An Efficient Digital Signature Scheme Based on an Elliptic Curve over the Ring Z_n

Tatsuaki Okamoto Atsushi Fujioka Eiichiro Fujisaki

NTT Laboratories
Nippon Telegraph and Telephone Corporation
1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan

Abstract. We propose a practical digital signature scheme based on the elliptic curve modulo n, where $n = p^2q$ such that p and q are large secret primes. The signature generation speed of our scheme is more than 10 times faster than that of the RSA scheme. Moreover, a pre-processing technique can significantly increase the signature generation speed.

1 Introduction

The use of *Digital signatures* is being increasingly demanded to ensure the integrity and authenticity of digital messages and documents. Applications include electronic mail, office automation, and electronic funds transfer.

Many digital signature schemes have been developed since Diffie and Hellman's seminal paper on public key cryptosystems [DH] was presented in 1976. Among these schemes, the RSA scheme [RSA] appears to be very promising from the practical viewpoint. However, the RSA scheme has the disadvantage of low processing speed, and is somewhat insecure against low multiplier attacks [Ha] and attacks using the homomorphic property [EH]. Although effective countermeasures are known against these attacks, the existence of these attacks may imply some implicit weaknesses in the RSA scheme.

The security of the RSA scheme can be increased with the scheme based on an elliptic curve over a ring Z_n [KMOV]. This variant (the KMOV scheme) seems to be more secure than the original RSA scheme against some attacks such as low multiplier attacks, although it is less efficient.

In this paper, we propose a new digital signature scheme based on an elliptic curve over a ring Z_n, that is more efficient than the RSA scheme as well as the KMOV scheme. We construct the new scheme on an elliptic curve over a ring using the idea of Okamoto's scheme [Ok]. The new scheme seems to be more secure than Okamoto's scheme against low degree attacks (or lattice attacks) and seems to be more secure than the RSA scheme against the homomorphic attacks. That is, our scheme with parameter $k = 2$, the double version, seems to be secure, while Okamoto's scheme with $k = 2$, the quadratic version, has been broken [BD, VGT]. Our scheme has no homomorphic property since the relationship between a message and its signature is randomized (or our signature is verified by an inequality not by an equation), so no homomorphic attack seems to apply to our scheme. This implies a possibility that our scheme may still be

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 54-65, 1993.

secure even if security weaknesses in Okamoto's or RSA scheme are found in the future.

The pre-processing technique (off-line processing) is possible with our scheme, as is true for Okamoto's scheme and DSA proposed by NIST as DSS (the Digital Signature Standard) [NIST]. This dramatically increases the signature generation (on-line processing) speed of our scheme. Thus, signature generation with our scheme is effectively instantaneous even if implemented on a smart card.

2 Notations

Z_n denotes the set of numbers between 0 and $n-1$, and Z_n^* denotes the set of numbers between 0 and $n-1$ which are relatively prime to n. $\lceil M \rceil$ denotes the least integer which is larger than or equal to M. $x \equiv y \pmod{n}$ denotes that n divides $x-y$. $f(x) \bmod n$ denotes an integer such that n divides $f(x) - (f(x) \bmod n)$ and $f(x) \bmod n \in Z_n$. $x/y \bmod n$ denotes an integer such that n divides $x - y(x/y \bmod n)$ and $x/y \bmod n \in Z_n$. $|X|$ denotes $\lfloor \log_2 X \rfloor + 1$, or the bit size of X.

3 Elliptic Curves over a Field and a Ring

Assume that K is the finite prime field $GF(p)$ with $p \neq 2,\ 3$. An elliptic curve over K (in affine coordinates), denoted by $\mathcal{C}_p$, is the set of all solutions $(x, y) \in K \times K$ to the equation

$$\mathcal{C}_p \ : \ y^2 \equiv x^3 + ax + b \mod p, \tag{1}$$

where $a,\ b \in K$, and $4a^3 + 27b^2 \not\equiv 0 \mod p$, together with a special point O, called the point at infinity. Here, the group law operation [Kol] (usually we call it the addition, and use the notation $+$) is defined over the points on $\mathcal{C}_p$, $P(x_1, y_1), Q(x_2, y_2)$, and $R(x_3, y_3)$ as follows:

- $P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) \end{cases} \quad \text{over } Z_p \tag{2}$$

- $2P(x_1, y_1) = R(x_3, y_3)$

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) \end{cases} \quad \text{over } Z_p \tag{3}$$

Let p and q be primes and $n = p^2 q$. Consider an elliptic curve modulo n: $\mathcal{C}_n$. The addition operation on $\mathcal{C}_n$ is analogous to the usual one over $GF(p)$, although $\mathcal{C}_n$ is not a group.

4 Okamoto's Digital Signature Scheme

4.1 Procedures

- *Keys:*
  - *Secret key:* large prime numbers p, q $(p > q)$.
  - *Public key:* a positive integer $n = p^2 q$.
- *Signature generation:*
  - The signature s of a message m is computed by the originator as follows:
    - Pick a random number $t \in Z_{pq}^*$.
    - Compute s such that

$$w = \left\lfloor \frac{h(m) - (t^k \bmod n)}{pq} \right\rfloor,$$

$$u = w/(kt^{k-1}) \bmod p,$$

$$s = t + upq,$$

    where h is a one-way hash function ($h(m) \in Z_n$ for any positive integer m), k is an integer ($4 \leq k$).
- *Signature verification:*
  - The signature message (s, m) is considered valid if the following verification inequality holds.

$$h(m) \leq s^k \bmod n < h(m) + 2^{2\cdot|n|/3}.$$

5 Proposed Digital Signature Scheme Based on Elliptic Curves over a Ring

Before describing our new proposed scheme, we introduce two extensions of Okamoto's scheme. The first one is the extension of the function type; from the *polynomial function* to the *rational function*. The other extension is the number of variables; from the *one variable function* to the *multi-variable function*.

5.1 Mathematical Preparations

The Taylor series expansion and the generalized Taylor series expansion for a multi-variable function are essential to prove the correctness of our schemes.

Proposition 1. (The Taylor expansion)
When function f is a one-variable infinitely differentiable function,

$$f(a + x) = f(a) + f^{(1)}(a)x + \frac{f^{(2)}(a)}{2}x^2 + \cdots + \frac{f^{(l)}(a)}{l!}x^l + \cdots,$$

where a is not a singular point, x is less than the convergence radii, and $f^{(l)}$ denotes l-th derived function of f.

Proposition 2. (The generalized Taylor expansion)
When function f is a t-variable infinitely differentiable function,

$$f(a_1+x_1, a_2+x_2, \ldots, a_t+x_t) =$$
$$f(a_1, a_2, \ldots, a_t) + (x_1\frac{\partial}{\partial x_1} + \cdots + x_t\frac{\partial}{\partial x_t})f(a_1, a_2, \ldots, a_t) +$$
$$\cdots + \frac{1}{l!}(x_1\frac{\partial}{\partial x_1} + \cdots + x_t\frac{\partial}{\partial x_t})^l f(a_1, a_2, \ldots, a_t) + \cdots,$$

where $(a_1, a_2, \ldots, a_t)$ is not a singular point, $(x_1, x_2, \ldots, x_t)$ is less than the convergence radii, and $(x_1\frac{\partial}{\partial x_1} + \cdots + x_t\frac{\partial}{\partial x_t})^l f(a_1, a_2, \ldots, a_t)$ denotes the value at $(a_1, a_2, \ldots, a_t)$ of $(x_1\frac{\partial}{\partial x_1} + \cdots + x_t\frac{\partial}{\partial x_t})^l f(x_1, x_2, \ldots, x_t)$.

5.2 Extension Using a Rational Function

In this section, we show an extension of Okamoto's scheme, in which a *rational* function f is used in place of the polynomial function.

5.2.1 Procedures

- *Keys:*
  - *Secret key:* large prime numbers p, q $(p > q)$.
  - *Public key:* a positive integer $n = p^2q$.
    a *rational* function f.
- *Signature generation:*
  - The signature s of a message m is computed by an originator as follows:
    * Pick a random number $t \in Z_{pq}^*$. If one of the following cases occurs, pick another random number $t \in Z_{pq}^*$: (1) $f(t) \bmod p = \infty$, (2) $f(t) \bmod q = \infty$, (3) $f(t) \bmod p = 0$, (4) $f(t) \bmod q = 0$, (5) $f'(t) \bmod p = 0$. Here, f is a rational function, or there exist polynomial functions, a and b, satisfying $f = a/b$. f' is the derived function of f, or $f'(x) = \frac{df(x)}{dx}$. Note that this check is not necessary in practice, since these cases occur with negligible probability.
    * Compute s such that

$$w = \left\lceil \frac{h(m) - (f(t) \bmod n)}{pq} \right\rceil,$$
$$u = w/f'(t) \bmod p,$$
$$s = t + upq.$$

      Here, h is a one-way hash function ($h(m) \in Z_n$ for any positive integer m). Functions h and f can be fixed in the system.
- *Signature verification:*
  - The signature message (s, m) is considered valid if the following verification inequality holds.

$$h(m) \leq f(s) \bmod n < h(m) + 2^{2|n|/3}.$$

5.2.2 Correctness

Theorem 3. *Let $0 \leq h(m) < n - pq$, and s be the signature of m, which is generated through the above-described procedure. Then,*

$$h(m) \leq f(s) \bmod n < h(m) + pq.$$

Proof. First, let $\tilde{f}(x) \equiv f(x) \pmod{n}$ for all $x \in \boldsymbol{Z}_n$ and all singular points of $\tilde{f}(x)$ do not lie in the interval $[0, n)$. For any rational function $f(x)$, $\tilde{f}(x)$ always exists. This is because: Let $a_i \in [0, n)$ $(i = 1, \ldots, k)$ be the singular points of $f(x)$. Then $f(x) = \frac{c(x)}{(x-a_1)(x-a_2)\cdots(x-a_k)b(x)}$. Let $\tilde{f}(x) = \frac{c(x)}{(x-\tilde{a}_1)(x-\tilde{a}_2)\cdots(x-\tilde{a}_k)b(x)}$, where $\tilde{a}_i = a_i + n$ $(i = 1, \ldots, k)$. Then, $\tilde{f}(x)$ satisfies the above conditions.

Since $\tilde{f}(x)$ is an analytic function and there exists no singular point in interval $[0, n)$, the Taylor expansion of $\tilde{f}(t + v)$ around t converges for any $t \in [0, n)$ and $t + v \in [0, n)$. That is,

$$\tilde{f}(t + v) = \tilde{f}(t) + \tilde{f}^{(1)}(t)v + \frac{\tilde{f}^{(2)}(t)}{2}v^2 + \cdots + \frac{\tilde{f}^{(l)}(t)}{l!}v^l + \cdots,$$

for any $t \in [0, n)$ and $t + v \in [0, n)$. Hence,

$$\begin{aligned}\tilde{f}(t + upq) \bmod n &= \tilde{f}(t) + \tilde{f}^{(1)}(t)upq + (upq)^2\left(\frac{\tilde{f}^{(2)}(t)}{2} + \cdots\right) \bmod n \\ &= \tilde{f}(t) + \tilde{f}^{(1)}(t)upq \bmod n,\end{aligned}$$

for any $t \in \boldsymbol{Z}_n$ and $t + upq \in \boldsymbol{Z}_n$. From the definition of $\tilde{f}(x)$, $\tilde{f}(t + upq) \bmod n = f(t + upq) \bmod n$. Therefore,

$$f(t + upq) \bmod n = f(t) + f^{(1)}(t)upq \bmod n.$$

Furthermore from the equation $w = f^{(1)}(t)u \bmod p$, we have

$$f(t + upq) \bmod n = f(t) + wpq \bmod n.$$

On the other hand, from the definition $w = \left\lceil \frac{h(m) - (f(t) \bmod n)}{pq} \right\rceil$, we obtain

$$wpq = h(m) - (f(t) \bmod n) + \gamma,$$

where $0 \leq \gamma < pq$. Therefore we have the following equation:

$$f(t + upq) \bmod n = f(t) + h(m) - (f(t) \bmod n) + \gamma \bmod n = h(m) + \gamma \bmod n.$$

Since $0 \leq h(m) < n - pq$,

$$h(m) \leq h(m) + \gamma \bmod n = h(m) + \gamma < h(m) + pq.$$

Hence we obtain

$$h(m) \leq f(s) \bmod n < h(m) + pq,$$

where $s = t + upq$.

□

5.3 Extension Using a Multi-Variable Function

In this section, we present another extension of Okamoto's scheme, in which a *multi-variable* rational function f takes the place of the single-variable function.

5.3.1 Procedures

Let f_j $(j = 1, \ldots, J)$ be an I-variable rational function and $\boldsymbol{f}$ denote $(f_1, \ldots, f_J)$. Let $\boldsymbol{x} = (x_1, \ldots, x_I)$, $\boldsymbol{y} = (y_1, \ldots, y_J)$, where $x_i \in Z_n$ $(i = 1, \ldots, I)$, and $y_j \in Z_n$ $(j = 1, \ldots, J)$. We write $\boldsymbol{y} = \boldsymbol{f}(\boldsymbol{x})$ as $y_j = f_j(x_1, \ldots, x_I)$ $(j = 1, \ldots, J)$.

In this subsection, we show a signature scheme that uses $\boldsymbol{f}$ only once. However, by repeating the following procedure, we can easily construct a signature scheme based on a more complicated multi-variable rational function. In the next section, we will show an example in which the basic procedure is repeatedly executed.

For explanation simplicity, we suppose that $I = J$.

- *Keys:*
  - *Secret key:* large prime numbers p, q $(p > q)$.
  - *Public key:* a positive integer $n = p^2 q$.
    a *multi-variable* function $\boldsymbol{f}$.
- *Signature generation:*
  - The signature $\boldsymbol{s} = (s_1, \ldots, s_I)$ $(s_i \in Z_n^*;\ i = 1, \ldots, I)$ of a message m is computed by originator A as follows:
    * Pick a random number vector $\boldsymbol{t} = (t_1, \ldots, t_I)$ $(t_i \in Z_{pq}^*; i = 1, \ldots, I)$. If one of the following cases occurs, pick another random number vector $\boldsymbol{t}$: for $j \in \{1, \ldots, I\}$, (1) $f_j(\boldsymbol{t}) \bmod p = \infty$, (2) $f_j(\boldsymbol{t}) \bmod q = \infty$, (3) $f_j(\boldsymbol{t}) \bmod p = 0$, (4) $f_j(\boldsymbol{t}) \bmod q = 0$, (5) $I \times I$ matrix $\Delta \boldsymbol{f}(\boldsymbol{t}) \bmod p$ is not regular. Here, f_j is a I-variable rational function, and
$$\Delta \boldsymbol{f}(\boldsymbol{t}) \bmod p = \begin{pmatrix} \frac{\partial f_1(\boldsymbol{t})}{\partial x_1} & \cdots & \frac{\partial f_1(\boldsymbol{t})}{\partial x_I} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_I(\boldsymbol{t})}{\partial x_1} & \cdots & \frac{\partial f_I(\boldsymbol{t})}{\partial x_I} \end{pmatrix} \bmod p.$$
      Note that this check is not necessary in practice, since these cases occur with negligible probability.
    * Compute $\boldsymbol{s}$ such that
$$(m_1, \ldots, m_I) = h(m), \quad (m_j \in Z_n; j = 1, \ldots, I)$$
$$w_j = \left\lceil \frac{m_j - (f_j(\boldsymbol{t}) \bmod n)}{pq} \right\rceil, \ (j = 1, \ldots, I)$$
$$\begin{pmatrix} u_1 \\ \vdots \\ u_I \end{pmatrix} = \begin{pmatrix} \frac{\partial f_1(\boldsymbol{t})}{\partial x_1} & \cdots & \frac{\partial f_1(\boldsymbol{t})}{\partial x_I} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_I(\boldsymbol{t})}{\partial x_1} & \cdots & \frac{\partial f_I(\boldsymbol{t})}{\partial x_I} \end{pmatrix}^{-1} \begin{pmatrix} w_1 \\ \vdots \\ w_I \end{pmatrix} \bmod p$$

$$s_i = t_i + u_i pq \quad (i = 1, \ldots, I)$$

$$\boldsymbol{s} = (s_1, \ldots, s_I)$$

Here, h is a one-way hash function. Functions h and $\boldsymbol{f}$ can be fixed in the system.

- *Signature verification:*
  - The signature message $(\boldsymbol{s}, m)$ is considered valid if the following verification inequality holds for all $j = 1, \ldots, I$,

$$m_j \leq f_j(\boldsymbol{s}) \bmod n < m_j + 2^{2|n|/3},$$

where $(m_1, \ldots, m_I) = h(m)$.

5.3.2 Correctness

Theorem 4. *Let $0 \leq m_j < n - pq$ for all $j = 1, \ldots, I$, and $\boldsymbol{s}$ be the signature of m, which is generated through the above-described procedure. Then,*

$$m_j \leq f_j(\boldsymbol{s}) \bmod n < m_j + pq.$$

This theorem can be proven in a manner similar to Theorem 3, using the generalized Taylor expansion.

5.4 A New scheme Based on Elliptic Curve over Z_n

This section introduces our new scheme based on an elliptic curve over Z_n. The correctness of the scheme is given as a combined specific example of two previous extensions of Okamoto's scheme; the new scheme is the *two-variable rational* function version.

5.4.1 Elliptic Curve and Some Definitions

We consider an elliptic curve $\mathcal{C}_n$:

$$y^2 = x^3 + ax + b \quad \text{over } Z_n.$$

As described in Section 3, the addition operation is defined over the points on $\mathcal{C}_n$, $P(x_1, y_1)$, $Q(x_2, y_2)$, and $R(x_3, y_3)$, by equations (2) and (3) over Z_n.

Here, let $\boldsymbol{f} = (f_x, f_y)$, $\boldsymbol{g} = (g_x, g_y)$ such that

$$\begin{cases} f_x(x_1, y_1) = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ f_y(x_1, y_1) = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - f_x(x, y)) \end{cases}$$

$$\begin{cases} g_x(x_1, y_1, x_2, y_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ g_y(x_1, y_1, x_2, y_2) = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - g_x(x_1, y_1, x_2, y_2)) \end{cases}$$

Then we can express

$$2P = \boldsymbol{f}(P) \bmod n,$$

$$P + Q = \boldsymbol{g}(P, Q) \bmod n.$$

Therefore, for an integer k, we can calculate $R = kP$ over $\boldsymbol{Z}_n$ by using an addition chain corresponding to k, where P and R are points on C_n.

Let

$$\Delta \boldsymbol{f} = \begin{pmatrix} \frac{\partial f_x}{\partial x} & \frac{\partial f_x}{\partial y} \\ \frac{\partial f_y}{\partial x} & \frac{\partial f_y}{\partial y} \end{pmatrix},$$

$$\Delta \boldsymbol{g} = \begin{pmatrix} \frac{\partial g_x}{\partial x_1} & \frac{\partial g_x}{\partial y_1} & \frac{\partial g_x}{\partial x_2} & \frac{\partial g_x}{\partial y_2} \\ \frac{\partial g_y}{\partial x_1} & \frac{\partial g_y}{\partial y_1} & \frac{\partial g_y}{\partial x_2} & \frac{\partial g_y}{\partial y_2} \end{pmatrix}.$$

Next, let $A = (A_1, A_2)$, $B = (B_1, B_2)$, $C = (C_1, C_2)$ such that

$$A_1 = (a_x, a_y),\ B_1 = (b_x, b_y),\ C_1 = (c_x, c_y),$$

$$A_2 = \begin{pmatrix} a_{11}\ a_{12} \\ a_{21}\ a_{22} \end{pmatrix},\quad B_2 = \begin{pmatrix} b_{11}\ b_{12} \\ b_{21}\ b_{22} \end{pmatrix},\quad C_2 = \begin{pmatrix} c_{11}\ c_{12} \\ c_{21}\ c_{22} \end{pmatrix},$$

where $a_x, a_y, b_x, b_y, c_x, c_y \in \boldsymbol{Z}_n^*$, and $a_{ij}, b_{ij}, c_{ij} \in \boldsymbol{Z}_p^*$ $(i, j \in \{1, 2\})$.

Definition 5. (Functions F and G)
Let F be a function such that $F(A) = (C_1, C_2)$, where

$$C_1 = \boldsymbol{f}(A_1) \bmod n, \text{ and } C_2 = \Delta \boldsymbol{f}(A_1) \cdot A_2 \bmod p.$$

Let G be another function such that $G(A, B) = (C_1, C_2)$, where

$$C_1 = \boldsymbol{g}(A_1, B_1) \bmod n, \text{ and } C_2 = \Delta \boldsymbol{g}(A_1, B_1) \cdot [A_2, B_2] \bmod p,$$

where $[A_2, B_2]$ denotes the 4×2 matrix in which i-th (1st and 2nd) row of A_2 is the i-th (1st and 2nd) row and the i-th (1st and 2nd) row of B_2 is the $(i+2)$-nd (3rd and 4th) row.

5.4.2 Procedures

- *Keys:*
  - *Secret key:* large prime numbers p, q $(p > q)$.
  - *Public key:* a positive integer $n = p^2 q$.
    a parameter (of the curve) a.
- *Signature generation:*
  - Signature $S = (s_x, s_y)$ of a message m is computed by the originator as follows:

* Pick a random number vector $T = (t_x, t_y)$ $(t_x, t_y \in Z_{pq}^*)$. If one of the following cases occurs during executing the following signature generation procedure, return to this stage and pick another random number vector t: for $i \in \{x, y\}$, (1) $(kT \text{ over } Z_n)_i \bmod p = \infty$, (2) $(kT \text{ over } Z_n)_i \bmod q = \infty$, (3) $(kT \text{ over } Z_n)_i \bmod p = 0$, (4) $(kT \text{ over } Z_n)_i \bmod q = 0$, (5) 2×2 matrix $D(T) \bmod p$ is not regular, where kT over Z_n means k times point of T by the addition formula on C_n, and $(\cdot)_x$ (or $(\cdot)_y$) means the x-coordinate (or y-coordinate) of point $(\cdot)$. (Note that the calculation, kT over Z_n, here is formally executed by the addition formula, and that T is not necessary to be on C_n.) Note that this check is not necessary in practice, since these cases occur with negligible probability.
* Compute S such that

$$M = (m_x, m_y) = h(m), \quad (m_x, m_y \in Z_n)$$

where, h is a one-way hash function$(m_x, m_y \in Z_n)$.

$$w_x = \left\lceil \frac{m_x - (kT \text{ over } Z_n)_x}{pq} \right\rceil,$$

$$w_y = \left\lceil \frac{m_y - (kT \text{ over } Z_n)_y}{pq} \right\rceil.$$

Next 2×2 matrix $D(T, k)$ is computed from T and k by Algorithm D below. Then

$$\begin{pmatrix} u_x \\ u_y \end{pmatrix} = D(T,k)^{-1} \begin{pmatrix} w_x \\ w_y \end{pmatrix} \bmod p$$

$$s_i = t_i + u_i pq \quad (i = x, y)$$

$$S = (s_x, s_y)$$

Integer k and functions h can be fixed in the system. Note that the parameter a in the public key can be fixed in the system. Therefore the real public key for each user is considered to be an only n.
* Note that kT over Z_n and $D(T,k)^{-1}$ can be computed as preprocessing works since they are independent of a message m.

Algorithm D

Input: T, k

Output: 2×2 matrix $D(T,k)$, whose element is in Z_p^*.

Step 1: Set $A = (A_1, A_2)$ such that

$$A_1 \leftarrow T, \quad A_2 \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Set $l \leftarrow 1$ and $t \leftarrow 0$.
The bit expression of k is "$b_L b_{L-1} \cdots b_1$."
(The initial setting for $B = (B_1, B_2)$ is not necessary, since the value of B is set in Step 2.)

Step 2: If $b_l = 1$ and $t = 0$, then $B \leftarrow A$ and $t \leftarrow 1$.
If $b_l = 1$ and $t = 1$, then $B \leftarrow G(A, B)$.
Step 3: If $l = L$, then output B_2 as $D(T, k)$.
Otherwise $l \leftarrow l + 1$, and $A \leftarrow F(A)$.
Return to Step 2.

Note that the value of B_1 that corresponds to the output value of B_2 or $D(T, k)$ is equivalent to kT over $\boldsymbol{Z}_n$.

- *Signature verification:*
  - The signature message (S, m) is considered valid if the following verification inequalities hold

$$m_x \leq (kS \text{ over } \boldsymbol{Z}_n)_x < m_x + 2^{2|n|/3},$$

$$m_y \leq (kS \text{ over } \boldsymbol{Z}_n)_y < m_y + 2^{2|n|/3},$$

where $(m_x, m_y) = h(m)$. Note that the first parameter a of $\mathcal{C}_n$ is fixed and given for the calculation kS over $\boldsymbol{Z}_n$, but that the other parameter b of $\mathcal{C}_n$ is not necessary for the calculation and is determined by the value $S = (s_x, s_y)$ such that

$$b = s_y^2 - s_x^3 - as_x \text{ over } \boldsymbol{Z}_n.$$

6 Security Consideration

The security of our scheme depends on the difficulty of factoring $n = p^2q$. Although it has not been proven that our scheme is as secure as factoring, our scheme seems to be more secure than Okamoto's scheme, against which no attack is known so far when its degree is greater than three. The quadratic version of Okamoto's scheme was broken by Brickell et.al. [BD], and this attack was generalized by Vallée et.al. [VGT] using the lattice algorithm. Their attacks essentially use and generalize the approximation property that $\left\lceil \sqrt{N} \right\rceil^2 - N = O(N^{1/2}) < O(N^{2/3})$. However, this approximation technique does not appear applicable to our scheme even if it is the double version ($k = 2$), since the rational function mod n is essentially used in our scheme. Although it is not clear that factoring $n = p^2q$ is as hard as factoring $n = pq$, no attack has been reported so far, that is specifically effective for a number with the square of a prime.

7 Performance

We have estimated the amount of work needed to generate a signature with our scheme and compare it with that of the RSA scheme. We assume that $n(= p^2q)$ is 96 bytes and $k = 2$ for our scheme, and $n'(= p'q')$ is 64 bytes for RSA.

Signature generation with the new scheme requires 4 modulo-n multiplications, 1 modulo-n division, 17 modulo-p multiplications, and 1 modulo-p division.

So, in total, it is almost equivalent to $(4 + 17/9) + (1 + 1/9)c$ modulo-n multiplications, which is less than $(6 + 1.2c)$ modulo-n multiplications. Here, c is the ratio of the amount of work for modulo-n division to that for modulo-n multiplication, and is considered to be less than 10 from our implementation data based on algorithm L (p.329) in [Kn]. The RSA scheme requires 750 modulo-n' multiplications.

As the computational complexity of one modulo-n multiplication is almost equivalent to that of 2.25 ($=1.5^2$) modulo-n' multiplications, signature generation with our scheme is considered to require less than 40 modulo-n' multiplications.

The signature generation speed of our new scheme is more than 10 times faster than that of the RSA scheme. If the Chinese Remainder Theorem technique is applied to the RSA scheme, the amount of work is theoretically reduced by 75%, while the work of our scheme is reduced by about 50%. In addition, the m-ary exponentiation and Montgomery arithmetic techniques can reduce the amount of work needed by the RSA scheme, however, they can also applied to our scheme. Therefore our new scheme is still at least several times faster than the RSA scheme.

Moreover, the pre-processing technique (off-line processing) is possible with our scheme, as is true for Okamoto's scheme [FOM] and DSA. In the pre-processing phase, some computations that do not depend on the message are executed. This dramatically increases the signature generation (on-line processing) speed of our scheme. Thus, signature generation with our scheme is effectively instantaneous even if implemented on a smart card, since the amount of work needed for signature generation is less than one modulo-n multiplication.

8 Conclusion

We have proposed a new practical digital signature scheme based on elliptic curves over a ring. To construct this scheme, we introduced two extensions of Okamoto's scheme. The signature generation speed of our scheme is more than 10 times faster than that of the RSA scheme. Moreover, a pre-processing technique can significantly increase the signature generation speed.

References

[BD] E. Brickell and J. DeLaurentis, "An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi", *Advances in Cryptology — CRYPTO'85*, Lecture Notes in Computer Science No.218, Springer-Verlag, pp.28–32 (1986).

[DH] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol.IT-22, No.6, pp.644–654 (Nov., 1976).

[EH] J. Evertse and E. van Heyst, "Which New RSA Signatures can be Computed from some Given RSA Signatures?", *Advances in Cryptology — EUROCRYPT'90*, Lecture Notes in Computer Science No.473, Springer-Verlag, pp.83–97 (1991).

[FOM] A. Fujioka, T. Okamoto, and S. Miyaguchi, "ESIGN: An Efficient Digital Signature Implementation for Smart Cards", *Advances in Cryptology — EUROCRYPT'91*, Lecture Notes in Computer Science No.547, Springer-Verlag, pp.446–457 (1991).

[Ha] J. Hastad, "On Using RSA with Low Exponent in a Public Key Network", *Advances in Cryptology — CRYPTO'85*, Lecture Notes in Computer Science No.218, Springer-Verlag, pp.403–408 (1985).

[Ka] B. S. Kaliski, Jr., "A Pseudo-Random Bit Generator Based on Elliptic Logarithms", *Advances in Cryptology — CRYPTO'86*, Lecture Notes in Computer Science No.263, Springer-Verlag, pp.84–103 (1986).

[KMOV] K. Koyama, U. Maurer, T. Okamoto, and S. A. Vanstone, "New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n", *Advances in Cryptology — CRYPTO'91*, Lecture Notes in Computer Science No.576, Springer-Verlag, pp.252–266 (1992).

[Kn] D. E. Knuth, *The Art of Computer Programming*, 2nd Edition, Addison-Wesley Publishing Company (1981).

[Ko1] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag (1987).

[Ko2] N. Koblitz, "Constructing Elliptic Curve Cryptosystems in Characteristics 2", *Advances in Cryptology — CRYPTO'90*, Lecture Notes in Computer Science No.537, Springer-Verlag, pp.156–167 (1991).

[NIST] National Institute for Standards and Technology, "Specifications for a Digital Signature Standard", *Federal Information Processing Standard Publication XX*, draft (Aug., 1991).

[Ok] T. Okamoto, "A Fast Signature Scheme Based on Congruential Polynomial Operations", *IEEE Transactions on Information Theory*, Vol.IT-36, No.1, pp.47–53 (Jan., 1990).

[RSA] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Vol.21, No.2, pp.120–126 (Feb., 1978).

[VGT] B. Vallée, M. Girault, and P. Toffin, "How to Break Okamoto's Cryptosystem by Reducing Lattice Bases", *Advances in Cryptology — Eurocrypt'88*, Lecture Notes in Computer Science No.330, Springer-Verlag, pp.281–292 (1988).