FINDING COMPOSITE ORDER ORDINARY ELLIPTIC CURVES USING THE COCKS-PINCH METHOD

D. BONEH, K. RUBIN, AND A. SILVERBERG

Abstract. We apply the Cocks-Pinch method to obtain pairing-friendly composite order groups with prescribed embedding degree associated to ordinary elliptic curves, and we show that new security issues arise in the composite order setting.

1. Introduction

Elliptic curve cryptography [22, 24] and efficient computations of pairings associated to elliptic curves [25] have given rise in recent years to pairing-based cryptography, an important emerging field in public key cryptography. A powerful new idea in pairing-based cryptography is to use composite order groups instead of prime order ones. This idea, due to Boneh, Goh, and Nissim, was used for partial homomorphic encryption in [5], and since then it has been used in a number of other important applications including non-interactive zero-knowledge proofs, group and ring signatures, searching encrypted data, and fully collusion-resistant traitor tracing [20, 6, 9, 10, 7, 21, 29, 12].

Initially, composite groups used in pairing-based cryptography were based on supersingular elliptic curves as constructed in [5]. In this paper we show that it is possible to obtain composite groups from ordinary (i.e., non-supersingular) elliptic curves, however some care must be taken to avoid potential security problems.

Waters [31] pointed out that for certain applications, composite order bilinear groups based on supersingular curves are insufficient; for example, constructions that use composite order groups that rely on the Symmetric External Diffie-Hellman (SXDH) assumption [2] cannot use supersingular curves. The assumption says roughly that Decision Diffie-Hellman (DDH) is hard in both of the groups being paired. Note that if there is an efficient isomorphism from a group G_1 to a group G_2, and an efficiently computable non-degenerate pairing whose domain is $G_1 \times G_2$, then DDH is easy in G_1. Because of this, it is not known how to use supersingular elliptic curves to construct pairings satisfying the SXDH assumption; ordinary elliptic curves such as the ones constructed in §5 and §6 here seem to be necessary for such applications.

In this paper we show that while the Cocks-Pinch method for finding pairing-friendly elliptic curves carries over essentially verbatim to the setting of composite groups, this setting introduces some security issues that do not occur in the original Cocks-Pinch construction.

This material is based upon work supported by the National Science Foundation under grants DMS-0457481, DMS-0757807, CNS-0831004, CNS-0331640, and CNS-0832820 and the National Security Agency under grants H98230-05-1-0044 and H98230-07-1-0039.

The goal is to produce, on input k, a "suitable" composite integer N and an elliptic curve E over a finite field $\mathbb{F}_q$ such that $|E(\mathbb{F}_q)|$ is a multiple of N and the embedding degree of E with respect to N is k. This leads to pairings $e : G_1 \times G_2 \to \boldsymbol{\mu}_N$ where G_1 is the cyclic group generated by a point of order N in $E(\mathbb{F}_q)$, G_2 is a cyclic subgroup of $E(\mathbb{F}_{q^k})$ of order N, and $\boldsymbol{\mu}_N \subseteq \mathbb{F}_{q^k}^\times$ is the cyclic group of N-th roots of unity in $\bar{\mathbb{F}}_q^\times$.

We slightly modify the Cocks-Pinch method, adapting it to the case where we are searching for an elliptic curve of embedding degree k with a point whose order N, rather than being a large prime, is a product of primes congruent to 1 modulo k. For many applications of composite order pairing groups, N is a product of two or three distinct primes. Our constructions are sufficiently general to allow N to have an arbitrary number of prime factors where some factors may be repeated.

Next is a definition of embedding degree that applies to possibly composite divisors N of the group order $|E(\mathbb{F}_q)|$. However, what we construct are elliptic curves with embedding degree k with respect to every prime divisor of N, which is a stronger statement.

Definition 1.1. *If q is a prime power, E is an elliptic curve over $\mathbb{F}_q$, and N is a divisor of the group order $|E(\mathbb{F}_q)|$ such that N is relatively prime to q, then the* embedding degree *of E with respect to N is the order of q in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e., the embedding degree is the smallest positive integer k such that $q^k - 1$ is divisible by N.*

In §2 we recall the Boneh-Goh-Nissim construction of supersingular composite order pairing-friendly groups. In §3 we recall the method of Cocks and Pinch.

In §4 we construct pairing-friendly groups of embedding degree 1 from ordinary elliptic curves. We note that the SXDH assumption can be false for certain subgroups of these curves by a result in Charles' [13], as discussed in Section 4.1.

In §§5–6 we construct pairing-friendly groups of order N and embedding degree k from ordinary elliptic curves, using the CM method for an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. We give two versions. In the first version of the algorithm, we choose D so that $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, where ζ_r will always denote a primitive r-th root of unity. In the second version of the algorithm, $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$. Thus $\sqrt{-D} = f(\zeta_k)$ for some polynomial $f(x) \in \mathbb{Z}[x]$. We let $s = f(X) \pmod N$, where X has order k modulo each prime power divisor of N. This method gives a square root s of $-D \pmod N$ that (provably) does not leak information about the factorization of N. We therefore recommend the second version of the algorithm, rather than the first.

In §7 we give the theorems that prove that the algorithms do what we claim. In §8 we give further remarks that address issues of security and efficiency. In §9 we give some details of our implementations of the algorithms.

The construction for embedding degree 1 is the simplest. In this case there are no restrictions on the prime divisors of N, and no information is leaked about N's factorization.

2. Supersingular composite order groups

We first recall the construction of supersingular composite order groups from §2.1 of [5].

Step 1: Choose a square-free integer $N > 3$ that is not divisible by 3.

Step 2: Find the smallest positive integer w such that $q = 3wN - 1$ is a prime number.

Step 3: The elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_q$ has $q + 1 = 3wN$ points over $\mathbb{F}_q$ and embedding degree 2 with respect to N.

3. Cocks-Pinch method

We next recall the Cocks-Pinch algorithm for finding pairing-friendly elliptic curves. See Algorithm IX.4 on p. 211 of [19] or slide 22 of [17].

Input: a positive integer k; k will be the embedding degree,
a prime p congruent to 1 modulo k.

Output: a prime q;
an elliptic curve E over $\mathbb{F}_q$ of embedding degree k with respect to p.

Step 1: Choose an integer X that has order k in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Step 2: Choose a positive integer D (the CM discriminant) so that $-D$ is a square modulo p.

Step 3: Fix $s \pmod p$ such that $s^2 \equiv -D \pmod p$.

Step 4: Take an integer Y congruent to $\pm(X-1)s^{-1} \pmod p$.

Step 5: Let $q = ((X+1)^2 + DY^2)/4$.

Step 6: If q is a prime number, use the CM method to obtain an elliptic curve E over $\mathbb{F}_q$ with trace $t = X + 1$, so

$$|E(\mathbb{F}_q)| = q + 1 - t = q - X.$$

Since $q \equiv X \pmod p$, the group order $|E(\mathbb{F}_q)|$ is divisible by p, and k is the embedding degree for E over $\mathbb{F}_q$ with respect to p.

If q is not a prime number, start again with a different X.

Recall that for the CM method [1], the input is a prime q of the form $(a^2+Db^2)/4$, and the output is an elliptic curve E over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = q + 1 - a$.

4. Ordinary composite order groups with embedding degree 1

To construct ordinary composite order groups with embedding degree 1, do the following (which is similar to what is done in the prime order case in Example 6.17 of [18], which follows §6 of [23]).

Input: a positive integer N (e.g., an RSA modulus).

Output: a prime q;
an elliptic curve E over $\mathbb{F}_q$ such that $E[N] \subseteq E(\mathbb{F}_q)$.

Step 1: Choose a positive integer D suitable for the CM method.

Step 2: Let

$$q = \begin{cases} 1 + DN^2 & \text{if } D \equiv 0, 4 \pmod 6, \\ 1 + 4DN^2 & \text{if } D \equiv 1, 3 \pmod 6, \\ (1-N)^2 + DN^2 & \text{if } D \equiv 5 \pmod 6, \\ (1-2N)^2 + DN^2 & \text{if } D \equiv 2 \pmod 6. \end{cases}$$

Step 3: If q is prime, use the CM method to obtain an elliptic curve over $\mathbb{F}_q$ that has $q - 1 = DN^2$ points when $D \equiv 0, 4 \pmod 6$, $q - 1 = 4DN^2$ points when $D \equiv 1, 3 \pmod 6$, $q - 1 + 2N = (D+1)N^2$ points when $D \equiv 5 \pmod 6$, and $q - 1 + 4N = (D+4)N^2$ points when $D \equiv 2 \pmod 6$. If q is not prime, start over with a new D and/or a new N.

Remarks 4.1.

(i) Since $N|(q-1)$, the embedding degree is 1.
(ii) In this case, the CM method produces an elliptic curve E such that $E[N] \subseteq E(\mathbb{F}_q)$. The pairing is computed entirely in the ground field $\mathbb{F}_q$, which is optimal from an efficiency standpoint.
(iii) No information about N's factorization is leaked, since knowledge of N's factors was not used.
(iv) When N and D are odd, then $1 + DN^2$ is even. When $D \equiv 2 \pmod 3$, then every integer of the form $1 + DY^2$ is divisible by 3, so is not prime (unless $D = 2$ and $Y = \pm 1$). This is why we needed to adjust q, as above, in these cases.
(v) More simply, instead of Steps 1 and 2, one could take the smallest positive integer D such that $q := 1 + DN^2$ is prime. (This forces D to be 0 or 4 (mod 6). Also D is potentially large, and is not even known to exist.) Given N, such a construction would provide elliptic curves E with $E[N] \subseteq E(\mathbb{F}_q)$ for which q is about as small as possible.

Example 4.2. Let $D = 16$, and let N be any positive integer such that $q := 1 + 16N^2$ is prime. Then $y^2 = x^3 - x$ has $q - 1 = 16N^2$ points over $\mathbb{F}_q$, and has embedding degree 1 with respect to every divisor of N.

4.1. **Distortion maps.**

Definition 4.3. *Suppose E is an elliptic curve over a finite field $\mathbb{F}_q$, p is a prime that does not divide q, and C is an order p subgroup of E. A* distortion map *for C is an endomorphism f of E such that $f(C) \not\subseteq C$.*

When distortion maps exist for a pairing-based group, then the Decision Diffie-Hellman Problem is easy for that group. The next result, which is part of Theorem 2.1(2) of [13], shows that distortion maps are common when the embedding degree is 1.

Proposition 4.4 ([13])**.** *Suppose p and q are distinct primes, and E is an ordinary elliptic curve over $\mathbb{F}_q$ such that $E[p] \subseteq \mathbb{F}_q$. Let $\mathcal{O} = \mathrm{End}(E)$, an order in an imaginary quadratic field K. Suppose $p \nmid [\mathcal{O}_K : \mathcal{O}]\mathrm{Disc}(K)$. If p is inert in $K/\mathbb{Q}$, then there are distortion maps for every order p subgroup of $E[p]$. If p is split in $K/\mathbb{Q}$, then every subgroup of $E[p]$ of order p has distortion maps except for the the two (distortion-free) eigenspaces of the action of $\sqrt{-D}$ on $E[p]$.*

Proposition 4.4 has consequences for the Subgroup Decision Assumption on the curves produced above. Recall that the Subgroup Decision Assumption [5], commonly used in pairing-based cryptography, says that given as input $N = p_1p_2$ and a description of a cyclic group G_N of order N, no efficient algorithm can distinguish the uniform distribution on G_N from the uniform distribution on its order p_1 subgroup. We discuss the implications of Proposition 4.4 to the Subgroup Decision Assumption in the following remarks.

Remark 4.5. Suppose that E, q, and N are as in the algorithm above. Then $\mathrm{End}(E) = \mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-D})$. Now suppose that $N = p_1p_2$ where p_1 is split in $K/\mathbb{Q}$, p_2 is inert, and $\gcd(p_1p_2, 2D) = 1$. Let G_{p_1} be one of the two order p_1 subgroups of $E(\mathbb{F}_q)$ that by Proposition 4.4 has no distortion maps and let G_{p_2} be any order p_2 subgroup of $E(\mathbb{F}_q)$. Let $G_N = G_{p_1} + G_{p_2} \subset E[N] \subseteq E(\mathbb{F}_q)$. By

Proposition 4.4, G_{p_2} has distortion maps $f \in \mathrm{End}(E)$. Since G_{p_1} has no distortion maps, every distortion map f for G_{p_2} maps G_{p_1} to itself. As a result, if e_N is the Weil pairing, then $e_N(P, f(P)) = 1$ if $P \in G_{p_1}$, but $e_N(P, f(P)) \neq 1$ if $P \in G_N \setminus G_{p_1}$. This observation gives an immediate algorithm to solve the Subgroup Decision Problem in G_N.

Remark 4.6. The attack on the Subgroup Decision Problem described in Remark 4.5 applies whenever one chooses a subgroup $G_N \subseteq E(\mathbb{F}_q)$ of order $N = p_1 p_2$ such that its order p_1 subgroup is one of the two subgroups of $E[p_1]$ that has no distortion maps while the order p_2 subgroup of G_N has distortion maps. If one chooses G_N by choosing its generator to be a random point of E of order N, then the probability that its order p_1 subgroup is one of the two distortion-free subgroups of $E[p_1]$ is negligible. Consequently the attack from Remark 4.5 is unlikely to apply to a subgroup G_N chosen this way. Nevertheless, to provably avoid the attack we recommend that one always choose N and D so that all of the prime divisors of N are inert in $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$. This will ensure that the attack in Remark 4.5 does not apply to any order N subgroup of E.

Remark 4.7. Alternatively, to avoid the attack in Remark 4.5 one could choose a pair of distortion-free order N cyclic subgroups of $E[N]$, as below (and in [13]). This has the advantage that one expects DDH to be hard in such groups. Suppose $\gcd(N, 2D) = 1$ and all the prime divisors of N are split in $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$. Using the factorization of N, compute a square root s of $-D \pmod N$. Let $P \in E(\mathbb{F}_q)$ be a point of order N, let σ be the endomorphism $\sqrt{-D} \in \mathrm{End}(E)$, let $P_- = (\sigma - s)P$, let $P_+ = (\sigma + s)P$, and let $G_\pm$ be the subgroup generated by $P_\pm$. Since $(\sigma - s)(\sigma + s)E[N] = 0$, we have $(\sigma \mp s)P_\pm = 0$. Then $G_+ \cap G_- = 0$, and G_+ and G_- are distortion-free. If both $P_\pm$ have exact order N (each has order N with probability $\varphi(N)/N \geq 1 - \sum_{p|N} \frac{1}{p}$; otherwise, repeat with a different P of order N), then G_+ and G_- generate $E[N]$ and are the two desired subgroups. One expects SXDH to hold for the pair (G_+, G_-). This construction leaks P_+, P_-, sP_+, and sP_-.

Example 4.8. In the setting of Example 4.2, we have $\mathrm{End}(E) = \mathbb{Z}[i]$. Suppose p is a prime divisor of N. If $\alpha^2 \equiv -1 \pmod q$, then $f(x, y) = (-x, \alpha y)$ is a distortion map for each of the $p + 1$ subgroups of order $p \equiv 3 \pmod 4$, and for all but two of the $p + 1$ subgroups of order $p \equiv 1 \pmod 4$. Note that f is efficiently computable, without knowing anything about the factorization of N. As discussed in the previous two remarks, while we recommend choosing N so that all its prime factors are congruent to $3 \pmod 4$ to avoid the attack on the Subgroup Decision Problem described in Remark 4.5, if one wants SXDH to hold one could instead take N so that all its prime factors are $1 \pmod 4$ and use distortion-free subgroups as constructed in Remark 4.7.

5. Ordinary composite order groups, Version I

We generalize the Cocks-Pinch method to the case where p is replaced by a composite N. In this version there is no restriction on the input k.

Input: a positive integer k; k will be the embedding degree,
distinct primes $p_1, \ldots, p_r$ congruent to 1 modulo k, and
positive integers $\alpha_1, \ldots, \alpha_r$.
Let $N = \prod_{i=1}^{r} p_i^{\alpha_i}$.

Output: a prime q;
an elliptic curve E over $\mathbb{F}_q$ of embedding degree k with respect to N.

Step 1: Choose an integer X that has order k in $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ for all i.

Step 2: Choose a positive square-free integer D (the CM discriminant) so that $-D$ is a square modulo N. If k is a multiple of 4, choose D so that D is not a divisor of $k/4$. If k is not a multiple of 4, choose D so that either D is not a divisor of k or $D \not\equiv 3 \pmod 4$.

Step 3: Fix any $s \pmod N$ such that $s^2 \equiv -D \pmod N$.

Step 4: Take an integer Y congruent to $\pm(X-1)s^{-1} \pmod N$.

Step 5: Let $q = ((X+1)^2 + DY^2)/4 \in \mathbb{Q}$.

Step 6: If q is a prime number, use the CM method to obtain an elliptic curve E over $\mathbb{F}_q$ with trace $t = X+1$, so

$$|E(\mathbb{F}_q)| = q + 1 - t = q - X.$$

If q is not a prime number, start again with a new X and/or Y and/or D.

Remarks 5.1.

(i) Since $q \equiv X \pmod N$, it follows that the group order $|E(\mathbb{F}_q)|$ is divisible by N. The embedding degree for E over $\mathbb{F}_q$ is k with respect to every divisor $d > 1$ of N, since X has order k modulo every divisor $d > 1$ of N.

(ii) When $k = 2$, one can simply take $X = N - 1$ (with odd primes $p_1, \ldots, p_r$ and $Y \equiv 2s^{-1} \pmod N$), and take $D \equiv 3 \pmod 4$ to ensure that q is an integer.

(iii) The case of $k = 1$ in §4 can be derived from the above algorithm with $X = 1$, $Y = N$ when $D \equiv 0, 4 \pmod 6$, $X = 1$, $Y = 2N$ when $D \equiv 1, 3 \pmod 6$, $X = 1 + 2N$, $Y = 2N$ when $D \equiv 5 \pmod 6$, and $X = 1 - 4N$, $Y = 2N$ when $D \equiv 2 \pmod 6$.

(iv) The fact that N is a product of primes that are $1 \pmod k$ is leaked in this construction. In addition, a square root s of $-D \pmod N$ is revealed from q, N, and E. We do not know how to use this information to factor N, but it is a potential security concern. In particular, the exposed square root of $-D \pmod N$ must be taken into account in any security proof using these curves.

6. Ordinary composite order groups, Version II

The only steps in which Versions I and II differ are Steps 2 and 3.

Input: a positive integer k such that either $4|k$ or
k has a prime divisor that is congruent to 3 modulo 4,
distinct primes $p_1, \ldots, p_r$ congruent to 1 modulo k, and
positive integers $\alpha_1, \ldots, \alpha_r$.
Let $N = \prod_{i=1}^{r} p_i^{\alpha_i}$.

Output: a prime q;
an elliptic curve E over $\mathbb{F}_q$ of embedding degree k with respect to N.

Step 1: Choose an integer X that has order k in $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ for all i.

Step 2: Choose a positive square-free divisor D of k such that if k is a multiple of 4 then D divides $k/4$, while if k is not a multiple of 4 then $D \equiv 3 \pmod 4$.

Step 3: With $\left(\frac{-D}{a}\right)$ denoting the Jacobi symbol, let

$$s = \begin{cases} \displaystyle\sum_{\substack{a=1 \\ (a,2D)=1}}^{2D-1} \left(\frac{-D}{a}\right) X^{\frac{ak}{D}} \pmod N & \text{if } D \equiv 3 \pmod 4, \\ \displaystyle\frac{1}{2} \sum_{\substack{a=1 \\ (a,2D)=1}}^{4D-1} \left(\frac{-D}{a}\right) X^{\frac{ak}{4D}} \pmod N & \text{otherwise.} \end{cases}$$

(By Remark 6.1(ii) below, $s^2 \equiv -D \pmod N$.)

Step 4: Take an integer Y congruent to $\pm(X-1)s^{-1} \pmod N$.

Step 5: Let $q = ((X+1)^2 + DY^2)/4 \in \mathbb{Q}$.

Step 6: If q is a prime number, use the CM method to obtain an elliptic curve E over $\mathbb{F}_q$ with trace $t = X+1$, so

$$|E(\mathbb{F}_q)| = q + 1 - t = q - X.$$

If q is not a prime number, start again with a different X and/or Y.

Remarks 6.1.

(i) Since $s^2 \equiv -D \pmod N$ and $Y \equiv \pm(X-1)s^{-1} \pmod N$, we have $DY^2 \equiv -(X-1)^2 \pmod N$ and $q = ((X+1)^2 + DY^2)/4 \equiv X \pmod N$. Since $|E(\mathbb{F}_q)| = q - X$, the group order is divisible by N. Since k is the order of X modulo every divisor > 1 of N, we have $N | (q^k - 1)$ and the embedding degree is k with respect to every divisor > 1 of N.

(ii) The restrictions on the input k and on D (in Step 2) ensure that $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$ (by Corollary 7.3 below), which then allows us to define s so that $s \equiv f(X) \pmod N$, where $f(x) \in \mathbb{Z}[x]$ is such that $\sqrt{-D} = f(\zeta_k)$ and X has order k modulo each prime divisor of N (see Proposition 7.1). By the definition of X we have $N | \Phi_k(X)$, where Φ_k is the k-th cyclotomic polynomial. Then $s^2 \equiv -D \pmod N$, since s is the image of $\sqrt{-D}$ under the following homomorphism of rings:

$$\begin{array}{ccccc} \mathbb{Z}[\zeta_k] & \cong & \mathbb{Z}[x]/(\Phi_k(x)) & \to & \mathbb{Z}/N\mathbb{Z} \\ \sqrt{-D} = f(\zeta_k) & \mapsto & f(x) & \mapsto & f(X) = s. \end{array}$$

Since s was computed without using any knowledge about the factorization of N, this method of computing a square root s of $-D \pmod N$ does not leak information about the factorization of N.

Example 6.2. A good example to use is when $k = D = 3$ and N is a product of two (distinct) primes. In this case, the construction reveals N of the form $p_1 p_2$ with primes $p_1 \equiv p_2 \equiv 1 \pmod 3$, and X such that $X^3 \equiv 1 \pmod N$. Anyone can compute s, Y, q, and E from N and X. For example, $s \equiv 2X + 1 \pmod N$ (giving $s^2 \equiv -3 \pmod N$). It is not known how to obtain any additional information about p_1 and p_2, as long as X has order 3 modulo *both* p_1 and p_2 (which is the case in our construction).

7. Computing s

The previous algorithm made use of the next result.

Proposition 7.1. *Suppose D is a square-free positive integer. Then*

$$\sqrt{-D} = \begin{cases} \displaystyle\sum_{\substack{a=1\\(a,2D)=1}}^{2D-1} \left(\frac{-D}{a}\right)\zeta_D^a & \text{if } D \equiv 3 \pmod 4, \\ \displaystyle\frac{1}{2}\sum_{\substack{a=1\\(a,2D)=1}}^{4D-1} \left(\frac{-D}{a}\right)\zeta_{4D}^a & \text{otherwise.} \end{cases}$$

Proof. Define a function $\chi_D : \mathbb{Z} \to \{\pm 1\}$ as follows:

$$\chi_D(a) = \begin{cases} \left(\frac{a}{D}\right) & \text{if } D \equiv 3 \pmod 4, \\ (-1)^{(a-1)/2}\left(\frac{a}{D}\right) & \text{if } D \equiv 1 \pmod 4, \\ (-1)^{(a^2-1)/8}\left(\frac{a}{D/2}\right) & \text{if } D \equiv 6 \pmod 8, \\ (-1)^{\frac{a^2-1}{8}+\frac{a-1}{2}}\left(\frac{a}{D/2}\right) & \text{if } D \equiv 2 \pmod 8. \end{cases}$$

Let $d = D$ when $D \equiv 3 \pmod 4$ and let $d = 4D$ otherwise. It follows from Theorem 7 on p. 349 and Problem 8 on p. 354 of [8] that

$$\sqrt{-d} = \sum_{\substack{a=0\\(a,d)=1}}^{d-1} \chi_D(a)\zeta_d^a.$$

(Note that the above definition of χ_D when $D \equiv 2 \pmod 8$ corrects a typo in Problem 8 of [8].) Using quadratic reciprocity, it is easy to check that when a is an odd positive integer, then $\chi_D(a) = \left(\frac{-D}{a}\right)$, and the desired result then follows. □

The next result follows from standard algebraic number theory facts about quadratic subfields of cyclotomic fields.

Proposition 7.2. *Suppose d is a square-free integer. The smallest positive integer k such that $\sqrt{d} \in \mathbb{Q}(\zeta_k)$ is $|d|$ if $d \equiv 1 \pmod 4$ and is $4|d|$ if $d \not\equiv 1 \pmod 4$.*

The following result that was used in Remark 6.1(ii) is an immediate corollary:

Corollary 7.3. *Suppose D is a square-free positive integer.*

(i) *If k is a multiple of 4, then $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$ if and only if D divides $\frac{k}{4}$.*
(ii) *If k is not a multiple of 4, then $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$ if and only if D divides k and $D \equiv 3 \pmod 4$.*

8. Remarks

We give some remarks about the above constructions.

Remark 8.1. As pointed out in [17], the Cocks-Pinch method is good for constructing elliptic curves with arbitrary k, and many curves will be found, and it is easy to specify the size q of the field $\mathbb{F}_q$. These favorable properties also hold with the above constructions.

Remark 8.2. As is usual for the Cocks-Pinch method, the group order in the above constructions is approximately N^2 (since q is approximately N^2), so the number $\rho := \log q / \log N$ that measures the efficiency of the construction is approximately 2. When using composite order ordinary elliptic curves, §8.4 of [18] recommends using curves of embedding degree 1 to optimize efficiency.

Remark 8.3. Merely requiring X to have order k in $(\mathbb{Z}/N\mathbb{Z})^\times$, while permitting X to have lower order in $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$, could lead to an easy way to factor N, as follows. If X has order k_i in $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$, and j is such that $k_j < k_i$ for all $i \neq j$, then $\gcd(X^{k_j} - 1, N) = p_j^{\alpha_j}$, so computing this gcd gives an easy way to factor N. Taking X to have exact multiplicative order k modulo each of the divisors $p_i^{\alpha_i}$ of N ensures that X has order k modulo every divisor $d > 1$ of N.

Remark 8.4. When $\sqrt{-D} \in \mathbb{Q}(\zeta_k) = \mathbb{Q}(e^{2\pi i/k})$, Version II computes a square root s of $-D \pmod N$ without knowing the factorization of N, so this s does not leak information. If we had used the factorization of N to choose a different square root $s' \neq \pm s$, one could use these two square roots of $-D \pmod N$ to factor N. So it is important to use the s that does not leak information. In Version I, to avoid this problem we choose k and D to satisfy properties that ensure that (by Corollary 7.3) we have $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$. Version I leaks a square root of $-D \pmod N$ (that is computed using the prime factors of N), but we do not know how to use that information to give any information about the factors of N. Note that every construction of pairing-friendly curves will leak a k-th root of unity mod N, by the definition of embedding degree and the existence of efficient point counting algorithms.

Remark 8.5. The CM discriminant D needs to be chosen small so that the CM method will be feasible. Common choices for D are 1 or 3, but if one is concerned about very small D one can choose $D > 200$. Small D give more efficient computation, but may be more prone to attack [15]. Optimizations of Sutherland [30] allow him to handle D as large as 10^{13}.

Remark 8.6. Starting with s and defining D to be $-s^2 \pmod N$ would solve the problem of leaking information about s. However, this will in general give very large D (around the size of N), for which the CM method is very inefficient. That is why we start with (small) D and then obtain s.

Remark 8.7. Composite order group cryptography applications rely on the difficulty of various problems, including the Subgroup Decision Problem, the Bilinear Subgroup Decision Problem, and the Decision 3-Party Diffie-Hellman Problem (see for example [6]). Parameters and curves need to be chosen so that these problems are believed to be hard. In particular, one needs the Computational Diffie-Hellman and Decision Bilinear Diffie-Hellman Problems to be hard, in addition to requiring that N be difficult to factor.

Remark 8.8. The groups constructed in §5 and §6 do not succumb to the attack on the Subgroup Decision Problem described in Remark 4.5, for the following reason. Since each output curve E is ordinary, all its endomorphisms are defined over $\mathbb{F}_q$. For every prime divisor p of N, $E[p]$ is not contained in $E(\mathbb{F}_q)$, since the embedding degree with respect to p is $k > 1$. Thus all order p subgroups of $E(\mathbb{F}_q)$ are preserved by all endomorphisms of E, and therefore such subgroups have no distortion maps.

Remark 8.9. Given an output curve E, without knowing the factorization of N one can compute a random point in $E(\mathbb{F}_q)$ killed by N, and it will have exact order N with high probability. Alternatively, the algorithms could additionally output a point of exact order N (using N's factorization).

Remark 8.10. There are families of prime order pairing-friendly groups parametrized by polynomials (see [3, 11, 14, 4, 16]). One would similarly like to obtain families of examples of composite order pairing-friendly groups. However, this seems to be much more difficult in the composite order case, since knowing a polynomial $N(x)$ that often evaluates to group orders of the form $N(x_0) = p_1p_2$ seems likely to reveal a factorization of $N(x_0)$ for particular values x_0 (if not a factorization of $N(x)$ itself). For example, if $N(x) = x^2 - 1$ and is public, this reveals the information that p_1 and p_2 are twin primes, and given $N(x_0) = x_0^2 - 1$ it is easy to solve for the quantities x_0, $p_1 = x_0 - 1$, and $p_2 = x_0 + 1$. It is an open problem to obtain parametrized families in which the prime factors of N will be random, unguessable primes of the desired size.

9. Implementation

For our implementation we fixed D and k. We took p_1 and p_2 to be 512-bit primes congruent to 1 modulo $4Dk$ (thereby forcing $-D$ to be a square modulo p_1 and p_2) and let $N = p_1p_2$. We then took $j^{(p_1-1)/k} \pmod{p_1}$ for $j = 1, 2, 3, \ldots$ until we found one of order $k \pmod{p_1}$, and similarly with p_1 replaced by p_2, and then applied the Chinese Remainder Theorem to obtain X of order k modulo both p_1 and p_2. If X was even, we replaced it with $X - N$, to obtain an odd X such that $0 < |X| < N$. If $X = -1$ we replaced X with $2N - 1$. If $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$ (as determined by Corollary 7.3), we used the formula for s in Step 3 of Version II of the algorithm. Otherwise, we computed a square root of $-D$ modulo p_1 and modulo p_2 (using PARI/GP [28]), and used the Chinese Remainder Theorem to obtain a square root s of $-D$ modulo N. We let Y be $(X-1)s^{-1} \pmod{N}$, but if it was odd we replaced it with $Y - N$, to obtain an even Y such that $0 < |Y| < N$. If $Y = 0$ we replaced Y with $4N$; if $Y = X + 1$ we replaced Y with $X + 1 - 2N$. Since $X + 1$ and Y are even, q is automatically a positive integer. We tested q for primality. If q was not prime, we started again with a new p_2.

Once parameters are obtained with q prime, one can apply the CM method.

We ran our program for all values of k between 1 and 40, with $D = 1, 2, 3$, 201, 202, and 203, and readily obtained examples in all cases. In the examples we obtained with $k > 1$, the value of ρ was between 1.992 and 2.006. For $k = 1$, ρ was between 2.00195 and 2.00943.

Acknowledgments

We thank IPAM and the organizers of its Fall 2006 Program. We also thank David Freeman and the other participants of the IPAM Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security Reunion Conference II for helpful feedback. Silverberg thanks Daniel Bernstein for helpful comments and Samuel Kadziela for helpful conversations.

References

[1] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68.

[2] L. Ballard, M. Green, B. de Medeiros, F. Monrose, *Correlation-Resistant Storage via Keyword-Searchable Encryption*, in Cryptology ePrint Archive, Report 2005/417, 2005, `http://eprint.iacr.org/2005/417.pdf`

[3] P. S. L. M. Barreto, B. Lynn, M. Scott, *Constructing Elliptic Curves with Prescribed Embedding Degrees*, in Security in Communication Networks – SCN 2002, Lect. Notes in Comp. Sci. **2576**, Springer, Berlin, 2003, 257–267.

[4] P. Barreto, M. Naehrig, *Pairing-Friendly Elliptic Curves of Prime Order*, Selected Areas in Cryptography – SAC 2005, Lect. Notes in Comp. Sci. **3897**, Springer, Berlin, 2006, 319–331.

[5] D. Boneh, E.-J. Goh, and K. Nissim, *Evaluating 2-DNF formulas on ciphertexts*, in Proceedings of TCC 2005, J. Kilian, ed., Lect. Notes in Comp. Sci. **3378**, Springer, Berlin, 2005, 325–341.

[6] D. Boneh, A. Sahai, B. Waters, *Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys*, in Advances in Cryptology — Eurocrypt 2006, S. Vaudenay, ed., Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2006, 573–592.

[7] D. Boneh, B. Waters, *Conjunctive, Subset, and Range Queries on Encrypted Data*, in Proceedings of TCC 2007, Lect. Notes in Comp. Sci. **4392**, Springer, Berlin, 2007, 535–554.

[8] A. I. Borevich, I. R. Shafarevich, Number theory, Academic Press, New York-London, 1966.

[9] X. Boyen, B. Waters, *Compact Group Signatures Without Random Oracles*, in Advances in Cryptology — Eurocrypt 2006, S. Vaudenay, ed., Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2006, 427–444.

[10] X. Boyen, B. Waters, *Full-Domain Subgroup Hiding and Constant-Size Group Signatures*, in Public Key Cryptography PKC 2007, S. Vaudenay, ed., Lect. Notes in Comp. Sci. **4450**, Springer, Berlin, 2007, 1–15.

[11] F. Brezing, A. Weng, *Elliptic Curves Suitable for Pairing Based Cryptography*, Designs, Codes and Cryptography **37** (2005), 133–141.

[12] N. Chandran, J. Groth, A. Sahai, *Ring Signatures of Sub-linear Size without Random Oracles*, in International Colloquium on Automata, Languages and Programming — ICALP 2007, Lect. Notes in Comp. Sci. **4596**, Springer, Berlin, 2007, 423–434.

[13] D. Charles, *On the existence of distortion maps on ordinary elliptic curves*, in Cryptology ePrint Archive, Report 2006/128, 2006, `http://eprint.iacr.org/2006/128.pdf`

[14] R. Dupont, A. Enge, F. Morain, *Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields*, J. Cryptology **18** (2005), 79–89.

[15] I. Duursma, P. Gaudry, F. Morain, *Speeding up the Discrete Log Computation on Curves with Automorphisms*, in Advances in Cryptology — Asiacrypt '99, Lect. Notes in Comp. Sci. **1716**, Springer, Berlin, 1999, 103–121.

[16] D. Freeman, *Constructing pairing-friendly elliptic curves with embedding degree 10*, in Proceedings of ANTS-VII, Lect. Notes in Comp. Sci. **4076**, Springer, Berlin, 2006, 452–465.

[17] D. Freeman, *Methods for constructing pairing-friendly elliptic curves*, lecture at ECC 2006, September 19, 2006, `http://www.cacr.math.uwaterloo.ca/conferences/2006/ecc2006/freeman.pdf`

[18] D. Freeman, M. Scott, E. Teske, *A taxonomy of pairing-friendly elliptic curves*, to appear in J. Cryptology.

[19] S. Galbraith, *Pairings*, in Advances in Elliptic Curve Cryptography, I. F. Blake, G. Seroussi, N. P. Smart, eds., London Math. Soc. Lect. Note Series **317**, Cambridge Univ. Press, Cambridge, 2005, 183–213.

[20] J. Groth, R. Ostrovsky, A. Sahai, *Perfect Non-interactive Zero Knowledge for NP*, in Advances in Cryptology — Eurocrypt 2006, S. Vaudenay, ed., Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2006, 339–358.

[21] J. Groth, A. Sahai, *Efficient Non-interactive Proof Systems for Bilinear Groups*, in Advances in Cryptology EUROCRYPT 2008, Lect. Notes in Comp. Sci. **4965**, Springer, Berlin, 2008, 415–432.

[22] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.

[23] N. Koblitz, A. Menezes, *Pairing-based cryptography at high security levels*, in Cryptography and Coding 2005, Lect. Notes in Comp. Sci. **3796**, Springer, Berlin Heidelberg, 2005, 13–36.

[24] V. Miller, *Uses of elliptic curves in cryptography*, in Advances in Cryptology — CRYPTO 85, Lect. Notes in Comp. Sci. **218**, Springer, Berlin, 1986, 417426.

[25] V. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology **17** (2004), 235–261.

[26] F. Morain, *Building cyclic elliptic curves modulo large primes*, in Advances in Cryptology — Eurocrypt '91, Lect. Notes in Comp. Sci. **547**, Springer, Berlin, 1991, 328–336.

[27] R. Ostrovsky, W. E. Skeith III, *Private Searching on Streaming Data*, in Advances in Cryptology — CRYPTO 2005, V. Shoup, ed., Lect. Notes in Comp. Sci. **3621**, Springer, Berlin, 2005, 223–240.

[28] PARI/GP computer algebra system, `http://pari.math.u-bordeaux.fr`

[29] H. Shacham, B. Waters, *Efficient Ring Signatures Without Random Oracles*, in Public Key Cryptography PKC 2007, T. Okamoto, X. Wang, eds., Lect. Notes in Comp. Sci. **4450**, Springer, Berlin, 2007, 166–80.

[30] A. V. Sutherland, *Computing Hilbert class polynomials with the Chinese Remainder Theorem*, `http://arxiv.org/pdf/0903.2785v2`

[31] B. Waters, *personal communication*, December 1, 2006.

Department of Computer Science, Stanford University, Stanford, CA 94305, USA
E-mail address: `dabo@cs.stanford.edu`

Department of Mathematics, University of California, Irvine, CA 92697-3875, USA
E-mail address: `krubin@math.uci.edu`

Department of Mathematics, University of California, Irvine, CA 92697-3875, USA
E-mail address: `asilverb@math.uci.edu`