An Algebraic Point of View on the Generation of Pairing-Friendly Curves

Jean Gasnier, Aurore Guillevic

AN ALGEBRAIC POINT OF VIEW ON THE GENERATION OF PAIRING-FRIENDLY CURVES

JEAN GASNIER AND AURORE GUILLEVIC

Abstract. In 2010, Freeman, Scott, and Teske published a well-known taxonomy compiling the best known families of pairing-friendly elliptic curves. Since then, the research effort mostly shifted from the generation of pairing-friendly curves to the improvement of algorithms or the assessment of security parameters to resist the latest attacks on the discrete logarithm problem. Consequently, very few new families were discovered. However, the need of pairing-friendly curves of prime order in some new applications such as SNARKs has reignited the interest in the generation of pairing-friendly curves, with hope of finding families similar to the one discovered by Barreto and Naehrig.

Building on the work of Kachisa, Schaefer, and Scott, we show that some elements of extensions of a cyclotomic field have a higher probability of generating a family of pairing-friendly curves. We present a general framework which embraces the KSS families and many of the other families in the taxonomy paper, and provide an open-source SageMath implementation of our technique. We finally introduce a new family with embedding degree $k = 20$ which we estimate to provide a faster Miller loop compared to KSS16 and KSS18 at the 192-bit security level.

Keywords: Elliptic Curves, Pairing-based Cryptography

1. Introduction

1.1. Pairing-friendly curves in cryptography.

Pairing-friendly curves are a key-ingredient in public-key cryptography. They allow identity-based encryption [10], short signatures [11] and more flexible key-exchange protocols [34]. A pairing is an efficient bilinear map $e_r\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. The input groups $\mathbb{G}_1$, $\mathbb{G}_2$ of points on the curve E have prime order r, and $\mathbb{G}_T$, the target group of same order r, embeds in an extension field $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. Usually in cryptography, $\mathbb{G}_1$ is defined over $\mathbb{F}_q$. The pairing efficiency is determined by the size of q, the size of q^k, and the availability of improvements in specific cases [16].

A pairing-based cryptosystem like the tri-partite Diffie–Hellman key exchange [34] relies on the bilinearity of the pairing: $e_r([a]P, [b]Q) = e_r([b]P, [a]Q) = e_r(P, Q)^{ab}$ that is, the pairing allows to multiply (in the exponents) two hidden secret scalars without knowing them. This property is a major key-ingredient for zero-knowledge proof systems, the latest trend being about SNARKs (Succinct Non-Interactive ARgument of Knowledge) where a quadratic equation shall be verified [27]. Cryptographic elliptic curves such as the ones standardised by NIST, and the Edwards curve 25519, do not allow an efficient pairing computation. Pairing-friendly curves shall be designed on purpose, with two criteria in mind: security and efficiency.

For cryptographic applications, $\mathbb{G}_1$ and $\mathbb{G}_2$ should offer a standard security level against a discrete logarithm computation. This problem is well-known for plain

Date: September 13, 2023.

elliptic curves and standard recommendations consist in taking a prime order r of $2n$ bits for a security level of n bits, that is, usually r is 256, resp. 384-bit long to ensure a 128-bit, resp. 192-bit security level. However there is no standard choice of size of finite field $\mathbb{F}_{q^k}$ yet, as the security in a finite field extension is much more difficult to analyse due to the many variants of the Number Field Sieve algorithm. In 2016, Kim and Barbulescu [37] published their Extended Tower NFS algorithm (exTNFS or TNFS for short), and they achieve the best *asymptotic* complexity in some particular instances of finite fields. In particular, exTNFS is expected to be very efficient in fields such as $\mathbb{F}_{p^{12}}$, where the extension degree has many small divisors. The heuristic complexity of TNFS follows a sub-exponential equation

$$L_Q(\alpha, c) = \exp\Big(\big(c + o(1)\big)(\ln Q)^{\alpha}(\ln\ln Q)^{1-\alpha}\Big)$$

where $Q = q^k$, $\alpha = 1/3$, and c varies from $(32/9)^{1/3} = 1.526$ to $(64/9)^{1/3} = 1.923$. This complexity is very different from the DL computation on the curve, in $O(\sqrt{r})$. The finite field extension degree k allows to adjust the DL-security in $\mathbb{F}_{q^k}$ to the security on $E(\mathbb{F}_q)$ so as to have parameters of minimal size. Before 2016 and Kim and Barbulescu's TNFS algorithm, the best known pairing-friendly curve family was given by Barreto and Naehrig (BN) [7]: a *prime-order* curve of about 256 bits, where the pairing transfers the DL problem into $\mathbb{F}_{q^{12}}$ of about 3072 bits. The security in the three groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ was believed to reach 128 bits. Nowadays these BN curves of 254 to 256 bits have about 103 bits of security in $\mathbb{F}_{q^{12}}$ [3].

Most of the known pairing-friendly curves are not of prime order: BN curves are an exception. $\mathbb{G}_1$ has prime order r of $\log_2 r$ bits but its elements are defined over a field $\mathbb{F}_q$ of $\log_2 q$ bits. The parameter ρ measures the loss for $\mathbb{G}_1$ elements compared to an optimal key-size:

$$\rho = \frac{\log q}{\log r}\ . \tag{1.1}$$

The successor curves of BN curves in cryptography are Barreto–Lynn–Scott curves (BLS) [6], where $\rho = 1.5$ and $k = 12$. One of the most widespread parameter set is BLS12-381, where r is 254-bit long, q is 381-bit long, and $k = 12$. Non-prime-order curves showed to have a very efficient pairing computation, and were investigated as replacements [29].

However with the development of *cycles* of pairing-friendly elliptic curves [9], prime-order pairing-friendly curves are again needed. There are only three known families of such curves: Miyaji–Nakabayashi–Takano (MNT) curves [41], BN curves [7] and Freeman curves [21]. Moreover, generalising their ideas gave new curves but none of prime order [24, 44]. At the moment, only the MNT curves allow the construction of cycles of pairing-friendly curves, but their instantiation is not efficient. It is an open problem [14, 8] to find cycles of prime-order pairing-friendly curves at cryptographic security levels, with efficient group operations. To this aim, finding new prime-order pairing-friendly curves is a prerequisite.

1.2. **Previous work on finding families of pairing-friendly curves.** Pairing-friendly curves are very rare and are obtained by dedicated methods. This paper focuses on *ordinary* curves defined over prime fields. The first solution was given by Miyaji, Nakabayashi and Takano [40]. They obtain ordinary curves (MNT) of prime order and embedding degree 3, 4 and 6. The curve parameters are given by quadratic polynomials $q(x)$, $r(x)$ and a linear polynomial $t(x)$. Solving a Pell

equation is needed [36] to obtain valid seeds u such that $q(u)$, $r(u)$, $t(u)$ are valid parameters. Then a Hilbert class polynomial is required to get the curve coefficients a, b [45].

Later Barreto, Lynn and Scott [5] focused on curves of embedding degree multiple of 3 and j-invariant 0. They obtained a much more simple way of generating parameters. Their curves of embedding degrees 12 and 24 (BLS12, BLS24) are now widely deployed at the 128-bit and 192-bit security level respectively. In particular, BLS12-381 is on the way to standardisation (through Hashing to Elliptic Curves IETF draft [19, §8.8]). This *cyclotomic polynomial* technique was explored by Brezing and Weng in [12]. The taxonomy paper of Freeman, Scott and Teske [22] generalises the BLS technique to all curves with $j(E) = 0$ and any k except $k = 0 \bmod 18$, and to all curves with $j(E) = 1728$ and any k except $k = 0 \bmod 8$. These techniques fail at certain embedding degrees: when $k = 0 \bmod 18$ with $j(E) = 0$ (BLS), when $k = 0 \bmod 8$ with $j(E) = 1728$ (BW). The BLS issue was fixed at $k = 0 \bmod 18$ with the Aurifeuillean factorisation of cyclotomic polynomials [44]. In 2008, Kachisa, Schaefer and Scott [35] published another method that obtains a factorisation of cyclotomic polynomials evaluated at sparse polynomials of degree at least 3. This new technique provides pairing-friendly curves of embedding degrees $8, 16, 18, 32, 36, 40$, filling some of the gaps at $k = 0 \bmod 8$ and $k = 0 \bmod 18$.

1.3. **Contributions.** In this paper, we revisit the KSS construction and expose a generalisation. Like in previous works [24, 44], we obtained new interesting families of pairing-friendly curves, but did not get any of prime order. Our contribution is twofold: first we narrow the exhaustive and time-consuming search of KSS, so that we obtain new KSS-like curves at new embedding degrees in a few seconds on a laptop. Second, we generalise the technique and explore other discriminants and settings. Our outcome on the constructive side is to provide new interesting pairing-friendly curves at the 192-bit security level. On the other side, we show that there is no pairing-friendly curve of prime order obtained with our generalised KSS technique. This article comes with with a SageMath open-source companion code available online [25] [30].

1.4. **Organisation of the paper.** The notation and definitions are introduced in section 2, and well-known constructions are recalled. The notions of a pairing-friendly curve and a family of pairing-friendly curves are defined at first, after which the work of Brezing and Weng [12] and Kachisa, Schaefer and Scott [35] are recalled. Our new construction method is presented at the beginning of section 3. Then follows theoretical results and more practical results, as well as some algorithmic ideas on the processing of potential families. Finally in section 4, two of the new families are examined. We show that the families contain curves which can be used at the 192-bit security level, and give an estimation of the cost of computing the pairing application on these curves.

2. Preliminaries

2.1. **Notation and pairing-friendly curves.** We start by recalling some facts on elliptic curves. We will use the same notation as in the taxonomy article of Freeman, Scott and Teske [22]. Let $\mathbb{F}_q$ be the finite field of size q and characteristic $p \neq 2, 3$, we denote $\overline{\mathbb{F}_q}$ its algebraic closure. We call $E : y^2 = x^3 + Ax + B$ an elliptic curve over $\mathbb{F}_q$ under short Weierstrass form, where $A, B \in \mathbb{F}_q$ are such that

$4A^3 + 27B^2 \neq 0$. We use the notation $E/\mathbb{F}_q$ to denote such a curve. We denote $E(\mathbb{F}_q)$ the subgroup of $\mathbb{F}_q$-rational points of E and $\#E(\mathbb{F}_q)$ its order. For any integer r, we denote $E[r]$ the subgroup of r-torsion points of E (defined over $\overline{\mathbb{F}_q}$) and $E(\mathbb{F}_q)[r]$ the subgroup of $\mathbb{F}_q$-rational points of $E[r]$. We define the trace t of E as $t = q + 1 - \#E(\mathbb{F}_q)$. The Hasse–Weil bound says that $|t| \leq 2\sqrt{q}$. We say that E is ordinary if $\gcd(t, q) = 1$ otherwise E is supersingular. Let $\mathrm{End}(E)$ be the set of $\overline{\mathbb{F}_q}$-endomorphisms of E, then $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, and we say that E has complex multiplication, or that E is a CM curve. Furthermore, $\mathrm{End}(E)$ is either an order of a quadratic imaginary number field or an order of a quaternion algebra, depending on whether E is ordinary or supersingular (respectively). If $E/\mathbb{F}_q$ is ordinary, we call CM discriminant of E the squarefree part of the non-negative integer $4q - t^2$. Note that it is different from the discriminant of the quadratic imaginary field K containing $\mathrm{End}(E)$: with usual definitions, denoting D the CM discriminant, we have $D = -\mathrm{disc}(K)$ if $D \equiv 3 \bmod 4$ and $D = -\mathrm{disc}(K)/4$ otherwise.

Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field. A pairing on E is a non-degenerate bilinear map defined over a subgroup $\mathbb{G}$ of E with values in $\overline{\mathbb{F}_q}^*$. Let e_r denote a pairing such that $e_r : E[r] \times E[r] \longrightarrow \mathbb{F}_q(\mu_r)^*$. It is well known that one can often use e_r to embed $E(\mathbb{F}_q)[r]$ in $\mathbb{F}_q(\mu_r)^*$. We define k the embedding degree of E with respect to r as the index of the extension $\mathbb{F}_q(\mu_r)$ over $\mathbb{F}_q$. We will omit r when it can be determined from the context. Since solving the discrete logarithm problem inside the group of invertible elements of a field can be done in subexponential time, the existence of such an embedding can be a liability for cryptographic use when k is small [39]. For cryptographic use, we need to ensure that k is large enough, so that the discrete logarithm has the same security level on the curve and in the field $\mathbb{F}_{q^k}$. The minimal embedding degree depends on the security level, and on the ρ-value of the curve $\rho = \log q / \log r$. Because of the new Tower Number Field Sieve algorithm of [4], and Kim's extended variant [37], the sizes recommended in [22, Table 1.1] are no longer up-to-date. There is not a strong consensus on the sizes for the usual security levels yet, though the following parameters tend to become very common [3, 33, 29, 28]:

Curve	Security level (in bits)	Subgroup size r (in bits)	Field size q (in bits)	Extension Field size q^k (in bits)	Embedding degree k	ρ
BN	≈ 100	256	256	3072	12	1
Security level 128						
MNT-4	128	1024	1024	4096	4	1
MNT-6	128	672	672	4032	6	1
CP-6	128	256	672	4032	6	2.625
CP-8	128	256	544	4352	8	2.125
BN	128	384	384	4608	12	1
BLS-12	128	256	384	4608	12	1.5
KSS-16	128	256	330	5280	16	1.29
KSS-18	128	256	348	6264	18	1.36
BLS-24	128	256	320	7680	24	1.25
Prime embedding degrees, for specific needs [32, 15]						
CP-5	128	256	663	3315	5	2.59
CP-7	128	256	512	3584	7	2
BW13-P310	128	267	310	4027	13	1.16
BW19-P286	128	259	286	5427	19	1.10
Security level 192						
BN	192	1024	1024	12288	12	1
BLS-12	192	768	1152	13824	12	1.5
KSS-16	192	608	768	9728	16	1.26
KSS-18	192	481	640	8658	18	1.33
BLS-24	192	409	512	7680	24	1.25
BLS-27	192	384	427	11529	27	1.11

TABLE 1. Bit sizes of curve parameters and corresponding embedding degrees to obtain commonly desired levels of security.

We use the definition from [22] for pairing-friendly curves:

Definition 1. Let $E/\mathbb{F}_q$ be an elliptic curve. We say that E is pairing-friendly if:

- there is a prime $r > \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$,
- the embedding degree of E with respect to r is less than $\log(r)/8$.

It should be mentioned that supersingular curves have a very particular behavior regarding their embedding degree.

Theorem 1 ([39])**.** *Let $E/\mathbb{F}_q$ be a supersingular elliptic curve. Then E is pairing-friendly with embedding degree $k \leq 6$.*

This means that supersingular curves can be interesting for small embedding degrees, but can not be used for higher ones. Since we aim at providing a method to generate pairing-friendly curves with an arbitrary embedding degree k, we will focus on ordinary curves.

2.2. **Criteria to Generate Ordinary Pairing-Friendly Curves.** While supersingular curves are always pairing-friendly, ordinary curves often are not. A result by Balasubramanian and Koblitz [2] shows that the probability of a randomly chosen ordinary curve over $\mathbb{F}_q$ to have an embedding degree bounded by $\log(q)^2$ is extremely small when $r \approx q$, for q a prime integer. Therefore, it is completely hopeless to try to randomly find ordinary pairing-friendly curves, and one has to find specific methods to generate them. A very common way to do so is to generate integers q, t and r representing the cardinal of the base field, the trace of the curve and the (prime) order of the subgroup of the curve that can be embedded, and to

recover the coefficients of the curve using the CM algorithm. This will require that the discriminant D of the curve is sufficiently small to be able to execute the CM algorithm. According to [45], $D \leq 10^{18}$ is manageable. Moreover, we also have to state the conditions on q, t and r required for ensuring the existence of a curve E over F_q with trace t, embedding degree k with respect to r and discriminant D. The following proposition shows that the embedding degree k depends only on r and q:

Proposition 1 ([22]). *The following conditions are equivalent:*

- *E has embedding degree k with respect to r.*
- *k is the smallest integer such that r divides $q^k - 1$.*
- *q has order k in $(\mathbb{Z}/r\mathbb{Z})^*$.*

The following theorem sums up the conditions on q, r and t:

Theorem 2 ([22]). *Fix k a positive integer and $D \leq 10^{18}$ a squarefree positive integer. Let q, r, t be integers such that:*

(1) q is a positive prime power.
(2) r is a positive prime.
(3) t is coprime to q.
(4) r divides $q + 1 - t$.
(5) r divides $q^k - 1$ and r does not divide $q^{k'} - 1$ for every $k' < k$.
(6) $4q - t^2 = Dy^2$ for some integer y (called CM equation).

Then there exists an ordinary elliptic curve $E/\mathbb{F}_q$ with trace t, having a subgroup of rational points of order r, with embedding degree k and discriminant D.

Proof. Conditions 1, 3 and 6 imply that there exists an ordinary elliptic curve E over $\mathbb{F}_q$ with trace t and discriminant D, that can be recovered with the complex multiplication method [18]. Condition 6 shows that $|t| \leq 2\sqrt{q}$.

Conditions 2 and 4 imply that there exists a subgroup of $E(\mathbb{F}_q)$ of prime order r (required for cryptographic applications), and condition 5 implies that the embedding degree of E with respect to r is k. □

Some conditions can be formulated slightly differently. First, if one defines h to be the cofactor of r in $q + 1 - t$, such that $q + 1 - t = hr$, one obtains a new CM equation for condition 6:

$$Dy^2 = 4hr - (t-2)^2 \tag{6'}$$

Then, Freeman, Scott and Teske also modify condition 5 by using the cyclotomic polynomial Φ_k:

Proposition 2 ([22, Prop. 2.4]). *Let k be an integer, and $E/\mathbb{F}_q$ be an elliptic curve such that $\#E(\mathbb{F}_q) = hr$, with r prime. Let t be the trace of E. Assume that $r \nmid k$. Then condition 5 is equivalent to $r \mid \Phi_k(t-1)$.*

Remark 1. The proposition implies as well that if r is not a prime but satisfies the other conditions from Theorem 2, then denoting r' the largest prime divisor of r, the integers q, r' and t describe a pairing-friendly curve with embedding degree k, as $r' \mid r \mid \Phi_k(t-1)$.

In our cryptographic context, r is greater than k, so we replace the condition 5 by the more convenient equation:

$$(r \mid \Phi_k(t-1)) \tag{5'}$$

The conditions from Theorem 2 do not take into account the first condition $r \geq \sqrt{q}$ from Definition 1. This is equivalent to asking that the ρ-value $\log q / \log r$ is less than 2. In general, unless there is a particular reason to do otherwise, the curve with the smallest ρ-value available should always be preferred.

2.3. **Families of pairing-friendly elliptic curves.** Another interesting problem is to generate families of pairing-friendly elliptic curves. Searching for families of curves rather than a single curve is a common idea which has two main purposes: easing the generation of a curve of specified security level, or the generation of multiple curves, and finding curves with a ρ-value significantly smaller than 2 [22, Sections 4-6]. To define families of curves with one-parameter x, we follow [22] and use polynomials Q, R and T in $\mathbb{Q}[X]$ instead of the previous integers q, r and t. When evaluating the polynomials at $x_0 \in \mathbb{Z}$, one hopes that $Q(x_0)$, $R(x_0)$ and $T(x_0)$ satisfy the conditions of Theorem 2. To achieve this, similar conditions on Q, R and T shall be set. With our representation, $Q(x)$ needs to take an infinite number of prime (or prime power) values at integers. We also want $R(x)$ to take prime values up to a small cofactor. However, for now very little is known about prime values of polynomials. There is a conjecture by Buniakowski and Schinzel:

Buniakowski–Schinzel Conjecture. Let f be a polynomial in $\mathbb{Q}[X]$. Then f takes an infinite number of prime values if and only if:

- f is non-constant,
- f has positive leading coefficient,
- f is irreducible,
- $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, (which implies that it happens for an infinite number of $x \in \mathbb{Z}$),
- $\gcd(\{f(x) \mid x, f(x) \in \mathbb{Z}\}) = 1$.

In the following, we will assume that the conjecture is true, and will say that a polynomial f represents primes if it satisfies the conditions of the conjecture. Polynomials taking integer values at integers will be very useful for defining families of curves, so we define:

Definition 2 ([22, Definition 2.6])**.** Let f be a polynomial in $\mathbb{Q}[X]$, we say that f is integer-valued if $f(x) \in \mathbb{Z}$ whenever $x \in \mathbb{Z}$.

We are now ready to define families of curves, inspired by [22, Definition 2.7]:

Definition 3. Let $k > 0$ be an integer and D be a positive squarefree integer, and let Q, R and T be polynomials in $\mathbb{Q}[X]$. We say that Q, R and T parameterize a complete family of elliptic curves with embedding degree k and discriminant D if:

(1) Q represents primes;
(2) R is non-constant, irreducible and has positive leading coefficient;
(3) There exists a polynomial $H \in \mathbb{Q}[X]$ such that $HR = Q + 1 - T$;
(4) R divides $\Phi_k(T-1)$, with Φ_k the k-th cyclotomic polynomial;
(5) There exists a polynomial $Y \in \mathbb{Q}[X]$ such that $DY^2 = 4Q - T^2$;
(6) Q, R, T, Y, H all take an integer value at a common integer.

We may also say that (Q, R, T, Y) or (Q, R, T, Y, H) parameterizes the family. We also define the notion of **potential family**: if the polynomials Q, R, T, Y and H satisfy condition 2 to 5, we say that they form a potential family of pairing-friendly elliptic curves.

We define the ρ-value of a family as $\rho = \deg Q / \deg R$ so that the ρ-values of the curves that the family generates are close to the ρ-value of the family asymptotically.

Remark 2. In [22], a more general notion of a family is defined. In this article, we are only interested in complete families, so we did not recall their definition of a family. In the following, we will use "family" to mean "complete family of pairing-friendly elliptic curves".

Remark 3. Notice that the third condition of Theorem 2 has not been adapted. Indeed, since $\deg Q = 2 \deg T$ and since we asked Q to represent primes so that $Q(x_0)$ can easily be a prime, we will only look for $Q(x_0)$ prime. Then, it is obvious that $Q(x_0)$ and $T(x_0)$ are coprime because of their sizes.

Let Q, R, T, Y and H be as above, and let x_0 be an integer. For $(Q(x_0), R(x_0), T(x_0))$ to define a pairing-friendly elliptic curve, the values need to satisfy the conditions of Theorem 2. In particular, $Y(x_0)$, $T(x_0)$ and $H(x_0)$ need to be integers simultaneously, while $Q(x_0)$ needs to be a prime and $R(x_0)$ needs to be a prime up to a small cofactor. It sometimes happen that there is no such $x_0 \in \mathbb{Z}$, even when every polynomial takes an integer value at —at least— one integer. This precision is all the more important as we are going to introduce new families with polynomials with large denominators, which increases the difficulty of finding a shared seed x_0.

Remark 4. We stress that conditions 1 to 5 give only mild constraints on R and H. If (Q, R, T, Y, H) is a potential family, for every rational $\lambda \in \mathbb{Q}$, another potential family is $(Q, \lambda R, T, Y, \frac{1}{\lambda} H)$. We will exploit this property later in this work.

2.4. **The Brezing–Weng method.** Condition 4 of Definition 3 suggests that the number field defined by the irreducible polynomial R contains the k-th cyclotomic field, which we will denote $\mathcal{C}_k$. The Brezing–Weng method described in [5] and [12] is a method for constructing families of curves using this observation: it relies on finding a polynomial R, and a polynomial T mapping to $\zeta_k + 1$ in $\mathbb{Q}[X]/\langle R \rangle$ where ζ_k is a primitive k-th root of unity in $\mathbb{Q}[X]/\langle R \rangle$. Similarly to what happens with the integers, we have $DY^2 = 4HR - (T-2)^2$, so we know that Y maps to $(T-2)/\sqrt{-D}$ in $\mathbb{Q}[X]/\langle R \rangle$. Algorithm 2.1 exploits these ideas.

Algorithm 2.1: Brezing–Weng method
Input: $k > 0$ and $D > 0$ squarefree.
Output: Polynomials Q, R, T, Y, H generating a family of elliptic curves with discriminant D and embedding degree k.
1 Let $R \in \mathbb{Z}[X]$ be an irreducible polynomial with positive leading coefficient such that $K = \mathbb{Q}[X]/\langle R \rangle$ contains $\sqrt{-D}$ and $\mathcal{C}_k$.
2 Fix a k-th root of unity $\zeta_k \in K$.
3 Let $T \in \mathbb{Q}[X]$ be a polynomial mapping to $\zeta_k + 1$ in K.
4 Let $Y \in \mathbb{Q}[X]$ be a polynomial mapping to $\frac{T-2}{\sqrt{-D}}$ in K.
5 $Q = (T^2 + DY^2)/4 \in \mathbb{Q}[X]$; $H = (Q + 1 - T)/R \in \mathbb{Q}[X]$
6 [Process the potential family] `// see subsection 3.5`

The goal of the last step (step 6) of Algorithm 2.1 is to check if conditions (1) and (6) of Definition 3 can be met. We expand on our processing method adapted to our new potential families in subsection 3.5.

As we can always choose T and Y to have degree strictly less than R, the method generates families with ρ-value strictly less than 2. In general, there is no particular reason why the polynomials T and Y should have degree less than $\deg R - 1$, but for particular choices of R, the ρ-value can decrease significantly. Below, we give examples of such families.

Example 1. From [12] and [22, Construction 6.2].

Let k be odd and $k < 1000$. Let:

- $R = \Phi_{4k}(X)$,
- $T = -X^2 + 1$,
- $Y = X^k(X^2 + 1)$,
- $Q = \frac{1}{4}(X^{2k+4} + 2X^{2k+2} + X^{2k} + X^4 - 2X^2 + 1)$.

Then (Q, R, T, Y) parameterizes a family of pairing-friendly elliptic curves with embedding degree k and discriminant 1. Its ρ-value is $\frac{k+2}{\varphi(k)}$ where φ is Euler's totient function.

The polynomials Q, R, T and $H = (Q + 1 - T)/R$ are even, and Y is odd. Therefore, denoting $R(X) = R'(X^2)$, $Q(X) = Q'(X^2)$, $T(X) = T'(X^2)$ and $Y = XY'(X^2)$, for every $\alpha \in \mathbb{N}$, the substitution $X^2 \mapsto \alpha X^2$ yields:

$$4Q'(\alpha X^2) - T'(\alpha X^2)^2 = \alpha X^2 Y'(\alpha X^2).$$

Therefore, $(Q'(\alpha X^2), R'(\alpha X^2), T'(\alpha X^2), XY'(\alpha X^2))$ is a potential family of elliptic curves with degree k, discriminant α, and ρ-value $\frac{k+2}{\varphi(k)}$ as well. This method is used to modify the discriminant of the family to avoid attacks targeting specific discriminants.

We give an example of a similar family achieving a better ρ-value for $k \equiv 3 \bmod 4$.

Example 2 (From [22, Constructions 6.20]). Let $k \equiv 3 \bmod 4$ and $k < 1000$. Let:

- $R = \Phi_{4k}(X)$,
- $T = X^{k+1} + 1$,
- $Y = X^k + X$,
- $Q = \frac{1}{4}(X^{2k+2} + X^{2k} + 4X^{k+1} + X^2 + 1)$.

Then (Q, R, T, Y) parameterizes a potential family of pairing-friendly elliptic curves with embedding degree k and discriminant 1. Its ρ-value is $\frac{k+1}{\varphi(k)}$.

Unfortunately, the polynomials (Q, R, T, Y) only define a potential family because 2 divides the integer values of Q. A solution to obtain a family of curves is to use the previous substitution method for a suitable α (for example, $\alpha = 3$). As a result, the discriminant will once again be multiplied by α.

We now state a very popular family of pairing-friendly elliptic curves of discriminant 3. The popular BLS12 and BLS24 curves fall in the case $k \equiv 0 \bmod 6$ of this family. The polynomials stated below give the best known ρ-values for many embedding degrees (see [22, Table 8.2]).

Example 3 (From [22, Construction 6.6]). Let k be an integer with $k \leq 1000$ and $18 \nmid k$. Let Q, R and T be defined as in Table 2: Then (Q, R, T) defines a complete family of pairing-friendly elliptic curves with embedding degree k and discriminant 3. Let $l = \mathrm{lcm}(k, 6)$, then the ρ-value of any such family is $(l/3+6)/\varphi(l)$ if $k \equiv 4 \bmod 6$ and $(l/3 + 2)/\varphi(l)$ otherwise.

k	$R(X)$	$T(X)$	$Q(X)$
1 mod 6	$\Phi_{6k}(X)$	$-X^{k+1}+X+1$	$(X+1)^2(X^{2k}-X^k+1)/3-X^{2k+1}$
2 mod 6	$\Phi_{3k}(X)$	$X^{k/2+1}-X+1$	$(X-1)^2(X^k-X^{k/2}+1)/3+X^{k+1}$
3 mod 18	$\Phi_{2k}(X)$	$X^{k/3+1}+1$	$(X^2-X+1)^2(X^{2k/3}-X^{k/3}+1)/3+X^{k/3+1}$
9, 15 mod 18	$\Phi_{2k}(X)$	$-X^{k/3+1}+X+1$	$(X+1)^2(X^{2k/3}-X^{k/3}+1)/3-X^{2k/3+1}$
4 mod 6	$\Phi_{3k}(X)$	X^3+1	$(X^3-1)^2(X^k-X^{k/2}+1)/3+X^3$
5 mod 6	$\Phi_{6k}(X)$	$X^{k+1}+1$	$(X^2-X+1)(X^{2k}-X^k+1)/3+X^{k+1}$
0 mod 6	$\Phi_k(X)$	$X+1$	$(X-1)^2(X^{k/3}-X^{k/6}+1)/3+X$

TABLE 2. Construction 6.6 from [22, Sect. 6], formulas for $k = 3 \bmod 6$ from ePrint.

2.5. **The Kachisa–Schaefer–Scott Method.** The previous families were all cyclotomic, meaning that R was a cyclotomic polynomial. There have been some attempts to apply the Brezing–Weng method with a non-cyclotomic polynomial R, such as the Barreto–Naehrig family [7], or the Kachisa–Schaefer–Scott (KSS) families [35]. In the next sections, we will extend the method of Kachisa et al., so we recall briefly their results. The KSS method consists in taking R as the minimal polynomial of an element of a cyclotomic field. Using this method, Kachisa et al. found some interesting families via enumeration (see Algorithm 2.2). KSS families are particularly interesting because they fill most of the gaps left by the cyclotomic methods: in Example 3, we have seen that the method does not work when k is a multiple of 18 and produces a larger ρ-value for $k \equiv 4 \bmod 6$, while the KSS method was successful for $k = 18, 36$, with the expected ρ-value $(k/3+2)/\varphi(k)$, and for for $k = 16, 40$, a ρ-value of $(k/2+2)/\varphi(k)$. The first two families are given in Example 4 and Example 5.

Example 4 (KSS16). Let:

- $R = X^8 + 48x^4 + 625$,
- $T = \frac{1}{35}(2X^5 + 41X + 35)$,
- $Y = \frac{1}{35}\left(X^5 - 5X^4 + 38X - 120\right)$,
- $Q = \frac{1}{980}(X^{10}+2X^9+5X^8+48X^6+152X^5+240X^4+625X^2+2398X+3125)$.

Then (Q, R, T, Y) parameterizes a complete family of elliptic curves with embedding degree $k = 16$, discriminant 1 and ρ-value $5/4$.

Example 5 (KSS18). Let:

- $R = X^6 + 37X^3 + 343$,
- $T = \frac{1}{7}(X^4 + 16X + 7)$,
- $Y = \frac{1}{21}\left(-5X^4 - 14X^3 - 94X - 259\right)$,
- $Q = \frac{1}{21}(X^8+5X^7+7X^6+37X^5+188X^4+259X^3+343X^2+1763X+2401)$.

Then (Q, R, T, Y) parameterizes a complete family of elliptic curves with embedding degree $k = 18$, discriminant 3 and ρ-value $4/3$.

Could these examples have been obtained with the Brezing–Weng method? Yes, if the ad hoc choices of R and T were given as input. Nevertheless, the Brezing–Weng is in some sense incomplete, as it does not provide a way to find R and T: they are used in the method as if they were parameters. The difficulty is to characterize the polynomials which could be suitable choices for R, as Step 1 of the Brezing–Weng method (Algorithm 2.1) mostly put constraints on the number field that R generates. The initial way to overcome this obstacle was to work with cyclotomic polynomials

Algorithm 2.2: Outline of KSS's algorithm

Input: k the embedding degree, $D \in \{1, 3\}$ the discriminant

1 Let $l = \mathrm{lcm}(3, k)$ if $D = 3$ or $l = \mathrm{lcm}(4, k)$ if $D = 1$, and ζ_l be a fixed primitive l-th root of unity in $\mathcal{C}_l$;
2 **for** θ *an integer linear combination of* $(\zeta_l^i)_{i=0,\dots,\varphi(l)-1}$ **do**
3 R=minpoly(θ);
4 **for** ζ_k *a primitive* k*-th root of the unity in* $\mathcal{C}_l$ **do**
5 Let $T \in \mathbb{Q}[X]$ such that $T(\theta) = \zeta_k + 1$;
6 Let $Y \in \mathbb{Q}[X]$ such that $Y(\theta) = (\zeta_k - 1)/\sqrt{-D}$;
7 Let $Q = (T^2 + DY^2)/4$;
8 Let $H = (Q + 1 - T)/R$;
9 [Process the potential family] ; // see subsection 3.5

for R (Barreto–Lynn–Scott, Brezing–Weng). This is however quite restrictive and does not offer the diversity we could have hoped for. For example, all families in the previous examples have a discriminant of 1 or 3. Moreover, a better choice of R could generate more efficient families.

To improve on the Brezing–Weng method, how to search for a better, non-cyclotomic polynomial R generating a cyclotomic field containing $\sqrt{-1}$ or $\sqrt{-3}$ (or any $\sqrt{-D}$)? Two paths arised: trying to find $U(X)$ such that $\Phi_l(U(X))$ factors for a chosen l and R is such a factor [7, 44], or taking R as the minimal polynomial of an element in a cyclotomic field $\mathcal{C}_l$ (KSS [35]). In KSS's case, the authors designed Algorithm 2.2. Define θ and ζ_k as in Algorithm 2.2. KSS's algorithm relies on the equivalence of giving ourselves R and T, or θ and ζ_k (when $\mathbb{Q}[X]/\langle R\rangle = \mathcal{C}_l$ is fixed). In practice, the representation by θ and ζ_k is more adapted to enumeration (over the a_i in $\theta = \sum_{i=0}^{\varphi(l)-1} a_i \zeta_l^i$). Unfortunately, KSS reported that bruteforce enumeration (step 2) did not work well, and they had to restrict themselves to the elements θ having a special form, which they selected using trial and error. Their method was effective as they were able to find some interesting curves. However, it is possible to improve their enumeration technique, as we will explain in the next section.

3. Results

In this section, our goal is to improve on the KSS method and generate new families with ρ-values as small as possible. We introduce a new enumeration method which allows to compute families very quickly with ρ-values depending uniquely on the embedding degree k and the discriminant D. Then, we present the results of the new enumeration method.

3.1. Properties of the number-theoretic representation.

We will work in a slightly more general context than KSS. Fix $k \geq 7$ and $D > 0$, and let K be any Galois extension of $\mathbb{Q}$ containing $\mathcal{C}_k(\sqrt{-D})$ (the compositum of $\mathcal{C}_k$ and $\mathbb{Q}(\sqrt{-D})$, Figure 1).

Let ζ_k be any primitive k-th root of unity in K, and let $\tau = \zeta_k + 1$ and $\gamma = (\zeta_k - 1)/\sqrt{-D}$. Let $\theta \in K$ such that the minimal polynomial of θ has degree $[K : \mathbb{Q}]$. This is equivalent to asking that θ generate the whole field, most elements of the field satisfy this property. We will note R_θ the minimal polynomial of θ, T_θ the polynomial

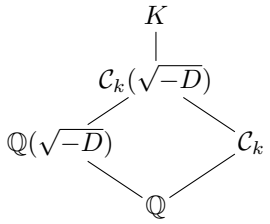


FIGURE 1. Our setting: K is a Galois extension of $\mathcal{C}_k(\sqrt{-D})$.

mapping θ to τ, Y_θ the polynomial mapping θ to γ, and $Q_\theta = (T_\theta^2 + DY_\theta^2)/4$. We will drop the indices when θ is clear from context.

We consider how affine transformations of θ affect the generated families. It is easy to see that adding a rational λ only induces the substitution $X \mapsto X - \lambda$. Multiplying by an integer is not much more interesting, but allows to simplify the enumeration process:

Proposition 3. *Let N be an integer, if $(R_\theta, T_\theta, Y_\theta, Q_\theta)$ is a family of curves then $(R_{N\theta}, T_{N\theta}, Y_{N\theta}, Q_{N\theta})$ is a family with the same ρ-value.*

Proof. It is easy to show that $R_{N\theta} = N^{\deg R} R_\theta(X/N)$, $T_{N\theta} = T_\theta(X/N)$, $Y_{N\theta} = Y_\theta(X/N)$, and therefore $Q_{N\theta} = Q_\theta(X/N)$. Every corresponding polynomial has the same degree so the potential families have the same ρ-value. It is clear that $Q(X/N)$ is irreducible if and only if Q is irreducible, and that if Q represents primes then $Q(X/N)$ represents primes as well (notice that Q is a weighted sum of squares, so $N < 0$ does not change the sign of the leading coefficient). □

Proposition 3 is useful because it shows we only have to consider integer linear combinations of elements of a basis of K as candidates for θ in our enumeration. However, the polynomials generated may have a large denominator.

We finally mention that in the context of the Brezing–Weng method, the degree of Q is $\deg Q = 2\max(\deg T, \deg Y)$. Then, the problem of generating a potential family with small ρ-value can be seen as a particular instance of the following problem:

Problem 1. Let K be a number field of degree d over $\mathbb{Q}$, let n be an integer, and let τ and γ be elements of K. Find an element $\theta \in K$ such that there exists polynomials Y and T satisfying:

- $Y(\theta) = \gamma$,
- $T(\theta) = \tau$,
- $\deg Y \leq n$ and $\deg T \leq n$.

In the general case, it seems unlikely to be able to find a solution when $n < d - 1$, and even more for $n \leq (d + \varepsilon)/2$. However, in our particular instance, many families with ρ-value significantly smaller than 2 have been found. In the following, we will explain which mathematical property of τ and γ allows to find families with small ρ-value in our specific setting and propose a method to compute such families.

3.2. **Subfield method.** Fix $k \geq 7$ and D. Let F be a number field containing $\sqrt{-D}$, and let K be the compositum of F and $\mathcal{C}_k$. We can see K as a F-vector space, and we can also see $\mathcal{C}_k$ as a subfield of K. Then, the vector line $F\zeta_k = \{\alpha\zeta_k; \alpha \in F\}$

contains ζ_k and $\zeta_k/\sqrt{-D}$. This method relies on the idea that elements of F will be represented by polynomials of small degree, and the polynomial corresponding to the multiplication by $\alpha \in F$ as well.

We take $\theta \in F\zeta_k$, that is we force θ to be of the form $\theta = \alpha\zeta_k$, and let $\alpha = \theta/\zeta_k \in F$. Notice that $\theta^k = \alpha^k \in F$, and most commonly α^k will generate F, or equivalently $\mathbb{Q}(\alpha^k) = F$. Then, let e be the minimal divisor of k such that $\theta^e \in F$ and θ^e generates F. Now let P_1, P_2, P_3 be the polynomials such that:

$$\begin{aligned} P_1(\theta^e) &= 1/\alpha \ , \\ P_2(\theta^e) &= 1/(\alpha\sqrt{-D}) \ , \\ P_3(\theta^e) &= 1/\sqrt{-D} \ . \end{aligned}$$

Notice that P_1, P_2 and P_3 have degree at most $[F : \mathbb{Q}] - 1$ (we will have equality in most cases). Now, notice that:

$$\begin{aligned} P_1(\theta^e)\theta + 1 &= \theta/\alpha + 1 = \zeta_k + 1 \ , \\ P_2(\theta^e)\theta - P_3(\theta^e) &= \zeta_k/\sqrt{-D} - 1/\sqrt{-D} = (\zeta_k - 1)/\sqrt{-D} \ . \end{aligned}$$

Therefore we can choose $T(X) = P_1(X^e)X$ and $Y(X) = P_2(X^e)X - P_3(X^e)$, which have degree at most (generally equal to) $e([F : \mathbb{Q}] - 1) + 1$. Let R be the minimal polynomial of θ. This method generates potential families with ρ-value:

$$\rho \leq \frac{2e([F : \mathbb{Q}] - 1) + 2}{[K : \mathbb{Q}]} \ . \tag{3.1}$$

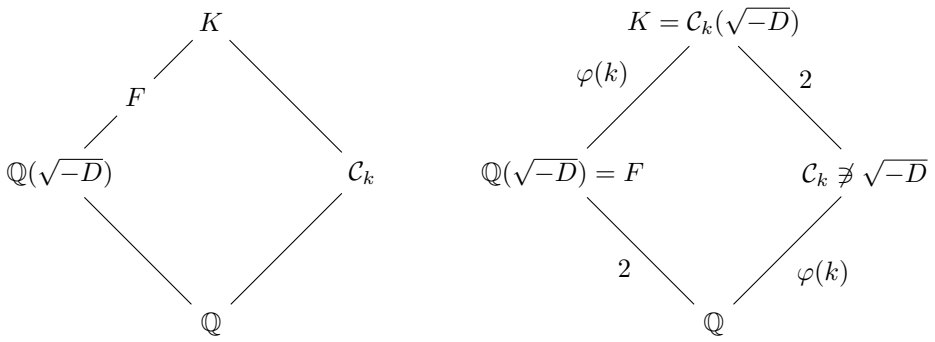
Generally, Eq. (3.1) is an equality (in fact we did not encountered any counterexample in our enumeration). From now on, we will assume that Eq. (3.1) is an equality, and try to choose F so that ρ is minimal. Notice that a decomposition of the extension degree of K over $\mathbb{Q}$ with the intermediate field F gives $[K : \mathbb{Q}] = [K : F][F : \mathbb{Q}]$ and it follows from Eq. (3.1) that

$$\begin{aligned} \rho &= 2e\frac{[F : \mathbb{Q}] - 1}{[K : \mathbb{Q}]} + \frac{2}{[K : \mathbb{Q}]} \\ &= 2e\frac{[F : \mathbb{Q}] - 1}{[K : F][F : \mathbb{Q}]} + \frac{2}{[K : \mathbb{Q}]} \\ &= \frac{2e}{[K : F]}\left(1 - \frac{1}{[F : \mathbb{Q}]}\right) + \frac{2}{[K : \mathbb{Q}]} \ . \end{aligned} \tag{3.2}$$

The term $\frac{2e}{[K:F]}\left(1 - \frac{1}{[F:\mathbb{Q}]}\right)$ is dominant in this sum. Therefore, when e is fixed, we should try to maximize $[K : F]$ and minimize $[F : \mathbb{Q}]$. In the following three cases, we give the optimized ρ-value for different choices of e.

Case 1. When $e = k$, that is, the minimal power of θ such that it belongs to F is $\theta^k \in F$, the extension diagram is the following (Figure 2). From the diagram 2(a) we deduce that the choice $F = \mathbb{Q}(\sqrt{-D})$ contributes to minimizing the ρ-value. In that case, it would be more favorable if $\sqrt{-D}$ were not an element of $\mathcal{C}_k$, so that $[K : F] = \varphi(k)$ (and not $\varphi(k)/2$) (see Figure 2(b)). Then, from Eq.(3.2) with $e = k$, $[K : F] = \varphi(k)$, $[F : \mathbb{Q}] = 2$, $[K : \mathbb{Q}] = 2\varphi(k)$,

$$\rho = \frac{2k}{\varphi(k)}\left(1 - \frac{1}{2}\right) + \frac{2}{2\varphi(k)} = \frac{k+1}{\varphi(k)} \ . \tag{3.3}$$



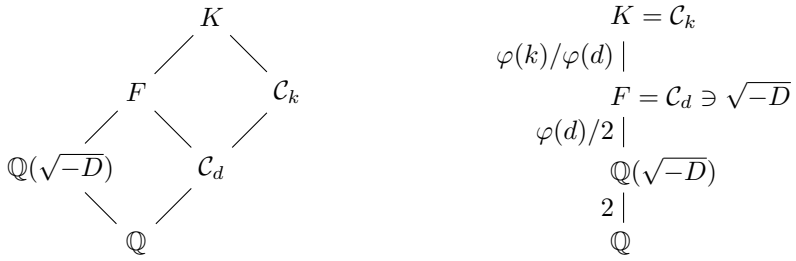
(a) General setting (b) Optimized setting

FIGURE 2. General and optimized setting for Case 1.

Case 2. When k is even, then $\theta^{k/2} = -\alpha^{k/2}$ which will generally be a generator of F. Therefore, the decrease of e to $e = k/2$ is free, as we do not have to make any further assumption on F. The diagram will be exactly the same as in Case 1, and in Eq. (3.2), $e = k/2$ instead. In this case,

$$\rho = \frac{2k/2}{\varphi(k)}\left(1 - \frac{1}{2}\right) + \frac{2}{2\varphi(k)} = \frac{k/2+1}{\varphi(k)} \,. \tag{3.4}$$

Case 3. Let d be a divisor of k, $d \geq 3$. If we want that $\mathbb{Q}(\theta^{k/d}) = F$, then $\zeta_k^{k/d} = \zeta_d$ has to be an element of F, and F has to be an algebraic extension of $\mathcal{C}_d$. This changes the extension diagram to Figure 3(a). Here from Figure 3(a) we deduce



(a) General setting (b) Optimized setting

FIGURE 3. General and optimized setting for Case 3.

that F should be the compositum of $\mathbb{Q}(\sqrt{-D})$ and $\mathcal{C}_d$. However, in that case, it would be better if $\sqrt{-D}$ were an element of $\mathcal{C}_d$ to minimize $[F : \mathbb{Q}]$ (here $[K : F]$ is already bounded by $[\mathcal{C}_k : \mathcal{C}_d]$) (Figure 3(b)). With $e = k/d$, $[K : F] = \varphi(k)/\varphi(d)$, $[F : \mathbb{Q}] = \varphi(d)$ and $[K : \mathbb{Q}] = \varphi(k)$,

$$\rho = \frac{2k/d}{\varphi(k)/\varphi(d)}\left(1 - \frac{1}{\varphi(d)}\right) + \frac{2}{\varphi(k)} = \frac{2(\varphi(d)-1)}{d}\frac{k}{\varphi(k)} + \frac{2}{\varphi(k)} \,. \tag{3.5}$$

We need to compare Case 3 to the first two cases. When k is odd, we mostly need to find which d satisfies $2(\varphi(d)-1)/d \leq 1$ (we authorize equality as the ρ-value

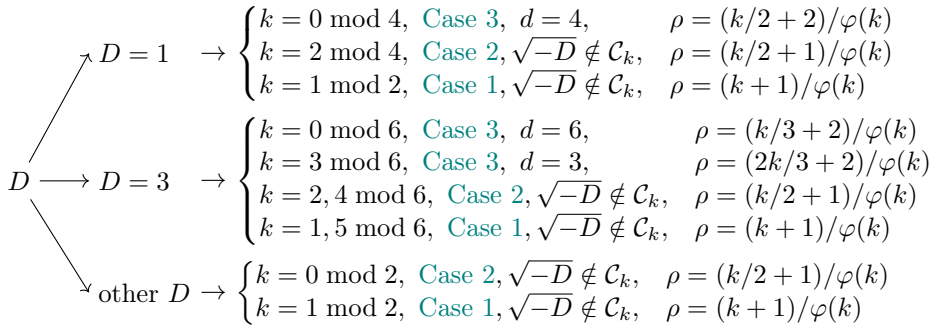


FIGURE 4. Best choice of k, d to minimize ρ, according to D.

will only differ by $1/\varphi(k)$). When k is even, d needs to satisfy $2(\varphi(d)-1)/d \leq 1/2$. Table 3 gives us the list of integers d such that $2(\varphi(d)-1)/d$ is small enough with respect to the parity of k:

k	$d,\ d \mid k$	$2(\varphi(d)-1)/d$	upper bound
odd	3	2/3	Case 1: 1
	15	14/15	
even	4	1/2	Case 2: 1/2
	6	1/3	
	12	1/2	
	30	7/15	

TABLE 3. Choices for d between 3 and 50 and corresponding coefficients.

We can notice that $d = 12, 15, 30$ are less interesting as they are multiples of 3 and 6 and are less efficient. Therefore, this case is interesting only if $d = 3, 4, 6$. Notice that in each case $\mathcal{C}_d$ is an imaginary quadratic field containing either $\sqrt{-1}$ or $\sqrt{-3}$. Notice also that when $d = 4$, the ρ-value from Case 3 is larger than the ρ-value from Case 2 by $1/\varphi(k)$, but it still provides an almost as efficient alternative. Moreover, Case 3 has the extra advantage of generating a polynomial R with degree $\varphi(k)$ instead of $2\varphi(k)$.

Remark 5. Notice that in every case, we obtain that K should be equal to $\mathcal{C}_k(\sqrt{-D})$. In particular, this means that the properties stated in subsection 3.1 apply.

Remark 6. Here we separated three cases depending on the value of e, which was more convenient for the proof on minimal ρ-value, but in practice it is more convenient to start from fixed k and D. Here is our strategy to minimize ρ (Figure 4), given D as input. Let $D = 1$, then if k is a multiple of 4, use Case 3 with $d = 4$, if $k \equiv 2 \bmod 4$, use Case 2, and if k is odd, use Case 1. When $D = 3$, if $d = \gcd(k, 6)$ is a multiple of 3, you can use Case 3 with d, else use Case 1 when k is odd and Case 2 when k is even. For any other D, if $\sqrt{-D} \notin \mathcal{C}_k$, use Case 1 when k is odd, and Case 2 when k is even.

Remark 7. Let $l = \mathrm{lcm}(k, 6)$, then the subfield method can always generate potential families with a ρ-value of $\rho = (l/3+2)/\varphi(l)$, the same as FST and KSS families.

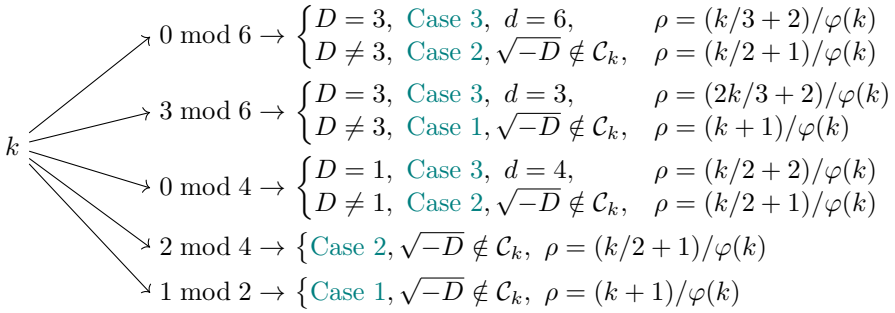


FIGURE 5. Best choice of D, d to minimize ρ, according to k.

It is important to see that this method only generates potential families. We hope that having a wide range for θ will allow to find a family among the generated potential families. We will see in the following that, in most cases, finding a family is not an issue. We summarize our findings in algorithm 3.1. Of course, the choice of F and K can be adapted to a specific context (for example when having a specific discriminant is more important than having a small ρ-value).

Algorithm 3.1: SubfieldMethod(k, D, F, e)

Let K be the compositum of F and $\mathcal{C}_k$;
Let ζ_k be a fixed primitive k-th root of unity in K;
for $\alpha \in F$ **do**
  $\theta = \alpha\zeta_k$;
  R=minpoly(θ);
  Let $P_1 \in \mathbb{Q}[X]$ such that $P_1(\theta^e) = 1/\alpha$;
  Let $P_2 \in \mathbb{Q}[X]$ such that $P_2(\theta^e) = 1/(\alpha\sqrt{-D})$;
  Let $P_3 \in \mathbb{Q}[X]$ such that $P_3(\theta^e) = 1/\sqrt{-D}$;
  $T(X) = XP_1(X^e) + 1$;
  $Y(X) = XP_2(X^e) - P_3(X^e)$;
  Let $Q = (T^2 + DY^2)/4$;
  Let $H = (Q + 1 - T)/R$;
  [Process the potential family] ; `// subsection 3.5`

We end this subsection by recalling what case is best suited to a given k (see also Figure 5). If k is a multiple of 6 (resp. 3) then use Case 3 with $d = 6$ (resp. $d = 3$). If you need to avoid the discriminant $D = 3$, you can use Case 2 (resp. Case 1) if k is even (resp. odd) with another discriminant, but the ρ-value will increase. Else if k is a multiple of 4 then use Case 3 with $d = 4$ for discriminant $D = 1$, and Case 2 for another discriminant. In this instance, the ρ-value only differ by $1/\varphi(k)$ with Case 2 having the smallest one. Else, if k is 2 modulo 4 (resp. odd), use Case 2 (resp. Case 1).

3.3. **Theoretical results.** In this subsection, we compare the ρ-values we obtain for each k with the values stated in [22, Table 8.2]. We should start with stating

that most of the families achieving the best ρ-values are particular instances of the subfield method (KSS families, FST families when $k \not\equiv 4 \bmod 6$ for example).

The reader can check if a family can be produced with the subfield method by checking if T has the form $(bX^e + a)X + 1$, with e dividing k and a, b rationals.

For example, the polynomials from Example 2 can be obtained by simply choosing $\theta = \zeta_k$, and the polynomials from Example 3 can be obtained by taking $\theta = \zeta_l$ when $k \not\equiv 4 \bmod 6$, where $l = \mathrm{lcm}(6, k)$ and ζ_l is a primitive l-th root of unity in the vector line $\mathcal{C}_6\zeta_k$. It is also interesting to see that every family obtained by KSS in [35], except for the Barreto-Naehrig family, are instances of the subfield method. In particular, as we have shown that the subfield method never achieves $\rho = 1$, it seems very unlikely to be able to find another family having this property via untargeted enumeration.

This method of generation of curves, when compared to previous methods, has the added advantage of generating multiple curves of the same quality regarding their ρ-value, for almost all k and D. Therefore, attacks such as the one in [29] targeting polynomials of a specific form are less effective, since we will usually be able to find a family not targeted by the attack (as in subsubsection 3.4.3). The biggest flaw of the method however is the size of the denominators of the generated families, which sometimes make the families unusable, or less practical.

Lastly, the method generates families with an improved ρ-value compared to the previously known families for some embedding degrees:

(1) when $k = 22, 46$, or more generally, $k \equiv 22 \bmod 24$,
(2) when $k = 16, 28, 40$, or more generally, $k \equiv 4 \bmod 12$.

However, the improvement for $k = 16, 28, 40$ are practically irrelevant, because the generated families have large denominators (see the next subsection for more details), and because the gain in ρ-value can only be obtained with $D \neq 1$, preventing the use of a high-degree (quartic) twist, hence missing four-fold $\mathbb{G}_2$-compression techniques.

Table 4 summarizes our results, and compares them to the values from [22, Table 8.2]. A dash symbol $(-)$ means that the case is not suited to the choice of k, and a colored cell means that the case produced families with very large denominators in the polynomials, making it difficult to obtain valid curve parameters.

3.4. **Experimental results.** In this subsection, we start by explaining our enumeration process. We then give more details about the cases $k = 16, 28, 40$, and finally give examples of new families for $k = 22, 46$. We ran our experients on an Intel Xeon Silver 4214 CPU at 2.20 GHz with 16 GB RAM with SageMath 9.7 using Python 3.10.5.

First note that in all cases of interest, F is a quadratic imaginary field and in most of the cases, $F = \mathbb{Q}(\sqrt{-D})$. Let $\{1, \omega\}$ be a basis of the integer ring of F. Usually, the basis is made of $\{1, (-1 + \sqrt{-D})/2\}$ if $D = 3 \bmod 4$, and $\{1, \sqrt{-D}\}$ otherwise. Set $a, b \in \mathbb{Z}$. We enumerate over $\alpha \in F$ (Algorithm 3.1 step 3) of the form $\alpha = a + b\omega$ where $-20 \leq a, b \leq 20$ and $\gcd(a, b) = 1$.

We observed that the period of the seed x_0 (so that (Q, R, T, Y, H) take integer values) and the size of the denominators are minimized for (a, b) of smallest coefficients (that is, $|a|, |b|$ as small as possible). As the choice $(a, b) = (1, \pm 1)$ does not produce a potential family for each D, we try many values of D until we obtain $(a, b) = (1, \pm 1)$. For $k = 22, 46$, we observed for $1 \leq D \leq 50$ and $|a|, |b| \leq 20$ that each D provides many potential families. We obtained

k	ρ, Case 1	ρ, Case 2	ρ, Case 3	ρ, Previous method
7	1.333	–	–	1.333, [22, 6.6]
8	–	1.250	1.500, $d = 4$	1.250, [22, 6.6]
9	1.667	–	1.333, $d = 3$	1.333, [22, 6.6]
10	–	1.500	–	1.500, [22, 6.24]
11	1.200	–	–	1.200, [22, 6.6]
12	–	1.750	1.500, $d = 6$	**1.000**, [22, 6.8]
13	1.167	–	–	1.167, [22, 6.6]
14	–	1.333	–	1.333, [22, 6.6]
15	2.000	–	1.500, $d = 3$	1.500, [22, 6.6]
16	–	1.125	1.250, $d = 4$	1.250, [22, 6.11]
17	1.125	–	–	1.125, [22, 6.6]
18	–	1.667	1.333, $d = 6$	1.333, [22, 6.12]
19	1.111	–	–	1.111, [22, 6.6]
20	–	1.375	1.500, $d = 4$	1.375, [22, 6.6]
21	1.833	–	1.333, $d = 3$	1.333, [22, 6.6]
22	–	**1.200**	–	1.300, [22, 6.3]
23	1.091	–	–	1.091, [22, 6.6]
24	–	1.625	1.250, $d = 6$	1.250, [22, 6.6]
25	1.300	–	–	1.300, [22, 6.6]
26	–	1.167	–	1.167, [22, 6.6]
27	1.556	–	1.111, $d = 3$	1.111, [22, 6.6]
28	–	1.250	1.333, $d = 4$	1.333, [22, 6.4]
29	1.071	–	–	1.071, [22, 6.6]
30	–	2.000	1.500, $d = 6$	1.500, [22, 6.6]
31	1.067	–	–	1.067, [22, 6.6]
32	–	1.063	1.125, $d = 4$	1.063, [22, 6.6]
33	1.700	–	1.200, $d = 3$	1.200, [22, 6.6]
34	–	1.125	–	1.125, [22, 6.24]
35	1.500	–	–	1.500, [22, 6.6]
36	–	1.583	1.167, $d = 6$	1.167, [22, 6.14]
37	1.056	–	–	1.056, [22, 6.6]
38	–	1.111	–	1.111, [22, 6.6]
39	1.667	–	1.167, $d = 3$	1.167, [22, 6.6]
40	–	1.3125	1.375, $d = 4$	1.375, [22, 6.11]
41	1.050	–	–	1.050, [22, 6.6]
42	–	1.833	1.333, $d = 6$	1.333, [22, 6.6]
43	1.048	–	–	1.048, [22, 6.6]
44	–	1.150	1.200, $d = 4$	1.150, [22, 6.6]
45	1.917	–	1.333, $d = 3$	1.333, [22, 6.6]
46	–	**1.091**	–	1.136, [22, 6.3]
47	1.043	–	–	1.043, [22, 6.6]
48	–	1.562	1.125, $d = 6$	1.125, [22, 6.6]
49	1.190	–	–	1.190, [22, 6.6]
50	–	1.300	–	1.300, [22, 6.6]

TABLE 4. Comparison of the ρ-values of the subfield method and previous methods

$(a,b) = (1,\pm 1)$ with $D = 7$ for both $k = 22$ (Example 6) and $k = 46$ (Appendix A). To the contrary for $k \in \{16, 28, 40\}$, most of D fail and we enlarged the search space over D. We obtain potential families for some D, $k = 16$ with $D \in \{19, 35, 59, 67, 83, 115, 203, 227\}$, and $(a,b) = (1 \pm 1)$ with $D = 35$ and $D = 227$; $k = 28$ with $D \in \{11, 19, 23, 43, 47, 55, 59, 67, 71, 79, 83, 103, 107, 115, 127, 131, 139\}$, and $(a,b) = (1 \pm 1)$ with $D = 11$; and $k = 40$ with $D \in \{11, 31, 71, 103, 143, 163\}$, we did not get $(a,b) = (1,\pm 1)$, the smallest period was reached at $D = 11$ with $(a,b) = (13,-9)$. We got $(a,b) = (1,-3)$ with $D = 103$. One can observe that for $k = 16, 28, 40$, the Ds that work satisfy $D = 3 \bmod 4$.

3.4.1. *We reproduce the previous KSS results.* Using Case 3 with $d = 4$, we generate families with the same ρ-value as the KSS16 (Example 4) and KSS40 families and the method from [22, Method 6.4], and with discriminant $D = 1$ as well. Using Case 3 with $d = 6$, we generate families of discriminant $D = 3$ with the same ρ-value as the KSS18 (Example 5), KSS36 families. Note that for $k = 54$, we obtain the same three families with $\rho = 10/9$ as in [44] with $(a,b) \in \{(1,1),(1,-2),(2,-1)\}$.

3.4.2. *New families with smaller ρ of theoretical interest for $k \in \{22, 46\}$ and $k \in \{16, 28, 40\}$.* We provide examples of new families with better ρ-values for $k = 22$. The case $k = 46$ is only of theoretical interest as the polynomials have very large coefficients. We provide the data in Appendix A. With $k = 46$ we select $D = 7$ and $(a,b) = (1,1)$ in Example 17, and $D = 15$, $(a,b) = (3,1)$ in Example 18.

Example 6. $k = 22$, $D = 7$, $F = \mathbb{Q}[x]/(x^2 + x + 2)$, $\omega = (-1 + \sqrt{-7})/2$, $\alpha = 1 + \omega$, $(a,b) = (1,1)$, $\theta = \alpha\zeta_k$.

- $T = (X^{12} + 45X + 46)/46$
- $Y = (X^{12} - 4X^{11} - 47X - 134)/322$
- $R = (X^{20} - X^{19} - X^{18} + 3X^{17} - X^{16} - 5X^{15} + 7X^{14} + 3X^{13} - 17X^{12} + 11X^{11} + 23X^{10} + 22X^9 - 68X^8 + 24X^7 + 112X^6 - 160X^5 - 64X^4 + 384X^3 - 256X^2 - 512X + 1024)/23$
- $Q = (X^{24} - X^{23} + 2X^{22} + 67X^{13} + 94X^{12} + 134X^{11} + 2048X^2 + 5197X + 4096)/7406$

Let $H = (Q + 1 - T)/R$. With $x \equiv 4 \bmod 7$, and $x \equiv 13, 9 \bmod 23$, then all polynomials take integer values and R, Q can take prime values. With $x \equiv 4 \bmod 7$, and $x \equiv 1, 2, 3, 4, 6, 8, 12, 16, 18 \bmod 23$, all polynomials and $23H$ take integer values and $R/23$, Q can take prime values. The seed $x_0 = -\texttt{0xbe503} = -779523$ produces a curve with $R(x_0)/23$ prime of 383 bits, $Q(x_0)$ prime of 457 bits. Curves with CM by $(-1 + \sqrt{-7})/2$ have j-invariant $j = -3375$. The curve defined over $\mathbb{F}_{Q(x_0)}$ by $E\colon y^2 = x^3 - 5/7x - 2/7$ has trace $T(x_0)$, and expected order.

Example 7. $k = 22$, $D = 1$, $F = \mathbb{Q}(i)$, $i = \sqrt{-1}$, $\alpha = 1 + 2i$, $(a,b) = (1,2)$, $\theta = \alpha\zeta_k$.

- $T = \frac{1}{6605}\left(-X^{12} - 5148X + 6605\right)$
- $Y = \frac{1}{13210}\left(X^{12} - 5X^{11} + 11753X - 32345\right)$
- $R = (X^{20} - 2X^{19} - X^{18} + 12X^{17} - 19X^{16} - 22X^{15} + 139X^{14} - 168X^{13} - 359X^{12} + 1558X^{11} - 1321X^{10} + 7790X^9 - 8975X^8 - 21000X^7 + 86875X^6 - 68750X^5 - 296875X^4 + 937500X^3 - 390625X^2 - 3906250X + 9765625)/1321$
- $Q = \frac{1}{139603280}\left(X^{24} - 2X^{23} + 5X^{22} + 12938X^{13} - 47012X^{12} + 64690X^{11} + 48828125X^2 - 206464378X + 244140625\right)$

With seeds $x \equiv 1 \bmod 2$, $x \equiv 0, 3 \bmod 5$, $x \equiv 105, 286, 350, 389, 416, 485, 506, 513, 692, 736, 806 \bmod 1321$, the polynomials take integer values and $Q(x)$ generates primes.

We discard $x \equiv 0 \bmod 5$ as is produces $5^{10} \mid R(x)$. For $x \equiv 513, 806 \bmod 1321$, $R(x)$ takes prime values, for the other congruences, $R(x)/1321$ takes prime values. The valid seeds producing prime $Q(x_0)$, $R(x_0)$ are very sparse and we did not get $r = R(x_0)$ of 384 bits. We mention $x_0 = \texttt{0x1a450d} = 1721613$ s.t. $Q(x_0)$ is a 471-bit prime and $R(x_0)/1321$ is a 394-bit prime; the curve is $y^2 = x^3 + 27x$.

Example 8. $k = 22$, $D = 3$, $F = \mathbb{Q}[x]/(x^2+x+1)$, $\omega = (-1+\sqrt{-3})/2$, $\alpha = (5+4\omega)$, $(a, b) = (5, 4)$, $\theta = \alpha\zeta_k$.

- $T = \frac{1}{341901}\left(-X^{12} + 18764460X + 341901\right)$
- $Y = \frac{1}{683802}\left(X^{12} - 7X^{11} - 18650493X + 131009319\right)$
- $R = (X^{20} - 6X^{19} + 15X^{18} + 36X^{17} - 531X^{16} + 2430X^{15} - 3429X^{14} - 30456X^{13} + 254745X^{12} - 888894X^{11} - 16281X^{10} - 18666774X^9 + 112342545X^8 - 282053016X^7 - 666875349X^6 + 9924365430X^5 - 45541810251X^4 + 64839187476X^3 + 567342890415X^2 - 4765680279486X + 16679880978201)/(3^{10} \cdot 67)$
- $Q = \frac{1}{267191528688}\left(X^{24} - 6X^{23} + 21X^{22} - 37431234X^{13} + 223805916X^{12} - 786055914X^{11} + 350277500542221X^2 - 2087000802936846X + 7355827511386641\right)$

With a seed $x \equiv 1 \bmod 2$, $x \equiv 0 \bmod 3$, $x \equiv 0, 1 \bmod 7$, and $2, 13, 18, 28, 30, 44, 48, 50, 51, 57, 61 \bmod 67$, the polynomials take integer values and Q generate primes. We discard $x \equiv 0 \bmod 7$ as in that case, $7^{10} \mid R$. When $x \equiv 13, 48 \bmod 67$, R generates primes and H takes integer values. When $x \equiv 2, 18, 28, 30, 44, 50, 51, 57, 61 \bmod 67$, $R/67$ generates primes and $67H$ takes integer values. The seed $x_0 = \texttt{0x214f5f} = 2183007 \equiv 13 \bmod 67$ gives valid parameters with Q prime of 468 bits and R prime of 400 bits, and the curve is $y^2 = x^3 - 1/\mathbb{F}_q$, of expected order.

Example 9. Let $k = 16$, $D = 35$, $F = \mathbb{Q}[x]/(x^2+x+9)$, $\omega = (-1+\sqrt{-35})/2$, $\alpha = \omega$, $(a, b) = (0, 1)$, $\theta = \alpha\zeta_k$. Case 2 gives $\rho = 9/8 = 1.125$ compared to the well-known KSS16 curve (Example 4) with $\rho = 5/4 = 1.25$. Note that in practice, because of the denominators and the cofactors, the ρ-value of KSS16-330 is 1.29, the ρ-value of KSS16-766 is 1.27.

- $T = \left(X^9 + 424X + 19431\right)/19431$
- $Y = \left(X^9 + 18X^8 + 39286X + 27063\right)/19431$
- $R = \left(X^{16} + 3007X^8 + 43046721\right)/(3^{16} \cdot 17^2 \cdot 127^2)$
- $Q = \left(X^{18} - X^{17} + 9X^{16} + 3007X^{10} - 78572X^9 + 27063X^8 + 43046721X^2 - 75086281X + 387420489\right)/1468303515$

The constrains on the seed x are $x \equiv 0 \bmod 3^2$, $x \equiv 3 \bmod 5$, $x \equiv 4 \bmod 7$, $x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \bmod 17$, and $x \equiv 3, 124 \bmod 127$. With this new family we were not able to produce any parameter sets of cryptographic size where r has 256 or 384 bits. The seeds producing curves are very sparse. Nevertheless we obtained $u_0 = \texttt{0x173d4fe} = 24368382$, q has 412 bits and r has 346 bits ($\rho = 1.19$), and $u_1 = \texttt{0x1bc63c0c} = 465976332$, q has 488 bits and r has 414 bits ($\rho = 1.18$). The curve equations are given in the companion code `replay_examples.sage`.

3.4.3. *New families performing as well as previous families for $k = 18, 20$.* We extend on $k = 20$ in Example 11 and Example 12 in subsubsection 3.4.3. See also Example 19 for an alternative family with $k = 18$.

Example 10. Let $k = 18$, k is a multiple of 6 so let $D = 3$ and $F = \mathcal{C}_6$, $\omega = \zeta_k^3 = (1 + \sqrt{-3})/2$, $e = 3$. Let $\theta = (1 + 3\zeta_k^3)\zeta_k$. Then:

- $T = (3X^4 + 176X + 221)/221$,

- $Y = (5X^4 - 26X^3 + 146X - 1157)/663$,
- $R = (X^6 + 89X^3 + 2197)/(13^3 \cdot 17^2)$,
- $Q = \frac{1}{11271}\left(X^8 - 5X^7 + 13X^6 + 89X^5 - 292X^4 + 1157X^3 + 2197X^2 - 2009X + 28561\right)$

is a family of elliptic curves with discriminant $D = 3$ and ρ-value $\rho = 1 + \frac{1}{3} = \frac{4}{3}$. With $x \equiv 1 \bmod 3$, $x \equiv 0 \bmod 13$, $x \equiv 9 \bmod 17$, Q, R generate primes and $T, Y, H = (Q + 1 - T)/R$ take integer values. The seed $x_0 = -2^{81} - 2^{79} + 2^{67} - 2^{55} - 2^{22}$ produces q prime of 638 bits and r prime of 469 bits, the curve is $y^2 = x^3 - 3$.

We investigate the KSS gap at $k = 20$. To benefit from the highest possible twist, one chooses $D = 1$, like for $k = 16$. For that we run Case 3 with $k = 20$, $d = 4$ and obtain different families. We choose the ones with the smallest denominators. We do obtain families with $\deg(R) = 8$, $\deg(Q) = 12$, $\rho = 3/2 = 1.5$, and $D = 1$. We do not reduce the ρ-value compared to the FST 6.4 family but we obtain an alternative Q that is not vulerable to the attack of [29]. The number field defined by $Q(x)$ has no automorphism and admits only a quadratic subfield with ζ_4. To further optimize the arithmetic operations on the curve, we would like to enforce $q \equiv 1 \bmod 5$ so as to define the extension $\mathbb{F}_{q^5}$ with a binomial, for a faster Frobenius map in $\mathbb{F}_{p^{20}}$. In other words, we add the condition $(Q(X) - 1)/5$ generates integers. Choosing r of 384 bits implies q of $\approx$576 bits and this size reaches the 192-bit security level. We obtain the following two families that we call GG20a and GG20b.

Example 11 (GG20a). Let $k = 20$, k is a multiple of 4, let $D = 1$ and $F = \mathcal{C}_4$. Let $\theta = (1 - 2\zeta_4)\zeta_k$. Then

- $T = (2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 - 44X - 190)/205$
- $R = (X^8 + 4X^7 + 11X^6 + 24X^5 + 41X^4 + 120X^3 + 275X^2 + 500X + 625)/25625$
- $Q = (X^{12} - 2X^{11} + 5X^{10} + 76X^7 + 176X^6 + 380X^5 + 3125X^2 + 12938X + 15625)/33620$

is a family of elliptic curves with discriminant $D = 1$ and ρ-value $\rho = 3/2$. With $x_0 \bmod 410 \in [69, 75, 79, 135, 175, 239, 299, 315, 325, 339]$, the conditions are met (T, Y are integers, $Q, R/\lambda, \lambda H$ generate primes for λ a small integer cofactor). With $x_0 = 1715, 1815 \bmod 2050$, Q and R generate primes, and $q = Q(x_0) \equiv 1 \bmod 5$.

Example 12 (GG20b). Let $k = 20$, k is a multiple of 4, let $D = 1$ and $F = \mathcal{C}_4$. Let $\theta = (1 + 2\zeta_4)\zeta_k$. Then

- $T = (-2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 + 44X + 190)/205$
- $R = (X^8 - 4X^7 + 11X^6 - 24X^5 + 41X^4 - 120X^3 + 275X^2 - 500X + 625)/25625$
- $Q = (X^{12} - 2X^{11} + 5X^{10} - 76X^7 - 176X^6 - 380X^5 + 3125X^2 + 12938X + 15625)/33620$

is a family of elliptic curves with discriminant $D = 1$ and ρ-value $\rho = 3/2$. With $x_0 \bmod 410 \in [71, 85, 95, 111, 171, 235, 275, 331, 335, 341]$, the conditions are met (T, Y are integers, $Q, R/\lambda, \lambda H$ generate primes for λ a small integer cofactor). With $x_0 = 1465, 1565 \bmod 2050$, Q and R generate primes, and $q = Q(x_0) \equiv 1 \bmod 5$.

3.5. **Processing potential families.** In Algorithm 2.2 and Algorithm 3.1, we mention processing the potential families, without giving much more details. By "processing", we mean two things: computing the common integer seeds of the polynomials Q, R, T, Y and H and checking that Q represents primes. We want

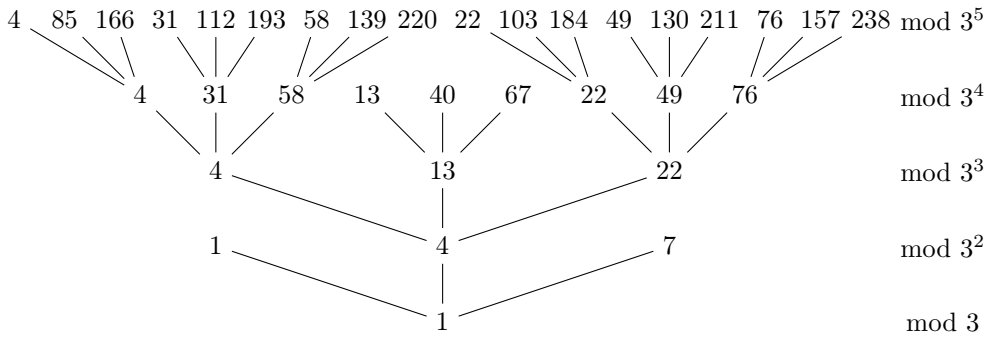


FIGURE 6. Tree of roots of $X^2 + X + 223$ modulo powers of 3 [43, Section 2.6].

this step to be fast since we generate a lot of potential families and we need to quickly discard the wrong ones that do not give valid curve parameters. There are arithmetic relations between the polynomials (Definition 3) which allow to avoid some computations. A suitable approach is to first compute the integer seeds of T and Y and use the relation $Q = (T^2 + DY^2)/4$ to find the common integer seeds of T, Y, and Q. Then, using Remark 4, find λ such that R/λ and λH take integer values at some of the integer seeds.

Let P be a polynomial with rational coefficients. Then there exists a unique polynomial P' with integral coefficients and a unique integer Δ, called denominator of P, such that $P = P'/\Delta$. Therefore, the set of integer seeds of P is the set of roots of P' modulo Δ. In particular, we see that the set of integer seeds of P is periodic (for some period dividing Δ). Using the Chinese Remainder Theorem (CRT), we can describe the roots of P' modulo Δ with the roots of P' modulo $p^{\mathrm{val}_p(\Delta)}$ for each prime p dividing Δ. Moreover, since the polynomials we generate have a quite large denominator, we had to find an efficient way of representing the set of integer seeds in order to be able to compute and store it. In the following, we give some information on the structure of the roots of a polynomial modulo a prime power, and explain how this structure allows to find a compressed representation of this set. Then we present the algorithm we designed to compute the set under its compressed representation, and the algorithm we used to check if Q represents primes. Finally, we give the integer seeds of the examples we introduced in the previous subsection, as well as the value of λ we used to balance R and H.

3.5.1. *Structure of the set of roots modulo a prime power.* In this paragraph, we explain that the roots of a polynomial with integral coefficients modulo successive powers of a prime form a tree, and we present some properties of this tree. Let P be a polynomial with integral coefficients, let p be a prime integer.

Notice that if $x \in \mathbb{Z}/p^k\mathbb{Z}$ is a root of P for an integer $k \geq 2$, then $x \bmod p^{k-1}$ is a root of P modulo p^{k-1}. Therefore, we can see $x \bmod p^{k-1}$ as the parent of x in a tree containing every root of P modulo the powers of p. We give in Figure 6 an example of such a tree taken from [43, Section 2.6], and another example in Figure 7. The tree can be represented in levels made of the nodes of same depth, i.e. the roots of P modulo a specific power of p. We set the depth of the initial root mod p to be 1 so that it matches the exponent p^1.

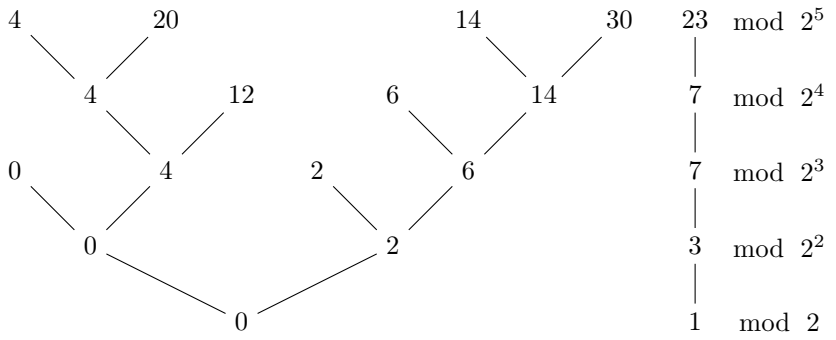


FIGURE 7. Trees of roots of $X^3 - 25X^2 + 70X - 522$ modulo powers of 2.

We can see from the figures that every root of P modulo p gives rise to a tree. We can also see that there are two types of trees: one kind where each node has a unique child, and the other kind where a node has either multiple children or none. The behavior of the tree depends on the multiplicity of the root. In the case where P has a simple root α_0 modulo p, Hensel's lemma [26, Section 3.4] states that each node has a unique child, and gives an algorithm to recover it.

When P has a root α_0 modulo p with multiplicity greather than 2, the following proposition from [43, Section 2.6] states that a node in the tree above α_0 has either p children or none:

Proposition 4. *Let $a \in \mathbb{Z}$ be a singular root of a polynomial $P \in \mathbb{Z}[X]$ modulo a prime power p^k. Then either a lifts to p roots modulo p^{k+1} or a lifts to no roots.*

For example on Figure 6, 1 is a multiple root of $X^2 + X + 223$ modulo 3, and in Figure 7, 0 is a multiple root of $X^3 - 25X^2 + 70X - 522$. They give rise to a non-degenerate tree. In Figure 7, 1 is a simple root, and gives rise to a degenerate tree like a linked list.

3.5.2. *Representation of the set of roots modulo a prime power.* Computing the roots of a polynomial P modulo p^k, where p is a prime, means computing the k-th level of the tree of roots of P modulo powers of p. We have seen in Figure 7 that the number of roots can grow quickly. In our case, the polynomials that we are interested in may have a large denominator, meaning that p can be quite large as well. Therefore, we have to find a way to store the roots in a way minimizing the amount of space required. For example, in Figure 6, we can represent the solutions modulo 3^4 by simply giving the node with label 4 at depth 2, and saying that $x \in \mathbb{Z}/3^4\mathbb{Z}$ is a root of P if and only if $x \equiv 4 \bmod 3^2$. As an other example, to represent the roots modulo 3^5, we can see that $x \in \mathbb{Z}/3^5\mathbb{Z}$ is a solution if and only if $x \equiv 4 \bmod 3^3$ or $x \equiv 22 \bmod 3^3$. Therefore, we can represent the roots by giving the two nodes 4 and 22 at depth 3.

Remark 8. We can look at this representation from the point of view of p-adic geometry ([26] for a reference). Then, saying that an integer $x \in \mathbb{Z}$ equals a modulo p^j means that $x \in D(a, p^{-j})$ where $D(a, p^{-j})$ is the disk of centre a and radius p^{-j} in $\mathbb{Q}_p$. Our representation can be interpreted as the covering of the preimage of $D(0, p^{-k})$ under P with a minimal number of disks. This point of view suggests

that our representation will have good properties for computing inclusions and intersections, as $\mathbb{Q}_p$ is an ultrametric space.

Remark 9. We used this particular representation to store the minimum amount of information possible. Therefore, it would be counterproductive to use the CRT to reassemble the roots of P' modulo Δ, instead of keeping everything under this compressed form. This means that, for example, when we use the family to generate curves, we have to iterate on the integer seeds using the representation modulo different prime powers, which is in fact not so difficult.

Example 13. Let $P = (X^2+2364019242458802X+39688175156984422)/68398769951398683$. Let $P' = X^2+2364019242458802X+39688175156984422$ and $\Delta = 68398769951398683 = 3^5 \times 16777259^2$. We find that $P' \equiv X^2 + X + 223 \bmod 3^5$ and $P' \equiv (X-1)^2 \bmod 16777259^2$. Therefore, P' has a multiple root modulo 16777259 which lifts modulo 16777259^2. Then, from Figure 6, we know that P takes integer values at an integer x if and only if $x \equiv 4, 22 \bmod 3^3$ and $x \equiv 1 \bmod 16777259$. Here it is convenient to avoid storing the 16777259 roots above 1 in the tree of roots modulo powers of 16777259. Instead, we store triplets $(4,3,3)$, $(22,3,3)$ and $(1,16777259,1)$ where (x,p,j) encodes the roots in the class $x \bmod p^j$ that make P' vanish modulo p^k. Note that here we have $j < k$, which means that we have saved some memory space.

3.5.3. *Computing the roots of a polynomial modulo a prime power.* In this paragraph, we finally explain how to compute the set of roots of a polynomial with integral coefficients modulo a prime power, under the representation from the last paragraph. Let p be a prime integer and k be a positive integer. In our experiments we encoutered some highly tricky cases and these situations led us to the following strategy to handle these technicalities. This section can be skipped on first read. More precisely, lifting the simple and multiple roots with a Panayi's like algorithm[1] does not end in all cases in a compressed form of roots and that caused memory issues in our implementation.

Let us first define

$$\mu(P) = \sup\{j \in \mathbb{Z}_+ \mid \forall x \in \mathbb{Z}, P(x) \equiv 0 \bmod p^j\} \ . \tag{3.6}$$

Our Algorithm 3.2 will essentially sum up to computing $\mu(P)$, or more realistically a good lower approximation of $\mu(P)$ for any P.

First, the content of the polynomial P obviously impacts $\mu(P)$. Let $\nu = \mathrm{val}_p(\mathrm{cont}(P))$, then $\mu(P) \geq \nu$. Moreover, $\mu(P/p^\nu) = \mu(P) - \nu$, therefore we only have to consider the case where p and the content of P are coprime. We have the following:

Proposition 5. *Let P be a polynomial with integral coefficients, and let p be a prime integer such that cont(P) and p are coprime. Let $\tilde{P} = P \bmod p$, and let $\tilde{P} = (X^p - X)^j \tilde{Q}$ where $\tilde{Q}$ and $X^p - X$ are coprime in $\mathbb{F}_p[X]$. Then $1 \leq \mu(P) \leq j$. Moreover, let $Q \in \mathbb{Z}[X]$ be a polynomial mapping to $\tilde{Q} \in \mathbb{F}_p[X]$, and let $R = P - (X^p - X)^j Q \in \mathbb{Z}[X]$. Then cont$(R) \geq 1$, and $\mu(P) \geq \min(j, \mu(R))$.*

Proof. We first prove that μ satisfies the following:

(1) $\mu(P) = \infty$ iff $P = 0$.

[1] we learned that this folklore algorithm is attributed to Peter Panayi who wrote a PhD thesis entitled *Computation of Leopoldt's p-adic regulator* at the University of East Anglia in 1995.

(2) $\forall P, Q \in \mathbb{Z}[X], \mu(PQ) \geq \mu(P) + \mu(Q)$.
(3) $\forall P, Q \in \mathbb{Z}[X], \mu(P+Q) \geq \min(\mu(P), \mu(Q))$.

Notice that $\mu(P) = \min_{x \in \mathbb{Z}} \nu_p(P(x))$, where ν_p is the p-adic valuation on $\mathbb{Z}$. Then (1) is easily verified. Let $P, Q \in \mathbb{Z}[X]$, then

$$\begin{aligned}\mu(PQ) &= \min_{x\in\mathbb{Z}} \nu_p(PQ(x)) = \min_{x\in\mathbb{Z}} \ (\nu_p(P(x)) + \nu_p(Q(x))) \\ &\geq \min_{x\in\mathbb{Z}} \nu_p(P(x)) + \min_{x\in\mathbb{Z}} \nu_p(Q(x)) = \mu(P) + \mu(Q) \quad (2)\end{aligned}$$

$$\begin{aligned}\mu(P+Q) = \min_{x\in\mathbb{Z}} \nu_p(P(x)+Q(x)) &\geq \min_{x\in\mathbb{Z}} \ \min(\nu_p(P(x)), \nu_p(Q(x))) \\ &\geq \min(\min_{x\in\mathbb{Z}} \nu_p(P(x)), \min_{x\in\mathbb{Z}} \nu_p(Q(x))) = \min(\mu(P), \mu(Q)) \quad (3)\end{aligned}$$

Then, with the notation of the proposition, $P = (X^p - X)^j Q + R$, so $\mu(P) \geq \min(\mu((X^p - X)^j Q), R) = \min(j, \mu(R))$. □

Corollary 1. *Let P be a polynomial with integral coefficients, and let p be a prime integer such that cont(P) and p are coprime. Then there exists integers j_0, j_1, ..., j_{j_0-1} and polynomials Q_0, Q_1, ..., Q_{j_0-1}, R, such that*

$$P = (X^p - X)^{j_0} Q_0 + p(X^p - X)^{j_1} Q_1 + ... + p^{j_0-1}(X^p - X)^{j_{j_0-1}} Q_{j_0-1} + p^{j_0} R.$$

Moreover, $\mu(P) >= \min\{j_0, j_1 + 1, ..., j_{j_0-1} + j_0 - 1\}$.

Generally, if we compute $\min\{j_0, j_1+1, ..., j_{j_0-1}+j_0-1\}$, the result will be equal to $\mu(P)$. During our enumeration, we never encountered a polynomial where the two values were different. Therefore, we designed a recursive algorithm (Alg. 3.2) to compute a good approximation of $\mu(P)$.

Algorithm 3.2: Approx-$\mu(P, p, depth, m)$

Initial call: Approx-$\mu(P, p, 0, +\infty)$ **Input:** $P \in \mathbb{Z}[X]$, p a prime integer, *depth* a variable initialized at 0 storing the global content of the term in the recursion, m the current minimum in the recursion, initialized at $+\infty$
Let $c = \nu_p(\text{cont}(P))$
$depth \leftarrow depth + c$
$P \leftarrow P/p^c$
Let j be the largest integer such that $(X^p - X)^j$ divides P mod p
$m \leftarrow \min(m, depth + j)$
if $m \leq depth + 1$ `// at which point the minimum stops decreasing`
then
  Return m
else
  Compute $Q \in \mathbb{Z}[X]$ such that $(X^p - X)^j Q = P$ mod p.
  Let $R = P - (X^p - X)^j Q$
  Return Approx-$\mu(R, p, depth, m)$

Now we come back to the main algorithm (computing the roots of P modulo Δ). The idea is that we can use μ and some substitutions to climb the tree of roots until we find the correct congruence relations to describe the set of roots.

Proposition 6. *Let P be a polynomial with integral coefficients, and let p be a prime integer. Let i be a positive integer. Let a be an integer such that $P(a) \equiv 0 \bmod p^i$. Let $P' = P(p^i X + a)$. Then, $\mu(P') = \max\{j \in \mathbb{Z}_+ \mid \forall x \in \mathbb{Z}$ such that $x \equiv a \bmod p^i, P(x) \equiv 0 \bmod p^j\}$.*

If we make two substitutions in a row, for example $pX + a$ then $pX + b$, the combined substitution is $X \mapsto p^2X + pb + a$ and the congruence relation in $\mu(P')$ is $x \equiv a + pb \bmod p^2$. Therefore, this kind of substitutions allows to climb the tree of roots modulo powers of p until we have $\mu(P') \geq k$.

We can give the idea of the algorithm with the example from Figure 6:

Example 14. Let $P = X^2 + X + 223$, $p = 3$ and $k = 5$. We want to find the roots of P modulo 3^5. We can compute $\mu(P) = 0$, therefore $\mathbb{Z}$ is not the answer. We have $P \equiv (X-1)^2 \bmod 3$, so 1 is a multiple root of P modulo 3, and the only root. Therefore we make the substitution $P \leftarrow P(3X+1) = 9X^2 + 9X + 225$, and our result becomes $\{(1, 3, 1)\}$. Now $3^2 \mid \mathrm{cont}(P)$, so $P \leftarrow P/3^2 = X^2 + X + 25$ and $k \leftarrow k - 2 = 3$. Still, $\mu(P) = 0$ and $P \equiv (X-1)^2 \bmod 3$, so we substitute $P \leftarrow P(3X+1) = 9X^2 + 9X + 27$, and our result becomes $\{(1+3, 3, 1+1)\} = \{(4, 3, 2)\}$. Similarly, $3^2 \mid \mathrm{cont}(P)$, so $P \leftarrow P/3^2 = X^2 + X + 3$ and $k \leftarrow k - 2 = 1$. We once more have $\mu(P) = 0$, but this time $P \equiv (X-2)X \bmod 3$. Since $k = 1$ here, it is not necessary to continue further. The substitutions $X \mapsto 3X$ and $X \mapsto 3X + 2$ give the desired result of $\{(4 + 0, 3, 2 + 1), (4 + 2 \cdot 3^2, 3, 2 + 1)\} = \{(4, 3, 3), (22, 3, 3)\}$.

Algorithm 3.3: RootsModPrimePowers($P, p, k, root, depth$)

Input: $P \in \mathbb{Z}[X]$, p a prime integer, k the power of p, *root* and *depth* are variables that store where we are in the tree of roots during the recursion

```
Let c = ν_p(cont(P))
P ← P/p^c
Let μ = Approx-μ(P, p, 0, ∞)
if k ≤ c + μ then
    Add (depth, root) to the list of solutions.
else
    for 0 ≤ r ≤ p − 1, root of P mod p do
        Run
          RootsModPrimePowers(P(pX + r), p, k − c, root + r p^depth, depth + 1)
```

3.5.4. *Checking if a polynomial represents primes.* The first three conditions from the Buniakowski–Schinzel conjecture (2.3) can be easily verified. The previous paragraph dealt with condition 4. Therefore, we mainly need to understand how we can verify that no prime integer divides every integer value of a polynomial P. We can assume that we know the integer seeds of P. Let Δ be the denominator of P. First fix a positive integer N. Compute d the greatest common divisor of N integer values of P. If d is 1 then there is nothing more to do. If $d > 1$ then let p be a prime dividing d. There are two possibilities: $p \mid \Delta$ or $p \nmid \Delta$. If $p \nmid \Delta$ then P can be projected onto a polynomial $\tilde{P}$ in $\mathbb{F}_p[X]$ by taking its coefficients modulo p. Then p is a divisor of every integer values of P iff $\tilde{P}$ evaluates to 0 at every element in $\mathbb{F}_p$

$$\text{iff } \tilde{P} \equiv 0 \bmod X^p - X \text{ in } \mathbb{F}_p[X].$$

If $p \mid \Delta$ then define $P' = \Delta P$. Let k_p be the valuation of p in Δ and let

$$L_p^{k_p} = \{x \in \mathbb{Z}/p^{k_p}\mathbb{Z} \mid P'(x) = 0\} \text{ and } L_p^{k_p+1} = \{x \in \mathbb{Z}/p^{k_p+1}\mathbb{Z} \mid x \bmod p^{k_p} \in L_p^{k_p}\}.$$

Then p is a divisor of every integer values of P if and only if for every $x \in L_p^{k_p+1}$ we have $P'(x) = 0$. We only have to compare $L_p^{k_p+1}$ and the set of roots of P' modulo p^{k_p+1}. Since $L_p^{k_p}$ and $L_p^{k_p+1}$ share the same representation with our representation method, and that we mentionned in Remark 8 that computing inclusions was not difficult, we do not have anything to add. We get the following algorithm:

Algorithm 3.4: Ensuring $\gcd(\{f(x) \mid x, f(x) \in \mathbb{Z}\}) = 1$

Input: $P \in \mathbb{Q}[X]$ a polynomial with denominator Δ, $N \in \mathbb{Z}$, $(L_p^{k_p})_{p|\Delta}$

$d = 0$;
for N *repetitions* **do**
  Pick a random element π in $\prod_{p|\Delta} L_p^{k_p}$;
  Let x be a representant in the equivalence class $CRT(\pi)$;
  $d = \gcd(d, P(x))$;
if $d = 1$ **then**
  Return True;
Let $\mathcal{P}$ be the set of prime divisors of d, trivial_gcd = True, and let $i = 0$;
while *trivial_gcd and* $i < \#\mathcal{P}$ **do**
  Let $p = \mathcal{P}[i]$ and let $i = i + 1$;
  if $p \mid \Delta$ **then**
    Let $P' = \Delta P$;
    Compute $\Lambda_p^{k_p+1}$ the set of roots of P' modulo p^{k_p+1};
    trivial_gcd=not $L_p^{k_p} \subset \Lambda_p^{k_p+1}$;
  else
    Let $\tilde{P}$ be the projection of P in $\mathbb{F}_p[X]$;
    trivial_gcd=not $\tilde{P} \equiv 0 \bmod X^p - X$
Return trivial_gcd ;

3.5.5. *Managing families with large denominators.* It is important to keep in mind that we want the families we computed to be able to generate pairing-friendly curves of a specific size. Two main obstacles are known in the litterature (for example see [22]): the degree of the polynomial R and the magnitude of the denominator of Q (which is related to the denominator of every polynomial in the family). In this paragraph, we elaborate on these obstacles and give a criterion telling if a family will be able to produce curves of a given size. First, we have seen that the set of integer seeds of a family is periodic. The LCM of the denominators of Q, T and Y is a period of this set, but usually not the smallest one.

Definition 4. Let Q, R, T, Y, H be a family of pairing-friendly curves. We call Π the smallest period of the set of integer seeds of the family. We call π the ratio of integer seeds by period of Π: $\pi = \#\{\text{integer seeds modulo } \Pi\}/\Pi$.

It is not difficult to see that Π is well-defined. It better describes the difficulty of finding curves of a certain size (of $q = Q(x_0)$ and $r = R(x_0)$) than the denominator.

For example, among the three families with embedding degree $k = 22$ we provided, Example 6 has a larger denominator than Example 7 while its period is smaller.

Let Q, R, T, Y, H be a family of pairing-friendly elliptic curves. Let d be the degree of R, Π the smallest period of the set of seeds of the family, and π the ratio of integer seeds per period of Π. Let n and N be two positive integers. Let λ be the denominator of R. We want to know if there are N integer seeds $x \in \mathbb{Z}$ such that $R(x)$ has size n. $R(x)$ has size n if x has size $(n + \log(\lambda))/d$ (here we assume $R \approx X^d/\lambda$). There are approximately $2^{(n+\log\lambda)/d}$ positive integers x of the correct size, and $2^{(n+\log\lambda)/d+1}$ integers in total. On the other hand, we need to consider N/π integers to find N integer roots. Therefore, we need:

$$N/\pi \leq 2^{(n+\log\lambda)/d+1},$$

or taking the logarithm:

$$d\log(1/\pi) - \log\lambda \leq n + d(1 - \log N).$$

4. Our new pairing-friendly curve families made practical

In this section we aim at instanciating our new pairing-friendly curve families at cryptographic sizes, and implementing the optimal ate pairing on them. We presented several new families in subsection 3.4. We focus on two families of embedding degree $k = 20$ (Example 11, Example 12 that we name GG20a and GG20b) and one of embedding $k = 22$ (Example 6 named GG22D7).

4.1. **Finding Seeds.**

The first step is to get seeds x_0 so that the parameters $Q(x_0), R(x_0)/\lambda$ are prime integers of cryptographic size. Moreover it is usefull to be able to generate *sparse seeds*, that have a very small Hamming weight in (signed) binary form. For that we use the Python/SageMath scripts available at [31] under `sage/tnfs/gen/generate_sparse_curve.py`. If we target the 192-bit security level, r should be about 384-bit long. We obtain the seeds in Table 5. For GG20a and GG20b we present the seeds of smallest possible Hamming weight such that $q = Q(x_0)$ is at most 576-bit long (9 limbs of 64-bits). It implies $r = R(x_0)$ of 379 or 380 bits (almost 384 bits). For GG22D7 we obtain only one seed so that r is close to 384 bits.

curve	seed	$\log q$	$\log r$	ρ	$\log q^k$	sec. $\mathbb{F}_{q^k}$
GG20a	$-(2^{49} + 2^{46} + 2^{41} + 2^{18} + 2^3 + 2^2 + 1)$	576	379	1.52	11520	196
GG20a	$2^{49} + 2^{46} + 2^{44} + 2^{40} + 2^{34} + 2^{27} + 2^{14} + 1$	576	380	1.52	11500	196
GG20b	$-2^{49} - 2^{45} - 2^{42} - 2^{36} + 2^{11} + 1$	575	379	1.52	11500	196
GG20b	$-2^{49} + 2^{46} - 2^{41} + 2^{35} + 2^{30} - 1$	575	379	1.52	11500	196
GG20b	$-2^{49} - 2^{47} + 2^{45} - 2^{27} - 2^{22} - 2^{18} - 1$	576	380	1.52	11520	196
GG22D7	$-2^{20} + 2^{18} + 2^{13} - 2^{10} - 2^8 - 2^2 + 1$	457	383	1.19	10054	220

Table 5. Parameters of our new curves at the 192-bit security level.

4.2. **Pairing formulas on our new curves.**

4.2.1. *Recap on Optimal Ate Pairing Computation.* The fastest known pairing in a standard setting is Vercauteren's *optimal ate pairing* [46], a variant of the Tate pairing. Other pairings such as α-Weil or β-Weil pairings might be competitive in parallel computation, but we do not consider this case. First, define $\mathbb{G}_1$ as the order-r subgroup over $\mathbb{F}_q$, $\mathbb{G}_1 = E(\mathbb{F}_q)[r] = E[r] \cap \ker(\pi - [1])$ where $\pi\colon (x, y) \mapsto (x^q, y^q)$ is the Frobenius endomorphism on E, and define $\mathbb{G}_2$ as the trace-zero subgroup of order r over $\mathbb{F}_{q^k}$, $\mathbb{G}_2 = E[r] \cap \ker(\pi - [q])$. With the LLL lattice reduction algorithm, obtain short vectors of the lattice spanned by the rows of the matrix

$$M = \begin{bmatrix} r & 0 & \dots & \dots & 0 \\ -q & 1 & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 & 0 \\ 0 & \dots & 0 & -q & 1 \end{bmatrix}_{\varphi(k)\times\varphi(k)}$$

With LLL, the shortest vector has coefficients bounded by $Cr^{1/\varphi(k)}$ where C depends on the dimension of the lattice and the LLL parameters (δ, γ). A row $(c_0, c_1, \dots, c_{\varphi(k)-1})$ of short vectors gives the formula, with some integers m, λ,

$$c_0 + c_1 q + c_2 q^2 + \ldots + c_{\varphi(k)-1} q^{\varphi(k)-1} = \lambda = mr = 0 \bmod r \ .$$

The optimal ate pairing formula is given by Theorem 3, where $f_{c,Q}(P)$ denotes a Miller function whose divisor is $\mathrm{div}(f_{c,Q}) = c(Q) - ([c]Q) - (c-1)(\mathcal{O})$, evaluated at the point P. In other words, the function $f_{c,Q}$ has a zero of order c at Q, a pole of order 1 at $[c]Q$, and a pole of order $(c-1)$ at the point at infinity $\mathcal{O}$. The classical formulas are $f_{1,Q} = 1$; $f_{i+j,Q} = f_{i,Q} \cdot f_{j,Q} \cdot \ell_{iQ,jQ}/v_{(i+j)Q}$ where $\ell_{iQ,jQ}$ denotes the line equation through iQ and jQ, and $v_{(i+j)Q}$ denotes the vertical line at $(i+j)Q$; and $f_{ij,Q} = f_{i,Q}^{j} \cdot f_{j,[i]Q}$.

Theorem 3 ([46])**.** *Let $\lambda = mr$ with $r \nmid m$ and write $\lambda = \sum_{i=0}^{l-1} c_i q^i$ then*

(4.1)

$$a_{[c_0,\dots,c_l]}\colon \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r\colon (Q, P) \mapsto \left(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} \frac{\ell_{[s_{i+1}]Q,[c_i q^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{(q^k-1)/r}$$

with $s_i = \sum_{j=i}^{l} c_j q^j$, defines a bilinear pairing, where $\ell_{Q_i,Q_j}(P)$ denotes the line equation through the points Q_i, Q_j evaluated at the coordinates of the point P, and $v_{Q_i}(P)$ is the vertical line through the point Q_i evaluated at the coordinates of P. Furthermore, if

$$mkq^{k-1} \not\equiv ((q^k - 1)/r) \cdot \sum_{i=0}^{l} i c_i q^{i-1} \bmod r \ ,$$

then the pairing is non-degenerate.

In the following subsections, we apply Theorem 3 to our new curves. The computation of a Miller function $f_{c,Q}(P)$ is explained in subsection 4.4 and algorithm 4.1. Because our curves have even embedding degrees, we omit the vertical lines $v_{Q_i}(P)$ in the formulas (see subsubsection 4.3.1 and subsubsection 4.3.3).

4.2.2. *Optimal Ate Pairing Formulas for our new $k = 20$ curves.* For the first $k = 20$ curve family (GG20a), we get

$$x - q(x) + 2(q(x))^6 \equiv 0 \bmod r(x) \tag{4.2}$$

hence the formula, where $\pi(Q) = [q]Q$, $\pi^6(Q) = [q^6]Q$:

$$e(P,Q) = f_{x,Q}(P) f_{-1,\pi(Q)}(P) f_{2,\pi^6(Q)}(P) \ell_{[x]Q,-\pi(Q)}(P) \ell_{xQ-\pi(Q),\pi^6([2]Q)}(P) \ .$$

Well-known simplifications apply: $f_{-1,\pi(Q)}(P)$ can be dropped off, and the same for the line $\ell_{xQ-\pi(Q),\pi^6([2]Q)}(P)$ as it will be a vertical. Moreover, $f_{2,\pi^6(Q)}(P)$ costs a double-line step $\ell_{\pi^6(Q),\pi^6(Q)}(P) = \ell^{q^6}_{Q,Q}(P)$. Finally,

$$e(P,Q) = f_{x,Q}(P) \ell^{q^6}_{Q,Q}(P) \ell_{[x]Q,\pi(-Q)}(P) \ . \tag{4.3}$$

For the second $k = 20$ family (GG20b), we obtain a similar formula, only a sign changes:

$$x - q(x) - 2(q(x))^6 \equiv 0 \bmod r(x) \tag{4.4}$$

$$e(P,Q) = f_{x,Q}(P) \ell^{q^6}_{-Q,-Q}(P) \ell_{[x]Q,\pi(-Q)}(P) \ . \tag{4.5}$$

The final exponentiation is decomposed into two parts, called easy and hard:

$$\frac{q^{20}-1}{r} = \frac{q^{20}-1}{\phi_{20}(q)} \frac{\phi_{20}(q)}{r} = \underbrace{(q^{10}-1)(q^2+1)}_{\text{easy}} \underbrace{\frac{\phi_{20}(q)}{r}}_{\text{hard}} \ .$$

The easy part costs one inversion and a few Frobenius powers. We apply the technique of Fuentes et al. [23] to simplify the hard pard. We note that $q^8 = q^6 - q^4 + q^2 - 1 \bmod \Phi_{20}(q)$ and after some ad-hoc improvements, we obtain the following exponents e_a, e_b for GG20a, resp. GG20b that are multiples of the hard part $\Phi_{20}(q)/r$ and coprime to r.

$$\begin{aligned}
e_a =& (x^6 - 2x^5 + 5x^4 + 328) \\
& \times (-41q^2 + xq(7 - 24q^5) + x^2(11 - 2q^5) + x^3q^4(4 - 3q^5) + x^4q^3(2 + q^5) + x^5q^7) \\
& + (x^2 - 2x + 5) \\
& \times (625q(2 - q^5) + 125x(4 + 3q^5) + 25x^2q^4(11 + 2q^5) + 5x^3q^3(7 + 24q^5) + 38x^4q^7) \\
& + 6724q^7
\end{aligned}$$

$$\begin{aligned}
e_b =& (x^6 - 2x^5 + 5x^4 - 328) \\
& \times (-41q^2 + xq(7 + 24q^5) + x^2(11 + 2q^5) - x^3q^4(4 + 3q^5) + x^4q^3(-2 + q^5) + x^5q^7) \\
& + (x^2 - 2x + 5) \\
& \times (-5^4q(q^5 + 2) + 5^3x(-4 + 3q^5) + 5^2x^2q^4(11 - 2q^5) + 5x^3q^3(7 - 24q^5) - 38x^4q^7) \\
& + 6724q^7
\end{aligned}$$

4.2.3. *Optimal Ate Pairing Formulas for our new $k = 22$ curve.* For our new $k = 22$ curve with $D = 7$, we get

$$x^2 - xq(x) + 2(q(x))^2 \equiv 0 \bmod r(x) \tag{4.6}$$

hence the optimal ate Miller loop formula

$$e(P,Q) = f_{x^2,Q}(P) f_{-x,\pi(Q)}(P) f_{2,\pi^2(Q)}(P) \ell_{[x^2]Q,-\pi([x]Q)}(P) \ell_{x^2Q-\pi([x]Q),\pi^2([2]Q)}(P)$$

and the latter line can be removed as it is a vertical. Finally,

$$e(P,Q) = f_{x^2,Q}(P) f_{x,Q}^{-q}(P) \ell_{Q,Q}^{q^2}(P) \ell_{[x^2]Q,-\pi([x]Q)}(P) \ . \tag{4.7}$$

Moreover one can share the computation of $f_{x,Q}$ inside $f_{x^2,Q}$:

$$e(P,Q) = f_{x,Q}^{x}(P) f_{x,[x]Q}(P) f_{x,Q}^{-q}(P) \ell_{Q,Q}^{q^2}(P) \ell_{[x^2]Q,-\pi([x]Q)}(P) \ . \tag{4.8}$$

For the final exponentiation, we apply the same technique ([23]) and we obtain

$$\begin{aligned} e =& (x^{12} - x^{11} + 2x^{10} + 161) \cdot (-23q^8 + 11xq^7 + 17x^2q^6 + 3x^3q^5 - 7x^4q^4 - 5x^5q^3 \\ &+ x^6q^2 + 3x^7q + x^8 + x^9q^{10} + x^{10}q^9) \\ &+ (x^2 - x + 2) \cdot (2^{10}q^7 + 2^9xq^6 - 2^8x^2q^5 - 3 \cdot 2^7x^3q^4 - 2^6x^4q^3 + 5 \cdot 2^5x^5q^2 \\ &+ 7 \cdot 2^4x^6q - 3 \cdot 2^3x^7 + 17 \cdot 2^2x^8q^{10} + 11 \cdot 2x^9q^9) \end{aligned}$$

Finally we mention that Fouotsa et al. x-super-optimal ate pairing [20] can apply to this curve but we did not investigate further.

4.3. **Twisted curves, $\mathbb{G}_2$ representation, and finite field extensions.**

4.3.1. *Twisted curve and sparse $\mathbb{G}_2$ representation for $k = 20$.* Our new GG20 curves have j-invariant 1728 (discriminant $D = 1$) and short Weierstrass curve equation $E\colon y^2 = x^3 + ax$ ($b = 0$). In this case, points in $\mathbb{G}_2$ can be represented in sparse form thanks to a quartic twist. There are two choices of quartic twist. Let $t = T(x_0)$ be the trace of E over $\mathbb{F}_q$ and let t_5 be the trace of E over F_{q^5}, $t_5 = t^5 - 5qt^3 + 5q^2t$. Let y_5 be the square-free part of $t_5^2 - 4q^5 = -Dy_5^2$, $y_5 = y(t^4 - 3pt^2 + p^2)$ where $t^2 - 4q = -Dy^2$. The two possible quartic twist orders are $q^5 + 1 + y_5$ and $q^5 + 1 - y_5$. By construction, one quartic twist curve has order multiple of $r = R(x_0)$ and with our choice of $y = Y(x_0)$ and y_5, this is $q^5 + 1 + y_5$.

A quartic D-twist of E over $\mathbb{F}_{q^5}$ is defined by $E'_D\colon y'^2 = x'^3 + a/w$ where the curve coefficient a is divided by w hence the name D, and $w \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$ is such that $X^4 - w$ is irreducible over $\mathbb{F}_{q^5}$. Let $\omega \in \mathbb{F}_{q^{20}}$ such that $\omega^4 = w$ and $\#E'_D(\mathbb{F}_{q^5}) = q^5 + 1 + y_5$. Let $Q'(x', y') \in E'_D(\mathbb{F}_{q^5})$. Then $Q = \phi(Q') = (x'\omega^2, y'\omega^3)$ lies on $E(\mathbb{F}_{q^{20}})$. Moreover $x'\omega^2$ is in the subfield $\mathbb{F}_{q^{10}}$. The vertical line equation at Q evaluated at P is $v_Q(P) = x_Q - x_P = x'\omega^2 - x_P \in \mathbb{F}_{q^{10}}$. Because it is in a proper subfield of $\mathbb{F}_{q^{20}}$, it becomes 1 after the easy part of the final exponentiation. As elements of $\mathbb{F}_{q^{20}} = \mathbb{F}_{q^5}[\omega]$, $x'\omega^2$ and $y'\omega^3$ are sparse.

A quartic M-twist of E over $\mathbb{F}_{q^5}$ is defined by $E'_M\colon y^2 = x^3 + az$ where the curve coefficient a is multiplied by z hence the name M, and $z \in \mathbb{F}_{q^5} \setminus \mathbb{F}_q$ is such that $X^4 - z$ is irreducible over $\mathbb{F}_{q^5}$. Let $\zeta \in \mathbb{F}_{q^{20}}$ such that $\zeta^4 = z$ and $\#E'_M(\mathbb{F}_{q^5}) = q^5 + 1 + y_5$. Let $Q'(x', y') \in E'_M(\mathbb{F}_{q^5})$. Then $Q = \phi(Q') = (x'/\zeta^2, y'/\zeta^3)$ lies on $E(\mathbb{F}_{q^{20}})$. Moreover x'/ζ^2 is in the subfield $\mathbb{F}_{q^{10}}$. The vertical line equation at Q evaluated at P is $v_Q(P) = x_Q - x_P = x'/\zeta^2 - x_P \in \mathbb{F}_{q^{10}}$. Because it is in a proper subfield of $\mathbb{F}_{q^{20}}$, it becomes 1 after the easy part of the final exponentiation. As elements of $\mathbb{F}_{q^{20}} = \mathbb{F}_{q^5}[\zeta]$, $x'/\zeta^2 = x'/z\zeta^2$ and $y'/\zeta^3 = y'/z\zeta$ are sparse.

4.3.2. *Field extension representation for $k = 20$.* Let $q = 1 \bmod 5$ and let $\mathbb{F}_{q^5}$ be defined with an irreducible binomial polynomial $x^5 - v$ in $\mathbb{F}_q[x]$. Let ν be a root of $x^5 - v$, that is, $\nu = \sqrt[5]{v}$ (for some choice of fifth root). Elements of $\mathbb{F}_{q^5} = \mathbb{F}_q[x]/(x^5 - v)$ can be represented as degree 4 polynomials modulo $x^5 - v$ or once ν is set, as $\vec{a} = a_0 + a_1\nu + a_2\nu^2 + a_3\nu^3 + a_4\nu^4$, where $a_i \in \mathbb{F}_q$. Let $x^4 - w$ be an irreducible polynomial in $\mathbb{F}_{q^5}[x]$, where $w \in \mathbb{F}_{q^5}$. Let ω be a root of $x^4 - w$ in

$\mathbb{F}_{q^{20}}$. Elements of $\mathbb{F}_{q^{20}}$ are represented as degree 3 polynomials modulo $x^4 - w$ with coefficients in $\mathbb{F}_{q^5}$ or as $\vec{a_0} + \vec{a_1}\omega + \vec{a_2}\omega^2 + \vec{a_3}\omega^3$, where $\vec{a_i} \in \mathbb{F}_{q^5}$.

Example 15 ((GG20b575a)). We take as example the curve GG20b whose seed is $u = -2^{49} - 2^{45} - 2^{42} - 2^{36} + 2^{11} + 1$. We define $\mathbb{F}_{q^5} = \mathbb{F}_q[x]/(x^5 - 2)$ and set ν a root of $x^5 - 2$ in $\mathbb{F}_{q^5}$. There are two options to define the quartic extension: on top of $\mathbb{F}_q$ or on top of $\mathbb{F}_{q^5}$. We can define $\mathbb{F}_{q^4} = \mathbb{F}_q[x]/(x^4 - 3)$ and set ω_D a root of $x^4 - 3$ in $\mathbb{F}_{q^4}$. We define $\mathbb{F}_{q^{20}} = \mathbb{F}_q[\nu, \omega_D]$. The quartic D-twist is $E'_D\colon y^2 = x^3 + a/(3\nu^4)x$ and the twisting map is $\phi_D\colon (x', y') \mapsto (x'\omega_D^2\nu^2, y'\omega_D^3\nu^3)$.

We can also define $\mathbb{F}_{q^4} = \mathbb{F}_q[x]/(x^4 - 11)$ and set ω_M a root of $x^4 - 11$ in $\mathbb{F}_{q^4}$. We define $\mathbb{F}_{q^{20}} = \mathbb{F}_q[\nu, \omega_M]$. The quartic M-twist is $E'_M\colon y^2 = x^3 + a(11\nu^4)x$ and the twisting map is $\phi_M\colon (x', y') \mapsto (x'/(\omega_M^2\nu^2), y'/(\omega_M^3\nu^3))$.

For Frobenius powers, $\nu^q = \nu^{5\frac{q-1}{5}}\nu = 2^{\frac{q-1}{5}}\nu$ where $2^{\frac{q-1}{5}} \in \mathbb{F}_q$ is precomputed. Also, $\omega_D^q = \omega_D^{4\frac{q-1}{4}}\omega_D = 3^{\frac{q-1}{4}}\omega_D$ where $3^{\frac{q-1}{4}} \in \mathbb{F}_q$ is precomputed. Note that $3^{\frac{q-1}{2}} = -1$. In the same way, $\omega_M^q = \omega_M^{4\frac{q-1}{4}}\omega_M = 11^{\frac{q-1}{4}}\omega_M$ where $11^{\frac{q-1}{4}} \in \mathbb{F}_q$ is precomputed. Note that $11^{\frac{q-1}{2}} = -1$. Moreover, $11^{\frac{q-1}{4}} = -3^{\frac{q-1}{4}}$.

A Frobenius power costs 18 multiplications in $\mathbb{F}_q$ ($\mathbf{f}_{20} = 18\mathbf{m}$), where 18 values in $\mathbb{F}_q$ shall be precomputed: the $(2^{i\frac{q-1}{5}}3^{j\frac{q-1}{4}})_{0\le i\le 4,\ 0\le j\le 3}$, except for $i = j = 0$ (the value is 1) and $i = 0$, $j = 2$ (the value is -1).

A usual alternative is to define $\mathbb{F}_{q^{20}}$ on top of $\mathbb{F}_{q^5}$. Let $\mathbb{F}_{q^{20}} = \mathbb{F}_{q^5}[x]/(x^4 - 3\nu)$. Let ω_D be a root in $\mathbb{F}_{q^{20}}$ of $x^4 - 3\nu$. The quartic D-twist is defined by $E'_D\colon y^2 = x^3 + a/(3\nu)x$ and the twisting map is $\phi_D\colon (x', y') \mapsto (x'\omega_D^2, y'\omega_D^3)$. Let $\mathbb{F}_{q^{20}} = \mathbb{F}_{q^5}[x]/(x^4 - 11\nu)$. Let ω_M be a root in $\mathbb{F}_{q^{20}}$ of $x^4 - 11\nu$. The quartic M-twist is defined by $E'_M\colon y^2 = x^3 + a(11\nu)x$ and the twisting map is $\phi_M\colon (x', y') \mapsto (x'/\omega_M^2, y'/\omega_M^3)$. A Frobenius power costs $\mathbf{f}_{20} = 18\mathbf{m}$ like before, with similar precomputations.

4.3.3. *Twisted curve and sparse $\mathbb{G}_2$ representation for $k = 22$.* Our new $k = 22$ curves $E\colon y^2 = x^3 + ax + b$ in short Weierstrass form have a quadratic twist defined over $\mathbb{F}_{q^{11}}$. Let t be the trace of E over $\mathbb{F}_q$. The trace of E over $\mathbb{F}_{q^{11}}$ is $t_{11} = t^{11} - 11qt^9 + 44q^2t^7 - 77q^3t^5 + 55q^4t^3 - 11q^5t$. The quadratic twist of E over $\mathbb{F}_{q^{11}}$ has order $q^{11} + 1 + t_{11}$ and by construction, its order is a multiple of $r = R(x_0)$. The quadratic M-twist is defined by $E'_M\colon y'^2 = x'^3 + aw^2x + bw^3$ where $w \in \mathbb{F}_{q^{11}} \setminus \mathbb{F}_q$ is not a square. Let ω in $\mathbb{F}_{q^{22}}$ be a root of $x^2 - w$. Let $Q'(x', y') \in E'_M(\mathbb{F}_{q^{11}})$. Then $Q = \phi(Q') = (x'/\omega^2, y'/\omega^3) = (x'/w, y'/w^2\omega)$ lies on $E(\mathbb{F}_{q^{22}})$. More precisely x'/w is in the subfield $\mathbb{F}_{q^{11}}$. The vertical line equation at Q evaluated at P is $v_Q(P) = x_Q - x_P = x'/w - x_P \in \mathbb{F}_{q^{11}}$. Because it is in a proper subfield of $\mathbb{F}_{q^{22}}$, it becomes 1 after the easy part of the final exponentiation. As elements of $\mathbb{F}_{q^{22}} = \mathbb{F}_{q^{11}}[\omega]$, x'/w and $y'/w^2\omega$ are sparse.

4.3.4. *Field extension representation for $k = 22$.* The polynomial shape of $q = Q(x_0)$ does not allow $q = 1 \bmod 11$ and finding an irreducible binomial polynomial is not possible. We have chosen the alternative with a sparse polynomial of the form $x^{11} + v_1x + v_0$ with tiny integers v_1, v_0. We represent elements of $\mathbb{F}_{q^{11}}$ as degree 10 polynomials modulo $x^{11} + v_1x + v_0$. The top extension $\mathbb{F}_{q^{22}}$ is represented as a quadratic extension of $\mathbb{F}_{q^{11}}$ with an irreducible quadratic polynomial $x^2 - w$, $w \in \mathbb{F}_{q^{11}}$.

Example 16 (GG22D7-457). With the seed $x_0 = -2^{20} + 2^{18} + 2^{13} - 2^{10} - 2^8 - 2^2 + 1$, $q = Q(x_0)$ is 457-bit long. We found the irreducible polynomials $x^{11} + x - 19$

and $x^{11} - 2x - 2$. Let ν be a root of either polynomial. Then $x^2 - \nu$ defines the quadratic extension. Let $\omega \in \mathbb{F}_{q^{22}}$ such that $\omega^2 = \nu$. The quadratic M-twist is $E'_M : y^2 = x^3 + a\nu^2 x + b\nu^3$. The twist map is $\phi_M : (x', y') \mapsto (x'/\nu, y'/\nu^2\omega)$.

A Frobenius power in this case is quite tedious, as $q = 3 \bmod 11$. We obtain $\mathbf{f}_{11} = 110\mathbf{m}$ and $\mathbf{f}_{22} = 21 \cdot 11\mathbf{m} = 231\mathbf{m}$.

4.4. **Miller function computation.** Miller algorithm (algorithm 4.1) computes a Miller function $f_{c,Q}(P)$. Because our curves have even embedding degrees, we omit the vertical lines $v_{Q_i}(P)$ in the formulas (see subsubsection 4.3.1 and subsubsection 4.3.3). Formulas for doubling step and addition step for our $k = 20$ curves can be found in Costello, Lange and Naehrig paper [16], and for $k = 22$ curves, in [13].

Algorithm 4.1: MillerFunction(c, P, Q)
Input: $E, \mathbb{F}_q, \mathbb{F}_{q^k}$, k even, $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})[r]$ such that $\pi(Q) = [q]Q$ in affine coord., $c \in \mathbb{Z}^*$.
Result: $f = f_{c,Q}(P)$

$f \leftarrow 1$; $R \leftarrow Q$;
if $c < 0$ **then** $R \leftarrow -R$; $c \leftarrow -c$;
for b *from the second most significant bit of* c *to the least* **do**
  $\ell_0 \leftarrow \ell_{R,R}(P)$; $R \leftarrow [2]R$; // Dbl step, tangent line
  $f \leftarrow f^2$; // $\mathbf{s}_k$
  if $b = 1$ **then**
    $\ell_1 \leftarrow \ell_{R,Q}(P)$; $R \leftarrow R + Q$; // Add step, chord line
    $f \leftarrow f \cdot (\ell_0 \cdot \ell_1)$; // $\mathbf{m}_k$ + sparse-sparse-$\mathbf{m}_k$
  else
    $f \leftarrow f \cdot \ell_0$; // full-sparse-$\mathbf{m}_k$
return f;

4.5. **SageMath proof-of-concept implementation.** We rely on SageMath for the finite field extension arithmetic. We base our implementation on the MIT-licensed library of pairings at [17]. We adapt the pairing computation on KSS16 curves to our $k = 20$ curves as they both have a quartic twist. More precisely we adapt `pairing.py` to our needs. Our implementation it available under MIT license at

https://gitlab.inria.fr/guillevi/pairings-on-gasnier-g-curves

We validated our pairing formulas (optimal ate Miller loop formulas, final exponentiation formulas) and checked that the pairing is bilinear.

4.6. **Pairing cost estimates.** We reproduce the results of [1], updated. The classical strategy is used to estimate a pairing computation cost in terms of multiplications and squarings in the base field $\mathbb{F}_q$. The costs of multiplication and squaring in the intermediate extensions are estimated in Table 6 ($\mathbb{F}_{q^5}$ and $\mathbb{F}_{q^{20}}$, $\mathbb{F}_{q^{11}}$ and $\mathbb{F}_{q^{22}}$ respectively). We denote $\mathbf{m}_i$, resp. $\mathbf{s}_i$ a multipliation, resp. squaring in $\mathbb{F}_{q^i}$. For degree 5 extension, [42] reports $\mathbf{m}_5 = 13\mathbf{m}$, $\mathbf{s}_5 = 13\mathbf{s}$. For degree eleven extension field $\mathbb{F}_{q^{11}}$, the Karatsuba rought estimate is $\mathbf{m}_{11} \geq 11^{\log_2 3} = 44.72$ but it seems more realistic from an implementation perspective to use [42, Eq. 6]: $\mathbf{m}_{11} = \mathbf{m}_5 + 2\mathbf{m}_6 - 1 = 48\mathbf{m}$ where $\mathbf{m}_5 = 13\mathbf{m}$ and $\mathbf{m}_6 = 18\mathbf{m}$. The quadratic extension $\mathbb{F}_{q^{22}}$ on top of $\mathbb{F}_{q^{11}}$ uses

k	$\mathbf{m}_k$	$\mathbf{s}_k$	$\mathbf{f}_k$	$\mathbf{s}_k^{\text{cyclo}}$	$\mathbf{i}_k - \mathbf{i}_1$	$\approx \mathbf{i}_k$
1	$\mathbf{m}$	$\mathbf{s}$	0	–	0	$25\mathbf{m}$
5	$13\mathbf{m}$ [42]	$13\mathbf{s}$ [42]	$4\mathbf{m}$	–	$3\mathbf{f}_5 + 2\mathbf{m}_5 + 10\mathbf{m} = 48\mathbf{m}$	$73\mathbf{m}$
10	$3\mathbf{m}_5 = 39\mathbf{m}$	$2\mathbf{m}_5 = 26\mathbf{m}$	$8\mathbf{m}$	$2\mathbf{s}_5 = 26\mathbf{s}$	$2\mathbf{m}_5 + 2\mathbf{s}_5 + \mathbf{i}_5 - \mathbf{i} = 74\mathbf{m} + 26\mathbf{s}$	$125\mathbf{m}$
20	$3\mathbf{m}_{10} = 117\mathbf{m}$	$2\mathbf{m}_{10} = 78\mathbf{m}$	$18\mathbf{m}$	$2\mathbf{s}_{10} = 52\mathbf{m}$	$2\mathbf{m}_{10} + 2\mathbf{s}_{10} + \mathbf{i}_{10} - \mathbf{i} = 255\mathbf{m}$	$280\mathbf{m}$
11	$48\mathbf{m}$ [42]	$48\mathbf{s}$ [42]	$110\mathbf{m}$	–	$5\mathbf{f}_{11} + 4\mathbf{m}_{11} + 22\mathbf{m} = 764\mathbf{m}$	$789\mathbf{m}$
22	$3\mathbf{m}_{11} = 144\mathbf{m}$	$2\mathbf{m}_{11} = 96\mathbf{m}$	$231\mathbf{m}$	$2\mathbf{s}_{11} = 96\mathbf{s}$	$2\mathbf{m}_{11} + 2\mathbf{s}_{11} + \mathbf{i}_{11} - \mathbf{i} = 860\mathbf{m} + 96\mathbf{s}$	$981\mathbf{m}$

TABLE 6. Relative cost of multiplication $\mathbf{m}_k$, squaring $\mathbf{s}_k$, Frobenius $\mathbf{f}_k$, and inversion $\mathbf{i}_k$ in finite field extensions. In the right-most column, $\mathbf{i}_k$ is estimated with $\mathbf{i}_1 = 25\mathbf{m}$, $\mathbf{s} = \mathbf{m}$.

the usual Karatsuba formula $\mathbf{m}_{22} = 3\mathbf{m}_{11}$, $\mathbf{s}_{22} = 2\mathbf{m}_{11}$. The quartic extension $\mathbb{F}_{q^{20}}$ on top of $\mathbb{F}_{q^5}$ uses recursively the Karatsuba quadratic formulas $\mathbf{m}_{20} = 3\mathbf{m}_{10} = 9\mathbf{m}_5$, $\mathbf{s}_{20} = 2\mathbf{m}_{10} = 6\mathbf{m}_5$.

Frobenius powers in $\mathbb{F}_{q^5}$ and $\mathbb{F}_{q^{20}}$ are cheap as the extensions use binomial polynomials. One has $\mathbf{f}_5 = 4\mathbf{m}$ and $\mathbf{f}_{20} = 18\mathbf{m}$. However in $\mathbb{F}_{q^{11}}$, $q = 3 \bmod 11$ and the irreducible polynomial has the form $x^{11} - 2x - 2$. Let ν be a root of $x^{11} - 2x - 2$, $\nu^q = \nu^{11\frac{q-3}{11}}\nu^3 = (2\nu+2)^{\frac{q-3}{11}}\nu^3$ so that $(a_0 + a_1\nu + \ldots + a_{10}\nu^{10})^q = a_0 + a_1\nu^q + \ldots + a_{10}\nu^{10q} = a_0 + a_1\delta_1\nu^3 + a_2\delta_2\nu^6 + a_3\delta_3\nu^9 + a_4\delta_4\nu + a_5\delta_5\nu^4 + a_6\delta_6\nu^7 + a_7\delta_7\nu^{10} + a_8\delta_8\nu^2 + a_9\delta_9\nu^5 + a_{10}\delta_{10}\nu^8$ where $\delta_1 = (2\nu+2)^{(q-3)/11}$, $\delta_i = \delta_1^i(2\nu+2)^{\lfloor 3i/11 \rfloor}$. Indeed, $\nu^{iq} = \nu^{11i(q-3)/11}\nu^{3i} = (2\nu+2)^{i(q-3)/11}(2\nu+2)^{\lfloor 3i/11 \rfloor}\nu^{3i \bmod 11}$. Precomputing the δ_is, it costs 10 multiplications of a $\mathbb{F}_q$ coefficient a_i times a $\mathbb{F}_{q^{11}}$ value δ_i, hence $110\mathbf{m}$.

Inversion in $\mathbb{F}_{q^5}$ is computed with the usual trick $x^{-1} = x^{q+q^2+q^3+q^4} / \mathrm{Norm}_{\mathbb{F}_{q^5}/\mathbb{F}_q}(x)$ ([38, page ix]) and the simplification $x^{q+q^2+q^3+q^4} = x^{q(q+1)(q^2+1)}$ that costs 3 Frobenius and 2 multiplications in $\mathbb{F}_{q^5}$. Once the numerator is computed, the norm costs 5 more multiplications in $\mathbb{F}_q$ as $\mathrm{Norm}(x) = x \cdot x^{q+q^2+q^3+q^4} \in \mathbb{F}_q$. Then five more multiplications in $\mathbb{F}_q$ are required to multiply the inverse of the norm to each of the five coefficients. The final count is $3\mathbf{f}_5 + 2\mathbf{m}_5 + 5\mathbf{m} + 5\mathbf{m} + \mathbf{i} = 48\mathbf{m} + \mathbf{i}$. Inversion in $\mathbb{F}_{q^{11}}$ is $x^{-1} = x^{\sum_{i=1}^{10} q^i} / \mathrm{Norm}_{\mathbb{F}_{q^{11}}/\mathbb{F}_q}(x)$ where the numerator simplifies as $q + \ldots + q^{10} = q(q^5+1)((q^2+1)(q+1)q+1)$ or $q(q+1)((q^4+1)(q^2+1)q^2+1)$ so it costs 5 Frobenius powers, 4 multiplications. The total cost is $5\mathbf{f}_{11} + 4\mathbf{m}_{11} + 22\mathbf{m} + \mathbf{i} = 764\mathbf{m} + \mathbf{i}$.

We report in Table 7 the cost of line computation and result accumulation that come from algorithm 4.1. Finally in Table 8 we estimate the total cost of a pairing computation in terms of multiplications in the base field.

TABLE 7. Miller loop cost in Weierstrass model from [13, 16].

k	curve	`Dbl step, tangent line` `Add step, chord line`	`sparse-sparse-`$\mathbf{m}_k$ `full-sparse-`$\mathbf{m}_k$	reference
$2 \mid k$	$y^2 = x^3 - 3x + b$ quadratic twist	$6\mathbf{m}_{k/2} + 4\mathbf{s}_{k/2} + k\mathbf{m}$ $10\mathbf{m}_{k/2} + 3\mathbf{s}_{k/2}$	$\mathbf{m}_k$ $\mathbf{m}_k$	[13]
$4 \mid k$	$y^2 = x^3 + ax$ quartic twist	$2\mathbf{m}_{k/4} + 8\mathbf{s}_{k/4} + (k/2)\mathbf{m}$ $9\mathbf{m}_{k/4} + 5\mathbf{s}_{k/4} + (k/2)\mathbf{m}$	$6\mathbf{m}_{k/4}$ $8\mathbf{m}_{k/4}$	[16, §4]

TABLE 8. Optimal ate pairing and final exponentiation cost estimates in terms of finite field multiplications. The bitsize of p has a scale color w.r.t. its 64-bit machine word size: $512 < 9\mathtt{w} \leq 576$, $448 < 8\mathtt{w} \leq 512$.

curve	p bits	r bits	Miller loop optimal ate	final exp			pairing total
				easy	hard	total	
GG20b	575	**379**	17554**m**	507**m**	41997**m**	42504**m**	60058**m**
GG22D7	457	**383**	45780**m**	1500**m**	79740**m**	81240**m**	127020**m**

5. CONCLUSION

This work generalizes the KSS technique to generate complete families of pairing-friendly curves. Every complete family of cryptographic interest listed in the taxonomy of Freeman, Scott and Teske fall in this global approach. Our contribution is twofold: we present a theoretical interpretation of KSS with the *subfield method* and display its versatility by generating new complete families of embedding degrees of cryptographic interest: 16, 18, 20, 22. For $k = 16$, $k = 18$, we obtain alternative choices of comparable performances as the well-known KSS curves. For $k = 20$, we improve on the previous FST 6.4 curves with parameters that are not vulnerable to a specific STNFS attack (the polynomial $Q(X)$ has no automorphism). Finally for $k = 22$, we improve on the previously best ρ-value curves: our new family with $D = 7$ has $\rho = 1.2$ compared to FST 6.3 with $\rho = 1.3$. This ρ improvement applies to all $k = 4 \bmod 6$ curves.

The polynomials defining the new families in some cases have larger denominators and we present an automated procedure to process them. First, we determine the congruence conditions on the seeds x_0 to generate valid parameters with prime integers at $Q(x_0)$, $R(x_0)$, and integers at $T(x_0), Y(x_0), H(x_0)$ (this step may discard many potential families). This contribution comes with a SageMath open-source companion code available online [25]. Second we obtain seeds to generate new instances of elliptic curves of cryptographic interest at the 192-bit security level for $k = 20$, $k = 22$ and derive the optimal ate pairing and final exponentiation formulas. Finally we implemented the pairing on our new curves in SageMath to validate the formulas [30].

The paramount goal remains families of pairing-friendy curves with $\rho = 1$, to reach optimal efficiency and also to satisfy new needs in recursive proofs of knowledge, where a *cycle* of prime-order pairing-friendly curves is sought. Complete families with $\rho = 1$ are very rare: apart from the BN family, all known families are sparse (MNT curves, Freeman curves). Moreover, these families all have quite small embedding degrees ($k \in \{3, 4, 6, 10, 12\}$). In particular, our new subfield method do not capture them. It remains a difficult open problem to generate new pairing-friendly curves with $\rho = 1$. In this work, we improved the ρ-value in certain cases ($k = 22$). With the $\rho = 1$ goal in mind, we foresee that such extremely rare curves are not likely to be given by complete families. We presume that new techniques to generate sparse families of curves are to be discovered in the quest to $\rho = 1$.

References

[1] Diego F. Aranha, Georgios Fotiadis, and Aurore Guillevic. A short-list of pairing-friendly curves resistant to the special TNFS at the 192-bit security level. Talk at SIAM-AG'23 conference, *Elliptic Curves and Pairings in Cryptography* minisymposium, July 13 2023. slides.

[2] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone algorithm. *Journal of Cryptology*, 11(2):141–145, March 1998.

[3] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of Cryptology*, 32(4):1298–1336, October 2019.

[4] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The tower number field sieve. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 31–55. Springer, Heidelberg, November / December 2015.

[5] 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 02*, volume 2576 of *LNCS*, pages 257–267. Springer, Heidelberg, September 2003.

[6] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. On the selection of pairing-friendly groups. In Mitsuru Matsui and Robert J. Zuccherato, editors, *SAC 2003*, volume 3006 of *LNCS*, pages 17–25. Springer, Heidelberg, August 2004.

[7] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *SAC 2005*, volume 3897 of *LNCS*, pages 319–331. Springer, Heidelberg, August 2006.

[8] Marta Bellés-Muñoz, Jorge Jiménez Urroz, and Javier Silva. Revisiting cycles of pairing-friendly elliptic curves. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO'2023*, volume 14082 of *LNCS*, pages 3–37. Springer-Verlag, 2023. ePrint 2022/1662.

[9] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Scalable zero knowledge via cycles of elliptic curves. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 276–294. Springer, Heidelberg, August 2014.

[10] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[11] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, September 2004.

[12] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography*, 37(1):133–141, 2005. https://eprint.iacr.org/2003/143.

[13] Sanjit Chatterjee, Palash Sarkar, and Rana Barua. Efficient computation of Tate pairing in projective coordinate over general characteristic fields. In Choonsik Park and Seongtaek Chee, editors, *ICISC 04*, volume 3506 of *LNCS*, pages 168–181. Springer, Heidelberg, December 2005.

[14] Alessandro Chiesa, Lynn Chua, and Matthew Weidner. On cycles of pairing-friendly elliptic curves. *SIAM Journal on Applied Algebra and Geometry*, 3(2):175–192, 2019.

[15] Rémi Clarisse, Sylvain Duquesne, and Olivier Sanders. Curves with fast computations in the first pairing group. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *CANS 20*, volume 12579 of *LNCS*, pages 280–298. Springer, Heidelberg, December 2020.

[16] Craig Costello, Tanja Lange, and Michael Naehrig. Faster pairing computations on curves with high-degree twists. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 224–242. Springer, Heidelberg, May 2010.

[17] Youssef El Housni and Aurore Guillevic. Families of SNARK-friendly 2-chains of elliptic curves. https://gitlab.inria.fr/zk-curves/snark-2-chains, 2022. SageMath/Python and Magma implementation.

[18] Andreas Enge. *Courbes Algébriques et Cryptologie*. Habilitation à diriger des recherches, Université Paris-Diderot - Paris VII, December 2007. https://tel.archives-ouvertes.fr/tel-00382535.

[19] Armando Faz-Hernandez, Sam Scott, Nick Sullivan, Riad S. Wahby, and Christopher A. Wood. Hashing to elliptic curves. draft 16, IETF, December 2022. https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/.

[20] Emmanuel Fouotsa, Laurian Azebaze Guimagang, and Raoul Ayissi. x-superoptimal pairings on elliptic curves with odd prime embedding degrees: Bw13-p310 and bw19-p286. *AAECC*, February 16 2023. ePrint 2022/716.

[21] David Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465. Springer, 2006. https://eprint.iacr.org/2006/026.

[22] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, April 2010.

[23] Laura Fuentes-Castañeda, Edward Knapp, and Francisco Rodríguez-Henríquez. Faster hashing to $\mathbb{G}_2$. In Ali Miri and Serge Vaudenay, editors, *SAC 2011*, volume 7118 of *LNCS*, pages 412–430. Springer, Heidelberg, August 2012.

[24] Steven D. Galbraith, James F. McKee, and P. C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields Their Appl.*, 13(4):800–814, 2007.

[25] Jean Gasnier. Sagemath code for the subfield method, 2023. https://gitlab.inria.fr/jgasnier/subfield-method.

[26] Fernando Q. Gouvêa. *p-adic Numbers*. Springer, Heidelberg, 1997.

[27] Jens Groth. On the size of pairing-based non-interactive arguments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 305–326. Springer, Heidelberg, May 2016.

[28] Aurore Guillevic. Pairing-friendly curves. https://members.loria.fr/AGuillevic/pairing-friendly-curves/, 9 2020. Last updated October 9, 2020.

[29] Aurore Guillevic. A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 535–564. Springer, Heidelberg, May 2020.

[30] Aurore Guillevic. Sagemath code for pairing computations, 2023. https://gitlab.inria.fr/guillevi/pairings-on-gasnier-g-curves.

[31] Aurore Guillevic. Tnfs-alpha. https://gitlab.inria.fr/tnfs-alpha/alpha, August 2023. SageMath–Python, MIT licence.

[32] Aurore Guillevic, Simon Masson, and Emmanuel Thomé. Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation. *Designs, Codes and Cryptography*, 88:1047–1081, March 2020. https://eprint.iacr.org/2019/431.

[33] Aurore Guillevic and Shashank Singh. On the alpha value of polynomials in the tower number field sieve algorithm. *Mathematical Cryptology*, 1(1):1–39, Feb. 2021.

[34] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. *Journal of Cryptology*, 17(4):263–276, September 2004.

[35] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field. In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 126–135. Springer, Heidelberg, September 2008.

[36] Koray Karabina and Edlyn Teske. On prime-order elliptic curves with embedding degrees $k = 3$, 4, and 6. In Alfred J. van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17-22, 2008, Proceedings*, volume 5011 of *LNCS*, pages 102–117. Springer, 2008. ePrint 2007/425.

[37] Taechan Kim and Razvan Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 543–571. Springer, Heidelberg, August 2016.

[38] Simon Masson. *Algorithmic of curves in the context of bilinear and post-quantum cryptography*. Doctorat, Université de Lorraine, Nancy, France, December 2020. https://tel.archives-ouvertes.fr/tel-03052499.

[39] Alfred Menezes, Tasuaki Okamoto, and Scott Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of Computing*, pages 80–89, 1991. https://doi.org/10.1145/103418.103434.

[40] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001. https://dspace.jaist.ac.jp/dspace/bitstream/10119/4432/1/73-48.pdf.

[41] Atsuko Miyaji, Masaki Nakabayashi, and Shunzo Takano. Characterization of elliptic curve traces under FR-reduction. In Dongho Won, editor, *ICISC 00*, volume 2015 of *LNCS*, pages 90–108. Springer, Heidelberg, December 2001.

[42] P. L. Montgomery. Five, six, and seven-term Karatsuba-like formulae. *IEEE Transactions on Computer*, 54:362–369, March 2005.

[43] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc.,New York, 1991.

[44] Michael Scott and Aurore Guillevic. A new family of pairing-friendly elliptic curves. In Lilya Budaghyan and Francisco Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields - 7th International Workshop, WAIFI, Revised Selected Papers*, volume 11321 of *LNCS*, pages 43–57, Bergen, Norway, June 14-16 2018. Springer. ePrint 2018/193.

[45] Andrew V. Sutherland. Computing Hilbert class polynomials with the chinese remainder theorem. *Mathematics of Computation*, 80(273):501–538, 2011. https://arxiv.org/abs/0903.2785.

[46] F. Vercauteren. Optimal pairings. *IEEE Transactions on Information Theory*, 56(1):455–461, Jan 2010.

Appendix A. Families with $k = 46$

Example 17. $k = 46$, $D = 7$, $F = \mathbb{Q}[x]/(x^2 + x + 2)$, $\omega = (-1 + \sqrt{-7})/2$, $\alpha = \omega$, $(a, b) = (0, 1)$, $\theta = \alpha\zeta_k$.

- $T = \frac{1}{1934}\left(X^{24} + 2115X + 1934\right)$
- $Y = \frac{1}{13538}\left(X^{24} + 4X^{23} + 5983X + 10394\right)$
- $R = (X^{44} + X^{43} - X^{42} - 3X^{41} - X^{40} + 5X^{39} + 7X^{38} - 3X^{37} - 17X^{36} - 11X^{35} + 23X^{34} + 45X^{33} - X^{32} - 91X^{31} - 89X^{30} + 93X^{29} + 271X^{28} + 85X^{27} - 457X^{26} - 627X^{25} + 287X^{24} + 1541X^{23} + 967X^{22} + 3082X^{21} + 1148X^{20} - 5016X^{19} - 7312X^{18} + 2720X^{17} + 17344X^{16} + 11904X^{15} - 22784X^{14} - 46592X^{13} - 1024X^{12} + 92160X^{11} + 94208X^{10} - 90112X^9 - 278528X^8 - 98304X^7 + 458752X^6 + 655360X^5 - 262144X^4 - 1572864X^3 - 1048576X^2 + 2097152X + 4194304)/967$
- $Q = \frac{1}{13091246}\left(X^{48} + X^{47} + 2X^{46} + 5197X^{25} + 11966X^{24} + 10394X^{23} + 8388608X^2 + 22705043X + 16777216\right)$

Seeds should satisfy $x_0 \equiv 3, 4 \bmod 7$. If $x_0 \equiv 268, 700 \bmod 967$ then R, Q can take prime values and $H = (Q+1-T)/R$ takes integer values. If $x_0 \equiv 12, 79, 116, 119, 310, 320, 355, 418, 475, 495, 616, 629, 799, 806, 828, 832, 837, 853, 864, 917, 923 \bmod 967$ then Q, $R/967$ can take prime values and $967H$ takes integer values.

Example 18. $k = 46$, $D = 15$, $F = \mathbb{Q}[x]/(x^2 + x + 4)$, $\omega = (-1 + \sqrt{-15})/2$, $\alpha = (1 - \omega)$, $(a, b) = (1, -1)$, $\theta = \alpha\zeta_k$.

- $T = \frac{1}{2347906338}\left(X^{24} + 122762871X + 2347906338\right)$
- $Y = \frac{1}{11739531690}\left(X^{24} - 4X^{23} - 1442508021X + 1856854854\right)$
- $R = X^{44} - 3X^{43} + 3X^{42} + 9X^{41} - 45X^{40} + 81X^{39} + 27X^{38} - 567X^{37} + 1539X^{36} - 1215X^{35} - 5589X^{34} + 24057X^{33} - 38637X^{32} - 28431X^{31} + 317115X^{30} - 780759X^{29} + 439587X^{28} + 3365793X^{27} - 12734901X^{26} + 18009945X^{25} + 22379571X^{24} - 175198383X^{23} + 391317723X^{22} - 1051190298X^{21} + 805664556X^{20} + 3890148120X^{19} - 16504431696X^{18} + 26172406368X^{17} + 20509371072X^{16} - 218562551424X^{15} + 532631427840X^{14} - 286518974976X^{13} - 2336231642112X^{12} + 8727808776192X^{11} - 12166036475904X^{10} - 15868743229440X^9 + 120602448543744X^8 - 266594886254592X^7 + 76169967501312X^6 + 1371059415023616X^5 -$

$4570198050078720X^4 + 5484237660094464X^3 + 10968475320188928X^2 - 65810851921133568X + 131621703842267136$

- $Q = \frac{1}{13781660430051425610}\left(X^{48} - 3X^{47} + 6X^{46} - 928427427X^{25} + 8655048126X^{24} - 5570564562X^{23} + 789730223053602816X^2 - 1648601361930867453X + 4738381338321616896\right)$

Appendix B. Families with $k \in \{18, 28, 40\}$

Example 19. Let $k = 18$, $D = 3$, KSS18 (Example 5) was obtained with Case 3, $d = 6$, $(a, b) = (-3, 1)$. With $(a, b) = (2, -3)$ we get a similar family, of same R and same congruence constraint $x_0 \equiv 14 \bmod 21$:

- $T = \frac{1}{7}\left(-3X^4 - 55X + 7\right)$
- $Y = \frac{1}{21}\left(X^4 - 14X^3 + 23X - 259\right)$
- $R = (X^6 + 37X^3 + 343)/343$
- $Q = \frac{1}{21}\left(X^8 - X^7 + 7X^6 + 37X^5 - 46X^4 + 259X^3 + 343X^2 - 508X + 2401\right)$

With $x_0 = -2^{80} - 2^{69} - 2^{51} - 2^3$, we get q prime of 636 bits, r prime of 472 bits, and the curve equation is $y^2 = x^3 + 3$.

Example 20. Let $k = 28$, $D = 11$, $F = \mathbb{Q}[x]/(x^2 + x + 3)$, $\omega = (-1 + \sqrt{-11})/2$, $\alpha = \omega$, $(a, b) = (0, 1)$, $\theta = \alpha\zeta_k$. With Case 2 one obtains

- $T = \frac{1}{3237}\left(X^{15} + 718X + 3237\right)$
- $Y = \frac{1}{35607}\left(X^{15} + 6X^{14} + 7192X + 7545\right)$
- $R = X^{24} + 5X^{22} + 16X^{20} + 35X^{18} + 31X^{16} - 160X^{14} - 1079X^{12} - 1440X^{10} + 2511X^8 + 25515X^6 + 104976X^4 + 295245X^2 + 531441$
- $Q = \frac{1}{38419953}\left(X^{30} + X^{29} + 3X^{28} + 2515X^{16} + 14384X^{15} + 7545X^{14} + 4782969X^2 + 13304911X + 14348907\right)$

Example 21. Let $k = 40$, $D = 11$, $F = \mathbb{Q}[x]/(x^2 + x + 3)$, $\omega = (-1 + \sqrt{-11})/2$, $\alpha = -2 + 9\omega$, $(a, b) = (-2, 9)$, $\theta = \alpha\zeta_k$. With Case 2 one obtains

- $T = \frac{1}{28371069490077576136284995}\left(X^{21} - 12989833320460810262936 64X + 28371069490077576136284995\right)$
- $Y = \frac{1}{28087358795176800374922145 05}\left(13X^{21} + 530X^{20} + 39855355663556098930752358X - 31963726261341445416393 6985\right)$
- $R = X^{32} + 10129X^{28} - 4828953984X^{24} - 98864151184561X^{20} + 22812836050543021631X^{16} - 48755356656431628990062 5X^{12} - 11744108595880792961415000 0000X^8 + 12148343362344675830953830566406 25X^4 + 59147171785255689169279057632446289 0625$
- $Q = \frac{1}{27063455371835182269505621776786931065396049704742 35}\left(X^{42} + 13X^{41} + 265X^{40} - 12061783494845828459016 49X^{22} + 79710711327112197861504716X^{21} - 31963726261341445416393 6985X^{20} + 29168727198456005970756386746670151710510253906 25X^2 - 85992012470381924311027266086623267898575772916467X + 77297127075908415822504424878675902032852172851562 5\right)$

Example 22. Let $k = 40$, $D = 103$, $F = \mathbb{Q}[x]/(x^2 + x + 26)$, $\omega = (-1 + \sqrt{-103})/2$, $\alpha = 1 + 3\omega$, $(a, b) = (1, 3)$, $\theta = \alpha\zeta_k$. With Case 2 one obtains

- $T = \frac{1}{42026206377163549924371 44}\left(X^{21} + 34873235880094679284301 7X + 42026206377163549924371 44\right)$
- $Y = \frac{1}{12986097770543536926630 76496}\left(X^{21} + 464X^{20} + 87539736342336567777173 05X + 16601443512135566687159 7032\right)$
- $R = X^{32} - 106721X^{28} + 8492348865X^{24} - 597138774199969X^{20} + 39124717339282369409X^{16} - 17299247487177862114877 44X^{12} + 71274094046504250746590986240X^8 - 25948108469505269493909471321128 96X^4 + 70438120351099559671412028074440523776$

- $Q = \frac{1}{705719515007180365927186780354314139780340738910 96}\,(X^{42}+X^{41}+232X^{40}$
  $+71557946172998132272240 1X^{22}+175079472684673135554346 10X^{21}$
  $+16601443512135566687159703 2X^{20}+20406085304338861123156365569441123572454627737 6X^{2}$
  $+60601028881399799064212908054145601003324225719 29X$
  $+47342117906066157805722768121103406688094736351232)$

Appendix C. Families from the Taxonomy of Freeman, Scott, and Teske

Example 23 ([22, Contruction 6.3]). Let $k = 2 \bmod 4$, $D = 1$.

$$\begin{aligned} T &= X^2+1 \\ Y &= (X^2-1)X^{k/2} \\ R &= \Phi_{2k}(X) \\ Q &= (X^{k+4}-2X^{k+2}+X^k+X^4+2X^2+1)/4 \end{aligned}$$

Then (Q, R, T, Y) parameterizes a complete family of pairing-friendly curves of embedding degree k and $\rho = (k/2+2)/\varphi(k)$. Because k is even, the polynomial Q is even (all monomials of even degree) and there exists a polynomial $Q_0 = (X^{k/2+2}-2X^{k/2+1}+X^{k/2}+X^2+2X+1)/4$ of degree $k/2+2$ such that $Q = Q_0(X^2)$. The improved Kim–Barbulescu variant of [29] can apply.

Example 24 ([22, Contruction 6.6] with $k = 20$). Let $k = 20$, $D = 3$. Let:

$$\begin{aligned} T &= X^{11}-X+1 \\ Y &= (X^{11}+2X^{10}+X-1)/3 \\ R &= \Phi_{60}(X) \\ Q &= (X-1)^2(X^{20}-X^{10}+1)/3+X^{21} \\ &= (X^{22}+X^{21}+X^{20}-X^{12}+2X^{11}-X^{10}+X^2-2X+1)/3 \end{aligned}$$

Then (Q, R, T, Y) parameterizes a complete family of pairing-friendly curves of embedding degree $k = 20$ and $\rho = (k/2+1)/\varphi(k) = 11/8 = 1.375$.

Example 25 ([22, Contruction 6.6] with $k = 22$). Let $k = 22$, $D = 3$.

$$\begin{aligned} T &= X^3+1 \\ Y &= (2X^{14}-2X^{11}-X^3+1)/3 \\ R &= \Phi_{66}(X) \\ Q &= (X^3-1)^2(X^{22}-X^{12}+1)/3+X^3 \\ &= (X^{28}-2X^{25}+X^{22}-X^{17}+2X^{14}-X^{11}+X^6+X^3+1)/3 \end{aligned}$$

Then (Q, R, T, Y) parameterizes a complete family of pairing-friendly curves of embedding degree $k = 22$ and $\rho = (k/2+3)/\varphi(k) = 7/5 = 1.4$.

Université de Bordeaux
Email address: jean.gasnier@u-bordeaux.fr

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
Email address: aurore.guillevic@inria.fr
URL: https://members.loria.fr/AGuillevic/