SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Generating pairing-friendly elliptic curves with fixed embedding degrees

Liang LI[1]

[1]*School of Mathematical Sciences, Fudan University, Shanghai* 200433, *P. R. China*

Appendix A The Cocks-Pinch method

The Cocks-Pinch method can construct pairing-friendly curves with arbitrary embedding degree k but usually has $\rho \sim 2$. It is worked via first fixing a subgroup of order r and a CM discriminant D, then computing a trace t and prime q satisfying the CM equation.

To be specific, give an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ where $D > 0$ is square-free and $\mathcal{O}$ is the maximal order in K. Take a prime r such that r splits in $\mathcal{O}$ and $k|r-1$. Let ζ_k be a primitive k-th root of unity in $(\mathbb{Z}/r\mathbb{Z})^*$. Set $t \equiv \zeta_k + 1(\text{mod } r)$ and $y \equiv (t-2)/\sqrt{-D}(\text{mod } r)$. Finally test whether $(t^2 + Dy^2)/4$ is a prime p (or a prime power q). When p (or q) is found, there exists an elliptic curve E over $\mathbb{F}_p$ (or $\mathbb{F}_q$) with an subgroup of order r and embedding degree k. The equation $4p = t^2 + Dy^2$ (or $4q = t^2 + Dy^2$) is called CM equation. If $D < 10^{12}$, then E can be constructed by the CM method.

Appendix B Attacking ECDLP by Pohlig-Hellman's method

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 $(i = 1, \cdots, c)$ are different prime numbers and $n_i \geqslant 1$. Let k be the embedding degree of n. Denote $N_i = p_i^{n_i}$ and let k_i be the embedding degree of N_i, so $k = [k_1, k_2, \cdots, k_c]$. Next we will apply Pohlig-Hellman's method [1] to solve ECDLP. When p_i is small for all i, this algorithm works fast. When p_i is large for some i and $k > k_i$ for all i, we give the detailed process to solve it by Tate-Lichtenbaum pairing [2].

Lemma 1. $\frac{E[n]}{N_i E[n]} \cong E[N_i]$ as group for all i. The map $\xi_i : \frac{E[n]}{N_i E[n]} \to E[N_i]$ by setting $\xi_i(\overline{Q}) = \frac{n}{N_i} Q$ is an isomorphism.

Proof. Since $(N_i, p) = 1$, then $E[N_i] \cong \mathbb{Z}_{N_i} \times \mathbb{Z}_{N_i}$. Because $N_i|n$ and $N_i\mathbb{Z}_n$ is a subgroup of $\mathbb{Z}_n$, we have $\mathbb{Z}_n/N_i\mathbb{Z}_n \cong \mathbb{Z}_{N_i}$ and $\frac{E[n]}{N_i E[n]} \cong \mathbb{Z}_{N_i} \times \mathbb{Z}_{N_i}$. Define a map:

$$\xi_i : \frac{E[n]}{N_i E[n]} \longrightarrow E[N_i]$$
$$\overline{Q} \longmapsto \frac{n}{N_i} Q.$$

It is well defined obviously. Let $\{A, B\}$ be the base of $E[n]$, for any $Q \in E[n]$, $Q = aA + bB$, where $a, b \in \mathbb{Z}$. If $\xi_i(\overline{Q}) = 0$, *i.e.* $\frac{an}{N_i} A + \frac{bn}{N_i} B = 0$, then $n|\frac{an}{N_i}$ and $n|\frac{bn}{N_i}$, so $N_i|a$ and $N_i|b$. Thus we have $Q \in N_i E[n]$, then ξ_i is injective. On the other hand, $\frac{n}{N_i} A$ and $\frac{n}{N_i} B$ have the exact order N_i and they are linearly independent, so ξ_i is surjective. □

For $Q, Q' \in E(\mathbb{F}_q)$, we need to find an m such that $Q' = mQ$. Obviously, $Q', Q \in E[n]$. Let $\overline{Q}$, $\overline{Q'} \in \frac{E[n]}{N_i E[n]}$. If p_i is large for some i and $k > k_i$ for all i, we can apply Tate-Lichtenbaum pairing to solve this discrete logarithm problem in the extension field $\mathbb{F}_{q^{d_i}}$. Then we can obtain $\widetilde{Q'} = m_i \widetilde{Q}$ where $\widetilde{Q'}, \widetilde{Q} \in \frac{E(\mathbb{F}_q)}{N_i E(\mathbb{F}_q)}$. Hence $\overline{Q'} = m_i \overline{Q}$ for $E(\mathbb{F}_q) \subseteq E[n]$, so $\xi_i(\overline{Q'}) = m_i \xi_i(\overline{Q})$. We need to solve the equations

$$x \equiv m_i (\text{mod } N_i).$$

Let $M_i = \frac{n}{N_i}$. we have $M_i M_i^{-1} \equiv 1(\text{mod } N_i)$ since $(M_i, N_i) = 1$. Set

$$m = \sum_{i=1}^{c} M_i M_i^{-1} m_i.$$

Email: liangli11@fudan.edu.cn

We have $m \equiv M_i M_i^{-1} m_i \equiv m_i \pmod{N_i}$ for all $1 \leqslant i \leqslant c$. So $\xi_i(\overline{Q'}) = m\xi_i(\overline{Q})$ for all i. For $(\frac{n}{N_1}, \cdots, \frac{n}{N_c}) = 1$, then we have $Q' = mQ$.

Appendix C The proof of Theorem 1

Proof. $g(x) \in \mathbb{Z}[x]$ has positive leading coefficient, then $g_i(x) \in \mathbb{Z}[x]$ is nonconstant, irreducible, and integer-valued and has positive leading coefficient for all i. Let $t(x) = g(x) + 1 + u(x)[f(x)^2 + d(x)s(x)^2] = g(x) + 1 + u(x)h(x)\prod_{j\in I} r_j(x)$ for some $u(x) \in \mathbb{Q}[x]$. $\Phi_k(t(x) - 1) = \Phi_k(g(x) + u(x)h(x)\prod_{j\in I} r_j(x))$, then $r_j(x)|\Phi_k(t(x) - 1)$ for $\forall\ j \in I$. In the ring A, we have

$$\begin{aligned} q(x) + 1 - t(x) =& \frac{1}{4}[t(x)^2 + d(x)y(x)^2] - g(x) \\ =& \frac{1}{4}\{t(x)^2 + d(x)[a(x) - b(x)f(x)]^2 s(x)^2 [g(x) - 1]^2 - 4g(x)\} \\ =& \frac{1}{4}\{t(x)^2 - f(x)^2[a(x) - b(x)f(x)]^2[g(x) - 1]^2 - 4g(x)\} \\ =& \frac{1}{4}\{t(x)^2 - [g(x) - 1]^2 - 4g(x)\} \\ =& \frac{1}{4}[t(x) - g(x) - 1][t(x) + g(x) + 1] \\ =& 0, \end{aligned}$$

i.e. $r_j(x)|q(x) + 1 - t(x)$ for all $j \in I$. □

Appendix D The proof of Proposition 1

Proof. Suppose the condition (1) holds, let $d(x) = ax + b$ with $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$. Choose x_0 such that $ax_0 + b = Dy_0{}^2$ where D is a square-free integer. For all $s \in \mathbb{Z}$, $(Das^2 + 2Dsy_0 + x_0, as + y_0)$ are the solutions to the equation $Dy^2 = ax + b$. If the condition (2) holds, analogously, choose x_0 such that $x_0{}^2 + c = Dy_0{}^2$ where $D > 1$ is a square-free integer. Then the equation $x^2 - Dy^2 = -c$ has a solution (x_0, y_0), so it has infinitely many integer solutions. □

Appendix E Some supplementary of the constructions

Appendix E.1 $k = 4$ in Construction 1

When $k = 4$, we have

$$\begin{aligned} &f(x) = x, \\ &D = d(x) = 1, \\ &s(x) = 1, \\ &t(x) = x + 1, \\ &q(x) = \frac{(x+1)^2}{2}. \end{aligned}$$

When x is chosen as $2^e - 1$ for $e \in \mathbb{N}^*$, q will be the power of 2. Let $n(x) = q(x) + 1 - t(x) = \frac{x^2+1}{2} = \frac{\Phi_4(x)}{2}$, then $(t(x), n(x), q(x), 1)$ parameterizes a complete family of elliptic curves with embedding degree 4 and they are supersingular elliptic curves of prime order. It is the same case of Miyaji-Nakabayashi-Takano [3]. From the point of view of [4], the only possible such curves are

$$E/\mathbb{F}_q : y^2 + y = x^3 + x$$

and

$$E/\mathbb{F}_q : y^2 + y = x^3 + x + 1.$$

Appendix E.2 $k = 6$ in Construction 2

When $k = 6$, we have

$$\begin{aligned} &f(x) = 2x - 1, \\ &D = d(x) = 3, \\ &s(x) = 1, \\ &t(x) = x + 1, \\ &q(x) = \frac{(x+1)^2}{3}. \end{aligned}$$

When x is chosen as $3^e - 1$ for $e \in \mathbb{N}^*$, q will be the power of 3. Let $n(x) = q(x) + 1 - t(x) = \frac{x^2-x+1}{3} = \frac{\Phi_6(x)}{3}$, then $(t(x), n(x), q(x), 1)$ parameterizes a complete family of elliptic curves with embedding degree 6 and they are supersingular elliptic curves of prime order. It is the same case of Miyaji-Nakabayashi-Takano. According to [5], the only possible such curves are

$$E/\mathbb{F}_q : y^2 = x^3 - x + \delta$$

and

$$E/\mathbb{F}_q : y^2 = x^3 - x - \delta,$$

where $\delta \in \mathbb{F}_q$ with $Tr_{\mathbb{F}_q/\mathbb{F}_3}\delta = 1$.

Appendix F The ρ-values of the constructions of embedding degree $k \leqslant 36$

Table F1 The ρ-values of the constructions of embedding degree $k \leqslant 36$

Embedding degree k	C[1)]1	C2	C3	C4	C5	C6
8	$\frac{3}{2}$	-	$\frac{3}{2}$	-	-	-
12	2	$\frac{3}{2}$	-	-	-	1
16	$\frac{5}{4}$	-	$\frac{5}{4}$	-	-	-
18	-	$\frac{4}{3}$	-	-	$\frac{11}{6}$	-
20	$\frac{3}{2}$	-	-	-	-	-
24	$\frac{7}{4}$	$\frac{5}{4}$	-	$\frac{7}{4}$	-	-
28	$\frac{4}{3}$	-	-	-	-	-
30	-	$\frac{3}{2}$	-	-	-	-
32	$\frac{9}{8}$	-	$\frac{9}{8}$	-	-	-
36	$\frac{5}{3}$	$\frac{7}{6}$	-	$\frac{5}{3}$	-	-

In this table, we list the ρ-values of our constructions.

References

1 Pohlig S, Hellman M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Transactions on Information Theory, 1978(24): 106-110.

2 Silverman J H. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Springer New York, 2009(106).

3 Miyaji A, Nakabayashi M, Takano S. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2001(E84-A): 1234-1243.

4 Menezes A, Vanstone S. Isomorphism classes of elliptic curves over finite fields of characteristic 2. Utilitas Mathematica, 1990(38): 135-153.

5 Morain F. Building cyclic elliptic curves modulo large primes. Advances in Cryptology-EUROCRYPT, the series Lecture Notes in Computer Science, Springer Berlin, 1991(547): 328-336.

1) C=Construction.