PAPER Special Section on Cryptography and Information Security

Elliptic Curves Suitable for Cryptosystems

Atsuko MIYAJI †, *Member*

SUMMARY Koblitz ([5]) and Miller ([6]) proposed a method by which the group of points on an elliptic curve over a finite field can be used for the public key cryptosystems instead of a finite field. To realize signature or identification schemes by a smart card, we need less data size stored in a smart card and less computation amount by it. In this paper, we show how to construct such elliptic curves while keeping security high.
key words: *public-key, elliptic curves, smart card*

1. Introduction

Public key cryptosystems based on the discrete logarithm problem on an elliptic curve (EDLP) can offer small key length cryptosystems. If an elliptic curve is chosen to avoid the Menezes-Okamoto-Vanstone reduction ([9]), then the only known attacks on EDLP are the Pollard ρ−method ([11]) and the Pohlig-Hellman method ([10]). So up to the present, such elliptic curve cryptosystems on E/F_q are secure if $\#E(F_q)$ is divisible by a prime only more than 30 digits ([3]).

If we use an elliptic curve E/F_q for digital signature or identification by a smart card ([12]), stored data size, computation amount for signature generation and public key size should be as small as possible. In order to reduce public key size, we may publish only the x-coordinate $x(P)$ of a public key P and one bit necessary to recover the y-coordinate $y(P)$ of P, instead of publishing P whose size is double of the definition field F_q. But it will cause the computation amount to recover $y(P)$.

In this paper, we investigate an elliptic curve suitable for cryptosystems, in the sense that it requires less data size and less computation, while maintaining the security. We also show the advantage of our elliptic curve in the case of the Schnorr's digital signature scheme on an elliptic curve.

This paper is organized as follows. Section 2 summarizes the addition formula of an elliptic curve ([13]). Section 3 describes the Schnorr signature on an elliptic curve, and show the data size and the computation amount for two cases, the basic version and the reducing-data version. Section 4 discusses the elliptic curve which gives cryptosystems that reduce both of data sizes and the computation amount.

Manuscript received August 1, 1993.
Manuscript revised September 10, 1993.
†The author is with Matsushita Electric Industrial Co., Ltd., Kadoma-shi, 571 Japan.

2. Addition Formula of Elliptic Curve

Cryptosystems on an elliptic curve E/F_q, for example the Diffie-Hellman key distribution and ElGamal cryptosystems, require the computation of kP ($P \in E(F_q)$). We will discuss the computation amount of kP. For simplicity, we neglect addition, subtraction and multiplication by a small constant in F_q because they are much faster than multiplication and division in F_q.

Let K be a finite field F_q of characteristic $\neq 2, 3$. An elliptic curve over K is given as follows,

$$E : y^2 = x^3 + ax + b \ \ (a, b \in K, 4a^3 + 27b^2 \neq 0).$$

Then the set of K-rational points on E (with a special element $\mathcal{O}$ at infinity), denoted $E(K)$, is a finite abelian group, where

$$E(K) = \{(x, y) \in K^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

For the curve E, the addition formulas in the affine coordinate are the following. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P + Q = (x_3, y_3)$ be points on $E(K)$.

• Curve addition formula in affine coordinates ($P \neq \pm Q$)

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \\ \lambda &= \frac{y_2 - y_1}{x_2 - x_1}; \end{aligned} \tag{1}$$

• Curve doubling formula in affine coordinates ($P = Q$)

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \\ \lambda &= \frac{3x_1^2 + a}{2y_1}. \end{aligned} \tag{2}$$

The formula (1) requires two multiplications and one division in K, while the formula (2) requires three multiplications and one division in K. The computation amount of division in K is more than that of multiplication in K. So we often use the projective coordinates to avoid divisions in K. The addition formulas in the projective coordinates are the following. Let $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$ and

$P+Q=(X_3,Y_3,Z_3)$.

• **Curve addition formula in projective coordinates ($P \neq \pm Q$)**

$$\begin{aligned} X_3 &= vA, \\ Y_3 &= u(v^2X_1Z_2 - A) - v^3Y_1Z_2, \\ Z_3 &= v^3Z_1Z_2, \end{aligned} \tag{3}$$

where $u = Y_2Z_1 - Y_1Z_2, v = X_2Z_1 - X_1Z_2, t = X_2Z_1 + X_1Z_2, A = u^2Z_1Z_2 - v^2t$;

• **Curve doubling formula in projective coordinates ($P = Q$)**

$$\begin{aligned} X_3 &= 2hs, \\ Y_3 &= w(4B-h) - 8{Y_1}^2s^2, \\ Z_3 &= 8s^3, \end{aligned} \tag{4}$$

where $w = a{Z_1}^2 + 3{X_1}^2, s = Y_1Z_1, B = X_1Y_1s, h = w^2 - 8B$. The formula (3) requires 15 multiplications, while the formula (4) requires 12 multiplications. For the use of cryptosystems, we may set $z(P) = Z_1$ to one in the formula (3). Then the formula (3) requires 12 multiplications.

Subtractions are as expensive as additions over elliptic curves. So the computation amount of kP by the addition-subtraction method ([2],[8]) is less than that by the binary method, while both methods need memory storage only for P. We assume to compute kP by the addition-subtraction method. Then the computation requires n times of curve doubling and $\frac{n}{3}$ times of curve adding on the average, where $n = |K|$. Computation of kP in the projective coordinate requires one division and two multiplications in the final stage. As long as the ratio of the computation amount of division in K to that of multiplication in K is larger than 9, the computations in the projective coordinates are faster than that in the affine coordinates for n equal to 100 or more. Here we assume to compute kP in the projective coordinate by the addition-subtraction method and compute the power residue by the binary method in order to compare the computation amount of Schnorr signature scheme on a finite field and on an elliptic curve.

3. Elliptic Curve Cryptosystems

If $E(K)$ and a basepoint $P \in E(K)$ are carefully chosen, then the only known attacks on the cryptosystems are the square root attacks. EDLP on such E to the base P is secure up to the present ([3]), if the order of P, $ord(P)$, is divisible by more than a 30-digit prime. Here we summarize the Schnorr signature on such an elliptic curve and establish a basis for evaluation of the elliptic curve proposed in the next chapter.

Let $M \in \mathbb{Z}$ be a message. User A sends the message M to user B with her or his signature of M.

- Initialization
  - system parameter
    - $E: y^2 = x^3 + ax + b$ $(a, b \in F_p$; p is a prime of $n(\geqq 97)$ bits).
    - $P \in E(F_p)$: a basepoint (chosen as the above).
    - $l = ord(P)$ (l is $m(\geqq 97)$ bits).
  - a one-way hash function

    $$h : \mathbb{Z}_l \times \mathbb{Z} \to \{0, \cdots, 2^t - 1\},$$

    where t is the security parameter.

- Key generation
  User A randomly chooses an integer s , a secret key, and makes public the point $P_A = -sP$ as a public key.

- Signature generation

  1 Pick a random number $k \in \{1, ..., l\}$ and compute

  $$R = kP = (r_x, r_y). \tag{5}$$

  Here $r_x = x(R)$ and $r_y = y(R)$.

  2 Compute $e := h(r_x, M) \in \{0, \cdots, 2^t - 1\}$.

  3 Compute $y \equiv k + se \pmod{l}$ and output the signature (e, y).

- Signature verification

  1 Compute $\overline{R} = yP + eP_A = (\overline{r_x}, \overline{r_y})$ and check that $e = h(\overline{r_x}, M)$.

As we described in Sect. 2, the computation of kP requires m curve doublings and $\frac{m}{3}$ curve additions on the average, where k is a m-bit number. Extending the addition-subtraction method to the computation in the verification, we can calculate $yP + eP_A$ in m curve doublings and $\frac{1}{3}(m-t) + \frac{5}{9}t$ curve additions on the average with precomputations of $\pm(P \pm P_A)$, which require about the same computation amount as one curve addition.

Here we set $n, m = 128$. Then the known attack on such an elliptic curve cryptosystem requires at least 2^{64} elliptic curve operations. This is roughly equal to that of the original Schnorr on F_p (p is 512 bits), since the known attack on the original Schnorr requires $O(\exp\sqrt{\log p \log\log p})$ finite field operations. If lower security is allowed, then n, m can be replaced by a smaller number like 97. For the security parameter, here we set $t = 128$. Of course if we use EC versions for identification, we can set $t \geqq 20$.

We will present two versions of Schnorr signature on an elliptic curve. One is the basic Schnorr signature on an elliptic curve described above, called Basic EC version. Another is called Reducing data EC version.

Table 1 Comparison of data size (in bits).

	System Key	Secret Key	Public Key	Signature size
Basic EC version	640	128	256	256
Reducing data EC version	641	128	129	256
Finite field version	1164	140	512	268

Table 2 Comparison of computation amount (in # of 512-bit modular multiplications).

	Signature Generation	Signature Verification
Basic EC version	129	151
Reducing data EC version	141	175
Finite field version	210	242

In this version, only $x(P_A)$ and the least significant bit of $y(P_A)$ are published as a public key to reduce the data size. The same is done for the basepoint P. On the other hand, the original Schnorr signature scheme on F_p, called Finite field version (p is 512 bits, the security parameter $t = 128$) roughly has the same security as that on the above elliptic curves. So the size of the definition field of Finite field version is four times as large as that of Basic and Reducing data EC versions.

We compare Basic EC version, Reducing data EC version and Finite field version, with respect to data size. Table 1 shows the comparison.

• **Basic EC version**

The system key is a, p, P, and l (640 bits). The secret key is s (128 bits). They are stored in a smart card. So the data size stored in a smart card is 768 bits. The public key is (P_A) (256 bits) and the signature is e and y (256 bits).

• **Reducing data EC version**

In this version, we have to publish one more parameter "b" of E as a system key to recover a point by the x-coordinate of the point and the least significant bit of the y-coordinate of the point. It requires power residue to recover the y-coordinate of P and increases computation for signature. The system key is a, b, p, $x(P)$, the least significant bit of $y(P)$ and l (641 bits). The secret key is s (128 bits). So the data size stored in a smart card is 769 bits. It is almost equal to that of Basic EC version. The public key is $x(P_A)$ and the least significant bit of $y(P_A)$ (129 bits) and the signature is e and y (256 bits).

• **Finite field version**

The system key of Finite field version is a set of the definition field, the basepoint and the order of basepoint (1164 bits), where the size of the definition field is 512 bits and the order of basepoint is 140 bits. The secret key is 140 bits. So the data size stored in a smart card is 1304 bits.

The size of the definition fields of both EC versions is reduced to 25% of Finite field version. But the stored data size is not so much reduced (59%). This is because an elliptic curve point has 2 coordinates and we need a parameter to decide E.

Let us compare the three cases with respect to the computation amount. We assume the computation method that we described in Sect. 2. Table 2 shows the comparison of the computation amount of signature generation and verification. Here we assume $m(n) = (n/t)^2 m(t)$, where $m(n)$ denotes the amount of work to perform one modular multiplication whose modulus size is n bits. We assume the ratio of the computation amount of division in K to that of multiplication in K to 10. We see the computation amount of signature generation of Reducing data EC version is reduced to 67% of Finite field version. It is not so reduced as the size of the definition field. This is because the computation amount of one elliptic curve addition is much more than that of one multiplication in the same definition field and we need 195m(128) to recover a basepoint.

We see that both EC versions seem to be better than Finite field version for both points of the data size and the computation amount. But actually they are not so efficient considering the less size of the definition field of E. For the stored data size, the ratio of the stored data size to the definition field for both EC versions is 6. On the other hand, for Finite field version, the ratio is 2.5. For the computation amount, one elliptic curve addition requires about 12 multiplications. If we require higher security, for example $t = 160$, then we will have to construct an elliptic curve over at least a 160-bit finite field. Then the advantage for EC versions shown in Table 1 and 2 decreases.

In the next section, we construct an elliptic curve cryptosystem, which has

(1) the less ratio of the stored data size to the definition field than 6;

(2) the same public key size as Reducing data EC version;

(3) the less computation amount than that of Basic EC version.

It will be also best implementation for the higher secu-

Table 3 Integers d and j-invariant j_d.

d	j_d
3	0
11	$(-2^5)^3$
19	$(-2^5 * 3)^3$
43	$(-2^6 * 3 * 5)^3$
67	$(-2^5 * 3 * 5 * 11)^3$
163	$(-2^6 * 3 * 5 * 23 * 29)^3$

rity parameter.

4. Elliptic Curves Suitable for Cryptosystems

If $E(F_p)$ and the basepoint $P \in E(F_p)$ are appropriately chosen, then the only known attacks on the cryptosystems are the square root attacks. We first discuss a method to construct such elliptic curves and then investigate what elliptic curve among them is suitable for implementation with respect to less data size (key length) and less computation amount.

4.1 Decision of the Class of Elliptic Curves

One method to avoid the recent attack is to construct EDLP on E/F_p with p elements ([7]). We describe a modified method to decide the class of such elliptic curves. There are two phases for the decision of E/F_p with p elements.

The first phase is to find an appropriate prime p. Such p is a form of $p = db^2+db+\frac{d+1}{4}$ for an integer b and $d \equiv 3 \pmod 4$, where d is not divisible by any square of a prime. Here we use $d \in \{3, 11, 19, 43, 67, 163\}$. Such integers d enable us to construct easily the j-invariant j_d of E/F_p with p elements for the prime p, which is uniquely determined by d. For more information on this, we refer the reader to [7]. Table 3 lists integers d and the j-invariant j_d.

Once the prime $p = db^2+db+\frac{d+1}{4}$ and j_d are given, then the next phase is to decide the class of E/F_p with p elements. There is a little difference between the case of $d = 3$ and others. First we investigate the case of $d \in \{11, 19, 43, 67, 163\}$. Then the elliptic curves over F_p with the j-invariant j_d are given as follows.

$$E_{c,d} : y^2 = x^3 + 3c^2 a_d x + 2c^3 a_d, \tag{6}$$

where $a_d = \frac{j_d}{1728-j_d}$ and c is any element in F_p^*. For each d, we can classify $\{E_{c,d} | c \in F_p^*\}$ into two equivalence classes of twists, namely

$$\mathcal{E}_d = \{E_{c,d} | c \in F_p^*, \left(\frac{c}{p}\right) = 1\}$$

and

$$\mathcal{E}'_d = \{E_{c,d} | c \in F_p^*, \left(\frac{c}{p}\right) = -1\},$$

Table 4 Integers d and α_d.

d	α_d
11	$3 * 7$
19	3
43	$2 * 5 * 7$
67	$3 * 5 * 7 * 11 * 31$
163	$2 * 3 * 5 * 7 * 11 * 19 * 23 * 29 * 127$

where $\left(\frac{c}{p}\right)$ denotes the Legendre symbol. Then only one of the two classes gives the elliptic curves with p elements. A general condition to decide the class was described ([1]). In our case, the condition can be simplified as follows.

Theorem 1: Let p be a prime represented by $p = db^2 + db + \frac{d+1}{4}$ (b is an integer) for $d \in \{11, 19, 43, 67, 163\}$. Then the class which gives elliptic curves with p elements is determined as:

$$\mathcal{E}_d \text{ if } \left(\frac{\alpha_d}{p}\right) = -1,$$

$$\mathcal{E}'_d \text{ if } \left(\frac{\alpha_d}{p}\right) = 1,$$

where α_d is an integer determined by d. Table 4 shows the values of α_d.

Now we get the following procedure to decide the class of elliptic curves with p elements.

Procedure 1

1 Search a large prime p such that $p = db^2 + db + \frac{d+1}{4}$ (b is an integer) for $d \in \{11, 19, 43, 67, 163\}$.

2 Calculate $\left(\frac{\alpha_d}{p}\right)$. If $\left(\frac{\alpha_d}{p}\right) = -1$, then $\mathcal{E}_d$ is the class. Else if $\left(\frac{\alpha_d}{p}\right) = 1$, then $\mathcal{E}'_d$ is the class.

Next we will investigate the case of $d = 3$. Then the elliptic curves over F_p ($p = 3b^2 + 3b + 1$) with the j-invariant j_d are given as follows.

$$E_\xi : y^2 = x^3 + \xi \ (\forall \xi \in F_p^*). \tag{7}$$

In this case, we can classify $\{E_\xi | \xi \in F_p^*\}$ into six equivalence classes of twists, namely

$$\mathcal{E}_{3,i} = \{E_\xi | \xi \in F_p^*, \left(\frac{\xi}{p}\right)_6 = (-\omega)^i\} \ (0 \leq i \leq 5),$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$ and $\left(\frac{\xi}{p}\right)_6$ denotes the sixth power residue symbol. Then exactly one of the six classes gives the elliptic curves with p elements. We have a next formula on the number of rational points of the elliptic curves (7).

Theorem 2: ([4]) Let $p \equiv 1 \pmod 3$ and $p = \pi\overline{\pi}$ with $\mathbb{Z}[\omega] \ni \pi \equiv 2 \pmod 3$. Then

$$\#E_\xi(F_p) = p + 1 + \left(\frac{\overline{4\xi}}{\pi}\right)_6 \pi + \left(\frac{4\xi}{\pi}\right)_6 \overline{\pi}. \quad (8)$$

Using the formula (8), the condition to decide the class can be given as follows.

Theorem 3: Let p be a prime represented by $p = 3b^2 + 3b + 1$ (b is an integer). Then the class which gives elliptic curves with p elements is determined as:

$\mathcal{E}_{3,1}$ if $b \equiv 0, 2, 4 \pmod 6$,

$\mathcal{E}_{3,5}$ if $b \equiv 1, 3, 5 \pmod 6$.

Proof: We prove only the case of $b \equiv 1 \pmod 6$. As for the other cases, we can do the same way. Let $\pi = (2b+1)\omega + (b+1)$. Then $p = \pi\overline{\pi}$ and $\pi \equiv 2 \pmod 3$. Since $\left(\frac{4}{\pi}\right)_6 = \omega$, we get that $\#E_\xi(F_p) = p$ if and only if

$$\left(\frac{\overline{\xi}}{\pi}\right)_6 \omega^2\pi + \left(\frac{\xi}{\pi}\right)_6 \omega\overline{\pi} = -1,$$

that is, $tr(\omega\left(\frac{\xi}{\pi}\right)_6 \overline{\pi}) = -1$. So we get $\left(\frac{\xi}{\pi}\right)_6 = -\omega^2$. This means that the class which gives elliptic curves with p elements is $\mathcal{E}_{3,5}$. □

Now we get the following procedure to decide the class of elliptic curves with p elements.

Procedure 2

1 Search a large prime p such that $p = 3b^2 + 3b + 1$ (b is an integer).

2 If $b \equiv 0, 2, 4 \pmod 6$, then $\mathcal{E}_{3,1}$ is the class. Else if $b \equiv 1, 3, 5 \pmod 6$, then $\mathcal{E}_{3,5}$ is the class.

We have seen that the time to decide the class of E/F_p with p elements depends on the time finding $p = db^2 + db + \frac{d+1}{4}$ for $d \in \{3, 11, 19, 43, 67, 163\}$. We can easily find such a prime. In fact we were convinced experimentally that finding a prime $p = db^2 + db + \frac{d+1}{4}$ in the range of 30–90 digits is as easy as finding a prime in that range. So we can easily decide the class of E/F_p with p elements which gives secure cryptosystems.

4.2 Selection of an Elliptic Curve and a Basepoint

Elliptic curve cryptosystems require the computation of kP, where $P = (X_1, Y_1, 1)$ is a fixed point called basepoint. It is accomplished by repeated doubling, adding and subtracting of P. If we can select a basepoint P with a small x-coordinate X_1 or a small y-coordinate Y_1, the amount of computation of kP will be reduced. Especially in the case of signature and identification by a smart card, reducing of total data size stored in a smart card and the computation amount by a smart card is important. If fewer parameters represent an elliptic curve and a basepoint, the data stored in a smart card is reduced. Furthermore we wish to recover P easily from the parameters.

In the last section, we have decided the class of elliptic curves which gives the secure cryptosystems. Note that any elliptic curve E/F_p of the class and any basepoint $P \in E(F_p)$ give cryptosystems with the same security. We will discuss how to select E of the class and P in E suitable for cryptosystems, in the sense that it reduces computation amount of kP and necessary data size to be stored. We will classify d into two cases, $d = 3$ and others.

• Proposed scheme A

First we deal with the case of

$d \in \{11, 19, 43, 67, 163\}$.

For a given $p = db^2 + db + \frac{d+1}{4}$, we know which class, $\mathcal{E}_d$ or $\mathcal{E}'_d$, gives an elliptic curve with p elements in Sect. 4.1. Without loss of generality, we will discuss the case of $\mathcal{E}_d$. Let $y_0 = x_0^3 + 3a_d x_0 + 2a_d$ for $x_0 \in F_p$. Then we get one elliptic curve in $\mathcal{E}_d$ and the basepoint following (9).

$$\mathcal{E}_d \ni E_{y_0,d},\ E_{y_0,d} \ni P = (y_0 x_0, y_0^2), \quad (9)$$

where $\left(\frac{y_0}{p}\right) = 1$. If y_0 satisfies the condition of (9) for $x_0 = 0$, then we get $\mathcal{E}_d \ni E_{y_0,d}$ and $E_{y_0,d} \ni P = (0, 4{a_d}^2)$. In fact such y_0 satisfies the condition of (9) if and only if

$$\left(\frac{y_0}{p}\right) = \left(\frac{2a_d}{p}\right) = 1.$$

Except for $d = 19$, there exists $p = db^2 + db + \frac{d+1}{4}$ which satisfies $\left(\frac{2a_d}{p}\right) = 1$. Combining the condition on p to decide a class (i.e. $\left(\frac{\alpha_d}{p}\right) = -1$ or 1), we obtain that such an elliptic curve over F_p exits if and only if $\left(\frac{\beta_d}{p}\right) = -1$ in both cases, $\mathcal{E}_d$ and $\mathcal{E}'_d$. Table 5 shows the value of β_d.

We were also convinced experimentally that, for $\forall p = db^2 + db + \frac{d+1}{4}$ ($d \in \{11, 43, 67, 163\}$), such an elliptic curve exists with a probability of about one half. Here is one example for a 128-bit prime in the case of $d = 11$.

$E : y^2 = x^3 + 12a^3x + 16a^4$; $E(F_p) \ni P = (0, 4a^2)$,
$p =$ 1701 41183 46046 92395 60785 96622 40717 16369,
$a =$ 527 15357 39869 82616 07887 30307 87012 55349.

Table 5 Integers d and β_d.

d	β_d
11	$3 * 7$
43	$3 * 7$
67	$7 * 31$
163	$7 * 11 * 19 * 127$

Table 6 Data size of Proposed schemes (in bits).

	System Key	Secret Key	Public Key	Signature size
Proposed scheme A	256(201)	128	129	256
Proposed scheme B	131 (76)	128	129	256

Table 7 Computation amount of Proposed schemes (in # of 512-bit modular multiplications).

	Signature Generation	Signature Verification
Proposed scheme A	121	158
Proposed scheme B	105	142

Let us use this elliptic curve $E_{y_0,d}$ and basepoint $P = (0, 4a_d{}^2)$ for Schnorr signature, where $E_{y_0,d} = E$ and $a = a_d$. We further assume that the public key P_A is represented by $x(P_A)$ and the least significant bit of $y(P_A)$. The computation of kP requires the addition to the basepoint P. The addition is calculated in 9 modular multiplications because we can neglect terms for the multiplications by $X_1 = 0$ in the formula (3). So the computation amount of kP is reduced to $1932m(128)$. The computation of $yP + eP_A$ requires $\frac{1}{3}(m-t) + \frac{2}{9}t$ curve additions to $\pm P$ on the average. So the computation amount of $yP + eP_A$ is reduced to $2316m(128)$. We can recover the basepoint in one modular multiplication, only if we store a_d. Since $ord(P)$ equals p, the system key is a_d and p (256 bits). Table 6 shows the data size and Table 7 shows the computation amount. The data size stored in a smart card is reduced to one half of that of Reducing data EC version and Basic EC version. The public key size is the same as that of Reducing data EC version.

The computation amount of the signature generation is reduced by 6% (resp. 14%) of that of Basic EC version (resp. Reducing data EC version). The computation amount of the signature verification is reduced by 10 % of that of Reducing data EC version. It is increased by 5 % of that of Basic EC version. This is because we need one power residue to recover one's public key in the signature verification. If we publish P_A instead of $x(P_A)$ and the least significant bit of $y(P_A)$ as a public key, then the computation amount of the signature verification is reduced by 3% of that of Basic EC version. Even in this case, the public key size is only 50% of Finite field version.

We can choose a prime p and an elliptic curve E/F_p as follows.

$$E : y^2 = x^3 + 12a^3x + 16a^4;\ E(F_p) \ni P = (0, 4a^2),$$
$$p = 2^{128} - 89\ 25388\ 84800\ 47273\ 94087$$
$$a = 1887\ 65172\ 00252\ 43003\ 83780\ 59753\ 00282\ 08521$$

The form of p simplifies the arithmetic modulo p and we can store p with only 73 bits. Of course, the particular form of p provides no disadvantage on the security for now.

- **Proposed scheme B**

Next we deal with the case of $d = 3$. For a given $p = 3b^2 + 3b + 1$, we know which class, $\mathcal{E}_{3,1}$ or $\mathcal{E}_{3,5}$, gives the elliptic curve with p elements in Sect. 4.1. We only discuss the case of $\mathcal{E}_{3,1}$. As for the other case, we can do in the same way. Let $y_0 = {x_0}^3 + \xi$ for ξ and $x_0 \in F_p$. Then an elliptic curve E/F_p with p elements and a basepoint P is given as follows,

$$E_{\xi y_0^3} : y^2 = x^3 + \xi {y_0}^3;\ \ E_{\xi y_0^3}(F_p) \ni P = (x_0 y_0, {y_0}^2),$$

where $\left(\frac{\xi}{p}\right)_6 = -\omega$ and $y_0 \in {F_p}^{*2}$. In this case, there doesn't exist an elliptic curve with the point whose x-coordinate equals 0 because of $\xi \notin {F_p}^{*2}$. But we can select a small ξ such that $\left(\frac{\xi}{p}\right)_6 = -\omega$ and a small x_0 such that $y_0 = {x_0}^3 + \xi \in {F_p}^{*2}$. Here is one example for a 128-bit prime.

$$E : y^2 = x^3 + 3 * 4^3;\ \ E(F_p) \ni P = (4, 16),$$
$$p = 1701\ 41183\ 46046\ 92480\ 63157\ 20930\ 49376\ 39647$$
$$(x_0 = 1,\ \xi = 3)$$

Let us use this elliptic curve $E_{\xi y_0^3}$ and basepoint $P = (x_0 y_0, {y_0}^2)$ for Schnorr signature, where $E_{\xi y_0^3} = E$, $x_0 = 1$ and $\xi = 3$. We further assume that one's public data P_A is represented by $x(P_A)$ and the least significant bit of $y(P_A)$. Then the addition to $P = (x_0 y_0, {y_0}^2) = (X_1, Y_1)$ is accomplished in 9 modular multiplications because we can neglect the multiplications by a small constants X_1 and Y_1 in the formula (3). Furthermore the simple equation of E reduces the computation amount of doubling. It is accomplished in 10 modular multiplications. This reduced computation amount of doubling makes the total computation amount of scheme B smaller than that of scheme A. As for the computation amount of kP, it is reduced to $1676m(128)$. The computation amount of $yP + eP_A$ is reduced to $2060m(128)$. As for the recovering the basepoint, we can recover it in a negligible computation amount only if we store x_0 and ξ whose data size is enough small. As for the data size, the data size of x_0 and ξ is neglected and $ord(P)$ equals p. So the size of system parameters x_0, ξ and p of Schnorr signature scheme on such E is about the

same as that of the definition field. Table 6 shows the data size and Table 7 shows the computation amount.

We see that the elliptic curves and the basepoints in Proposed scheme B give good properties for the cryptosystems, especially in the application of digital signature and identification by a smart card. The data size stored in a smart card is reduced to one third of that of Reducing data EC version and Basic EC version. The public key size is the same as that of Reducing data EC version. The computation amount of the signature generation is reduced by 19% (resp. 26%) of that of Basic EC version (resp. Reducing data EC version). The computation amount of the signature verification is reduced by 6% (resp. 19%) of Basic EC version (resp. Reducing data EC version). If we publish P_A as a public key, then the computation amount of the signature verification is reduced by 14% of that of Basic EC version.

In the same way as Proposed scheme A, we can choose a prime p and an elliptic curve E/F_p as follows.

$$E : y^2 = x^3 + 3 * 4^3; \quad E(F_p) \ni P = (4, 16),$$
$$p = 2^{128} - 86\ 61755\ 49264\ 58706\ 00985$$
$$(x_0 = 1, \ \xi = 3)$$

The form of p simplifies the arithmetic modulo p and we can store p with only 73 bits.

We have seen that we can reduce both of stored data size and computation amount in elliptic curve cryptosystems by the above schemes A and B. Those schemes do not change parameters which relate to security. In other words, they keep the size of the greatest prime divisor of the order of basepoint and satisfy the condition to avoid the recent attack. Therefore they provide no disadvantage on the security. We have also seen that Proposed scheme B is more suitable than Proposed Scheme A in both points of stored data size and computation amount. But the idea of Proposed scheme B is effective only for $d = 3$. The idea of Proposed scheme A is effective for any d as long as $p = db^2 + db + \frac{d+1}{4}$ and $\left(\frac{2a_d}{p}\right) = 1$ hold.

5. Conclusion

Elliptic curve cryptosystems often require the computation of kP, where P is a fixed basepoint. We have proposed the elliptic curves and basepoints suitable for cryptosystems, in the sense that they require less data size and less computation amount for kP. Especially if we use the Proposed version B in Schnorr signature scheme by a smart card, we have seen that

(1) the data size stored in a smart card is reduced to one third of that of Basic EC version and Reducing data EC version;

(2) the data size of public key is reduced to one half of that of Basic EC version and is the same as Reducing data EC version;

(3) the computation amount of the signature generation is reduced by 19% (resp. 26%) of that of Basic EC version (resp. Reducing data EC version);

(4)The computation amount of the signature verification is reduced by 6% (resp. 19%) of Basic EC version (resp. Reducing data EC version);

(5)In the case where we publish the point P_A as a public key, the computation amount of the signature verification is reduced by 14% of that of Basic EC version.

Acknowledgements

The author wishes to thank the anonymous referees for their valuable comments.

References

[1] Atkin, A.O.L. and Morain, F., "Elliptic curves and primality proving", *Research Report 1256, INRIA*, Juin 1990. Submitted to Math. Comp.

[2] Coster, M.J., "Some algorithms on addition chains and their complexity", *Centre for Mathematics and Computer Science Report*, CS-R9024.

[3] Harper, G., Menezes A. and Vanstone, S., "Public-key cryptosystems with very small key lengths", *Advances in Cryptology-Proceedings of Eurocrypt'92*, Lecture Notes in Computer Science, 658 (1993), Springer-Verlag, 163-173.

[4] Ireland, K. and Rosen, M., *A classical introduction to modern number theory*, GTM 84, Springer-Verlag, New-York, 1982.

[5] Koblitz, N., "Elliptic curve cryptosystems", *Mathematics of Computation*, vol.48, pp.203–209, 1987.

[6] Miller, V.S., "Use of elliptic curves in cryptography", *Advances in Cryptology-Proceedings of Crypto'85*, Lecture Notes in Computer Science, 218 , Springer-Verlag, pp.417-426, 1986.

[7] Miyaji, A., "Elliptic curve cryptosystems immune to any reduction into the discrete logarithm problem", *IEICE Trans. Fundamentals*, vol.E76-A, no.1, pp.50–54,1993.

[8] Morain, F. and Olivos, J., "Speeding up the computations on an elliptic curve using addition-subtraction chains", *Theoretical Informatics and Applications*, vol.24, no.6, pp.531–544, 1990.

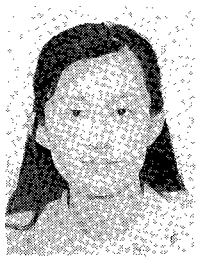
[9] Menezes, A., Okamoto, T. and Vanstone, S., "Reducing elliptic curve logarithms to logarithms in a finite field", *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing*, pp.80–89, 1991.

[10] Pohlig, S. and Hellman, J., "An improved algorithm for computing logarithm over $GF(p)$ and its cryptographic significance", *IEEE Trans. Inf. Theory*, vol.IT-24, pp.106–110, 1978.

[11] Pollard, J., "Monte Carlo methods for index computation(mod p)", *Mathematics of Computation*, vol.32, pp.918–924, 1978.

[12] Schnorr, C.P., "Efficient Signature Generation by Smart Cards", *Journal of Cryptology*, vol.4, no.3, pp.161–174,1991.

[13] Silverman, J.H., *The Arithmetic of Elliptic Curves*, GTM106, Springer-Verlag, New York, 1986.



Atsuko Miyaji She was born in Osaka, Japan, in 1965. She received the B. Sc. and the M. Sc. degrees in mathematics from Osaka University, Osaka, Japan in 1988 and 1990, respectively. Since 1990, she has been with Communication Systems Research Laboratory in Matsushita Electric Industrial Co., LTD. and engaged in research for secure communication. Her research interests include the application of projective varieties theory into cryptography and information security. She is a member of the International Association for Cryptologic Research.