Pairing-friendly Hyperelliptic Curves of Type $y^2 = x^5 + ax$

Mitsuru Kawazoe and Tetsuya Takahashi

Faculty of Liberal Arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho Naka-ku Sakai Osaka 599-8531 Japan
{kawazoe, takahashi}@las.osakafu-u.ac.jp

Abstract. An explicit construction of pairing-friendly hyperelliptic curves with ordinary Jacobians was firstly given by D. Freeman. In this paper, we give other explicit constructions of pairing-friendly hyperelliptic curves. Our methods are based on the closed formulae for the order of the Jacobian of a hyperelliptic curve of type $y^2 = x^5 + ax$ over a finite prime field $\mathbb{F}_p$ which are given by E. Furukawa, M. Haneda, M. Kawazoe and T. Takahashi. We present two methods in this paper. One is an analogue of the Cocks-Pinch method and the other is a cyclotomic method. Our methods construct a pairing-friendly hyperelliptic curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$ whose Jacobian has a prescribed embedding degree with respect to some prime number ℓ. Curves constructed by the analogue of the Cocks-Pinch method satisfy $p \approx \ell^2$, whereas $p \approx \ell^4$ in Freeman's construction. Moreover, for the case of embedding degree 24, we can construct a cyclotomic family with $p \approx \ell^{3/2}$.

Keywords: pairing-based cryptography, hyperelliptic curves

1 Introduction

Pairing based cryptography is a new public key cryptographic scheme, which was proposed around 2000 by three important works due to Joux [11], Sakai, Ohgishi and Kasahara [16] and Boneh and Franklin [4]. In these last two papers, the authors constructed an identity-based encryption scheme by using the Weil pairing of elliptic curves. Pairing-based cryptosystem can be constructed by using the Weil or Tate pairing on abelian varieties over finite fields. In cryptography, abelian varieties obtained as Jacobians of hyperelliptic curves are often used. Suitable elliptic or hyperelliptic curves for pairing-based cryptography are called "pairing-friendly". For the case of elliptic curves, there are many results for constructing pairing-friendly elliptic curves: Miyaji, Nakabayashi and Takano [14], Cocks and Pinch [6], Brezing and Weng [5], Barreto and Naehrig [2], Scott and Barreto [17], Freeman, Scott and Teske [7] and so on. On the other hand, there are very few results for constructing pairing-friendly hyperelliptic curves. In particular, for an explicit construction of pairing-friendly hyperelliptic curves with ordinary Jacobians, the only known result is Freeman's construction [8].

In this paper, we give other explicit constructions of pairing-friendly hyperelliptic curves. We present two different methods in this paper. One is an analogue of the Cocks-Pinch method and the other is a cyclotomic method. Both methods are based on the closed formulae for the order of the Jacobian of a hyperelliptic curve of type $y^2 = x^5 + ax$ over a finite prime field $\mathbb{F}_p$ which are given by E. Furukawa, M. Haneda, M. Kawazoe and T. Takahashi [9], [12]. For a given embedding degree k, our methods construct a pairing-friendly hyperelliptic curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$ whose Jacobian has embedding degree k with respect to some prime number ℓ. Curves constructed by the analogue of the Cocks-Pinch method satisfy $p \approx \ell^2$, whereas $p \approx \ell^4$ in Freeman's construction. Moreover, when the embedding degree equals 24, we can construct a cyclotomic family with $p \approx \ell^{3/2}$.

2 Definition and Basic Facts on Pairing Based Cryptography

In this section, we recall pairing based cryptography using abelian varieties over finite fields. For the simplicity, we describe only for the case of abelian varieties over finite prime fields in the following. We remark that all facts we state in this section hold for abelian varieties over finite fields. Let p be a prime, $K := \mathbb{F}_p$ a finite field with p elements and A an abelian variety defined over K. The finite abelian group of K-rational points of A and its order are denoted by $A(K)$ and $\#A(K)$, respectively. Assume that $A(K)$ has a subgroup G of a large prime order. Let ℓ be the order of G. We denote by $A[\ell]$ the group of ℓ-torsion points of $A(\overline{K})$ where $\overline{K}$ is an algebraic closure of K.

For a positive integer ℓ coprime to the characteristic of K, the Weil pairing is a non-degenerate bilinear map

$$e_\ell : A[\ell] \times A[\ell] \to \mu_\ell \subset \hat{K}^*$$

where μ_ℓ is the group of ℓth roots of unity in $\overline{K}^*$ and $\hat{K}$ is the smallest field extension of K contains μ_ℓ.

The key idea of pairing based cryptography is based on the fact that the subgroup G of prime order ℓ is embedded to the multiplicative group μ_ℓ via the Weil pairing or some other pairing map. The extension degree of the field extension $\hat{K}/K$ is called the *embedding degree* of E with respect to ℓ. The embedding degree with respect to ℓ equals the smallest positive integer k such that ℓ divides $p^k - 1$.

When A is an elliptic curve, $\hat{K}$ is the field extension of K generated by coordinates of all ℓ-torsion points [1]. For the case of $\dim A \geq 2$, the following result is known:

Proposition 1 ([8]). *Let A be an abelian variety over $\mathbb{F}_p$, $\chi(t)$ the characteristic polynomial of pth power Frobenius map of A. For a prime number $\ell \nmid p$ and*

a positive integer k, suppose the following hold:

$$\chi(1) \equiv 0 \pmod{\ell}$$
$$\Phi_k(p) \equiv 0 \pmod{\ell}$$

where Φ_k is the kth cyclotomic polynomial. Then A has the embedding degree k with respect to ℓ. Furthermore, if $k > 1$ then $A(\mathbb{F}_{p^k})$ contains two linearly independent ℓ-torsion points.

In pairing based cryptography, the following conditions must be satisfied to make a system secure:

- the order ℓ of a prime order subgroup of $A(K)$ should be large enough so that solving a discrete logarithm problem on the group is computationally infeasible and
- the order p^k of the field $\mathbb{F}_{p^k}$ should be large enough so that solving a discrete logarithm problem on the multiplicative group $\mathbb{F}_{p^k}^*$ is computationally infeasible.

Moreover for an efficient implementation of a pairing based cryptosystem, the following are important:

- the embedding degree k should be appropriately small and
- the ratio $\log_2 p / \log_2 \ell$ should be appropriately small.

For an abelian variety of dimension g, the above ratio $g \log_2 p / \log_2 \ell$ is denoted by ρ.

Abelian varieties satisfying the above four conditions are called "pairing-friendly". Hyperelliptic curves whose Jacobian varieties are pairing-friendly are also called "pairing-friendly". In practice, it is currently recommended that ℓ should be larger than 2^{160} and p^k should be larger than 2^{1024}.

3 Formulae for the order of the Jacobian of hyperelliptic curves of type $y^2 = x^5 + ax$

Our methods are based on the closed formulae for the order of the Jacobian of a hyperelliptic curve of type $y^2 = x^5 + ax$ over a finite prime field $\mathbb{F}_p$ which are given by E. Furukawa, M. Haneda, M. Kawazoe and T. Takahashi [9], [12].

First, we recall the relation between the order of Jacobian and the Frobenius map. Let p be an odd prime, $\mathbb{F}_p$ a finite field of order p and C a hyperelliptic curve of genus g defined over $\mathbb{F}_p$. Then the defining equation of C is given as $y^2 = f(x)$ where $f(x)$ is a polynomial in $\mathbb{F}_p[x]$ of degree $2g + 1$. Let J_C be the Jacobian variety of a hyperelliptic curve C. The Jacobian variety J_C is an abelian variety of dimension g. We denote the group of $\mathbb{F}_p$-rational points on J_C by $J_C(\mathbb{F}_p)$ and call it the Jacobian group of C. Let $\chi(t)$ be the characteristic polynomial of the pth power Frobenius endomorphism of C. We call $\chi(t)$ for C

the characteristic polynomial of C. Then, it is well-known that the order $\sharp J_C(\mathbb{F}_p)$ is given by

$$\sharp J_C(\mathbb{F}_p) = \chi(1).$$

In [9] and [12], the characteristic polynomial of a hyperelliptic curve of type $y^2 = x^5 + ax$ over a finite prime field $\mathbb{F}_p$ are determined as follows:

Theorem 1 ([9], [12]). *Let p be a prime, C a hyperelliptic curve defined by an equation $y^2 = x^5 + ax$ over $\mathbb{F}_p$, J_C the Jacobian variety of C and $\chi(t)$ the characteristic polynomial of pth power Frobenius map of C. Write p as $p = c^2 + 2d^2$ where c and d are integers and $c \equiv 1 \pmod 4$. Then the following hold:*

(1) If $p \equiv 1 \pmod 8$ and $a^{(p-1)/2} \equiv -1 \pmod p$, then $\chi(t) = t^4 + (-1)^f 4dt^3 + 8d^2t^2 + (-1)^f 4dpt + p^2$ where $f = (p-1)/8$ and $2d \equiv -(a^f + a^{3f})c \pmod p$.
(2) If $p \equiv 1 \pmod 8$ and $a^{(p-1)/4} \equiv -1 \pmod p$, or if $p \equiv 3 \pmod 8$ and $a^{(p-1)/2} \equiv -1 \pmod p$, then $\chi(t) = t^4 + (4c^2 - 2p)t^2 + p^2$.

Characteristic polynomials for other cases are also given in [9]. We remark that $\chi(t)$ for other cases are reducible over the ring $\mathbb{Z}$. The above theorem leads to the following formulae for the order of the Jacobian group $J_C(\mathbb{F}_p)$.

Corollary 1 ([9], [12]) *Let p be a prime and C a hyperelliptic curve defined by an equation $y^2 = x^5 + ax$ over $\mathbb{F}_p$. Write p as $p = c^2 + 2d^2$ where c and d are integers and $c \equiv 1 \pmod 4$.*

(1) If $p \equiv 1 \pmod 8$ and $a^{(p-1)/2} \equiv -1 \pmod p$, then $\sharp J_C(\mathbb{F}_p) = 1 + (-1)^f 4d + 8d^2 + (-1)^f 4dp + p^2$ where $f = (p-1)/8$ and $2d \equiv -(a^f + a^{3f})c \pmod p$.
(2) If $p \equiv 1 \pmod 8$ and $a^{(p-1)/4} \equiv -1 \pmod p$, or if $p \equiv 3 \pmod 8$ and $a^{(p-1)/2} \equiv -1 \pmod p$, then $\sharp J_C(\mathbb{F}_p) = 1 + 4c^2 - 2p + p^2$.

4 Analogue of the Cocks-Pinch method

By using the formulae given in Corollary 1, we obtain the following theorems:

Theorem 2. *For a given positive integer k, execute the following procedure:*

(1) Let ℓ be a prime such that $\mathrm{LCM}(8, k) | (\ell - 1)$.
(2) Let α be a primitive kth root of unity in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, β a positive integer such that $\beta^2 \equiv -1 \pmod \ell$ and γ a positive integer such that $\gamma^2 \equiv 2 \pmod \ell$.
(3) Let c and d be integers such that

$$\begin{aligned} c &\equiv 1 \pmod 4, \\ c &\equiv (\alpha + \beta)(\gamma(\beta + 1))^{-1} \pmod \ell, \\ d &\equiv (\alpha\beta + 1)(2(\beta + 1))^{-1} \pmod \ell. \end{aligned}$$

If $p = c^2 + 2d^2$ is a prime satisfying $p \equiv 1 \pmod 8$, then for an integer a satisfying

$$a^{(p-1)/2} \equiv -1 \pmod p$$
$$2(-1)^{(p-1)/8} d \equiv (a^{(p-1)/8} + a^{3(p-1)/8})c \pmod p,$$

the Jacobian group $J_C(\mathbb{F}_p)$ of a hyperelliptic curve C defined by $y^2 = x^5 + ax$ over $\mathbb{F}_p$ has a subgroup of order ℓ and the embedding degree of J_C with respect to ℓ is k.

Theorem 3. *For a given positive integer k, execute the following procedure:*

(1) , (2) are as in Theorem 2.
(3) Let c and d be integers such that

$$c \equiv 1 \pmod 4,$$
$$c \equiv 2^{-1}(\alpha - 1)\beta \pmod \ell,$$
$$d \equiv (\alpha + 1)(2\gamma)^{-1} \pmod \ell.$$

If $p = c^2 + 2d^2$ is a prime satisfying $p \equiv 1, 3 \pmod 8$, take an integer δ satisfying $\delta^{(p-1)/2} \equiv -1 \pmod p$ and set an integer a as

$$a = \delta^2 \quad \text{when } p \equiv 1 \pmod 8,$$
$$a = \delta \quad \text{when } p \equiv 3 \pmod 8.$$

Then the Jacobian group $J_C(\mathbb{F}_p)$ of a hyperelliptic curve C defined by $y^2 = x^5 + ax$ over $\mathbb{F}_p$ has a subgroup of order ℓ and the embedding degree of J_C with respect to ℓ is k.

Remark 1. Then condition $k|(\ell - 1)$ means that a primitive kth root of unity are contained in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. The condition $8|(\ell - 1)$ means that square roots of -1 and 2 are contained in $(\mathbb{Z}/\ell\mathbb{Z})^\times$.

Theorem 2 and 3 give an analogue of the Cocks-Pinch method for a hyperelliptic curve of type $y^2 = x^5 + ax$. We call curves obtained by Theorem 2 "Type I", and curves obtained by Theorem 3 "Type II".

We emphasize that our analog of the Cocks-Pinch method does not require the CM method for constructing explicit curves. Constructing explicit curves using the CM method is a heavy part of Freeman's construction. Moreover, we remark that $p \approx \ell^2$ (i.e. $\rho \approx 4$) in our construction, whereas $p \approx \ell^4$ (i.e. $\rho \approx 8$) in Freeman's construction.

5 Result of search for pairing-friendly hyperelliptic curves: the analogue of the Cocks-Pinch method

In Table 1, we show the number of pairing-friendly hyperelliptic curves of Type I, II for $4 \leq k \leq 36$ obtained by using our method.

k	Type I	Type II	
		$p \equiv 1 \pmod 8$	$p \equiv 3 \pmod 8$
4	35	76	64
5	45	43	36
6	33	52	31
7	47	40	33
8	140	171	165
9	37	31	44
10	31	42	48
11	36	34	35
12	83	69	71
13	44	42	39
14	34	38	40
15	42	43	38
16	149	163	169
17	33	42	46
18	29	39	48
19	32	42	44
20	78	75	81

k	Type I	Type II	
		$p \equiv 1 \pmod 8$	$p \equiv 3 \pmod 8$
21	34	29	30
22	35	50	34
23	64	46	45
24	141	152	124
25	33	47	32
26	43	35	36
27	41	45	31
28	82	90	69
29	31	40	36
30	32	31	30
31	29	26	37
32	143	161	164
33	32	30	35
34	34	36	32
35	50	50	42
36	72	63	80

Table 1. The number of pairing-friendly hyperelliptic curves for $4 \leq k \leq 36$ obtained by the analogue of the Cocks-Pinch method for $\ell \in [2^{160}, 2^{160} + 2^{20}]$ with $|c| < \ell$ and $|d| < 2\ell$.

Here we show examples of pairing-friendly hyperelliptic curves obtained by the analogue of the Cocks-Pinch method.
(Type I)

k =12

ℓ =1461501637330902918203684832716283019655933242609 (161 bits)

p =156944452196861903300139904833021704858667901724820580807966576\
6936583206099394434616202168385 7

a =243

ρ =3.91139

k =16

ℓ =1461501637330902918203684832716283019655932840529 (161 bits)

p =221088489434679844214516548152596018490081773707598735783339933\
5226916051626079472576037262113

a =3

ρ =3.87605

(Type II, $p \equiv 1 \pmod 8$)

k =12
ℓ =1461501637330902918203684832716283019655933051401 (161 bits)
p =1632602178388172958667084294365664861300872737133820054877337525\
375458952176252808357478789499 53
a =25
ρ =3.95363

k =16
ℓ =1461501637330902918203684832716283019655932635041 (161 bits)
p =6013300217687864234648174070831976672330956639931526918110147404\
996390188849261707653397583749 7
a =9
ρ =3.93562

(Type II, $p \equiv 3 \pmod 8$)

k =12
ℓ =1461501637330902918203684832716283019655933142121 (161 bits)
p =5200414358851436030207390198712837840574260460011915231054535741\
607784506438359115350808142 7667
a =2
ρ =3.933

k =16
ℓ =1461501637330902918203684832716283019655933261329 (161 bits)
p =1225507417189915284657440942525236908784564653725351434657747928\
373431071254461450714750780406 59
a =2
ρ =3.94846

6 Another construction: cyclotomic families

Here we give another construction of pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$. It is also based on the formulae given in Corollary 1, but it is a hyperelliptic version of cyclotomic families.

Cyclotomic families for the case of elliptic curves have been investigated by Brezing and Weng [5], Freeman, Scott and Teske [7] and some other researchers. In a cyclotomic family, a cyclotomic polynomial is used to set a prime ℓ as $\ell = \Phi_k(t)$ or $\ell = \Phi_{ck}(t)$ for some $c > 1$ where k is the embedding degree. Though a prime ℓ is not taken arbitrary, cyclotomic families have advantage that $\log_2 p/\log_2 \ell$ of obtained curves can be smaller than the one obtained by the analogue of the Cocks-Pinch method.

For a hyperelliptic curves of type $y^2 = x^5 + ax$, we require the condition that the embedding degree k is divisible by 8. Assume that the embedding degree k is divisible by 8 and $\ell - 1$ is divisible by k. Let α be a primitive kth root of unity modulo ℓ, β an integer such that $\beta^2 \equiv -1 \pmod{\ell}$ and γ an integer such that $\gamma^2 \equiv 2 \pmod{\ell}$. Then we have that $\beta = \pm\alpha^{k/4}$ and $\gamma = \pm\left(\alpha^{k/8} - \alpha^{3k/8}\right)$. Note that if $\gcd(k, h) = 1$, then α^h is also a primitive kth root of unity modulo ℓ.

6.1 A cyclotomic family of type I

From Theorem 2, we have

$$c = \frac{\alpha+\beta}{\beta\gamma+\gamma} = \frac{(\alpha+\beta)(\beta\gamma-\gamma)}{(\beta\gamma+\gamma)(\beta\gamma-\gamma)} = \frac{\alpha(\gamma-\beta\gamma)+(\gamma+\beta\gamma)}{4}$$
$$d = \frac{\alpha\beta+1}{2(\beta+1)} = \frac{(\alpha\beta+1)(-\beta)\beta(1-\beta)}{(2(1+\beta)(1-\beta)} = \frac{(\alpha-\beta)(\beta+1)}{4}.$$

Hence we obtain the following for curves of type I.

$$c = \begin{cases} \pm\frac{1}{4}\left(\alpha^{h+3k/8} - \alpha^{k/8}\right) & \text{when } \beta = \alpha^{k/4} \\ \pm\frac{1}{4}\left(\alpha^{h+k/8} - \alpha^{3k/8}\right) & \text{when } \beta = -\alpha^{k/4} \end{cases}$$
$$d = \begin{cases} \pm\frac{1}{4}\left(\alpha^h - \alpha^{k/4}\right)\left(\alpha^{k/4}+1\right) & \text{when } \beta = \alpha^{k/4} \\ \pm\frac{1}{4}\left(\alpha^h + \alpha^{k/4}\right)\left(-\alpha^{k/4}+1\right) & \text{when } \beta = -\alpha^{k/4}. \end{cases}$$

Let $\tilde{c}_i(t)$ and $\tilde{d}_i(t)$ for $i = 1, 2$ be polynomials of minimal degree satisfying the following condition:

$$\begin{aligned} \tilde{c}_1(t) &\equiv t^{h+3k/8} - t^{k/8} \mod \Phi_k(t) \\ \tilde{d}_1(t) &\equiv \left(t^h - t^{k/4}\right)\left(t^{k/4}+1\right) \mod \Phi_k(t) \\ \tilde{c}_2(t) &\equiv t^{h+k/8} - t^{3k/8} \mod \Phi_k(t) \\ \tilde{d}_2(t) &\equiv \left(t^h + t^{k/4}\right)\left(-t^{k/4}+1\right) \mod \Phi_k(t) \end{aligned}$$

Set polynomials $\tilde{p}_i(t)$ for $i = 1, 2$ as

$$\tilde{p}_i(t) = \tilde{c}_i(t)^2 + 2\tilde{d}_i(t)^2.$$

Since $c = \pm\tilde{c}_i(\alpha)/4$ and $d = \pm\tilde{d}_i(\alpha)/4$, we have

$$\tilde{p}_i(\alpha) = \tilde{c}_i(\alpha)^2 + 2\tilde{d}_i(\alpha)^2 = 16(c^2 + 2d^2) = 16p.$$

It is necessary for $p = c^2 + 2d^2$ being prime with $p \equiv 1 \pmod 8$ and $c \equiv 1 \pmod 4$ that $\tilde{p}_i(x)$ is irreducible, $\tilde{c}_i(j) \equiv 4 \pmod 8$ and $\tilde{d}_i(j) \equiv 0 \pmod 4$ for some $i = 1, 2$ and $0 \le j \le 7$. Note that the above condition is only necessary condition.

Searching suitable h which gives polynomials $\tilde{c}_i(t)$, $\tilde{d}_i(t)$ and $\tilde{p}_i(t)$ satisfying the above condition, we find the following for $k = 56$ and $k = 88$.

For $k = 56$, the following is found:

$$\begin{aligned}
h &= 15 \quad (t^h = t^{15}) \\
\tilde{c}_2(t) &= -2t^{21} + 2t^{22} \\
\tilde{d}_2(t) &= 1 + t + t^{14} + t^{15} \\
\tilde{p}_2(t) &= 1 + 2t + t^2 + 2t^{14} + 4t^{15} + 2t^{16} + t^{28} + 2t^{29} + t^{30} + 4t^{42} - 8t^{43} + 4t^{44}
\end{aligned}$$

Since $\Phi_{56}(t) = 1 - t^4 + t^8 - t^{12} + t^{16} - t^{20} + t^{24}$, it is expected that $p \approx \ell^{11/6}$. Actually, using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^{11/6}$ ($\rho \approx 11/3 = 3.667$). For example, we obtain the following curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$:

$$\begin{aligned}
a =& 16807 \\
t =& 17783 \\
\ell =& \Phi_{56}(t) \\
=& 1000277923068656865827189119874013991669139100253326573068816\backslash \\
& 1699826871536785155992184003939305985553619(339 \text{ bits}) \\
p =& 250099265879557406524307111682994614744774870053308144482663\backslash \\
& 0921859994292374132881840001627580847758991403586307212832793884\backslash \\
& 5930368310268742121685087183200859257243103525687050639140080\backslash \\
& 09 \\
\rho =& 3.655
\end{aligned}$$

For $k = 88$, the following is found:

$$\begin{aligned}
h &= 23 \quad (t^h = t^{23}) \\
\tilde{c}_2(t) &= -2t^{33} + 2t^{34} \\
\tilde{d}_2(t) &= 1 + t + t^{22} + t^{23} \\
\tilde{p}_2(t) &= 1 + 2t + t^2 + 2t^{22} + 4t^{23} + 2t^{24} + t^{44} + 2t^{45} + t^{46} + 4t^{66} - 8t^{67} + 4t^{68}
\end{aligned}$$

Since $\Phi_{88}(t) = 1 - t^4 + t^8 - t^{12} + t^{16} - t^{20} + t^{24} - t^{28} + t^{32} - t^{36} + t^{40}$, it is expected that $p \approx \ell^{17/10}$. Actually, using the above polynomials we obtain pairing-friendly

hyperelliptic curves of type I with $p \approx \ell^{17/10}$ ($\rho \approx 3.4$). For example, we obtain the following curve:

a =3
t =199
ℓ =$\Phi_{88}(t)$
=899752487733759802877368997803737754825362055306207413664214955\
0547320829320778021064171960 01(306 bits)
p =519485502753407483076493310086468610566323328319931376559714045\
2074879675662287514219520606507610498216123319723496588038721445\
4224196313410953197800422845660 1
ρ =3.387

Changing polynomial $\tilde{d}_i(t)$ as

$$\tilde{d}_1(t) = \left((t^h \mod \Phi_k(t)) - t^{k/4}\right)\left(t^{k/4}+1\right)$$
$$\tilde{d}_2(t) = \left((t^h \mod \Phi_k(t)) + t^{k/4}\right)\left(-t^{k/4}+1\right),$$

we find polynomials satisfying the condition for $k = 8$.

$$\begin{aligned} h &= 1 \quad (t^h = t) \\ \tilde{c}_1(t) &= 2 + 2t \\ \tilde{d}_1(t) &= (t - t^2)(1 + t^2) \\ \tilde{p}_1(t) &= 4 + 8t + 5t^2 - 2t^3 + 3t^4 - 4t^5 + 3t^6 - 2t^7 + t^8 \end{aligned}$$

Since $\Phi_8(t) = 1 + t^4$, it is expected that $p \approx \ell^2$.

Actually, using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^2$ ($\rho \approx 4$).

a =13
t =1099511628193
ℓ =$\Phi_8(t)/2$ = 730750819774027608217118960060276298985251336001(160 bits)
p =266998380299721022208485052678564002078078952591552189819810720885\
0440889507772121638755455925409
ρ =3.987

6.2 A cyclotomic family of type II

From Theorem 3, we have

$$c = \frac{\beta(\alpha-1)}{2}$$
$$d = \frac{\alpha+1}{2\gamma} = \frac{\gamma(\alpha+1)}{4}.$$

Hence we obtain the following for curves of type II.

$$c = \pm\frac{\alpha^{k/4}\left(\alpha^h - 1\right)}{2}$$
$$d = \pm\frac{\left(\alpha^{k/8} - \alpha^{3k/8}\right)\left(\alpha^h + 1\right)}{4}.$$

Let $\tilde{c}(t)$ and $\tilde{d}(t)$ are polynomials of minimal degree satisfying

$$\tilde{c}(t) \equiv t^{k/4}\left(t^h - 1\right) \mod \Phi_k(t)$$
$$\tilde{d}(t) \equiv \left(t^{k/8} - t^{3k/8}\right)\left(t^h + 1\right) \mod \Phi_k(t)$$

and set a polynomial $\tilde{p}(t)$ as

$$\tilde{p}(t) = 2\tilde{c}(t)^2 + \tilde{d}(t)^2.$$

Since $c = \pm\tilde{c}(\alpha)/2$ and $d = \pm\tilde{d}(\alpha)/4$, we have

$$\tilde{p}(\alpha) = 2\tilde{c}(\alpha)^2 + \tilde{d}(\alpha)^2 = 8(c^2 + 2d^2) = 8p.$$

It is necessary for $p = c^2 + 2d^2$ being prime with $p \equiv 1, 3 \pmod 8$ and $c \equiv 1 \pmod 4$ that $\tilde{p}(x)$ is irreducible, $\tilde{c}(j) \equiv 2 \pmod 4$ and $\tilde{d}(j) \equiv 0 \pmod 4$ for $0 \leq j \leq 3$. Note that the above condition is only necessary condition.

Searching suitable h which gives polynomials $\tilde{c}(t)$, $\tilde{d}(t)$ and $\tilde{p}(t)$ satisfying the above condition, we find the following for $k = 24$.

$$\begin{aligned}
h &= 11 \\
t^h &\equiv -t^3 + t^7 \pmod{\Phi_{24}(t)} \\
\tilde{c}(t) &= -t^5 - t^6 \\
\tilde{d}(t) &= -1 + t - t^2 + t^3 + t^4 - t^5 \\
\tilde{p}(t) &= 1 - 2t + 3t^2 - 4t^3 + t^4 + 2t^5 - 3t^6 + 4t^7 - t^8 - 2t^9 + 3t^{10} + 4t^{11} + 2t^{12}
\end{aligned}$$

Since $\Phi_{24}(t) = 1 - t^4 + t^8$, it is expected that $p \approx \ell^{3/2}$.

Actually, using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^{3/2}$ ($\rho \approx 3$). For example, we obtain the following curve:

$$\begin{aligned}
a =& 2 \\
t =& 1049085 \\
\ell =& \Phi_{24}(t) = 146718682892712893651454019963417202720810469000 1 \text{(161 bits)} \\
p =& 444292483637841082598410015665493978083277385484222711267571600 8\backslash \\
& 30352907 \\
\rho =& 2.975
\end{aligned}$$

7 Conclusion

In this paper, we give two different methods constructing explicit pairing-friendly hyperelliptic curves based on the formulae for the order of the Jacobian of a hyperelliptic curve of type $y^2 = x^5 + ax$. One is an analogue of the Cocks-Pinch method and the other is a cyclotomic method. Our methods construct a pairing-friendly hyperelliptic curve $y^2 = x^5 + ax$ over a prime field $\mathbb{F}_p$ whose Jacobian has a prescribed embedding degree with respect to some prime number ℓ. We obtain pairing-friendly hyperelliptic curves with $p \approx \ell^2$ for arbitrary embedding degree by using the analogue of the Cocks-Pinch method, whereas $p \approx \ell^4$ in Freeman's construction. Moreover, by using the cyclotomic method, we obtain pairing-friendly hyperelliptic curves with $p \approx \ell^{3/2}$ for the embedding degree 24.

References

1. R. Balasubramanian and N. Koblitz, *Neal The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology **11** (1998), no. 2, pp. 141–145.
2. P.S.L.M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, In Proceedings of SAC 2005 Workshop on Selected Areas in Cryptography, LNCS3897, pp. 319–331. Springer, 2006.
3. I.-F. Blake, G. Seroussi and N.-P. Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.
4. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM Journal of Computing, **32**(3) (2003), pp. 586–615.
5. F. Brezing and A. Weng, *Elliptic curves suitable for pairing based cryptography*, Design, Codes and Cryptography, **37** (2005), pp. 133–141.
6. C. Cocks and R. G. E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, Unpublished manuscript, 2001.
7. D. Freeman, M. Scott and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, Cryptology ePrint Archive, Report 2006/372, 2006 http://eprint.iacr.org/.
8. D. Freeman, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*, In: T. Takagi, T. Okamoto, E. Okamoto and T. Okamoto (eds.) Pairing-Based Cryptography – Pairing 2007, LNCS 4575, pp. 152–176, Springer, 2007.
9. E. Furukawa, M. Kawazoe and T. Takahashi, *Counting Points for Hyperelliptic Curves of Type $y^2 = x^5 + ax$ over Finite Prime Fields*, In: M. Matsui and R. Zuccherato (eds.) Selected Areas in Cryptography (SAC 2003), LNCS 3006, pp. 26–41, Springer, 2004.
10. S. Galbraith, J. McKee and P. Valença, *Ordinary abelian varieties having small embedding degree*, Finite Fields and Their Applications, **13** (2007), pp. 800–814.
11. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, In Algorithmic Number Theory Symposium ANTS-IV, volume 1838 of Lecture Notes in Computer Science, pp. 385–393. Springer-Verlag, 2000. Full version: Journal of Cryptology **17** (2004), 263–276.
12. M. Haneda, M. Kawazoe and T. Takahashi, *Suitable Curves for Genus-4 HCC over Prime Fields: Point Counting Formulae for Hyperelliptic Curves of Type $y^2 = x^{2k+1} + ax$*, In: L. Gaires, G. F. Italiano, L. Monteiro, C. Palamidessi and M. Yung (eds.) Automata, Languages and Programming (ICALP2005), LNCS 3580, pp. 539–550, Springer, 2005.

13. M. Kawazoe, R. Sakaeyama and T. Takahashi, *Pairing-friendly Hyperelliptic Curves of type* $y^2 = x^5 + ax$, In 2008 Symposium on Cryptography and Information Security (SCIS 2008), Miyazaki, Japan, 2008.
14. A. Miyaji, M. Nakabayashi and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Transactions on Fundamentals **E84-A**(5) (2001), pp. 1234–1243.
15. K. Rubin and A. Silverberg, *Supersingular abelian varieties in cryptology*, In: M. Yung (ed.) CRYPTO 2002, LNCS 2442, pp. 336–353, Springer, 2002.
16. R. Sakai, K. Ohgishi and M. Kasahara, *Cryptosystem based on pairing*, In 2000 Symposium on Cryptography and Information Security (SCIS 2000), Okinawa, Japan, 2000.
17. M. Scott and P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography **38** (2006), pp. 209–217.