PARTICULARLY FRIENDLY MEMBERS OF FAMILY TREES

CRAIG COSTELLO

Abstract. The last decade has witnessed many clever constructions of parameterized families of pairing-friendly elliptic curves that now enable implementors targeting a particular security level to gather suitable curves in bulk. However, choosing the best curves from a (usually very large) set of candidates belonging to any particular family involves juggling a number of efficiency issues, such as the nature of binomials used to construct extension fields, the hamming-weight of key pairing parameters and the existence of compact generators in the pairing groups. In light of these issues, two recent works considered the best families for $k = 12$ and $k = 24$ respectively, and detailed subfamilies that offer very efficient pairing instantiations. In this paper we closely investigate the other eight attractive families with $8 \leq k < 50$, and systematically sub-divide each family into its *family tree*, branching off until concrete subfamilies are highlighted that simultaneously provide highly-efficient solutions to all of the above computational issues.

1. Introduction

At the turn of the century, the seminal papers of Sakai *et al.* [23], Joux [16] and Boneh and Franklin [6] gave birth to the now thriving field of pairing-based cryptography. While new and interesting cryptographic protocols exploiting the powerful bilinearity property of pairings are likely to continue arriving on the scene for a while yet, the accompanying field that focusses on optimized pairing computation is fast approaching full maturity [10, 31, 13, 2, 27].

In the context of cryptography, the most efficient pairings make use of large prime order subgroups of elliptic curves $E/\mathbb{F}_q$. For optimal performance, pairings at different security levels demand elliptic curves with different embedding degrees [24], so in their widely used taxonomy [10], Freeman, Scott and Teske present the best constructions of pairing-friendly curves corresponding to all embedding degrees $1 \leq k \leq 50$. For current levels of security, and for those in the foreseeable future, the optimal curve choices come from *parameterized families* of ordinary (non-supersingular) curves over prime fields $\mathbb{F}_p$. This means that the field size and the number of points on the curve are parameterized as $p(x)$ and $n(x)$ respectively. If $n(x)$ is reducible then $n = n(x_0)$ will not be prime in general, so we usually also write down $r(x)$, the largest irreducible factor of $n(x)$. The straightforward way to find curves within a given family is to seek x_0's of appropriate size such that $p(x_0)$ and $r(x_0)$ are prime (or $r(x_0)$ is almost prime), at which point we have suitable pairing-friendly curves with $r(x_0) \mid n(x_0) = \#E(\mathbb{F}_{p(x_0)})$. If left for a few minutes, a simple code that does exactly this can return many pairing-friendly curves, and in most cases this is just a tiny fraction of the potential curves that could be used to target a particular security level. A natural problem that faces serious implementors then, is how to find and use only the very best curves within a family: this is the motivation for this paper.

Related work. Since they are a perfect fit for the 128-bit security level, the Barreto-Naehrig (BN) family of curves [4] with $k = 12$ have already received a great deal of attention. Although several prior papers looked at subclasses of BN curves that offer advantages with respect to some aspects of a pairing computation [9, 5, 28], Pereira *et al.* [12] were the first to consider this problem from a holistic standpoint, factoring in all of the major parameter choices that arise in a pairing-based protocol. Among other things, their particular *implementation-friendly* subclass of BN curves gives highly-efficient and uniform tower constructions, automatic curve parameters for the correct sextic twist, and compact generators in the two elliptic curve groups (G_1 and G_2) involved in a pairing. Motivated by [12], Costello, Lauter and Naehrig [8] recently targeted

Key words and phrases. pairing-friendly curves, subfamilies, pairing implementation.

the 256-bit security level with a similar flavored but slightly different approach and pointed out implementation-friendly subfamilies of Barreto-Lynn-Scott (BLS) curves [3] with $k = 24$ that essentially exhibit the same attractive properties.

This work. We thoroughly treat the other eight stand-out candidates for pairing implementations with $8 \leq k < 50$, and point out highly attractive subfamilies of each. Since it is widely accepted that embedding degrees of the form $k = 2^i 3^j$ perform most efficiently [18], we look at the Kachisa-Schaefer-Scott (KSS) families [17] with $k = 16$, $k = 18$, $k = 32$ and $k = 36$, and at the BLS families [3] with $k = 27$ and $k = 48$. Following a recent (and quite surprising!) announcement by Aranha [1], we also include the BLS family with $k = 12$. In addition, thanks to a suggestion made to us by Michael Scott, we also consider the Brezing-Weng family [7] with $k = 8$; a prime candidate for pairings at the (triple-DES equivalent) 112-bit security level. In all eight scenarios, our systematic approach allows us to point out several implementation-friendly subfamilies that simultaneously offer all of the desirable properties mentioned above, and many more (see [12, §1]). As a resource for implementors, we provide many examples of pairing-friendly curves according to our favorite *picks* from each tree, which are all readily found within the corresponding families.

Organization. In Section 2 we begin by detailing how to read and use the family trees, as well as the main advantages of our approach. The next eight sections (§3-§10) are dedicated to the eight selected families; in each of these sections we present the corresponding family tree and our favourite picks from it. We conclude in Section 11 with recommendations.

2. Family Trees

For all of the parameterized families considered in this paper, the polynomials for the prime field characteristic $p(x)$ and/or the elliptic curve group order $n(x)$ have denominators, i.e. $p(x), n(x) \in \mathbb{Q}[x]$, but $p(x), n(x) \notin \mathbb{Z}[x]$. This means that only a subset of $x \in \mathbb{Z}$ will be such that $p(x)$ and $n(x)$ can both take on integers, and in all cases this subset is simply defined by some congruency condition, say $x \equiv a \bmod u$. In the simplest scenario, one then kick-starts a search for pairing-friendly curves by initializing an appropriately sized $x_0 \equiv a \bmod u$, and iterating with $x_0 \leftarrow x_0 + u$ until $p(x)$ is prime and $r(x)$, the largest irreducible factor of $n(x)$, is either a prime or almost prime. At this stage it is then possible to compute the curve equation, find simple irreducible polynomials over $\mathbb{F}_p$ to tower up to the full extension field, and determine which twisted curve is the correct one. In general, from one successful x_0 value (i.e. pairing-friendly curve) to the next, all of these parameters are likely to be different. In the end, there are many different combinations of the necessary pairing parameters to choose from, and therefore most of the curves encountered in a basic search will inevitably be discarded in favor of the very best ones. The ideal alternative is to be able to prescribe the desired properties in advance, and only search for curves that are guaranteed to exhibit all of them. This way, searches will avoid a great deal of unnecessary testing and, over any given time, have a better chance of finding supreme curves.

2.1. Branching out.

The natural way to proceed towards this goal is to start by subdividing the major equivalence class $x \equiv a \bmod u$ into smaller subclasses $x \equiv \{a + iu\}_{0 \leq i < v} \bmod uv$, and to individually separate each of the resulting subclasses again, repeating the process with the goal of arriving at subclasses where the curves found within it share identical parameters. There are three traits of the curve we aim to synchronize: the extension field tower used to represent $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$, the curve equation, and the *type* of twist (which only has two options - see below). Thus, we leave the twist classification until the end, so that subdivisions or *branchings* depend only on the towering choice and on the curve equation; at each stage, the choice of v that inflates the modulus above will be dictated by one or the other, or sometimes both. We always take the choice that we believe was most obvious, but argue that the end result doesn't matter; overall it will take the same sized inflation (and probably number of intermediate subdivisions) of the original modulus to determine the specific subclasses that give identical pairing parameters.

2.2. **Extension field towers.** For each family, we present between two and six stand-out towering options for the construction of $\mathbb{F}_{p^k}$. Our towers are presented using two binomials: one used for the first extension from $\mathbb{F}_p$ to either $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^3}$, and the other for the remainder of the extension up to $\mathbb{F}_{p^k}$. More often than not, this produces more preferable towers (faster extension field arithmetic) than if only one binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^k}$ was used to define the tower. For example, for any of the k considered in this paper, it is easy to show that $x^k \pm 1$ will never be irreducible[1] in $\mathbb{F}_p[x]$. However, choosing instead a different degree k irreducible binomial $x^k + s$ ($s \neq \pm 1$), means that the quadratic extension (if applicable) from $\mathbb{F}_p$ to $\mathbb{F}_{p^2}$ can no longer be constructed optimally as $\mathbb{F}_p[u]/(u^2+1)$. Alternatively, defining the tower with two binomials allows for $\mathbb{F}_{p^2} = \mathbb{F}_p[u]/(u^2+1)$, and $\mathbb{F}_{p^k}$ being constructed as, say $\mathbb{F}_{p^2}[v]/(v^{k/2} - (u+1))$, which is clearly preferable (cf. [2, 12, 8]). The towers T_i are described in the sections corresponding to each family, are given in (our) preferential order, and are marked red in the trees.

2.3. **Curve equations.** All families under consideration either have j-invariant 0 or 1728, meaning that the elliptic curve equation is defined by one constant: b in $y^2 = x^3 + b$ for $j = 0$ or a in $y^2 = x^3 + ax$ for $j = 1728$. In both cases, we always take the correct curve whose constant has the smallest absolute value, so any multiplications by it (if at all) incur the minimal number of $\mathbb{F}_p$ additions. In all scenarios herein, this results in less than 10 distinct a or b values that rear their heads most commonly. The curve constants used to subdivide congruencies are the subscripts of the a_i or b_i values marked blue in the trees.

2.4. **Type of twist.** If the binomial used to extend from the twisted subfield $\mathbb{F}_{p^d}$ to the full extension field $\mathbb{F}_{p^k}$ is $x^{k/d} - i$ with $i \in \mathbb{F}_{p^d}$, then Scott [26] shows that for the sake of quartic twists on $y^2 = x^3 + ax$ and sextic twists on $y^2 = x^3 + b$, the correct twist is either type M (multiplication) which is given by $y^2 = x^3 + ax \cdot i$ and $y^2 = x^3 + b \cdot i$ respectively, or type D (division) which is given by $y^2 = x^3 + ax/i$ and $y^2 = x^3 + b/i$ respectively. The only other case is the cubic twist for $k = 27$ in Section 7, where we define the type M twist as $y^2 = x^3 + b \cdot i^2$ and the type D twist as $y^2 = x^3 + b/i^2$; this is to force quadratic reciprocity of the element in the twisted subfield. The type of twist corresponding to any given congruency is found immediately above (or in rare cases besides) the subclass; this is marked dark green in the trees. There is no great difference or preference between the two, if they are dealt with correctly (see [26, §5] and [8, §4]).

2.5. **Fruits.** If a subclass or subclasses of a family share all three traits, we call them *fruits*[2] and they are labelled light green in the trees. Any equivalence classes found in the same fruit *bunch* share the same three parameters described in the previous three paragraphs; all three parameters can be easily seen by following the branches back up to the top of the tree. The most immediate bold number found above any bunch is the modulus corresponding to the equivalence classes in the bunch. Any branchings that don't (yet) produce consistent pairing parameters for its congruencies are marked grey, and are called *unripe*. In almost all cases pursuing further branching of the unripe fruits gives either undesirable pairing parameters, or congruency classes that are too scarce for our recommendation.

2.6. **Our "picks".** After presenting a family tree, we pick our favorite subfamilies in it, and give them a star rating (up to 5). Our choice is mostly influenced by the towering option, since we believe this has the greatest effect on the pairing efficiency. For each of our favorite subfamilies, we searched for compact representations of generators in both the elliptic curve groups G_1 and G_2. In most families, our favorite subfamilies either exhibit one or the other, or both. In many cases there are several suitable generators, so we have put some of the extra options in Appendix B. For subfamilies where generators in either group aren't given, it does not mean that one or more compact generators doesn't exist; it just means that our (somewhat basic) searches weren't able to find any. Moreover, for any one particular curve belonging to the subfamily, there's still a good chance that compact generators (that don't apply to the entire subfamily) can be found. Beside

[1] See [8, Prop. 1] for the $3 \nmid k$ cases, whilst the $3 \mid k$ case is obvious.

[2] Our analogy has no intended relation to the well known "low-hanging fruit" analogy, which is also sometimes used in the context of pairing-based cryptography [25].

each of our picks, we give approximate frequencies of the corresponding subfamily across the entire family of curves. Most of these percentages were calculated from somewhere between $5,000$ and $175,000$ example curves from each family[3], and are essentially always as we would expect, given the corresponding resctriction on the original congruency. In Appendix C, we account for a wide range of security levels and provide comprehensive lists of low hamming-weight curves belonging to 5-star subfamilies.

2.7. **Advantages.** The tree approach is exhaustive and complete, i.e. the branching technique described above doesn't lose track of any congruencies, which means that every curve belonging to a family under consideration fits somewhere in the family tree presented. Another advantage of presenting the entire tree, rather than just presenting specific subfamilies, is that many implementors will only want to simultaneously assure some proper subset of the properties we used to form the family trees. Thus, one can group together separate bunches of the tree that share this subset of desirable properties, and ignore the other property/s that caused them to branch away from one another. As an example, suppose one is using affine coordinates for a pairing implementation on a $k = 18$ KSS curve of the form $y^2 = x^3 + b$. The curve and pairing arithmetic will therefore be independent of b (cf. [19]), so if the implementors are not necessitating consistent compact generators in G_1 or G_2, then all bunches with identical towers and twist types (but different curve equations) could be grouped in the same search, and use the same ($\mathbb{F}_p$-independent) pairing code.

2.8. **Proofs.** Since the proofs are tedious and repetitive, they have been tightly crammed into Appendix A. We provide proofs of the irreducibility criterions for the extension field towers, which rely on elementary number theory (quadratic and cubic reciprocity modulo p) that is essentially due to Gauss and Euler. We also make constant use of a helpful theorem due to Benger and Scott [5]. Since all the elliptic curves within have special CM discriminants, we don't need the (deeper) more general CM theory for the correct curve equations, but instead draw heavily on Algorithms 3.4 and 3.5 of [22], which are also "essentially due to Gauss". For every family, the proofs of the twist type (which is always one of two options - see [14, Prop. 8]) follow the recipe in the proof of [8, Prop. 4], so we omit them for space considerations. We do not prove any non-existence or negative results, e.g. that an extension field tower which would clearly be preferred does not (always) apply to this congruency, but the reader should rest assured that we tried all such options, and this is indeed the case.

2.9. **Other parameters.** Along with $p(x)$, $r(x)$ and $n(x)$, the description of the polynomial parameterizations for each family include the trace of Frobenius $t(x)$, the G_1 cofactor $h(x) = n(x)/r(x)$, and $f(x)$, which comes from the CM norm equation $4p = t^2 - Df^2$. The polynomials $f(x)$ and $t(x)$ are commonly used in the proofs.

2.10. **x or x′.** The four KSS families all start with congruencies of the form $x \equiv \pm au \bmod bu$. For the purpose of simplicity, we replace x by $x' = x/u$ and work instead with the simpler expression $x' \equiv a \bmod b$. We therefore remind those making use of the results within to inflate the x' congruency back to the congruency in x when searching for curves, or alternatively update the polynomials for $p(x)$ and $n(x)$ to $p'(x')$ and $n'(x')$, etc.

3. Brezing-Weng $k = 8$ curves

The polynomial parameterizations for Brezing-Weng family with $k = 8$ are:

$$p(x) = (81x^6 + 54x^5 + 45x^4 + 12x^3 + 13x^2 + 6x + 1)/4; \qquad f(x) = 3x + 1;$$
$$t(x) = -9x^3 - 3x^2 - 2x; \qquad n(x) = (9x^2 - 6x + 5) \cdot (9x^4 + 12x^3 + 8x^2 + 4x + 1)/4;$$
$$h(x) = 9x^2/2 - 3x + 5/2; \qquad r(x) = (9x^4 + 12x^3 + 8x^2 + 4x + 1)/2. \tag{3.1}$$

We found three towers that were often applicable to the congruencies found in the family tree. They are defined by the binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^2}$ and the binomial from $\mathbb{F}_{p^2}$ to $\mathbb{F}_{p^8}$ (see Table 1). The polynomials for $p(x)$ and $n(x)$ in (3.1) insist that x is odd, so we begin with the congruence

[3]See `http://www.craigcostello.com.au/pairing`

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^2+u_i)} \mathbb{F}_{p^2} \xrightarrow{\mathbb{F}_{p^2}[v]/(u^4-v_i)} \mathbb{F}_{p^8}$			
T_i	T_1	T_2	T_3
(u_i, v_i)	$(2, u)$	$(3, u)$	$(5, u)$

TABLE 1. Efficient towering options in the $k = 8$ Brezing-Weng tree.

$x \equiv 1 \bmod 2$ and branch off into sub-congruencies to form the family tree in Figure 1 (see Appendix A for the proofs). We pick several fruit bunches that offer particularly friendly parameters for the pairing computation, and provide compact generators in the groups G_1 and G_2 where we found them (see Table 2). The frequencies in the final column were calculated from over 128,000 different Brezing-Weng curves and are entirely as expected. Our 5-star picks constitute approximately 50% of the entire family.

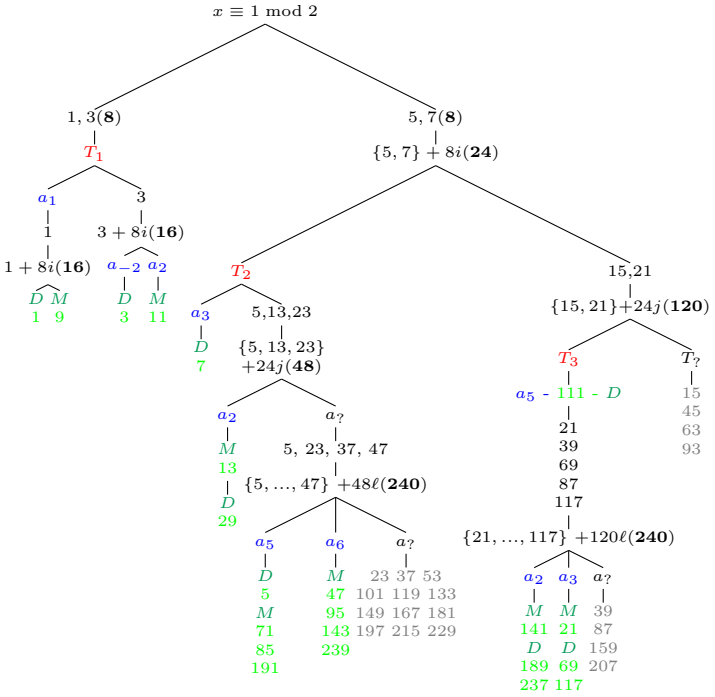

FIGURE 1. The $k = 8$ Brezing-Weng tree.

rating	equiv. class for x	tower	a	twist type	G_1 gen. $[h](\cdot,\cdot)$	G_2' gen. $[h^7](\cdot,\cdot)$	more §B.1	%
	1 mod 16	T_1	1	D	-	$(u, \sqrt{1-2u})$	(i)	12.5
	9 mod 16	T_1	1	M	-	$(u-1, \sqrt{3})$	(ii)	12.6
⋆⋆⋆⋆⋆	3 mod 16	T_1	-2	D	$(1, \sqrt{-1})$	$(u-1, \sqrt{3})$	(iii)	12.3
	11 mod 16	T_1	2	M	-	$(1, \sqrt{1+2u})$	(iv)	12.5
	7 mod 24	T_2	3	D	$(1, 2)$	$(1, 1+3/u)$	(v)	8.4
	13 mod 48	T_2	2	M	$(4, 6\sqrt{2})$	$(u-1, \sqrt{2-2u})$	(vi)	4.1
	29 mod 48	T_2	2	D	$(4, 6\sqrt{2})$	-	(vii)	4.2
⋆⋆⋆⋆	$\{47, \ldots, 239\}_4 \bmod 240$	T_2	6	M	-	$(1, \sqrt{1+6u})$		3.4
	71, 85, 191 mod 240	T_2	5	M	$(2, 2\sqrt{3})$	-	$(viii)$	2.4
	5 mod 240	T_2	5	D	$(2, 2\sqrt{3})$	$(5, \sqrt{125+25/u})$	(ix)	0.9

TABLE 2. Our favorite picks from the $k = 8$ Brezing-Weng tree.

4. BLS $k = 12$ curves

The polynomial parameterizations for BLS family with $k = 12$ are:

$$p(x) = (x-1)^2(x^4 - x^2 + 1)/3 + x; \quad n(x) = (x-1)^2(x^4 - x^2 + 1)/3; \quad t(x) = x + 1;$$
$$h(x) = (x-1)^2/3; \qquad f(x) = (x-1)(2x^2 - 1)/3; \qquad r(x) = x^4 - x^2 + 1. \tag{4.1}$$

We found six towers that were often applicable to the congruencies found in the family tree. They

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^2+u_i)} \mathbb{F}_{p^2} \xrightarrow{\mathbb{F}_{p^2}[v]/(u^6-v_i)} \mathbb{F}_{p^{12}}$						
T_i	T_1	T_2	T_3	T_4	T_5	T_6
(u_i, v_i)	$(1, u+1)$	$(1, u+2)$	$(1, u+3)$	$(2, u)$	$(2, u+2)$	$(5, u)$

TABLE 3. Efficient towering options in the $k = 12$ BLS tree.

are defined by the binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^2}$ and the binomial from $\mathbb{F}_{p^2}$ to $\mathbb{F}_{p^{12}}$ (see Table 3). The

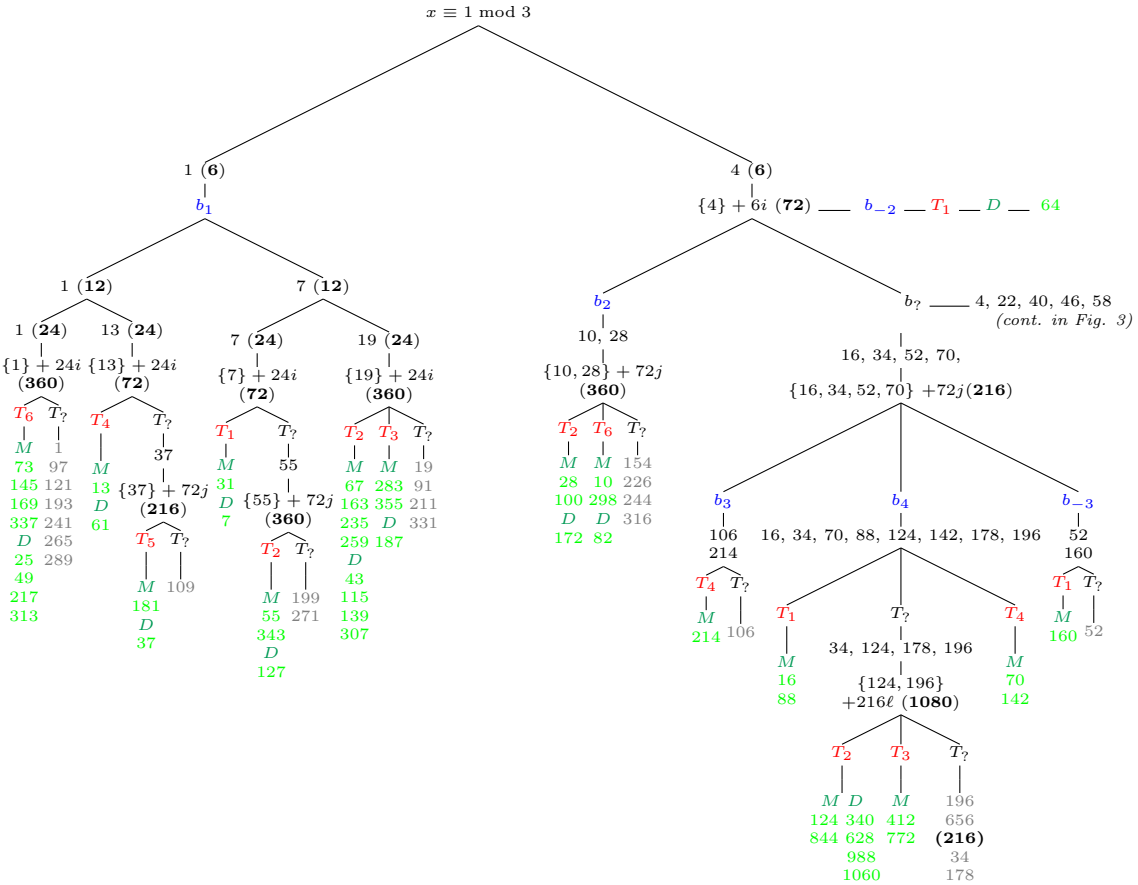

FIGURE 2. The $k = 12$ BLS tree.

polynomials for $p(x)$ and $n(x)$ in (4.1) insist that $x \equiv 1 \bmod 3$, so we begin with this congruence and branch off into sub-congruencies to form the family tree in Figure 2 (see Appendix A for the proofs). To fit the tree in, one of the branches has been snapped off and is on its own in Figure 3. We pick several fruit bunches that offer particularly friendly parameters for the pairing computation, and provide compact generators in the groups G_1 and G_2 where we found them (see Table 4). The frequencies in the final column were calculated from over 170,000 different BLS curves and are entirely as expected. Our 5-star picks constitute approximately 17% of the entire family.

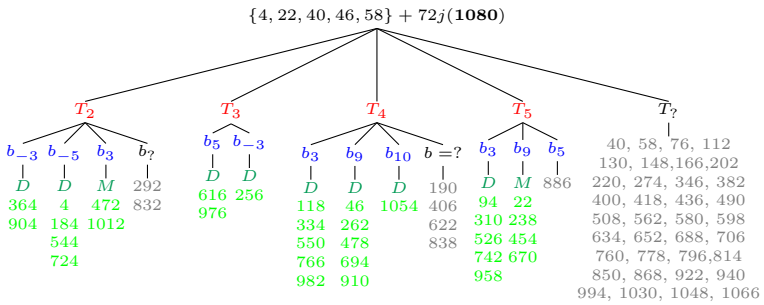

FIGURE 3. Another branch of the $k = 12$ BLS family tree.

rating	equiv. class for x	tower	b	twist type	G_1 gen. $[h](\cdot,\cdot)$	G_2' gen. $[h'](\cdot,\cdot)$	more §B.2	%
	64 mod 72	T_1	-2	D	$(-1,\sqrt{-3})$	$\left(1,\sqrt{\frac{u-1}{u+1}}\right)$		4.2
	31 mod 72	T_1	1	M	-	$(-1,\sqrt{u})$		4.1
⋆⋆⋆⋆⋆	7 mod 72	T_1	1	D	-	-		4.2
	16, 88 mod 216	T_1	4	M	-	$(-1,\sqrt{4u+3})$		2.8
	160 mod 216	T_1	-3	M	$(-1,\sqrt{-2})$	$(-1,\sqrt{-3u-4})$	(i)	1.4
	$\{67,...,259\}_4$ mod 360	T_2	1	M	$\left(1,\sqrt{2}\right)$	$(-1,\sqrt{u+1})$		3.3
	55, 343 mod 360	T_2	1	M	-	$(1,\sqrt{u+3})$		1.7
	$\{43,...,307\}_4$ mod 360	T_2	1	D	$\left(1,\sqrt{2}\right)$	$\left(1,\sqrt{\frac{u+3}{u+2}}\right)$		3.3
	127 mod 360	T_2	1	D	-	$\left(-1,\sqrt{-\frac{u+1}{u+2}}\right)$		0.8
⋆⋆⋆⋆	28, 100 mod 360	T_2	2	M	$(-1,1)$	-		1.7
	172 mod 360	T_2	2	D	$(-1,1)$	-		0.8
	124, 844 mod 1080	T_2	4	M	-	$(-2,2\sqrt{u})$		0.6
	$\{340,...,1060\}_4$ mod 1080	T_2	4	D	-	$\left(-1,\sqrt{\frac{2-u}{2+u}}\right)$		1.1
	283, 355 mod 360	T_3	1	M	$\left(1,\sqrt{2}\right)$			1.7
⋆⋆⋆	187 mod 360	T_3	1	D	$\left(1,\sqrt{2}\right)$	$\left(-1,\sqrt{-\frac{u+2}{u+3}}\right)$		0.8

TABLE 4. Our favorite picks from the $k = 12$ BLS tree.

5. KSS $k = 16$ CURVES

The polynomial parameterizations for KSS family with $k = 16$ are:

$$p(x) = (x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125)/980;$$
$$r(x) = x^8 + 48x^4 + 625; \quad t(x) = (2x^5 + 41x + 35)/35; \quad h(x) = (x^2 + 2x + 5)/980;$$
$$n(x) = (x^2 + 2x + 5)(x^8 + 48x^4 + 625)/980; \quad f(x) = (x^5 + 5x^4 + 38x + 120)/35. \tag{5.1}$$

There were three common towers found in the family tree. They are defined by the binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^2}$ and the binomial from $\mathbb{F}_{p^2}$ to $\mathbb{F}_{p^{16}}$ (see Table 5). The polynomials for $p(x)$ and

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^2+u_i)} \mathbb{F}_{p^2} \xrightarrow{\mathbb{F}_{p^2}[v]/(u^8-v_i)} \mathbb{F}_{p^{16}}$			
T_i	T_1	T_2	T_3
(u_i, v_i)	$(2, u)$	$(3, u)$	$(5, u)$

TABLE 5. Efficient towering options in the $k = 16$ KSS tree.

$n(x)$ in (5.1) insist that $x \equiv \pm 25 \bmod 70$, so for simplicity we rescale $x' = x/5$ and begin with $x' \equiv \pm 5 \bmod 14$, branching off into sub-congruencies to form the family tree in Figure 4 (see Appendix A for the proofs). It is easy to see that $r(x)$ always has $2 \cdot 5^4 \cdot 7^2$ as a factor, so this division is necessary for (the updated) $r(x)$ to represent primes. We pick several fruit bunches that offer particularly friendly parameters for the pairing computation, and provide compact generators in the groups G_1 and G_2 where we found them (see Table 6). The frequencies in the final column were calculated from over 13,000 different KSS curves with $k = 16$ and are entirely as expected. Our 5-star picks constitute approximately 50% of the entire family. The generators in $G_2' = E'(\mathbb{F}_{p^4})$ use $v \in \mathbb{F}_{p^4}$, where $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}[v]/(v^2 - u)$.

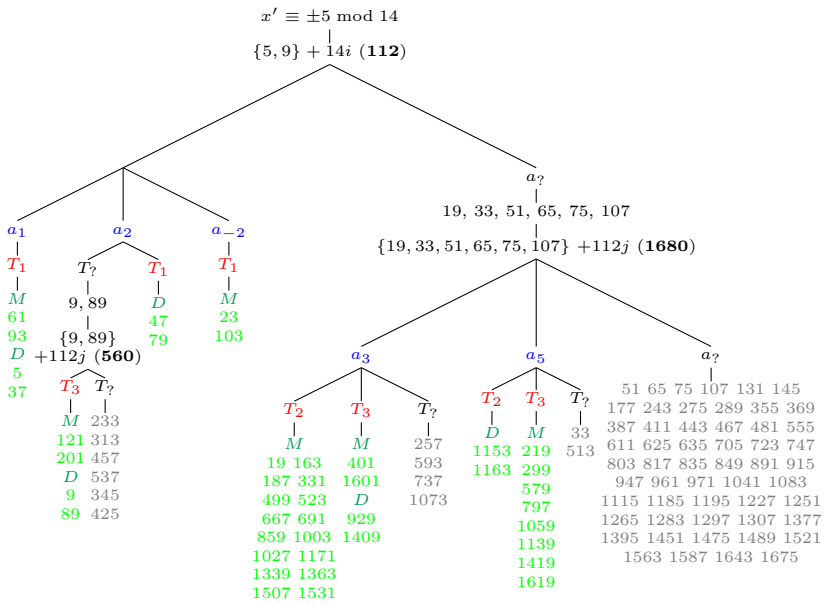

FIGURE 4. The $k = 16$ KSS family tree.

rating	equiv. class for x' ($x' = x/5$)	tower	a	twist type	G_1 gen. $[h](\cdot, \cdot)$	G_2' gen. $[h'](\cdot, \cdot)$	%
	$61, 93 \bmod 112$	T_1	1	M	-	$\left(v-1, \sqrt{(v-1)^3 + v(v-1)}\right)$	12.2
	$5, 37 \bmod 112$	T_1	1	D	-	$\left(-v, \sqrt{-v^3 - 1}\right)$	12.7
⋆⋆⋆⋆⋆	$47, 79 \bmod 112$	T_1	2	D	-	$\left(2/v, \sqrt{\frac{8}{v^3} + \frac{4}{v^2}}\right)$	12.1
	$23, 103 \bmod 112$	T_1	-2	M	$\left(1, \sqrt{-1}\right)$	-	13.1
⋆⋆⋆⋆	$\{19, ..., 1531\}_{16} \bmod 1680$	T_2	3	M	$(1, 2)$	$\left(3/v, \sqrt{\frac{27}{v^3} + \frac{9}{v^2}}\right)$	7.9
⋆⋆⋆	$1153, 1633 \bmod 1680$	T_2	5	D	$\left(2, 2\sqrt{3}\right)$	-	0.9

TABLE 6. Our favorite picks from the $k = 16$ KSS tree.

6. KSS $k = 18$ CURVES

The polynomial parameterizations for KSS family with $k = 18$ are:

$$p(x) = (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21;$$
$$r(x) = x^6 + 37x^3 + 343; \qquad t(x) = (x^4 + 16x + 7)/7; \qquad h(x) = (x^2 + 5x + 7)/21;$$
$$n(x) = (x^2 + 5x + 7)(x^6 + 37x^3 + 343)/21; \qquad f(x) = (5x^4 + 14x^3 + 94x + 259)/21. \tag{6.1}$$

There were five common towers found in the family tree. They are defined by the cubic binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^3}$ and the binomial from $\mathbb{F}_{p^3}$ to $\mathbb{F}_{p^{18}}$ (see Table 7). The polynomials for $p(x)$ and

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^3+u_i)} \mathbb{F}_{p^3} \xrightarrow{\mathbb{F}_{p^3}[v]/(u^6-v_i)} \mathbb{F}_{p^{18}}$					
T_i	T_1	T_2	T_3	T_4	T_5
(u_i, v_i)	$(2, u)$	$(2, 2u)$	$(3, 2u)$	$(5, u)$	$(2, 5u)$

TABLE 7. Efficient towering options in the $k = 18$ KSS tree.

$n(x)$ in (6.1) insist that $x \equiv 14 \bmod 42$, so we rescale $x' = x/14$ and begin with $x' \equiv \pm 1 \bmod 3$, branching off into sub-congruencies to form the family tree in Figure 5 (see Appendix A for the proofs). As it stands, $r(x)$ will always contain 7^3 as a factor, so this division is necessary for (the updated) $r(x)$ to represent primes. Our favorite picks and the associated generators are in Table 8. The frequencies in the final column were calculated from over 25,000 different KSS curves with $k = 18$ and are as expected. Our 5-star picks constitute approximately 27% of the entire family.

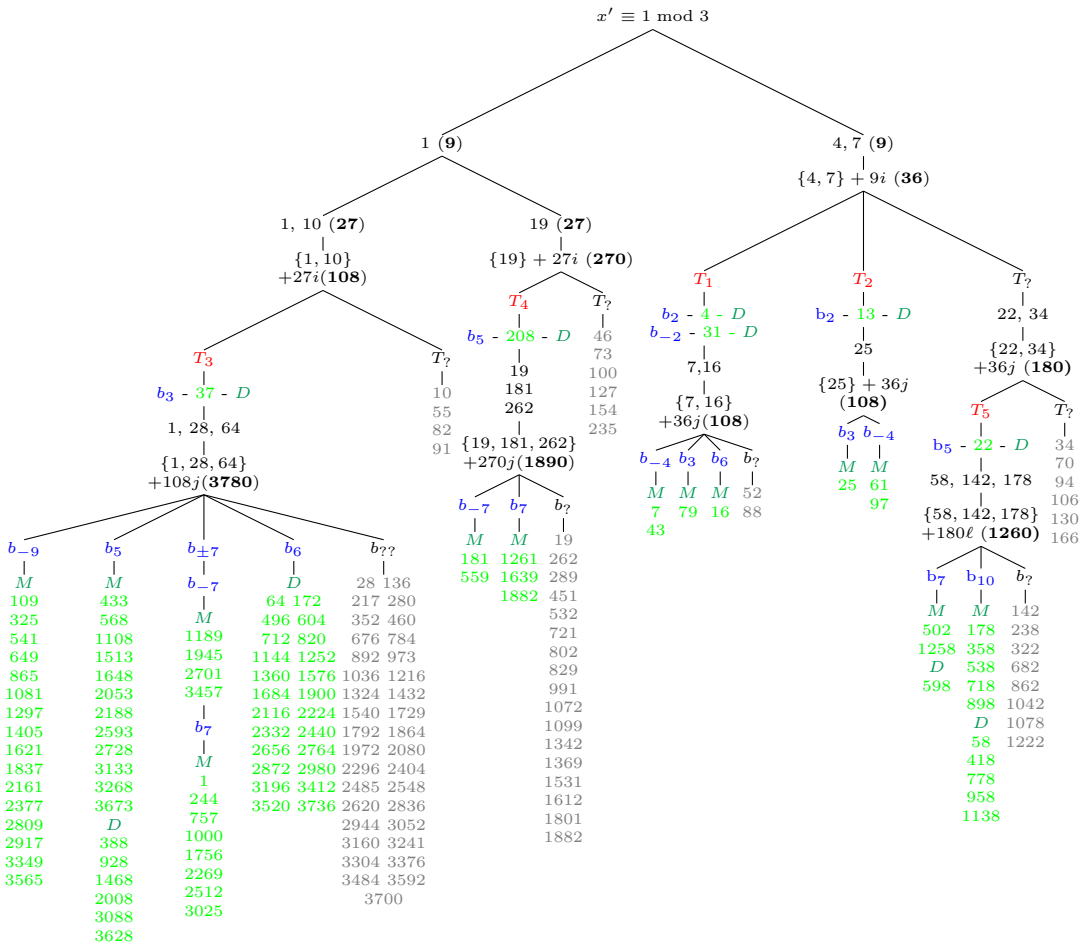

FIGURE 5. The $k = 18$ KSS family tree.

rating	equiv. class for $x' = x/14$	tower	b	twist type	G_1 gen. $[h](\cdot,\cdot)$	G_2' gen. $[h'](\cdot,\cdot)$	more §B.3	%
	$4 \bmod 36$	T_1	2	D	$(-1,1)$	$\left(1, \sqrt{\frac{u+2}{u}}\right)$	(i)	8.4
	$31 \bmod 36$	T_1	-2	D	$(3,5)$	$\left(1-u, \sqrt{(1-u)^3 - 2/u}\right)$	(ii)	7.9
⋆⋆⋆⋆⋆	$7, 43 \bmod 108$	T_1	-4	M	$(2,2)$	$\left(-2, 2\sqrt{-(u+2)}\right)$	(iii)	5.3
	$79 \bmod 108$	T_1	3	M	$(1,2)$	$\left(-1, \sqrt{-1+3u}\right)$	(iv)	2.9
	$16 \bmod 108$	T_1	6	M	$\left(-1, \sqrt{5}\right)$	$\left(2, \sqrt{2+6u}\right)$		2.9
	$13 \bmod 36$	T_2	2	D	$(-1,1)$	-		8.3
⋆⋆⋆⋆	$61, 97 \bmod 108$	T_2	-4	M	$(2,2)$	$\left(2, 2\sqrt{2-2u}\right)$	(v)	5.5
	$25 \bmod 108$	T_2	3	M	$(1,2)$	-		2.8
	$37 \bmod 108$	T_3	3	D	$(1,2)$	$\left(1, \sqrt{\frac{2u+3}{2u}}\right)$		2.9
	$\{109, ..., 3565\}_{16} \bmod 3708$	T_3	-9	M	$\left(1, 2\sqrt{-2}\right)$	$\left(-3, 6\sqrt{-1}\right)$		1.4
	$\{568, ..., 3673\}_{13} \bmod 3708$	T_3	5	M	$(-1,2)$	-	(vi)	1.0
⋆⋆⋆	$\{328, ..., 3628\}_6 \bmod 3708$	T_3	5	D	$(-1,2)$	-	(vi)	0.5
	$\{1189, ..., 3457\}_4 \bmod 3708$	T_3	-7	M	$(2,1)$	-	(vii)	0.4
	$\{1, ..., 2512\}_8 \bmod 3708$	T_3	7	M	$\left(7, 5\sqrt{14}\right)$	-		0.7
	$\{64, ..., 3736\}_{24} \bmod 3708$	T_3	6	D	-	$\left(u-1, \sqrt{(u-1)^3 + 3/u}\right)$		1.9

TABLE 8. Our favorite picks from the $k = 18$ KSS tree.

7. BLS $k = 27$ curves

The polynomial parameterizations for BLS family with $k = 27$ are:

$$p(x) = (x+1)^2(x^{18} - x^9 + 1)/3 - x^{19}; \quad r(x) = x^{18} - x^9 + 1; \quad f(x) = (x^{10} - 2x^9 + x + 1)/3;$$
$$n(x) = (x^2 - x + 1)(x^{18} - x^9 + 1)/3; \quad t(x) = -x^{10} + x + 1; \quad h(x) = (x^2 - x + 1)/3. \tag{7.1}$$

There were three common towers found in the family tree. They are defined by the cubic binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^3}$ and the binomial from $\mathbb{F}_{p^3}$ to $\mathbb{F}_{p^{27}}$ (see Table 9). The polynomials for $p(x)$ and

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^3+u_i)} \mathbb{F}_{p^3} \xrightarrow{\mathbb{F}_{p^3}[v]/(u^9-v_i)} \mathbb{F}_{p^{27}}$			
T_i	T_1	T_2	T_3
(u_i, v_i)	$(3, u)$	$(5, u)$	$(7, u)$

Table 9. Efficient towering options in the $k = 27$ BLS tree.

$n(x)$ in (7.1) insist that $x \equiv 1 \bmod 3$, which we use to branch off into sub-congruencies, forming the family tree in Figure 6 (see Appendix A for the proofs). As it stands, $r(x)$ will always contain 3 as a factor, so division by 3 is necessary for (the updated) $r(x)$ to represent primes. Our favorite

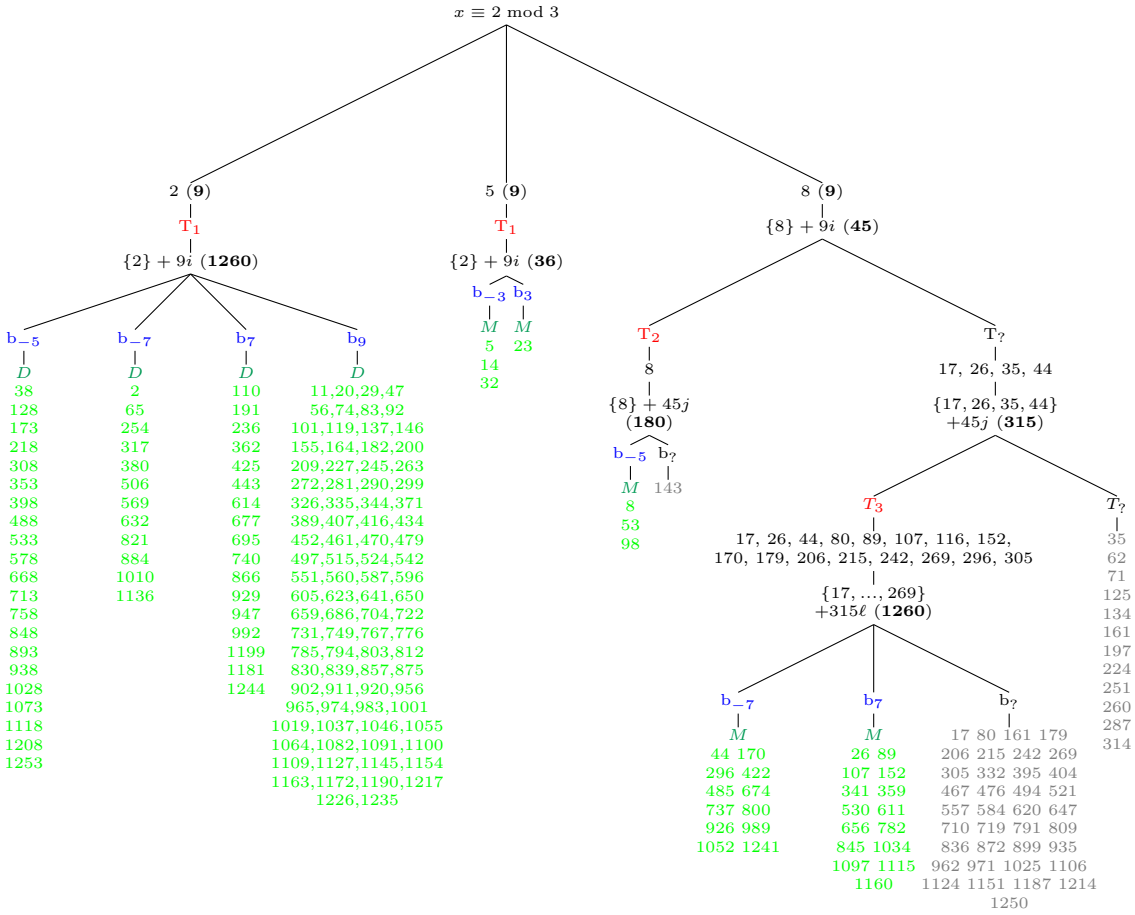

Figure 6. The $k = 27$ BLS family tree.

picks and the associated generators are in Table 10. The frequencies in the final column were calculated from over 6,000 different BLS curves with $k = 27$ and behave as expected. Our 5-star picks constitute approximately 66% of the entire family. The generators in $G_2' = E'(\mathbb{F}_{p^9})$ use $v \in \mathbb{F}_{p^9}$, where $\mathbb{F}_{p^9} = \mathbb{F}_{p^3}[v]/(v^3 - u)$.

rating	equiv. class for x	tower	b	twist type	G_1 gen.	G_2' gen.	more §B.4	%
	5 mod 36	T_1	-3	M	-	-		8.5
	$14, 32 \bmod 36$	T_1	-3	M	$[h]\,(1, \sqrt{-2})$	-		16.8
	23 mod 36	T_1	3	M	$[h]\,(1, 2)$	-		7.8
⋆⋆⋆⋆⋆	$\{38, ..., 1253\}_{21} \bmod 1260$	T_1	-5	D	-	-		5.0
	$\{2, .., 1136\}_{12} \bmod 1260$	T_1	-7	D	$[h]\,(2, 1)$	-	(i)	3.1
	$\{110, .., 1244\}_{17} \bmod 1260$	T_1	7	D	$[h]\,(-7, 4\sqrt{-21})$	-	(ii)	4.0
	$\{11, .., 1235\}_{89} \bmod 1260$	T_1	9	D	$[h]\,(-2, 1)$	-	(iii)	21.0
⋆⋆⋆⋆	$8, 98 \bmod 180$	T_2	-5	M	$[h]\,(-3, 4\sqrt{-2})$	-		3.3
	$53 \bmod 180$	T_2	-5	M	-	-		1.67

TABLE 10. Our favorite picks from the $k = 27$ BLS tree.

8. KSS $k = 32$ CURVES

The polynomial parameterizations for the KSS family with $k = 32$ are:

$$p(x) = (x^{18} - 6x^{17} + 13x^{16} + 57120x^{10} - 344632x^9 + 742560x^8 + 815730721x^2 - 4948305594x + 10604499373)/2970292; \qquad t(x) = (-2x^9 - 56403x + 3107)/3107;$$

$$r(x) = x^{16} + 57120x^8 + 815730721; \quad f(x) = 3x^9 - 13x^8 + 86158x - 371280;$$

$$n(x) = (x^2 - 6x + 13)(x^{16} + 57120x^8 + 815730721)/2970292; \quad h(x) = (x^2 - 6x + 13)/2970292. \tag{8.1}$$

There were only two common (and efficient) towers found in the family tree. They are defined by the quadratic binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^2}$ and the binomial from $\mathbb{F}_{p^2}$ to $\mathbb{F}_{p^{32}}$ (see Table 11). The polynomials for $p(x)$ and $n(x)$ in (8.1) insist that $x \equiv \pm 325 \bmod 6214$, so we rescale with

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^2+u_i)} \mathbb{F}_{p^2} \xrightarrow{\mathbb{F}_{p^2}[v]/(u^{16}-v_i)} \mathbb{F}_{p^{32}}$		
T_i	T_1	T_2
(u_i, v_i)	$(2, u)$	$(3, u)$

TABLE 11. Efficient towering options in the $k = 32$ KSS tree.

$x' = x/13$ and begin with $x' \equiv \pm 25 \bmod 478$, which branches off into sub-congruencies forming the family tree in Figure 7 (see Appendix A for the proofs). As it stands, $r(x)$ will always contain $2 \cdot 13^8 \cdot 239^2$ as a factor, so we must divide this factor out before (the updated) $r(x)$ can represent primes. Our favorite picks and the associated generators are in Table 12. The frequencies in the

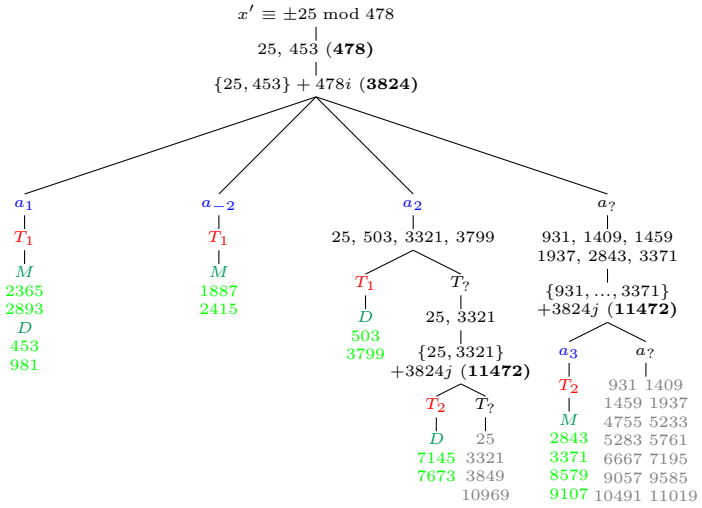

FIGURE 7. The $k = 32$ KSS family tree.

final column were calculated from over 2,600 different KSS curves with $k = 32$ and are roughly as expected. Our 5-star picks constitute approximately 51% of the entire family. The generators in $G_2' = E'(\mathbb{F}_{p^8})$ use $w \in \mathbb{F}_{p^8}$, where $\mathbb{F}_{p^8} = \mathbb{F}_{p^4}[w]/(w^2 - v)$, and $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}[v]/(v^2 - u)$.

rating	equiv. class for $x' = x/13$	tower	a	twist type	G_1 gen. $[h](\cdot,\cdot)$	G_2' gen. $[h']$$(\cdot,\cdot)$	more §B.5	%
	$2365, 2893 \bmod 3824$	T_1	1	M	-	$\left(w-1, \sqrt{w^3-2w^2+2w-1}\right)$		13.2
⋆⋆⋆⋆⋆	$453, 981 \bmod 3824$	T_1	1	D		$\left(w, \sqrt{w^3+1}\right)$		11.5
	$1887, 2415 \bmod 3824$	T_1	-2	M	$(-1,1)$	-	(i)	13.3
	$503, 3799 \bmod 3824$	T_1	2	D	-	-		12.7
	$7145, 7673 \bmod 11472$	T_2	2	D	$\left(4, 6\sqrt{2}\right)$	-	(ii)	5.4
⋆⋆⋆⋆	$\{2843, ..., 9107\}_4$ mod11472	T_2	3	M	$(1,2)$	-	(iii)	13.0

TABLE 12. Our favorite picks from the $k = 32$ KSS tree.

9. KSS $k = 36$ CURVES

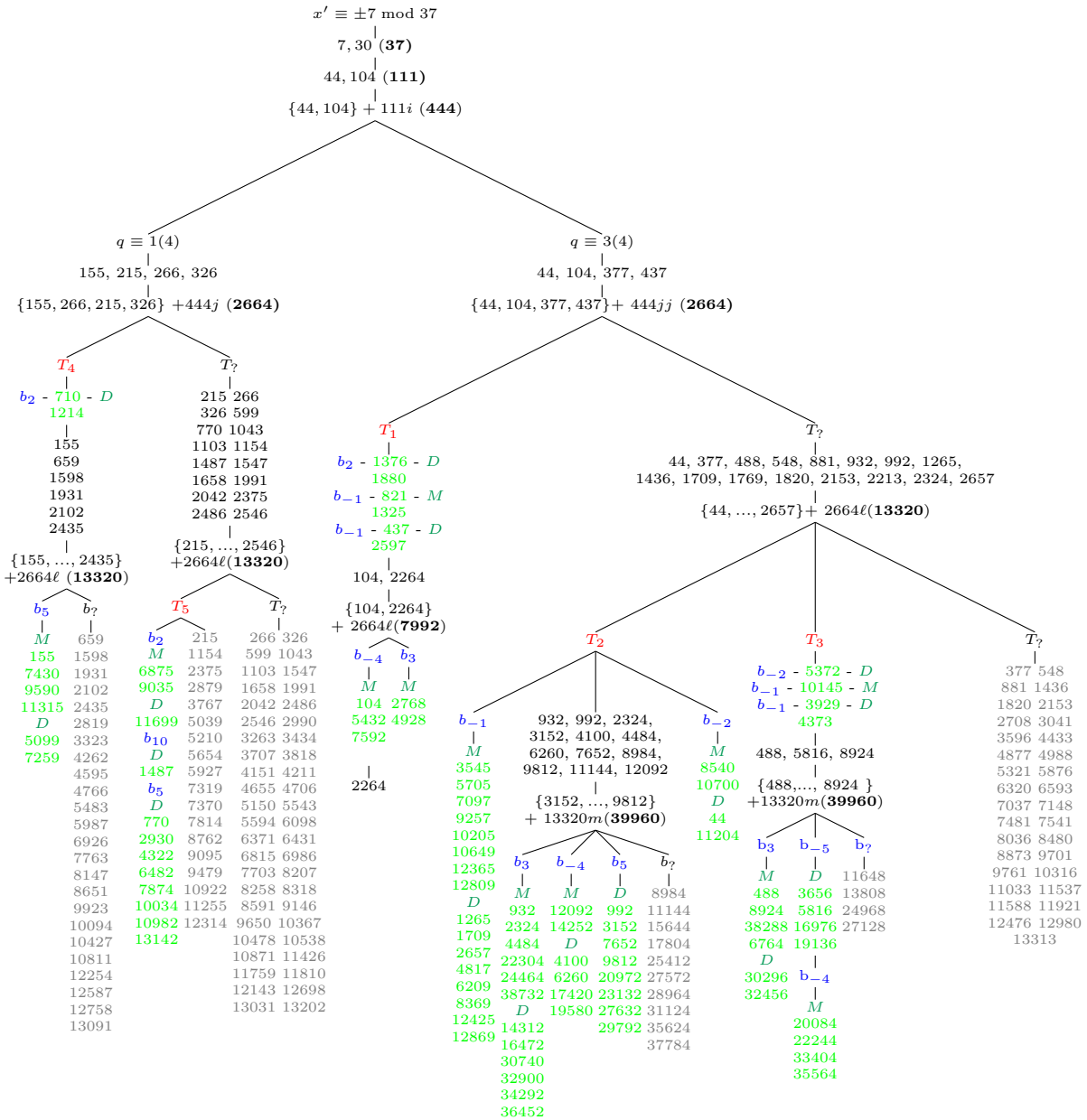

FIGURE 8. The $k = 36$ KSS family tree.

The polynomial parameterizations for the KSS family with $k = 36$ are:

$$p(x) = (x^{14} - 4x^{13} + 7x^{12} + 683x^8 - 2510x^7 + 4781x^6 + 117649x^2 - 386569x + 823543)/28749;$$
$$r(x) = x^{12} + 683x^6 + 117649; h(x) = (x^2 - 4x + 7)/28749; t(x) = (259 + 757x + 2x^7)/259;$$
$$n(x) = (x^2 - 4x + 7)(x^{12} + 683x^6 + 117649)/28749; f(x) = (4x^7 - 14x^6 + 1255x - 4781)/777. \tag{9.1}$$

There are five common towers found in the family tree. They are defined by the quadratic binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^2}$ and the binomial from $\mathbb{F}_{p^2}$ to $\mathbb{F}_{p^{36}}$ (see Table 13). The polynomials for $p(x)$ and $n(x)$

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^2+u_i)} \mathbb{F}_{p^2} \xrightarrow{\mathbb{F}_{p^2}[v]/(u^{18}-v_i)} \mathbb{F}_{p^{36}}$					
T_i	T_1	T_2	T_3	T_4	T_5
(u_i, v_i)	$(1, u+1)$	$(1, u+2)$	$(1, u+3)$	$(2, u)$	$(5, u)$

TABLE 13. Efficient towering options in the $k = 36$ KSS tree.

in (9.1) insist that $x \equiv \pm 49 \bmod 259$, so we rescale with $x' = x/7$ and begin with $x' \equiv \pm 7 \bmod 37$, which branches off into sub-congruencies forming the family tree in Figure 8 (see Appendix A for the proofs). As it stands, $r(x)$ will always contain $7^6 \cdot 37^2$ as a factor, so we must divide this factor out before (the updated) $r(x)$ can represent primes. Our favorite picks and the associated generators are in Table 14. The frequencies in the final column were calculated from almost 7,000 different KSS curves with $k = 36$ and are roughly as expected. Our 5-star picks constitute approximately 17% of the entire family. The generators in $G_2' = E'(\mathbb{F}_{p^6})$ use $v \in \mathbb{F}_{p^6}$, where $\mathbb{F}_{p^6} = \mathbb{F}_{p^2}[v]/(v^3 - u)$.

rating	equiv. class for $x' = x/7$	tower	b	twist type	G_1 gen. $[h](\cdot,\cdot)$	G_2' gen. $[h'](\cdot,\cdot)$	§B.6	%
	$1376, 1880 \bmod 2664$	T_1	2	D	$(-1, 1)$	$\left(-1, \sqrt{\frac{2-v}{v}}\right)$		4.1
	$821, 1325 \bmod 2664$	T_1	-1	M	$\left(-1, \sqrt{-2}\right)$	$\left(1, \sqrt{1-v}\right)$		4.1
⋆⋆⋆⋆⋆	$437, 2597 \bmod 2664$	T_1	-1	D	$\left(-1, \sqrt{-2}\right)$	-		4.3
	$\{104, ..., 7592\}_4 \bmod 7992$	T_1	-4	M	$(2, 2)$	$\left(1-v, \sqrt{(1-v)^3 - 4v}\right)$	(i)	3.0
	$2768, 4928 \bmod 7992$	T_1	3	M	$(1, 2)$	$\left(1-v, \sqrt{(1-v)^3 + 3v}\right)$		1.1
	$\{3545, ..., 12809\}_8 \bmod 13320$	T_2	-1	M	-	$\left(v, \sqrt{u+2-v}\right)$		2.2
	$\{1265, ..., 12869\}_8 \bmod 13320$	T_2	-1	D	-	$\left(1/v, \sqrt{\frac{1}{u+2} - v}\right)$		3.4
	$8540, 10700 \bmod 13320$	T_2	-2	M	$(3, 5)$	$\left(1, \sqrt{1 - 2/v}\right)$	(ii)	1.0
	$44, 11204 \bmod 13320$	T_2	-2	D	$(3, 5)$	-	(ii)	0.9
⋆⋆⋆⋆	$\{932, ..., 38732\}_5 \bmod 39960$	T_2	3	M	$(1, 2)$	-	(iii)	0.7
	$\{14312, ..., 36452\}_6 \bmod 39960$	T_2	3	D	$(1, 2)$	-	(iii)	1.0
	$12092, 14252 \bmod 39960$	T_2	-4	M	$(2, 2)$	-	??	0.3
	$\{4100, ..., 19580\}_4 \bmod 39960$	T_2	-4	D	$(2, 2)$	-	??	0.6
	$\{992, ..., 29792\}_8 \bmod 39960$	T_2	5	D	-	$\left(-v, \sqrt{\frac{5-v^4}{v}}\right)$		1.1
	$5372 \bmod 13320$	T_3	-2	D	$(3, 5)$	-		0.5
	$10145 \bmod 13320$	T_3	-1	D	-	-		0.5
	$3929, 4373 \bmod 13320$	T_3	-1	M	-	-		0.8
⋆⋆⋆	$\{488, ..., 38288\}_4 \bmod 39960$	T_3	3	M	$(1, 2)$	-	??	0.5
	$30296, 32456 \bmod 39960$	T_3	3	D	$(1, 2)$	-	??	0.3
	$\{3656, ..., 19136\}_4 \bmod 39960$	T_3	-5	D	$(-3, 4\sqrt{-2})$	-	(v)	0.6
	$\{20084, ..., 35564\}_4 \bmod 39960$	T_3	-4	M	$(2, 2)$	-	(vi)	0.6

TABLE 14. Our favorite picks from the $k = 36$ KSS tree.

10. BLS $k = 48$ CURVES

The polynomial parameterizations for the BLS family with $k = 48$ are:

$$p(x) = (x-1)^2(x^{16} - x^8 + 1)/3 + x; \qquad r(x) = x^{16} - x^8 + 1; \qquad t(x) = x + 1;$$
$$n(x) = (x-1)^2(x^{16} - x^8 + 1)/3; \quad f(x) = (x-1)(2x^8 - 1)/3; \quad h(x) = (x-1)^2/3. \tag{10.1}$$

There are five common towers found in the family tree. They are defined by the quadratic binomial from $\mathbb{F}_p$ to $\mathbb{F}_{p^2}$ and the binomial from $\mathbb{F}_{p^2}$ to $\mathbb{F}_{p^{48}}$ (see Table 15). The polynomials for $p(x)$ and $n(x)$ in (10.1) insist that $x \equiv \pm 1 \bmod 3$, which branches off into sub-congruencies forming the family

$\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^2+u_i)} \mathbb{F}_{p^2} \xrightarrow{\mathbb{F}_{p^2}[v]/(u^{24}-v_i)} \mathbb{F}_{p^{48}}$					
T_i	T_1	T_2	T_3	T_4	T_5
(u_i, v_i)	$(1, u+1)$	$(1, u+2)$	$(2, u)$	$(2, u+2)$	$(5, u)$

TABLE 15. Efficient towering options in the $k = 48$ BLS tree.

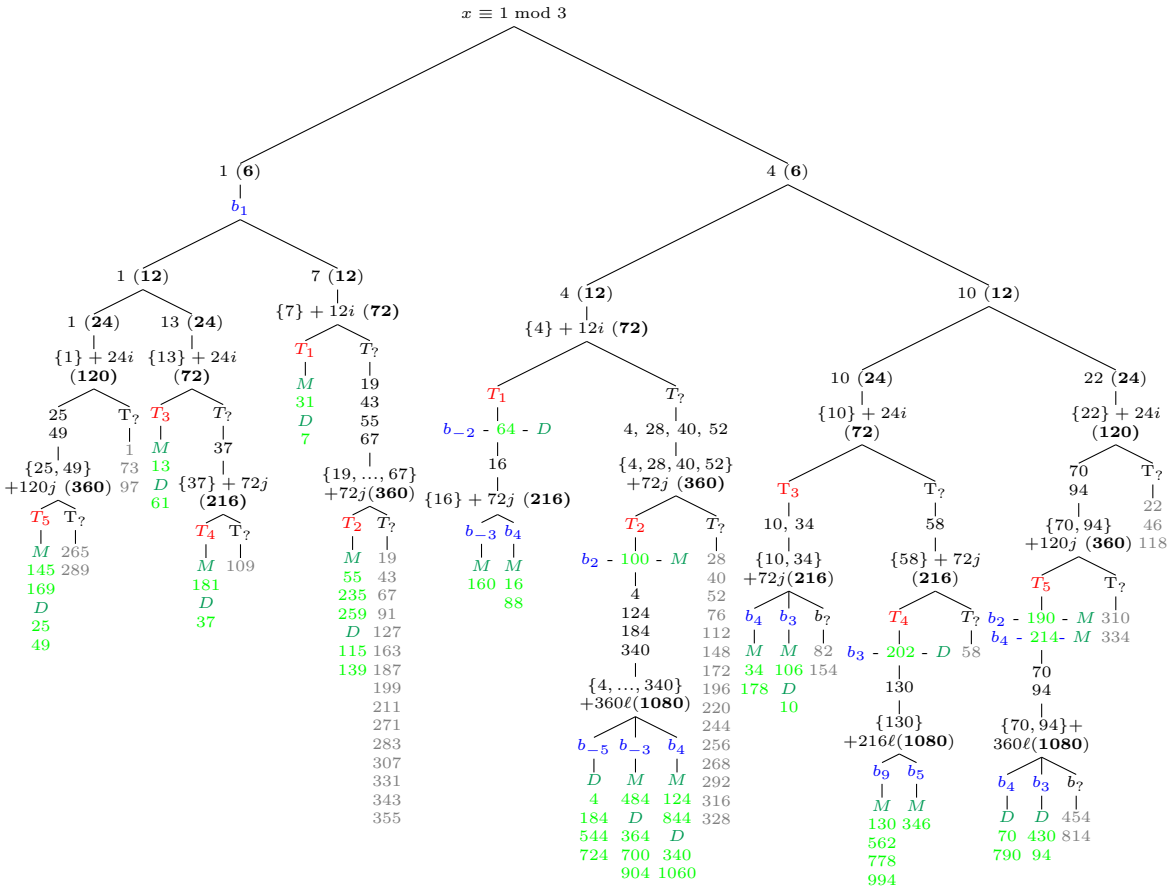

FIGURE 9. The $k = 48$ BLS family tree.

rating	equiv. class for x	tower	b	twist type	G_1 gen. $[h](\cdot,\cdot)$	G_2' gen. $[h'](\cdot,\cdot)$	more §B.7	% %
	$64 \bmod 72$	T_1	-2	D	$(3, 5)$	$\left(1-2/w, \sqrt{(1-2/w)^3-2}\right)$	(i)	4.5
⋆⋆⋆⋆⋆	$31 \bmod 72$	T_1	1	M	-	$\left(w+1, \sqrt{(w+1)^3+1}\right)$	(ii)	4.5
	$7 \bmod 72$	T_1	1	D	-	-		4.4
	$55, 235, 259 \bmod 360$	T_2	1	M	-	-		2.0
	$115, 139 \bmod 360$	T_2	1	D	$\left(1, \sqrt{2}\right)$	-		1.4
	$100 \bmod 360$	T_2	2	M	-	-		0.7
	$\{4, ..., 724\}_4 \bmod 1080$	T_2	-5	D	$\left(-15, 26\sqrt{-5}\right)$	-		1.1
⋆⋆⋆⋆	$364, 700, 904 \bmod 1080$	T_2	-3	D	-	-		0.6
	$484 \bmod 1080$	T_2	-3	M	-	-		
	$124, 844 \bmod 1080$	T_2	4	M	-	$\left(2, \sqrt{8+4w}\right)$	(iii)	0.2
	$340, 1060 \bmod 1080$	T_2	4	D	-	$\left(1, \sqrt{1+4w}\right)$	(iv)	0.4
	$13 \bmod 72$	T_3	1	M	–	$\left(1, \sqrt{w+1}\right)$	(v)	3.9
	$61 \bmod 72$	T_3	1	D	–	-		4.1
⋆⋆⋆	$34, 178 \bmod 216$	T_3	4	M	$\left(-1, \sqrt{3}\right)$	-	(vi)	2.9
	$106 \bmod 216$	T_3	3	M	$(1, 2)$	-		1.4
	$10 \bmod 216$	T_3	3	D	$(1, 2)$	-		1.5

TABLE 16. Our favorite picks from the $k = 48$ BLS tree.

tree in Figure 9 (see Appendix A for the proofs). Our favorite picks and the associated generators

are in Table 16. The frequencies in the final column were calculated from over $5,000$ different BLS curves with $k = 48$ and are as expected. Our 5-star picks constitute approximately 51% of the entire family. The generators in $G_2' = E'(\mathbb{F}_{p^8})$ use $w \in \mathbb{F}_{p^8}$, where $\mathbb{F}_{p^8} = \mathbb{F}_{p^4}[w]/(w^2 - v)$, and $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}[v]/(v^2 - u)$.

11. Recommendations

For all curve families under consideration, as well as BN $k = 12$ and BLS $k = 24$ curves, Table 17 gives the approximate security level at which the DLP and ECDLP complexities are balanced. The ECDLP security is computed as half the bit-length of the group order r, whilst the calculation of the security in $\mathbb{F}_{p^k}$ comes directly from the formula in [30, §6.2.1]. This gives a rough indication of which security level(s) a family is particularly suitable for, and where the family will best compete against other families. For such security levels, we point to where examples of strong curves with low hamming-weights and implementation-friendly parameters can be found.

192-bit secure curves						
family	ρ-value ($\log q/\log r$)	x_0 (bits)	$E[r(x_0)]$ sec. (bits)	$\mathbb{F}_{q(x_0)^k}$ sec. (bits)	security levels accounted for (bits)	example curves found in
BW $k = 8$	1.5	60	121	121	112	Table 18
BN $k = 12$	1	60	122	122	80 - 192	[12, §4]
BLS $k = 12$	1.5	85	170	170	192, 224	Table 19, Table 20
KSS $k = 16$	1.25	49	188	189	192, 224	Table 19, Table 20
KSS $k = 18$	1.33	74	217	217	192, 224	Table 19, Table 20
BLS $k = 24$	1.25	62	252	253	192 - 320	[8, §6]
BLS $k = 27$	1.11	28	251	253	256, 288	Table 21, Table 22
KSS $k = 32$	1.125	41	304	302	288, 320	Table 22, Table 23
KSS $k = 36$	1.167	57	328	330	320, 352	Table 23, Table 24
BLS $k = 48$	1.125	49	392	390	352, 384	Table 24, Table 25

Table 17. Balancing ECDLP and DLP security in families, and where example curves are found.

Our advice on how to proceed agrees almost entirely with that at the end of Scott's note [26, §6], who recommends first finding the optimal degree k binomial $x^k - i \in \mathbb{F}_p[x]$ to define the entire tower, before going searching for curves (that support this tower). The only difference in our recommendation is in the slight performance gain that's achieved when defining the tower using two binomials. Thus, we recommend choosing one or more of the subfamilies that guarantee our favorite tower choices (or yours), and restricting the search parameter x_0 to the corresponding congruences and to be of low hamming-weight before kick-starting a search. If, in addition, there is a preference in the size of a curve constant, the nature of the twist, or the existence of compact generators, then the subfamilies herein give a concrete way to also simultaneously prescribe these desired properties in advance.

Alternatively, the lists of curves in Appendix C should stand implementors in good stead for a while yet, at least until accepted levels of security go beyond the AES equivalent of 384-bits, or perhaps until even better curve families are found.

References

[1] Diego F. Aranha. Software implementation of pairings. Talk at ECC, `http://ecc2011.loria.fr/slides/aranha.pdf`., October 2011.

[2] Diego F. Aranha, Koray Karabina, Patrick Longa, Catherine H. Gebotys, and Julio López. Faster explicit formulas for computing pairings over ordinary curves. In Kenneth G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 48–68. Springer, 2011.

[3] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN*, volume 2576 of *Lecture Notes in Computer Science*, pages 257–267. Springer, 2002.

[4] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer, 2005.

[5] Naomi Benger and Michael Scott. Constructing tower extensions of finite fields for implementation of pairing-based cryptography. In M. Anwar Hasan and Tor Helleseth, editors, *WAIFI*, volume 6087 of *Lecture Notes in Computer Science*, pages 180–195. Springer, 2010.

[6] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.
[7] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptography*, 37(1):133–141, 2005.
[8] Craig Costello, Kristin Lauter, and Michael Naehrig. Attractive subfamilies of BLS curves for implementing high-security pairings. In Daniel J. Bernstein and Sanjit Chatterjee, editors, *INDOCRYPT*, volume 7107 of *Lecture Notes in Computer Science*, pages 320–342. Springer, 2011.
[9] Augusto Jun Devegili, Michael Scott, and Ricardo Dahab. Implementing cryptographic pairings over Barreto-Naehrig curves. In *Pairing*, pages 197–207, 2007.
[10] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2):224–280, 2010.
[11] Steven D. Galbraith and Kenneth G. Paterson, editors. *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, volume 5209 of *Lecture Notes in Computer Science*. Springer, 2008.
[12] C. C. F. Pereira Geovandro, Marcos A. Simplício Jr., Michael Naehrig, and Paulo S. L. M. Barreto. A family of implementation-friendly BN elliptic curves. *Journal of Systems and Software*, 84(8):1319–1326, 2011.
[13] Florian Hess. Pairing lattices. In Galbraith and Paterson [11], pages 18–38.
[14] Florian Hess, Nigel P. Smart, and Frederik Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.
[15] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate texts in mathematics*. Springer-Verlag, 1990.
[16] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. *J. Cryptology*, 17(4):263–276, 2004.
[17] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field. In Galbraith and Paterson [11], pages 126–135.
[18] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. In Nigel P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36. Springer, 2005.
[19] Kristin Lauter, Peter L. Montgomery, and Michael Naehrig. An analysis of affine coordinates for pairing computation. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2010.
[20] Emma Lehmer. Criteria for cubic and quartic residuacity. *Mathematika*, 5(20-29), 1958.
[21] F. Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein*. Springer Verlag, 2000.
[22] Karl Rubin and Alice Silverberg. Choosing the correct elliptic curve in the CM method. *Math. Comput.*, 79(269):545–561, 2010.
[23] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan*, pages 135–148, 2000.
[24] Michael Scott. Scaling security in pairing-based protocols. Cryptology ePrint Archive, Report 2005/139, 2005. http://eprint.iacr.org/.
[25] Michael Scott. An introduction to pairings. Talk at ICE-EM RNSA 2007 Cryptography Workshop, Queensland University of Technology, Australia `http://conf.isi.qut.edu.au/ice-em2007/program/`, June 2007.
[26] Michael Scott. A note on twists for pairing friendly curves.
Personal webpage: ftp://ftp.computing.dcu.ie/pub/resources/crypto/twists.pdf, February 2009.
[27] Michael Scott. On the efficient implementation of pairing-based protocols. In Liqun Chen, editor, *IMA Int. Conf.*, volume 7089 of *Lecture Notes in Computer Science*, pages 296–308. Springer, 2011.
[28] Masaaki Shirase. Barreto-Naehrig curve with fixed coefficient - efficiently constructing pairing-friendly curves -. Cryptology ePrint Archive, Report 2010/134, 2010. http://eprint.iacr.org/.
[29] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate texts in mathematics. Springer-Verlag, 1986.
[30] Nigel Smart. ECRYPT II yearly report on algorithms and keysizes (2009-2010). Technical report, ECRYPT II – European Network of Excellence in Cryptology, EU FP7, ICT-2007-216676, 2010. Published as deliverable D.SPA.13, `http://www.ecrypt.eu.org/documents/D.SPA.13.pdf`.
[31] Frederik Vercauteren. Optimal pairings. *IEEE Transactions on Information Theory*, 56(1):455–461, 2010.

Appendix A. Proofs

For each family, we first give proofs for the towers T_i in the corresponding tree, before giving proofs for the correct curve constants a_i or b_i. The proofs for the curve constants sometimes need results that follow from the towers they are associated with, so rather than prove things twice, we occasionally rely on the reader to match congruencies with their corresponding reciprocity results from the tower proofs.

A.1. **Towers.** Our proofs of the towers mostly make use of the following theorem.

Theorem A.1 (Benger-Scott [5], Thm. 4)**.** *Let $m > 1$, $n > 0$ be integers, p and odd prime and $\alpha \in \mathbb{F}_{p^n}^{\times}$. The binomial $x^m - \alpha$ is irreducible in $\mathbb{F}_{p^n}[x]$ if the following two conditions are satisfied:*

(1) Each prime factor q or m divides $p-1$ and $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) \in \mathbb{F}_p$ is not a q^{th} residue in $\mathbb{F}_p$;
(2) If $m \equiv 0 \bmod 4$, then $p^n \equiv 1 \bmod 4$.

The *Norm* of $\alpha \in \mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is defined as

$$N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) = \prod_{i=0}^{n-1} \alpha^{p^i}$$

We will only be using Theorem A.1 to prove irreducibility in $\mathbb{F}_{p^2}[x]$ or $\mathbb{F}_{p^3}[x]$, i.e. we only need to compute $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ and $N_{\mathbb{F}_{p^3}/\mathbb{F}_p}$, which we abbreviate to $N_{2,1}$ and $N_{3,1}$ respectively. The norm computation usually requires a trivial (possibly repeated) application of Fermat's little theorem, so we omit the details to save space.

Whether towering up to $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^3}$, or towering beyond them to $\mathbb{F}_{p^k}$ then, the proofs all amount to showing quadratic or cubic non-reciprocity in $\mathbb{F}_p$. We write the quadratic and cubic characters of a as usual, i.e. $(\frac{a}{p})_2$ and $(\frac{a}{p})_3$ respectively, and for quadratic reciprocity, we use the following two results.

Proposition A.2 ([15], §5, Prop. 5.1.3)**.** *2 is a quadratic residue modulo p iff $p \equiv 1, 7 \bmod 8$.*

Theorem A.3 ([15], §5, Thm. 2)**.** *Let q be an odd prime.*

(a) If $q \equiv 1 \bmod 4$, then q is a quadratic residue modulo p iff $p \equiv r \bmod q$, where r is a quadratic residue modulo q.
(b) If $q \equiv 3 \bmod 4$, then q is a quadratic residue modulo p iff $p \equiv \pm b^2 \bmod 4q$, where b is an odd integer prime to q.

For cubic reciprocity, we apply Euler's conjectures [21], which were originally based on Fermat's observation that for $p \equiv 1 \bmod 3$, p can be written as $p = a^2 + 3b^2$, where a and b are unique up to sign. For our purposes, a more convenient formulation of Euler's conjectures (which are also special cases of Lehmer's result [20]) can be made in the following theorem, by instead writing $4p$ as $4p = L^2 + 27M^2$, where L and M are unique up to sign ([15, Prop. 8.3.2]).

Theorem A.4 (Euler's conjectures [21], Prop. 7.1 - 7.4)**.** *For $p \equiv 1 \bmod 3$, let L and M be the unique integers (up to sign) such that $4p = L^2 + 27M^2$. Then,*

$$(i): \quad \left(\frac{2}{p}\right)_3 = 1 \leftrightarrow L \equiv M \equiv 0 \bmod 2; \qquad (ii): \quad \left(\frac{3}{p}\right)_3 = 1 \leftrightarrow M \equiv 0 \bmod 3;$$
$$(iii): \quad \left(\frac{5}{p}\right)_3 = 1 \leftrightarrow LM \equiv 0 \bmod 5; \qquad (iv): \quad \left(\frac{7}{p}\right)_3 = 1 \leftrightarrow LM \equiv 0 \bmod 7;$$

The convenience of analyzing the equation $4p = L^2 + 27M^2$ comes from the CM norm equation for curves with discriminant D: $4p = t^2 - Df^2$. Curves of discriminant $D = -3$ are the only curves requiring cubic reciprocity (extensions) in this paper, so we can always write $4p = t^2 + 3f^2$ where $t = t(x)$ and $f = f(x)$ are given in the family parameterizations. Depending on the different cases for $(t, f) \bmod 6$, three different manipulations of the CM norm equation (taken from [8]) can be employed to write $4p = L^2 + 27M^2$, given below.

$$\begin{aligned} &(i) && 4p = t^2 + 27\,(f/3)^2 \\ &(ii) && 4p = \left(\frac{3f+t}{2}\right)^2 + 27\left(\frac{t-f}{6}\right)^2 \\ &(iii) && 4p = \left(\frac{t-3f}{2}\right)^2 + 27\left(\frac{t+f}{6}\right)^2 \end{aligned} \tag{A.1}$$

Throughout the towering proofs we refer to equation (A.1)-(i),(ii), or (iii) depending on how L and M (in $4p = L^2 + 27M^2$) are computed from $t(x)$ and $f(x)$, which we abbreviate to t and f for short.

A.2. **Curve equations.** For $k = 8$, $k = 16$ and $k = 32$ KSS curves, the correct curve has CM discriminant $D = -1$ and is of the form $E/\mathbb{F}_p : y^2 = x^3 + ax$. If g is a fourth-power-free integer, then a is precisely one of $\{1, g, g^2, g^3\}$ ([29, §X.6]). For all the other families, the correct curve has discriminant $D = -3$ and is of the form $E/\mathbb{F}_p : y^2 = x^3 + b$. In this scenario, if g is neither square or cube in $\mathbb{F}_p$, then b is precisely one of $\{1, g, g^2, g^3, g^4, g^5\}$ ([29, §X.5, Corr. 5.4.1]). For both of these special scenarios (CM discriminants), Rubin and Silverberg [22] present simple algorithms (Alg. A.5 and Alg. A.6 below) to determine the correct a or b value, both of which they say are "essentially due to Gauss". Our proofs make constant use of these algorithms.

Algorithm A.5 (Rubin-Silverberg [22], Alg 3.4)**.** *Suppose $D = -1$, i.e. $4p = t^2 + f^2$ and $E/\mathbb{F}_p : y^2 = x^3 - ax$. Set $L = t/2$ and $M = f/2$. A correct curve (value of a) is found by the following algorithm.*

- *Step 1: If L is odd and $L - 1 \equiv M \bmod 4$, then $a = 1$.*
- *Step 2: If L is odd and $L - 1 \not\equiv M \bmod 4$, then $a \in \mathbb{F}_p$ is any square that is not a fourth power (i.e. $a^{(p-1)/4} \equiv -1 \bmod p$).*
- *Step 3: If L is even, replace M by $-M$ if necessary to ensure that $M - 1 \equiv L \bmod 4$, then output any $a \in \mathbb{F}_p$ such that $a^{(p-1)/4} \equiv L/M \bmod p$.*

Notice that the choice of a in Alg. A.5 is such that $y^2 = x^3 - ax$ is the correct curve, whilst we have been using $y^2 = x^3 + ax$ as the correct curve throughout. Thus, a specific proof that $a = \tilde{a}$ will actually use $-\tilde{a}$ when Alg. A.5 is invoked.

Algorithm A.6 (Rubin-Silverberg [22], Alg 3.5)**.** *Suppose $D = -3$, i.e. $4p = t^2 + 3f^2$ and $E/\mathbb{F}_p : y^2 = x^3 + b$. A correct curve (value of b) is found by the following algorithm.*

- *Step 1: If $f \equiv 0 \bmod 3$ and $t \equiv 2 \bmod 3$, then $b = 16$.*
- *Step 2: If $f \equiv 0 \bmod 3$ and $t \equiv 1 \bmod 3$, then $b = 16b'$, where $b' \in \mathbb{F}_p$ is any cube that is not a square (i.e. $b'^{(p-1)/6} \equiv -1 \bmod p$).*
- *Step 3: If $f \not\equiv 0 \bmod 3$. replace f by $-f$ if necessary to ensure that $f \equiv 1 \bmod 3$. If $t \equiv 2 \bmod 3$, output $b = 16b'$ for any b' satisfying $b'^{(p-1)/6} \equiv 2t/(3f - t) \bmod p$.*
- *Step 4: Otherwise, output $b = 16b'$ for any b' satisfying $b'^{(p-1)/6} \equiv 2t/(3f + t) \bmod p$.*

A.3. **Proofs for each family.** We shrink the proofs themselves for space considerations.

$k = 8$ **Brezing-Weng curves.** T_1: $x \equiv 1, 3, 9, 11 \bmod 16$ all imply $p \equiv 5 \bmod 8$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+2)$ by Prop. A.2. Now, $N_{2,1}(u) = 2$ and we already have $(\frac{2}{p})_2 = -1$, so that $x^4 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
T_2: $x \equiv 5, 7, 13, 23 \bmod 24$ all imply $p \equiv 17 \bmod 24$. Using Thm. A.3-(b), with $p \equiv 5 \bmod 12$, and since the odd squares modulo 12 are either 1 or 9, we have that $(\frac{\pm 3}{p})_2 = -1$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+3)$. We also have that $N_{2,1}(u) = 3$, so that $x^4 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
T_3: $x \equiv 21, ..., 117 \bmod 120$ all give $p \equiv 13, 17 \bmod 20$, invoking Thm. A.3-(b), and since the odd squares modulo 20 are either $1, 5$ or 9, we have that $(\frac{\pm 5}{p})_2 = -1$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 5)$. We also have that $N_{2,1}(u) = 5$, so that $x^4 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
a_1: $x \equiv 1, 9 \bmod 16$ gives $(L, M) \equiv (1, 2) \bmod 4$, then Step 2 of Alg. A.5 equipped with $(\frac{-1}{p})_2 = 1$ but $(\frac{-1}{p})_4 = -1$ gives the result. □
a_2: $x \equiv 11 \bmod 16$ gives $(L, M) \equiv (2, 1) \bmod 4$, so replace M by $-M$ and use Alg. A.5-Step 3 to give $-2^{(p-1)/4} \equiv L/M \bmod p$. $x \equiv 13, 29 \bmod 48$ and $x \equiv 141, 189, 237 \bmod 240$ gives $(L, M) \equiv (3, 0) \bmod 4$, so Step 2 of Alg. A.5 this time equipped with $(\frac{-2}{p})_2 = 1$ but $(\frac{-2}{p})_4 = -1$ ([29, Prop. 6.6]) gives the result. □
a_{-2}: $x \equiv 3 \bmod 16$ gives $(L, M) \equiv (2, 1) \bmod 4$, so replace M by $-M$ in Alg. A.5 - Step 3 and observe that $2^{(p-1)/4} \equiv L/M \bmod p$. □
a_3: $x \equiv 7 \bmod 24$ gives $(L, M) \equiv (0, 3) \bmod 4$, so replace M by $-M$ and use Alg. A.5-Step 3 and observe that $-3^{(p-1)/4} \equiv L/M \bmod p$. $x \equiv 21, 69, 117 \bmod 240$ gives $(L, M) \equiv (3, 0) \bmod 4$, so Step 2 of Alg. A.5 this time equipped with $(\frac{-3}{p})_2 = 1$ but $(\frac{-3}{p})_4 = -1$ gives the result. □
a_5: $x \equiv 11 \bmod 120$ and $x \equiv 71, 191 \bmod 240$ give $(L, M) \equiv (0, 3) \bmod 4$, so replace M by $-M$ and use Alg. A.5-Step 3 and observe that $-5^{(p-1)/4} \equiv L/M \bmod p$. $x \equiv 5, 85 \bmod 240$ gives $(L, M) \equiv (3, 0) \bmod 4$, so Step 2 of Alg. A.5 equipped with $(\frac{-5}{p})_2 = 1$ but $(\frac{-5}{p})_4 = -1$ gives the result. □

a_6: $x \equiv 47, 95, 143, 239 \bmod 240$ gives $(L, M) \equiv (0, 3) \bmod 4$, so replace M by $-M$ and use Alg. A.5-Step 3 and observe that $-6^{(p-1)/4} \equiv L/M \bmod p$.

$k = 12$ **BLS curves.** T_1: $x \equiv 7, 31, 64 \bmod 72$ and $160 \bmod 216$ all imply $p \equiv 19 \bmod 24$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 1)$. Note that $2, 3 \mid p - 1$, and $N_{2,1}(u + 1) = 2$, $(\frac{2}{p})_2 = -1$ (Prop. A.2) and $(\frac{2}{p})_3 = -1$ as follows. For $x \equiv 7 \bmod 72$, $t \equiv f \equiv 2 \bmod 6$, so use eq. (A.1)-(ii) and observe that both L and M are both odd. For $x \equiv 31 \bmod 72$, $t \equiv 2 \bmod 6$ and $f \equiv 4 \bmod 6$, so use eq. (A.1)-(iii) to see that L and M are both odd. For $x \equiv 64 \bmod 72$, eq. (A.1)-(i) yields this directly since f is a multiple of 3, say $f = 3M$, giving $4p = L^2 + 27M^2$, where $L = t = x + 1 \equiv 65 \bmod 72$ is odd. For $x \equiv 160 \bmod 216$, observe that $t \equiv f \equiv 5 \bmod 6$ so use eq. (A.1)-(ii) to further deduce that L and M are both odd. Thus $N_{2,1}(u + 1) = 2$, and $(\frac{2}{p})_3 = (\frac{2}{p})_2 = -1$ by Thm. A.4-(i), so that $v^6 - (u + 1)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_2: $x \equiv 55, 127, 343 \bmod 360$ imply $p \equiv 19 \bmod 144$, $x \equiv 43, ..., 307 \bmod 360$ imply $p \equiv 7 \bmod 24$, $x \equiv 28, 100, 172 \bmod 360$ implies $p \equiv 127 \bmod 216$, $x \equiv 124, ..., 1060 \bmod 1800$ implies $p \equiv 127 \bmod 360$, $x \equiv 4, ..., 1012 \bmod 1080$ implies $p \equiv 79 \bmod 108$. In all cases, $p \equiv 7 \bmod 12$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 1)$. $N_{2,1}(u + 2) = 5$, $(\frac{5}{p})_2 = -1$ ($p \equiv 2, 3 \bmod 5$ in all cases, and use Thm. A.3), and $(\frac{5}{p})_3 = -1$ as follows. $x \equiv 28, 100, 172 \bmod 360$ gives $(t, f) \equiv 5, 3 \bmod 6$, and $x \equiv 55, ..., 307 \bmod 360$ gives $(t, f) \equiv (2, 0) \bmod 6$, so applying eq. (A.1)-(i) to both gives one of $(L, M) \equiv (1, 4), (3, 3), (4, 1) \bmod 5$, so that $LM \not\equiv 0 \bmod 5$. $x \equiv 43, 115, 259$ gives $(t, f) \equiv (2, 2) \bmod 6$, so using eq. (A.1)-(ii) further gives $(L, M) \equiv (1, 4), (4, 1) \bmod 5$, so that $LM \not\equiv 0 \bmod 5$. Finally, $x \equiv 139 \bmod 360$ gives $(t, f) \equiv (2, 4) \bmod 6$, so we use eq. (A.1)-(iii) to give $(L, M) \equiv (1, 1) \bmod 5$, implying $LM \not\equiv 0 \bmod 5$. Thus, $(\frac{5}{p})_3 = (\frac{5}{p})_2 = -1$ by Thm. A.4-(iii), so that $v^6 - (u + 2)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_3: $x \equiv 187, 283, 355 \bmod 360$ implies $p \equiv 7 \bmod 336$, $x \equiv 412, 772 \bmod 1800$ implies $p \equiv 343 \bmod 360$, $x \equiv 616, 976, 256 \bmod 1080$ implies $p \equiv 331 \bmod 360$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 1)$. Note that $2, 3 \mid p - 1$, and this time $N_{2,1}(u + 3) = 10$. For $x \equiv 187, 283, 355 \bmod 360$ and $x \equiv 412, 772 \bmod 1800$ we will prove that 2 is a quadratic residue but a cubic non-residue, whilst 5 is a quadratic non-residue but is a cube in $\mathbb{F}_p$. 2 being a quadratic residue follows from Prop. A.2. 5 being a quadratic non-residue follows from $p \equiv 2, 3 \bmod 5$ for these cases. For $x \equiv 187 \bmod 360$ and $x \equiv 283, 355 \bmod 360$, we have $(t, f) \equiv (2, 2) \bmod 6$ and $(t, f) \equiv (2, 4) \bmod 6$ respectively, which use eq. (A.1)-(ii) and eq. (A.1)-(iii) respectively to show that L and M are always odd, meaning that 2 is a cubic non-residue. Furthermore, both cases further reveal that $L \equiv 0 \bmod 5$ so that 5 is always a cubic residue. Combining $(\frac{2}{p})_2 = 1$, $(\frac{5}{p})_2 = -1$, $(\frac{2}{p})_3 = -1$ and $(\frac{5}{p})_3 = 1$ yields the result for $x \equiv 187, 283, 355 \bmod 360$ and $x \equiv 412, 772 \bmod 1800$. We now address $x \equiv 256, 616, 976 \bmod 1080$. This time we prove the opposite of the previous cases: namely that 5 is a quadratic but non-cubic residue, and that 2 is a non-quadratic but cubic residue. $(\frac{2}{p})_2 = -1$ follows from Prop. A.2. $(\frac{5}{p})_2 = 1$ follows from $p \equiv 1 \bmod 5$ and Thm. A.3. For all three congruencies we have $(t, f) \equiv (5, 1) \bmod 6$ which invokes the use of eq. (A.1)-(iii) to show that L and M are always even (so that $(\frac{2}{p})_3 = 1$)), but $(L, M) \equiv (1, 2) \bmod 5$, so that $(\frac{5}{p})_3 = -1$ from $LM \not\equiv 0 \bmod 5$ and Thm. A.4-(iii). This completes the proof. □

T_4: $x \equiv 13, 61 \bmod 72$ implies $p \equiv 13 \bmod 24$, $x \equiv 70, 142, 214 \bmod 216$ implies $p \equiv 37 \bmod 72$, $x \equiv 118, ..., 1054 \bmod 1080$ implies $p \equiv 37 \bmod 72$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 2)$ (Prop. A.2). Since $2, 3 \mid p - 1$ and $N_{2,1}(u) = 2$, $(\frac{2}{p})_2 = -1$ (Prop. A.2), and $(\frac{2}{p})_3 = -1$ as follows. For $x \equiv 13 \bmod 72$, $t \equiv 2 \bmod 6$ and $f \equiv 4 \bmod 6$, so use eq. (A.1)-(iii) to see that L and M are both odd. For $x \equiv 61 \bmod 72$, $t \equiv f \equiv 2 \bmod 6$, so use eq. (A.1)-(ii) to see that L and M are both odd. For $x \equiv 70, 142, 214 \bmod 216$, $t \equiv f \equiv 5 \bmod 6$, so use eq. (A.1)-(ii) to further observe that L and M are again both odd. For all $x \equiv 118, ..., 1054 \bmod 1080$, $f = 3M$ so use eq. (A.1)-(i) and observe that M is always odd. Thus $N_{2,1}(u) = 2$ and $(\frac{2}{p})_3 = (\frac{2}{p})_2 = -1$ by Thm. A.4-(i), so that $v^6 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_5: $x \equiv 37, 181 \bmod 216$ implies $p \equiv 37 \bmod 144$, $x \equiv 94, ..., 670 \bmod 1080$ implies $p \equiv 133 \bmod 216$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 2)$ (Prop. A.2). Since $2, 3 \mid p - 1$ and $N_{2,1}(u) = 6$, which is not a quadratic or cubic residue as follows. To show $(\frac{6}{p})_2 = -1$, we see immediately that $(\frac{-2}{p})_2 = -1$ from Prop. A.2. To see that $(\frac{3}{p})_2 = 1$, we use Thm. A.3-(b) with $p \equiv 1 \bmod 12$. For the cubic non-residuosity, we have to split the cases. Observe that for $x \equiv 37, 181 \bmod 216$ we have $(t, f) \equiv (2, 0) \bmod 6$ so that eq. (A.1)-(i) can be used to see that $(L, M) \equiv (2, \pm 2) \bmod 3$, so that 3 is a cubic non-residue. On the other hand, $(L, M) \equiv (0, 0) \bmod 2$ for this case so that 2 is a cubic residue, which concludes the first case(s). For $x \equiv 94, ..., 670 \bmod 1080$, we always have $(t, f) \equiv (5, 1) \bmod 6$, so using eq. (A.1)-(iii) gives $(L, M) \equiv (4, \pm 2) \bmod 6$, so that 3 is again a cubic non-residue but a quadratic residue. Thus, $(\frac{6}{p})_3 = (\frac{6}{p})_2 = -1$ by Thm. A.4-(i),(ii), so that $v^6 - (u + 2)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_6: $x \equiv 25, ..., 337 \bmod 360$ implies $p \equiv 1 \bmod 24$, $x \equiv 10, 82, 288 \bmod 360$ implies $p \equiv 73 \bmod 144$. In all cases, $p \equiv 2, 3 \bmod 5$ so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+5)$. Now, $N_{2,1}(u) = 5$ so it remains to show $(\frac{5}{p})_3 = -1$. $x \equiv 73, 145, 217 \bmod 360$ gives $(t, f) \equiv (2, 0) \bmod 6$ so that eq. (A.1)-(i) gives $(L, M) \equiv (1, 4), (3, 3), (4, 1) \bmod 5$. For $x \equiv 25, 169, 313 \bmod 360$ we get $(t, f) \equiv (2, 2) \bmod 6$, so applying eq. (A.1)-(ii) gives $(L, M) \equiv (1, 4), (4, 1) \bmod 5$. $x \equiv 49, 337 \bmod 360$ gives $(t, f) \equiv (2, 4) \bmod 6$, so applying eq. (A.1)-(iii) gives $(L, M) \equiv (3, 2), (1, 1) \bmod 5$. Lastly, $x \equiv 10, 82, 288 \bmod 360$ all give $(t, f) \equiv (5, 3) \bmod 6$, so we can apply eq. (A.1)-(i) to see $(L, M) \equiv (3, 3), (1, 4) \bmod 5$. In all cases then, $LM \not\equiv 0 \bmod 5$, so that $(\frac{5}{p})_3 = (\frac{5}{p})_2 = -1$ by Thm. A.4-(iii), so $v^6 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

b_1: $n \equiv 0 \bmod 12$. b must be square and cube, and one of $\{1, g, g^2, g^3, g^4, g^5\}$ for g non-square and non-cube, so $b = 1$ is the only option. □

b_2: $n \equiv 27 \bmod 108$, $p \equiv 1 \bmod 16$. $(t, f) \equiv (2, 0) \bmod 3$, so apply Algorithm A.6-Step 1 and take $b = 16$. $(\frac{2}{p})_2 = 1$ by Prop A.2. so $8 = \mu^6$ for $\mu^2 = 2$, thus the curve with $b = 16/\mu^6 = 2$ is isomorphic. □

b_{-2}: $n \equiv 27 \bmod 432$, $p \equiv 19 \bmod 72$. $(t, f) \equiv (2, 0) \bmod 3$, so apply Algorithm A.6 - Step 1 and take $b = 16$. This time $(\frac{-2}{p})_2 = 1$ by Prop A.2, so $-8 = \mu^6$ for $\mu^2 = -2$, thus the curve with $b = 16/\mu^6 = -2$ is isomorphic. □

b_4: $n \equiv 3 \bmod 36$, $p \equiv 1 \bmod 12$. Proof is identical to case $x_0 \equiv 16 \bmod 72$ for $k = 24$ BLS curves in [8, Prop. 3]. □

b_3: $n \equiv 15 \bmod 24$, $p \equiv 1 \bmod 12$. There are three cases that arise: $(t, f) \equiv (2, 0), (2, 1), (2, 2) \bmod 3$. For $(t, f) \equiv (2, 0) \bmod 3$, we terminate with $b = 16$ from A.6, so $b = 3$ follows from observing $16/3$ (equivalently $2^4 3^5$) is μ^6 for some μ, which follows from the cubic and quadratic reciprocities of 2 and 3. For the other two cases $(t, f) \equiv (2, 1) \bmod 3$ and $(t, f) \equiv (2, 2) \bmod 3$, we use Alg. A.5 and take $b'^{(q-1)/6} = 12^{(q-1)/6} \equiv 2t/(3f - t) \bmod p$ and $b'^{(q-1)/6} = 12^{(q-1)/6} \equiv 2t/(-3f - t) \bmod p$ respectively, so we can take $b = 16b'/2^6 = 3$ in both cases. □

b_{-3}: $n \equiv 147 \bmod 216$, $p \equiv 7 \bmod 12$. This time the two latter cases of the previous proof arise: $(t, f) \equiv (2, 1) \bmod 3$ and $(t, f) \equiv (2, 2) \bmod 3$, so again we use Alg. A.5, but this time it we take $b' = -12$ to see $b'^{(q-1)/6} = -12^{(q-1)/6} \equiv 2t/(3f - t) \bmod p$ and $b'^{(q-1)/6} = -12^{(q-1)/6} \equiv 2t/(-3f - t) \bmod p$ respectively, so we can take $b = 16b'/2^6 = -3$ in both cases. □

b_{-5}: $n \equiv 3 \bmod 360$, $p \equiv 727 \bmod 1620$. We always have $(t, f) \equiv (2, 1) \bmod 3$, so Alg. A.5 with $b' = -20$ gives $b'^{(q-1)/6} = -20^{(q-1)/6} \equiv 2t/(3f - t) \bmod p$, so we can take $b = 16b'/2^6 = -5$. □

b_5: $n \equiv 75 \bmod 900$, $p \equiv 214 \bmod 810$. Again we always have $(t, f) \equiv (2, 1) \bmod 3$, so Alg. A.5 this time with $b' = 20$ gives $b'^{(q-1)/6} = 20^{(q-1)/6} \equiv 2t/(3f - t) \bmod p$, so we can take $b = 16b'/2^6 = 5$. □

b_9: $n \equiv 3 \bmod 12$, $p \equiv 1 \bmod 6$. Two cases: $(t, f) \equiv (2, 0) \bmod 3$ means $b = 16$ is the curve from Alg. A.5. It is easily seen that $(\frac{36}{p})_3 = 1$, so $(\frac{36}{p})_6 = 1$, meaning we can multiply b by $36/2^6$ to get the isomorphic curve with $b = 9$. For the second case we have $(t, f) \equiv (2, 1) \bmod 3$, so Alg. A.5 - Step 3 with $b' = 36$ gives $b'^{(q-1)/6} = 36^{(q-1)/6} \equiv 2t/(3f - t) \bmod p$, so we can take $b = 16b'/64 = 9$. □

b_{10}: $n \equiv 183 \bmod 240$, $p \equiv 37 \bmod 120$. Two cases: $(t, f) \equiv (2, 0) \bmod 3$ means $b = 16$ is the curve from Alg. A.5. It is easily seen that $(\frac{40}{p})_6 = 1$, meaning we can multiply b by $40/2^6$ to get the isomorphic curve with $b = 10$. For the second case we have $(t, f) \equiv (2, 1) \bmod 3$, so Alg. A.5 - Step 3 with $b' = 40$ gives $b'^{(q-1)/6} = 40^{(q-1)/6} \equiv 2t/(3f - t) \bmod p$, so we can take $b = 16b'/64 = 10$. □

$k = 16$ **KSS curves.** T_1: $x' \equiv 5, 37, 61, 93 \bmod 112$, $x' \equiv 47, 79 \bmod 112$, $x' \equiv 23, 103 \bmod 112$ all imply $p \equiv 5 \bmod 8$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+2)$ by Prop. A.2. Now, $N_{2,1}(u) = 2$ and we already have $(\frac{2}{p})_2 = -1$, so that $x^8 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_2: $x' \equiv 19, ..., 1531 \bmod 1680$, $x' \equiv 1153, 1633 \bmod 1680$ all imply $p \equiv 17 \bmod 24$. Using Thm. A.3-(b), with $p \equiv 5 \bmod 12$, and since the odd squares modulo 12 are either 1 or 9, we have that $(\frac{\pm 3}{p})_2 = -1$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+3)$. We also have that $N_{2,1}(u) = 3$, so that $x^8 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_3: This proof requires a special splitting of the elements in bunches. Namely, $x' \equiv 9, 89 \bmod 560$ implies $p \equiv 57 \bmod 80$; $x' \equiv 121, 201$ implies $p \equiv 73 \bmod 180$; $x' \equiv 401, 1601$ implies $p \equiv 193 \bmod 240$; $x' \equiv 929, 1409$ implies $p \equiv 97 \bmod 240$. We can now use Thm. A.3-(b), with $p \equiv 13, 17 \bmod 20$, and since the odd squares modulo 20 are either $1, 5$ or 9, we have that $(\frac{\pm 5}{p})_2 = -1$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+5)$. We also have that $N_{2,1}(u) = 5$, so that $x^8 - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

a_1 : $n \equiv 2500 \bmod 10000$, $p \equiv 5 \bmod 8$. $(L, M) \equiv (1, 2) \bmod 4$, so we use Step 2 of Alg. A.5 and -1 is easily seen to be a square that is not a quartic residue. □

a_2 : $n \equiv 0 \bmod 1250$, $p \equiv 1 \bmod 4$. Two cases arise: $(L, M) \equiv (3, 0) \bmod 4$, so use Step 2 of A.5 where $(\frac{-2}{p})_2 = 1$ but $(\frac{-2}{p})_4 = -1$ gives the result. For $(L, M) \equiv (2, 3) \bmod 4$, we use Step 3 of Alg. A.5 and the fact that $-2^{(p-1)/4} \equiv L/M \bmod p$ to give the result. □

a_{-2} : $n \equiv 1250 \bmod 40000$, $p \equiv 13 \bmod 16$. $(L, M) \equiv (2, 3) \bmod 4$, and this time we have $2^{(p-1)/4} \equiv L/M \bmod p$. □

a_3 : $n \equiv 0 \bmod 1250$, $p \equiv 1 \bmod 8$. Two cases: $(L, M) \equiv (3, 0) \bmod 4$, so Step 2 of A.5 and $(\frac{-3}{p})_2 = 1$ but $(\frac{-3}{p})_4 = -1$ gives the result. For the second case, $(L, M) \equiv (0, 1) \bmod 4$, so Step 3 of Alg. A.5 and $-3^{(p-1)/4} \equiv L/M$ gives the result. □

a_5 : $n \equiv 0 \bmod 1250$, $p \equiv 1 \bmod 8$. Two cases: $(L, M) \equiv (3, 0) \bmod 4$ so Step 2 of Alg. A.5 with $(\frac{-5}{p})_2 = 1$ and $(\frac{-5}{p})_4 = -1$ gives the result. For $(L, M) \equiv (0, 1) \bmod 4$, Step 3 of Alg. A.5 with $-5^{(p-1)/4} \equiv L/M \bmod p$ finishes the proof. □

$k = 18$ **KSS curves.** T_1: $x' \equiv 4, 7, 16, 31 \bmod 36$ implies $p \equiv 1 \bmod 6$. We need to prove $(\frac{2}{p})_3 = -1$. $x' \equiv 4, 31 \bmod 36$ gives $t \equiv 1 \bmod 6$ and $f \equiv 3 \bmod 6$, so $f \equiv 3M$ and further $M \equiv 1 \bmod 2$, so we can use eq. (A.1)-(i) to give $4p = L^2 + 27M^2$, where L and M are both odd. $x' \equiv 7, 16 \bmod 36$ gives $t \equiv f \equiv 1 \bmod 6$, so we can use eq. (A.1)-(ii) to further show that L and M are both odd. Thus, $(\frac{\pm 2}{p})_3 = -1$ by Thm. A.4-(i), so that $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3 + 2)$. Note that $x' \equiv 4, 16 \bmod 36$ gives $p \equiv 5 \bmod 8$, and $x' \equiv 7, 31 \bmod 36$ gives $p \equiv 7 \bmod 8$, so $(\frac{-2}{p})_2 = -1$ by Prop. A.2. Now, $N_{3,1}(u) = -2$ and $(\frac{2}{p})_2 = -1$, so that $x^6 - u$ is irreducible in $\mathbb{F}_{p^3}[x]$ by Thm. A.1. □

T_2: $x' \equiv 13, 25 \bmod 36$ implies $p \equiv 7 \bmod 24$. We need to prove that $(\frac{2}{p})_3 = -1$. With $x' \equiv 13 \bmod 36$, $f \equiv 0 \bmod 3$, i.e. $f = 3M$, insists use of eq. (A.1)-(i), which further reveals $4p = L^2 + 27M^2$ has L and M as odd. With $x' \equiv 25 \bmod 36$, $f \equiv t \equiv 1 \bmod 6$ insists use of eq. (A.1)-(ii) to give $(3f + t)/2$ and $(t - f)/6$ both odd. Thus, $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3 + 2)$. This time, we have $N_{3,1}(2u) = -16$ and $(\frac{-16}{p})_2 = -1$ (since $(\frac{-1}{p})_2 = -1$ and $-16 = -1 \cdot 4^2$), and further $(\frac{-16}{p})_3 = -1$ (since $(\frac{-2}{p})_3 = -1$ by Thm. A.4-(i) and $-16 = -2 \cdot 2^3$), so $x^6 - u$ is irreducible in $\mathbb{F}_{p^3}[x]$ by Thm. A.1. □

T_3: $x' \equiv 1, 28, 37, 64 \bmod 108$ implies $p \equiv 7 \bmod 18$, and also that $f \equiv 2, 8 \bmod 9$, so that $(\frac{3}{p})_3 = -1$ by Thm. A.4-(ii), and $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3 + 3)$. Now, $N_{3,1}(u) = -24$, which is not a cubic residue (since -3 isn't). To apply Thm. A.1, it remains to show that $(\frac{-24}{p})_2 = -1$. $x' \equiv 1, 28, 37, 64 \bmod 108$ also implies $p \equiv 3, 5 \bmod 8$, so that $(\frac{2}{p})_2 = -1$. Since $-24 = 2 \cdot -3 \cdot 2^2$, and $(\frac{2}{p})_2 = -1$, we have that $(\frac{-24}{p})_2 \cdot (\frac{-3}{p})_2 = -1$, so it suffices to show that $(\frac{-3}{p})_2 = 1$. We have to split the possible congruences: for $x' \equiv 1, 37$ we always have $p \equiv 7 \bmod 12$, and taking $q = 3$ in Thm. A.3 does the trick, since 1 and 9 are the only "odd squares" modulo 12. Thus, for $x' \equiv 1, 37$, $(\frac{3}{p})_2 = -1$ and $(\frac{-1}{p})_2 = -1$ gives $(\frac{-3}{p})_2 = 1$. For $x' \equiv 28, 64$, we have $p \equiv 1 \bmod 12$, which does just the opposite, meaning $(\frac{3}{p})_2 = 1$, but $(\frac{-1}{p})_2 = 1$ also, meaning $(\frac{-3}{p})_2 = 1$ as well. □

T_4: $x' \equiv 22, 58, 142, 178 \bmod 180$ implies $p \equiv 1 \bmod 12$. To prove $(\frac{-2}{p})_3 = -1$, we need to split into two separate cases and use Thm. A.4-(i). For $x' \equiv 22, 58 \bmod 180$, we have $f \equiv 0 \bmod 3$, i.e. $f = 3M$, insists use of eq. (A.1)-(i), which further reveals $4p = L^2 + 27M^2$ has L and M always odd. For $x' \equiv 142, 178 \bmod 180$ we have $t \equiv f \equiv 1 \bmod 6$ and application of eq. (A.1)-(ii) shows that L and M are both odd. Thus, $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3 + 2)$. $N_{3,1}(5u) = -250$, and $(\frac{-250}{p})_3 = -1$ follows from $(\frac{2}{p})_3 = -1$ (since $-250 = -2 \cdot 5^3$), so it remains to prove $(\frac{-250}{p})_2 = -1$ before applying Thm. A.1. Since $p \equiv 1 \bmod 4$, $(\frac{-1}{p})_2 = 1$ so that $(\frac{-250}{p})_2 = (\frac{10}{p})_2$. Further, $x' \equiv 22, 58, 142, 178 \bmod 180$ implies $p \equiv 1 \bmod 8$ so Prop. A.2 says that $(\frac{2}{p})_2 = 1$, meaning that $(\frac{10}{p})_2 = (\frac{2}{p})_2 \cdot (\frac{5}{p})_2 = (\frac{5}{p})_2$. For this, combine the fact that $x' \equiv 22, 58, 142, 178 \bmod 180$ implies $p \equiv 2, 3 \bmod 5$ with Thm. A.3-(a) to give that $(\frac{5}{p})_2 = -1$. Thus, $(\frac{-250}{p})_2 = -1$ so that $x^6 - 2u$ is irreducible in $\mathbb{F}_{p^3}[x]$ by Thm. A.1. □

T_5: $x' \equiv 19, 181, 208, 262 \bmod 270$ implies $p \equiv 7 \bmod 54$. We now show that $(\frac{-5}{p})_3 = (\frac{5}{p}) - 1$ using Thm. A.4 - (iii). First, for $x' \equiv 19, 181, 208, 262 \bmod 270$, we always have $t \equiv 1 \bmod 6$ and $f \equiv 5 \bmod 6$, so we make use eq. (A.1)-(iii) and see that niether L nor M is divisible by 5. Thus, $(\frac{5}{p})_3 = -1$ and $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3 + 5)$. $N_{3,1}(u) = -5$, so to finish the proof we need to show that $(\frac{-5}{p})_2 = -1$. We split the congruencies into two cases: $x' \equiv 19, 181 \bmod 270$ gives $p \equiv 3 \bmod 4$ and $p \equiv \pm 1 \bmod 5$ which means firstly that $(\frac{-5}{p})_2 = -(\frac{5}{p})_2$, and also that $(\frac{5}{p})_2 = 1$ from Thm. A.3-(a). For the other two congruencies $x' \equiv 208, 262 \bmod 270$, $p \equiv 1 \bmod 4$ and $p \equiv \pm 2 \bmod 5$ which means firstly that this time $(\frac{-5}{p})_2 = (\frac{5}{p})_2$, but secondly that $(\frac{5}{p})_2 = -1$ from Thm. A.3-(a). In both cases then, $(\frac{-5}{p}) = -1$ and $(\frac{-5}{p})_2 =) \frac{-5}{p})_3 = -1$, so that $x^6 - u$ is irreducible in $\mathbb{F}_{p^3}[x]$ by Thm. A.1. □

b_3: $n \equiv 16807 \bmod 37044$, $p \equiv 7 \bmod 36$. Two cases arise: $(t, f) \equiv (1, 1) \bmod 3$, so Step 4 of Alg. A.6 with $b' = 12$ gives $12^{(p-1)/6} \equiv 2t/(3f + t) \bmod p$, and dividing $b = 16b'$ by 2^6 gives the result. For the other case, $(t, f) \equiv (1, 2) \bmod 3$, so Step 3 of Alg. A.6 with $b' = 12$ (and the division by 2^6) gives the same result. □

b_{-9}: $n \equiv 4459 \bmod 37044$. We always have the case $(t, f) \equiv (1, 2) \bmod 3$, so Step 4 of Alg. A.6 with $b' = -36$ gives $-36^{(p-1)/6} \equiv 2t/(-3f + t) \bmod p$. Division of $b = 16b'$ by 2^6 gives the result. □
b_5: $n \equiv 343 \bmod 2058$, $p \equiv 1 \bmod 6$. Two cases arise: $(t, f) \equiv (1, 0) \bmod 3$, so Step 2 of Alg. A.6 with $b' = 20$ gives $20^{(p-1)/6} \equiv -1 \bmod p$ gives the result. For the second case, $(t, f) \equiv (1, 2) \bmod 3$ so Step 4 of Alg. A.6 with $b' = 20$ gives the same constant. □
b_7: $n \equiv 343 \bmod 2058$, $p \equiv 1 \bmod 6$. Three cases arise: $(t, f) \equiv (1, 0) \bmod 3$ means Step 2 of Alg. A.6 applies, here with $b' = 36$ gives $36^{(p-1)/6} \equiv -1 \bmod p$. The second two cases are $(t, f) \equiv (1, 1) \bmod 3$ and $(t, f) \equiv (1, 2) \bmod 3$, which both use Step 4. of Alg. A.6 and $b' = 36$ to give $36^{(p-1)/6} \equiv 2t/(3f + t), 2t/(-3f + t) \bmod p$ respectively. All three cases give $b = 16b'$ which can be divided by 2^6 to give $b = 7$. □
b_{-7}: $n \equiv 53851 \bmod 86436$, $p \equiv 115 \bmod 252$. One case: $(t, f) \equiv (1, 2) \bmod 3$ so Step 4. of Alg A.6 with $b' = -28$ gives $-28^{(p-1)/6} \equiv 2t/(-3t + f) \bmod p$. Division of $b = 16b'$ by 2^6 gives the result. □
b_6: $n \equiv 22981 \bmod 24696$, $p \equiv 61 \bmod 72$. Two cases arise, both requiring Step 4 of Alg. A.6. Namely $(t, f) \equiv (1, 2) \bmod 3$ and $(t, f) \equiv (1, 1) \bmod 3$ take $b' = 24$ to give $24^{(p-1)/6} \bmod p$ as $2t/(-3f + t)$ and $2t/(3f + t)$ respectively. Division of $b = 16b'$ by 2^6 gives the result. □
b_2: $n \equiv 12691 \bmod 18522$, $p \equiv 31 \bmod 54$. $(t, f) \equiv (1, 0) \bmod 3$ is the only case, so taking $b' = 8$ gives $8^{(p-1)/6} \equiv -1 \bmod p$ in Step 2 of Alg. A.6, and dividing $b = 16b'$ by 2^6 gives the result. □
b_{-4}: $n \equiv 4459 \bmod 12348$, $p \equiv 7 \bmod 36$. The only case is $(t, f) \equiv (1, 1) \bmod 3$ which requires Step 4 of Alg. A.6 with $b' = -16$ to give $-16^{(p-1)/6} \equiv 2t/(3f + t)$ to give the result (again, after division of b by 2^6). □
b_{-2}: $n \equiv 49735 \bmod 74088$, $p \equiv 31 \bmod 216$. The only case is $(t, f) \equiv (1, 0) \bmod 3$, for which we can use Step 2 of Alg. A.6 to deduce that $b' = -8$ always gives $-8^{(p-1)/6} \equiv -1 \bmod p$. Division of b by 2^6 gives $b = -2$. □
b_{10}: $n \equiv 10633 \bmod 41160$, $p \equiv 97 \bmod 120$. Two cases arise: $(t, f) \equiv (1, 0) \bmod 3$ requires Step 2 of Alg. A.6 with $b' = 40$ to always give $40^{(p-1)/6} \equiv -1 \bmod p$. The second case is $(t, f) \equiv (1, 1) \bmod 3$, which uses $b' = 40$ in Step 4 of Alg. A.6 to give $40^{(p-1)/6} \equiv 2t/(3f + t) \bmod p$. In both cases we again divide b by 2^6 to give the smaller constant. □

$k = 27$ **BLS curves.** T_1: $x \equiv 2 \bmod 9$ implies $p \equiv 7 \bmod 9$. Once case: $t \equiv 5 \bmod 6$ and $f \equiv 1 \bmod 6$, so applying eq. (A.1)-(iii) gives further that $M \not\equiv 0 \bmod 3$ so Thm. A.4-(ii) gives $(\frac{3}{p})_3 = -1$. Thus, $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3 + 3)$, and furthermore since $N_{3,1}(u) = -3$, we immediately have that $x^9 - u$ is irreducible in $\mathbb{F}_{p^3}[x]$ by Thm. A.1. □
T_2: $x \equiv 8 \bmod 45$ implies $p \equiv 37 \bmod 45$. Again, $x \equiv 8 \bmod 45$ gives $t \equiv 5 \bmod 6$ and $f \equiv 1 \bmod 6$, insisting the use of eq. (A.1)-(iii) which gives both $L, M \not\equiv 0 \bmod 5$, so $(\frac{5}{p})_3 = -1$ by Thm. A.4-(iii). Thus, $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3+5)$, and since $N_{3,1}(u) = -5$, we immediately have that x^9-u is irreducible in $\mathbb{F}_{p^3}[x]$ by Thm. A.1. □
T_3: $x \equiv 17, ..., 269 \bmod 315$ implies $p \equiv 1 \bmod 45$. Again, $x \equiv 17, ..., 269 \bmod 45$ gives $t \equiv 5 \bmod 6$ and $f \equiv 1 \bmod 6$, so applying eq. (A.1)-(iii) to see that $L, M \not\equiv 0 \bmod 7$ and Thm. A.4-(iv) gives $(\frac{7}{p})_3 = -1$. Thus, $\mathbb{F}_{p^3} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^3 + 7)$, and since $N_{3,1}(u) = -7$, $x^9 - u$ is irreducible in $\mathbb{F}_{p^3}[x]$ by Thm. A.1. □
b_{-5}: $n \equiv 1083 \bmod 1350$. We always have $(t, f) \equiv (2, 1) \bmod 3$, so Step 3 of Alg. A.6 with $b' = -20$ gives $-20^{(p-1)/6} \equiv 2t/(3f - t) \bmod p$. Division by 2^6 gives a smaller constant as usual. □
Other b's: All other proofs are identical, i.e. have $(t, f) \equiv (1, 2) \bmod 3$ and use Step 3 of Alg. A.6 with the appropriate b'. □

$k = 32$ **KSS curves.** T_1: $x' \equiv 453, ..., 2893 \bmod 3824$, $x' \equiv 1887, 2415 \bmod 3824$ and $x' \equiv 503, 3799 \bmod 3824$ all imply $p \equiv 5 \bmod 8$, so that $(\frac{2}{p})_2 = (\frac{-2}{p})_2 - 1$ by Prop. A.2. Thus, $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 2)$, and since $N_{2,1}(u) = 2$, $x^{16} - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
T_2: $x' \equiv 7145, 7673 \bmod 11472$ implies $p \equiv 17 \bmod 48$, $x' \equiv 2843, 3371, 8579, 9148 \bmod 11472$ implies $p \equiv 17 \bmod 24$. So we always have $p \equiv 5 \bmod 12$. The "odd squares" modulo 12 are 1 and 9 only, so that Thm. A.3-(ii) allows us to immediately conclude that $(\frac{3}{p})_2 = (\frac{-3}{p})_2 = -1$ in all cases. Thus, $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 3)$, and since $N_{2,1}(u) = 3$, $x^{16} - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
a_1: $n \equiv 81573072100 \bmod 117465223824$, $p \equiv 5 \bmod 8$. $(L, M) \equiv (1, 2) \bmod 4$, so using Step 2 of Alg. A.5 with $(\frac{-1}{p})_2 = 1$ and $(\frac{-1}{p})_4 = -1$ gives the result. □
a_{-2}: $n \equiv 8157307210 \bmod 939721790592$, $p \equiv 5 \bmod 16$. $(L, M) \equiv (2, 1) \bmod 4$, so using Step 3 of Alg. A.5 with $2^{(p-1)/4} \equiv L/M \bmod p$ gives the result. □

a_2: $n \equiv 8157307210 \bmod 14683152978$, $p \equiv 1 \bmod 4$. Two cases: $(L, M) \equiv (2, 1) \bmod 4$, so using Step 3 of Alg. A.5 with $-2^{(p-1)/4} \equiv L/M \bmod p$ gives the first result. For the second result $(L, M) \equiv (3, 0) \bmod 4$ so Step 2 of Alg. A.5 with $-2^{(p-1)/4} \equiv -1 \bmod p$ completes the proof. □
a_3: $n \equiv 301820366770 \bmod 469860895296$, $p \equiv 17 \bmod 72$. $(L, M) \equiv (0, 3) \bmod 4$ is the only scenario, so Step 2 of Alg. A.5 with $-3^{(p-1)/4} \equiv -1 \bmod p$ gives the result. □

$k = 36$ **KSS curves.** T_1: $x' \equiv 1880, ..., 2264 \bmod 2664$ implies $p \equiv 19 \bmod 24$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 1)$. Now, $N_{2,1}(u + 1) = 2$, and $(\frac{2}{p})_2 = -1$ from Prop. A.2. To prove $(\frac{2}{p})_3 = -1$, we need to split the congruencies into 4 sets. Firstly, $x' \equiv 1376, 1880 \bmod 2664$ gives $t \equiv 1 \bmod 6$ and $f \equiv 3 \bmod 6$, so eq. (A.1)-(i) with $f = 3M$ gives L and M both odd. For $x' \equiv 821, 1325 \bmod 2664$ gives $t \equiv 4 \bmod 6$ and $f \equiv 2 \bmod 6$, so eq. (A.1)-(iii) reveals that L and M are both odd. For $x' \equiv 437, 2597 \bmod 2664$, we have $t \equiv f \equiv 4 \bmod 6$, and using eq. (A.1)-(ii) reveals that L and M are both odd. Lastly, $x' \equiv 104, 2264 \bmod 2664$ gives $t \equiv f \equiv 1 \bmod 6$, so again using eq. (A.1)-(ii) gives L and M as both odd. Thus, $(\frac{2}{p})_3 = -1$ by Thm. A.4-(i) so that $x^{18} - (u + 1)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
T_2: $x' \equiv 3152, ..., 7652 \bmod 13320$ implies $p \equiv 31 \bmod 36$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 1)$. $N_{2,1}(u + 2) = 5$, and $(\frac{5}{p})_2 = -1$ since $x' \equiv 3152, ..., 7652 \bmod 13320$ always gives $p \equiv 2, 3 \bmod 5$, allowing us to apply Thm. A.3-(i). To prove $(\frac{5}{p})_3 = -1$, we must split the congruences into 6 different sets: $x' \equiv 932, 6260, 4100, 12092 \bmod 13320$ gives $t \equiv f \equiv 1 \bmod 6$, so using eq. (A.1)-(ii) gives $(L, M) \equiv (1, 4), (2, 2) \bmod 5$. $x' \equiv 3152, ..., 7652 \bmod 13320$ gives $t \equiv 1 \bmod 6$ and $f \equiv 5 \bmod 6$ so using eq. (A.1)-(iii) gives $(L, M) \equiv (3, 3), (1, 4) \bmod 5$. $x' \equiv 44, ..., 11204 \bmod 13320$ gives $t \equiv 1 \bmod 6$ and $f \equiv 3 \bmod 6$ so using eq. (A.1)-(i) gives $(L, M) \equiv (1, 1), (1, 4) \bmod 5$. $x' \equiv 1709, ...12869 \bmod 13320$ gives $t \equiv 4 \bmod 6$ and $f \equiv 0 \bmod 6$, so using eq. (A.1)-(i) with $f \equiv 3M$ gives $(L, M) \equiv (1, 1), (1, 4) \bmod 5$. $x' \equiv 1265, ..., 12425 \bmod 13320$ gives $t \equiv f \equiv 4 \bmod 6$ so we can use eq. (A.1)-(ii) to further give $(L, M) \equiv (1, 4), (2, 2) \bmod 5$. Lastly, $x' \equiv 2657, ..., 10649 \bmod 13320$ gives $t \equiv 4 \bmod 6$ and $f \equiv 2 \bmod 6$, and then eq. (A.1)-(iii) gives $(L, M) \equiv (3, 3), (1, 4) \bmod 5$. Thus, $(\frac{5}{p})_3 = (\frac{5}{p})_2 = -1$ by Thm. A.4-(iii), so that $x^{18} - (u + 2)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
T_3: $x' \equiv 5372, ..., 10145 \bmod 13320$ implies $p \equiv 7 \bmod 12$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 1)$. $N_{2,1}(u + 3) = 10$. To show $(\frac{10}{p})_3 = (\frac{10}{p})_2 = -1$ we must split the congruencies. $x' \equiv 3929, ..., 10145 \bmod 13320$ implies $p \equiv 7 \bmod 24$ so that $(\frac{2}{p})_2 = 1$, and also that $p \equiv 2, 3 \bmod 5$ so that $(\frac{5}{p})_2 = -1$, which gives $(\frac{10}{p})_2 = -1$. Each of the four congruencies give a different pair for $(t, f) \bmod 6$: $x' \equiv 5372 \bmod 13320 \rightarrow (t, f) \equiv (1, 3) \bmod 6$, so using eq. (A.1)-(i) gives L, M both odd but $L \equiv 0 \bmod 5$. $x' \equiv 3929 \bmod 13320 \rightarrow (t, f) \equiv (4, 4) \bmod 6$, so using eq. (A.1)-(ii) gives L, M both odd but again $L \equiv 0 \bmod 5$. $x' \equiv 8924 \bmod 13320 \rightarrow (t, f) \equiv (1, 1) \bmod 6$, so using eq. (A.1)-(ii) again gives L, M both odd and $L \equiv 0 \bmod 5$. $x' \equiv 10145 \bmod 13320 \rightarrow (t, f) \equiv (4, 2) \bmod 6$, so using eq. (A.1)-(iii) this time gives L, M both odd and $L \equiv 0 \bmod 5$. Thus, for all four cases $(\frac{2}{p})_3 = -1$ by Thm. A.4-(i) and $(\frac{5}{p})_3 = 1$ by Thm. A.4-(iii) so that $(\frac{10}{p})_3 = -1$. For the second set $x' \equiv 488, 4373, 5816 \bmod 13320$. For both $x' \equiv 488, 5816 \bmod 13320$, $(t, f) \equiv (1, 5) \bmod 6$ so using eq. (A.1)-(iii) gives both L and M as even, but with either $(L, M) \equiv (3, 1), (3, 4) \bmod 5$ so that $(\frac{2}{p})_3 = -1$ but $(\frac{5}{p})_3 = 1$ from A.4-(i) and (iii), meaning $(\frac{10}{p})_3 = -1$. Lastly, $x' \equiv 4373 \bmod 13320$ gives $(t, f) \equiv (4, 0) \bmod 6$ so eq. (A.1)-(i) shows that $(L, M) \equiv (2, 4) \bmod 10$, meaning again that $(\frac{10}{p})_3 = -1$. Thus, $(\frac{10}{p})_2 = (\frac{10}{p})_3 = -1$ in all cases so $x^{18} - (u + 3)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
T_4: $x' \equiv 710, ..., 2102 \bmod 2664$ implies $p \equiv 13 \bmod 24$ so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 2)$ (by Prop. A.2). $N_{2,1}(u) = 2$, and $(\frac{2}{p})_3 = -1$ as follows. Again, we need to split the possibilities: $x' \equiv 710, 1214 \bmod 2664$ gives $(t, f) \equiv (1, 3) \bmod 6$ so using eq. (A.1)-(i) gives L and M both odd. $x' \equiv 155, 659 \bmod 2664$ gives $(t, f) \equiv (4, 2) \bmod 6$ so that eq. (A.1)-(iii) gives both L and M as odd. $x' \equiv 1931, 2435 \bmod 2664$ gives $(t, f) \equiv (4, 4) \bmod 6$ so that this time eq. (A.1)-(ii) gives both L and M as odd. Lastly, $1598, 2102 \bmod 2664$ gives $(t, f) \equiv (1, 1) \bmod 6$ so again eq. (A.1)-(ii) gives both L and M as odd. Thus, $(\frac{2}{p})_3 = (\frac{2}{p})_3 = -1$ by Thm. A.4-(i), so that $x^{18} - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □
T_5: $x' \equiv 9035, ..., 5210 \bmod 13320$ implies $p \equiv 37 \bmod 180$, and the only possibilities for p modulo 5 are 2, 3, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2 + 5)$ by Thm. A.3. $N_{2,1}(u) = 5$, and $(\frac{5}{p})_3 = -1$ as follows. Again we require splitting the congruencies: for $x' \equiv 4322, ..., 10982 \bmod 13320$ we have $(t, f) \equiv (1, 5) \bmod 6$ and $x' \equiv 1487 \bmod 13320$ we have $(t, f) \equiv (4, 2) \bmod 6$, so for both these cases eq. (A.1)-(iii) reveals that $(L, M) \equiv (3, 3) \bmod 5$ so that $LM \not\equiv 0 \bmod 5$. $x' \equiv 7874, 10034 \bmod 13320$ gives $(t, f) \equiv (1, 3) \bmod 6$ and $x' \equiv 6875, 11699, 9035 \bmod 13320$ gives $(t, f) \equiv (4, 0) \bmod 6$ so applying eq. (A.1)-(i) to both gives $(L, M) \equiv (1, 4), (1, 1) \bmod 5$ so that $LM \not\equiv 0 \bmod 5$. Lastly, $x' \equiv 770, 2930 \bmod 13320$ gives $(t, f) \equiv$

$(1,1)$ mod 6 demanding the use of eq. (A.1)-(ii) to show that $(L,M) \equiv (1,4) \bmod 5$ so that $LM \not\equiv 0 \bmod 5$. In all cases then, $(\frac{5}{p})_3 = (\frac{5}{p})_2 = -1$ by Thm. A.4-(iii), $x^{18} - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

b_5: $n \equiv 117649 \bmod 352947$, $p \equiv 1 \bmod 6$. Three cases arise: $(t,f) \equiv (1,0) \bmod 3$ uses Step 2 of Alg. A.6 with $b' = 20$ to give $20^{(p-1)/6} \equiv -1 \bmod p$. $(t,f) \equiv (1,1) \bmod 3$ needs Step 4 and $(t,f) \equiv (1,2) \bmod 3$ both use Step 4 with $b' = 20$ to give $20^{(p-1)/6} \bmod p$ as $2t/(3f+t)$ and $2t/(-3f+t)$ respectively. All three cases require further division of b by 2^6 to give the smaller constant $b = 5$. □

b_2: $n \equiv 470596 \bmod 3176523$, $p \equiv 19 \bmod 54$. $(t,f) \equiv (1,0) \bmod 3$ always, so Step 2 of Alg. A.6 with $b' = 8$ gives $8^{(p-1)/6} \equiv -1 \bmod p$, and division of b by 2^6 gives the result.

b_{10}: $n \equiv 117649 \bmod 1764735$, $p \equiv 1 \bmod 12$. Three cases arise: $(t,f) \equiv (1,0) \bmod 3$ uses Step 2 of Alg. A.6 with $b' = 40$ to give $40^{(p-1)/6} \equiv -1 \bmod p$. $(t,f) \equiv (1,1) \bmod 3$ needs Step 4 and $(t,f) \equiv (1,2) \bmod 3$ both use Step 4 with $b' = 40$ to give $40^{(p-1)/6} \bmod p$ as $2t/(3f+t)$ and $2t/(-3f+t)$ respectively. All three cases require further division of b by 2^6 to give the smaller constant $b = 10$. □

b_{-1}: $n \equiv 470596 \bmod 2823576$, $p \equiv 7 \bmod 12$. Three cases arise: $(t,f) \equiv (1,0) \bmod 3$ uses Step 2 of Alg. A.6 with $b' = -4$ to give $-4^{(p-1)/6} \equiv -1 \bmod p$. $(t,f) \equiv (1,1) \bmod 3$ needs Step 4 and $(t,f) \equiv (1,2) \bmod 3$ both use Step 4 with $b' = -4$ to give $-4^{(p-1)/6} \bmod p$ as $2t/(3f+t)$ and $2t/(-3f+t)$ respectively. All three cases require further division of b by 2^6 to give the smaller constant $b = -1$. □

b_{-4}: $n \equiv 30471091 \bmod 33882912$, $p \equiv 31 \bmod 36$. $(t,f) \equiv (1,1) \bmod 3$ is the only case. Thus, $b' = -16$ into Step 4 of Alg. A.6 gives $-16^{(p-1)/6} \equiv 2t/(3f+t)$, and division of b by 2^6 gives $b = -4$. □

b_3: $n \equiv 30471091 \bmod 33882912$, $p \equiv 103 \bmod 108$. Two cases arise: $(t,f) \equiv (1,1) \bmod 3$ and $(t,f) \equiv (1,2) \bmod 3$, so applying Step 4 of Alg. A.6 with $b' = 12$ to both gives $-16^{(p-1)/6} \bmod p$ as $2t/(3f+t)$ and $2t/(-3f+t)$ respectively. Division by 2^6 gives the result. □

b_{-2}: $n \equiv 41765395 \bmod 101648736$, $p \equiv 127 \bmod 216$. We always have $(t,f) \equiv (1,0) \bmod 3$, so Step 2 of Alg. A.6 with $b' = -8$ gives $-8^{(p-1)/6} \equiv -1 \bmod p$. Further division of $b = 16b'$ by 2^6 gives the result. □

b_{-5}: $n \equiv 166002739 \bmod 169414560$, $p \equiv 139 \bmod 180$. We always have $(t,f) \equiv (1,2) \bmod 3$ so Step 4 of Alg. A.6 with $b' = -20$ gives $-20^{(p-1)/6} \equiv 2t/(-3f+t) \bmod p$. Again, further division of $b = 16b'$ by 2^6 gives the result. □

$k = 48$ **BLS curves.** T_1: $x \equiv 7, 31 \bmod 72$ implies $p \equiv 19 \bmod 24$, $x \equiv 16, 64 \bmod 72$ implies $p \equiv 19 \bmod 24$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+1)$. $N_{2,1}(u) = 2$, $(\frac{2}{p})_2 = -1$ (Prop. A.2) and $(\frac{2}{p})_3 = -1$ as follows. We have to prove each case separately: $x \equiv 7 \bmod 72$ gives $t \equiv f \equiv 2 \bmod 6$, whilst $x \equiv 16 \bmod 72$ gives $t \equiv f \equiv 5 \bmod 6$, so using eq. (A.1)-(ii) gives L and M both odd for both cases. $x \equiv 31 \bmod 72$ gives $t \equiv 2 \bmod 6$ and $f \equiv 4 \bmod 6$, so using A.1-(iii) gives L and M both odd for both cases. Lastly, $x \equiv 64 \bmod 72$ gives $t \equiv 5 \bmod 6$ and $f \equiv 3 \bmod 6$, so applying eq. (A.1)-(i) further gives L and M both odd for both cases. Thus, $(\frac{2}{p})_3 = (\frac{2}{p})_2 = -1$ by Thm. A.4-(i), so that $x^{24} - (u+1)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_2: $x \equiv 235, ..., 139 \bmod 360$ implies $p \equiv 7 \bmod 60$, $x \equiv 4, ..., 340 \bmod 360$ implies $p \equiv 7 \bmod 60$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+1)$. $N_{2,1}(u+2) = 5$, which is not a quadratic residue since $x \equiv 235, ..., 139 \bmod 360$ gives $p \equiv 2 \bmod 5$, invoking Thm. A.3. To prove $(\frac{5}{p})_3 = -1$, we need to case bash. $x \equiv 55, 235 \bmod 360$ gives $(t,f) \equiv (2,0) \bmod 6$ so we can apply eq. (A.1)-(i) to further yield $(L,M) \equiv (1,4) \bmod 5$, so that $LM \not\equiv 0 \bmod 5$, $x \equiv 115, 259 \bmod 360$ gives $(t,f) \equiv (2,2) \bmod 6$ so we apply eq. (A.1)-(ii) to further yield $(L,M) \equiv (1,1), (1,4) \bmod 5$, giving $LM \not\equiv 0 \bmod 5$. Lastly, $x \equiv 139 \bmod 360$ gives $(t,f) \equiv (2,4) \bmod 6$, so applying A.1-(iii) to further yield $(L,M) \equiv (1,1) \bmod 5$ gives $LM \not\equiv 0 \bmod 5$. Thus, $(\frac{5}{p})_3 = (\frac{5}{p})_2 = -1$ by Thm. A.4-(iii), meaning that $x^{24} - (u+2)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_3: $x \equiv 13, 61 \bmod 72$ implies $p \equiv 13 \bmod 24$, $x \equiv 10, 34 \bmod 72$ implies $p \equiv 13 \bmod 24$,so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+2)$ from (Prop. A.2). $N_{2,1}(u) = 2$, and $(\frac{2}{p})_3 = -1$ as follows. $x \equiv 34, 61 \bmod 72$ gives $(t,f) \equiv (5,5) \bmod 6$ and $(t,f) \equiv (2,2) \bmod 6$ respectively, which insists use of eq. (A.1)-(ii) to give L and M as both odd. $x \equiv 10 \bmod 72$ gives $(t,f) \equiv (1,0) \bmod 6$ so that eq. (A.1)-(i) can be used to show L is odd. Lastly, $x \equiv 13 \bmod 72$ gives $(t,f) \equiv (2,4)$ so that A.1-(iii) can be used to show L and M are both odd. Thus, $(\frac{2}{p})_3 = (\frac{2}{p})_2 = -1$ by Thm. A.4-(i), so that $x^{24} - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_4: $x \equiv 37, 181 \bmod 216$ implies $p \equiv 37 \bmod 144$, $x \equiv 130, 202 \bmod 216$ implies $p \equiv 133 \bmod 216$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+2)$. $N_{2,1}(u+2) = 6$. We first have that $(\frac{2}{p})_2 = -1$ Prop. A.2, but $(\frac{2}{p})_3 = 1$ for all cases as follows. $x \equiv 37, 181 \bmod 216$ gives $(t,f) \equiv (2,0) \bmod 6$ so that we can use eq. (A.1)-(i) to show that L and M are both even. $x \equiv 130, 202 \bmod 216$ gives $(t,f) \equiv (5,1) \bmod 6$ so we can use A.1-(iii) to show that L and M are both even. Thus, $(\frac{2}{p})_3 = 1$. On the other hand, we show that $(\frac{3}{p})_2 = 1$ but $(\frac{3}{p})_3 = -1$. Note that $p \equiv 1 \bmod 12$ so that Thm. A.3-(b) gives $(\frac{3}{p})_2 = 1$. To show $(\frac{3}{p})_3 = -1$, the

same congruencies and corresponding (t, f) pairs immediately give that $M \not\equiv 0 \bmod 3$ in all cases. Thus, $(\frac{6}{p})_3 = (\frac{6}{p})_2 = -1$ by Thm. A.4-(i) and (ii), so that $x^{24} - (u+2)$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

T_5: $x \equiv 25, 145, 49, 169 \bmod 360$ implies $p \equiv 97 \bmod 120$, $x \equiv 70, 190, 94, 214 \bmod 360$ implies $p \equiv 97 \bmod 120$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p(u) = \mathbb{F}_p[u]/(u^2+5)$. $N_{2,1}(u) = 5$, and $(\frac{5}{p})_2 = -1$ (by Thm. A.3-(a) with $p \equiv 2 \bmod 5$), and further $(\frac{5}{p})_3 = -1$ as follows. $x \equiv 190 \bmod 360$ gives $(t, f) \equiv (5, 3) \bmod 6$ and $x \equiv 145 \bmod 360$ gives $(t, f) \equiv (2, 0) \bmod 6$. In both cases, eq. (A.1)-(i) gives $(L, M) \equiv (1, 4) \bmod 5$ so that $LM \not\equiv 0 \bmod 5$. For $x \equiv 25, 169 \bmod 360$, $(t, f) \equiv (2, 2) \bmod 6$ whilst for $x \equiv 70, 214 \bmod 360$, $(t, f) \equiv (5, 5) \bmod 6$, so eq. (A.1)-(ii) gives $(L, M) \equiv (1, 4), (4, 4) \bmod 5$ so that $LM \not\equiv 0 \bmod 5$. Lastly, $x \equiv 49 \bmod 360$ gives $(t, f) \equiv (2, 4) \bmod 6$ so application of A.1-(iii) further reveals that $(L, M) \equiv (1, 1) \bmod 5$, meaning that $LM \not\equiv 0 \bmod 5$. Thus, $(\frac{5}{p})_3 = (\frac{5}{p})_2 = -1$ by Thm. A.4-(iii), so that $x^{24} - u$ is irreducible in $\mathbb{F}_{p^2}[x]$ by Thm. A.1. □

b_1: $n \equiv 0 \bmod 12$. $n \equiv 0 \bmod 12$ needs b as square and cube, so for any non-square, non-cube g, 1 is the only possibility in $\{1, g, g^2, g^3, g^4, g^5\}$. □

b_{-2}: $n \equiv 27 \bmod 432$, $p \equiv 19 \bmod 72$. $(t, f) \equiv (2, 0) \bmod 3$ means $b = 16$, and $(\frac{-2}{p})_2 = 1$ so $-8 \equiv \mu^6$ for $\mu = \sqrt{-2}$, so $b = -2$ gives an isomorphic curve. □

b_{-3}: $n \equiv 147 \bmod 216$, $p \equiv 7 \bmod 12$. Two cases: $(t, f) \equiv (2, 1) \bmod 3$ and $(t, f) \equiv (2, 2) \bmod 3$, both of which use Step 3 of Alg. A.6 with $b' = -12$ to give $-12^{(p-1)/6} \bmod p$ as $2t/(3f - t)$ and $2t/(-3f - t)$ respectively. Division of $b = 16b'$ by 2^6 gives the result. □

b_4: $n \equiv 3 \bmod 72$, $p \equiv 1 \bmod 18$. $(t, f) \equiv (2, 2) \bmod 3$ is the only option, so $b' = 16$ into Step 3 of Alg. A.6 gives $16^{(p-1)/6} \equiv 2t/(-3f - t) \bmod p$. Division of $b = 16b'$ by 2^6 finishes the proof. □

b_2: $n \equiv 243 \bmod 432$. $(t, f) \equiv (2, 0) \bmod 3$ means $b = 16$ from Step 1 of Alg. A.6. Division by $8 = \mu^3$ for $\mu = \sqrt{2}$ gives an isomorphic curve with $b = 2$. □

b_{-5}: $n \equiv 3 \bmod 360$, $p \equiv 1267 \bmod 1620$. $(t, f) \equiv (2, 1) \bmod 3$ is the only option, so Step 3 with $b' = -20$ yields $-20^{(p-1)/6} \equiv 2t/(3f - t) \bmod p$. Division of $b = 16b'$ by 2^6 gives the result. □

b_3: $n \equiv 3 \bmod 24$, $p \equiv 1 \bmod 12$. Three cases arise: $(t, f) \equiv (2, 0) \bmod 3$ means $b = 16$. It isn't hard to show $3/16 = \mu^6$ for $\mu \in \mathbb{F}_p$ so that $b = 3$ gives an isomorphic curve. The other two cases are $(t, f) \equiv (2, 1) \bmod 3$ and $(t, f) \equiv (2, 2) \bmod 3$, both of which use $b' = 12$ in Step 3 of Alg. A.6 to give $12^{(p-1)/6} \bmod p$ as $2t/(3f-t)$ and $2t/(-3f-t)$ respectively. Division of $b = 16b'$ by 2^6 gives an isomorphic curve and finishes the proof. □

b_9: $n \equiv 3 \bmod 24$, $p \equiv 1 \bmod 6$. Two cases: $(t, f) \equiv (2, 0) \bmod 3$ means $b = 16$, for which it isn't hard to show $9/16 = \mu^3$ (and hence $\tilde{\mu}^6$), giving $b = 9$ as an isomorphic curve. □

b_5: $n \equiv 3 \bmod 24$, $p \equiv 1 \bmod 30$. Two cases: $(t, f) \equiv (2, 0) \bmod 3$ means $b = 16$. Again we use $5/16 = \mu^6$ for some μ to give the smaller constant. For the second case, $(t, f) \equiv (2, 1) \bmod 3$, so Step 3 of Alg. A.6 with $b' = 20$ gives $20^{(p-1)/6} \equiv 2t/(3f - t) \bmod p$, and division of $b = 16b'$ by 2^6 finishes the proof. □

b_2: $n \equiv 243 \bmod 432$. $(t, f) \equiv (2, 0) \bmod 3$ is the only case, which immediately gives $b = 16$ from Step 1 of Alg. A.6. $(\frac{2}{p})_2 = 1$ is easy (Prop. A.2), so $8 = \mu^6$ and $b = 2$ is a smaller constant. □

Appendix B. Some more generators

For the sake of protocols or implementations that may require them, this section lists extra generators that were found in the pairing groups G_1 and G_2 in each of the subfamilies. For the most part we stopped looking for any more once we had found 2 or 3 extra generators in any subfamily.

B.1. **More compact generators for $k = 8$.** Refer back to Table 2 - (i) : In G_2, we also have $[h'](2/u, \sqrt{-4/u - 1})$. (ii) : In G_2, $[h'](u-3, \sqrt{(u-3)^3 + (u-3)u}$, $[h'](u+2, \sqrt{(u+2)^3 + u(u+2)})$. (iii) : In G_1, $(-1, \sqrt{1})$, $(-2, \sqrt{-4})$, $(2, 2)$. In G_2, $(u + 2, \sqrt{(u+2)^3 - 2(u+2)/u})$ and $(u - 3, \sqrt{(u-3)^3 - 2(u-3)/u}$ also work. (iv) : In G_2 is $[h'](-1, \sqrt{-1 - 2u})$. (v) : In G_2 we also have $[h](-3, 2\sqrt{-6})$, $[h](-1, \sqrt{2})$ and $[h](3, \sqrt{30})$; G_2 also has $[h'](-1, -1 + 3/u)$. (vi) : G_1 also has $[h](-4, 6\sqrt{-2})$. (vii) : Again, G_1 also has $[h](-4, 6\sqrt{-2})$. $(viii)$: G_1 also has $[h](-2, 2\sqrt{-3})$. (ix) : Again, G_1 has $[h](-2, 2\sqrt{-3})$ too. G_2 also has $[h']\left(-5, \sqrt{-125 - 25/u}\right)$.

B.2. **More compact generators for $k = 12$.** Refer back to Table 4 - (i) : In G_1, we also have $[h']\left(-5, \sqrt{-128}\right)$, $[h']\left(3, \sqrt{24}\right)$ and $[h']\left(9, \sqrt{726}\right)$.

B.3. **More compact generators for $k = 18$.** Refer back to Table 8 - for all cases here, the extra generators are in G_1: (i) $[h](-3, \sqrt{-25})$, $[h](1, \sqrt{3})$; (ii) $[h](-1, \sqrt{3})$; (iii) $[h](-2, 4\sqrt{-3})$, $[h](1, \sqrt{-3})$, $[h](5, 11)$; (iv) $[h](-3, 2\sqrt{-6})$, $[h](-1, \sqrt{2})$; (v) $[h](-2, 2\sqrt{-3})$, $[h](1, \sqrt{-3})$; (vi) $[h](-5, 2\sqrt{-30})$, $[h](-2, \sqrt{-3})$; (vii) $[h](-1, 2\sqrt{-2})$.

B.4. **More compact generators for $k = 27$.** Refer back to Table 10 - all the extra generators are in G_1: (i) : $[h](-5, 8\sqrt{-2})$, $[h](3, 2\sqrt{6})$ $[h](9, 11\sqrt{6})$; (ii): $[h](7, 4\sqrt{21})$; (iii) : $[h](3, 6)$, $[h](6, 3\sqrt{5})$.

B.5. **More compact generators for $k = 32$.** Refer back to Table 12 - all the extra generators are in G_1: (i): $[h](-5, 8\sqrt{-2})$, $[h](3, 2\sqrt{6})$, $[h](9, 11\sqrt{6})$; (ii): $[h](-4, 6\sqrt{2})$; (iii): $[h](-3, 6\sqrt{-1})$, $[h](-1, 2\sqrt{-1})$, $[h](3, 6)$.

B.6. **More compact generators for $k = 36$.** Refer back to Table 14 - all the extra generators are in G_1: (i): $[h](-2, 2\sqrt{-3})$, $[h](1, \sqrt{-3})$, $[h](5, 11)$; (ii): $[h](-2, \sqrt{-10})$, $[h](-1, \sqrt{-3})$; (iii): $[h](-2, \sqrt{-5})$; (iv): $[h](3, \sqrt{30})$; (v): $[h](5, 2\sqrt{30})$; (vi): $[h](-2, 2\sqrt{-3})$, $[h](-1, \sqrt{-5})$, $[h](1, \sqrt{-3})$, $[h](4, 2\sqrt{15})$.

B.7. **More compact generators for $k = 48$.** Refer back to Table 16 - (i): Both in G_2 are $[h'](-1 - 2/w, \sqrt{(-1 - 2/w)^3 - 2})$, $[h'](\pm 5 - 2/w, \sqrt{(\pm 5 - 2/w)^3 - 2})$; (ii): In G_2 is $[h'](1 - w, \sqrt{(1 - w)^3 + 1})$; (iii): In G_2 is $[h'](-2, \sqrt{-8 + 4w})$; (iv): All in G_2 are $[h'](-1, \sqrt{-1 + 4w})$, $[h'](-3, \sqrt{-27 + 4w})$, $[h'](3, \sqrt{27 + 4w})$; (v): In G_2 is $[h'](-1, \sqrt{1 - w})$; (vi): All in G_1 are $[h](-5, 11\sqrt{1})$, $[h](-2, 2\sqrt{-1})$, $[h](2, 2\sqrt{3})$.

Appendix C. Example curves from 5-star subfamilies

We give numerous examples of pairing-friendly curves that belong to some of the 5-star subfamilies in each family. The security levels covered by a particular family come from Table 17. In most cases, our searches returned many more low-weight curves than what we have presented, so we have chosen a small sample that also spans a few bits slightly below the exact security level. When we found them, we chose to include curves whose hamming-weight is equal to their NAF-weight, and have marked these cases with an asterix (next to the weight given) in the tables.

As mentioned in [8], odd congruencies generally find curves with a signed binary (NAF) representation whose weight is one more than those of even congruencies, since the last bit is forced to be ± 1 in the former case.

The reader is reminded that although the KSS subfamilies are presented with simplified congruencies $x' \equiv a \bmod b$, the actual congruencies in should be re-inflated (before searching) to $x \equiv au \bmod bu$, where $u = 5, 14, 13, 7$ for $k = 16, 18, 32, 36$ respectively. Thus, for $k = 18$ where $u = 14$, congruencies in x' that appear to be odd, are actually even congruencies in x.

Lastly, we remark that the curves in Tables 18-25 have certainly not exhausted all curves belonging to the associated family, up to the given weights, and for the given security ranges. In most cases, our searches would terminate when a prescribed number of curves were found, and if resumed, would be kick-started somewhere else entirely, in order to better span neighboring bits the targeted level of security.

E-mail address: craig.costello@qut.edu.au

112-bit secure curves					
family	subfamily/details	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
Brezing-Weng $k = 8$ (see §3)	$x \equiv 1 \bmod 16$ $T_1,\ a_1,\ D$	$1 - 2^{21} + 2^{48} - 2^{52}$	4	316 / 113	210 / 104
		$1 - 2^{46} - 2^{49} - 2^{52}$	4	318 / 113	211 / 105
		$1 + 2^{18} + 2^{52}$	3*	317 / 113	211 / 105
		$1 + 2^{12} + 2^{28} + 2^{52}$	4*	317 / 113	211 / 105
		$1 - 2^{6} + 2^{33} + 2^{53}$	4	323 / 114	215 / 107
		$1 - 2^{4} - 2^{14} - 2^{54}$	4	329 / 115	219 / 109
		$1 - 2^{24} + 2^{33} + 2^{54}$	4	329 / 115	219 / 109
		$1 - 2^{17} - 2^{35} - 2^{54}$	4	329 / 115	219 / 109
		$1 + 2^{16} - 2^{48} - 2^{54}$	4	329 / 115	219 / 109
		$1 + 2^{43} - 2^{53} + 2^{55}$	4	332 / 116	221 / 110
		$1 + 2^{9} + 2^{55}$	3*	335 / 116	223 / 111
		$1 - 2^{5} + 2^{20} - 2^{55}$	4	335 / 116	223 / 111
		$1 + 2^{18} + 2^{37} - 2^{55}$	4	335 / 116	223 / 111
		$1 - 2^{21} + 2^{40} - 2^{55}$	4	335 / 116	223 / 111
		$1 + 2^{37} + 2^{41} + 2^{55}$	4*	335 / 116	223 / 111
		$1 + 2^{5} + 2^{46} + 2^{55}$	4*	335 / 116	223 / 111
		$1 - 2^{43} - 2^{47} + 2^{55}$	4	335 / 116	223 / 111
		$1 - 2^{13} + 2^{54} - 2^{56}$	4	338 / 117	225 / 112
	$x \equiv 3 \bmod 16$ $T_1,\ a_{-2},\ D$	$-1 + 2^{2} - 2^{18} - 2^{52}$	4	317 / 113	211 / 105
		$-1 + 2^{2} + 2^{25} + 2^{27} + 2^{53}$	5	323 / 114	215 / 107
		$-1 + 2^{2} - 2^{21} - 2^{49} - 2^{53}$	5	323 / 114	215 / 107
		$-1 + 2^{2} + 2^{9} + 2^{51} - 2^{54}$	5	328 / 115	218 / 108
		$-1 + 2^{2} - 2^{4} - 2^{12} - 2^{54}$	5	329 / 115	219 / 109
		$-1 + 2^{2} - 2^{18} + 2^{20} + 2^{54}$	5	329 / 115	219 / 109
		$-1 + 2^{2} + 2^{13} + 2^{24} + 2^{54}$	5	329 / 115	219 / 109
		$-1 + 2^{2} - 2^{34} - 2^{54}$	4	329 / 115	219 / 109
		$-1 + 2^{2} - 2^{6} - 2^{18} + 2^{55}$	5	335 / 116	223 / 111
		$-1 + 2^{2} + 2^{11} - 2^{26} - 2^{55}$	5	335 / 116	223 / 111
		$-1 + 2^{2} + 2^{34} - 2^{40} + 2^{55}$	5	335 / 116	223 / 111
		$-1 + 2^{2} + 2^{11} - 2^{43} - 2^{55}$	5	335 / 116	223 / 111
		$-1 + 2^{2} + 2^{41} + 2^{48} + 2^{55}$	5	335 / 116	223 / 111
	$x \equiv 9 \bmod 16$ $T_1,\ a_1,\ M$	$1 - 2^{3} + 2^{24} + 2^{48} - 2^{53}$	5	323 / 114	214 / 106
		$1 + 2^{3} + 2^{5} - 2^{25} + 2^{53}$	5	323 / 114	215 / 107
		$1 - 2^{3} - 2^{5} + 2^{48} + 2^{53}$	5	323 / 114	215 / 107
		$1 - 2^{3} - 2^{19} - 2^{29} - 2^{54}$	5	329 / 115	219 / 109
		$1 + 2^{3} - 2^{7} - 2^{42} - 2^{54}$	5	329 / 115	219 / 109
		$1 + 2^{3} - 2^{39} + 2^{45} + 2^{54}$	5	329 / 115	219 / 109
		$1 + 2^{3} + 2^{35} - 2^{48} - 2^{54}$	5	329 / 115	219 / 109
		$1 - 2^{3} - 2^{41} - 2^{53} + 2^{55}$	5	332 / 116	221 / 110
		$1 - 2^{3} - 2^{11} + 2^{16} - 2^{55}$	5	335 / 116	223 / 111
		$1 + 2^{3} + 2^{6} + 2^{30} + 2^{55}$	5*	335 / 116	223 / 111
		$1 - 2^{3} + 2^{13} + 2^{38} - 2^{55}$	5	335 / 116	223 / 111
		$1 - 2^{3} - 2^{20} + 2^{38} - 2^{55}$	5	335 / 116	223 / 111
		$1 + 2^{3} - 2^{23} + 2^{38} + 2^{55}$	5	335 / 116	223 / 111
		$1 - 2^{3} - 2^{17} + 2^{39} + 2^{55}$	5	335 / 116	223 / 111
		$1 - 2^{3} + 2^{37} + 2^{39} - 2^{55}$	5	335 / 116	223 / 111
		$1 - 2^{3} - 2^{23} - 2^{44} + 2^{55}$	5	335 / 116	223 / 111
		$1 - 2^{3} + 2^{9} - 2^{46} + 2^{55}$	5	335 / 116	223 / 111
		$1 + 2^{3} - 2^{36} - 2^{47} - 2^{55}$	5	335 / 116	223 / 111
		$1 - 2^{3} - 2^{28} - 2^{49} - 2^{55}$	5	335 / 116	223 / 111
		$1 - 2^{3} - 2^{37} - 2^{52} - 2^{55}$	5	336 / 116	223 / 111
	$x \equiv 11 \bmod 16$ $T_1,\ a_2,\ M$	$-1 - 2^{2} - 2^{5} - 2^{13} + 2^{53}$	5	323 / 114	215 / 107
		$-1 - 2^{2} - 2^{9} + 2^{23} + 2^{53}$	5	323 / 114	215 / 107
		$-1 - 2^{2} + 2^{19} + 2^{33} + 2^{53}$	5	323 / 114	215 / 107
		$-1 - 2^{2} - 2^{12} - 2^{27} - 2^{54}$	5*	329 / 115	219 / 109
		$-1 - 2^{2} - 2^{24} - 2^{37} - 2^{54}$	5*	329 / 115	219 / 109
		$-1 - 2^{2} + 2^{37} + 2^{39} + 2^{54}$	5	329 / 115	219 / 109
		$-1 - 2^{2} - 2^{7} + 2^{13} - 2^{55}$	5	335 / 116	223 / 111
		$-1 - 2^{2} + 2^{13} + 2^{17} - 2^{55}$	5	335 / 116	223 / 111
		$-1 - 2^{2} + 2^{42} - 2^{45} + 2^{55}$	5	335 / 116	223 / 111
		$-1 - 2^{2} - 2^{25} + 2^{46} + 2^{55}$	5	335 / 116	223 / 111
		$-1 - 2^{2} - 2^{11} + 2^{48} + 2^{55}$	5	335 / 116	223 / 111
		$-1 - 2^{2} + 2^{32} + 2^{54} - 2^{56}$	5	338 / 117	225 / 112

TABLE 18. Low weight curves offering 112-bit security.

192-bit secure curves					
family	subfamily/details	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
BLS $k = 12$ (see §4)	$x \equiv 64 \bmod 72$ $T_1,\ b_{-2},\ D$	$2^{48} - 2^{72} - 2^{105}$	3	629 / 187	421 / 210
		$2^{23} + 2^{34} + 2^{106}$	3^*	635 / 188	425 / 212
		$2^{46} + 2^{74} - 2^{108}$	3	647 / 189	432 / 215
		$-2^{71} + 2^{81} - 2^{109}$	3	653 / 190	436 / 217
		$-2^{21} + 2^{91} - 2^{109}$	3	653 / 190	436 / 217
		$-2^{49} + 2^{73} - 2^{111}$	3	665 / 192	444 / 221
		$-2^{40} - 2^{67} - 2^{111}$	3^*	665 / 192	445 / 222
		$2^{79} - 2^{91} - 2^{111}$	3	665 / 192	445 / 222
	$x \equiv 16, 88 \bmod 216$ $T_1,\ b_4,\ M$	$-2^{52} + 2^{62} - 2^{105}$	3	629 / 187	420 / 209
		$2^{19} + 2^{84} - 2^{107}$	3	641 / 189	428 / 213
		$-2^{23} + 2^{96} + 2^{109}$	3	653 / 190	437 / 218
		$2^{11} - 2^{25} + 2^{110}$	3	659 / 191	440 / 219
		$-2^{41} + 2^{82} - 2^{110}$	3	659 / 191	440 / 219
		$2^{60} - 2^{107} - 2^{112}$	3	671 / 192	449 / 224
	$x \equiv 160 \bmod 216$ $T_1,\ M,\ b_{-3}$	$-2^{24} - 2^{32} - 2^{34} - 2^{105}$	4^*	629 / 187	421 / 210
		$-2^{14} - 2^{16} - 2^{44} - 2^{107}$	4^*	641 / 189	429 / 214
		$-2^{4} - 2^{30} - 2^{61} - 2^{108}$	4^*	647 / 189	433 / 216
		$-2^{8} - 2^{45} - 2^{94} - 2^{108}$	4^*	647 / 189	433 / 216
		$-2^{34} - 2^{96} - 2^{103} - 2^{108}$	4^*	647 / 189	433 / 216
		$2^{15} + 2^{25} + 2^{44} + 2^{109}$	4^*	653 / 190	437 / 218
		$-2^{9} - 2^{91} - 2^{99} - 2^{109}$	4^*	653 / 190	437 / 218
		$-2^{16} - 2^{81} + 2^{110}$	3	659 / 191	440 / 219
		$-2^{4} - 2^{62} - 2^{101} - 2^{110}$	4^*	659 / 191	441 / 220
		$2^{5} + 2^{47} + 2^{58} + 2^{111}$	4^*	665 / 192	445 / 222
		$2^{23} + 2^{25} + 2^{66} + 2^{111}$	4^*	665 / 192	445 / 222
		$-2^{73} - 2^{85} - 2^{93} - 2^{111}$	4^*	665 / 192	445 / 222
KSS $k = 16$ (see §5)	$x' \equiv 61, 93 \bmod 112$ $T_1,\ a_1,\ M$	$1 + 2^{12} + 2^{25} + 2^{45} - 2^{48}$	5	469 / 186	367 / 183
		$1 - 2^{26} - 2^{33} + 2^{40} - 2^{48}$	5	471 / 187	369 / 184
		$1 + 2^{21} - 2^{39} + 2^{46} + 2^{48}$	5	474 / 187	371 / 185
		$1 - 2^{12} - 2^{42} + 2^{44} - 2^{46} + 2^{49}$	6	479 / 188	375 / 187
		$1 - 2^{5} + 2^{7} + 2^{29} + 2^{43} - 2^{49}$	6	480 / 188	376 / 187
		$1 + 2^{14} + 2^{21} + 2^{25} + 2^{30} + 2^{49}$	6^*	481 / 189	377 / 188
		$1 - 2^{14} + 2^{24} + 2^{36} + 2^{46} + 2^{49}$	6	482 / 189	378 / 188
		$1 - 2^{29} + 2^{31} - 2^{41} - 2^{47} - 2^{49}$	6	484 / 189	379 / 189
		$1 - 2^{29} - 2^{36} + 2^{38} - 2^{48} + 2^{50}$	6	486 / 189	381 / 190
		$1 - 2^{20} + 2^{23} - 2^{27} + 2^{30} - 2^{50}$	6	491 / 190	385 / 192
	$x' \equiv 23, 103 \bmod 112$ $T_1,\ M,\ a_{-2}$	$-1 + 2^{2} - 2^{17} - 2^{32} - 2^{45} + 2^{49}$	6	480 / 188	376 / 187
		$-1 + 2^{2} - 2^{7} - 2^{11} + 2^{20} + 2^{49}$	6	481 / 189	377 / 188
		$-1 + 2^{2} + 2^{8} + 2^{20} + 2^{23} + 2^{49}$	6	481 / 189	377 / 188
		$-1 + 2^{2} - 2^{21} - 2^{29} + 2^{38} + 2^{49}$	6	481 / 189	377 / 188
		$-1 + 2^{2} + 2^{34} + 2^{36} + 2^{48} - 2^{50}$	6	486 / 189	381 / 190
		$-1 + 2^{2} - 2^{20} - 2^{22} + 2^{31} + 2^{50}$	6	491 / 190	385 / 192
		$-1 + 2^{2} - 2^{7} + 2^{37} + 2^{51}$	5	501 / 192	393 / 196
	$x' \equiv 5, 37 \bmod 112$ $T_1,\ a_1,\ D$	$1 + 2^{3} - 2^{17} + 2^{29} + 2^{47} - 2^{49}$	6	476 / 188	373 / 186
		$1 - 2^{3} + 2^{15} + 2^{20} + 2^{32} + 2^{49}$	6	481 / 189	377 / 188
		$1 + 2^{3} + 2^{9} - 2^{15} + 2^{38} - 2^{49}$	6	481 / 189	377 / 188
		$1 - 2^{3} + 2^{18} - 2^{32} + 2^{41} + 2^{49}$	6	481 / 189	377 / 188
		$1 - 2^{3} + 2^{30} + 2^{39} - 2^{47} - 2^{49}$	6	484 / 189	379 / 189
		$1 - 2^{3} - 2^{10} - 2^{12} + 2^{31} + 2^{50}$	6	491 / 190	385 / 192
		$1 + 2^{3} + 2^{7} - 2^{10} - 2^{37} + 2^{50}$	6	491 / 190	385 / 192
		$1 + 2^{3} + 2^{26} - 2^{44} + 2^{51}$	5	500 / 192	393 / 196
	$x' \equiv 47, 79 \bmod 112$ $T_1,\ a_2,\ D$	$-1 - 2^{2} - 2^{31} - 2^{35} + 2^{48}$	5	471 / 187	369 / 184
		$-1 - 2^{2} + 2^{20} - 2^{41} + 2^{47} - 2^{49}$	6	481 / 189	377 / 188
		$-1 - 2^{2} + 2^{11} - 2^{21} - 2^{35} + 2^{49}$	6	481 / 189	377 / 188
		$-1 - 2^{2} - 2^{4} - 2^{16} - 2^{26} - 2^{50}$	6^*	491 / 190	385 / 192
KSS $k = 18$ (see §6)	$x' \equiv 4 \bmod 36$ $T_1,\ b_2,\ D$	$2^{18} + 2^{34} - 2^{45} - 2^{64}$	4	508 / 203	376 / 187
		$2^{12} + 2^{46} - 2^{51} - 2^{64}$	4	508 / 203	376 / 187
		$2^{28} + 2^{47} - 2^{51} + 2^{64}$	4	508 / 203	376 / 187
		$2^{5} - 2^{15} + 2^{42} - 2^{65}$	4	516 / 205	382 / 190
	$x' \equiv 16 \bmod 108$ $T_1,\ b_6,\ M$	$2^{20} - 2^{24} + 2^{28} + 2^{35} - 2^{64}$	5	508 / 203	376 / 187
		$2^{4} - 2^{8} - 2^{23} + 2^{39} - 2^{64}$	5	508 / 203	376 / 187
		$-2^{13} - 2^{31} - 2^{44} - 2^{62} - 2^{64}$	5^*	511 / 204	378 / 188
		$2^{22} - 2^{36} - 2^{38} - 2^{63} + 2^{65}$	5	513 / 204	380 / 189
		$-2^{15} - 2^{20} + 2^{45} + 2^{63} - 2^{65}$	5	513 / 204	380 / 189
		$-2^{12} + 2^{25} - 2^{60} + 2^{62} - 2^{65}$	5	515 / 205	381 / 190
		$2^{18} + 2^{29} - 2^{35} + 2^{37} + 2^{65}$	5	516 / 205	382 / 190
		$2^{7} - 2^{16} + 2^{40} + 2^{60} + 2^{65}$	5	516 / 205	382 / 190
		$-2^{5} + 2^{21} + 2^{35} - 2^{62} - 2^{65}$	5	517 / 205	383 / 191
		$-2^{24} - 2^{31} + 2^{43} + 2^{62} + 2^{65}$	5	517 / 205	383 / 191
		$2^{25} + 2^{34} + 2^{37} + 2^{64} - 2^{66}$	5	521 / 206	386 / 192
		$-2^{3} - 2^{32} - 2^{42} - 2^{64} + 2^{66}$	5	521 / 206	386 / 192
	$x' \equiv 79 \bmod 108$ $T_1,\ M,\ b_3$	$2^{1} + 2^{29} + 2^{59} + 2^{65}$	4^*	516 / 205	382 / 190
	$x' \equiv 7, 43 \bmod 108$ $T_1,\ M,\ b_{-4}$	$2^{1} - 2^{15} + 2^{18} + 2^{63} + 2^{65}$	5	519 / 205	384 / 191

TABLE 19. Low weight curves offering 192-bit security.

224-bit secure curves					
family	subfamily/details/rating	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
BLS $k = 12$ (see §4)	$x \equiv 64 \bmod 72$ $T_1,\ b_{-2},\ D$	$-2^{34} + 2^{58} + 2^{150}$	3	899 / 219	601 / 300
		$2^{76} + 2^{95} - 2^{151}$	3	905 / 219	604 / 301
		$-2^{101} - 2^{138} - 2^{151}$	3*	905 / 219	605 / 302
		$2^{43} - 2^{59} + 2^{152}$	3	911 / 220	608 / 303
		$-2^{5} - 2^{61} + 2^{153}$	3	917 / 221	612 / 305
		$2^{50} - 2^{131} - 2^{154}$	3	923 / 221	617 / 308
		$2^{96} - 2^{131} + 2^{155}$	3	929 / 222	620 / 309
		$2^{7} - 2^{95} - 2^{155}$	3	929 / 222	621 / 310
		$-2^{65} + 2^{77} + 2^{156}$	3	935 / 222	625 / 312
		$-2^{75} + 2^{111} + 2^{156}$	3	935 / 222	625 / 312
		$2^{30} - 2^{59} - 2^{158}$	3	947 / 224	633 / 316
		$-2^{21} + 2^{60} + 2^{159}$	3	953 / 224	637 / 318
	$x \equiv 16, 88 \bmod 216$ $T_1,\ b_{4},\ M$	$-2^{51} + 2^{88} - 2^{150}$	3	899 / 219	600 / 299
		$2^{88} + 2^{91} - 2^{151}$	3	905 / 219	604 / 301
		$2^{22} + 2^{46} + 2^{151}$	3*	905 / 219	605 / 302
		$-2^{105} - 2^{124} + 2^{152}$	3	911 / 220	608 / 303
		$-2^{47} + 2^{144} - 2^{154}$	3	923 / 221	616 / 307
		$-2^{4} + 2^{88} + 2^{154}$	3	923 / 221	617 / 308
		$-2^{7} + 2^{137} - 2^{155}$	3	929 / 222	620 / 309
		$-2^{127} + 2^{140} + 2^{155}$	3	929 / 222	621 / 310
		$-2^{27} - 2^{147} + 2^{155}$	3	929 / 222	620 / 309
	$x \equiv 160 \bmod 216$ $T_1,\ b_{-3},\ M$	$-2^{95} + 2^{116} - 2^{150}$	3	899 / 219	600 / 299
		$-2^{59} - 2^{67} - 2^{152}$	3*	911 / 220	609 / 304
		$2^{22} - 2^{69} + 2^{153}$	3	917 / 221	612 / 305
		$-2^{22} - 2^{35} - 2^{153}$	3*	917 / 221	613 / 306
		$-2^{83} - 2^{150} - 2^{155}$	3*	929 / 222	621 / 310
		$2^{14} - 2^{34} - 2^{159}$	3	953 / 224	637 / 318
		$-2^{89} - 2^{100} - 2^{159}$	3*	953 / 224	637 / 318
KSS $k = 16$ (see §5)	$x' \equiv 61, 93 \bmod 112$ $T_1,\ a_{1},\ M$	$1 - 2^{22} + 2^{56} + 2^{66} - 2^{69}$	5	679 / 219	535 / 267
		$1 + 2^{14} + 2^{17} + 2^{36} + 2^{69}$	5	681 / 220	537 / 268
		$1 + 2^{25} - 2^{33} - 2^{65} - 2^{70}$	5	691 / 221	545 / 272
		$1 - 2^{20} - 2^{62} + 2^{69} - 2^{71}$	5	696 / 222	549 / 274
		$1 - 2^{47} - 2^{54} - 2^{65} + 2^{71}$	5	700 / 222	552 / 275
		$1 + 2^{21} - 2^{38} + 2^{51} + 2^{71}$	5	701 / 222	553 / 276
		$1 + 2^{23} + 2^{48} + 2^{57} + 2^{71}$	5*	701 / 222	553 / 276
		$1 - 2^{15} - 2^{55} - 2^{66} - 2^{72}$	5	711 / 224	561 / 280
	$x' \equiv 5, 37 \bmod 112$ $T_1,\ a_{1},\ D$	$1 - 2^{3} + 2^{12} + 2^{22} + 2^{30} - 2^{69}$	6	681 / 220	537 / 268
		$1 - 2^{3} + 2^{11} - 2^{47} - 2^{71}$	5	701 / 222	553 / 276
KSS $k = 18$ (see §6)	$x' \equiv 4 \bmod 36$ $T_1,\ b_{2},\ D$	$2^{20} + 2^{26} + 2^{36} - 2^{76}$	4	604 / 219	448 / 223
		$2^{31} - 2^{36} + 2^{51} - 2^{76}$	4	604 / 219	448 / 223
		$2^{38} + 2^{41} + 2^{62} + 2^{76}$	4*	604 / 219	448 / 223
		$2^{6} + 2^{18} - 2^{39} - 2^{78}$	4	620 / 222	460 / 229
		$-2^{19} - 2^{45} + 2^{50} - 2^{78}$	4	620 / 222	460 / 229
		$2^{18} - 2^{57} + 2^{61} - 2^{79}$	4	628 / 223	466 / 232
		$2^{7} - 2^{24} - 2^{26} - 2^{80}$	4	636 / 224	472 / 235
		$-2^{3} - 2^{18} - 2^{49} + 2^{80}$	4	636 / 224	472 / 235
		$2^{24} - 2^{40} + 2^{56} + 2^{80}$	4	636 / 224	472 / 235
		$2^{6} - 2^{13} - 2^{73} - 2^{80}$	4	636 / 224	472 / 235
	$x' \equiv 16 \bmod 108$ $T_1,\ b_{6},\ M$	$2^{18} - 2^{40} - 2^{66} + 2^{74} - 2^{76}$	5	601 / 219	446 / 222
		$-2^{30} + 2^{40} + 2^{50} + 2^{76}$	4	604 / 219	448 / 223
		$2^{13} + 2^{41} + 2^{58} + 2^{71} + 2^{76}$	5*	604 / 219	448 / 223
		$-2^{15} + 2^{18} - 2^{26} - 2^{72} - 2^{76}$	5	605 / 220	449 / 224
		$2^{13} + 2^{23} - 2^{28} + 2^{72} + 2^{76}$	5	605 / 220	449 / 224
		$-2^{6} - 2^{24} - 2^{37} + 2^{75} - 2^{77}$	5	609 / 220	452 / 225
		$-2^{20} - 2^{62} + 2^{68} + 2^{75} - 2^{77}$	5	609 / 220	452 / 225
		$2^{20} + 2^{32} - 2^{62} - 2^{77}$	4	612 / 221	454 / 226
		$-2^{13} + 2^{31} + 2^{37} + 2^{54} + 2^{77}$	5	612 / 221	454 / 226
	$x' \equiv 7, 43 \bmod 108$ $T_1,\ b_{-4},\ M$	$2^{1} + 2^{17} - 2^{22} + 2^{30} + 2^{76}$	5	604 / 219	448 / 223
		$2^{1} - 2^{14} - 2^{55} - 2^{63} - 2^{76}$	5	604 / 219	448 / 223
		$2^{1} + 2^{14} - 2^{61} - 2^{64} - 2^{76}$	5	604 / 219	448 / 223
	$x' \equiv 79 \bmod 108$ $T_1,\ b_{3},\ M$	$2^{1} + 2^{7} - 2^{11} - 2^{41} + 2^{77}$	5	612 / 221	454 / 226

TABLE 20. Low weight curves offering 224-bit security.

256-bit secure curves					
	subfamily/details	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
BLS $k = 27$ (see §7)	$x \equiv 5, 14, 32 \bmod 36$ $T_1,\ b_{-3},\ M$	$-2^{11} - 2^{15} - 2^{23} - 2^{26}$	4^*	522 / 245	470 / 234
		$-2^4 - 2^7 + 2^{21} - 2^{25} + 2^{27}$	5	531 / 247	478 / 238
		$2^2 + 2^7 - 2^{18} - 2^{21} + 2^{27}$	5	538 / 249	484 / 241
		$2^6 - 2^{12} - 2^{17} - 2^{27}$	4	539 / 249	485 / 242
		$2^4 + 2^8 + 2^{16} - 2^{23} - 2^{27}$	5	541 / 249	486 / 242
		$-2^2 + 2^{11} + 2^{14} - 2^{24} - 2^{27}$	5	542 / 249	488 / 243
		$2^9 + 2^{19} - 2^{21} - 2^{26} + 2^{28}$	5	550 / 251	495 / 247
		$-2^4 - 2^{12} + 2^{24} - 2^{26} + 2^{28}$	5	553 / 252	498 / 248
		$2^4 - 2^7 + 2^{14} - 2^{25} + 2^{28}$	5	555 / 252	499 / 249
		$2^3 + 2^7 - 2^{19} - 2^{24} + 2^{28}$	5	557 / 252	501 / 250
		$-2^2 - 2^9 + 2^{11} + 2^{17} + 2^{28}$	5	559 / 253	503 / 251
		$-2^6 + 2^{11} + 2^{13} + 2^{24} + 2^{28}$	5	561 / 253	504 / 251
		$-2^1 - 2^4 + 2^{22} - 2^{26} - 2^{28}$	5	565 / 254	508 / 253
		$-2^{11} + 2^{14} + 2^{20} + 2^{26} + 2^{28}$	5	565 / 254	509 / 254
		$-2^3 - 2^5 + 2^{12} - 2^{14} + 2^{27} - 2^{29}$	6	571 / 255	513 / 256
		$2^6 - 2^{13} + 2^{19} + 2^{22} - 2^{27} + 2^{29}$	6	571 / 255	514 / 256
		$2^{10} + 2^{12} - 2^{18} - 2^{23} + 2^{27} - 2^{29}$	6	571 / 255	514 / 256
		$2^1 + 2^5 + 2^{15} + 2^{26} - 2^{29}$	5	575 / 256	517 / 258
	$x \equiv 11, ..., 1235 \bmod 1260$ $T_1,\ b_9,\ D$	$-1 + 2^7 + 2^{14} + 2^{23} - 2^{27}$	5	537 / 248	483 / 241
		$-1 - 2^9 - 2^{14} + 2^{16} + 2^{27}$	5	539 / 249	485 / 242
		$2^1 + 2^5 + 2^{15} - 2^{25} + 2^{28}$	5	555 / 252	499 / 249
		$2^4 + 2^7 + 2^{22} + 2^{25} - 2^{28}$	5	555 / 252	499 / 249
		$-2^1 + 2^5 - 2^{21} + 2^{23} - 2^{28}$	5	558 / 253	502 / 250
		$-2^2 + 2^5 + 2^{15} - 2^{28}$	4	559 / 253	503 / 251
		$2^3 - 2^{11} + 2^{17} + 2^{23} + 2^{28}$	5	560 / 253	504 / 251
		$1 - 2^{10} + 2^{13} + 2^{20} + 2^{26} + 2^{28}$	6	565 / 254	509 / 254
		$1 + 2^9 - 2^{13} - 2^{15} + 2^{27} - 2^{29}$	6	571 / 255	513 / 256
		$1 + 2^2 - 2^{10} + 2^{18} + 2^{27} - 2^{29}$	6	571 / 255	513 / 256
	$x \equiv 23 \bmod 36$ $T_1,\ b_3,\ M$	$-1 + 2^8 + 2^{13} - 2^{15} + 2^{27}$	5	539 / 249	485 / 242
		$-1 - 2^8 - 2^{20} - 2^{24} + 2^{26} - 2^{28}$	6	553 / 252	498 / 248
		$-1 - 2^7 - 2^{17} - 2^{21} + 2^{24} - 2^{28}$	6	557 / 252	501 / 250
		$-1 + 2^2 + 2^5 + 2^{10} + 2^{12} + 2^{28}$	6	559 / 253	503 / 251
		$-1 + 2^2 - 2^{21} - 2^{24} + 2^{26} + 2^{28}$	6	564 / 254	507 / 253
		$-1 - 2^6 + 2^{14} - 2^{20} - 2^{26} - 2^{28}$	6	565 / 254	509 / 254
		$-1 - 2^{11} - 2^{17} - 2^{21} - 2^{27} + 2^{29}$	6	570 / 255	513 / 256
	$x \equiv 110, ..., 1244(1260)$ $T_1,\ b_7,\ D$	$-1 - 2^2 - 2^6 + 2^{27}$	4	539 / 249	485 / 242
		$-2^3 - 2^7 + 2^{19} - 2^{27}$	4	539 / 249	485 / 242
		$1 - 2^{11} - 2^{18} + 2^{20} - 2^{26} + 2^{28}$	6	551 / 251	496 / 247
		$1 - 2^{13} + 2^{15} - 2^{21} + 2^{24} - 2^{28}$	6	557 / 252	501 / 250
		$1 - 2^9 - 2^{12} + 2^{14} + 2^{20} - 2^{28}$	6	559 / 253	503 / 251
	$x \equiv 2, ..., 1136 \bmod 1260$ $T_1,\ b_{-7},\ D$	$2^1 + 2^8 - 2^{14} + 2^{22} - 2^{28}$	5	558 / 253	503 / 251
		$1 - 2^4 - 2^6 + 2^{25} + 2^{28}$	5	562 / 253	506 / 252

TABLE 21. Low weight curves offering 256-bit security.

288-bit secure curves					
	subfamily/details	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
BLS $k = 27$ (see §7)	$x \equiv 5, 14, 32 \bmod 36$ $T_1,\ b_{-3},\ M$	$1 - 2^4 - 2^9 + 2^{36}$	4	719 / 281	647 / 323
		$1 + 2^{20} + 2^{26} - 2^{30} - 2^{35} + 2^{37}$	6	730 / 283	657 / 328
		$1 + 2^8 + 2^{12} + 2^{19} - 2^{35} + 2^{37}$	6	731 / 283	657 / 328
		$1 - 2^2 + 2^{16} + 2^{32} - 2^{35} + 2^{37}$	6	732 / 284	659 / 329
		$1 + 2^2 - 2^{11} + 2^{33} - 2^{35} + 2^{37}$	6	733 / 284	660 / 329
		$1 - 2^{10} - 2^{18} - 2^{24} - 2^{34} + 2^{37}$	6	735 / 284	661 / 330
		$1 + 2^{17} + 2^{20} + 2^{24} - 2^{33} + 2^{37}$	6	737 / 284	663 / 331
		$1 + 2^{11} + 2^{15} + 2^{17} + 2^{31} + 2^{37}$	6*	739 / 285	665 / 332
		$2^{10} + 2^{12} - 2^{17} + 2^{37}$	4	739 / 285	665 / 332
		$1 + 2^7 - 2^9 + 2^{15} + 2^{37}$	5	739 / 285	665 / 332
		$2^7 + 2^{24} - 2^{29} - 2^{37}$	4	739 / 285	665 / 332
		$1 + 2^2 + 2^{18} - 2^{22} + 2^{32} + 2^{37}$	6	740 / 285	666 / 332
		$1 + 2^{10} + 2^{17} + 2^{21} - 2^{35} - 2^{37}$	6	745 / 286	671 / 335
		$-2^9 + 2^{24} - 2^{36} + 2^{38}$	4	751 / 287	675 / 337
		$1 - 2^{12} - 2^{20} - 2^{32} + 2^{38}$	5	758 / 288	683 / 341
		$1 + 2^8 - 2^{25} - 2^{31} + 2^{38}$	5	759 / 288	683 / 341
		$2^{26} - 2^{35} - 2^{37} + 2^{39}$	4	768 / 289	691 / 345
	$x \equiv 11, \ldots, 1235 \bmod 1260$ $T_1,\ b_9,\ D$	$-1 + 2^5 + 2^7 - 2^{26} - 2^{31} + 2^{37}$	6	738 / 285	664 / 331
		$1 + 2^8 - 2^{12} + 2^{17} + 2^{37}$	5	739 / 285	665 / 332
		$-2^1 - 2^{14} - 2^{20} + 2^{24} + 2^{37}$	5	739 / 285	665 / 332
		$2^5 - 2^{17} - 2^{21} - 2^{24} + 2^{37}$	5	739 / 285	665 / 332
		$2^5 - 2^9 + 2^{25} - 2^{27} + 2^{37}$	5	739 / 285	665 / 332
		$1 + 2^3 + 2^{15} + 2^{19} + 2^{27} + 2^{37}$	6*	739 / 285	665 / 332
		$2^6 + 2^{11} + 2^{27} - 2^{29} + 2^{37}$	5	739 / 285	665 / 332
		$2^1 + 2^5 - 2^{15} + 2^{29} - 2^{37}$	5	739 / 285	665 / 332
		$-1 + 2^{16} - 2^{26} - 2^{34} - 2^{37}$	5	742 / 285	668 / 333
		$2^8 + 2^{24} - 2^{33} - 2^{38}$	4	760 / 288	684 / 341
	$x \equiv 23 \bmod 36$ $T_1,\ b_3,\ M$	$-1 + 2^{13} + 2^{23} + 2^{28} + 2^{36}$	5	719 / 281	647 / 323
		$-1 - 2^{25} - 2^{29} - 2^{31} - 2^{35} + 2^{37}$	6	730 / 283	657 / 328
		$-1 + 2^7 - 2^{16} + 2^{22} - 2^{34} + 2^{37}$	6	735 / 284	661 / 330
		$-1 - 2^{10} - 2^{22} - 2^{29} - 2^{37}$	5*	739 / 285	665 / 332
		$-1 + 2^7 - 2^{13} - 2^{30} - 2^{37}$	5	739 / 285	665 / 332
		$-1 + 2^{15} + 2^{29} - 2^{31} + 2^{38}$	5	759 / 288	683 / 341
		$-1 - 2^2 - 2^8 - 2^{21} - 2^{30} - 2^{38}$	6*	759 / 288	683 / 341
		$-1 + 2^{15} + 2^{29} - 2^{31} + 2^{38}$	5	759 / 288	683 / 341
		$-1 - 2^8 - 2^{11} - 2^{22} + 2^{38}$	5	759 / 288	683 / 341
	$x \equiv 110, \ldots, 1244 \bmod 1260$ $T_1,\ b_7,\ D$	$-2^6 - 2^{20} - 2^{27} - 2^{30} - 2^{37}$	5*	739 / 285	665 / 332
		$-2^2 - 2^{20} - 2^{26} - 2^{31} - 2^{37}$	5*	739 / 285	665 / 332
		$-1 + 2^2 - 2^6 - 2^{26} + 2^{38}$	5*	759 / 288	683 / 341
	$x \equiv 38, \ldots, 1253 \bmod 1260$ $T_1,\ b_{-5},\ D$	$2^7 + 2^{13} - 2^{37}$	3	739 / 285	665 / 332
		$1 - 2^4 - 2^8 - 2^{27} + 2^{37}$	5	739 / 285	665 / 332
		$2^7 + 2^9 + 2^{22} - 2^{26} - 2^{37}$	5	739 / 285	665 / 332
		$-2^1 + 2^8 + 2^{11} - 2^{28} + 2^{37}$	5	739 / 285	665 / 332
		$2^8 + 2^{15} - 2^{18} + 2^{28} + 2^{37}$	5	739 / 285	665 / 332
		$1 + 2^{16} + 2^{33} + 2^{38}$	4*	760 / 288	684 / 341
KSS $k = 32$ (see §8)	$x' \equiv 453, 981 \bmod 3824$ $T_1,\ a_1,\ D$	$1 + 2^{14} + 2^{17} + 2^{21} + 2^{30} - 2^{32} + 2^{37} - 2^{39}$	8	674 / 294	572 / 285
		$1 - 2^5 + 2^{10} + 2^{12} - 2^{18} - 2^{37} + 2^{39}$	7	674 / 294	571 / 285
		$1 + 2^6 - 2^{14} - 2^{21} - 2^{30} + 2^{32} + 2^{35} - 2^{39}$	8	679 / 295	576 / 287
		$1 - 2^7 - 2^9 + 2^{21} + 2^{26} - 2^{28} - 2^{30} + 2^{39}$	8	681 / 296	578 / 288
		$1 + 2^9 - 2^{11} + 2^{14} + 2^{19} - 2^{21} - 2^{24} - 2^{39}$	8	681 / 296	578 / 288
		$1 + 2^7 - 2^9 - 2^{14} - 2^{17} - 2^{20} - 2^{29} - 2^{39}$	8	681 / 296	578 / 288
		$1 - 2^7 - 2^9 + 2^{21} + 2^{26} - 2^{28} - 2^{30} + 2^{39}$	8	681 / 296	578 / 288
		$1 - 2^7 - 2^{12} + 2^{17} + 2^{22} - 2^{28} - 2^{35} - 2^{39}$	8	683 / 296	580 / 289
		$1 - 2^{23} - 2^{32} + 2^{35} + 2^{39}$	5	682 / 296	579 / 289
	$x' \equiv 2365, 2893 \bmod 3824$ $T_1,\ a_1,\ M$	$1 - 2^3 - 2^7 + 2^{25} - 2^{36} + 2^{38}$	6	656 / 291	555 / 277
		$1 - 2^3 + 2^7 - 2^{12} - 2^{28} - 2^{31} - 2^{35} - 2^{39}$	8	683 / 296	580 / 289

TABLE 22. Low weight curves offering 288-bit security.

320-bit secure curves					
	subfamily/details	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
KSS $k = 32$ (see §8)	$x' \equiv 453, 981 \bmod 3824$ $T_1,\ a_1,\ D$	$1 - 2^9 - 2^{13} - 2^{28} + 2^{31} + 2^{40} - 2^{45}$	7	788 / 314	673 / 336
		$1 - 2^7 - 2^{10} - 2^{19} + 2^{35} + 2^{40} - 2^{45}$	7	788 / 314	673 / 336
		$1 + 2^9 + 2^{12} - 2^{15} + 2^{21} - 2^{23} - 2^{25} + 2^{45}$	8	789 / 315	674 / 336
		$1 + 2^4 + 2^6 - 2^{18} + 2^{26} - 2^{28} - 2^{34} + 2^{45}$	8	789 / 315	674 / 336
		$1 - 2^6 + 2^{14} - 2^{20} - 2^{22} + 2^{34} - 2^{46}$	7	807 / 318	690 / 344
		$1 + 2^5 + 2^{17} - 2^{25} + 2^{29} - 2^{36} + 2^{46}$	7	807 / 318	690 / 344
		$1 + 2^6 + 2^8 - 2^{13} - 2^{18} - 2^{36} - 2^{47}$	7	825 / 320	706 / 352
		$1 - 2^8 - 2^{18} + 2^{24} + 2^{37} - 2^{46} + 2^{48}$	7	836 / 322	715 / 357
KSS $k = 36$ (see §9)	$x' \equiv 1376, 1880 \bmod 2664$ $T_1,\ b_2,\ D$	$-2^3 - 2^{17} - 2^{28} - 2^{52} + 2^{55}$	5	753 / 324	631 / 315
		$2^3 + 2^{14} - 2^{23} + 2^{34} - 2^{36} - 2^{55}$	6	756 / 325	633 / 316
		$2^5 + 2^9 + 2^{26} - 2^{31} + 2^{40} - 2^{55}$	6	756 / 325	633 / 316
		$-2^9 + 2^{25} - 2^{27} + 2^{38} + 2^{42} + 2^{55}$	6	756 / 325	633 / 316
		$-2^3 + 2^{12} + 2^{14} - 2^{33} + 2^{43} + 2^{55}$	6	756 / 325	633 / 316
		$-2^3 - 2^8 - 2^{29} - 2^{34} - 2^{45} - 2^{55}$	6^*	756 / 325	633 / 316
		$-2^8 - 2^{21} - 2^{31} + 2^{42} + 2^{45} - 2^{55}$	6	756 / 325	633 / 316
		$-2^7 - 2^{19} - 2^{32} + 2^{44} - 2^{48} - 2^{55}$	6	756 / 325	633 / 316
	$x' \equiv 104, ..., 7592 \bmod 7992$ $T_1,\ b_{-4},\ M$	$-2^3 + 2^{12} - 2^{15} + 2^{24} - 2^{34} + 2^{55}$	6	756 / 325	633 / 316
		$-2^5 + 2^8 - 2^{11} + 2^{35} + 2^{37} - 2^{55}$	6	756 / 325	633 / 316
		$-2^7 - 2^{25} + 2^{31} - 2^{34} - 2^{39} - 2^{55}$	6	756 / 325	633 / 316
		$-2^{11} + 2^{21} + 2^{36} + 2^{42} - 2^{44} - 2^{55}$	6	756 / 325	633 / 316
		$2^3 + 2^7 - 2^{24} - 2^{33} + 2^{47} + 2^{55}$	6	756 / 325	633 / 316
	$x' \equiv 2768, 4928 \bmod 7992$ $T_1,\ b_3,\ M$	$2^{10} - 2^{17} + 2^{19} - 2^{21} - 2^{51} + 2^{55}$	6	754 / 324	632 / 315
		$2^4 + 2^7 + 2^{32} - 2^{48} + 2^{52} - 2^{55}$	6	753 / 324	631 / 315
		$-2^{30} - 2^{33} - 2^{40} - 2^{48} - 2^{50} + 2^{55}$	6	755 / 324	633 / 316
		$2^{12} + 2^{32} + 2^{41} - 2^{45} + 2^{50} + 2^{55}$	6	756 / 325	634 / 316
		$-2^6 - 2^{19} - 2^{44} + 2^{47} + 2^{51} + 2^{55}$	6	757 / 325	634 / 316
		$2^3 + 2^{15} + 2^{17} + 2^{24} - 2^{29} + 2^{40} + 2^{55}$	7	756 / 325	633 / 316
		$-2^5 + 2^{11} - 2^{24} - 2^{30} + 2^{39} - 2^{41} - 2^{55}$	7	756 / 325	633 / 316
		$-2^5 - 2^{16} + 2^{18} - 2^{21} - 2^{31} - 2^{41} - 2^{55}$	7	756 / 325	633 / 316
		$-2^{15} + 2^{22} + 2^{27} - 2^{31} - 2^{33} - 2^{41} - 2^{55}$	7	756 / 325	633 / 316
		$2^{11} + 2^{16} + 2^{23} + 2^{34} - 2^{37} + 2^{56}$	6	770 / 327	645 / 322
		$2^6 + 2^{10} + 2^{31} + 2^{34} + 2^{50} - 2^{56}$	6	769 / 327	645 / 322
		$-2^{27} - 2^{34} + 2^{39} - 2^{44} - 2^{50} - 2^{56}$	6	770 / 327	646 / 322
		$2^3 - 2^6 - 2^{34} + 2^{39} + 2^{53} + 2^{56}$	6	772 / 327	647 / 323

TABLE 23. Low weight curves offering 320-bit security.

352-bit secure curves					
	subfamily/details	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
KSS $k=36$ (see §9)	$x' \equiv 2768, 4928 \bmod 7992$ $T_1,\ b_3,\ M$	$-2^{12} - 2^{32} + 2^{34} - 2^{45} + 2^{65}$	5	896 / 348	753 / 376
	$x' \equiv 1376, 1880 \bmod 2664$ $T_1,\ b_2,\ D$	$-2^5 - 2^{16} - 2^{18} + 2^{27} + 2^{31} + 2^{65}$	6	896 / 348	753 / 376
		$-2^{10} + 2^{23} + 2^{42} + 2^{57} - 2^{65}$	5	896 / 348	753 / 376
		$-2^{26} + 2^{41} - 2^{45} + 2^{62} + 2^{65}$	5	898 / 349	755 / 377
		$2^{21} - 2^{31} + 2^{49} - 2^{58} + 2^{66}$	5	910 / 351	765 / 382
	$x' \equiv 104, ..., 7592 \bmod 7992$ $T_1,\ b_{-4},\ M$	$-2^5 - 2^{16} - 2^{46} + 2^{50} + 2^{65}$	5	896 / 348	753 / 376
		$2^{10} + 2^{16} - 2^{23} - 2^{30} + 2^{32} + 2^{65}$	6	896 / 348	753 / 376
	$x' \equiv 821, 1325 \bmod 2664$ $T_1,\ b_{-1},\ M$	$-1 + 2^2 + 2^{33} + 2^{37} + 2^{43} - 2^{55} + 2^{66}$	7	910 / 351	765 / 382
		$-1 + 2^2 + 2^7 - 2^9 + 2^{19} + 2^{28} - 2^{66}$	7	910 / 351	765 / 382
		$-1 + 2^2 - 2^{19} - 2^{31} - 2^{49} + 2^{52} + 2^{66}$	7	910 / 351	765 / 382
	$x \equiv 437, 2597 \bmod 2664$ $T_1,\ b_{-1},\ D$	$-1 + 2^2 + 2^5 - 2^{21} + 2^{45} + 2^{54} - 2^{66}$	7	910 / 351	765 / 382
		$-1 - 2^2 + 2^6 + 2^{18} - 2^{22} - 2^{33} - 2^{66}$	7	910 / 351	765 / 382
BLS $k=48$ (see §10)	$x \equiv 16, 88 \bmod 216$ $T_1,\ b_4,\ M$	$-2^{11} - 2^{21} + 2^{43}$	3	773 / 369	688 / 343
		$-2^{30} - 2^{36} - 2^{38} + 2^{44}$	4	790 / 373	704 / 351
		$2^3 - 2^{11} - 2^{21} - 2^{24} + 2^{44}$	5	791 / 373	704 / 351
		$2^9 + 2^{26} - 2^{42} - 2^{44}$	4	797 / 374	710 / 354
	$x \equiv 64 \bmod 72$ $T_1,\ b_{-2},\ D$	$-2^3 + 2^8 - 2^{13} + 2^{19} - 2^{44}$	5	791 / 373	704 / 351
		$-2^7 + 2^{10} + 2^{17} + 2^{20} - 2^{44}$	5	791 / 373	704 / 351
		$-2^8 - 2^{15} - 2^{17} + 2^{23} + 2^{44}$	5	791 / 373	705 / 352
		$2^{12} - 2^{14} + 2^{17} + 2^{26} + 2^{44}$	5	791 / 373	705 / 352
	$x \equiv 160 \bmod 216$ $T_1,\ b_{-3},\ M$	$-2^{15} + 2^{29} + 2^{31} - 2^{41} + 2^{44}$	5	787 / 372	701 / 350
		$-2^{20} - 2^{26} - 2^{38} + 2^{41} - 2^{44}$	5	788 / 372	702 / 350
		$2^{11} + 2^{18} + 2^{27} - 2^{31} + 2^{44}$	5	791 / 373	704 / 351
		$-2^4 - 2^{18} - 2^{21} + 2^{24} + 2^{44}$	5	791 / 373	705 / 352
		$-2^8 + 2^{13} - 2^{25} + 2^{34} + 2^{44}$	5	791 / 373	705 / 352
		$-2^8 + 2^{15} + 2^{30} + 2^{40} + 2^{44}$	5	792 / 373	706 / 352
		$-2^7 + 2^{25} - 2^{29} + 2^{43} - 2^{45}$	5	801 / 375	714 / 356
	$x \equiv 7 \bmod 72$ $T_1,\ b_1,\ D$	$-1 + 2^3 + 2^{33} + 2^{41} - 2^{44}$	5	787 / 372	701 / 350
		$-1 + 2^6 - 2^{23} + 2^{28} - 2^{44}$	5	791 / 373	704 / 351
		$-1 - 2^6 - 2^{11} - 2^{25} - 2^{28} - 2^{44}$	6*	791 / 373	705 / 352
		$-1 + 2^{18} - 2^{25} + 2^{29} + 2^{44}$	5	791 / 373	705 / 352
		$-1 - 2^{30} - 2^{37} + 2^{40} + 2^{44}$	5	792 / 373	706 / 352
		$-1 + 2^{18} - 2^{25} + 2^{29} + 2^{44}$	5	791 / 373	705 / 352
		$-1 - 2^{14} - 2^{17} - 2^{26} - 2^{31} - 2^{44}$	6*	791 / 373	705 / 352
	$x \equiv 31 \bmod 72$ $T_1,\ b_1, M$	$-1 + 2^4 - 2^{15} - 2^{19} - 2^{23} + 2^{44}$	6	791 / 373	704 / 351
		$-1 - 2^7 - 2^{10} - 2^{13} - 2^{16} - 2^{44}$	6*	791 / 373	705 / 352
		$-1 - 2^{13} + 2^{18} - 2^{27} - 2^{44}$	5	791 / 373	705 / 352
		$-1 + 2^{17} - 2^{19} + 2^{40} + 2^{44}$	5	792 / 373	706 / 352

TABLE 24. Low weight curves offering 352-bit security.

384-bit secure curves					
	subfamily/details	x_0	weight	$\mathbb{F}_q$ (bits) / $\mathbb{F}_{q^k}$ sec.	r (bits) / $E[r]$ sec.
BLS $k=48$ (see §10)	$x \equiv 64 \bmod 72$ $T_1,\ b_{-2},\ D$	$2^7 + 2^{17} + 2^{32} - 2^{48}$	4	863 / 387	768 / 383
		$-2^{17} + 2^{30} - 2^{35} + 2^{48}$	4	863 / 387	768 / 383
		$-2^6 - 2^{22} + 2^{36} - 2^{48}$	4	863 / 387	768 / 383
		$-2^4 + 2^{11} - 2^{16} + 2^{19} - 2^{48}$	5	863 / 387	768 / 383
		$2^7 + 2^{35} + 2^{47} - 2^{49}$	4	873 / 388	778 / 388
	$x \equiv 160 \bmod 216$ $T_1,\ b_{-3},\ M$	$2^7 - 2^{10} + 2^{16} - 2^{29} + 2^{48}$	5	863 / 387	768 / 383
		$2^6 + 2^{34} + 2^{40} + 2^{48}$	4*	863 / 387	769 / 384
	$x \equiv 7 \bmod 72$ $T_1,\ b_1,\ D$	$-1 + 2^4 - 2^{16} - 2^{31} + 2^{48}$	5	863 / 387	768 / 383
		$-1 + 2^{16} + 2^{18} + 2^{30} - 2^{48}$	5	863 / 387	768 / 383
		$-1 + 2^{12} + 2^{17} - 2^{20} + 2^{22} - 2^{48}$	6	863 / 387	768 / 383
		$-1 + 2^6 - 2^{13} + 2^{20} - 2^{23} + 2^{48}$	6	863 / 387	768 / 383
		$-1 - 2^{13} + 2^{15} + 2^{18} + 2^{48}$	5	863 / 387	769 / 384
		$-1 + 2^8 - 2^{15} + 2^{17} - 2^{24} - 2^{48}$	6	863 / 387	769 / 384
		$-1 - 2^{10} - 2^{13} + 2^{23} - 2^{29} - 2^{48}$	6	863 / 387	769 / 384
	$x \equiv 16, 88 \bmod 216$ $T_1,\ b_4,\ M$	$2^3 + 2^{14} + 2^{17} - 2^{19} + 2^{48}$	5	863 / 387	768 / 383
		$2^3 - 2^9 - 2^{19} + 2^{30} - 2^{48}$	5	863 / 387	768 / 383
		$-2^4 - 2^{16} + 2^{20} - 2^{25} + 2^{48}$	5	863 / 387	768 / 383
		$2^7 - 2^{12} - 2^{17} - 2^{27} + 2^{48}$	5	863 / 387	768 / 383
		$2^5 + 2^{18} - 2^{27} + 2^{36} - 2^{48}$	5	863 / 387	768 / 383
		$-2^5 - 2^{11} + 2^{25} + 2^{29} + 2^{48}$	5	863 / 387	769 / 384
		$2^5 - 2^8 + 2^{15} - 2^{36} - 2^{48}$	5	863 / 387	769 / 384
	$x \equiv 31 \bmod 72$ $T_1,\ b_1,\ M$	$-1 + 2^4 - 2^8 - 2^{27} + 2^{48}$	5	863 / 387	768 / 383
		$-1 + 2^{13} + 2^{23} + 2^{28} - 2^{30} + 2^{48}$	6	863 / 387	768 / 383
		$-1 - 2^{10} - 2^{21} + 2^{25} + 2^{30} - 2^{48}$	6	863 / 387	768 / 383
		$-1 + 2^9 - 2^{22} + 2^{25} + 2^{30} + 2^{48}$	6	863 / 387	769 / 384
		$-1 + 2^7 + 2^{17} + 2^{19} + 2^{26} + 2^{48}$	6	863 / 387	769 / 384

TABLE 25. Low weight curves offering 384-bit security.