Pairing-friendly Hyperelliptic Curves with Ordinary Jacobians 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 with ordinary Jacobians based on the closed formulae for the order of the Jacobian of a hyperelliptic curve of type $y^2 = x^5 + ax$. We present two methods in this paper. One is an analogue of the Cocks-Pinch method and the other is a cyclotomic method. By using these methods, we construct a pairing-friendly hyperelliptic curve $y^2 = x^5 + ax$ over a finite prime field $\mathbb{F}_p$ whose Jacobian is ordinary and simple over $\mathbb{F}_p$ with a prescribed embedding degree. Moreover, the analogue of the Cocks-Pinch produces curves with $\rho \approx 4$ and the cyclotomic method produces curves with $3 \leq \rho \leq 4$.

Keywords: pairing-based cryptography, hyperelliptic curves

1 Introduction

Pairing-based cryptography was proposed around 2000 by three important works due to Joux [15], Sakai, Ohgishi and Kasahara [19] 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. The key idea is that for an abelian variety of dimension g defined over a finite field $\mathbb{F}_q$, its subgroup of prime order ℓ is embedded into the multiplicative group of some extension field $\mathbb{F}_{q^k}$ as the multiplicative group of ℓth roots of unity via the Weil pairing or some other pairing map. The ratio $g \log q / \log \ell$ and the extension degree k are important for the construction of pairing-based cryptosystem. This ratio $g \log q / \log \ell$ is denoted by ρ, and the extension degree k is called the embedding degree with respect to ℓ.

In cryptography, abelian varieties obtained as Jacobians of hyperelliptic curves are often used. The Jacobian variety of a hyperelliptic curve of genus g is an abelian variety of dimension g. Note that an elliptic curve is a hyperelliptic curve of genus one and also an abelian variety of dimension one. Suitable abelian varieties for pairing-based cryptography are called "pairing-friendly". Moreover, hyperelliptic curves whose Jacobians are suitable for pairing-based cryptography are also called "pairing-friendly". One of important conditions for being pairing-friendly is that the embedding degree should be in a appropriate size. It is known that supersingular abelian varieties have small embedding degree (cf. [18]). For example, for the case of dimension one (i.e. elliptic curves) it is at most 6, and for the case of dimension two it is at most 12. Hence, if we need a larger embedding degree, we need ordinary abelian varieties. Another important condition is that the value of ρ should be small. By the definition of ρ, its theoretical minimum is $\rho \approx 1$ for abelian varieties of any dimension.

For the case of elliptic curves, there are many results for constructing pairing-friendly ordinary elliptic curves: Miyaji, Nakabayashi and Takano [17], Cocks and Pinch [7], Brezing and Weng [5], Barreto and Naehrig [2], Scott and Barreto [20], Freeman, Scott and Teske [10] and so on. Using the above methods, we can construct pairing-friendly elliptic curves with $\rho \approx 1$ for the embedding degree less than or equal to 6 (cf. [17]), $\rho \approx 2$ (cf. [7]) or $1 < \rho < 2$ for many embedding degrees (cf. [10]). On the other hand, there are very few results for explicit constructions of pairing-friendly ordinary abelian varieties of higher dimension. The only known results are Freeman [8], Freeman, Stevenhagen and Streng [11] and Freeman [9]. The ρ-values in these results are $4 \leq \rho \leq 8$ for dimension two (one family with $\rho \approx 4$ is given in [9]) and $\rho \approx 12$ for dimension three.

In this paper, we give other explicit constructions of pairing-friendly hyperelliptic curves with ordinary Jacobians. 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. Kawazoe and T. Takahashi [12] and M. Haneda, M. Kawazoe and T. Takahashi [14]. By using these methods, for a given embedding degree k, we construct a pairing-friendly hyperelliptic curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$. Though Jacobians of curves constructed by our methods are not absolutely simple, our methods produce curves whose Jacobians are simple over defining fields with smaller ρ-values than previously obtained. In fact, the analogue of the Cocks-Pinch method produces curves with $\rho \approx 4$ for arbitrary embedding degree and the cyclotomic method produces curves with $3 \leq \rho \leq 4$. In particular, when the embedding degree equals 24, we obtain a cyclotomic family with $\rho \approx 3$.

2 Definition and Basic Facts on Hyperelliptic Curves and Pairing-Based Cryptography

In this section, we recall some basic facts on hyperelliptic curves and pairing-based cryptography.

2.1 Hyperelliptic curves and their Jacobians

First, we recall the relation between the order of the Jacobian and the Frobenius map. Let p be an odd prime and $\mathbb{F}_q$ a finite field with q elements where $q = p^r$ for a positive integer r.

Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$. Then the defining equation of C is given as $y^2 = f(x)$ where $f(x)$ is a polynomial in $\mathbb{F}_q[x]$ of degree $2g+1$ or $2g+2$. Let J_C be the Jacobian variety of a hyperelliptic curve C. The Jacobian variety J_C is an abelian variety of dimension g. Note that if $g = 1$ (i.e. C is an elliptic curve), then C is isomorphic to J_C. The finite abelian group of $\mathbb{F}_q$-rational points on J_C is denoted by $J_C(\mathbb{F}_q)$ and called the Jacobian group of C. Let $\chi(t)$ be the characteristic polynomial of the qth power Frobenius endomorphism of C. We call $\chi(t)$ for C the characteristic polynomial of C. Then, it is well-known that the order $\#J_C(\mathbb{F}_q)$ is given by

$$\#J_C(\mathbb{F}_q) = \chi(1).$$

2.2 Pairing-based cryptography

Here we recall pairing-based cryptography using Jacobian varieties of hyperelliptic curves over finite fields. Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$. Assume that $J_C(\mathbb{F}_q)$ has a subgroup G of a large prime order. Let ℓ be the order of G. The group of ℓ-torsion points of $J_C(\overline{\mathbb{F}_q})$ is denote by $J_C[\ell]$ where $\overline{\mathbb{F}_q}$ is an algebraic closure of $\mathbb{F}_q$ and $J_C(\overline{\mathbb{F}_q})$ is a group of $\overline{\mathbb{F}_q}$-rational points on J_C.

For a positive integer ℓ coprime to the characteristic of $\mathbb{F}_q$, the Weil pairing is a non-degenerate bilinear map

$$e_\ell : J_C[\ell] \times J_C[\ell] \to \mu_\ell \subset \mathbb{F}_{q^k}^\times$$

where μ_ℓ is the multiplicative group of ℓth roots of unity in $\overline{\mathbb{F}_q}^\times$ and $\mathbb{F}_{q^k}$ is the smallest field extension of $\mathbb{F}_q$ containing 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 group μ_ℓ via the Weil pairing or some other pairing map. The extension degree k of the field extension $\mathbb{F}_{q^k}/\mathbb{F}_q$ is called the *embedding degree* of J_C with respect to ℓ. The embedding degree with respect to ℓ equals the smallest positive integer k such that ℓ divides $q^k - 1$. In other words, q is a primitive kth root of unity modulo ℓ.

When C is an elliptic curve and k is the embedding degree of C with respect to ℓ, $\mathbb{F}_{q^k}$ is a field generated by coordinates of all ℓ-torsion points [1]. For the higher genus case, we refer to the following result for an abelian varieties due to Freeman [8].

Proposition 1 ([8]). *Let A be an abelian variety over a finite field $\mathbb{F}_q$, $\chi(t)$ the characteristic polynomial of the qth power Frobenius map of A. For a prime* *number $\ell \not| q$ and a positive integer k, suppose the following hold:*

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

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

In pairing-based cryptography, for the Jacobian variety J_C defined over $\mathbb{F}_q$, the following conditions must be satisfied to make a system secure:

- the order ℓ of a prime order subgroup of $J_C(\mathbb{F}_q)$ should be large enough so that solving a discrete logarithm problem on the group is computationally infeasible and
- the order q^k of the field $\mathbb{F}_{q^k}$ should be large enough so that solving a discrete logarithm problem on the multiplicative group $\mathbb{F}_{q^k}^\times$ 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 $\rho = g \log_2 q / \log_2 \ell$ should be appropriately small.

Jacobian 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 q^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 were given by E. Furukawa, M. Kawazoe and T. Takahashi [12] and M. Haneda, M. Kawazoe and T. Takahashi [14]. Due to the results of [12] and [14], the characteristic polynomial of a hyperelliptic curve of type $y^2 = x^5 + ax$ over $\mathbb{F}_p$ are determined completely as follows. For the proof of the following theorem, see [14] for the proof of (1) and see [12] for others.

Theorem 1 ([12], [14]). *Let p be an odd 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 the pth power Frobenius map of C. Then the following holds: (In the following, c and d denote integers such that $p = c^2 + 2d^2$ and $c \equiv 1 \pmod{4}$. Note that such c and d exist if and only if $p \equiv 1, 3 \pmod{8}$.)*

(1) *If* $p \equiv 1 \pmod 8$ *and* $a^{(p-1)/2} \equiv -1 \pmod p$, *then* $\chi(t) = t^4 - 4dt^3 + 8d^2t^2 - 4dpt + p^2$ *where* $f = (p-1)/8$ *and* $2(-1)^f d \equiv (a^f + a^{3f})c \pmod p$.
(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* $\chi(t) = t^4 + (4c^2 - 2p)t^2 + p^2$.
(3) *If* $p \equiv 1 \pmod{16}$ *and* $a^{(p-1)/8} \equiv 1 \pmod p$, *or if* $p \equiv 9 \pmod{16}$ *and* $a^{(p-1)/8} \equiv -1 \pmod p$, *then* $\chi(t) = (t^2 - 2ct + p)^2$.
(4) *If* $p \equiv 1 \pmod{16}$ *and* $a^{(p-1)/8} \equiv -1 \pmod p$, *or if* $p \equiv 9 \pmod{16}$ *and* $a^{(p-1)/8} \equiv 1 \pmod p$, *then* $\chi(t) = (t^2 + 2ct + p)^2$.
(5) *If* $p \equiv 3 \pmod 8$ *and* $a^{(p-1)/2} \equiv 1 \pmod p$, *then* $\chi(t) = (t^2 + 2ct + p)(t^2 - 2ct + p)$.
(6) *If* $p \equiv 5 \pmod 8$ *and* $a^{(p-1)/4} \equiv 1 \pmod p$, *or if* $p \equiv 7 \pmod 8$, *then* $\chi(t) = (t^2 + p)^2$.
(7) *If* $p \equiv 5 \pmod 8$ *and* $a^{(p-1)/4} \equiv -1 \pmod p$, *then* $\chi(t) = (t^2 - p)^2$.
(8) *If* $p \equiv 5 \pmod 8$ *and* $a^{(p-1)/2} \equiv -1 \pmod p$, *then* $\chi(t) = t^4 + p^2$.

Remark 1. For the convenience in the following argument, we replaced d in [14] by $(-1)^{f+1}d$ in Theorem 1 (1).

We remark that $\chi(t)$ for the case (3)-(7) are reducible over the ring $\mathbb{Z}$. Moreover, the case (6), (7) and (8) are the supersingular case. In the following we restrict our interest to the case (1) and (2), because these are the only cases that J_C is a simple ordinary Jacobian over $\mathbb{F}_p$. The above theorem leads to the closed formulae for the order of the Jacobian group $J_C(\mathbb{F}_p)$ by using $\#J_C(\mathbb{F}_p) = \chi(1)$.

4 Analogue of the Cocks-Pinch method

By using the formulae given in Theorem 1 (1) and (2), we obtain an analogue of the Cocks-Pinch method for hyperelliptic curves $y^2 = x^5 + ax$. Let χ be $1 - 4d + 8d^2 - 4dp + p^2$ or $1 + 4c^2 - 2p + p^2$. Then we can construct pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$ over $\mathbb{F}_p$ if we find integers c, d and odd primes p, ℓ satisfying the following conditions: (Note that $p \equiv 1, 3 \pmod 8$.)

$$\begin{aligned} \chi &\equiv 0 \pmod \ell \\ \Phi_k(p) &\equiv 0 \pmod \ell \\ p &= c^2 + 2d^2 \quad \text{with } c \equiv 1 \pmod 4. \end{aligned}$$

The first condition means that the order of the Jacobian of a constructed curve has a subgroup of prime order ℓ. The second condition means that the embedding degree with respect to ℓ of the Jacobian of a constructed curve is k. Note that the second condition implies that p is a primitive kth root of unity modulo ℓ and therefore it implies that $\ell - 1$ must be divisible by k. Moreover, in both cases of Theorem 1 (1) and (2), square roots of -1 and 2 are required to be contained in the ring $\mathbb{Z}/\ell\mathbb{Z}$ so that integers c and d satisfying the above conditions exist. Hence $\ell - 1$ is required to be divisible by 8.

According to Theorem 1 (1) and (2), we have 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

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

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.

Proof. First note that the condition $k|(\ell-1)$ implies that a primitive kth root of unity is contained in the ring $\mathbb{Z}/\ell\mathbb{Z}$ and the condition $8|(\ell-1)$ implies that square roots of -1 and 2 are contained in $\mathbb{Z}/\ell\mathbb{Z}$.

Let ℓ be a prime as in (1) and let α, β and γ be as in (2). Substituting $c \equiv (\alpha+\beta)(\gamma(\beta+1))^{-1} \pmod{\ell}$ and $d \equiv (\alpha\beta+1)(2(\beta+1))^{-1} \pmod{\ell}$ into $p = c^2+2d^2$, we have

$$p \equiv \left((\alpha+\beta)^2+(\alpha\beta+1)^2\right)\left(2(\beta+1)^2\right)^{-1} \equiv (4\alpha\beta)(4\beta)^{-1} \equiv \alpha \pmod{\ell}.$$

Since α is a primitive kth root of unity in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, we have $\Phi_k(p) \equiv 0 \pmod{\ell}$.

Next we check the condition on the order of the Jacobian. From the condition $d \equiv (\alpha\beta+1)(2(\beta+1))^{-1} \pmod{\ell}$, we have

$$1-2d \equiv (2d-\alpha)\beta \pmod{\ell}.$$

Substituting this into the formula $\#J_C(\mathbb{F}_p) = 1-4d+8d^2-4dp+p^2$ and using $p \equiv \alpha \pmod{\ell}$, we have

$$\#J_C(\mathbb{F}_p) = (1-2d)^2+(2d-p)^2 \equiv -(2d-\alpha)^2+(2d-p)^2 \equiv 0 \pmod{\ell}$$

Thus the Jacobian variety of a constructed curve $y^2 = x^5+ax$ over $\mathbb{F}_p$ has a subgroup of order ℓ and its embedding degree 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

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

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

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

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.

Proof. As in the proof of Theorem 2, substituting $c \equiv 2^{-1}(\alpha - 1)\beta \pmod \ell$ and $d \equiv (\alpha + 1)(2\gamma)^{-1} \pmod \ell$ into $p = c^2 + 2d^2$, we have

$$p \equiv 4^{-1}\left((\beta(\alpha - 1))^2 + (\alpha + 1)^2\right) \equiv \alpha \pmod \ell.$$

In particular, we have $\Phi_k(p) \equiv 0 \pmod \ell$.

Next we check the condition on the order of the Jacobian. Substituting $c \equiv 2^{-1}(\alpha - 1)\beta \pmod \ell$ into the formula $\#J_C(\mathbb{F}_p) = 1 + 4c^2 - 2p + p^2$ and using $p \equiv \alpha \pmod \ell$, we have

$$\#J_C(\mathbb{F}_p) = 4c^2 + (p - 1)^2 \equiv -(\alpha - 1)^2 + (p - 1)^2 \equiv 0 \pmod \ell.$$

Thus the Jacobian variety of constructed curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$ has a subgroup of order ℓ and its embedding degree with respect to ℓ is k. □

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”.

Since our method based on the closed formulae of the order of the Jacobian, we can construct a pairing-friendly hyperelliptic curve in a very short time. For the running time of our algorithm, see Section 5. Moreover, we remark that $\rho \approx 4$ in our construction. This ρ-value is smaller than previously obtained. (Recently, Freeman [9] proposed another method to construct pairing-friendly hyperelliptic curves and obtained one family with $\rho \approx 4$ for the embedding degree 5.)

We remark one more thing. As is shown in [12], Jacobians for curves of type I and II are isogenous to the product of two elliptic curves over the extension field which contains $a^{1/4}$.

Lemma 1 ([12]). *Let p be an odd prime and C a hyperelliptic curve defined by $y^2 = x^5 + ax$, $a \in \mathbb{F}_p^\times$ and $\mathbb{F}_q = \mathbb{F}_{p^r}$, $r \geq 1$. If $a^{1/4} \in \mathbb{F}_q$, then J_C is isogenous to the product of the following two elliptic curves E_1 and E_2 over $\mathbb{F}_q$:*

$$E_1 : Y^2 = X(X^2 + 4a^{1/4}X - 2a^{1/2}),$$
$$E_2 : Y^2 = X(X^2 - 4a^{1/4}X - 2a^{1/2}).$$

By the above lemma, we have the following: (1) Jacobian for type I splits over $\mathbb{F}_{p^4}$, (2) Jacobian for type II with $p \equiv 3 \pmod 8$ splits over $\mathbb{F}_{p^4}$, and (3) Jacobian for type II with $p \equiv 1 \pmod 8$ splits over $\mathbb{F}_{p^2}$.

Let C be a pairing-friendly hyperelliptic curve of type I or II with embedding degree k with respect to ℓ. We write the value $2\log_2 p/\log_2 \ell$ for C as $\rho(C)$. If C is of type I, or of type II with $p \equiv 3 \pmod 8$, then E_1 or E_2 is a pairing-friendly elliptic curve over $\mathbb{F}_{p^4}$ with embedding degree $k/4$ with $\rho = \log_2 p^4/\log_2 \ell = 2\rho(C)$. If C is of type II with $p \equiv 1 \pmod 8$, then E_1 or E_2 is a pairing-friendly elliptic curve over $\mathbb{F}_{p^2}$ with embedding degree $k/2$ with $\rho = \log_2 p^2/\log_2 \ell = \rho(C)$.

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

In Table 1 and Table 2, we show the number of pairing-friendly hyperelliptic curves of Type I, II for $7 \leq k \leq 36$ obtained by using our method.

These tables show that we can find many pairing-friendly hyperelliptic curves with ordinary Jacobians by using our method. All computations have been done by Mathematica 6 on Mac OS X (1.66GHz Intel Core Duo with 1GB memory). For each k, the running time of the search is on average 90 seconds in Table 1 and 170 seconds in Table 2, respectively.

k	Type I	Type II		k	Type I	Type II	
		$p \equiv 1 \pmod 8$	$p \equiv 3 \pmod 8$			$p \equiv 1 \pmod 8$	$p \equiv 3 \pmod 8$
7	47	40	33	22	35	50	34
8	140	171	165	23	64	46	45
9	37	31	44	24	141	152	124
10	31	42	48	25	33	47	32
11	36	34	35	26	43	35	36
12	83	69	71	27	41	45	31
13	44	42	39	28	82	90	69
14	34	38	40	29	31	40	36
15	42	43	38	30	32	31	30
16	149	163	169	31	29	26	37
17	33	42	46	32	143	161	164
18	29	39	48	33	32	30	35
19	32	42	44	34	34	36	32
20	78	75	81	35	50	50	42
21	34	29	30	36	72	63	80

Table 1. The number of pairing-friendly hyperelliptic curves 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 only one example of pairing-friendly hyperelliptic curves of type I with $k = 16$ obtained by the analogue of the Cocks-Pinch method. For examples of other type and other k, see Appendix.

k	Type I	Type II		k	Type I	Type II	
		$p \equiv 1 \pmod 8$	$p \equiv 3 \pmod 8$			$p \equiv 1 \pmod 8$	$p \equiv 3 \pmod 8$
7	10	7	11	22	15	17	26
8	60	55	52	23	21	13	17
9	16	13	18	24	70	67	61
10	11	18	21	25	21	12	24
11	15	18	18	26	26	17	12
12	26	38	43	27	16	13	17
13	16	19	12	28	34	25	26
14	6	13	18	29	17	14	10
15	16	13	18	30	15	13	14
16	55	59	81	31	6	10	17
17	9	16	19	32	64	59	47
18	14	14	10	33	13	11	22
19	18	28	26	34	14	12	9
20	30	27	29	35	13	11	13
21	15	7	18	36	29	40	28

Table 2. The number of pairing-friendly hyperelliptic curves obtained by the analogue of the Cocks-Pinch method for $\ell \in [2^{256}, 2^{256} + 2^{20}]$ with $|c| < \ell$ and $|d| < 2\ell$.

$$
\begin{aligned}
k &= 16 \quad \text{(Type I)} \\
\ell &= 1461501637330902918203684832716283019655932840529 \text{ (161 bits)} \\
\alpha &= 81844167457893182397317622245688612690934307989 \\
\beta &= 195562276567303320541291199692793181706146839127 \\
\gamma &= 759224753535341599938962978629340510421546983720 \\
c &= 44377152517514522371933429191352073808466251009 \\
d &= 10989841417965341398489085346020251473054265996 \\
p &= 2210884894346798442145165481525960184900817737075987357833399335\backslash \\
&\quad 226916051626079472576037262113 \text{ (311 bits)} \\
a &= 3 \\
\#J_C(\mathbb{F}_p) &= 48880120160508541101232277959462765729571682125818741808\backslash \\
&\quad 2910733116855655035560868542777327696362024706637568420695212814\backslash \\
&\quad 3139938957120301819393955637481342467018816294397128800020723098\backslash \\
&\quad 722 \text{ (621 bits)} \\
\rho &= 3.88
\end{aligned}
$$

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 Theorem 1 (1) and (2), 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 [10] 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 and t is a positive integer. Though a prime ℓ is not taken arbitrarily, cyclotomic families have an advantage that the ρ-value of obtained curves can be smaller than the one obtained by 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

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

Hence we obtain the following for curves of type I:

$$c = \begin{cases} \pm\frac{1}{2}\left(\alpha^{h+3k/8} - \alpha^{k/8}\right) & \text{when } \beta = \alpha^{k/4} \\ \pm\frac{1}{2}\left(\alpha^{h+k/8} - \alpha^{3k/8}\right) & \text{when } \beta = -\alpha^{k/4} \end{cases}$$

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

where h is a positive integer such that $\gcd(k,h) = 1$. Here we consider all choices of primitive kth roots of unity modulo ℓ.

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

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

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

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

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

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

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, $\tilde{c}_i(j) \equiv 2 \pmod 4$ and $\tilde{d}_i(j) \equiv 0 \pmod 4$ for some $i = 1, 2$ and $0 \le j \le 3$.

Searching suitable h which gives polynomials $\tilde{c}_i(t)$, $\tilde{d}_i(t)$ and $\tilde{p}_i(t)$ satisfying the above condition and $\rho < 4$, we find the following pairs of (k, h) for $k \le 96$.

k	h	$t^h \pmod{\Phi_k(t)}$	$\tilde{c}(t)$	$\tilde{d}(t)$	ρ
16	5	t^5	$-x^6 + x^7$	$1 + x + x^4 + x^5$	3.5
16	13	$-t^5$	$-x^6 - x^7$	$1 - x + x^4 - x^5$	3.5
32	9	t^9	$-x^{12} + x^{13}$	$1 + x + x^8 + x^9$	3.25
32	25	$-t^9$	$-x^{12} - x^{13}$	$1 - x + x^8 - x^9$	3.25
56	15	t^{15}	$-x^{21} + x^{22}$	$1 + x + x^{14} + x^{15}$	3.67
56	43	$-t^{15}$	$-x^{21} - x^{22}$	$1 - x + x^{14} - x^{15}$	3.67
64	17	t^{17}	$-x^{24} + x^{25}$	$1 + x + x^{16} + x^{17}$	3.125
64	49	$-t^{17}$	$-x^{24} - x^{25}$	$1 - x + x^{16} - x^{17}$	3.125
80	21	t^{21}	$-x^{30} + x^{31}$	$1 + x + x^{20} + x^{21}$	3.875
80	61	$-t^{21}$	$-x^{30} - x^{31}$	$1 - x + x^{20} - x^{21}$	3.875
88	23	t^{23}	$-x^{33} + x^{34}$	$1 + x + x^{22} + x^{23}$	3.4
88	67	$-t^{23}$	$-x^{33} - x^{34}$	$1 - x + x^{22} - x^{23}$	3.4

Table 3. A list of $(k, h, t^h \pmod{\Phi_k(t)}, \rho)$ which gives the best ρ-value less than 4 for each k

Here we show examples of pairing-friendly curves for k in Table 3.

For $k = 16$, the following is found:

$$\begin{aligned}
h &= 5 \quad (t^h = t^5)\\
\tilde{c}_2(t) &= -t^6 + t^7\\
\tilde{d}_2(t) &= 1 + t + t^4 + t^5\\
\tilde{p}_2(t) &= 1 + 2t + t^2 + 2t^4 + 4t^5 + 2t^6 + t^8 + 2t^9 + t^{10} + 2t^{12} - 4t^{13} + 2t^{14}
\end{aligned}$$

Since $\Phi_{16}(t) = 1 + t^8$, it is expected that $p \approx \ell^{7/4}$. Actually, using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^{7/4}$ ($\rho \approx 7/2 = 3.5$). For example, we obtain the following curve $y^2 = x^5 + ax$

over $\mathbb{F}_p$:

$$\begin{aligned}
a =&161051\\
t =&1051667\\
\ell =&\Phi_{16}(t)/2\\
=&748162569063423099637274524451199719643782405521(160\text{ bits})\\
p =&506098015003692075403451446275653325150097426016349218406968953\backslash\\
&2354388303076095790281\\
\rho =&3.497
\end{aligned}$$

For $k = 32$, the following is found:

$$\begin{aligned}
h &= 9 \quad (t^h = t^9)\\
\tilde{c}_2(t) &= -t^{12} + t^{13}\\
\tilde{d}_2(t) &= 1 + t + t^8 + t^9\\
\tilde{p}_2(t) &= 1 + 2t + t^2 + 2t^8 + 4t^9 + 2t^{10} + t^{16} + 2t^{17} + t^{18} + 2t^{24} - 4t^{25} + 2t^{26}
\end{aligned}$$

Since $\Phi_{32}(t) = 1 + t^{16}$, it is expected that $p \approx \ell^{13/8}$. Actually, using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^{13/8}$ ($\rho \approx 13/4 = 3.25$). For example, we obtain the following curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$:

$$\begin{aligned}
a =&243\\
t =&1491\\
\ell =&\Phi_{32}(t)/2\\
=&298271871767803247714167829477325151003146936379 21(168\text{ bits})\\
p =&808678670399443987243514553224709749323983686347431095112442873\backslash\\
&74478774931 87018297\\
\rho =&3.246
\end{aligned}$$

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

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

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 $\mathbb{F}_p$:

$$\begin{aligned}
a =&16807\\
t =&17783\\
\ell =&\Phi_{56}(t)\\
=&1000277923068656865827189119874013991669139100253326573068816 1\backslash\\
&69982687153678515599218400393930598555361 (339 \text{ bits})\\
p =&25009926587955740652430711168299461474477487005330814448266309\backslash\\
&21859994292374132881840001627580847758991403586307212832793884\backslash\\
&59303683102687421216850871832008592572431035256870506391400800 9\\
\rho =&3.655
\end{aligned}$$

For $k = 64$, the following is found:

$$\begin{aligned}
h &= 17 \quad (t^h = t^{17})\\
\tilde{c}_2(t) &= -t^{24} + t^{25}\\
\tilde{d}_2(t) &= 1 + t + t^{16} + t^{17}\\
\tilde{p}_2(t) &= 1 + 2t + t^2 + 2t^{16} + 4t^{17} + 2t^{18} + t^{32} + 2t^{33} + t^{34} + 2t^{48} - 4t^{49} + 2t^{50}
\end{aligned}$$

Since $\Phi_{64}(t) = 1 + t^{32}$, it is expected that $p \approx \ell^{25/16}$. Actually, using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^{25/16}$ ($\rho \approx 25/8 = 3.125$). For example, we obtain the following curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$:

$$\begin{aligned}
a =&7\\
t =&527\\
\ell =&\Phi_{32}(t)/2\\
=&62648357772543703301005438973620924004221846867043603752647141\backslash\\
&1841278385528854236092161 (289 \text{ bits})\\
p =&30677575045546872361962043882902056514095176791575855579833087\backslash\\
&82578378747763956641725522035763587621193146183433232810845021\backslash\\
&729737057201\\
\rho =&3.122
\end{aligned}$$

For $k = 80$, the following is found:

$$\begin{aligned}
h &= 61 \quad (t^h \equiv -t^{21} \mod \Phi_{80}(t))\\
\tilde{c}_2(t) &= -t^{30} - t^{31}\\
\tilde{d}_2(t) &= 1 - t + t^{20} - t^{21}\\
\tilde{p}_2(t) &= 1 - 2t + t^2 + 2t^{20} - 4t^{21} + 2t^{22} + t^{40} - 2t^{41} + t^{42} + 2t^{60} + 4t^{61} + 2t^{62}
\end{aligned}$$

Since $\Phi_{80}(t) = 1 - t^8 + t^{16} - t^{24} + t^{32}$, it is expected that $p \approx \ell^{31/16}$. Actually, using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^{31/16}$ ($\rho \approx 31/8 = 3.875$). For example, we obtain the following curve $y^2 = x^5 + ax$ over $\mathbb{F}_p$:

$$
\begin{aligned}
a =& 3 \\
t =& 5921 \\
\ell =& \Phi_{80}(t) \\
=& 520765199653252359060781545446544766276885220146241360852311891\backslash \\
& 95835873073892609505663600513142013994178583633631762731521 \\
& (402 \text{ bits}) \\
p =& 1934552319915167927168223517545934132908259523562071146324542 7\backslash \\
& 05469079909207934329770211444887059634614931641804025676952280\backslash \\
& 69843534955787163283893883369970172935464105827397521204178068\backslash \\
& 951851135706224480242884499312400755231373077921 \\
\rho =& 3.865
\end{aligned}
$$

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

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

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:

$$
\begin{aligned}
a =& 3 \\
t =& 199 \\
\ell =& \Phi_{88}(t) \\
=& 89975248773375980287736899780373775482536205530620741366421495\backslash \\
& 0547320829320778021064171960 01(306 \text{ bits}) \\
p =& 51948550275340748307649331008646861056632332831993137655971404\backslash \\
& 20748796756622875142195206065076104982161233197234965880387214\backslash \\
& 422419631341095319780042284566 01 \\
\rho =& 3.387
\end{aligned}
$$

For some k, there is no h for which the necessary condition on the polynomials $\tilde{p}(t)$, $\tilde{c}_i(t)$ and $\tilde{d}_i(t)$ is satisfied. In such case, changing a choice of polynomials $\tilde{c}_i(t)$ and $\tilde{d}_i(t)$, we might obtain h for which the necessary condition is satisfied.

For example, when $k = 8$, taking a polynomial $\tilde{d}_i(t)$ without modulo $\Phi_k(t)$, we obtain the following with $h = 1$ ($t^h = t$) which gives $\rho \approx 4$:

$$\tilde{c}_1(t) = 1 + t, \quad \tilde{d}_1(t) = (t - t^2)(1 + t^2),$$
$$\tilde{p}_1(t) = 2 + 4t + 3t^2 - 2t^3 + 3t^4 - 4t^5 + 3t^6 - 2t^7 + t^8.$$

Since $\Phi_8(t) = 1 + t^4$, it is expected that $p \approx \ell^2$. Using the above polynomials we obtain pairing-friendly hyperelliptic curves of type I with $p \approx \ell^2$ ($\rho \approx 4$) when t is odd and $\ell = \Phi_8(t)/2$. We show an example of such curves:

a =13
t =1099511628193
ℓ =$\Phi_8(t)/2$ = 730750819774027608217118960060276298985251336001(160 bits)
p =2669983802997210222084850526785640020780789525915521898198107208 8\
044088950777212163875545592540 9
ρ =3.987.

6.2 A cyclotomic family of type II

From Theorem 3, we have

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

Hence we obtain the following for curves of type II:

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

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

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

As in Section 6.1, 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 $0 \leq j \leq 3$.

Searching suitable h which gives polynomials $\tilde{c}(t)$, $\tilde{d}(t)$ and $\tilde{p}(t)$ satisfying the above condition and $\rho < 4$, we find $(k, h) = (24, 11)$, $(24, 23)$. Here we show the detail only for $(k,h)=(24,11)$:

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

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 curves.

$$\begin{aligned}
a =&2\\
t =&1049085\\
\ell =&\Phi_{24}(t)=1467186828927128936514540199634172027208104690001 (161 \text{ bits})\\
p =&44429248363784108259841001566549397808327738548422271126757160083\backslash\\
&30352907 \quad (p\equiv 3 \mod 8)\\
\rho =&2.975.
\end{aligned}$$

$$\begin{aligned}
a =&4\\
t =&1053485\\
\ell =&\Phi_{24}(t)=1517144162644737377550369518008477083193100900001 (161 \text{ bits})\\
p =&46717662922982833531526759133069240351124562691144117778868158688\backslash\\
&14707307 \quad (p\equiv 1 \mod 8)\\
\rho =&2.975.
\end{aligned}$$

7 Conclusion

In this paper, we present the analogue of the Cocks-Pinch method and the cyclotomic method by which we can construct pairing-friendly hyperelliptic curves of type $y^2=x^5+ax$ with ordinary Jacobians for a prescribed embedding degree. These methods produce pairing-friendly hyperelliptic curves with small ρ-values. More precisely, we obtain pairing-friendly hyperelliptic curves with $\rho\approx 4$ for arbitrary embedding degree by using the analogue of the Cocks-Pinch method and with $3\le\rho\le 4$ by using the cyclotomic method.

Constructing pairing-friendly ordinary abelian varieties of higher dimension with smaller ρ-values are still in progress. The current best ρ-values are still large compared with elliptic curves. Thus the problem is still open.

References

1. R. Balasubramanian and N. Koblitz, *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. G. Cardona and E. Nart, *Zeta Function and Cryptographic Exponent of Supersingular Curves of Genus 2*, In: T. Takagi, T. Okamoto, E. Okamoto and T. Okamoto (eds.) Pairing-Based Cryptography – Pairing 2007, LNCS 4575, pp. 132–151, Springer, 2007.
7. C. Cocks and R. G. E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, Unpublished manuscript, 2001.
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. D. Freeman, *A generalized Brezing-Weng method for constructing pairing-friendly ordinary abelian varieties*, preprint, 2008.
10. 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/.
11. D. Freeman, P. Stevenhagen and M. Streng, *Abelian varieties with prescribed embedding degree*, In: A.-J. Poorten and A. van der Stein (eds.) Algorithmic Number Theory, LNCS 5011, pp. 60–73, Springer, 2008.
12. 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.
13. S. Galbraith, J. McKee and P. Valença, *Ordinary abelian varieties having small embedding degree*, Finite Fields and Their Applications, **13** (2007), pp. 800–814.
14. 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.
15. 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.
16. 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.
17. 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.
18. K. Rubin and A. Silverberg, *Supersingular abelian varieties in cryptology*, In: M. Yung (ed.) CRYPTO 2002, LNCS 2442, pp. 336–353, Springer, 2002.
19. R. Sakai, K. Ohgishi and M. Kasahara, *Cryptosystem based on pairing*, In: 2000 Symposium on Cryptography and Information Security (SCIS 2000), Okinawa, Japan, 2000.

20. M. Scott and P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography **38** (2006), pp. 209–217.
21. Wolfram Research, Inc., *Mathematica*, Version 6.0, Champaign, IL (2007).

Appendix. Examples of pairing-friendly hyperelliptic curves obtained by using the analogue of the Cocks-Pinch method

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

$k = 24$ (Type I)
$\ell = 1461501637330902918203684832716283019655932607833$ (161 bits)
$p = 1847897864407894552288699809460676006668888779550356111198433454\backslash$
$9731951205842130479887529417649$
$a = 243$
$\rho = 3.914$

$k = 16$ (Type I)
$\ell = 1157920892373161954235709850086879078532699846656405640394575840\backslash$
07913130160457 (257 bits)
$p = 1481146215498410360424614463856750745944411770248019012076220169\backslash$
$0729222878658709908471226638555684580055423116081360950900530695\backslash$
$8769615381413525533112616\,9$
$a = 7$
$\rho = 3.975$

$k = 16$ (Type II, $p \equiv 1 \pmod 8$)
$\ell = 1461501637330902918203684832716283019655932635041$ (161 bits)
$p = 6013300217687864234648174070831976672330956639931526918110147404\backslash$
$9963901888492617076533975837497$
$a = 9$
$\rho = 3.936$

$$k = 24 \quad (\text{Type II}, p \equiv 1 \pmod 8)$$
$$\ell = 1461501637330902918203684832716283019655932813801 \text{ (161 bits)}$$
$$p = 19459929216494310500309443280237553321879095830173414397910189906700500204899677291876916119281$$
$$a = 9$$
$$\rho = 3.915$$

$$k = 16 \quad (\text{Type II}, p \equiv 3 \pmod 8)$$
$$\ell = 1461501637330902918203684832716283019655933261329 \text{ (161 bits)}$$
$$p = 12255074171899152846574409425252369087845646537253514346577479283734310712544614507147507804065 9$$
$$a = 2$$
$$\rho = 3.948$$

$$k = 24 \quad (\text{Type II}, p \equiv 3 \pmod 8)$$
$$\ell = 1461501637330902918203684832716283019655933525833 \text{ (161 bits)}$$
$$p = 38949214428803064509409444699452395623042236376391478617673172338025473134423535136743780780093 9$$
$$a = 2$$
$$\rho = 3.969$$