$, put $j = 0$, $G = \overline{E}$, $H = \overline{F}$; if $3 \mid \overline{E}$, put $j = 1$, $G = \overline{F} - \overline{E}$, $H = -\overline{E}$; if $3 \nmid \overline{FE}$, put $j = 2$, $G = -\overline{F}$, $H = \overline{E} - \overline{F}$. Then $\gamma = G + H\rho$ and $g \equiv (2k + j)(C^2 - 1)/3 - jCD/3 \pmod 3$.

We have $[\alpha/\beta] = \rho^g[\beta/\gamma]$ and $N(\gamma) < 3/4\ N(\beta)$. Clearly we can repeat this algorithm until we get a symbol of the form $[\pm 1/\lambda] = 1$; the accumulated power of ρ will then be the value of $[\alpha/\beta]$. Since $N(\gamma) < 3/4\ N(\beta)$, we see that this algorithm must terminate in $O(\log N(\beta))$ operations.

REFERENCES

[1] R.A. Demillo, G.I. Davida, D.P. Dobkin, M.A. Harrison, and R.J. Lipton, **On the Safety of Cryptosystems**, Applied Cryptology, Cryptographic Protocols and Computer Security Models, AMS Short Courses Lecture Notes, Vol. 29, Providence, 1983.

[2] Shafi Goldwasser, Silvio Micali, R.L. Rivest, **A "paradoxical" solution to the signature problem**, Proc. 25th IEEE Symposium on Foundations of Computer Science, to appear.

[3] D.H. Lehmer, **Computer technology applied to the theory of numbers**, Studies in Number Theory, Math. Assoc. of America, 1969, Theorem 5, p. 133.

[4] H.W. Lenstra, jr., **Euclidean number fields I.**, Math. Intelligencer 2 (1979/80), 6 - 15.

[5] M.O. Rabin, ***Digitized signatures and public-key functions as intractable as factorization***, M.I.T. Lab. for Computer Science, Tech. Rep. LCS/TR212, 1979.

[6] Rene Schoof, **Elliptic curves over finite fields and the computation of square roots mod p**, Math. Comp. 44 (1985), 483 - 494.

[7] D. Shanks, **Five number theoretic algorithms**, Congressus Numerantium 7 (1973), 51 - 69.

[8] Peter Wilker, **An effecient algorithmic solution of the diophantine equation** $u^2 + 5v^2 = m$, Math. Comp. 35 (1980), 1347 - 1352.

[9] H.C. Williams and R. Holte, **Computation of the solution of** $x^3 + Dy^3 = 1$, Math. Comp. 31 (1977), 778 - 785.

[10] H.C. Williams, **A modification of the RSA public-key enryption procedure**, IEEE Transactions on Information Theory, IT-26 (1980), 726 - 729.