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

Jean Gasnier [1] Aurore Guillevic [2]

23 November 2023

[1]CANARI, Université de Bordeaux, CNRS, Inria, Bordeaux INP, IMB

[2]CARAMBA, Université de Lorraine, CNRS, Inria, LORIA

Introduction

Notation

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 2$.

Let $A, B \in \mathbb{F}_q$ such that $4A^3 + 27B^2 \neq 0$. We define an elliptic curve E with:

$$E: \; y^2 = x^3 + Ax + B$$

We ask $\#E(\mathbb{F}_q) = rh$ with $r \neq p$ prime and h small.

The trace of E is $t = \#E(\mathbb{F}_q) - (q+1)$.

Theorem: Hasse-Weil bound

With the previous notation, $\mid t \mid \leqslant 2\sqrt{q}$.

Pairings

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be groups of exponent r. We call pairing an application

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

which is:

Pairings

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be groups of exponent r. We call pairing an application

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

which is:

- non-degenerate: $\forall P \in \mathbb{G}_1, \exists Q \in \mathbb{G}_2, e(P, Q) \neq 1$
  and $\forall Q \in \mathbb{G}_2, \exists P \in \mathbb{G}_1, e(P, Q) \neq 1$.

Pairings

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be groups of exponent r. We call pairing an application

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

which is:

- non-degenerate: $\forall P \in \mathbb{G}_1, \exists Q \in \mathbb{G}_2, e(P, Q) \neq 1$
  and $\forall Q \in \mathbb{G}_2, \exists P \in \mathbb{G}_1, e(P, Q) \neq 1$.
- bilinear: $\forall P_1, P_2 \in \mathbb{G}_1, \forall Q_1, Q_2 \in \mathbb{G}_2,$ $e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1)$ and $e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2)$.

Examples

We denote the r-torsion of E by $E[r]$.

Let μ_r be the set of r-th roots of unity in $\overline{\mathbb{F}_q}$. Then $\mathbb{F}_q(\mu_r)$ has cardinal q^k.

We call k the embedding degree of E.

Examples

We denote the r-torsion of E by $E[r]$.

Let μ_r be the set of r-th roots of unity in $\overline{\mathbb{F}_q}$. Then $\mathbb{F}_q(\mu_r)$ has cardinal q^k.

We call k the embedding degree of E.

Example:

$$e_{Weil} : E[r] \times E[r] \longrightarrow \mu_r$$

Example:

$$e_{Tate} : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r$$

Applications of pairings

Pairings have some interesting cryptographic applications:

- Identity-based encryption (Boneh–Franklin, 2003)
- Short signatures (Boneh–Lynn–Shacham, 2004)
- Flexible key-exchange protocols (Joux, 2004)

MOV attack

If a pairing can be computed quickly,

$$\text{DLP in } E[r](\mathbb{F}_q) \longrightarrow \text{DLP in } \mathbb{F}_{q^k}^\times$$

To use pairings, we need $\mathbb{F}_{q^k}^\times$ to be large enough, which means k is large enough.

Supersingular curves and pairings

Definition

Let $\mathrm{End}(E)$ be the endomorphism ring of the curve E. Then either:

- $\mathrm{End}(E)$ is isomorphic to a maximal order in a quaternion algebra. We say that E is supersingular.
- $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic field. We say that E is ordinary.

Proposition

If E is supersingular, then $k \leqslant 6$.

Pairing-friendly curves

If E is an ordinary curve, usually $k \approx r$.

We want curves with small enough k: **pairing-friendly curves**.

Pairing-friendly curves are rare, so we need to find ad hoc constructions.

Previous Work

General strategy

We define the D discriminant of E as the squarefree part of the discriminant of $\mathrm{End}(E)$.

General strategy to generate PF curves of a given security level n:

- Fix k and D.
- Find q and $E/\mathbb{F}_q$ with a subgroup of size $r \approx 2^{2n}$, embedding degree k, and discriminant D.
- Compute the ρ-value: $\rho = \log(q)/\log(r)$.

Goal: getting $\rho \approx 1$.

Describing PF curves with integers

Proposition

Fix k and D. Let q, r and t be integers satisfying:

- q is a prime (power).
- r is a prime.
- t is coprime to q.
- $rh = q + 1 - t$ for some integer h.
- r divides $\Phi_k(q)$ where Φ_k is the k-th cyclotomic polynomial.
- $Dy^2 = 4q - t^2$ for some integer y (CM equation).

Then there exists a curve E over $\mathbb{F}_{q^k}$ with discriminant D, trace t and a subgroup of order r with embedding degree k.

Describing PF curves with integers

Proposition

Fix k and D. Let q, r and t be integers satisfying:

- q is a prime (power).
- r is a prime.
- t is coprime to q.
- $rh = q + 1 - t$ for some integer h.
- r divides $\Phi_k(t-1)$ where Φ_k is the k-th cyclotomic polynomial.
- $Dy^2 = 4q - t^2 = -(t-2)^2 \bmod r$ for some integer y (CM equation).

Then there exists a curve E over $\mathbb{F}_{q^k}$ with discriminant D, trace t and a subgroup of order r with embedding degree k.

Considering families of curves

Two reasons to consider families of curves:

- smaller ρ-values.
- Adaptation to the security level.

Goal: Find polynomials Q, R, T in $\mathbb{Q}[X]$ and take $q = Q(x_0)$, $r = R(x_0)$, $t = T(x_0)$ for some integer x_0.

Prime values of polynomials

Conjecture: Buniakowski–Schinzel

Let $P \in \mathbb{Q}[X]$. P takes an infinite number of prime values if and only if:

- P is irreducible.
- P has a positive leading coefficient.
- P is non-constant.
- P takes integer values.
- $\gcd(\{P(x) \mid x, P(x) \in \mathbb{Z}\}) = 1$.

P represents primes if P satisfies the 5 conditions of the conjecture.

Complete families of curves

Fix k and D. Let Q, R, T, Y and H be polynomials in $\mathbb{Q}[X]$. The polynomials form a potential (complete) family of curves if:

- R is irreducible, non-constant, has positive leading coefficient.
- $RH = Q + 1 - T$.
- R divides $\Phi_k(T - 1)$.
- $DY^2 = 4Q - T^2$.

They form a (complete) family if they additionally satisfy:

- Q represents primes.
- Q, R, T, Y, H all take an integer value at a common integer.

The ρ-value of a family: $\deg Q / \deg R$.

Brezing–Weng method

Let $\mathcal{C}_k$ be the field extension containing the k-th roots of unity.

Algorithm 2.1: Brezing–Weng method
Input: $k > 0$ and $D > 0$ squarefree.

Output: A potential family of elliptic curves.

1 Let $R \in \mathbb{Q}[X]$ be an irreducible polynomial with positive leading coefficient such that $K = \mathbb{Q}[X]/\langle R \rangle$ contains $\sqrt{-D}$ and $\mathcal{C}_k$. Fix a primitive k-th root of unity $\zeta_k \in K$.

Let $\mathcal{C}_k$ be the field extension containing the k-th roots of unity.

Algorithm 2.2: Brezing–Weng method
Input: $k > 0$ and $D > 0$ squarefree.

Output: A potential family of elliptic curves.

1 Let $R \in \mathbb{Q}[X]$ be an irreducible polynomial with positive leading coefficient such that $K = \mathbb{Q}[X]/\langle R \rangle$ contains $\sqrt{-D}$ and $\mathcal{C}_k$. Fix a primitive k-th root of unity $\zeta_k \in K$.

2 Let $T \in \mathbb{Q}[X]$ be a polynomial mapping to $\zeta_k + 1$ in K.

3 Let $Y \in \mathbb{Q}[X]$ be a polynomial mapping to $\frac{T-2}{\sqrt{-D}}$ in K.

4 $Q = (T^2 + DY^2)/4 \in \mathbb{Q}[X]$; $H = (Q + 1 - T)/R \in \mathbb{Q}[X]$

5 Return Q,R,T,Y,H

Example

Example:
The Barreto–Lynn–Scott family for $k = 24$, $D = 3$, and $\rho = 5/4$:

- $R = \Phi_{24}(X)$,
- $T = X + 1$,
- $Q = \frac{1}{3}(X - 1)^2(X^8 + X^4 + 1) + X$.

KSS's approach

The problem in the Brezing-Weng method is to find R. The first candidate polynomials were the cyclotomic ones, but it is a bit restrictive.

The problem in the Brezing-Weng method is to find R. The first candidate polynomials were the cyclotomic ones, but it is a bit restrictive.

Kachisa–Shaefer–Scott suggested to take R as the minimal polynomial of an element θ in a suitable number field, and were successful in finding new families.

KSS's approach

The problem in the Brezing-Weng method is to find R. The first candidate polynomials were the cyclotomic ones, but it is a bit restrictive.

Kachisa–Shaefer–Scott suggested to take R as the minimal polynomial of an element θ in a suitable number field, and were successful in finding new families.

One of its interests is that it is easy to enumerate potential families through the enumeration of the elements of the number field.

KSS'algorithm

Algorithm 2.3: KSS algorithm

Input: $k > 0$ and $D > 0$ squarefree.

Output: A potential family of elliptic curves.

Fix K a number field containing $\sqrt{-D}$ and a primitive k-th root of unity ζ_k.

Pick $\theta \in K$ such that $\mathbb{Q}(\theta) = K$.

Let $R \in \mathbb{Q}[X]$ be the minimal polynomial of θ over $\mathbb{Q}$.

Let $T \in \mathbb{Q}[X]$ such that $T(\theta) = \zeta_k + 1$.

Let $Y \in \mathbb{Q}[X]$ such that $Y(\theta) = \frac{\zeta_k - 1}{\sqrt{-D}}$.

$Q = (T^2 + DY^2)/4 \in \mathbb{Q}[X]$; $H = (Q + 1 - T)/R \in \mathbb{Q}[X]$

Return Q, R, T, Y, H

Example

Let $k = 11$ and $D = 1$. Set $K = \mathcal{C}_{11}(\sqrt{-1})$. Let ζ_{11} be a 11-th root of unity in K.

Let $\theta = \zeta_{11}/\sqrt{-1}$. We have:

- $\theta^{11} = 1/\sqrt{-1}^{11} = -1/\sqrt{-1} = \sqrt{-1}$
- $-\theta^2 = \zeta_{11}^2$

Let $T = -X^2 + 1$ and $Y = -(-X^2 - 1)X^{11}$.

Example

Let $k = 11$ and $D = 1$. Set $K = \mathcal{C}_{11}(\sqrt{-1})$. Let ζ_{11} be a 11-th root of unity in K.

Let $\theta = \zeta_{11}/\sqrt{-1}$. We have:

- $\theta^{11} = 1/\sqrt{-1}^{11} = -1/\sqrt{-1} = \sqrt{-1}$
- $-\theta^2 = \zeta_{11}^2$

Let $T = -X^2 + 1$ and $Y = -(-X^2 - 1)X^{11}$. Let R be the minimal polynomial of θ, and $Q = (T^2 + DY^2)/4$.
We obtain a family with ρ-value $\frac{13}{10}$ first discovered by Brezing and Weng.

KSS16

Example:
The KSS16 family, $k = 16$, $D = 1$ and $\rho = 5/4$:

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

Example:
The KSS18 family, $k = 18$, $D = 3$ and $\rho = 4/3$:

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

Subfield method

KSS enumeration

For their enumeration, KSS restricted themselves to $K = \mathcal{C}_\ell$ where $\ell = \mathrm{lcm}(k, 4)$ or $\ell = \mathrm{lcm}(k, 6)$.

They noticed that for most θ in K, the potential families have a ρ-value around 2.

They restricted themselves to algebraic integers with sparse coefficients in the base of powers of ζ_ℓ.

In this subset of K, they managed to find some elements generating interesting potential families.

Goal: Describe the elements generating interesting families.

Our field extension pattern

Let $k \geqslant 7$ and $D > 0$ squarefree.

$$\begin{tikzcd}
& K & \\
F \arrow[ur, dash] \arrow[dd, dash] & & \\
& \mathcal{C}_k(\sqrt{-D}) \arrow[uu, dash] \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-D}) \arrow[dr, dash] & & \mathcal{C}_k \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Figure 1: Our setting

K is an extension of $\mathcal{C}_k(\sqrt{-D})$, F is a subfield of K containing $\sqrt{-D}$ such that $K = F\mathcal{C}_k$.

First observations

The generator change $\theta_2 = \theta_1 - \lambda$, $\lambda \in \mathbb{Q}$, yields the polynomial substitution $X \mapsto X + \lambda$:

$$Q_2(X) = Q_1(X + \lambda), \ \ldots$$

The ρ-value is not affected.

The generator change $\theta_2 = N\theta_1$, $N \in \mathbb{Q}$, yields the polynomial substitution $X \mapsto X/N$:

$$Q_2(X) = Q_1(X/N), \ \ldots$$

The ρ-value is not affected.

Therefore, affine rational transformations on θ does not affect the ρ-value of the generated potential family.

Subfield method

Fix ζ_k a primitive k-th root of unity.

Consider the $\mathbb{Q}$-vector space $F\zeta_k = \{\alpha\zeta_k \ ; \ \alpha \in F\}$. Take $\theta = \alpha\zeta_k$ for some $\alpha \in F$, such that $\mathbb{Q}(\theta) = K$.

Define e an integer such that $\mathbb{Q}(\theta^e) = F$. Let P_1, P_2, P_3 in $\mathbb{Q}[X]$ such that:

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

Subfield method

Then $T(X) = P_1(X^e)X + 1$ as

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

Subfield method

Then $T(X) = P_1(X^e)X + 1$ as

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

Similarly, $Y(X) = P_2(X^e)X - P_3(X^e)$.

Then $\rho = \frac{2e([F:\mathbb{Q}]-1)+2}{[K:\mathbb{Q}]} = \frac{2e}{[K:F]}\left(1 - \frac{1}{[F:\mathbb{Q}]}\right) + \frac{2}{[K:\mathbb{Q}]}$.

$$
\begin{tikzcd}
& & K \arrow[dl, dash] \arrow[ddrr, dash] & & \\
& F \arrow[dl, dash] & & & \\
\mathbb{Q}(\sqrt{-D}) \arrow[drr, dash] & & & & \mathcal{C}_k \arrow[dll, dash] \\
& & \mathbb{Q} & &
\end{tikzcd}
$$

Figure 2: General setting for Case 1.

First case: $e = k$

$$
\begin{tikzcd}
 & & K \arrow[dl, dash] \arrow[ddrr, dash] & & \\
 & F \arrow[dl, dash] & & & \\
\mathbb{Q}(\sqrt{-D}) \arrow[ddrr, dash] & & & & \mathcal{C}_k \arrow[ddll, dash] \\
 & & & & \\
 & & \mathbb{Q} & &
\end{tikzcd}
$$

Figure 2: General setting for Case 1.

The ρ-value is optimal if $F = \mathbb{Q}(\sqrt{-D})$.

First case: $e = k$

$$
\begin{tikzcd}
 & K = \mathcal{C}_k(\sqrt{-D}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-D}) = F \arrow[dr, dash] & & \mathcal{C}_k \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Figure 2: Optimized setting for Case 1.

First case: $e = k$

$$
\begin{tikzcd}
 & K = \mathcal{C}_k(\sqrt{-D}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-D}) = F \arrow[dr, dash] & & \mathcal{C}_k \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Figure 2: Optimized setting for Case 1.

$$\rho = \frac{k+1}{\varphi(k)} \text{ if } \sqrt{-D} \notin \mathcal{C}_k \text{ and } \rho = \frac{2(k+1)}{\varphi(k)} \text{ if } \sqrt{-D} \in \mathcal{C}_k$$

Second case: $e = k/2$

$$
\begin{tikzcd}[arrows=dash]
 & & K \arrow[dl] \arrow[ddrr] & & \\
 & F \arrow[dl] & & & \\
\mathbb{Q}(\sqrt{-D}) \arrow[ddrr] & & & & \mathcal{C}_k \arrow[ddll] \\
 & & & & \\
 & & \mathbb{Q} & &
\end{tikzcd}
$$

Figure 3: General setting for Case 2.

Second case: $e = k/2$

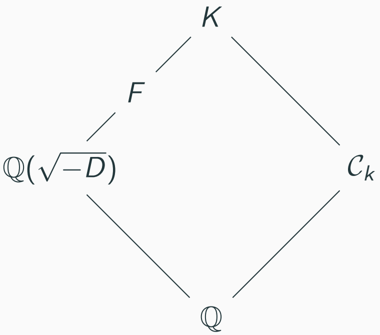

Figure 3: General setting for Case 2.

The ρ-value is optimal if $F = \mathbb{Q}(\sqrt{-D})$.

Second case: $e = k/2$

$$
\begin{tikzcd}
 & K = \mathcal{C}_k(\sqrt{-D}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-D}) = F \arrow[dr, dash] & & \mathcal{C}_k \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Figure 3: Optimized setting for Case 2.

Second case: $e = k/2$

$$\begin{tikzcd}
& K = \mathcal{C}_k(\sqrt{-D}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-D}) = F \arrow[dr, dash] & & \mathcal{C}_k \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Figure 3: Optimized setting for Case 2.

$$\rho = \frac{k/2+1}{\varphi(k)} \text{ if } \sqrt{-D} \notin \mathcal{C}_k \text{ and } \rho = \frac{2(k/2+1)}{\varphi(k)} \text{ if } \sqrt{-D} \in \mathcal{C}_k$$

Let d be a divisor of k, $d \geq 3$, and let $e = k/d$.

$$
\begin{tikzcd}
 & & K \arrow[dl, dash] \arrow[dr, dash] & \\
 & F \arrow[dl, dash] \arrow[dr, dash] & & \mathcal{C}_k \arrow[dl, dash] \\
\mathbb{Q}(\sqrt{-D}) \arrow[dr, dash] & & \mathcal{C}_d \arrow[dl, dash] & \\
 & \mathbb{Q} & &
\end{tikzcd}
$$

Figure 4: General setting for Case 3.

The ρ-value is optimal if $F = \mathcal{C}_d(\sqrt{-D})$.

Third case: $e = k/d$

Let d be a divisor of k, $d \geq 3$, and let $e = k/d$.

$$\begin{tikzcd}
 & & K \arrow[dl, dash] \arrow[dr, dash] & \\
 & F \arrow[dl, dash] \arrow[dr, dash] & & \mathcal{C}_k \arrow[dl, dash] \\
\mathbb{Q}(\sqrt{-D}) \arrow[dr, dash] & & \mathcal{C}_d \arrow[dl, dash] & \\
 & \mathbb{Q} & &
\end{tikzcd}$$

Figure 4: General setting for Case 3.

$$\rho = \frac{2(\varphi(d) - 1)}{d} \frac{k}{\varphi(k)} + \frac{2}{\varphi(k)} \text{ if } \sqrt{-D} \in \mathcal{C}_d$$

Possibilities for d

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 1: Choices for d between 3 and 50 and corresponding coefficients.

Sum-up

The optimal case is when F is an imaginary quadratic field, $F = \mathbb{Q}(\sqrt{-D})$. The discriminant you can choose depends on k:

- if $3 \mid k$, $D = 3$, and $e = k/\gcd(6, k)$.
- else if $4 \mid k$, $D = 1$ and $e = k/4$, or $\sqrt{-D} \notin \mathcal{C}_k$ and $e = k/2$.
- else if k is even, $\sqrt{-D} \notin \mathcal{C}_k$ and $e = k/2$.
- else $\sqrt{-D} \notin \mathcal{C}_k$ and $e = k$.

Example

Let $k = 18$, $D = 3$. Let $K = \mathcal{C}_{18}$ and $\theta = (1 + 3\zeta_{18}^3)\zeta_{18}$. We obtain:

$$
\begin{aligned}
T &= (3X^4 + 176X + 221)/221, \\
Y &= (5X^4 - 26X^3 + 146X - 1157)/663, \\
R &= (X^6 + 89X^3 + 2197)/(13^3 \cdot 17^2), \\
Q &= \tfrac{1}{11271}\left(X^8 - 5X^7 + 13X^6 + 89X^5 - 292X^4 + 1157X^3 + 2197X^2 \right. \\
&\quad \left. -2009X + 28561\right)
\end{aligned}
$$

The family has the same ρ-value as KSS18: $\rho = 4/3$.

Results

Theoretical results

- We found a $\mathbb{Q}$-vector space of good generators. We are able to generate many families at any embedding degree k, for almost any discriminant.
- Our method generalizes most previous works (not BN curves).
- Our families have ρ-values at least equal to previous best families. We improved the ρ-value for $k = 22$.
- The new families have larger denominators.

New families

Our new curve GG22 for $k = 22$ and $D = 7$, from $\alpha = (1 + \sqrt{7})/2$:

$$T = (X^{12} + 45X + 46)/46$$

$$Y = (X^{12} - 4X^{11} - 47X - 134)/322$$

$$R = (X^{20} - X^{19} - X^{18} + 3X^{17} - X^{16} - 5X^{15} + 7X^{14} + 3X^{13} - 17X^{12} + 11X^{11} + 23X^{10} + 22X^9 - 68X^8 + 24X^7 + 112X^6 - 160X^5 - 64X^4 + 384X^3 - 256X^2 - 512X + 1024)/23$$

$$Q = (X^{24} - X^{23} + 2X^{22} + 67X^{13} + 94X^{12} + 134X^{11} + 2048X^2 + 5197X + 4096)/7406$$

Its ρ-value: $\rho = 1.2$ (previous was 1.3).

Our new GG20a curve for $k = 20$ and $D = 1$, from $\alpha = 1 - 2\zeta_4$:

$$T = (2X^6 + 117X + 205)/205$$

$$Y = (X^6 - 5X^5 - 44X - 190)/205$$

$$R = (X^8 + 4X^7 + 11X^6 + 24X^5 + 41X^4 + 120X^3 + 275X^2 + 500X + 625)/25625$$

$$Q = (X^{12} - 2X^{11} + 5X^{10} + 76X^7 + 176X^6 + 380X^5 + 3125X^2 + 12938X \\ +15625)/33620$$

Its ρ-value: $\rho = 1.5$.

New families

Our new GG20b curve for $k = 20$ and $D = 1$, from $\alpha = 1 + 2\zeta_4$:

$$T = (-2X^6 + 117X + 205)/205$$

$$Y = (X^6 - 5X^5 + 44X + 190)/205$$

$$R = (X^8 - 4X^7 + 11X^6 - 24X^5 + 41X^4 - 120X^3 + 275X^2 - 500X + 625)/25625$$

$$Q = (X^{12} - 2X^{11} + 5X^{10} - 76X^7 - 176X^6 - 380X^5 + 3125X^2 + 12938X$$
$$+15625)/33620$$

Its ρ-value: $\rho = 1.5$.

Some new curves for the 192-bit security level:

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

Optimal ate pairing cost estimates

Table 3: Optimal ate pairing and final exponentiation cost estimates in terms of finite field multiplications.

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

The bitsize of p has a scale color w.r.t. its 64-bit machine word size: $512 < 9\mathtt{w} \leq 576$, $448 < 8\mathtt{w} \leq 512$.

Optimal ate pairing cost estimates

Table 4: Optimal ate pairing and final exponentiation cost estimates in terms of finite field multiplications.

curve	p bits	r bits	pairing total
GG20b	575	**379**	60058**m**
GG22D7	457	**383**	127020**m**

The bitsize of p has a scale color w.r.t. its 64-bit machine word size: $512 < 9\mathtt{w} \leq 576$, $448 < 8\mathtt{w} \leq 512$.

Conclusion

- We generalizes the KSS technique to generate complete families of pairing-friendly curves.
- 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 STNFS attack.
- For $k = 22$, we improve on the previously best ρ-values.

Links:

- Sagemath code for generating families and optimal ate pairing implementation.
- HAL

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

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

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

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

Aurore Guillevic.
Pairing-friendly curves.
`https://members.loria.fr/AGuillevic/pairing-friendly-curves/`, 9 2020.

Last updated October 9, 2020.

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.

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.

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

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.

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.

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.