PAPER Special Section on Discrete Mathematics and Its Applications

On Secure and Fast Elliptic Curve Cryptosystems over F_p

Atsuko MIYAJI†, *Member*

SUMMARY From a practical point of view, a cryptosystem should require a small key size and less running time. For this purpose, we often select its definition field in such a way that the arithmetic can be implemented fast. But it often brings attacks which depend on the definition field. In this paper, we investigate the definition field F_p on which elliptic curve cryptosystems can be implemented fast, while maintaining the security. The expected running time on a general construction of many elliptic curves with a given number of rational points is also discussed.
key words: *public-key, elliptic curves*

1. Introduction

Koblitz[6] and Miller[10] proposed a method by which public key cryptosystems can be constructed on the group of points on an elliptic curve over a finite field instead of a finite field. If elliptic curve cryptosystems avoid the Menezes-Okamoto-Vanstone reduction[14], then the only known attacks are the Pollard ρ-method[16] and the Pohlig-Hellman method[15]. So up to the present, we can construct elliptic curve cryptosystems over a smaller definition field than that of cryptosystems based on a finite field discrete logarithm problem (called finite field cryptosystems in this paper). But the running time is not so reduced as the size of the definition field[11]. That is a problem we must solve.

The purpose of this paper is to study an elliptic curve cryptosystem which is implemented fast, while keeping the security high at the same time. For this purpose, we investigate the fundamental operations which determine the running time and show how to make the fundamental operations fast, considering the relation between the fundamental operations and the related attacks. We also show that a general algorithm which constructs many elliptic curves with a given number of rational points, including an elliptic curve with the fast fundamental operations, runs in time

$$O((\log p)^{2+2k} L(\sqrt{p})^{2\sqrt{2}+O(1)}),$$

where $L(x) = \exp(\sqrt{\log x \log\log x})$. In fact, the general algorithm constructs *isogenous elliptic curves*, where elliptic curves are called *isogenous* each other when they have the same number of rational points on the same definition field[18]. Isogenous elliptic curve cryptosystems modulo isomorphism can give different cryptosystems implemented by the same fundamental operations. This paper shows that there exist many isogenous elliptic curve cryptosystems, each of which is constructed in the above time. These results mean that we can offer enough many isogenous elliptic curve cryptosystems over F_p whose size is 100-bit or more in a practical time.

This paper is organized as follows. Section 2 summarizes elliptic curve cryptosystems and discusses the fundamental operations. Section 3 investigates the relation between the fundamental operations of elliptic curve cryptosystems over F_p and the related attacks. Section 4 discusses the expected running time of a general algorithm that constructs many elliptic curves with a given number of rational points. It also shows examples of elliptic curves over F_p investigated in Sect. 3. Section 5 describes the characteristic of isogenous elliptic curve cryptosystems.

2. Elliptic Curve Cryptosystems

We will summarize cryptosystems using an elliptic curve over F_p, where $p \geqq 5$. An elliptic curve over F_p is given as follows,

$$E : y^2 = x^3 + Ax + B \qquad (A, B \in F_p, 4A^3 + 27B^2 \neq 0).$$

Then the set of F_p-rational points on E (with a special element $\mathcal{O}$ at infinity), denoted $E(F_p)$, is a finite abelian group, where $E(F_p) = \{(x, y) \in F_p^2 | y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$.

The security of cryptosystems on E/F_p chosen appropriately depends on the size of a large prime l with $l \mid \#E(F_p)$. Here we show one example of elliptic curve cryptosystems, ElGamal Signature scheme and discuss the fundamental operations of elliptic curve cryptosystems.

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).

Manuscript received September 20, 1993.
Manuscript revised November 22, 1993.
†The author is with Matsushita Electric Industrial Co., Ltd., Kadoma-shi, 571 Japan.

- $P \in E(F_p)$: a basepoint.
- $l = ord(P)$.

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

- Signature generation

  1 User A picks a random number $k \in \{1, ..., l\}$ and computes

  $$R = kP = (r_x, r_y). \tag{1}$$

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

  2 User A computes

  $$y = \frac{m - sr_x}{k} \bmod l \tag{2}$$

  and outputs the signature (R, y).

- Signature verification

  1 User B checks that

  $$mP = yR + r_x P_A. \tag{3}$$

What is supposed to be the fundamental operations of elliptic curve cryptosystems? The most critical operation is an elliptic curve addition in Eqs. (1) and (3). The addition is accomplished by the arithmetic on the definition field F_p (arithmetic modulo p). In order to implement them fast, we may use a precomputation table in the arithmetic modulo p. In fact, generally, the running time of elliptic curve cryptosystems is determined by the arithmetic modulo p (definition field). Only in the signature scheme, the arithmetic modulo l (the order of a basepoint) is required, as seen in the above example. In the signature generation, the computation of Eq. (2) becomes rather important since we can compute Eq. (1) in off-line using idle-time.

Therefore the arithmetic modulo p and modulo l are regarded as fundamental operations of an elliptic curve cryptosystem. In the next section, we discuss one of fundamental operations, arithmetic modulo p, which is required in all cryptosystems using elliptic curve.

3. Optimal Definition Field F_p

In order to implement cryptosystems fast, we often select its definition field in such a way that the arithmetic can be implemented fast. But it often brings critical attacks which depends on the definition field. Therefore we must investigate the relation between the definition field and attacks. In the case of F_{2^r}, we may select such definition field that there exists a basis which enables fast multiplication over F_{2^r}, for example optimal normal basis, and E over such F_{2^r} avoiding the attacks [4], [7]. Here we investigate the case of F_p.

To construct elliptic curve or finite field cryptosystems over F_p, we had better select the definition field F_p with $p = 2^e - s$ (s is a small t-bit integer): Multiplications over F_p can be done by replacing $2^e \equiv s \pmod p$ without computing a residue modulo p [19]. Thus we can compute multiplications over F_p by repeating the following Eq. (4).
Let $a, b \in F_p$.

$$\begin{aligned} a * b &= \sum_{i=0}^{2e-1} x_i 2^i \equiv \sum_{i=0}^{e-1} (x_i + s x_{i+e}) 2^i \pmod p \\ &= \sum_{i=0}^{e+t} y_i 2^i \\ &\vdots \end{aligned} \tag{4}$$

This means that the smaller s is, the faster modular multiplication is. Especially when s is enough small, modular multiplication (over F_p) can be accomplished by computation amount of only one multiplication of two e-bit integers.

Here we will discuss the security of elliptic curve or finite field cryptosystems over F_p with $p = 2^e - s$. If we consider a finite field cryptosystem over such F_p, there exists an attack of the number field sieve [8]. The attack especially will be applied to primes $p = r^e - s$ for a small positive integer r and a nonzero integer s of small absolute value. Since the above $p = 2^e - s$ is the case of $r = 2$, we would be forced to enlarge s or e in order to avoid the attack. To the contrary, the definition field F_p with $p = 2^e - s$ does not bring a critical attack for the elliptic curve cryptosystems. Since the attack is a generalization of the Gaussian integer method [2] to a general number field, the discussion of Ref.[10] that the index-calculus attacks do not extend to elliptic curve cryptosystems still holds. Therefore only E over such a special finite field F_p would not be less secure than a randomly chosen elliptic curve. Thus we should select F_p ($p = 2^e - s$, s is small) and E/F_p satisfying the two conditions:
(1) $\#E(F_p)$ has a large prime factor,
(2) $p^l - 1$ is not divisible by a prime factor for a small integer l (to avoid the attack of Ref.[14]).
Next section will show elliptic curve cryptosystems satisfying these conditions.

4. Fast Elliptic Curve Cryptosystems over F_p

There are two algorithms to construct elliptic curves over F_p, where p is any prime. One is a trial-and-error algorithm to find a suitable elliptic curve by computing the number of rational points of a randomly chosen elliptic curve. The other is the algorithm to construct an elliptic curve with a given number of rational points [13], [12]. Both algorithms work for constructing a single elliptic curve. Here we show a generalized

version of the latter algorithm, which can construct any elliptic curve with a given number of rational points.

Algorithm

1. Choose a prime p.

2. Choose D with $\left(\frac{-D}{p}\right) = 1$, where $\left(\frac{-D}{p}\right)$ denotes the Legendre symbol.

3. Check $4p = a^2 + Db^2$ for an integer a, b. If such integers a and b do not exist, then goto step 2.

4. Set $N = p+1-a$ and $\widetilde{N} = p+1+a$. Check either N or $\widetilde{N}$ is divided by a large prime. If it is not divided, then goto step 2.

5. Calculate a class polynomial $P_{Db'^2}(X)$, which is a polynomial uniquely determined by Db'^2, and solve $P_{Db'^2}(X) \equiv 0 \pmod{p}$ for an integer b' with $b'|b$.

6. Take a solution j_0 of $P_{Db'^2}(X) \equiv 0 \pmod{p}$. Construct an elliptic curves E/F_p with j-invariant j_0 and $\#E(F_p)$ equal to the one divisible by a large prime, N or $\widetilde{N}$. Stop.

In step4, we check either N or $\widetilde{N}$ is divided by a large prime. The size of the large prime depends on a security level. If "a large prime" is more than 120-bit, then the known attacks on such an elliptic curve cryptosystems require at least 2^{60} elliptic curve operations. The amount of necessary operations is roughly equal to that of attacks on finite field cryptosystems on F_p (p is 512 bits). Sometimes lower security is necessary when fast implementation is required or memory storage is limited. In such a case, "a large prime" is replaced by a smaller prime like 100 bits. We will show examples for each case later. Here we call the former case Higher Security Case and the latter case Lower Security Case.

In step 5, the number of different solutions j for $P_{Db'^2}(X) \equiv 0 \pmod{p}$ is equal to the degree of $P_{Db'^2}(X)$, $deg(P_{Db'^2}(X))$. Any solution j can give an elliptic curve with the required number of rational points, N or $\widetilde{N}$. We will discuss this topic later. As for the construction of $P_{Db'^2}(X)$, it is difficult for a large Db'^2 since $deg(P_{Db'^2}(X)) = O(\sqrt{Db'^2})$ (Siegel's result). Therefore we will choose a small D and set $b' = 1$ in step 5 when we need an elliptic curve over F_p [13].

Now we discuss the running time of Algorithm. Since construction of $P_{Db'^2}(X)$ requires $O(\sqrt{p})$ time in the case of $b' = O(\sqrt{p})$, the next condition for step 3 of Algorithm should be required: b is $L(\sqrt{p})^{\alpha}$-smooth. Here we call an integer $L(x)^{\alpha}$-smooth when all of its prime factors are at most $L(x)^{\alpha}$, where $L(x) = \exp(\sqrt{\log x \log\log x})$ and α is a positive real number. Then the probability that a random positive integer $b \leq \sqrt{p}$ is $L(\sqrt{p})^{\alpha}$-smooth is

$$L(\sqrt{p})^{1/(-2\alpha)+O(1)}$$

for $p \to \infty$ [1]. Here we assume that the probability holds for an integer b in step 5.

In this case, Algorithm consists of three parts:
(1) Find D such that $4p = a^2 + Db^2$ for an integer a and b, that $N = p+1-a$ or $\widetilde{N} = p+1+a$ is divisible by a large prime, and that b is $L(\sqrt{p})^{\alpha}$-smooth (step 2, 3 and 4);
(2) For $b'|b$ with $b' \leq L(\sqrt{p})^{\alpha}$, construct a polynomial $P_{Db'^2}(X)$ and solve the equation $P_{Db'^2}(X) \equiv 0 \pmod{p}$ (step 5);
(3) Construct an elliptic curve E/F_p with j-invariant j_0 and the given number of rational points, where j_0 is a solution of $P_{Db'^2}(X) \equiv 0 \pmod{p}$ (step 6).

The expected running time of each step **(1)**–**(3)** is analyzed as follows.
(1) The expected time needed to test a candidate is $O(\log^3 p)$ by using a probabilistic primality test [17]. The expected number of repetition depends deeply on the product of the next two probabilities:
1. the probability that N or $\widetilde{N}$ is divisible by a large prime;
2. the probability that b is $L(\sqrt{p})^{\alpha}$-smooth.
From Cramer's conjecture, we assume that the former probability is $O(\log^{-k} p)$ for a positive integer k. Combining the probability of smooth integer, we see that the product is $O(L(\sqrt{p})^{1/(-2\alpha)+O(1)} \log^{-k} p)$. The remaining problem is the number of D necessary to be checked. It is reasonable to expect that we have to try roughly $O((\log^{2k} p)L(\sqrt{p})^{1/\alpha+O(1)})$ values of D by the following reason: For the bound B on D, we would expect that there are

$$\sum_{D=1}^{B} \frac{1}{2deg(P_D(x))} \geq \sum_{D=1}^{B} \frac{1}{2\sqrt{B}} = \frac{\sqrt{B}}{2}$$

values of D with $4p = a^2 + Db^2$. Therefore the expected final D is

$$O((\log^{2k} p)L(\sqrt{p})^{1/\alpha+O(1)})$$

and the expected time required in **(1)** is

$$O((\log^{2k+3} p)L(\sqrt{p})^{1/\alpha+O(1)}).$$

(2) Since the degree of $P_{Db'^2}(X)$ with the final D is

$$O(\sqrt{\log^{2k} pL(\sqrt{p})^{2\alpha+1/\alpha+O(1)}}),$$

the optimal choice of α is $\frac{1}{\sqrt{2}}$. So the expected time to construct a polynomial $P_{Db'^2}(X)$ is

$$O(\log^k pL(\sqrt{p})^{\sqrt{2}+O(1)}).$$

The remaining problem is to factorize $P_D(X)$ modulo p. Using a formula [5], it is computed in time

$$O((\log^{2+3k} p)L(\sqrt{p})^{3\sqrt{2}+O(1)}).$$

Therefore the expected time required in **(2)** is

$$O((\log^{2+3k} p)L(\sqrt{p})^{3\sqrt{2}+O(1)}).$$

(3) The only problem in this stage is to determine which elliptic curve of at most 6 classes modulo F_p-isomorphism with a given j-invariant has the given number of rational points. Therefore the expected time required in **(3)** is $O(\log p)$.

Combining the above discussion, we conclude that the total expected time is

$$O((\log^{2+3k} p)L(\sqrt{p})^{3\sqrt{2}+O(1)})$$

for $p \to \infty$. In fact, we can construct elliptic curves with the required number of rational points in $deg(P_{Db'^2}(x))$ numbers in this expected time. Therefore we can construct an elliptic curve cryptosystem in time

$$O((\log p)^{2+2k} L(\sqrt{p})^{2\sqrt{2}+O(1)}).$$

Note that the running time of Algorithm for the other $b''|b$ with $b'' \neq b'$ and $b'' \leqq L(\sqrt{p})^{1/\sqrt{2}}$ in step 5 is also the same. Since we select D such that $4p = a^2 + Db^2$ and b is $L(\sqrt{p})^{\frac{1}{\sqrt{2}}}$-smooth, we conclude that we can construct enough many elliptic curve cryptosystems over F_p (p is 100-bit or more) with a required number of rational points in a practical time.

We set $b' = 1$ in step 5 and 6 when we construct a single elliptic curve. Omitting the condition for b from the above discussion, we get that the expected running time to construct a single elliptic curve is $O(\log^{2k+3} p)$. We see that this result follows the conjecture [13].

4.1 Example

We show two examples of elliptic curves over F_p ($p = 2^e - s$) constructed by Algorithm. First we show an example in the case that higher security is required.

• Higher security Case

step 1 We set $p = 2^{127} - 1$. As we know well, the prime is the 12th Mersenne prime.

step 2 For $D = 51$, we get $\left(\frac{-51}{p}\right) = 1$.

step 3 Computing the expansion into continued fraction, we find that

$$4p = a^2 + 51b^2,$$

with

$$a = 509\ 07740\ 96623\ 87813,$$

$$b = 3652\ 30406\ 47016\ 56567.$$

step 4 Set $N = p + 1 - a$ and $\widetilde{N} = p + 1 + a$. Then $\widetilde{N} = 3 * 567\ 13727\ 82015\ 64105\ 77398\ 79370\ 85154\ 97847$, where the last prime is a 126-bit prime.

step 5 Calculate a class polynomial $P_{51}(X)$ for $b' = 1$. Then we get

$$P_{51}(X) = X^2 + 5541101568X + 6262062317568.$$

Then

$$j = 760057286460957768473818082668707532 32$$

is one solution of $P_{51}(X) \equiv 0 \pmod{p}$. Construct an elliptic curve E/F_p with j-invariant j and $\#E(F_p) = N$. We get $E : y^2 = x^3 + Ax + B$, where

$$A = 684\ 63438\ 46595\ 72910\ 76199\ 13576\ 67282\ 37150,$$
$$B = 1590\ 69747\ 95095\ 10152\ 05257\ 62632\ 17415\ 61918.$$

In the above example, $\#E(F_p)$ is divisible by a 126-bit prime. So $E/F_{2^{127}-1}$ can offer a fast cryptosystem keeping a desirable security.

Next we show an example in the case that lower security is allowed.

• Lower security Case

step 1 We set $p = 2^{107} - 1$. As we know well, the prime of $s = 1$ is the 11th Mersenne prime.

step 2 For $D = 3$, we get $\left(\frac{-3}{p}\right) = 1$.

step 3 Computing the expansion into continued fraction, we find that

$$4p = a^2 + 3b^2,$$

with

$$a = 24\ 38789\ 23037\ 40815$$

$$b = 4\ 25314\ 84925\ 08931.$$

step 4 Set $N = p + 1 - a$ and $\widetilde{N} = p + 1 + a$. Then

$$N = 3 * 661 * 8182\ 51522\ 08377\ 88149\ 45464\ 98511,$$

where the last prime is a 97-bit prime.

step 5 Calculate a class polynomial $P_3(X)$ for $b' = 1$. Then we get $P_3(X) = X$. So $j = 0$ is one solution of $P_3(X) \equiv 0 \pmod{p}$. Construct an elliptic curve E/F_p with j-invariant 0 and $\#E(F_p) = N$. We get

$$E : y^2 = x^3 + 625.$$

In the above example, $\#E(F_p)$ is divisible by a 97-bit prime. So $E/F_{2^{107}-1}$ can offer a fast cryptosystem keeping a desirable security.

5. Isogenous Elliptic Curve

In this section, we will describe the isogenous elliptic curves modulo isomorphism. By Hasse's theorem, we

have $|a| \leq 2\sqrt{p}$ for $a = p + 1 - \#E(F_p)$. Conversely, for any integer $|a| \leq 2\sqrt{p}$, there exists E/F_p with $\#E(F_p) = p + 1 - a$ [3]. On the other hand, there are p elliptic curves over F_p modulo isomorphism. Therefore there exist a number of elliptic curves over F_p with a certain $\#E(F_p)$ points modulo isomorphism. Two elliptic curves E and E_1 over F_p are called isogenous if $\#E(F_p) = \#E_1(F_p)$ [18]. So isogenous elliptic curves modulo isomorphism can give different elliptic curve cryptosystems implemented by the same fundamental operations. We have the next fact about the isogenous elliptic curves: For any $|a| \leq 2\sqrt{p}$, j-invariants of E/F_p with $p + 1 \pm a$ elements are represented as a solution of

$$\prod_{b'|b} P_{Db'^2}(X) \equiv 0 \pmod{p}, \ 4p = a^2 + Db^2. \quad (5)$$

For more information about this, we would refer the reader to Ref.[9].

An isomorphism between $E'/F_{p'}$ and E/F_p exists if and only if $p = p'$ and j-invariant of E, $j(E)$ equals $j(E')$. Therefore, in fact, Algorithm can construct the isogenous elliptic curves modulo isomorphism. From the fact that the solutions of Eq. (5) are different each other [3], all elliptic curves constructed in Algorithm for $\forall b''|b$ are not isomorphic each other but have the same rational points on F_p. So Algorithm also shows that we can construct enough many isogenous elliptic curve cryptosystems over F_p (p is 100 bit or more) in a practical time.

We show one example of isogenous elliptic curves. In the example of Higher Security Case (Sect. 4),

$$\begin{aligned} P_{51}(X) &= X^2 + 5541101568X + 6262062317568 \\ &\equiv (X - j)(X - j_1) \pmod{p}, \end{aligned}$$

where

$$j = 760\ 05728\ 64609\ 57768\ 47381\ 80826\ 68707\ 53232,$$

$$j_1 = 941\ 35454\ 81437\ 34548\ 84305\ 49544\ 34722\ 50927.$$

Then we construct an elliptic curve E_1/F_p with j-invariant j_1 and $\#E_1(F_p) = N$, where N is divisible by a 126-bit prime. We get

$$E_1 : y^2 = x^3 + A_1 x + B_1,$$

where

$$A_1 = 427\ 82780\ 40718\ 49464\ 98718\ 92250\ 95650\ 88061,$$

$$B_1 = 852\ 35581\ 42494\ 63749\ 09708\ 38291\ 16714\ 27283.$$

The j-invariants of two elliptic curves E, $E_1/F_{2^{127}-1}$ are not equal but they have the same N rational points. So E and E_1 can construct two different cryptosystems, implemented by the same fundamental operations.

6. Conclusions

In order to give fast and secure cryptosystems, we have proposed E/F_p ($p = 2^e - s$: s is a small integer) and shown examples of E/F_p for two Mersenne primes $p = 2^{107} - 1$ and $p = 2^{127} - 1$. We have shown a general algorithm can construct such an elliptic curve cryptosystem in time

$$O((\log p)^{2+2k} L(\sqrt{p})^{2\sqrt{2}+O(1)}),$$

where $L(x) = \exp(\sqrt{\log x \log\log x})$. We also show that there exist enough elliptic curve cryptosystems, each of which is constructed in this time. These results mean that we can offer enough many isogenous elliptic curve cryptosystems over F_p whose size is 100-bit or more in a practical time.

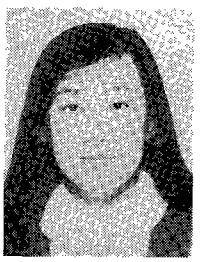
Acknowledgements

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

References

[1] Canfield, E.R., Erdös, P. and Pomerance, C., On a problem of Oppenheim concerning, "Factorisatio numerorum," *J. Number Theory*, vol.17, pp.1–28, 1983.
[2] Coppersmith, D., Odlyzko, A.M. and Schroeppel, R., "Discrete logarithms in GF(p)," *Algorithmica*, vol.1, pp.1–15, 1986.
[3] Deuring, M., "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abh. Math. Sem. Hamburg*, vol.14, pp.197–272, 1941.
[4] Harper, G., Menezes, A. and Vanstone, S., "Public-key cryptosystems with very small key lengths," *Abstracts for Eurocrypt 92*, 1992.
[5] Knuth, D.E., "The art of computer programming," vol. 2, *Seminumerical Algorithms*, second edition, Addison-Wesley, Reading, Mass. 1981.
[6] Koblitz, N., "Elliptic curve cryptosystems," *Mathematics of Computation*, vol.48, pp.203–209, 1987.
[7] Koblitz, N., "Cm-curves with good cryptographic properties," *Advances in Cryptology—Proceedings of CRYPTO'91*, Lecture Notes in Computer Science, vol.576, pp.279–287, Springer-Verlag, 1992.
[8] Gordon, D.M., "Discrete logarithms in $GF(p)$ using the number field sieve," to appear in *SIAM Journal on Discrete Math.*
[9] Lang, S., *Elliptic Functions*, GTM112, Springer-Verlag, New York, 1987.
[10] Miller, V.S., "Use of elliptic curves in cryptography," *Advances in Cryptology—Proceedings of Crypto'85*, Lecture Notes in Computer Science, vol.218, pp.417–426, Springer-Verlag, 1986.
[11] Miyaji, A., "Elliptic curve over F_p suitable for cryptosystems," *Abstract of proceedings of AUSCRYPT'92*, 1992.
[12] 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.
[13] Morain, F., "Building cyclic elliptic curves modulo large primes," *Advances in Cryptology—Proceedings of Eurocrypt'91*, Lecture Notes in Computer Science, vol.547, pp.328–336, Springer-Verlag, 1991.

[14] 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.
[15] Pohlig, S. and Hellman, M., "An improved algorithm for computing logarithm over $GF(p)$ and its cryptographic significance," *IEEE Trans. Inf. Theory*, vol.IT-24, pp.106–110, 1978.
[16] Pollard, J., "Monte Carlo methods for index computation (mod p)," *Mathematics of Computation*, vol.32, pp.918–924, 1978.
[17] Rabin, M.O., "Probabilistic algorithms" in *Algorithms and complexity-new directions and recent results*, edited by J. F. Traub, Academic Press, 1976.
[18] Silverman, J.H., *The Arithmetic of Elliptic Curves*, GTM106, Springer-Verlag, New York, 1986.
[19] Taylor, F.J., "A VLSI residue arithmetic multiplier," *IEEE Trans. Comp.*, vol.C-31, pp.540–546, 1982.



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.