Efficient pairing computation on Barreto-Naehrig elliptic curves of embedding degree 12

Séminaire 3A – Option Mathématiques Appliquées
Supervisors : Damien Vergnaud (ENS Paris), Claude Lamoureux (ECP)

Florence Clerc, Rémi Géraud

Menu

Outline

Cryptography 1/3 : context

- *Cryptography* : "practice and study of techniques for secure communication in the presence of third parties" (Wikipedia).
- *Basic setting* : Alice, Bob, Eve.
- *Applications* : nearly everywhere.

Cryptography 2/3 : setting

- (*Symmetric-key crypto* : shared, secret, key)
- *Public-key crypto* : public/private key (pk/sk)
- *Basic setting* : finite groups and fields

Intermission : Diffie-Hellman key agreement

Alice and Bob want to agree on a key.

- They agree on $\mathbb{K} = \mathbb{Z}/181\mathbb{Z}$.
- They agree on $g = 42$ ($\langle g \rangle = \mathbb{K}$)
- Alice chooses her secret key $a = 107$
- Bob chooses his secret key $b = 99$
- Alice computes her public key $A = ag = 4494 \equiv 150 \pmod{181}$
- Bob computes his public key $B = bg = 4158 \equiv 176 \pmod{181}$
- They share their public keys.

Alice can compute $aB = 8$, Bob can compute $Ab = 8$. Bingo.

Cryptography 3/3 : hypotheses and limits

Fundamental assumption of public-key crypto :

- sk $\rightarrow$ pk *easy*
- pk $\rightarrow$ sk *very hard*

Discrete logarithm problem (DLP) :

$$a = x^b, \quad x = ?$$

On usual groups $(\mathbb{Z}/p\mathbb{Z})$, not always that hard...
Larger groups ? Other groups ?

Outline

Elliptic curves 1/5 : definition

Definition

An elliptic curve over a field $\mathbb{K}$ is a non-singular complete curve of genus 1, with a distinguished point "at infinity".

In the cases we are interested in [20, 16] :

Definition

An *elliptic curve* E over a field $\mathbb{K}$ is defined by an equation of the form

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K} \quad \text{(Weierstrass equation)}$$

along with a distinguished point P_∞

Elliptic curves 2/5 : illustration

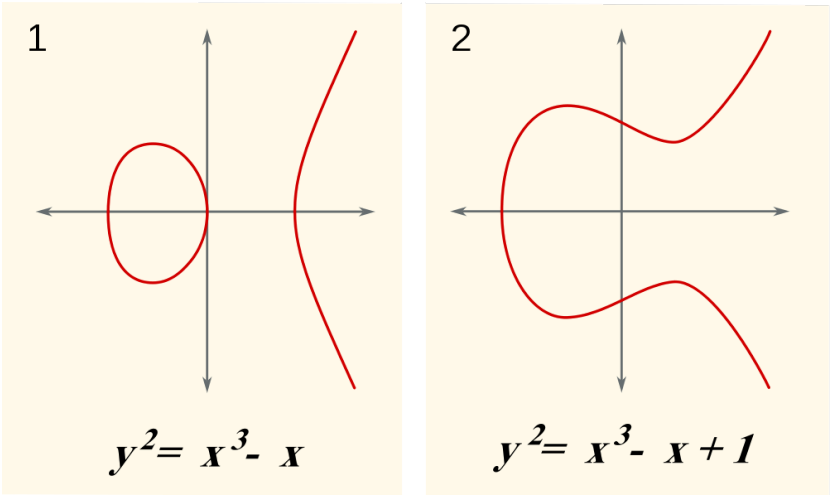

Figure: Two different elliptic curves considered in $\mathbb{R}$.

Elliptic curves 3/5 : abelian group structure

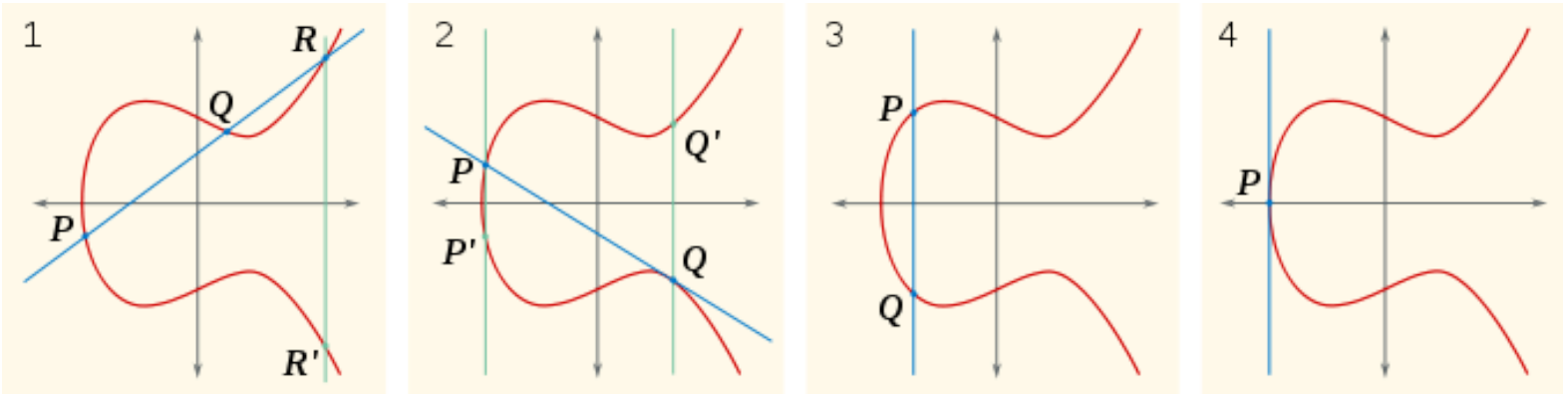

Figure: Sums on an elliptic curve. Four different cases are presented, the general one (1), when $Q = R$ (2), when $P = -Q$ (3) and when $P = Q = R$ (4)

Elliptic curves 4/5

We can use elliptic curves for their group structure

- $k \cdot P = P + \cdots + P$
- $P = (x, y) \Rightarrow -P = (x, -y)$
- P_∞ is the identity

No sub-exponential solution to the DLP known !

- Same "old" algorithms : RSA, etc.
- Smaller keys for the same level of security

Elliptic curves 5/5

Not all curves are suitable for cryptography... oftentimes, special properties are understood as weaknesses and looked upon warily.

But we can turn weaknesses into strengths !

- Endomorphisms !
- Pairings !

Outline

Point multiplication

Point multiplication : the operation of computing

$$k \cdot P = P + \cdots + P$$

- Adding is tiresome (remember)
- Doubling is not harder : double-and-add algorithm

Example:

$$\begin{aligned} 33 \cdot P &= 100001_2 \cdot P \\ &= P + 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot P \end{aligned}$$

(5 doublings + 1 addition)
Remember : small multiplications are faster.

Efficient endomorphisms

Some curves have *shortcuts* :

$$\phi : P \mapsto Q = \lambda P$$

where ϕ is "easy" to compute. Example [25, 11] :

$$E_1 : y^2 = x^3 + ax$$
$$\phi : (x, y) \mapsto (-x, \beta y)$$

where β is an element of order 4.

Gallant-Lambert-Vanstone method

Gallant, Lambert and Vanstone [11, 25] propose to use such endomorphisms to *speed-up point multiplication*

- Identify ϕ such that $\phi(P) = \lambda P$
- Break down $kP = k_1 P + k_2 \lambda P = k_1 P + k_2 \phi(P)$
- Compute $k_1 P + k_2 \phi(P)$

1 big multiplication $\Rightarrow$ 2 small ones + 1 addition

Gallant-Lambert-Vanstone method

The hard part:

- Find an efficient endomorphism ϕ
- Find k_1 and k_2

The reward:

- Faster computation, hence, algorithms

Outline

Pairings

- Introduced in ECC to attack the DLP (Menezes, Okamoto and Vanstone [19]).
- Have many interesting applications : identity-based encryption, short signatures...
- Make “weak” curves more interesting

Pairings

A pairing is essentially a function

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

so that

$$e(aP, Q) = e(P, Q)^a = e(P, aQ)$$
$$e(P, Q) \neq 1 \text{ if } P, Q \neq P_\infty$$

Examples : Weil pairing, Tate pairing (Eta pairing, Ate pairing, twisted Ate pairing...)

Divisors

Definition

A *divisor* $D \in \mathrm{Div}(E)$ is a formal sum of points on the elliptic curve E :

$$D = \sum_{P \in E} a_P(P)$$

with $a_P \in \mathbb{Z}$ and $a_P = 0$ except for finitely many $P \in E$.

Definition

Given f a function defined on the elliptic curve E, the *divisor of* f is :

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P)$$

where $\mathrm{ord}_P(f)$ is the order of the zero (or the pole) which f has at the point P and it is positive if P is a zero and negative otherwise.

Tate Pairing

Definition

Tate pairing of P and Q:

$$\mathcal{A}_P \sim (P) - (P_\infty)$$
$$\mathcal{A}_Q \sim (Q) - (P_\infty)$$
$$f_P \text{ s.t. } \operatorname{div}(f_P) = n\mathcal{A}_Q$$
$$t_l(P, Q) = f_P(\mathcal{A}_Q)$$

it has to be raised to the power $(q^k - 1)/l$ to obtain a unique value.

Properties of the Tate pairing

- bilinearity:

$$t_l(P_1 + P_2, Q) = t_l(P_1, Q)t_l(P_2, Q)$$
$$t_l(P, Q_1 + Q_2) = t_l(P, Q_1)t_l(P, Q_2)$$

- non-degeneracy:

$$\text{if } t_l(P, Q) = 1 \text{ for all } Q \text{ then } P = P_\infty$$

- compatibility:

$$P \in E(\mathbb{F}_q)[l], Q \in E(\mathbb{F}_{q^k})[hl] \Rightarrow t_{hl}(h \cdot P, Q) = t_l(P, Q)^h$$

How to compute the Tate pairing

- (modified) Miller's algorithm
- Essentially modified double-and-add...
- Can we improve computation with efficient endomorphisms *à la* GLV ?

Security versus efficiency

Definition

E defined on $\mathbb{F}_q$
r a number prime to q such than $r \mid \#E(\mathbb{F}_q)$
embedding degree with respect to r : $k \in \mathbb{N}$ minimal with $r \mid (q^k - 1)$.

Definition

ρ-value :

$$\rho = \frac{\log q}{\log r}$$

Security versus efficiency

- k high : security improved
- ρ low : faster arithmetics

Outline

Ionică-Joux pairing [13]

The idea is to design a pairing based on an efficiently computable endomorphism ϕ such that its characteristic equation is $X^2 + aX + b = 0$.
Done on two types of curves :

- NSS : of form $y^2 = x^3 + B$ so take $\phi : (x, y) \to (\beta x, y)$ with β non trivial square root of unity ($k = 2$ and $\rho \sim 2$)
  get an equation for λ : $\lambda^2 + \lambda + 1 = cr$
- Cocks-Pinch with $k = 4, 6$: take ϕ satisfying $x^2 + ax + b = 0$, get an equation for λ : $\lambda^2 + a\lambda + b = cr$

The pairing that is obtained is a power of the Tate Pairing.

Exact Pairing

Theorem

Let E on $\mathbb{F}_q$, r a prime number such that $r \mid \#E(\mathbb{F}_q)$, k the embedding degree with respect to r. Let ϕ be an efficiently computable separable endomorphism of E, whose characteristic equation is $X^2 + aX + b = 0$. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the subgroups of order r whose elements are eigenvectors of ϕ defined over $\mathbb{F}(q)$ and $\mathbb{F}(q^k)$ respectively. Let λ be the eigenvalue of ϕ on $\mathbb{G}_1$, verifying $\lambda^2 + a\lambda + b = cr$ with $r \nmid bc$.
Then the map $a_\phi(.,.) : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$ is a bilinear non-degenerate pairing :

$$a_\phi(P,Q) = f_{\lambda,P}^{\lambda+a}(bQ)\, f_{\lambda,P}^{b}(\hat{\phi}(Q))\, f_{a,\lambda P}(bQ)\, f_{b,P}(bQ) \times \left(\prod_{K \in Ker\phi \setminus \{P_\infty\}} corr_{P,K}(\hat{\phi}(Q))\right)^{-\lambda} \left(\prod_{K \in Ker\phi \setminus \{P_\infty\}} corr_{\lambda P,K}(\hat{\phi}(Q))\right) \times corr_{\lambda^2 P, a\lambda P}(bQ)\, l_{\lambda^2 P + a\lambda P, bP}(bQ)$$

Outline

Pairing-friendly curves

Pairing-friendly : elliptic curve that has a small embedding degree and a large prime-order subgroup [8].

How to find such curves ?

- Chance ?
- Complex multiplication methods: Cocks-Pinch algorithm, Barreto-Naehrig curves etc.

Baretto-Naehrig curves

Definition

A *BN curve* [1] is an elliptic curve E_b of the form $y^2 = x^3 + b$ defined over $\mathbb{F}_p$ such that $b \neq 0$ and $n = \#E_b(\mathbb{F}_p)$ and n, q ad t (the trace of the frobenius) are given by :

$$q = q(u) = 36u^4 + 36u^3 + 24u^2 + 6u + 1$$
$$n = n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$$
$$t = t(u) = 6x^2 + 1$$

Such a curve has embedding degree 12.

Example of BN curve

160 bits BN curve of prime order p and $k = 12$ [1]:

$$p = 1461501624496790265145448589920785493717258890819$$
$$n = 1461501624496790265145447380994971188499300027613$$
$$t = 120892581430521795886320 7$$
$$b = 3$$
$$y = 2$$

Endomorphisms on BN curves

BN curves are of the form

$$E : y^2 = x^3 + b$$

On these curves there exist an efficient endomorphism

$$\begin{aligned} \phi : E &\to E \\ (x, y) &\mapsto (\beta x, y) \end{aligned}$$

where β is a non-trivial third root of unity. This endomorphism satisfies $\phi^2 + \phi + 1 = 0$ ($a = b = 1$).

Example: on previous curve, $y^2 = x^3 + 3$. A third root of unity in $\mathbb{F}_p$ is

$$\beta = 2923003248995208495450923854321783187178438239430$$

Ionică-Joux pairings

In the theorem, we use :

$r = n = 146150162449679026514544738099497118849930002761 3$

$k = 12$

$a = b = 1$

$c = 2$

$\lambda = 187659270257192420140128694203749166360656435260$

We can check that $r \mid \#E(\mathbb{F}_q)$ and $r \nmid bc$.

$P = (1, 2)$

$Q = (325593032004972218298147844747942917 7, 146150162449679026514544738$

$a(P, Q) = 292300324899683646061094448417292385544607948440 3$

which is a third root of unity.

Outline

Future work

- Work may be done more quickly in the dual world, thanks to a skew Frobenius map [22] ;
- Computing independent functions in parallel and then computing products could improve performance [23] ;
- GLV enables faster computation directly in $\mathbb{G}_2$ and $\mathbb{G}_T$ when computing a pairing $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ [10]


P. Barreto and M. Naehrig.
Pairing-friendly elliptic curves of prime order.
In *Selected areas in cryptography*, pages 319–331. Springer, 2006.


P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott.
Efficient algorithms for pairing-based cryptosystems.
pages 354–368. Springer-Verlag, 2002.


D. Boneh and M. Franklin.
Identity-based encryption from the weil pairing.
In *Advances in Cryptology—CRYPTO 2001*, pages 213–229. Springer, 2001.


D. Boneh, B. Lynn, and H. Shacham.
Short signatures from the weil pairing.
Advances in Cryptology—ASIACRYPT 2001, pages 514–532, 2001.


H. Cohen, G. Frey, and R. Avanzi.
Handbook of elliptic and hyperelliptic curve cryptography.
CRC press, 2006.


H. Daudé, P. Flajolet, and B. Vallée.
An average-case analysis of the gaussian algorithm for lattice reduction.
Combinatorics, Probability and Computing, 6(04):397–433, 1997.


A. Enge.
Courbes algébriques et cryptologie.
Habilitation ‘a diriger des recherches, Université Paris-Diderot - Paris VII, 2007.


D. Freeman, M. Scott, and E. Teske.
A taxonomy of pairing-friendly elliptic curves.
Journal of Cryptology, 23(2):224–280, 2010.


G. Frey and H.G. Rück.
A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves.
Mathematics of computation, 62(206):865–874, 1994.


S. Galbraith and M. Scott.
Exponentiation in pairing-friendly groups using homomorphisms.
Pairing-Based Cryptography–Pairing 2008, pages 211–224, 2008.


R. Gallant, R. Lambert, and S. Vanstone.
Faster point multiplication on elliptic curves with efficient endomorphisms.
In *Advances in Cryptology – CRYPTO 2001*, pages 190–200. Springer, 2001.


S. Goldwasser and M. Bellare.
Lecture notes on cryptography.
Summer course "Cryptography and computer security" at MIT, 1999:1999, 1996.


S. Ionică and A. Joux.
Pairing computation on elliptic curves with efficiently computable endomorphism and small embedding degree.
Pairing-Based Cryptography-Pairing 2010, pages 435–449, 2010.


A. Joux.
A one round protocol for tripartite diffie-hellman.
Algorithmic number theory, pages 385–393, 2000.


A. Joux.
The weil and tate pairings as building blocks for public key cryptosystems.
Algorithmic number theory, pages 11–18, 2002.


N. Koblitz.
Elliptic curve cryptosystems.
Mathematics of computation, 48(177):203–209, 1987.


M. Maas.
Pairing-based cryptography.
PhD thesis, Master's Thesis, Technische Universiteit Eindhoven, 2004.


A. Menezes.
An introduction to pairing-based cryptography.
Department of Combinatorics and Optimazion, 2005.


A.J. Menezes, T. Okamoto, and S.A. Vanstone.
Reducing elliptic curve logarithms to logarithms in a finite field.
Information Theory, IEEE Transactions on, 39(5):1639–1646, 1993.


V. Miller.
Use of elliptic curves in cryptography.
In Hugh Williams, editor, *Advances in Cryptology – CRYPTO '85 Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer Berlin / Heidelberg, 1986.


G.C.C.F. Pereira, M.A. Simplício, M. Naehrig, and P.S.L.M. Barreto.
A family of implementation-friendly bn elliptic curves.
Journal of Systems and Software, 2011.


Y. Sakemi, Y. Nogami, K. Okeya, H. Kato, and Y. Morikawa.
Skew frobenius map and efficient scalar multiplication for pairing–based cryptography.
Cryptology and Network Security, pages 226–239, 2008.


Y. Sakemi, S. Takeuchi, Y. Nogami, and Y. Morikawa.
Accelerating twisted ate pairing with frobenius map, small scalar multiplication, and multi-pairing.
Information, Security and Cryptology–ICISC 2009, pages 47–64, 2010.


M. Scott.
Faster pairings using an elliptic curve with an efficient endomorphism.
Progress in Cryptology – INDOCRYPT 2005, pages 258–269, 2005.


F. Sica, M. Ciet, and J.J. Quisquater.
Analysis of the Gallant-Lambert-Vanstone method based on efficient endomorphisms: Elliptic and hyperelliptic curves.
In *Selected areas in cryptography*, pages 21–36. Springer, 2003.


J.H. Silverman.
The arithmetic of elliptic curves, volume 106.
Springer Verlag, 2009.


W. A. Stein et al.
Sage Mathematics Software (Version 4.8.0).
The Sage Development Team, 2012.
`http://www.sagemath.org`.


M. Stögbauer.
Efficient algorithms for pairing-based cryptosystems.
Germany: Darmstadt University of Technology, 2004.

E. Verheul.
Evidence that XTR is more secure than supersingular elliptic curve cryptosystems.
Advances in Cryptology – EUROCRYPT 2001, pages 195–210, 2001.

E. R. Verheul.
Self-blindable credential certificates from the weil pairing.
pages 533–551. Springer-Verlag, 2001.