More constructing pairing-friendly elliptic curves for cryptography

Tanaka Satoru and Nakamula Ken

Department of Mathematics and Information Sciences, Tokyo Metropolitan University†
email: {satoru,nakamula}@tnt.math.metro-u.ac.jp

Overview

We study the problem of computing suitable parameters of "pairing-friendly" elliptic curves, finding a polynomial $u(x)$ by the method of indeterminate coefficients so that $u(a) = \zeta_k$ for some $a \in \mathbf{Q}(\zeta_k)$ as in [5] to construct new families of curves in the framework defined by Freeman, Scott and Teske [4].

Elliptic curve and families

Let E be an elliptic curve defined over a finite field $\mathbf{F}_q$, and r be the largest prime dividing $\#E(\mathbf{F}_q) = q + 1 - t$, the order of the group of $\mathbf{F}_q$-rational points of E with the Frobenius trace t. We define the *embedding degree* as the smallest positive integer k such that r divides $q^k - 1$ when q is a prime. The parameters required to determine pairing-friendly elliptic curves are t, r, q, k and the CM discriminant D for the CM method to construct elliptic curves. To produce such integers q, r, t from given k, D, Freeman et al. introduced families of polynomials $q(x), r(x), t(x)$ over $\mathbf{Q}$ satisfying:

(1) $q(x) = p(x)^d$ for some $d \geq 1$ and $p(x)$ that represents primes.
(2) $r(x) = c \cdot \tilde{r}(x)$ with $c \in \mathbf{Z}_{\geq 1}$ and $\tilde{r}(x)$ that represents primes.
(3) $r(x) \mid q(x) + 1 - t(x)$.
(4) $r(x) \mid \Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.
(5) $4q(x) - t(x)^2 = Dy^2$ has infinitely many integer solutions (x, y).

One of the method constructing such family was proposed in [3]. Briefly speaking, the key point of this method is to find an algebraic number field $K \cong \mathbf{Q}[x]/(r(x))$ including $\sqrt{-D}$ and a primitive kth root ζ_k of 1. Once such an $r(x)$ is found, there is a straightforward way to compute $t(x)$ satisfying (4) and $q(x)$ satisfying (3), (5).

Factorization of cyclotomic polynomial

Assume $\sqrt{-D} \in \mathbf{Q}(\zeta_k)$. If $\Phi_k(u(x))$ is reducible with a factor of degree $\varphi(k)$ for some $u(x) \in \mathbf{Q}[x]$, we can take $r(x)$ to be one of its irreducible factor. To obtain such $u(x)$, it is necessary and sufficient that

$$u(a(x)) \equiv x \pmod{\Phi_k(x)}$$

for some $a(x) \in \mathbf{Q}[x]$. we consider the case

$$u(x) = \sum_{i=0}^{\varphi(k)-1} u_i x^i, \qquad a(x) = \sum_{i=0}^{\varphi(k)-1} a_i x^i.$$

Let $v(x)$ be the polynomial of degree $< \varphi(k)$ such that $v(x) \equiv u(a(x)) \pmod{\Phi_k(x)}$. Then $v(x)$ can be written in the form

$$v(x) = \sum_{i=0}^{\varphi(k)-1} \sum_{j=0}^{\varphi(k)-1} u_j v_{ij} x^i.$$

where v_{ij} are explicit polynomials of $a_0, \cdots, a_{\varphi(k)-1}$ of degree $< \varphi(k)$. Therefore, from given $a_0, \cdots, a_{\varphi(k)-1} \in \mathbf{Q}$, we should solve the linear equation

$$V \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{\varphi(k)-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

where $V = (v_{ij})$ is a $\varphi(k) \times \varphi(k)$ matrix with entries in $\mathbf{Q}$. It is well known that the general solution $u_0, \cdots, u_{\varphi(k)-1}$ can be written as explicit rational functions of $a_0, \cdots, a_{\varphi(k)-1}$. We now take an irreducible factor $r(x)$ of $\Phi_k(u(x))$. The computation of $u(x)$ and $r(x)$ depends only on k. We can apply them for any D such that $\sqrt{-D} \in \mathbf{Q}(\zeta_k)$.

Example for $k = 8$

In this case, we have

$$V = \begin{pmatrix} 1 & a_0 & {a_0}^2 - {a_2}^2 - 2a_1a_3 & {a_0}^3 - 3a_2(a_0a_2 + {a_1}^2 - {a_3}^2) - 6a_0a_1a_3 \\ 0 & a_1 & 2a_0a_1 - 2a_2a_3 & {a_3}^3 - 3a_1(a_1a_3 + {a_2}^2 - {a_0}^2) - 6a_0a_2a_3 \\ 0 & a_2 & {a_1}^2 - {a_3}^2 + 2a_0a_2 & -{a_2}^3 + 3a_0(a_0a_2 + {a_1}^2 - {a_3}^2) - 6a_1a_2a_3 \\ 0 & a_3 & 2a_1a_2 + 2a_0a_3 & {a_1}^3 - 3a_3(a_1a_3 + {a_2}^2 - {a_0}^2) + 6a_0a_1a_2 \end{pmatrix}.$$

Let d and n_i be as follows:

$$\begin{aligned} d &:= ({a_1}^2 + {a_3}^2)((a_1 - a_3)^2 + 2{a_2}^2)((a_1 + a_3)^2 - 2{a_2}^2), \\ n_0 &:= -a_2(5{a_1}^4a_3 - 5{a_1}^3{a_2}^2 + 5a_1{a_2}^2{a_3}^2 - 2{a_2}^4a_3 + 3{a_3}^5), \\ n_1 &:= {a_1}^5 - 4{a_1}^3{a_3}^2 + 9{a_1}^2{a_2}^2a_3 + a_1(2{a_2}^4 + 3{a_3}^4) + 3{a_2}^2{a_3}^3, \\ n_2 &:= {a_1}^3a_2 + 3a_1a_2{a_3}^2 - 2{a_2}^3a_3, \\ n_3 &:= {a_3}^3 - {a_1}^2a_3 + 2a_1{a_2}^2. \end{aligned}$$

If d is nonzero, then we can solve the system above. The solution is

$$\begin{cases} u_0 = -\left(n_3{a_0}^3 + n_2{a_0}^2 + n_1a_0 - n_0\right)/d \\ u_1 = \left(3n_3{a_0}^2 + 2n_2a_0 + n_1\right)/d \\ u_2 = -\left(3n_3a_0 + n_2\right)/d \\ u_3 = -n_3/d \end{cases}.$$

New data for $D = 1, k = 8$

After the computation, we challenge to construct new families of curves of embedding degree 8 by the algorithm in [6].

$\mathrm{lc}\,(u)$	$u(x)$	$t(x)$	$\deg r(x)$	$\deg q(x)$	$\rho(t,r,q)$
2	$\mathbf{2x^3 + 4x^2 + 6x + 3}$	$\mathbf{u(x)^3 + 1}$	**4**	**6**	**3/2**
9	$9x^3 + 3x^2 + 2x + 1$	$u(x)^5 + 1$	4	6	3/2
17	$17x^3 + 32x^2 + 24x + 6$	$u(x)^3 + 1$	4	6	3/2
18	$18x^3 + 39x^2 + 31x + 7$	$u(x)^3 + 1$	4	6	3/2
64	$64x^3 + 112x^2 + 75x + 18$	$u(x)^5 + 1$	8	14	7/4
68	$68x^3 + 110x^2 + 65x + 15$	$u(x)^5 + 1$	4	6	3/2
82	$\mathbf{82x^3 + 108x^2 + 54x + 9}$	$\mathbf{u(x)^5 + 1}$	**4**	**6**	**3/2**
144	$144x^3 + 480x^2 + 539x + 202$	$u(x)^5 + 1$	8	14	7/4
144	$144x^3 + 96x^2 + 29x + 2$	$u(x)^5 + 1$	8	14	7/4
257	$257x^3 + 256x^2 + 96x + 12$	$u(x)^3 + 1$	4	6	3/2
388	$388x^3 + 798x^2 + 561x + 134$	$u(x)^5 + 1$	4	6	3/2
392	$392x^3 + 980x^2 + 821x + 231$	$u(x)^5 + 1$	8	14	7/4
626	$\mathbf{626x^3 + 500x^2 + 150x + 15}$	$\mathbf{u(x)^5 + 1}$	**4**	**6**	**3/2**
738	$\mathbf{738x^3 + 1488x^2 + 1006x + 229}$	$\mathbf{u(x)^5 + 1}$	**4**	**6**	**3/2**
800	$800x^3 + 9x$	$u(x)^5 + 1$	8	14	7/4
873	$873x^3 + 969x^2 + 379x + 53$	$u(x)^7 + 1$	4	6	3/2

We succeeded to rediscover a family which has $\mathrm{lc}\,(u) = 9$ by Freeman et al.

Conclusion

The method of the indeterminate coefficients and the factorization of cyclotomic polynomial gives us a chance to find more families of curves. Our experiments [1, 2] use the curves constructed from our results to assess the performance of several kinds of pairings.

References

[1] Antonio, C.A., Tanaka, S., Nakamula, K.: Comparing implementation effi ciency of ordinary and squared pairings. Cryptology ePrint Archive: 2007/457 (2007). http://eprint.iacr.org/2007/457/.

[2] Antonio, C.A., Tanaka, S., Nakamula, K.: Implementing cryptographic pairings over curves of embedding degrees 8 and 10. Cryptology ePrint Archive: 2007/426 (2007). http://eprint.iacr.org/2007/426/.

[3] Brezing, F., Weng, A.: Elliptic curves suitable for pairing based cryptography. Designs, Code and Cryptography **37**(1) (2005) 133–141.

[4] Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive: 2006/372 (2006). http://eprint.iacr.org/2006/372/.

[5] Galbraith, S., McKee, J., Valença, P.: Ordinary abelian varieties having small embedding degree. In: Workshop on Mathematical Problems and Techniques in Cryptology, Barcelona, CRM (2005) 29–45.

[6] Tanaka, S., Nakamula, K.: More constructing pairing-friendly elliptic curves for cryptography. arXiv e-print report 0711.1942. http://arxiv.org/abs/0711.1942.

† **Address for correspondence: Department of Mathematics and Infomation Sciences, Tokyo Metropolitan University, 1-1 Minami Osawa, Hachioji-shi, Tokyo, 192-0397 Japan**