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 particular elements of quadratic extensions of a cyclotomic field generate families of pairing-friendly curves with small parameters. By exhaustive search among these elements, we discovered new families of curves of embedding degree $k = 20$, $k = 22$ and $k = 28$. We provide an open-source SageMath implementation of our technique. We obtain curves of cryptographic size from our new families and we give a proof-of-concept SageMath implementation of a pairing on some new curves.

Keywords: Elliptic Curves, Pairing-based Cryptography

Contents

Date: December 16, 2024.

1. Overview about finding pairing-friendly curves

In cryptography, proof systems based on the hardness of the discrete logarithm problem need the construction of secure groups, with an efficiently computable bilinear map [3, 17]. As preferred instantiation, elliptic curves over finite fields play a crucial role. In particular cases, they come with an efficient pairing, obtained as a variant of the Tate or Weil pairing. Such appropriate curves with an efficient map are called pairing-friendly. They are known to be rare and should be designed on purpose. With the recent development of new proof systems in the trend of SNARK (Succinct Non-interactive ARgument of Knowledge), came back the need for dedicated pairing-friendly curves, designed specifically. We recall briefly the area of pairing-friendly constructions since 2000. To lighten this presentation, we refer to the references in [14]. In the 2000s, as pairings started to be used to design protocols, supersingular curves were used (the trace of the Frobenius is zero modulo the characteristic). Because supersingular curves are not very efficient, there was a series of contributions to design ordinary curves. Barreto, Lynn and Scott and independently Brezing and Weng expressed the curve parameters as polynomials in one integer variable. There were many contributions of curve families in the 2000s. Barreto and Naehrig in 2005 discovered one of the rare prime-order families, of embedding degree 12 and discriminant 3. Kachisa, Schaefer, and Scott in 2008 published a technique to obtain interesting families and obtained the well-known KSS16 and KSS18 that fill the gap of BLS at embedding degrees $k = 16$ and $k = 18$. Freeman, Scott and Teske published their taxonomy of pairing-friendly curves and filled many other gaps of BLS [14].

In this work, we obtain a generalization of and a mathematical perspective on the work of Kachisa, Schaefer, and Scott [22]. We obtained new parameterized pairing-friendly curves, with a proportionally larger prime factor of the group order. Some of our new constructions are already implemented, in [23, 1].

In Section 2, we recall some background on the generation of pairing-friendly curves, and fix some notations.

We then present, in Section 3, the subfield method, a new method for generating families of pairing-friendly curves by exhaustive search over some algebraic numbers. We introduce explicit sets of algebraic numbers producing potential families of curves with a small ρ-value.

Methods of generation of family of curves based on exhaustive search require being able to check at which integers a polynomial P in $\mathbb{Q}[X]$ takes integer values. They also require being able to check if the integer values of P have a common prime divisor. Both problems reduce to solving

$$P(x) \equiv 0 \bmod p^n$$

for some prime power p^n, where x is an integer variable. In Section 4, we present a general algorithm to solve such polynomial equations.

In Section 5, we present new families with embedding degrees $k = 20$, $k = 22$ and $k = 28$ we think have a cryptographic interest. Following the publication of a preprint of this work, the algorithmic properties of our $k = 20$ and $k = 28$ curves with $j = 1728$ were studied in [1] and $k = 22$ with $D = 7$, $k = 28$ with $D = 11$ in [23]. We keep this section condensed to avoid overlapping the subsequent works.

2. Notations and technical background

In this work, we consider ordinary elliptic curves E defined over a prime field $\mathbb{F}_q$ of large characteristic (this implies $q \geq 5$), given by an equation in short Weierstrass form $y^2 = x^3 + ax + b$. Let t be the trace of the Frobenius map $(x, y) \mapsto (x^q, y^q)$. Write $t^2 - 4q = -Dy^2$ where D is squarefree. Since E is ordinary, one has that

$\mathrm{End}(E)$ is isomorphic to an order of $\mathbb{Q}(\sqrt{-D})$. We call D the *discriminant* of E (see Remark 3). The curve order over $\mathbb{F}_q$ is $|E(\mathbb{F}_q)| = q + 1 - t$. For cryptography, one desires this order to be a large prime number, or to have a large prime factor denoted r (say, of 256 bits to resist to a Discrete Logarithm (DL) computation), with a tiny cofactor h. We also ask that r be coprime to q.

2.1. **Torsion subgroup, embedding degree, and pairing.** Recall that one has the following group isomorphism

$$E[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

Consider the extension field $\mathbb{F}_{q^k}$ such that $E[r] \subset E(\mathbb{F}_{q^k})$ and k is minimal. The degree k is named the *embedding degree*. Note that k is also the minimal degree such that $\mu_r(\mathbb{F}_{q^k})$ has order r, where μ_r denotes the group of r-th roots of unity. As we asked that h, the cofactor of r in the curve order, be small, we may assume $r \nmid h$, which forces $k > 1$. Define $\mathbb{G}_1$ the subgroup of order r of $E(\mathbb{F}_q)$, that is

$$\mathbb{G}_1 = E[r] \cap \ker(\pi_q - \mathrm{Id}) = E(\mathbb{F}_q)[r]$$

and $\mathbb{G}_2$ the trace-zero subgroup of order r of $E(\mathbb{F}_{q^k})$, that is

$$\mathbb{G}_2 = E[r] \cap \ker(\pi_q - [q]).$$

In this way, $\mathbb{G}_1 \cap \mathbb{G}_2 = \{\mathcal{O}\}$. Finally, $\mathbb{G}_T = \mu_r(\mathbb{F}_{q^k})$ is the group of r-th roots of unity in $\mathbb{F}_{q^k}^*$. The *optimal ate pairing* is a bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ that maps pairs of points on the curve to a finite field extension.

For a randomly selected curve E, the embedding degree is usually very large, $k \sim r$ which makes it impractical. To obtain an efficiently computable pairing, one requires k to be very small, in practice $k \leq 54$ (the Taxonomy of Freeman, Scott and Teske considers $1 \leq k \leq 50$). We call curves meeting this condition pairing-friendly.

2.2. **Measuring the gap to optimal curves.** One desires an elliptic curve E of prime order r over a base field, with a small embedding degree k. A parameter ρ was introduced to measure the gap to primality, that is the ratio of the subgroup r compared to the full curve order, of same magnitude as q:

$$\rho = \frac{\log q}{\log r} \quad \text{where } r \cdot h = \#E(\mathbb{F}_q) = q + 1 - t \text{ and } r \text{ is prime.} \tag{2.1}$$

The ρ-value is closer to 1 when the cofactor h is smaller. Curves with a ρ-value of 1 are notoriously hard to find: the only known curves that have a prime order are the MNT curves with $k \in \{3, 4, 6\}$, the Freeman curves with $k = 10$, and the Barreto–Naehrig curves with $k = 12$. The generic Cocks–Pinch method (see subsection 2.3), usually produces pairing-friendly curves with $\rho \approx 2$. Hence, one is interested in finding methods able to produce curves with $1 \leq \rho < 2$.

2.3. **The Cocks–Pinch method.** Given k as input, the Cocks–Pinch method generates a pairing-friendly curve with embedding degree k. Two relations between elliptic curve parameters are involved. First, the curve order is such that

$$r \mid q + 1 - t \iff t - 1 \equiv q \bmod r\ . \tag{2.2}$$

The second equation (2.3) combines the CM equation $t^2 - 4q = -Dy^2$ to (2.2) with the definition of k (the smallest integer such that $r \mid q^k - 1$):

$$r \mid \Phi_k(t - 1) \iff t - 1 \equiv \zeta_k \bmod r\ , \tag{2.3}$$

where ζ_k is a primitive k-th root of unity modulo r.

We briefly sketch the Cocks–Pinch idea to generate a pairing-friendly curve of given embedding degree k. Choose a small discriminant $D > 0$ and a prime integer r such that $-D$ is a square modulo r and $r \equiv 1 \bmod k$, so that there exists a primitive k-th root of unity ζ_k modulo r. Set

- $t \in \mathbb{Z}$ such that $t = \zeta_k + 1 \bmod r$,
- $y \in \mathbb{Z}$ such that $y = (t-2)/\sqrt{-D} \bmod r$,
- $q = (t^2 + Dy^2)/4$.

If $q \notin \mathbb{Z}$ or q is not prime, restart with a new r or D. Otherwise, applying the CM method with q as finite field order and t as trace produces a curve with a subgroup of r rational points with embedding degree k.

2.4. **Previous work on polynomial families.** Brezing and Weng [5] obtained a method to generate families of curves by replacing the integer parameters q, r, t, y, h of the Cocks–Pinch method by polynomials Q, R, T, Y, H in $\mathbb{Q}[X]$, required to satisfy some relations (see Definition 2). To obtain a curve from a family given by (Q, R, T, Y, H), one needs an integer seed $x \in \mathbb{Z}$ such that $Q(x) = q$, $R(x) = r$ are prime integers, and $T(x) = t, Y(x) = y, H(x) = h$ are integers.

Dupont, Enge and Morain define $R(X)$ as a resultant of two equations [11]. Barreto, Lynn and Scott [2] choose to parameterize $R(X)$ as a cyclotomic polynomial, $R(X) = \Phi_k(X)$, for $3 \mid k$, producing curves with $D = 3$. Their original paper can be reinterpreted as follows: set

$$T(X) = X + 1,$$

and set

$$S(X) = 2X^{k/3} + 1 \text{ if } k \equiv 3 \bmod 6,$$

or

$$S(X) = 2X^{k/6} - 1 \text{ if } k \equiv 0 \bmod 6.$$

One has $S^2(X) + 3 = 0 \bmod R(X)$. Then

$$Y(X) = (X-1)S(X)/3,$$

and

$$Q(X) = (T^2(X) + 3Y^2(X))/4.$$

The final polynomial $Q(X)$ is never irreducible for $18 \mid k$.

Example 1. A classical example happens with embedding degree $k = 12$, producing the BLS12 family of pairing-friendly curves:

- $R(X) = X^4 - X^2 + 1$,
- $T(X) = X + 1$,
- $S(X) = 2X^2 - 1$,
- $Y(X) = (X-1)(2X^2 - 1)/3$,
- $Q(X) = (X^6 - 2X^5 + 2X^3 + X + 1)/3$.

2.5. **Using number fields to produce families.** Here we give the prerequisites necessary to present the KSS method and our new method in Section 3.

Definition 1. We say that a polynomial $P \in \mathbb{Q}[X]$ represents primes if the following conditions are satisfied:

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

Remark 1. Definition 1 is motivated by the Buniakowski-Schinzel conjecture, which states that these conditions are sufficient for a rational polynomial to take an infinite number of prime values.

Let $k \geq 1$ be a positive integer, let D be a positive squarefree integer and let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Let $\zeta_k \in \overline{\mathbb{Q}}$ be a primitive k-th root of unity. As in [14], we use two levels of satisfiability for a set of polynomials (Q, R, T, Y, H), a first level where the polynomials satisfy some relations, and a second level where in addition, they take integer values and the relevant ones generate primes.

Definition 2. Let Q, R, T, Y and H be polynomials in $\mathbb{Q}[X]$. We say that (Q, R, T, Y, H) parameterizes a *potential family* of pairing-friendly curves (with embedding degree k and discriminant D) if:

(1) R is non-constant, irreducible and has positive leading coefficient.
(2) $HR = Q + 1 - T$.
(3) R divides $\Phi_k(T-1)$, with Φ_k the k-th cyclotomic polynomial.
(4) $DY^2 = 4Q - T^2$.

We say that (Q, R, T, Y, H) parameterizes a *family* of pairing-friendly curves (with embedding degree k and discriminant D) if it is a potential family of pairing-friendly curves and:

(5) Q represents primes.
(6) There exists $x \in \mathbb{Z}$ such that $Q(x)$, $R(x)$, $T(x)$, $Y(x)$, $H(x)$ all are integers.

Remark 2. In the following, we will only consider (potential) families parameterized by polynomials. For the sake of simplicity, we will identify the (potential) families with the polynomials that parameterize them.

Remark 3. Our convention for the definition of the discriminant D of an elliptic curve E is the standard convention in the literature on the generation of pairing-friendly curves. It is related to the more traditional convention D', which is the discriminant of the fraction field of the endomorphism ring of E. One has that $-D'/D$ is a positive square in $\mathbb{Z}$ (either 1 or 4).

Remark 4. Note that conditions 1 to 4 imply that

$$(4') \qquad DY^2 = 4Q - T^2 = 4Q - 4T + 4 - (T-2)^2 \equiv -(T-2)^2 \bmod R.$$

Definition 3. Let (Q, R, T, Y, H) be a potential family of pairing-friendly curves. We define its ρ-value to be

$$\rho = \frac{\deg Q}{\deg R}.$$

We need the following lemma to introduce the standard method for producing families of curves.

Lemma 1. *Let K be a number field and let θ be a primitive element in K, i.e. $K = \mathbb{Q}(\theta)$. Let ζ be an element of K. Then there exists a unique polynomial T in $\mathbb{Q}[X]$ with minimal degree such that:*

$$T(\theta) = \zeta \ .$$

We call it the canonical rational polynomial mapping θ to ζ.

Proof. Let R be the minimal polynomial of θ. We get a canonical isomorphism

$$\begin{array}{ccc} \mathbb{Q}[X]/\langle R \rangle & \longrightarrow & K \\ P \bmod R & \longmapsto & P(\theta) \end{array}$$

Let $P \in \mathbb{Q}[X]$ such that $P(\theta) = \zeta$. Then T is the remainder of the Euclidean division of P by R. □

Let $K \subset \overline{\mathbb{Q}}$ be a number field containing $\mathcal{C}_k$ the k-th cyclotomic field and $\mathbb{Q}(\sqrt{-D})$. Proposition 1 summarizes the methods of Brezing–Weng and Kachisa–Schaefer–Scott for producing (potential) families of curves.

Proposition 1. *Let $\theta \in K$ be a primitive element in K. We associate a potential family to the pair (θ, ζ_k) by letting*

- *R be the minimal polynomial of θ.*
- *T be the canonical rational polynomial mapping θ to $\zeta_k + 1$ (condition 3).*
- *Y be the canonical rational polynomial mapping θ to $(\zeta_k - 1)/\sqrt{-D}$ (condition 4').*
- *$Q = (T^2 + DY^2)/4$ (condition 4).*
- *H be the unique polynomial such that $RH = Q + 1 - T$.*

We denote the ρ-value of this potential family by $\rho(\theta, \zeta_k)$. In particular, one has

$$\rho(\theta, \zeta_k) < 2.$$

Definition 4. Let $\mathcal{S}$ be a set of primitive elements in K. We define

$$\rho(\mathcal{S}, \zeta_k) = \max_{\theta \in \mathcal{S}} \rho(\theta, \zeta_k) \ .$$

Remark 5. If one can show that $\rho(\mathcal{S}, \zeta_k)$ is significantly smaller than 2, doing an exhaustive search over the elements of $\mathcal{S}$ is likely to produce a family with a small ρ-value.

3. The subfield method

The KSS method aims at generating families of pairing-friendly curves where R is not a cyclotomic polynomial, to fill the gaps left by BLS families (see Section 2.4) and other cyclotomic families. First, Kachisa, Schaefer, and Scott make the observation that any monic irreducible polynomial with rational coefficients must be the minimal polynomial of an algebraic number θ. As a consequence of Definition 2 one only needs to look for algebraic numbers θ defining number fields $\mathbb{Q}(\theta)$ containing a primitive k-th root of unity and some $\sqrt{-D}$, where k and D are the desired embedding degree and discriminant.

Yet, most of these algebraic numbers define potential families which are of little interest to us as their ρ-value is too large. One of the main components of the KSS method is to define a set of algebraic numbers that empirically contains a relatively large proportion of algebraic numbers defining (potential) families with a small ρ-value. We recall their construction. Assume $D = 1$, resp. $D = 3$. Let $\ell = \mathrm{lcm}(4, k)$, resp. $\ell = \mathrm{lcm}(3, k)$, and let $\mathcal{C}_\ell$ be the ℓ-th cyclotomic field in $\overline{\mathbb{Q}}$. The degree of the extension is $[\mathcal{C}_\ell : \mathbb{Q}] = \varphi(\ell)$, where φ is the Euler totient function. Let ζ_ℓ be a primitive ℓ-th root of unity in $\mathcal{C}_\ell$. Let B_1 and B_2 be two integers and let $\mathbf{KSS}(B_1, B_2)$ be the set of primitive elements of $\mathcal{C}_\ell$ of the form

$$P(\zeta_\ell) = \sum_{i=0}^{\varphi(\ell)-1} P_i \zeta_\ell^i \ ,$$

where

- $P \in \mathbb{Q}[X]$ has at most B_1 non-zero coefficients.
- $\forall i \in [0, \varphi(\ell) - 1], \max(\mathrm{num}(|P_i|), \mathrm{denom}(|P_i|)) \leq B_2$.

The families found by Kachisa, Schaefer and Scott were generated by exhaustive search over the algebraic integers in $\mathbf{KSS}(2, 3)$.

Typically, one gets $\rho(\mathbf{KSS}(B_1, B_2), \zeta_k) \approx 2$. In fact, usually most elements in $\mathbf{KSS}(B_1, B_2)$ do not generate potential families with a small ρ value. In subsection 3.1, we exhibit sets of algebraic numbers with a proven bound on the ρ-value of the potential families they generate. Theorem 1 is the main result, giving the general formula for the bound on the ρ-value. We give more explicit bounds in Theorem 2. In subsection 3.2, we discuss the interest of the method.

3.1. **The method.** Let $k \geq 1$ be an integer, let D be a squarefree positive integer, and let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Let $F = \mathbb{Q}(\sqrt{-D}) \subset \overline{\mathbb{Q}}$ and let $K = F\mathcal{C}_k \subset \overline{\mathbb{Q}}$. One can see K as an F-vector space. Let $F\zeta_k$ be the F-vector line in K spanned by ζ_k.

$$F\zeta_k = \{\alpha\zeta_k; \alpha \in F\} = \{(a + b\sqrt{-D})\zeta_k; a, b \in \mathbb{Q}\}.$$

Let $\theta \in F\zeta_k$, and assume θ is a primitive element in K (over $\mathbb{Q}$). Let R be the minimal polynomial of θ (over $\mathbb{Q}$). Set

$$\alpha = \theta/\zeta_k \in F.$$

Let e be the minimal divisor of k such that $\zeta_k^e \in F$. Assume that $\theta^e \in F$ is a primitive element in F. Note that this assumption is not very restrictive.

Since $\alpha, \sqrt{-D} \in F$, there exist P_1, P_2 and P_3, three rational polynomials of degree at most 1 such that:

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

Then one has

$$P_1(\theta^e)\theta + 1 = \theta/\alpha + 1 = \zeta_k + 1$$

and

$$P_2(\theta^e)\theta - P_3(\theta^e) = \zeta_k/\sqrt{-D} - 1/\sqrt{-D} = (\zeta_k - 1)/\sqrt{-D}\ .$$

Let T be the canonical rational polynomial mapping θ to $\zeta_k + 1$, and let Y be the canonical rational polynomial mapping θ to $(\zeta_k - 1)/\sqrt{-D}$. Then T is the remainder of the Euclidean division of $P_1(X^e)X + 1$ by R. As such, one has

$$\deg T \leq \deg(P_1(X^e)X + 1) \leq e + 1\ .$$

Similarly, one has $\deg(Y) \leq \deg(P_2(X^e)X - P_3(X^e)) \leq e + 1$. Consequently

$$\max(\deg(T), \deg(Y)) \leq e + 1\ .$$

Let $Q = (T^2 + DY^2)/4$, then

$$\deg(Q) \leq 2e + 2\ .$$

Thus, since $\deg R = [K : \mathbb{Q}]$, one has

$$\rho(\theta, \zeta_k) \leq \frac{2e + 2}{[K : \mathbb{Q}]}\ .$$

Moreover, if $\frac{2e+2}{[K:\mathbb{Q}]} < 2$, i.e. if $e + 1 < \deg R$, one has

$$T = P_1(X^e)X + 1 \text{ and } Y = P_2(X^e)X - P_3(X^e)$$

by definition of remainder of a Euclidean division of polynomials. Now, since α and $\alpha\sqrt{-D}$ can not be rationals simultaneously, then at least one of P_1 or P_2 must have degree 1. Then at least one of T or Y must have degree $e + 1$. Thus, in this case we have an equality

$$\rho(\theta, \zeta_k) = \frac{2e + 2}{[K : \mathbb{Q}]}\ .$$

Theorem 1. *With the notation of the beginning of subsection 3.1, let*

$$\mathcal{S} = \{\theta \in F\zeta_k \text{ primitive in } K \mid \theta^e \text{ is primitive in } F\}.$$

Then

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{2e + 2}{[K : \mathbb{Q}]}.$$

Moreover, if $\frac{2e+2}{[K:\mathbb{Q}]} < 2$, *then*

$$\rho(\mathcal{S}, \zeta_k) = \frac{2e+2}{[K:\mathbb{Q}]}.$$

Remark 6. Note that the construction can be generalized very simply to the case where F is an extension of $\mathbb{Q}(\sqrt{-D})$. Then P_1,P_2,P_3 have degree at most $[F:\mathbb{Q}]-1$ and the bound on the ρ-value becomes:

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{2e([F:\mathbb{Q}]-1)+2}{[K:\mathbb{Q}]}.$$

We studied the cases where F is not quadratic as well, and found that the method produced potential families with a larger ρ-value (but smaller than 2 in some cases).

We now give more explicit bounds on $\rho(\mathcal{S}, \zeta_k)$.

Theorem 2. *With the notation of Theorem 1:*

(1) Assume that k *is a multiple of* 6 *and* $D = 3$. *Then* $e = k/6$ *and*

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{(k/3+2)}{\varphi(k)}.$$

(2) Assume that k *is a multiple of* 4 *and* $D = 1$. *Then* $e = k/4$ *and*

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{(k/2+2)}{\varphi(k)}.$$

(3) Assume that k *is an odd multiple of* 3 *and* $D = 3$. *Then* $e = k/3$ *and*

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{(2k/3+2)}{\varphi(k)}.$$

(4) Assume that k *is even and* $\sqrt{-D} \notin \mathcal{C}_k$. *Then* $e = k/2$ *and*

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{(k/2+1)}{\varphi(k)}.$$

(5) Assume that k *is odd and* $\sqrt{-D} \notin \mathcal{C}_k$. *Then* $e = k$ *and*

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{(k+1)}{\varphi(k)}.$$

Proof. We only prove case 4 as an example. Assume that k is even and $\sqrt{-D} \notin \mathcal{C}_k$. Then $[K:\mathbb{Q}] = 2\varphi(k)$ as K is a quadratic extension of $\mathcal{C}_k$. Now we prove $e = k/2$. Since $\sqrt{-D} \notin \mathcal{C}_k$, then ζ_k^e is not primitive in F (otherwise $F \subset \mathcal{C}_k$), and F is quadratic so ζ_k^e is rational. Then $\zeta_k^e \in \{1, -1\}$, because ζ_k^e is a root of unity. Since k is even, $e = k/2$ and $\zeta_k^e = -1$. Thus,

$$\rho(\mathcal{S}, \zeta_k) \leq \frac{2e+2}{[K:\mathbb{Q}]} = \frac{k+2}{2\varphi(k)} = \frac{k/2+1}{\varphi(k)}.$$

□

We refer to the method of generation of families via exhaustive search over the algebraic integers of $\mathcal{S}$ as the subfield method. Note that considering only algebraic integers is not very restrictive, as one can obtain remaining potential families by applying an affine substitution (over $\mathbb{Q}$).

Example 2. Let $k = 22$ and $D = 7$. Fix an algebraic closure of $\mathbb{Q}$. Let $F = \mathbb{Q}(\sqrt{-7})$. Let $K = F\mathcal{C}_{22}$. Let ζ_{22} be a primitive 22-th root of unity, and let $\omega = \frac{1+\sqrt{-7}}{2}$. In particular, we have $K = \mathbb{Q}(\omega, \zeta_{22})$. Let $\alpha = 1 + \omega$ and $\theta = \alpha\zeta_{22}$. We have $\zeta_{22}^{11} \in F$, and $\theta^{11} \notin \mathbb{Q}$. Therefore, $\mathbb{Q}(\theta^{11}) = F$, and $\theta \in \mathcal{S}$.

We obtain using our Sagemath implementation [27, 16]:

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

Therefore, the potential family generated by θ has ρ-value $\rho = 6/5$. In fact, one can check that this is a family. Note that R is not monic, because we wanted to make R represent primes. In fact, this family has a smaller ρ-value than the previous record family for the embedding degree $k = 22$ (the previous record was $\rho = 13/10$). We obtain seeds in Section 5.2.

Remark 7. Note that when $D = 1$ or $D = 3$ and for some values of k, every element in $\mathcal{S}$ is an element in $\mathbf{KSS}(2, B)$ for B sufficiently large. More precisely, take $\ell = \mathrm{lcm}(k, 4))$ if $D = 1$ or $\ell = \mathrm{lcm}(k, 3)$ if $D = 3$. Let ζ_ℓ be a ℓ-th root of unity in $\mathcal{C}_\ell$. Then $\zeta_k := \zeta_\ell^{\ell/k}$ is a primitive k-th root of unity. Moreover, there exists $d \in \{3, 4, 6\}$ maximal such that $\zeta_d := \zeta_\ell^{\ell/d} \in F$ is a non-rational root of unity in $F = \mathbb{Q}(\sqrt{-D})$. Then for any $\theta \in \mathcal{S}$, there exists two rationals a and b such that

$$\theta = (a\zeta_d + b)\zeta_k = (a\zeta_\ell^{\ell/d} + b)\zeta_\ell^{\ell/k}.$$

If $\ell/d + \ell/k < \varphi(\ell)$ then $\theta \in \cup_{B>0} \mathbf{KSS}(2, B)$. In particular, one can check that the inequality holds when $k \in \{16, 18, 22, 32, 36, 40, 46\}$. Moreover, it so happens that the families introduced by Kachisa et al. come from elements in such an $\mathcal{S}$. Therefore, we can see the subfield method as a refinement of the enumeration method of Kachisa et al. in these cases. This also means that when $D \in \{1, 3\}$ one can produce any family generated with the subfield method using the KSS method, at the expense of a longer exhaustive search. However, when $D \notin \{1, 3\}$, the subfield method is a strict generalization of the work of Kachisa et al.

3.2. **Discussion on the interest of the method.** The interest of the subfield method relies on being able to satisfy the following conditions:

(1) the method produces potential families with a smaller ρ-value than the reference values from the first column of [14, Table 8.2].
(2) the method produces families (i.e. not only potential families).
(3) the method produces families which themselves produce pairing-friendly curves of an appropriate size.

The idea behind condition 3 is that, in practice, we need to find an integer x such that the polynomial $Q(x)$ is a prime integer and such that $R(x)$ is (almost) a prime integer of a given size (related to the desired level of security). It may happen that such an integer x does not exist (the first primes $Q(x)$ and $R(x)$ are too large). For a given embedding degree k, the main obstacle to the existence of such an x is the denominator Δ of Q (i.e. the smallest positive integer such that ΔQ is integer-valued). The subfield method, like the KSS method, can produce families where Δ is quite large. Yet, we will present in Section 5 new families suitable for the 192-bit security level, for which all the conditions are satisfied.

The ρ-values of the (actual) families we found with the new method were at least as small as the ρ-values in [14, Table 8.2] for every embedding degree $k \nmid 12$. In Table 1, we compiled the cases where the ρ-value is improved. The ρ-value is in bold when it is an improvement over [14, Table 8.2], and a cell is green if we were able to

find a family among the potential families we computed. We think the family for $k = 22$ has a cryptographic interest (when the base field $\mathbb{F}_q$ should have minimal size), and give more details in Section 5. Our new families with $k = 20$ improve over Construction 6.4 [14]: the ρ-value is unchanged but our $Q(X)$ is not affected with the refined SNFS attack of [18], as we explain in Section 5.1.1.

k	$\rho, D = 1$	$\rho, D = 3$	$\rho, \sqrt{-D} \notin \mathcal{C}_k$	ρ, Previous method
16	1.250	1.125	**1.125**	1.250, [14, 6.11]
22	**1.200**	**1.200**	**1.200**	1.300, [14, 6.3]
28	1.333	1.250	**1.250**	1.333, [14, 6.4]
40	1.375	1.3125	**1.3125**	1.375, [14, 6.11]
46	1.091	1.091	**1.091**	1.136, [14, 6.3]

TABLE 1. Comparison of the ρ-values of potential families generated by the subfield method with the state of the art [14].

4. Algorithms for computing integer roots modulo prime powers

Checking if a potential family is indeed a family requires essentially to be able to check if a rational polynomial takes an integer value at some integer, and if a rational polynomial represents primes. Both problems reduce to being able to solve the following.

Let $P \in \mathbb{Z}[X]$ be an integral polynomial, p be a prime integer, and n be a positive integer. We want to solve

$$P(x) \equiv 0 \bmod p^n \tag{4.1}$$

where x is an integer variable. The standard approach to this problem is to start by solving

$$P(x) \equiv 0 \bmod p$$

and then lifting the solutions modulo p^n. Hensel's lemma [25] is used to lift any *simple* root modulo p to a unique root modulo p^n. However, the literature is quite sparse for the degenerate case. In this section, we give a general algorithm for solving such polynomial equations. We start by giving an appropriate way to represent the set of solutions of Equation (4.1) in subsection 4.1. In subsection 4.2, we introduce the μ function, which is central in the final algorithm, and explain how to compute it. Finally, in subsection 4.3, we present Algorithm 4.1 which solves Equation (4.1).

4.1. Representing the set of solutions.

We will use the following elementary sets to describe the set of solutions of $P(x) = 0 \bmod p^n$ in $\mathbb{Z}$.

Definition 5. Let a be an integer and let $j \geq 0$ be an integer. We define

$$D(a, j) = \{x \in \mathbb{Z} \mid x \equiv a \bmod p^j\}$$

the p-congruence class of a modulo p^j. It is indeed a congruence class.

The following proposition will prove useful later.

Proposition 2. *Let a_1, a_2 be integers and let j_1, j_2 be two integers larger than 0 such that $j_1 \leq j_2$. Define $D(a_1, j_1)$ and $D(a_2, j_2)$ as in Definition 5. Assume that*

$$D(a_1, j_1) \cap D(a_2, j_2) \neq \emptyset.$$

Then

$$D(a_2, j_2) \subset D(a_1, j_1).$$

Proof. Let $x \in D(a_1, j_1) \cap D(a_2, j_2)$ be an integer. Then

$$x \equiv a_1 \bmod p^{j_1} \text{ and } x \equiv a_2 \bmod p^{j_2}.$$

Since $j_1 \leq j_2$, one has

$$x \equiv a_2 \bmod p^{j_1}.$$

Thus,

$$a_2 \equiv a_1 \bmod p^{j_1} \text{ and } D(a_2, j_2) \subset D(a_1, j_1).$$

□

Now, let $S \subset \mathbb{Z}$ be a p^n-periodic set of integers.

Definition 6. A representation by p-congruence classes of S is a collection of p-congruence classes $(D(a_i, j_i))_{i \in I}$ such that

$$S = \cup_{i \in I} D(a_i, j_i).$$

It is called finite if I is finite.

Remark 8. S always admits a finite representation by p-congruence classes. Indeed, S is p^n-periodic, which means that S is a (finite) union of classes of integers modulo p^n. More clearly,

$$S = \cup_{a \in S \cap [0, p^n - 1]} D(a, n).$$

We want to define a canonical finite representation by p-congruence classes of S. A first step is to ask that the congruence classes $(D(a_i, j_i))_{i \in I}$ be disjoint, but it is not sufficient. Let a be an integer and let $j \geq 0$ be an integer. Then $D(a, j) = \cup_{i=0}^{p-1} D(a + i \cdot p^j, j + 1)$, and the union on the right is disjoint. It turns out that this is the only other obstacle.

Definition 7. Let C be a p-congruence class in S. We say that C is maximal in S if it is maximal as a p-congruence class for the inclusion.

Let $a \in S$ be an integer. According to Proposition 2, S is the disjoint union of its maximal p-congruence classes. The representation of S composed of its maximal p-congruence classes is called the **reduced representation** of S.

4.2. **The key quantity.** Recall that we ultimately want to compute the set

$$S = \{x \in \mathbb{Z} \mid P(x) \equiv 0 \bmod p^n\}. \tag{4.2}$$

Since S is p^n-periodic, we ask to compute a reduced representation of S by p-congruence classes. The content of this section will help us to achieve this goal in the following subsection. Let us define

$$\mu(P) = \sup\{j \in \mathbb{Z}_{\geq 0} \mid \forall x \in \mathbb{Z}, P(x) \equiv 0 \bmod p^j\}\ . \tag{4.3}$$

Example 3. We give two toy examples for the prime $p = 2$:

- let $P = X^2 + 3$. Observe that $P(0) = 3 \not\equiv 0 \bmod 2$. Then $\mu(P) = 0$.
- let $P = X^2 - X$. Since for any integer x, either x or $x - 1$ is even, $P(x)$ is even. Thus, one can check that $\mu(P) = 1$.

It is easily seen that $S = \mathbb{Z}$ if and only if $\mu(P) \geq n$. More generally, one can use the μ function to check if a p-congruence class is in S.

Proposition 3. *Let n be a positive integer, let $P \in \mathbb{Z}[X]$, and let S and μ be as in Equations (4.2) and (4.3). Let a be an integer and let $j \geq 0$ be an integer. Define $D(a, j)$ as in Definition 5. Then*

$$\mu(P(a + p^j X)) \geq n \text{ if and only if } D(a, j) \subset S.$$

Proof.

$$\begin{aligned}\mu(P(a+p^jX)) \geq n &\Leftrightarrow \forall b \in \mathbb{Z}, P(a+p^jb) \equiv 0 \bmod p^n \\ &\Leftrightarrow \forall x \in D(a,j), P(x) \equiv 0 \bmod p^n \\ &\Leftrightarrow D(a,j) \subset S.\end{aligned}$$

□

Therefore, being able to evaluate μ allows us to check if a p-congruence class is in the set of solutions S. The following theorem explains how to evaluate μ.

Theorem 3. *Let $P \in \mathbb{Z}[X]$ and let p be a prime integer. Let μ be the function defined in Equation (4.3). Let $a_0, a_1, \ldots, a_{\deg P}$ be integers such that*

$$P = \sum_{i=0}^{\deg P} a_i \binom{X}{i}$$

where

$$\binom{X}{i} = \frac{X(X-1)\ldots(X-i+1)}{i!}.$$

Then

$$\mu(P) = \min_{0 \leq i \leq \deg P} (\mathrm{val}_p(a_i)).$$

Proof. It is well-known that $(\binom{X}{i})_{i \in \mathbb{Z}}$ is a $\mathbb{Z}$-basis of the group of integer-valued polynomials. Since P is integer valued, such $a_0, a_1, \ldots, a_{\deg P}$ exists.

Let $m = \min_{0 \leq i \leq \deg P} (\mathrm{val}_p(a_i))$. It is clear that

$$\mu(P) \geq m.$$

Let $0 \leq i_0 \leq \deg P$ be the smallest integer such that

$$\mathrm{val}_p(a_{i_0}) = m.$$

Then

$$\begin{aligned}P(i_0) &= \sum_{i=0}^{\deg P} a_i \binom{i_0}{i} \\ &= \sum_{i=0}^{i_0} a_i \binom{i_0}{i} \\ &\equiv a_{i_0} \binom{i_0}{i_0} \bmod p^{m+1} \text{ by minimality of } i_0 \\ &\equiv a_{i_0} \bmod p^{m+1} \\ &\not\equiv 0 \bmod p^{m+1}.\end{aligned}$$

Thus,

$$\mu(P) \leq m.$$

□

4.3. **Computing the roots of a polynomial modulo a prime power.** We design a recursive algorithm to compute a reduced representation of the set S of integer solutions of

$$P(x) \equiv 0 \bmod p^n.$$

The idea of the algorithm is actually very straightforward. One computes μ to check if $\mu(P) \geq n$. If the answer is yes, one knows that $S = \mathbb{Z}$. Otherwise, we recursively search for solutions in every congruence class modulo p using substitutions.

Before presenting Algorithm 4.1, let us recall the following lemma.

Lemma 2. *Let $P \in \mathbb{Z}[X]$, let p be a prime integer and let a be any integer. Then*

$$P(a) \equiv 0 \bmod p$$

if and only if

$$p \mid P(a + pX), \text{ i.e. } \frac{P(a+pX)}{p} \in \mathbb{Z}[X].$$

Proof. One can check that there exists a polynomial $Q \in \mathbb{Z}[X]$ such that

$$P(a + X) = P(a) + X \cdot Q(X).$$

Thus,

$$P(a + pX) = P(a) + pX \cdot Q(pX),$$

and one can easily deduce the lemma. □

Algorithm 4.1 is given below. One can easily see that the algorithm finishes because n is strictly decreasing in the tree of recursion, and is lower bounded by 0. Correctness comes from Proposition 3 and the observation that if

$$P(a) \not\equiv 0 \bmod p$$

then

$$\forall x \equiv a \bmod p, P(x) \not\equiv 0 \bmod p.$$

Algorithm 4.1: RootsModPrimePowers(P, p, n)
Input: $P \in \mathbb{Z}[X]$, p a prime integer, $n \geq 0$ an integer

```
if μ(P) ≥ n then
    Return D(0, 0).
else
    S ← ∅
    for 0 ≤ a ≤ p − 1 do
        if P(a) ≡ 0 mod p then
            Q ← P(a + pX)/p
            ∪_{i∈I} D(a_i, j_i) ← RootsModPrimePowers(Q, p, n − 1)
            S ← ∪_{i∈I} D(a + p · a_i, j_i + 1) ∪ S
    Return S.
```

Remark 9. We presented the algorithm with the goal to make it as clear as possible. It can be improved in many ways. Firstly, rather than testing if $P(a) \equiv 0 \bmod p$ for every $a \bmod p$, one should use the Berlekamp algorithm to compute every root of P modulo p. Secondly, one should divide $P(a + pX)$ by the largest power of p possible, in order to reduce the size of the tree of recursion. Finally, one should always seek to use Hensel's lemma, whenever possible during the recursion. The algorithm is implemented with all these improvements in [16].

5. Applications

This section investigates the practical aspects of our new families of curves. First, we identify possible interesting embedding degrees and discriminants (Section 5.1). Second, we generate seeds for these families, that produce curves of cryptographic size (Section 5.2). Third, we sketch and estimate the cost of an optimal ate pairing on these curves (Section 5.3). We also give $\mathbb{G}_1$ group operation formulas for the curve with $k = 22$.

5.1. Our selected families of curves.

We highlight $k = 20, 28$ curves with $D = 1$, and $k = 22$, $D = 7$, $k = 28$, $D = 11$ curves.

5.1.1. *Better security for $k = 20$, $k = 28$ with $D = 1$.* In [18], Guillevic identified that the curve families whose polynomial $Q(X)$ defining the field characteristic has an endomorphism, are weaker with respect to the Special Number Field Sieve algorithm to compute discrete logarithms in the field, as the endomorphism allows selecting a better polynomial for NFS (it works also for the Tower variant TNFS). To illustrate this, take a target embedding degree $k = 20$ and consider [14, Construction 6.4], having $\rho = 3/2$. The polynomials are

- $R(X) = \Phi_{20}(X) = X^8 - X^6 + X^4 - X^2 + 1$,
- $T(X) = X + 1$,
- $H = (X - 1)^2(X^2 + 1)/4$,
- $Q = (X^{12} - 2X^{11} + X^{10} + X^2 + 2X + 1)/4$,
  with an automorphism $\sigma(X) = -1/X$, so that $X^{12}Q(\sigma(X)) = Q(X)$.

From the trace $\mathrm{Id} + \sigma$, a polynomial of degree 6 is obtained, $M(X) = X^6 - 2X^5 + 7X^4 - 10X^3 + 13X^2 - 10X + 4$ (the minimal polynomial of $\alpha - 1/\alpha$, where α is a root of $Q(X)$). $M(X)$ allows a better parameterization of the special number field sieve. Without going into details, a pair of polynomials $(m(x), u(x))$ such that $\mathrm{Res}(m, u) = q$ (or a small multiple of q) is required for running the SNFS algorithm [21]. The pair $(4Q(X), X - x)$, with x the seed so that $q = Q(x)$, usually plays this role. With the automorphism, one can choose instead $(M(X), xX - x^2 + 1)$ whose resultant in X is $4Q(x) = 4q$. Because of this automorphism exploited in SNFS, the field size for $k = 20$ should be enlarged (otherwise, only 180 bits of security are offered for q of 574 bits, r of 384 bits). In [18, Table 10], a field size of 670 bits with a subgroup order of 448 bits corresponds to the 192-bit security level. With our new $k = 20$ family of curves (having the same ρ-value $3/2$), no automorphism exists, and the trick above does not apply, so there is no need to take a larger field size. We can consider the minimal size such that r is about 384-bit long, and q about 576 bits. The same observation applies to $k = 28$: $\sigma(X) = -1/X$ acts on $Q(X) = (X^{16} - 2X^{15} + X^{14} + X^2 + 2X + 1)/4$ of Construction 6.4, and the minimal polynomial of $\alpha - 1/\alpha$ is $M(X) = X^8 - 2X^7 + 9X^6 - 14X^5 + 26X^4 - 28X^3 + 25X^2 - 14X + 4$. The pair $(M(X), xX - x^2 + 1)$ can be chosen to parameterize SNFS, obtaining a better estimated running-time. Our $k = 28$, $D = 1$ family of curves (Example 6) does not have this weakness. That is why later, Aranha, Fotiadis and Guillevic take our new $k = 20$ and $k = 28$ curves with $D = 1$ [1] instead of the Freeman-Scott-Teske 6.4 construction. We summarize the polynomials of the two families in Examples 4 and 5. To further optimize the arithmetic operations on the curves with $k = 20$, 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 $\mathbb{F}_{q^{20}}$. In other words, we add the condition $(Q(X) - 1)/5$ generates integers. We obtain the following two families that we call GG20a and GG20b.

Example 4 (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

- $T = (2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 - 44X - 190)/205$
- $H = 125(X^2 - 2X + 5)(X^2 - 4X + 5)/164$
- $R = (X^8 + 4X^7 + 11X^6 + 24X^5 + 41X^4 + 120X^3 + 275X^2 + 500X + 625)/25625$
- $Q = (X^{12} - 2X^{11} + 5X^{10} + 76X^7 + 176X^6 + 380X^5 + 3125X^2 + 12938X + 15625)/33620$

is a family of elliptic curves with discriminant $D = 1$ and ρ-value $\rho = 3/2$. With $x \equiv 69, 75, 79, 135, 175, 239, 299, 315, 325, 339 \bmod 410$, the first conditions of Definition 2 are met (all parameters take integer values). Furthermore with $x = 1715, 1815 \bmod 2050$, Q and R generate primes, and $q = Q(x) \equiv 1 \bmod 5$.

Example 5 (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

- $T = (-2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 + 44X + 190)/205$
- $H = 125(X^2 - 2X + 5)(X^2 + 4X + 5)/164$
- $R = (X^8 - 4X^7 + 11X^6 - 24X^5 + 41X^4 - 120X^3 + 275X^2 - 500X + 625)/25625$
- $Q = (X^{12} - 2X^{11} + 5X^{10} - 76X^7 - 176X^6 - 380X^5 + 3125X^2 + 12938X + 15625)/33620$

is a family of elliptic curves with discriminant $D = 1$ and ρ-value $\rho = 3/2$. With $x \equiv 71, 85, 95, 111, 171, 235, 275, 331, 335, 341 \bmod 410$, the first conditions of Definition 2 are met. Furthermore with $x \equiv 1465, 1565 \bmod 2050$, Q and R generate primes, and $q = Q(x) \equiv 1 \bmod 5$.

For completeness, we also mention $k = 28$, $D = 1$.

Example 6 (GG28). Let $k = 28$ a multiple of 4, $D = 1$ and $F = \mathcal{C}_4$. Let $\theta = (1 + 2\zeta_4)\zeta_k$. Then

- $T = (-2X^8 - 527X + 145)/145$
- $Y = (X^8 - 5X^7 + 336X - 1390)/145$
- $H = (X^2 - 2X + 5)(X^2 - 4X + 5)/580$
- $R = (X^{12} + 4X^{11} + 11X^{10} + 24X^9 + 41X^8 + 44X^7 - 29X^6 + 220X^5 + 1025X^4 + 3000X^3 + 6875X^2 + 12500X + 15625)/29$
- $Q = (X^{16} - 2X^{15} + 5X^{14} + 556X^9 - 1344X^8 + 2780X^7 + 78125X^2 - 217382X + 390625)/16820$

is a family of elliptic curves with discriminant $D = 1$ and ρ-value $\rho = 3/4$. With $x \equiv 309, 449, 1759, 1899 \bmod 2030$, the conditions of Definition 2 are met, Q and R generate primes, and $q = Q(x) \equiv 1 \bmod 7$. (The family obtained with $\theta = (1 - 2\zeta_4)\zeta_k$ does not have $q \equiv 1 \bmod 7$).

5.1.2. *Smallest ρ-values for $k = 22$, $k = 28$.* We already presented our family with $k = 22$, $D = 7$ in Example 2. The seed should satisfy $x \equiv 32, 151 \bmod 161$ for Q, R to generate primes. For $x \equiv 4, 18, 25, 39, 81, 95, 116, 123, 144 \bmod 161$, Q and $R/23$ generate primes.

Here is our family with smallest ρ-value at $k = 28$. We obtain manageable denominators with $D = 11$ (Example 7).

Example 7. Let $k = 28$, $D = 11$, $F = \mathbb{Q}[x]/(x^2 + x + 3)$, $\omega = (-1 + \sqrt{-11})/2$, $\alpha = \omega$, $(a, b) = (0, 1)$, $\theta = \alpha\zeta_k$.

- $T = (X^{15} + 718X + 3237)/3237$
- $Y = (X^{15} + 6X^{14} + 7192X + 7545)/35607$
- $R = (X^{24} + 5X^{22} + 16X^{20} + 35X^{18} + 31X^{16} - 160X^{14} - 1079X^{12} - 1440X^{10} + 2511X^8 + 25515X^6 + 104976X^4 + 295245X^2 + 531441)/(3^{12} \cdot 13^2 \cdot 83^2)$
- $Q = (X^{30} + X^{29} + 3X^{28} + 2515X^{16} + 14384X^{15} + 7545X^{14} + 4782969X^2 + 13304911X + 14348907)/38419953$
- $H = 3^{11}(X^2 + X + 3)(X^4 - 5X^2 + 9)/11$

With a seed $x \equiv 5076, 9366, 13293, 17583 \bmod 35607$.

5.2. **Generating seeds for curves of cryptographic size.** To generate seeds, we incorporated our families of curves in [20] in `tnfs/curve/gg.py` and adapted `tnfs/gen/generate_sparse_curve.py` to be able to call the generation of seeds for each curve family. We obtain the seeds in Table 2. For GG20a and GG20b we present the seeds of smallest possible Hamming weight such that $q = Q(x)$ is at most 576-bit long (9 limbs of 64-bits). It implies $r = R(x)$ of 379 or 380 bits (almost 384 bits). For GG22D7 we obtain only three seeds of Hamming weight at most 8, so that r is close to 384 bits. Later in [1], seeds for $k = 28$, $D = 1$ were given.

curve family	seed x	$\log q$	$\log r$	ρ	$\log q^k$	secu $\mathbb{F}_{q^k}$
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	$-2^{19}-2^{17}-2^{15}-2^{13}-2^7+1$	453	380	1.19	9966	220
GG22D7	$-2^{20}+2^{18}+2^{14}+2^{12}+2^{10}-2^8-2^5+1$	457	382	1.20	10054	220
GG22D7	$-2^{20}+2^{18}+2^{13}-2^{10}-2^8-2^2+1$	457	383	1.19	10054	220

TABLE 2. Parameters of our new curves at the 192-bit security level.

5.3. **Pairing implementation.** We refer to [8] for an introduction on pairing computation. Curves with a twist are well-suited for an efficient *optimal ate pairing* computation. The pairing is a bilinear map on input two groups of points $\mathbb{G}_1$, $\mathbb{G}_2$ on the elliptic curve, to a target group $\mathbb{G}_T$ in the finite field extension $\mathbb{F}_{p^k}$. From Section 2.1, for the optimal ate pairing, $\mathbb{G}_1 = E[r] \cap \ker(\pi_q - \mathrm{Id}) = E(\mathbb{F}_q)[r]$ and $\mathbb{G}_2 = E(\mathbb{F}_{q^k})[r] \cap \ker(\pi_q - [q])$.

5.3.1. *Miller loop of optimal ate pairing.* Our GG20a, GG20b curves have a quartic twist, our GG22D7 curve has a quadratic twist so that we consider the formulas for an optimal ate pairing. The key-ingredient is to obtain an equation of the form $s = \sum_{i=0}^{\varphi(k)-1} c_i q^i \equiv 0 \bmod r$, with tiny coefficients c_i. We wrote a Magma script for that, as Magma [4] has lattice reduction over polynomial rings available, while SageMath does not. Once the equation in terms of powers of q is obtained, the optimal ate pairing formula on input points $(P_1, P_2) \in \mathbb{G}_1 \times \mathbb{G}_2$ is given by a Miller function evaluated at P_1, written $f_{s,P_2}(P_1) = f_{c_0+c_1 q+\ldots+c_{\varphi(k)-1}q^{\varphi(k)-1},P_2}(P_1)$ that can be further simplified. A *Miller function* $f_{c,P_2}(P_1)$ has principal divisor $\mathrm{div}(f_{c,P_2}) = c(P_2) - ([c]P_2) - (c-1)(\mathcal{O})$ and is evaluated at the coordinates of the point P_1. In other words, the function f_{c,P_2} has a zero of order c at P_2, a pole of order 1 at $[c]P_2$, and a pole of order $(c-1)$ at the point at infinity $\mathcal{O}$. The classical formulas are $f_{1,P_2} = 1$; $f_{i+j,P_2} = f_{i,P_2} \cdot f_{j,P_2} \cdot \ell_{iP_2,jP_2}/v_{(i+j)P_2}$ where ℓ_{iP_2,jP_2} denotes the line equation through iP_2 and jP_2, and $v_{(i+j)P_2}$ denotes the vertical line at $(i+j)P_2$; and $f_{ij,P_2} = f_{i,P_2}^j \cdot f_{j,[i]P_2}$.

Improvements when computing the Miller function $f_{s,P_2}(P_1)$ apply, in our case because of the even embedding degree k, the vertical lines in the Miller algorithm to compute the Miller function can be omitted. We sketch the other obvious optimizations for each curve in the following.

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

$$x - q(x) + 2(q(x))^6 \equiv 0 \bmod r(x) \tag{5.1}$$

hence the formula, where $\pi(P_2) = [q]P_2$, $\pi^6(P_2) = [q^6]P_2$:

$$e(P_1,P_2) = f_{x,P_2}(P_1) f_{-1,\pi(P_2)}(P_1) f_{2,\pi^6(P_2)}(P_1) \ell_{[x]P_2,-\pi(P_2)}(P_1) \ell_{xP_2-\pi(P_2),\pi^6([2]P_2)}(P_1)\,.$$

Well-known simplifications apply: $f_{-1,\pi(P_2)}(P_1)$ can be dropped off, and the same for the line $\ell_{xP_2-\pi(P_2),\pi^6([2]P_2)}(P_1)$ as it will be a vertical. Moreover, $f_{2,\pi^6(P_2)}(P_1)$ costs a double-line step $\ell_{\pi^6(P_2),\pi^6(P_2)}(P_1) = \ell^{q^6}_{P_2,P_2}(P_1)$. Finally,

$$e(P_1,P_2) = f_{x,P_2}(P_1) \ell^{q^6}_{P_2,P_2}(P_1) \ell_{[x]P_2,\pi(-P_2)}(P_1)\,. \tag{5.2}$$

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

$$x - q(x) - 2(q(x))^6 \equiv 0 \bmod r(x) \tag{5.3}$$

$$e(P_1, P_2) = f_{x,P_2}(P_1)\ell^{q^6}_{-P_2,-P_2}(P_1)\ell_{[x]P_2,\pi(-P_2)}(P_1)\ . \tag{5.4}$$

For our new $k = 22$ curve with $D = 7$, we get

$$x^2 - xq(x) + 2(q(x))^2 \equiv 0 \bmod r(x) \tag{5.5}$$

hence the optimal ate Miller loop formula

$$e(P_1, P_2) = f_{x^2,P_2}(P_1)f_{-x,\pi(P_2)}(P_1)f_{2,\pi^2(P_2)}(P_1)\ell_{[x^2]P_2,-\pi([x]P_2)}(P_1)\ell_{x^2P_2-\pi([x]P_2),\pi^2([2]P_2)}(P_1)$$

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

$$e(P_1, P_2) = f_{x^2,P_2}(P_1)f^{-q}_{x,P_2}(P_1)\ell^{q^2}_{P_2,P_2}(P_1)\ell_{[x^2]P_2,-\pi([x]P_2)}(P_1)\ . \tag{5.6}$$

Moreover one can share the computation of f_{x,P_2} inside f_{x^2,P_2}:

$$e(P_1, P_2) = f^x_{x,P_2}(P_1)f_{x,[x]P_2}(P_1)f^{-q}_{x,P_2}(P_1)\ell^{q^2}_{P_2,P_2}(P_1)\ell_{[x^2]P_2,-\pi([x]P_2)}(P_1)\ . \tag{5.7}$$

k	curve family	Equation	Optimal ate formula
20	GG20a	$u - q + 2q^6 \equiv 0 \bmod r$	$f_{u,P_2}(P_1) \cdot f_{2,\pi_{q^6}(P_2)}(P_1) \cdot \ell_{[u]P_2,-\pi_q(P_2)}(P_1)$
20	GG20b	$u - q - 2q^6 \equiv 0 \bmod r$	$f_{u,P_2}(P_1) \cdot f_{2,\pi_{q^6}(-P_2)}(P_1) \cdot \ell_{[u]P_2,-\pi_q(P_2)}(P_1)$
22	GG22D7	$u^2 - uq + 2q^2 \equiv 0 \bmod r$	$f^u_{u,P_2}(P_1)f_{u,[u]P_2}(P_1)f^{-q}_{u,P_2}(P_1)\ell^{q^2}_{P_2,P_2}(P_1)\ell_{[u^2]P_2,-\pi_q([u]P_2)}(P_1)$

TABLE 3. Optimal ate Miller loop formulas.

Miller algorithm (algorithm 5.1) computes a Miller function $f_{c,P_2}(P_1)$. Because our curves have even embedding degrees, we omit the vertical lines $v_{P_2}(P_1)$ in the formulas. Formulas for doubling step and addition step for our $k = 20$ curves can be found in Costello, Lange and Naehrig paper [9], and for $k = 22$ curves, in [7].

Algorithm 5.1: MILLERFUNCTION(c, P_1, P_2)
Input: $E, \mathbb{F}_q, \mathbb{F}_{q^k}$, k even, $P_1 \in E(\mathbb{F}_q)[r]$, $P_2 \in E(\mathbb{F}_{q^k})[r]$ such that $\pi(P_2) = [q]P_2$ in affine coord., $c \in \mathbb{Z}^*$.
Result: $f = f_{c,P_2}(P_1)$

$f \leftarrow 1$; $P_i \leftarrow P_2$;
if $c < 0$ **then** $P_i \leftarrow -P_i$; $c \leftarrow -c$;
for b *from the second most significant bit of* c *to the least* **do**
  $\ell_0 \leftarrow \ell_{P_i,P_i}(P_1)$; $P_i \leftarrow [2]P_i$; // Dbl step, tangent line
  $f \leftarrow f^2$; // $\mathbf{s}_k$
  if $b = 1$ **then**
    $\ell_1 \leftarrow \ell_{P_i,P_2}(P_1)$; $P_i \leftarrow P_i + P_2$; // 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;

5.3.3. *Final Exponentiation.* Like for KSS curves, the final exponentiation formulas are tedious to write down. The final exponentiation is decomposed into two parts, called easy and hard. For $k = 20$, one has:

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

For $k = 22$, this is

$$\frac{q^{22}-1}{r} = \frac{q^{22}-1}{\phi_{22}(q)}\frac{\phi_{22}(q)}{r} = \underbrace{(q^{11}-1)(q+1)}_{\text{easy}}\underbrace{\frac{\phi_{22}(q)}{r}}_{\text{hard}} .$$

The easy part costs one inversion and a few Frobenius powers. We apply the technique of Fuentes et al. [15] to simplify the hard part. We note that $q^8 \equiv q^6 - q^4 + q^2 - 1 \bmod \Phi_{20}(q)$ 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.

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

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

For the final exponentiation on GG22D7, with the same technique we obtain

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

Remark 10. We observe that in each hard final exponentiation formula, a factor of $H(X)$ shows up, namely $x^2 - 2x + 5$ for GG20a and GG20b, and $x^2 - x + 2$ for GG22D7. A similar pattern can be found for KSS16 and KSS18 curves [6].

Finally, we mention that Fouotsa et al. x-super-optimal ate pairing [13] can apply to this curve, but we did not investigate further. The formulas for this alternative pairing can be found in [23].

5.3.4. *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 $r = R(x)$. 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 $P'_2(x', y') \in E'_M(\mathbb{F}_{q^{11}})$. Then

$P_2 = \phi(P_2') = (x'/\omega^2, y'/\omega^3) = (x'/w, y'/w^2\omega)$ lies on $E(\mathbb{F}_{q^{22}})$. More precisely, x'/w is in the subfield $\mathbb{F}_{q^{11}}$. The vertical line equation at P_2 evaluated at P_1 is $v_{P_2}(P_1) = x_{P_2} - x_{P_1} = x'/w - x_{P_1} \in \mathbb{F}_{q^{11}}$. 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.

5.3.5. *Field extension representation for $k = 22$.* The polynomial shape of $q = Q(x)$ does not allow $q \equiv 1 \bmod 11$ and finding an irreducible binomial polynomial is not possible. We have chosen the alternative with a sparse polynomial of the form $x^{11} + v_1 x + v_0$ with tiny integers v_1, v_0. We represent elements of $\mathbb{F}_{q^{11}}$ as degree 10 polynomials modulo $x^{11} + v_1 x + v_0$. 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 8 (GG22D7-457). With the seed $x = -2^{20} + 2^{18} + 2^{13} - 2^{10} - 2^8 - 2^2 + 1$, $q = Q(x)$ 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 $E'_M \colon y^2 = x^3 + a\nu^2 x + b\nu^3$. The twist map is $\phi_M \colon (x', y') \mapsto (x'/\nu, y'/\nu^2\omega)$.

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

5.3.6. *SageMath proof-of-concept implementation.* We rely on SageMath for the finite field extension arithmetic (including Frobenius powers). We base our implementation on the MIT-licensed library of pairings at [12]. 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 is 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.

5.3.7. *Pairing cost estimation.* Our estimates are given in Table 4.

Curve family	q (bits)	r (bits)	Miller loop	final exponentiation easy	final exponentiation hard	final exponentiation total	pairing 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**

TABLE 4. Optimal ate pairing and final exponentiation cost estimates in terms of finite field multiplications $\mathbf{m}$ in $\mathbb{F}_q$.

5.3.8. *Group operations.* It becomes standard to give the formulas for subgroup membership testing and co-factor clearing on the three groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$. We apply the technique of Scott [24], generalized by Yu Dai et al. [10]. The formulas for GG20a, GG20b can be found in [1]. For GG2D7, on $\mathbb{G}_1$ the formulas are obtained with a GLV-like decomposition. The endomorphism comes from the Complex Multiplication by $(-1 + \sqrt{-7})/2$. It is textbook to obtain the formula on a curve of j-invariant -3375 from a 2-isogeny [26, Proposition 2.3.1]. With $E \colon y^2 = x^3 - 35x + 98$, $j(E) = -3375$, $\alpha = \frac{1+\sqrt{-7}}{2}$,

$$\phi(x, y) = \left(\alpha^{-2}\left(x - \frac{7(1-\alpha)^4}{x + \alpha^2 - 2}\right), \alpha^{-3} y \left(1 - \frac{7(1-\alpha)^4}{(x + \alpha^2 - 2)^2}\right)\right) .$$

The eigenvalue of ϕ is $(1+\sqrt{-7})/2$ in the appropriate subgroup of $E(\mathbb{F}_q)$. On $E(\mathbb{F}_q)[r]$, $\lambda = (x^{11}+45)/23$ is a root of $X^2 - X + 2$ modulo r. With SageMath, the endomorphism is easily obtained from a 2-isogeny whose kernel is a 2-torsion point, either $(3+\alpha, 0)$ or $(4-\alpha, 0)$. The rational point $(-7, 0)$ does not give an endomorphism. A fast multiplication by r for subgroup membership testing can be achieved with the formula $a_0 - a_1\lambda$, where $a_0^2 - a_0a_1 + 2a_1^2 = r$ exactly (Yu Dai's criterion). According to the congruence of the seed modulo 23, we give the integer values of (a_0, a_1) in Table 5. The subgroup membership testing boils down to testing if $[a_0]P - \phi([a_1]P)$ is $\mathcal{O}$. Yu Dai et al. [10] provided a trick to optimize and share the cost of the two scalar multiplications more efficiently than a generic multi-scalar multiplication. We refer to the online SageMath source code for further formulas [19].

$x \equiv 9 \bmod 23$
$a_0 = (-3x^{10} + 7x^9 - x^8 - 13x^7 + 15x^6 + 11x^5 - 41x^4 + 19x^3 + 63x^2 - 101x - 25)/23$ $a_1 = (2x^{10} + 3x^9 - 7x^8 + x^7 + 13x^6 - 15x^5 - 11x^4 + 41x^3 - 19x^2 - 63x + 101)/23$
$x \equiv 13 \bmod 23$
$a_0 = (-5x^{10} + x^9 + 9x^8 - 11x^7 - 7x^6 + 29x^5 - 15x^4 - 43x^3 + 73x^2 + 13x - 159)/23$ $a_1 = (-2x^{10} + 5x^9 - x^8 - 9x^7 + 11x^6 + 7x^5 - 29x^4 + 15x^3 + 43x^2 - 73x - 13)/23$
$x \equiv 1, 2, 3, 4, 6, 8, 12, 16, 18 \bmod 23$
$a_0 = (x^{10} - x^9 - x^8 + 3x^7 - x^6 - 5x^5 + 7x^4 + 3x^3 - 17x^2 + 11x + 23)/23$ $a_1 = (-x^9 + x^8 + x^7 - 3x^6 + x^5 + 5x^4 - 7x^3 - 3x^2 + 17x - 11)/23$

TABLE 5. $\mathbb{G}_1$ subgroup membership testing formulas for Example 2.

CONCLUSION

In this work, we generalized the KSS technique to generate complete families of pairing-friendly curves. Firstly, we introduced the *subfield method*, a method of generation of families of pairing-friendly curves generalizing the method of KSS. This new method uniformizes many of the previous best performing families, including the cyclotomic families and the KSS families, and provides a deeper mathematical understanding of the related methods. Using our new method, we have found new families of embedding degrees $k = 20$ and $k = 22$. 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 $\rho = 1.3$.

Secondly, we studied the problem of computing integer roots of an integral polynomial modulo prime powers. We proposed a simple and efficient method for solving this problem and use it to compute the integers x at which a rational polynomial takes integer values, and to check if a rational polynomial represents primes. This contribution comes with a SageMath open-source companion code available online [16]. We obtain seeds to generate new instances of elliptic curves of cryptographic interest at the 192-bit security level for the new families of embedding degrees $k = 20$, $k = 22$, and derive the optimal ate pairing and final exponentiation formulas. Finally, we implemented the pairing and group operations on our new curves in SageMath to validate the formulas [19].

As a closing remark, we would like to point out that the subfield method, in many cases, do not require a specific discriminant D. Thus, one could hope to improve the second column of [14, Table 8.2], which is concerned with the "variable

D" case. To accomplish this, one would need a better understanding of which choice of discriminant D allows us to produce (actual) families.

References

[1] Diego F. Aranha, Georgios Fotiadis, and Aurore Guillevic. A short-list of pairing-friendly curves resistant to the special TNFS algorithm at the 192-bit security level. *IACR Communications in Cryptology*, 1(3), 2024. ePrint 2024/1223.

[2] 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, Berlin, Heidelberg, September 2003.

[3] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 514–532. Springer, Berlin, Heidelberg, December 2001.

[4] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

[6] Shi Ping Cai, Zhi Hu, and Chang-An Zhao. Faster final exponentiation on the KSS18 curve. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E105.A(8):1162–1164, 2022. ePrint 2021/1309.

[7] 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, Berlin, Heidelberg, December 2005.

[8] Craig Costello. Pairings for beginners. www.craigcostello.com.au/s/PairingsForBeginners.pdf, 2012.

[9] 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, Berlin, Heidelberg, May 2010.

[10] Yu Dai, Kaizhan Lin, Chang-An Zhao, and Zijian Zhou. Fast subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on pairing-friendly curves. *Designs, Codes and Cryptography*, 91(10):3141–3166, 2023.

[11] Régis Dupont, Andreas Enge, and François Morain. Building curves with arbitrary small MOV degree over finite prime fields. *Journal of Cryptology*, 18(2):79–89, April 2005.

[12] 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.

[13] 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.

[14] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, April 2010. ePrint 2006/372.

[15] 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, Berlin, Heidelberg, August 2012.

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

[17] 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, Berlin, Heidelberg, May 2016.

[18] 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, *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part II*, volume 12111 of *LNCS*, pages 535–564. Springer, 2020. ePrint 2019/1371.

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

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

[21] Antoine Joux and Cécile Pierrot. The special number field sieve in $\mathbb{F}_{p^n}$ - application to pairing-friendly constructions. In Zhenfu Cao and Fangguo Zhang, editors, *PAIRING 2013*, volume 8365 of *LNCS*, pages 45–61. Springer, Cham, November 2014.

[22] 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. ePrint 2007/452.

[23] Jianming Lin, Chang-An Zhao, and Yuhao Zheng. Efficient implementation of super-optimal pairings on curves with small prime fields at the 192-bit security level. ePrint 2024/1195, 2024.

[24] Michael Scott. A note on group membership tests for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_t$ on BLS pairing-friendly curves. ePrint 2021/1130, 2021.

[25] Jean-Pierre Serre. *A course in arithmetic. Translation of "Cours d'arithmetique". 2nd corr. print*, volume 7 of *Grad. Texts Math.* Springer, Cham, 1978.

[26] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer New York, NY, 1 edition, 1994.

[27] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3)*, 2022. https://www.sagemath.org.

Univ. Bordeaux, INRIA, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
E-mail address: jean.gasnier@math.u-bordeaux.fr
URL: https://www.math.u-bordeaux.fr/~jgasnier001/

Univ Rennes, CNRS, Inria, IRISA, Rennes, France
E-mail address: aurore.guillevic@inria.fr
URL: https://people.rennes.inria.fr/Aurore.Guillevic/