International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

BLS Curves with Embedding Degrees 9, 15, 21 and 27 against Small-Subgroup Attacks

Mahamadou Abdou Toure[1], Karim Samake[2], Sinaly Traore[3]

[1]Centre de Recherche et de Formation pour l'Industrie Textile, Ségou, BP: 323, Mali

[2, 3]Université des Sciences, des Techniques et des Technologies de Bamako, Faculté des Sciences et des Techniques, Bamako, Mali

Abstract: ***Pairing Based Cryptography depends on the existence of groups where the DDH problem is easy to solve but the problem CDH is difficult. Barreto, Lynn, and Scott examined criteria for curves of larger embedding degrees that generalize the prior work of Miyaji et al. based on the properties of cyclotomic polynomials. To achieve an average level of security, at least two of the three groups of the pairing must necessarily be subgroups proper to groups of orders composed of large prime factors to resist of the small-subgroup attacks. In this article, we have taken over the article of Barreto, Lynn and Scott by bringing clarifications at the level of some basic formulas, by bringing correctives to the case of power of 3 and adding the general case divisible by 3. This theory has been applied to see its impact on the security of the subgroups in pairing-based cryptography.***

Keywords: Pairings, Cryptography, Elliptic Curves, small-subgroup attacks

1. Introduction and state of the art

A subgroup G of order r of an elliptic curve $E(\mathrm{F}_q)$ has k us embedding degree or security multiplier if r divide $q^k - 1$ but does not divide any $q^i - 1$ for all $i = 1, \ldots, k-1$.

In pairing-based cryptography, an open problem is to construct curves containing a subgroup with a embedding degree k which is at the same time large enough to prevent the Frey-Rück attack, but small enough to efficiently compute the Tate pairing (or its variants) which means that the arithmetic in F_{q^k} is feasible. For a long time the supersingular curves had remained the same as those which admitted subgroups which had reasonable embedding degrees as indicated in [1]. Miyaji, Nakabayashi and Takano have shown in [2] using properties of cyclotomic polynomials of order k, how to construct non-supersingular prime order curves over F_{q^k}, with k = 3; 4; 6 using the complex multiplication method (CM). By naming this method "MNT criteria" which is based on the size of the field q, the trace of Frobenius t and the order of the curve n, Barreto, Lynn and Scott, in [3], invested generalities of this criteria for curves with a general embedding degree k and presented the current construction of such curves. In [4], Barreto et al. have proposed new examples of adapted elliptic curves that aim to provide stronger resistance against Small-Subgroup Attacks introduced by Lim and Lee in [5]. A small subgroup attack can be mounted on a discrete logarithmic cryptographic scheme that uses a prime order group that is contained in a larger order group divisible by small prime factors. Indeed, Small-subgroup attacks are based on choosing an element belonging to a subgroup in which DLP is easy by forcing a protocol participant to perform an exponentiation of that element with its secret key. Thus, an attacker could easily obtain information on a private key of a protocol participant. So, the user's private key could be completely identified although the discrete logarithm problem (DLP) in the large prime order subgroup is computationally difficult if the implementation of the protocol does not check whether the element of the group used belongs to the correct subgroup and therefore has a large prime order.

Barreto, Lynn and Scott began by illustrating the possibility of such attacks in the context (based on pairing) of the digital signature schemes; many of them are based on the famous short signature scheme of Boneh, Lynn and Shacham described in [6]. Barreto et al. worked on the family of Barreto-Naehrig (BN) curves for k = 12, the Barreto Lynn Scott family (BLS) curves for k = 12 and 24 and those of Kachisa - Schaefer - Scott (KSS) for k = 18.

In this paper, we provide clarifications and correctives in [3], construct BLS curves for k = 9; 15; 21 and 27 using the particular case (D = –3), and study the resistance of these curves to the small-subgroup attacks.

2. Contribution to solving the BLS CM equation for D = –3

Following the same approach as Barreto et al. (BLS) have used, we bring correctives in the computation of the parameters for D = –3. To construct our curves, the same methodology in [3] has been used as follows:

- Choose l and h ;
- Find a prime q and a corresponding trace t according to the relations proposed;
- Solve, to obtain the discriminant of CM D (and V), the equation of CM (For computational reasons, we have multiplied the CM equation by –1 to have a positive D) $DV^2 = 4q - t^2$ or equivalent $DV^2 = 4n - (t-2)^2$;
- And use the CM method to compute the coefficients of the curve's equation.

Let p be a prime number. BLS described in [3, §3.] how to find algebraic solutions of the equation

$$DV^2 = 4m\phi_k(l) - (l^d - 1)^2 \quad (1)$$

where l is an integer with $|l|>1$, ϕ_k the k-th cyclotomic polynomial and d a satisfying integer $1 \le d \le \frac{1}{2} deg\phi_k$ for special cases of $D = 3$, $d = 1$ and $k = 3^i 2^j p^s$, for some exponents i; j; s and p > 3. In principle, this method avoids the m/r ratio from being arbitrarily small for k wide if s = 0. Using the properties of cyclotomic polynomials as follows:

- if v is a prime number that divides u then $\phi_{uv}(x) = \phi_u(x^v)/\phi_u(x)$.
- if v does not divide u then $\phi_{uv}(x) = \phi_u(x^v)$,

it is easy to inductively show that for all $i > 0$

$\phi_{3^i}(l) = l^{2\times 3^{i-1}} + l^{3^{i-1}} + 1$ and $\phi_{2^i 3}(l) = l^{2^i} - l^{2^{i-1}} + 1$

Taken l such that $l \equiv 1[3]$, BLS found

$$4\phi_{3^i}(l) - 1 = 3\left(\left(2l^{3^{i-1}} + 1\right)/3\right)^2 \text{ and}$$

$$4\phi_{2^i 3}(l) - 3 = \left(2l^{2^{i-1}} - 1\right)^2$$

But by developing the two members of the first relationship, we find

$$4\phi_{3^i}(l) - 1 = 4l^{2\times 3^{i-1}} + 4l^{3^{i-1}} + 3 \text{ and}$$

$$3\left(\left(2l^{3^{i-1}} + 1\right)/3\right)^2 = \frac{4}{3}l^{2\times 3^{i-1}} + \frac{4}{3}l^{3^{i-1}} + \frac{1}{3}$$

We see that the two expressions are different.

The solution we obtained is $4\phi_{3^i}(l) - 3 = \left(2l^{3^{i-1}} + 1\right)^2$.

In the first case, BLS multiplied both sides by $(l-1)^2$ to obtain

$$4(l-1)^2\phi_{3^i}(l) - (l-1)^2 = 3\left((l-1)\left(2l^{3^{i-1}} + 1\right)/3\right)^2$$

With our solution, multiply both sides by $(l-1)^2/3$. We have:

$$\frac{4}{3}(l-1)^2\phi_{3^i}(l) - (l-1)^2 = 3\left((l-1)\left(2l^{3^{i-1}} + 1\right)/3\right)^2$$

which gives the solution:

$$k = 3^i,\ r = \frac{1}{3}\phi_{3^i}(l),\ t = l+1,\ m = (l-1)^2,$$

$$V = (l-1)\left(2l^{3^{i-1}} + 1\right)/3$$

In the second case, multiplying the two sides by $(l-1)^2/3$, we find :

$$\frac{4}{3}(l-1)^2\phi_{2^i 3}(l) - (l-1)^2 = 3\left((l-1)\left(2l^{2^{i-1}} - 1\right)/3\right)^2$$

which gives the solution:

$$k = 2^i \times 3,\ r = \phi_{2^i 3}(l),\ t = l+1,\ m = (l-1)^2/3,$$

$$V = (l-1)\left(2l^{2^{i-1}} - 1\right)/3$$

In both cases we assume that $q = mr + l$ is prime [3, §2]. Similarly, it can be shown by induction that for all prime $p>3$ and for all integers $i>0$ and $j>0$

$$\phi_{3^i p^j}(l) = \frac{\left(2l^{3^{i-1}p^j} + 1\right)^2 + 3}{\left(2l^{3^{i-1}p^{j-1}} + 1\right)^2 + 3}$$

Multiply both sides by $12z^2\left(\left(2l^{3^{i-1}p^{j-1}} + 1\right)^2 + 3\right)$

pour tout z, which give

$$4\times 3z^2\left(\left(2l^{3^{i-1}p^{j-1}} + 1\right)^2 + 3\right)\phi_{3^i p^j}(l) - (6z)^2 =$$

$$3\left(2z\left(2l^{3^{i-1}p^j} + 1\right)\right)^2$$

By choosing r to be a big factor in $\phi_{3^i p^j}(l)$, this gives the solution : $k = 3^i \times p^j$, $l = 6z + 1$,

$$n = 3z^2\left(\left(2l^{3^{i-1}p^{j-1}} + 1\right)^2 + 3\right)\phi_{3^i p^j}(l)$$

$$V = 2z\left(2l^{3^{i-1}p^j} + 1\right)$$

As we will see in 4, it is necessary for the construction to check that $q = m\phi_k(l) + l$ is prime in all cases. Solutions for $D = 3$ gives us a Hilbert polynomial $P_H(x) = x$ which has only one root 0. So with a j-invariant $j = 0$ we get curves of the form $E : y^2 = x^3 + B$ with B to determinate. Examples have been given in the section 4 for $k = 9$; 15; 21 and 27.

3. Resistance of BLS curves against small-subgroup attacks

Let $e : g_1 \times g_2 \to g_T$ be an asymmetric pairing such that $|g_1| = |g_2| = |g_T| = n$. Let $G_1 = E(\mathrm{F}_q)$, $G_2 = E(\mathrm{F}_{q^{k/d}})$ and $G_1 = G_{\phi_k(q)}$ be the three naturel groups associated respectively with g_1, g_2 and g_T. The relevant indices or associated cofactors h_1, h_2, h_T are defined as:

$$h_1 = \frac{|G_1|}{n};\quad h_2 = \frac{|G_2|}{n};\quad h_T = \frac{|G_T|}{n}.$$

We will not detail much the pairing theory here, see [9] for more information.

In this section, we study the security of BLS curves as defined in the previous section for $k = 9; 15; 21$, and 27 against the threat of subgroup attacks.

We rely on the following lemma from [7, §A:14:2:3] which determines the orders of groups of these twists over F_q.

Lemma 1: Let t be the trace of Frobenius of the elliptic curve $E / \mathrm{F}_q : y^2 = x^3 + B$ and $v \in Z$ such that $t^2 - 4q = -3v^2$. Up to isomorphism, there are at most six curves (including E) defined over F_q with a trace t' such that $t'^2 - 4q = -3v'^2$ for some square-free $v' \in Z$. The six possibilities for t' are $\pm t, \pm \frac{t + 3v}{2}, \pm \frac{t - 3v}{2}$.

The curves on which our studies have been drawn are those of BLS with embedding degrees 9, 15, 21 and 27. Each curve has been studied according to its subgroup security.
Since h_1 is always more than n in all cases, only h_2 and h_T have been factored (partially) to test the security of the subgroups. To do their partial factorizations, we used the ECM method in SageMath.

3.1 BLS curves with k = 9

This family has the following parametrizations:

$$q(u) = \frac{(u-1)^2\phi_9(u)}{3} + u = \frac{(u-1)^2\left(u^6 + u^3 + 1\right)}{3} + u;$$
$$t(u) = u + 1$$

$t(u) = u + 1$ and $n(u) = \frac{\phi_9(u)}{3} = \frac{\left(u^6 + u^3 + 1\right)}{3}$.

We have in this case, $\#E'\left(\mathrm{F}_q\right) = h_1(u) \times n(u)$ with $h_1(u) = (u-1)^2$. There is always a cofactor that is smaller than n in the order of G_1. Here, the cofactor for $G_T = G_{\phi_k(q)}$ is

$$h_T(u) = \frac{\phi_9(q(u))}{n(u)} = \frac{\left((q(u))^6 + (q(u))^3 + 1\right)}{n(u)}.$$

The following proposition gives the cofactor $h_2(u)$.

Proposition 2: With the parameters as defined above the good twist E'/F_{q^3} for a curve with $k = 9$ has a group order $\#E'\left(\mathrm{F}_{q^3}\right) = h_2(u) \times n(u)$ where

$$h_2(u) = \frac{1}{27}(u-1)^2(u^2+u+1)(u^6 - 3u^5 + 3u^4 + u^3 - 3u^2 + 4)(u^8 - 2u^7 + u^6 + u^5 - 5u^4 + 4u^3 + u^2 + u + 7).$$

Proof: According to the corollary [8, Corollary VI.2],

$\#E'\left(\mathrm{F}_{q^3}\right) = q_3 + 1 - t_3$ with $q_3 = q^3$ and $t_3 = t^3 - 3qt$.

The CM equation for $E'\left(\mathrm{F}_{q^3}\right)$ is $t_3^2 - 4q_3 = -3v_3^2$, which gives $v_3 = \frac{1}{9}(u^4 - u^3 + 2u + 1)(u^4 - u^3 - u - 2)(2u^3 + 1)(u - 1)$.

The lemma 1 reveals that $t' = t_3$ provides us the right twist E'/F_{q^3} with $n|\#E'\left(\mathrm{F}_{q^3}\right) = q^3 + 1 - t'$ and the cofactor is obtained as follows: $h_2 = \frac{q^3 + 1 - t'}{n}$.

3.2 BLS curves with k = 15

This family has the following parametrizations:

$$q(u) = \frac{(u-1)^2\left((2u+1)^2 + 3\right)\phi_{15}(u)}{12} + u;\ t(u) = u + 1$$

and $n(u) = \phi_{15}(u) = u^8 - u^7 + u^5 - u^4 + u^3 - u + 1$

We have in this case, $\#E'\left(\mathrm{F}_q\right) = h_1(u) \times n(u)$ with $h_1(u) = \frac{(u-1)^2\left((2u+1)^2 + 3\right)}{12}$. Again there is always a cofactor that is smaller than n in the order of G_1. Here, for $G_T = G_{\phi_T(q)}$ the cofactor is $h_T = \frac{\phi_{15}(q(u))}{n(u)}$.

The following proposition gives the cofactor $h_2(u)$.

Proposition 3: With the parameters as defined above the good twist E'/F_{q^5} for a curve with $k = 15$ has a group order $\#E'\left(\mathrm{F}_{q^5}\right) = h_2(u) \times n(u)$ where

$$h_2(u) = \frac{1}{243}(u-1)^2(u^2+u+1)(u^{48} - 8u^{47} + 28u^{46} - 56u^{45} + 70u^{44} - 52u^{43} - 4u^{42} + 104u^{41} - 223u^{40} + 280u^{39} - 214u^{38} + 47u^{37} + 158u^{36} - 331u^{35} + 400u^{34} - 319u^{33} + 107u^{32} + 113u^{31} - 211u^{30} + 220u^{29} - 202u^{28} + 116u^{27} - u^{26} - 58u^{25} + 70u^{24} - 58u^{23} + 59u^{22} - 64u^{21} - 22u^{20} + 100u^{19} - 31u^{18} + 8u^{17} - 13u^{16} - 4u^{15} - 20u^{14} - 151u^{13} + 158u^{12} + 167u^{11} - 124u^{10} - 80u^9 - 133u^8 + 164u^7 + 176u^6 - 52u^5 + 175u^4 + 349u^3 + 568u^2 + 547u + 271).$$

Proof: According to the corollary [8, Corollary VI.2],

$\#E'\left(\mathrm{F}_{q^5}\right) = q_5 + 1 - t_5$ with $q_5 = q^5$ and

$t_5 = t^5 - 5qt^2 + 5q^2t$. The CM equation for $E'\left(\mathrm{F}_{q^5}\right)$ is $t_5^2 - 4q_5 = -3v_5^2$, which gives

$v_5 = \frac{1}{9}(2u^5+1)(u-1)(u^{24} - 4u^{23} + 6u^{22} - 4u^{21} + u^{20} + 2u^{19} - 8u^{18} + 12u^{17} - 8u^{16} + 2u^{15} - 6u^{14} - 6u^{13} + 24u^{12} - 6u^{11} - 6u^{10} - 7u^9 - 2u^8 + 18u^7 - 2u^6 - 7u^5 + u^4 + 11u^3 + 21u^2 + 11u + 1)$.

The lemma 1 reveals that $t' = t_5$ provides us the right twist E'/F_{q^5} with $n|\#E'\left(\mathrm{F}_{q^5}\right) = q^5 + 1 - t'$ and the cofactor is obtained as follows: $h_2 = \frac{q^5 + 1 - t'}{n}$.

3.3 BLS curves with k = 21

This family has the following parametrizations:

$$q(u) = \frac{(u-1)^2\left((2u+1)^2+3\right)\phi_{21}(u)}{12} + u;\ t(u) = u + 1$$

and

$$n(u) = \phi_{21}(u) = u^{12} - u^{11} + u^9 - u^8 + u^6 - u^4 + u^3 - u + 1$$

We have in this case, $\#E'\left(\mathrm{F}_q\right) = h_1(u) \times n(u)$ with $h_1(u) = \frac{(u-1)^2\left((2u+1)^2+3\right)}{12}$. Again there is always a cofactor that is smaller than n in the order of G_1. Here, for $G_T = G_{\phi_T(q)}$ the cofactor is $h_T = \frac{\phi_{21}(q(u))}{n(u)}$.

The following proposition gives the cofactor $h_2(u)$.

Proposition 4: With the parameters as defined above the good twist E'/F_{q^7} for a curve with $k = 21$ has a group order $\#E'\left(\mathrm{F}_{q^7}\right) = h_2(u) \times n(u)$ where

$h_2(u) = \frac{1}{243}(u-1)^2(u^2+u+1)(u^{96} - 12u^{95} + 66u^{94} - 220u^{93} + 495u^{92} - 792u^{91} + 924u^{90} - 786u^{89} + 423u^{88} + 176u^{87} - 1254u^{86} + 2958u^{85} - 4751u^{84} + 5544u^{83} - 4731u^{82} + 2739u^{81} - 144u^{80} - 3279u^{79} + 7803u^{78} - 12216u^{77} + 14112u^{76} - 12172u^{75} + 7380u^{74} - 1425u^{73} - 5099u^{72} + 11919u^{71} - 17529u^{70} + 19740u^{69} - 17460u^{68} + 11385u^{67} - 3296u^{66} - 4887u^{65} + 11547u^{64} - 15664u^{63} + 17010u^{62} - 15588u^{61} + 11160u^{60} - 4365u^{59} - 2439u^{58} + 7173u^{57} - 9738u^{56} + 10584u^{55} - 9687u^{54} + 7191u^{53} - 3672u^{52} + 102u^{51} + 2763u^{50} - 4761u^{49} + 5544u^{48} - 4761u^{47} + 3204u^{46} - 2040u^{45} + 864u^{44} + 765u^{43} - 1560u^{42} + 1512u^{41} - 1611u^{40} + 1377u^{39} - 801u^{38} + 297u^{37} + 72u^{36} - 90u^{35} + 401u^{33} - 1158u^{32} + 825u^{31} + 988u^{30} - 2034u^{29} + 558u^{28} + 840u^{27} + 1056u^{26} - 3537u^{25} + 2167u^{24} + 2397u^{23} - 3372u^{22} + 995u^{21} - 252u^{20} - 1884u^{19} - 3369u^{18} + 5310u^{17} + 5421u^{16} - 3141u^{15} - 1770u^{14} - 882u^{13} - 2357u^{12} - 1494u^{11} + 4206u^{10} + 4229u^9 - 1236u^8 - 1290u^7 + 1869u^6 + 3240u^5 + 5535u^4 + 8096u^3 + 7983u^2 + 5112u + 2269)$.

Proof: According to the corollary [8, Corollary VI.2], $\#E'\left(\mathrm{F}_{q^7}\right) = q_7 + 1 - t_7$ with $q_7 = q^7$ and $t_7 = t^7 - 7qt^5 + 14q^2t^3 - 7q^3t$. The CM equation for $E'\left(\mathrm{F}_{q^7}\right)$ is $t_7^2 - 4q_7 = -3v_7^2$, which gives

$v_7 = \frac{1}{81}(2u^7+1)(u-1)(u^{48} - 6u^{47} + 15u^{46} - 20u^{45} + 15u^{44} - 6u^{43} + u^{42} + 3u^{41} - 18u^{40} + 45u^{39} - 60u^{38} + 45u^{37} - 18u^{36} + 3u^{35} - 12u^{34} + 9u^{33} + 72u^{32} - 138u^{31} + 72u^{30} + 9u^{29} - 12u^{28} - 29u^{27} + 48u^{26} + 69u^{25} - 176u^{24} + 69u^{23} + 48u^{22} - 29u^{21} - 3u^{20} + 81u^{19} + 18u^{18} - 192u^{17} + 18u^{16} + 81u^{15} - 3u^{14} + 12u^{13} + 54u^{12} - 9u^{11} - 114u^{10} - 9u^9 + 54u^8 + 12u^7 + u^6 - 6u^5 - 48u^4 - 83u^3 - 48u^2 - 6u + 1)$.

The lemma 1 reveals that $t' = t_7$ provides us the right twist E'/F_{q^7} with $n|\#E'\left(F_{q^7}\right) = q^7 + 1 - t'$ and the cofactor is obtained as follows: $h_2 = \frac{q^7 + 1 - t'}{n}$.

3.4 BLS curves with k = 27

This family has the following parametrizations:

$$q(u) = \frac{(u-1)^2\phi_{27}(u)}{3} + u = \frac{(u-1)^2\left(u^{18} + u^9 + 1\right)}{3} + u;$$

$$t(u) = u + 1 \text{ and } n(u) = \frac{\phi_{27}(u)}{3} = \frac{u^{18} + u^9 + 1}{3}$$

We have in this case, $\#E'\left(F_q\right) = h_1(u) \times n(u)$ with $h_1(u) = (u-1)^2$. Again there is always a cofactor that is smaller than n in the order of G_1. Here, for $G_T = G_{\phi_T(q)}$ the cofactor is $h_T = \frac{\phi_{27}(q(u))}{n(u)} = \frac{(q(u))^{18} + (q(u))^9 + 1}{n(u)}$.

The following proposition gives the cofactor $h_2(u)$.

Proposition 5: With the parameters as defined above the good twist E'/F_{q^9} for a curve with $k = 27$ has a group order $\#E'\left(F_{q^9}\right) = h_2(u) \times n(u)$ where

$$h_2(u) = \frac{1}{19683}(u-1)^2(u^2+u+1)(u^{18} - 3u^{17} + 3u^{16} - 3u^{14} + 3u^{13} - 3u^{11} + 3u^{10} + u^9 - 3u^8 + 3u^6 - 3u^5 + 3u^3 - 3u^2 + 4)(u^{20} - 2u^{19} + u^{18} + u^{11} - 5u^{10} + 4u^9 + u^2 + u + 7)(u^{60} - 6u^{59} + 15u^{58} - 20u^{57} + 15u^{56} - 6u^{55} + u^{54} + 3u^{51} - 18u^{50} + 45u^{49} - 60u^{48} + 45u^{47} - 18u^{46} + 3u^{45} + 6u^{42} - 27u^{41} + 54u^{40} - 66u^{39} + 54u^{38} - 27u^{37} + 6u^{36} + 7u^{33} - 24u^{32} + 33u^{31} - 41u^{30} + 60u^{29} - 51u^{28} + 16u^{27} + 6u^{24} - 9u^{23} + 9u^{22} - 39u^{21} + 63u^{20} - 36u^{19} + 6u^{18} + 3u^{15} - 6u^{12} + 54u^{11} - 27u^{10} - 24u^9 + u^6 + 3u^5 + 6u^4 + 16u^3 + 33u^2 + 3u + 19)(u^{60} - 6u^{59} + 15u^{58} - 20u^{57} + 15u^{56} - 6u^{55} + u^{54} + 3u^{51} - 18u^{50} + 45u^{49} - 60u^{48} + 45u^{47} - 18u^{46} + 3u^{45} + 6u^{42} - 27u^{41} + 54u40 - 66u^{39} + 54u^{38} - 27u^{37} + 6u^{36} + 7u^{33} - 24u^{32} + 33u^{31} - 23u^{30} + 6u^{29} + 3u^{28} - 2u^{27} + 6u^{24} - 9u^{23} + 9u^{22} - 12u^{21} - 18u^{20} + 45u^{19} - 21u^{18} + 3u^{15} - 33u^{12} - 27u^{11} + 54u^{10} + 3u^9 + u^6 + 3u^5 + 6u^4 - 2u^3 + 6u^2 + 30u + 37).$$

Proof: According to the corollary [8, Corollary VI.2], $\#E'\left(F_{q^9}\right) = q_9 + 1 - t_9$ with $q_9 = q^9$ and $t_9 = t^9 - 9qt^7 + 27q^2t^5 - 30q^3t^3 + 9q^4t$. The CM equation for $E'\left(F_{q^9}\right)$ is $t_9^2 - 4q_9 = -3v_9^2$, which gives

$$v_9 = \frac{1}{243}(2u^9+1)(u-1)(u^{10} - u^9 - u - 2)(u^{10} - u^9 + 2u + 1)(u^{30} - 3u^{29} + 3u^{28} - u^{27} + 6u^{21} - 9u^{20} + 3u^{18} + 3u^{12} - 9u^{11} + 6u^9 - u^3 - 6u^2 - 3u + 1)(u^{30} - 3u^{29} + 3u^{28} - u^{27} - 3u^{21} + 9u^{19} - 6u^{18} - 6u^{12} + 9u^{10} - 3u^9 - u^3 + 3u^2 + 6u + 1)$$

.

The lemma 1 reveals that $t' = t_9$ provides us the right twist E'/F_{q^9} with $n|\#E'\left(F_{q^9}\right) = q^9 + 1 - t'$ and the cofactor is obtained as follows: $h_2 = \frac{q^9 + 1 - t'}{n}$.

4. Construction examples

This simple construction implements the method of section 2 for embedding degrees k = 9; 15; 21 and 27. Here is the algorithm used in each case:

1) Choose z of an appropriate size at random;
2) Set w = 3z and t = w + 2;
3) Compute r (See the section 2 for the formula);
4) If r is not prime, return to 1.;
5) Compute q (See the section 2 for the formula);
6) If q is not prime, return to step 1..

For three tests per case and a choice of 36 bits for z (k = 9; 15; 21) et 32 bits (k = 27), this algorithm allowed us to have the results below:

k = 9

TEST 1

z = 36415757326
r=566685827310513356807476630848122757994295821107358696924953260 28
q=676337632793440186288233767872832558926566282094642368205256956924747563288960580243488 7
n=676337632793440186288233767872832558926566282094642368205256956924747563288949655516290 8

the number of bits of r = 219 and the one of q = 292. The curve is $E: y^2 = x^3 + 1$ over F_q.

TEST 2

z = 27321889190
r=101081255467249090563088285326757198639449530714402780566810333111
q=679101341026917506879370736221511982968429367410035407518264542233461500700830914611471
n=679101341026917506879370736221511982968429367410035407518264542233461500700748948943900

the number of bits of r = 216 and the one of q = 289. The curve is $E: y^2 = x^3 + 1$ over F_q.

TEST 3

z = 6436858756

r=172842345364297139028781193814999977831846414216075093959329 97

q=64452626399350153015668800399527244895591949098096903853763248080154765247559447 97

n=64452626399350153015668800399527244895591949098096903853763248080154765054453685 28

the number of bits of r = 204 and the one of q = 272. The curve is $E: y^2 = x^3 + 1$ over F_q.

****

k = 15

TEST 1

z = 48973686304

r=55579209265812261882695387914798848748364565247950892734705743566285135050001315160793772801

q=13811704905557659693882480078094309642244413469712002075053362383018744281187112308122468421136530627387407285638408285478126216500828281717

n=13811704905557659693882480078094309642244413469712002075053362383018744281187112308122468421136530627387407285638408285478126187116616499292

the number of bits of r = 305 and the one of q = 456. The curve is $E: y^2 = x^3 + 1$ over F_q.

TEST 2

z = 55534775417

r=15196030705041885784527441669296051561170234570263148434270177383069469343448858123881269456161

q=62441595116711137024479034529981168248127721945764848669339510408230067485992868667031411375148293712356594863685554534753146545330550822727

n=62441595116711137024479034529981168248127721945764848669339510408230067485992868667031411375148293712356594863685554534753146512009685572424

the number of bits of r = 307 and the one of q = 458. The curve is $E: y^2 = x^3 + 1$ over F_q.

TEST 3

z = 12116384137

r=78017902983512929132436412581723443914629986637108006024400784399713167139958908077328 1

q=72639049817514329673305352427710679799287105607641800014632495485683955918718830410014880025143908726840577168572890646647966082277

n=72639049817514329673305352427710679799287105607641800014632495485683955918718830410014880025143908726840577168572890645920983034047

the number of bits of r = 289 and the one of q = 432. The curve is $E: y^2 = x^3 + 1$ over F_q.

****

k = 21

TEST 1

z = 25624898059

r=17448606995791526776788204168021844585677515618041440232515438902113396551788385534689564953627019301515006078749389216976731459029052 1

q=32500728306423326591493531013183087892128795719230721186639471607616219671138242862689520865681979591322530755673671173474762526189859443193252901165653466157736453492647261748127

n=32500728306423326591493531013183087892128795719230721186639471607616219671138242862689520865681979591322530755673671173474762526189859443193252901165653466157736453492493512359772

the number of bits of r = 446 and the one of q = 594. The curve is $E: y^2 = x^3 + 1$ over F_q.

TEST 2

z = 20656502916

r=13137011753853767514363020424983195961583870069159422381082204343068169700121597495860847377240805897283632296215409162131973144997969

q=10332550342029024527370502479551547020821170024569538416457302368958180608895164457498574082858810450078662743197515044816321107963855308215963882844408299534955302047271244451673

n=10332550342029024527370502479551547020821170024569538416457302368958180608895164457498574082858810450078662743197515044816321107963855308215963882844408299534955302041473054341 76

the number of bits of r = 443 and the one of q = 589. The curve is $E: y^2 = x^3 + 1$ over F_q.

TEST 3

z = 24159108282

r=86056922022687222074379473947071464243577659731347846674712075009268729647403456578629955850129102344221371960413976990334446862548249

q=12664648972426057031390477587645218708518751485321407938277064087765295277931065549025042975302582140058749772404912725278175681015671277094623198408366849386462871684116580808109

n=12664648972426057031390477587645218708518751485321407938277064087765295277931065549025042975302582140058749772404912725278175681015671277094623198408366849386462871683971626158416

the number of bits of r = 445 and the one of q = 592. The curve is $E: y^2 = x^3 + 1$ over F_q.

****

k = 27

TEST 1

z = 1761852512

r=34555185720510377565746672789472362345878796458662443539844805287089916527557451057735174399026736631101552113994076584108462318808552518693866334467190304444739041089367311695

q=96537231710119070331631199248259131314071631753924208957109025967522470427242839040600816704828045773731122865804522553917255424962634420228865410678738443897548426649303877731800720874299062561

n=96537231710119070331631199248259131314071631753924208957109025967522470427242839040600816704

48280457737311228658045225539172554249626344202288654106787384438975484266493038777318007208690135050 24
the number of bits of r = 580 and the one of q = 645.

TEST 2
z = 3166945406
r=13261471395388848205736798736491184837963753768196899777595889378429189620329934432325399179718113690186465779420554915704087637945335671777831579561697704606275245392286841577360 7
q=11970585028477261226008399811131262835193049551197746817163224722457514627249829658612479026570748310895622992753000614227569380318689893175249200840235560900523860670109914655574892244853449254807287
n=11970585028477261226008399811131262835193049551197746817163224722457514627249829658612479026570748310895622992753000614227569380318689893175249200840235560900523860670109914655574892244853439753971068
the number of bits of r = 596 and the one of q = 662.

TEST 3
z = 1547837572
r=33582904321788313351156195410819572015630746860286193720732651058248305740805571529072358448424340170124030544050661186947871332274170773129176787844452429061815796750760866 9
q=72412164693719640265074607607323386849600194806564674113863480622418264537341595025662053738674214716896709062799363363308382575509212909234013251950264636334898360088827961014774391312542358 1
n=72412164693719640265074607607323386849600194806564674113863480622418264537341595025662053738674214716896709062799363363308382575509212909234013251950264636334898360088827961014774390848191086 4
the number of bits of r = 577 and the one of q = 641.

5. Conclusion

We have shown how to effectively solve the problem of constructing elliptic curves from odd embedding degree, and have suggested ways to implement them efficiently so that pairing-based cryptosystems are more practical. In addition we defined the measures taken to circumvent the small subgroup attacks.

In the cases studied (k = 9; 15; 21; 27) for the subgroup security, we find that the cofactor h_2 is divisible by $(u-1)^2\left(u^2+u+1\right)$. So there is always a cofactor that is smaller than n in the order of G_2. This allows us to conclude that BLS curves for embedding degrees k = 9; 15; 21; 27 are sensitive to subgroup attacks. The membership test is always necessary to be sure to operate in the correct subgroup.

References

[1] T. Okamoto A. Menezes, S. Vanstone. “Reducing elliptic curve logarithms to logarithms in a finite field”. IEEE Transactions on Information Theory 39(1993), pp. 1639–1646, 1993.
[2] M. Nakabayashi, A. Miyaji, S. Takano. “New explicit conditions of elliptic curve traces for fr-reduction”. IEICE Trans. Fundamentals, E84 A, no. 5, May 2001.
[3] Ben Lynn Paulo S. L. M. Barreto, Michael Scott. “Constructing elliptic curves with prescribed embedding degrees”. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, SCN, 2576 of Lecture Notes in Computer Science, Springer, pp. 257–267, 2002.
[4] Paulo S. L. M. Barreto, Rafael Misoczki, Michael Naehrig, Geovandro C. C. F. Pereira, Craig Costello and Gustavo Zanon. “Subgroup security in pairing-based cryptography”. Progress in Cryptology - LATINCRYPT 2015, pp. 245-265, 2015.
[5] Chae Hoon Lim, Pil Joong Lee. “A key recovery attack on discrete log-based schemes using a prime order subgroup”. In Burton S. Kaliski Jr.,CRYPTO volume 1294 of Lecture Notes in Computer Science, Springer, pp. 249–263, 1997.
[6] B. Lynn D. Boneh, H. Shacham. “Short signatures from the weil pairing”. In Advances in Cryptology - Asiacrypt 2001, volume 2248 of Lecture Notes in Computer Science, Springer, pp. 514–532, 2002.
[7] IEEE P1363Working Group. “Standard specifications for public-key cryptography ieee std”. pp. 1363–2000, 2000.
[8] Ian F Blake, Gadiel Seroussi, Nigel Smart. “Elliptic curves in cryptography”. Cambridge university press, Lecture Note Series 265, 1999.
[9] Alfred Menezes. “Asymmetric pairings”. 2009. Talk at ECC2009. Slides at http://math.ucalgary.ca/ecc/files/ecc/u5/Menezes_ECC2009.pdf.