such a *large composite order* pairing–friendly curve.

It is well known that Cocks–Pinch (CP) method [4] is efficient for generating such a *composite order* ordinary pairing–friendly curve. It is based on complex multiplication (CM) method and thus practically supports most of parameter settings of characteristic p, embedding degree k, discriminant D, order r, and Frobenius trace t. An important point is that the ratio ρ of the pairing–friendly curve generated by CP method becomes more than 2. It is an advantage for the purpose of this paper because CP method efficiently supports the case that the ratio $\rho \approx 2$ and the embedding degree $k = 1$. However, it originally has no viewpoints of GLV–based efficiencies such as reported in [10], [7]. Based on CP method, Takashima embedded an GLV–based efficient structure to a certain ordinary pairing–friendly curve by restricting the order r [12]. Then, a pairing calculation became more efficient with some efficient endomorphisms. It is basically available for ordinary pairing–friendly curves whose embedding degree is more than or equal to 2, moreover, it leaves *composite order* ordinary pairing–friendly curves of embedding degree 1 dealt with in this paper out of view.

In the same of Takashima's approach [12], this paper focuses on cyclotomic polynomials of periods 3 (cubic), 4 (quatic), and 6 (sextic), where GLV method relates these periods to efficiently computable endomorphisms with scalar multiplications. In detail, it is important that the degrees of these cyclotomic polynomials are 2. Denoting the cyclotomic polynomial of period n by $\Phi_n(\chi)$, where $n = 3,\ 4,\ 6$, the algorithm proposed in this paper sets the order as $r(\chi) = \Phi_n(\chi)$ and then finds $\chi = \lambda_n$ such that $r(\lambda_n)$ has two large prime factors $v,\ w$. Then, based on CP method, it determines the characteristic p such that a rank 2 *torsion* group structure for *pairing* is embedded in $E(\mathbb{F}_p)$ with the embedding degree $k = 1$. After the proposal of the generating algorithm, some experimental results show that it efficiently generates *ordinary* pairing–friendly elliptic curves of the embedding degree $k = 1$ whose order r has two large prime factors v and w with about 500 or 1000 bits. Moreover, the generated pairing–friendly curve has an efficient structure for the GLV method. It is also shown that a scalar multiplication on the generated *composite order* pairing–friendly curve is about two times accelerated by applying GLV method and joint sparse form (JSF) technique [11] with multi–scalar multiplication.

Throughout this paper, p, k, and r denote characteristic, embedding degree, and order, respectively. $\mathbb{F}_p$ denotes a prime field and $\mathbb{F}_{p^k}$ does its extension field. Small alphabets such as a denote elements in prime. $X \mid Y$ and $X \nmid Y$ mean that X divides and does not divide Y, respectively. $\Phi_n(x)$ denotes the cyclotomic polynomial of order n.

2 Fundamentals

Let us briefly review elliptic curve, *pairing–friendly* curve of composite order, complex multiplication (CM) technique, Gallant–Lambert–Vanstone (GLV) method [8], Cocks–Pinch (CP) method [4], and Takashima's approach for accelerating *pairing* calculation with GLV viewpoints [12].

2.1 Ordinary pairing–friendly curve of composite order

Let $\mathbb{F}_p$ be prime field and E be an *ordinary* elliptic curve over $\mathbb{F}_p$. $E(\mathbb{F}_p)$ that denotes the set of rational points on the curve, including the *infinity point* $\mathcal{O}$, forms an additive Abelian group. Let $\#E(\mathbb{F}_p)$ be its order, consider a large prime number r that divides $\#E(\mathbb{F}_p)$. The smallest positive integer k such that r divides $p^k - 1$ is especially called *embedding degree*. One can consider a pairing such as Tate and Ate pairings on $E(\mathbb{F}_{p^k})$. Usually, $\#E(\mathbb{F}_p)$ is written as

$$\#E(\mathbb{F}_p) = p + 1 - t, \tag{1}$$

where t is the Frobenius trace of $E(\mathbb{F}_p)$.

This paper especially deals with a certain *ordinary* pairing–friendly curve $E(\mathbb{F}_{p^k})$ of composite order as the RSA modulus. In detail, suppose that the order r of a certain subgroup in $E(\mathbb{F}_{p^k})$ has two large prime factors v and w. As also introduced in [6], define the following parameter ρ.

$$\rho = \lfloor \log_2 p \rfloor / \lfloor \log_2 r \rfloor. \tag{2}$$

This ratio ρ is often used for evaluating the redundancy between the order r and the characteristic p. In the case of Barreto–Naehrig curve, ρ is almost 1 and thus it is quite efficient [1]. For *pairing*, $\rho \cdot k$ becomes more than or equal to 2 since it needs to have a rank 2 *torsion group* structure. According to [6], in the case of *composite order* pairing, it is preferred to be small and the minimum is 2. It is briefly, because, since the order r becomes more than 1000–bit as the RSA modulus, $\rho \cdot k \approx 2$ will be the best as the size of the discrete logarithm problem in the embedded extension field $\mathbb{F}^*_{p^k}$. On the same reason, this paper mainly discusses the case of $\rho \cdot k \approx 2$, especially $\rho \approx 2$ and $k = 1$.

2.2 Complex multiplication (CM) technique

The following equation is often called *CM equation* that has the parameters p (characteristic), t (trace of Frobenius), and D (discriminant).

$$4p = t^2 - Ds^2. \tag{3}$$

Note here that, especially when the discriminant D is 1 or 3, the defining equation of elliptic curve is respectively given as

$$E_a : y^2 = x^3 + ax,\ a \in \mathbb{F}_p, \tag{4a}$$
$$E_b : y^2 = x^3 + b,\ b \in \mathbb{F}_p. \tag{4b}$$