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

Jean Gasnier [1] Aurore Guillevic [2]

October 16, 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:

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

There exists an additive group structure on the set of points on E.

Curve-based cryptography

Let $P \in E(\mathbb{F}_q)$ with prime order r.

Secret: $s \in \mathbb{Z}/r\mathbb{Z}$

Public Key: $sP \in E(\mathbb{F}_q)$

Discrete Logarithm Problem

Given P and sP, compute s.

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 $e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2)$.

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

Weil Pairing

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 (with respect to r).

Example:

$$e_{Weil} : E[r] \times E[r] \longrightarrow \mu_r \subset \mathbb{F}_{q^k}$$

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)

DLP and pairings

In a cryptographic context, r is a prime such that $\log(r) \approx \log(q)$.

If a pairing can be computed quickly,

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

MOV-attack: when k is to small.

Pairing-friendly curves

We want curves with k of a suitable size: **pairing-friendly curves**.

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

Generation of pairing-friendly curves

Describing PF curves with integers

Proposition

Fix k and D a squarefree integer. 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.
- $4q - t^2 = Dy^2$ for some integer y (CM equation).

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

Complete families of curves

Let Q, R, T, Y and H be polynomials in $\mathbb{Q}[X]$. Fix k and D. 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.

Then you can generate q, r and t by evaluating at some $x_0 \in \mathbb{Z}$.

KSS strategy

Algorithm 2.1: KSS method
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

KSS16

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

$$R = X^8 + 48x^4 + 625,$$

$$T = \frac{1}{35}(2X^5 + 41X + 35),$$

$$Y = \frac{1}{35}\left(X^5 - 5X^4 + 38X - 120\right),$$

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

Good generators

By taking $\theta = \alpha\zeta_k$, α an element of $F = \mathbb{Q}(\sqrt{-D})$, we generate potential families of high quality. Let e be an integer such that $\mathbb{Q}(\theta^e) = F$ (for example, $e = k$), and define P_1, P_2, P_3 in $\mathbb{Q}[X]$ such that:

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

Then:

- $T(X) = P_1(X^e)X + 1$
- $Y(X) = P_2(X^e)X - P_3(X^e)$

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).
- 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: $\rho = \deg Q / \deg R = 1.2$ (previous was 1.3).

New families

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: $\rho = 1.5$.

Conclusion

- For $k = 16$, $k = 18$, we obtain alternative choices of comparable performances as the well-known KSS curves.
- For $k = 20$, we improve on the previous FST 6.4 curves with parameters that are not vulnerable to a specific STNFS attack.
- For $k = 22$, we decrease the size of the field, allowing faster computation.
- Sagemath code for generating families and optimal ate pairing implementation.
- ArXiv

References i

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.