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

Jean Gasnier, Aurore Guillevic

SIAM AG-23, July 13 2023

IMB (Université de Bordeaux, Inria, CNRS, Bordeaux INP), France `jean.gasnier@math.u-bordeaux.fr`

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France `aurore.guillevic@inria.fr`

Recalls

Context

$\mathbb{F}_{\boldsymbol{q}}$ a finite field, $\boldsymbol{E} : y^2 = x^3 + Ax + B$ be a (smooth) elliptic curve over $\mathbb{F}_q$

$\boldsymbol{t}$ the trace of E , $\mathbb{G}_1$ a subgroup of E of prime order $\boldsymbol{r}$, $\boldsymbol{e_r} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T \subset \mathbb{F}_{q^k}$ a pairing application

Pairing applications:

- identity-based encryption
- short signatures
- flexible key-exchange protocols

Pairing $\rightarrow$ attacks on the DL on E

Pairing-friendly curves: curves having a small enough embedding degree $\boldsymbol{k}$

We focus on the generation of pairing-friendly curves. Main criterion: $\boldsymbol{\rho} = \log q / \log r$.

If E is ordinary: $\boldsymbol{D}$ the squarefree part of the discriminant of the endomorphism ring.

Generating an ordinary pairing-friendly curve

Theorem:

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

From now on, we assume E to be ordinary.

To generate E, we first generate q, r and t, and then use the CM method to recover E.

The generated integers q, r and t have to satisfy two kinds of conditions:

- Number-theoretic conditions: q and r are prime.
- Arithmetic conditions: q, r, t and two other integers y and h satisfy polynomial relations.

Generating a complete family of curves

Generating a complete family of elliptic curves means fiding Q, R, T, Y, H in $\mathbb{Q}[X]$ satisfying:

- Number-theoretic conditions:
  - Q represents primes (Bunyakovsky-Schinzel conjecture),
  - R represents prime up to a rational,
  - all the polynomials take integer values simultanously.
- Arithmetic relations:
  - $RH = Q + 1 - T$,
  - R divides $\Phi_k(T-1)$,
  - $DY^2 = 4Q - T^2$, (CM equation)

  where Φ_k is the k-th cyclotomic polynomial.

We define the ρ-value of a family as $\rho = \deg Q / \deg R$.

Examples of families

Example:

The Barreto-Lynn-Scott (BLS) family for $k = 12$ and $D = 3$, which has $\rho = 3/2$:

- $R(x) = X^4 - X^2 + 1$,
- $T(x) = X + 1$,
- $Q = \left(X^6 - 2X^5 + 2X^3 + X + 1\right)/3$.

Example:

The Barreto-Naehrig (BN) family for $k = 12$ and $D = 3$, which has $\rho = 1$:

- $R(x) = 36X^4 + 36X^3 + 18X^2 + 6X + 1$,
- $T(x) = 6X^2 + 1$,
- $Q(x) = 36X^4 + 36X^3 + 24X^2 + 6X + 1$.

Brezing-Weng method

Use the arithmetic relations to generate a potential family:

- Fix k and D;
- Let R be an irreducible polynomial such that $\mathbb{Q}[X]/\langle R\rangle$ contains a primitive k-th root of unity ζ_k and $\sqrt{-D}$;
- Let T be a polynomial such that $T \equiv \zeta_k + 1 \bmod R$;
- Let Y be a polynomial such that $Y \equiv \dfrac{\zeta_k - 1}{\sqrt{-D}} \bmod R$;
- Compute $Q = (T^2 + DY^2)/4$ and $H = (Q + 1 - T)/R$.

Then check if Q, R, T, Y, H satisfy the number-theoretic conditions.

Kachisa-Schaefer-Scott method

The KSS method is a variant of the Brezing-Weng method that specify how to find R.

- Fix k and D;
- Fix K a number field containing a primitive k-th root of unity ζ_k and $\sqrt{-D}$;
- Pick $\theta \in K$ such that $\mathbb{Q}(\theta) = K$;
- Let R be the minimal polynomial of θ over $\mathbb{Q}$;
- Let T be a polynomial such that $T(\theta) = \zeta_k + 1$;
- Let Y be a polynomial such that $Y(\theta) = \dfrac{\zeta_k - 1}{\sqrt{-D}}$;
- Compute $Q = (T^2 + DY^2)/4$ and $H = (Q + 1 - T)/R$.

In particular, the KSS method allows an enumeration on θ.

Examples of KSS families

Example: ($KSS16$)

Family generated from $\theta = (2\sqrt{-1} - 1)\zeta_{16}$ for $k = 16$ and $D = 1$, which has $\rho = 5/4$:

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

Example: ($KSS18$)

Family generated from $\theta = (\sqrt{-3} - 5)\zeta_{18}/2$ for $k = 18$ and $D = 3$, which has $\rho = 4/3$:

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

Subfield method

Goals

The goals of this talk are:

- to exhibit the mathematical components allowing us to generate families with small ρ-value.
- to introduce new families performing better than older ones at the same embedding degree.
- to compare them to the state of the art and discuss their cryptographic interest.

Main Idea

Fix $k \geq 7$.

Let $\mathcal{C}_k$ be the k-th cyclotomic field, and let $F = \mathbb{Q}(\sqrt{-D})$ be a quadratic imaginary field. We call $K = \mathcal{C}_k F = \mathcal{C}_k(\sqrt{-D})$ the compositum. Fix ζ_k a primitive k-th root of unity.

Let $\theta = \alpha\zeta_k,\ \alpha \in F$, such that $K = \mathbb{Q}(\theta)$. Let e be an integer such that $F = \mathbb{Q}(\theta^e)$. Choose $R = \text{minpoly}(\theta)$. Then, there exists P_1, P_2, P_3 such that:

- $P_1(\theta^e) = 1/\alpha$.
- $P_2(\theta^e) = 1/(\alpha\sqrt{-D})$.
- $P_3(\theta^e) = 1/\sqrt{-D}$.
- $T(X) = P_1(X^e)X + 1$, so that $T(\theta) = P_1(\theta^e)\theta + 1 = \alpha\zeta_k/\alpha + 1 = \zeta_k + 1$.
- $Y(X) = P_2(X^e)X - P_3(X^e)$, so that $Y(\theta) = \dfrac{\zeta_k}{\sqrt{-D}} - \dfrac{1}{\sqrt{-D}}$.

First case: odd k, non-specific discriminant

If k is odd, then we can take $e = k$ (because $\theta^e = \alpha^k$). Suppose that $F \not\subset \mathcal{C}_k$.

Then we have:

$$
\begin{tikzcd}
& K = \mathcal{C}_k(\sqrt{-D}) \arrow[dl, dash, "\varphi(k)"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{-D}) = F \arrow[dr, dash, "2"'] & & \mathcal{C}_k \not\ni \sqrt{-D} \arrow[dl, dash, "\varphi(k)"] \\
& \mathbb{Q} &
\end{tikzcd}
$$

and we generate families with $\rho = \frac{k+1}{\varphi(k)}$.

Second case: even k, non-specific discriminant

If k is even, then we can take $e = k/2$ (because $\theta^e = -\alpha^{k/2}$). Suppose that $F \not\subset \mathcal{C}_k$.

Then we have:

$$\begin{tikzcd}[column sep=small]
 & K = \mathcal{C}_k(\sqrt{-D}) \arrow[dl, dash, "\varphi(k)"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{-D}) = F \arrow[dr, dash, "2"'] & & \mathcal{C}_k \not\ni \sqrt{-D} \arrow[dl, dash, "\varphi(k)"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

and we generate families with $\rho = \frac{k/2+1}{\varphi(k)}$.

Third case: discriminant 1 and 3

For these special discriminants, we have another construction.

If $4 \mid k$, let $D = 1$ and $d = 4$. If $3 \mid k$, then let $D = 3$ and $d = \gcd(6, k)$.

In any case, we can take $e = k/d$. Then we have:

$$\begin{array}{c} K = \mathcal{C}_k \\ \varphi(k)/2 \Big| \\ F = \mathbb{Q}(\sqrt{-D}) = \mathbb{Q}(\zeta_d) \\ 2 \Big| \\ \mathbb{Q} \end{array}$$

We can generate families with $\rho = \frac{2k/d+2}{\varphi(k)}$.

An example with $k = 18$

Fix $k = 18$. In that case, $6 \mid k$ so the construction with $D = 3$ gives the best ρ-value. We take $e = k/6 = 3$.

We enumerate on α:

- Take $-10 \leq a \leq 10$ and $0 \leq b \leq 10$, let $\alpha = b\sqrt{-D} + a$ and $\theta = \alpha\zeta_k$.
- Ensure that θ^3 generates F.
- Compute P_1, P_2, P_3...

With $\alpha = 5 + 3\sqrt{-D}$, we obtain a family with $\rho = 4/3$:

- $P_1 = (3X + 1408)/3536$, $P_2 = (5X + 1168)/10608$, $P_3 = (X + 356)/204$
- $T = (3X^4 + 1408X + 3536)/3536$, $Y = (5X^4 - 52X^3 + 1168X - 18512)/10608$
- $R = X^6 + 712X^3 + 140608$, $Q = \frac{1}{2885376}(X^8 - 10X^7 + 52X^6 + 712X^5 - 4672X^4 + 37024X^3 + 140608X^2 - 257152X + 7311616)$

Results

Theoretical results

- The method allows to generate many new families, with a small ρ-value, which depends only on k.
- We showed that we can obtain families with an improved ρ-value for $k \equiv 4 \bmod 12$ (for example $k = 16$) and $k \equiv 22 \bmod 24$ (for example $k = 22$).
- We proved that we can not obtain $\rho = 1$ in this way.

New families

Example: (GG22)

A family for $k = 22$ and $D = 7$, which has $\rho = 6/5$:

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

Example: (GG20b)

A family for $k = 20$ and $D = 1$, which has $\rho = 3/2$:

- $T = (2X^6 + 117X + 205)/205$
- $R = X^8 + 4X^7 + 11X^6 + 24X^5 + 41X^4 + 120X^3 + 275X^2 + 500X + 625$
- $Q = \frac{1}{33620}(X^{12} - 2X^{11} + 5X^{10} + 76X^7 + 176X^6 + 380X^5 + 3125X^2 + 12938X + 15625)$

Comparison with the state of the art

We are going to compare these families:

Curve	k	$R(X)$	twist $d \mid k$	ρ
KSS16	16	$(X^8 + 48x^4 + 625)/1250$	4	$5/4 = 1.25$
KSS18	18	$(X^6 + 37X^3 + 343)/343$	6	$4/3 = 1.33$
FST 6.4	20	$\Phi_{20}(X)$	4	$3/2 = 1.5$
GG20b	20	R_{GG20b}	4	$3/2 = 1.5$
FST 6.6	20	$\Phi_{60}(X)$	2	$11/8 = 1.375$
FST 6.3	22	$\Phi_{2k}(X) = \Phi_k(X^2)$	2	$13/10 = 1.3$
GG22	22	R_{GG22}	2	$6/5 = 1.2$
BLS24	24	$\Phi_{24}(X)$	6	$5/4 = 1.25$

Pre-selected curves

k	curve	seed	$\log q$	$\log r$	ρ	$\log q^k$	secu
16	KSS16	$2^{78} - 2^{76} - 2^{28} + 2^{14} + 2^{7} + 1$	766	605	1.25	12256	194
18	KSS18	$2^{80} + 2^{77} + 2^{76} - 2^{61} - 2^{53} - 2^{14}$	638	474	1.33	11484	193
20	FST 6.4	$-2^{56} + 2^{44} + 1$	670	448	1.5	13400	193
	GG20b	$2^{49} + 2^{46} - 2^{41} + 2^{35} + 2^{30} - 1$	575	379	1.52	11500	196
	FST 6.6	$-2^{24} + 2^{15} - 2^{8} - 2^{6} - 1$	527	384	1.37	10540	193
22	GG22	`-0xbe503`=-779523	457	383	1.19	10054	220
	FST 6.3	$2^{21} - 2^{13} + 2^{6} + 2^{3} + 1$	544	420	1.30	11968	192
24	BLS24	$-2^{51} - 2^{28} + 2^{11} - 1$	509	409	1.25	12216	193

Estimated cost in $\mathbb{F}_q$-multiplications m of 512 bits

k	curve	q bits	r bits	Miller loop optimal ate	final exp easy	final exp hard	final exp total	pairing total
16	KSS16	766	605	37024**m**	530**m**	72411**m**	72940**m**	109964**m**
18	KSS18	638	474	26919**m**	742**m**	41704**m**	42445**m**	69364**m**
20	FST 6.4	670	448	34260**m**	944**m**	65624**m**	66567**m**	100827**m**
	GG20b	575	379	22072**m**	638**m**	≈62868**m**	≈63497**m**	≈85577**m**
	FST 6.6	527	384	36090**m**	638**m**	47303**m**	47941**m**	84031**m**
22	GG22	457	383	41154**m**	789**m**	72352**m**	73141**m**	114295**m**
	FST 6.3	544	420	49926**m**	993**m**	82488**m**	66393**m**	133406**m**
24	BLS24	509	409	15345**m**	658**m**	24310**m**	24968**m**	40313**m**

Optimal Ate Pairing implementation on the curves considered in Sagemath

Conclusion

- We introduced a new method for generating families of pairing-friendly curves. It can produce many families with a ρ-value depending only on k, and (almost) chosen discriminant. For every $k \neq 12$, the ρ-value is at least as small as previous records of complete families.
- We presented new families for $k = 20$ and $k = 22$ performing better than previous ones at the same enbedding degree. We gave examples of pairing-friendly curves with an estimation of the cost of computation of the pairing.
- Lastly, it should be noted that this method does not achieve $\rho = 1$.

Links:

- Main article
- Sagemath implementation of subfield method
- Sagemath implementation of optimal ate pairing

Diego F. Aranha, Koray Karabina, Patrick Longa, Catherine H. Gebotys, and Julio Cesar López-Hernández.
Faster explicit formulas for computing pairings over ordinary curves.
In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 48–68. Springer, Heidelberg, May 2011.

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

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.

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.

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`.

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.

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.

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, 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.
- 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.

- 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.
- 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.

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.

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