SCIENCE CHINA
Information Sciences

• LETTER •

November 2017, Vol. 60 119101:1–119101:3
doi: 10.1007/s11432-016-0412-0

Generating pairing-friendly elliptic curves with fixed embedding degrees

Liang LI

School of Mathematical Sciences, Fudan University, Shanghai 200433*, China*

Received June 15, 2016; accepted August 12, 2016; published online December 13, 2016

Citation Li L. Generating pairing-friendly elliptic curves with fixed embedding degrees. Sci China Inf Sci, 2017, 60(11): 119101, doi: 10.1007/s11432-016-0412-0

Dear editor,

For an elliptic curve E defined over a finite field $\mathbb{F}_q$, the elliptic curve discrete logarithm problem, which is abbreviated as ECDLP, needs to find a solution m to the equation $[m]P = Q$ with fixed points $P, Q \in E(\mathbb{F}_q)$. Many results are based on MOV and FR-reduction to reduce ECDLP in a subgroup (of order r) of $E(\mathbb{F}_q)$ to DLP in a subgroup of $\mathbb{F}^*_{q^k}$, where k, the embedding degree of r, is settled as the minimum integer such that $r|q^k - 1$. For constructive applications of pairings, k needs to be small enough so that the pairing is easy to compute in applications but large so that the DLP in $\mathbb{F}^*_{q^k}$ is computationally infeasible.

An elliptic curve is called pairing-friendly if it has a suitable small embedding degree k and a large prime-order r subgroup such that $r \geqslant \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$. Let $\rho = \log q/\log r$, pairing-friendly one hopes ρ to be close to 1 according to this sense. The Cocks-Pinch method (see Appendix A) usually achieves $\rho \sim 2$. Brezing and Weng [1] generalized to produce families of elliptic curves with smaller ρ in certain cases, achieving $\rho \sim 5/4$ with $k = 8$ or $k = 24$. Barreto and Naehrig [2] successfully constructed a family of elliptic curves with embedding degree $k = 12$, achieving $\rho \sim 1$. However, generating pairing-friendly curves with prime order, i.e., $\rho \sim 1$, is still hard.

In this article, we consider the circumstance of the parameters t (the trace of Frobenius), r, q given as polynomials. The idea of this circumstance has been built by some researchers in their constructions [1, 3–5]. We describe pairing-friendly elliptic curves, then provide a method to construct them with a fixed embedding degree in Theorem 1 and provide constructions with various embedding degrees. And in some of our constructions, the ρ-values are small, even we get the Barreto-Naehrig curves [2] with ρ-value 1 in Construction 6.

Let $E/\mathbb{F}_q$ be an elliptic curve with $n = \#E(\mathbb{F}_q)$ satisfying $(n, p) = 1$, $n = p_1^{n_1} p_2^{n_2} \cdots p_c^{n_c}$, where p_i $(i = 1, \ldots, c)$ are different prime numbers and $n_i \geqslant 1$. Let k be the embedding degree of n, and let k_i be the embedding degree of $p_i^{n_i}$, so $k = [k_1, k_2, \ldots, k_c]$. When p_i is large for some i and $k > k_i$ for all i, we describe the detailed process to attack ECDLP by Pohlig-Hellman's method [6] (see Appendix B). We know that when p_i is small for all i, i.e., n is smooth, Silver-Pohlig-Hellman gives a fast algorithm to solve it. So we need to consider the time complexity of the solution to the ECDLP depends only on the largest prime dividing the order of Q. Based on this and other reasons, using a point of prime order is generally advisable. Thus our task is to search elliptic curves which have large prime-order subgroups and suitable embedding degrees.

Email: liangli11@fudan.edu.cn

Generating elliptic curves. First we introduce some revised definitions based on Freeman-Scott-Teske [7].

Definition 1. The polynomials below are nonzero with rational coefficients.

- We say that $f(x)$ represents primes if $f(x)$ is nonconstant and irreducible with positive leading coefficient, $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$ and $\gcd(\{f(x) : x, f(x) \in \mathbb{Z}\})=1$.
- $f(x)$ is integer-valued if $f(x) \in \mathbb{Z}$ for every $x \in \mathbb{Z}$.
- For a given positive integer k, the quadruple $(t(x), r(x), q(x), d(x))$ parameterizes a class of elliptic curves with embedding degree k if the following conditions are satisfied: (1) $q(x) = p(x)^n$ for some $n \geqslant 1$ and $p(x)$ represents primes; (2) $r(x)$ is nonconstant, irreducible, and integer-valued and has positive leading coefficient; (3) $d(x)$ is an integer-valued, square-free polynomial and has positive leading coefficient; (4) $r(x)|q(x)+1-t(x)$; (5) $r(x)|\Phi_k(t(x) - 1)$, where Φ_k is the k-th cyclotomic polynomial; (6) There is some $y(x) \in \mathbb{Q}[x]$ such that $d(x)y(x)^2 = 4q(x) - t(x)^2$.
- We say a class $(t(x), r(x), q(x), d(x))$ is a family of elliptic curves if the equation $Dz^2 = d(x)$ has infinitely many integer solutions (x, z) for some positive square-free integer D. We say the family of elliptic curves has discriminant D.
- We say that a family $(t(x), r(x), q(x), d(x))$ is complete if $d(x)$ is a constant of positive square-free integer D. So this complete family of elliptic curves has discriminant D.

Definition 2. Let $t(x)$, $r(x)$, $q(x)$, $d(x) \in \mathbb{Q}[x]$, and suppose that $(t(x), r(x), q(x), d(x))$ parameterizes a family of elliptic curves with embedding degree k. The ρ-value of $(t(x), r(x), q(x), d(x))$, denoted as $\rho(t, r, q, d)$, is $\rho(t, r, q, d) = \lim_{x\to\infty} \frac{\log\ q(x)}{\log\ r(x)} = \frac{\deg\ q(x)}{\deg\ r(x)}$.

According to the method of Brezing-Weng, we give an approach from another point of view to construct elliptic curves where D is not fixed at the beginning. The best situation is that $d(x)$ is a constant D with $D < 10^{12}$. We will give this situation in the following constructions.

Theorem 1. Fix a positive integer k. Execute the following steps.

(1) Find a polynomial $g(x) \in \mathbb{Z}[x]$ with positive leading coefficient such that $\Phi_k(g(x)) = r_1(x)r_2(x) \cdots r_l(x)$, where $r_i(x)$ is irreducible and has positive leading coefficient for all $i \in \{1, \dots, l\}$.

(2) Choose $I \subset \{1, \dots, l\}$ and $h(x)|\frac{g(x)^k-1}{\Phi_k(g(x))}$ such that the degree of $d(x)$ is sufficiently small where the polynomial $h(x)\prod_{j\in I} r_j(x)$ is written as the form of $f(x)^2 + d(x)s(x)^2$ satisfying $(f(x), d(x)s(x)^2) = 1$ and $d(x)$ is an integer-valued, square-free polynomial and has positive leading coefficient.

(3) Let $A = \mathbb{Q}[x]/[f(x)^2 + d(x)s(x)^2]$. Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $g(x) + 1$ in A.

(4) Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $[a(x) - b(x)f(x)]s(x)[g(x) - 1]$ in A where $a(x)f(x) + b(x)d(x)s(x)^2 = 1$ in $\mathbb{Q}[x]$.

(5) Let $q(x) \in \mathbb{Q}[x]$ be given by $[t(x)^2 + d(x)y(x)^2]/4$.

Suppose that $q(x)$ is a power of $p(x)$ which represents primes and $y(x_0) \in \mathbb{Z}$ for some $x_0 \in \mathbb{Z}$. Then for all $j \in I$, the quadruple $(t(x), r_j(x), q(x), d(x))$ parameterizes a class of elliptic curves with embedding degree k (the proof is provided in Appendix C).

Remark 1. For each x_0 such that $r_j(x_0)$ is a prime and $q(x_0)$ is the power of a prime, there is an elliptic curve E defined over $\mathbb{F}_{q(x_0)}$ with embedding degree k and CM discriminant D where D is the square-free part of nonnegative integer $d(x_0)$. If such $D < 10^{12}$, then E can be constructed via the CM method. But it is not suitable by this way because the value of x is limited. In practice, we want to find a family $(t(x), r(x), q(x), d(x))$ in order to get (x_0, z_0), a solution to the equation $Dz^2 = d(x)$, such that $r_j(x_0)$ is a prime and $q(x_0)$ is the power of a prime. Then there exists an elliptic curve $E/\mathbb{F}_{q(x_0)}$ with a subgroup of order $r_j(x_0)$ and embedding degree k and CM discriminant D. If $D < 10^{12}$, then E can be constructed via the CM method. We hope the degree of $d(x)$ is sufficiently small for the possibility of getting a family with a discriminant D. When $\deg(d) = 1$1), it is easy to get a family. We know that $\deg(d) = 0$ is the best, i.e., $d(x)$ is a constant.

Proposition 1. When $(t(x), r_j(x), q(x), d(x))$ parameterizes a class of elliptic curves, and either of the following conditions holds: (1) $\deg(d) = 1$; (2) $d(x)$ has the form of $x^2 + c$ where $c \in \mathbb{Z} \setminus \{0\}$, then $(t(x), r_j(x), q(x), d(x))$ can be a family (the proof is provided in Appendix D).

Remark 2. If $d(x) = x + c$ where $c \in \mathbb{Z}$, then $Dy^2 = d(x)$ has infinitely many integers solutions for any square-free integer D. The family can be switched to a complete one via replacing x by $Dy^2 - c$.

We give following constructions by Theorem 1.

Construction 1. Let $k = 4m$ for $m > 1$, and $g(x) = x$. Let $f(x) = x^m$, then $f(x)^2 + 1|x^{4m} - 1$. In this case, $D = d(x) = 1$, $s(x) = 1$, $t(x) =$

1) $\deg(d)$ means the degree of polynomial $d(x)$.

$x+1$, $q(x) = \frac{1}{4}[(x+1)^2+(x-1)^2x^{2m}]$. We see that $\Phi_k(x)|f(x)^2+1$, then $(t(x), \Phi_k(x), q(x), 1)$ parameterizes a complete family of elliptic curves with embedding degree k. The ρ-value of this family is $(2m+2)/\varphi(k)$. When $k = 4$, we get supersingular elliptic curves of prime order (see Appendix E.1).

Construction 2. Let $k = 6m$ for $m > 1$, and $g(x) = x$. Let $f(x) = 2x^m - 1$, then $f(x)^2+3 = 4(x^{2m}-x^m+1)|x^{6m}-1$. In this case, $D = d(x) = 3$, $s(x) = 1$, $t(x) = x+1$, $q(x) = \frac{1}{12}[3(x+1)^2 + (x-1)^2(2x^m-1)^2]$. We see that $\Phi_k(x)|f(x)^2+3$, then $(t(x), \Phi_k(x), q(x), 3)$ parameterizes a complete family of elliptic curves with embedding degree k. The ρ-value of this family is $(2m+2)/\varphi(k)$. When $k = 6$, we get supersingular elliptic curves of prime order (see Appendix E.2).

Construction 3. Let $k = 2^m$ for $m > 2$, we know that $\Phi_k(x) = x^{2^{m-1}} + 1$. In this case, $D = d(x) = 1$, $f(x) = x^{2^{m-2}}$, $s(x) = 1$, $t(x) = x+1$, $q(x) = \frac{1}{4}[(x+1)^2 + x^{2^{m-1}}(x-1)^2]$. Then $(t(x), \Phi_k(x), q(x), 1)$ parameterizes a complete family of elliptic curves with embedding degree k. The ρ-value of this family is $(k+4)/k$. When $k = 4$, it is same to Construction 1.

Construction 4. Let $k = 2^m3^n$ for $m \geqslant 2$, $n \geqslant 1$ and $k > 12$, we know that $\Phi_k(x) = x^{2^m3^{n-1}} - x^{2^{m-1}3^{n-1}} + 1$. Then $\Phi_k(x) = (x^{2^{m-1}3^{n-1}} - 1)^2 + (x^{2^{m-2}3^{n-1}})^2$. In this case, $D = d(x) = 1$, $f(x) = x^{2^{m-1}3^{n-1}} - 1$, $s(x) = x^{2^{m-2}3^{n-1}}$, $t(x) = x+1$, $q(x) = \frac{1}{4}[(x+1)^2 + x^{2^{m-1}3^n}(x-1)^2]$. Then $(t(x), \Phi_k(x), q(x), 1)$ parameterizes a complete family of elliptic curves with embedding degree k. The ρ-value of this family is $(\frac{3}{2}k+6)/k$.

Construction 5. Let $k = 2 \times 3^n$ for $n > 1$, we know that $\Phi_k(x) = x^{2\times3^{n-1}} - x^{3^{n-1}} + 1$. Then $\Phi_k(x) = (x^{3^{n-1}} - 1)^2 + x(x^{\frac{3^{n-1}-1}{2}})^2$. Then $d(x) = x$. For $\deg(d) = 1$, we can get a family of elliptic curves with embedding degree k. Based on Remark 2, this family can be switched to a complete one, by replacing x by Dx^2 for some square-free integer D such that $\Phi_k(Dx^2)$ is irreducible. In this case, $d(x) = D$, $g(x) = Dx^2$, $f(x) = (Dx^2)^{3^{n-1}} - 1$, $s(x) = D^{\frac{3^{n-1}-1}{2}}x^{3^{n-1}}$, $t(x) = Dx^2+1$, $q(x) = \frac{1}{4}[(Dx^2+1)^2 + D^{3^n}x^{2\times3^n}(Dx^2-1)^2]$. Then $(t(x), \Phi_k(Dx^2), q(x), D)$ parameterizes a complete family of elliptic curves with embedding degree k. The ρ-value of this family is $(\frac{3}{2}k+6)/k$. Clearly $D \neq 3$. If not, $\Phi_k(3x^2) = (3^{3^{n-1}}x^{2\times3^{n-1}} - 3^{\frac{3^{n-1}+1}{2}}x^{3^{n-1}}+1)(3^{3^{n-1}}x^{2\times3^{n-1}} + 3^{\frac{3^{n-1}+1}{2}}x^{3^{n-1}}+1)$, then the ρ-value is strictly larger than 2.

According to our method, we also can get the Barreto-Naehrig curves [2] as below.

Construction 6. Let $k = 12$, $g(x) = 6x^2$. Since $\Phi_{12}(g(x)) = (36x^4 + 36x^3 + 18x^2 + 6x + 1)(36x^4 - 36x^3 + 18x^2 - 6x + 1) = r_1(x)r_2(x)$, we choose $I = \{1\}$ and $h(x) = 1$. We know $r_1(x) = (3x^2+3x+1)^2+3(3x^2+x)^2$. Then $d(x) = 3$, $f(x) = 3x^2+3x+1$, $s(x) = 3x^2+x$, $t(x) = 6x^2+1$, $q(x) = 36x^4+36x^3+24x^2+6x+1$. We have $r_1(x) = q(x)+1-t(x)$. Then $(t(x), r_1(x), q(x), 3)$ parameterizes a complete family of elliptic curves with embedding degree 12, and ρ-value 1. It could construct pairing-friendly curves of prime order.

Conclusion. We have presented a simple algorithm to construct pairing-friendly curves with a fixed embedding degree k. There is a table listed detailed results of ρ-values, which can be found in Appendix F. Specifically, the general cases of $k = 2^m$ in Construction 3, $k = 2^m3^n$ in Construction 4 with CM discriminant 1 and $k = 2 \times 3^n$ in Construction 5 with some discriminants have never been given before as far as we know.

Supporting information Appendixes A–D, E.1, E.2, and F. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Brezing F, Weng A. Elliptic curves suitable for pairing based cryptography. Des Codes Cryptogr, 2005, 37: 133–141

2 Barreto P S L M, Naehrig M. Pairing-friendly elliptic curves of prime order. In: Proceedings of the 12th International Conference on Selected Areas in Cryptography. Berlin: Springer, 2005. 319–331

3 Barreto P S L M, Lynn B, Scott M. Constructing elliptic curves with prescribed embedding degrees. In: Proceedings of the 3rd International Conference on Security in Communication Networks. Berlin: Springer, 2002. 263–273

4 Miyaji A, Nakabayashi M, Takano S. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans Fund Electron Commun Comput Sci, 2001, 84: 1234–1243

5 Scott M, Barreto P S L M. Generating more MNT elliptic curves. Des Codes Cryptogr, 2006, 38: 209–217

6 Pohlig S, Hellman M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Trans Inf Theory, 1978, 24: 106–110

7 Freeman D, Scott M, Teske E. A taxonomy of pairing-friendly elliptic curves. J Cryptol, 2010, 23: 224–280