Efficient Optimal Ate Pairing at 128-bit Security Level

Loubna GHAMMAM

GREYC Université de Caen Normandie
France

Co-authored with
Md. Al-Amin Khandaker, Yuki Nanjo, Sylvain Duquesne, Yasuyuki Nogami

(INDOCRYPT 2017)

Cryptography and Algorithmic Number Theory
Caen 2018

June 22, 2018

Outline

Sommaire

Generality on Elliptic Curves

Definition

An elliptic curve E defined over a field $\mathbb{K}$ with car$(\mathbb{K}) \geq 5$, is a non-singular plane algebraic curve defined by an equation of the form

$$y^2 = x^3 + ax + b, \ \textit{with} \quad a, \ b \in \mathbb{K}$$

This type of equation is called a short Weierstrass equation.

The set of points of an elliptic curve E forms an additive abelian group with P_∞ is the identity element.

Definition

Let E be an Elliptic curve defined over $\mathbb{F}_p$ and r an integer.

$$E[r] = \{P \in E(\overline{\mathbb{F}_p}) / rP = P_\infty\}$$

A point $P \in E[r]$ is called a r-torsion point.

Definition

The embedding degree of E relatively to r is the smallest integer k such that $r | p^k - 1$.

Properties

An important property is that:

$$E[r] \subset E(\mathbb{F}_{p^k})$$

Generality on Pairings

What is a Pairing?

Let G_1, G_2, G_3 three abelian groups of order r. G_1 and G_2 are additive groups, G_3 is a multiplicative group. A pairing is the following application:

$$e : G_1 \times G_2 \rightarrow G_3$$

verifying:

- *Non degeneracy,*
- *Bilinearity.*

Using Pairings in Cryptography

- *Simplification of existing protocols (Joux's protocol).*
- *Identity based Cryptography, Short Signature.*
- *Cryptanalysis.*

Example

Tate Pairing

The following pairing:

$$\begin{array}{rcl} e_T : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})[r] & \longrightarrow & \mathbb{F}^*_{p^k} \\ (P, Q) & \longmapsto & e_T(P, Q) = (f_{r,P}(Q))^{\frac{p^k-1}{r}} \end{array}$$

is a bilinear and non-degenerate pairing.

This pairing requires the computation of:

1. Miller function $f_{r,P}(Q)$ defined by:

$$div(f_{r,P}) = r(P) - (rP) - (r-1)(P_\infty)$$

2. The final exponentiation $\frac{p^k-1}{r}$.

Miller equality: $$f_{[i+j],P} = f_{[i],P} \times f_{[j],P} \times \frac{l_{[i]P,[j]P}}{v_{[i+j]P}}.$$

Example: the computation of $f_{5,P}$

1. W write $5 = 4 + 1$ then, we apply Miller's equality:
   - $f_{5,P} = f_{1,P} \times f_{4,P} \times \frac{l_{[4]P,P}}{v_{[5P]}} = f_{4,P} \times \frac{l_{[4]P,P}}{v_{[5P]}}.$
2. We decompose 4 en $4 = 2 \times 2$, and then:
   - $f_{4,P} = f_{2,P}^2 \times \frac{l_{[2]P,[2]P}}{v_{[4P]}}.$
3. By the same way, we find:
   - $f_{2,P} = f_{1,P} \times f_{1,P} \times \frac{l_{P,P}}{v_{[2P]}} = \frac{l_{P,P}}{v_{[2P]}}.$
4. Then,

$$f_{5,P} = \left(\frac{l_{P,P}}{v_{[2P]}}\right)^2 \times \frac{l_{[2]P,[2]P}}{v_{[4P]}} \times \frac{l_{[4]P,P}}{v_{[5P]}}$$

Miller algorithm

Input: $P \in G_1, Q \in G_2,\ r = (r_{n-1}, \ldots, \ldots r_0)$: with $r_{n-1} = 1$
Output: $f_{r,P}(Q) \in \mathbb{F}^*_{p^k}$

$f \leftarrow 1$
$T \leftarrow P$
For $i = n - 2$ **to** 0 **do**
    $f \leftarrow f^2 \cdot \dfrac{l_{T,T}(Q)}{v_{2[T]}(Q)}$
    $T \leftarrow [2]T$
    if $r_i = 1$ **then**
        $f \leftarrow f \cdot \dfrac{l_{T,P}(Q)}{v_{T+P}(Q)}$
        $T \leftarrow T + P$
    end if
    return f
end for

Final exponentiation:

$$\frac{p^k - 1}{r} = \frac{(p^k - 1)}{\phi_k(p)} \times \frac{\phi_k(p)}{r},$$

- $\frac{(p^k-1)}{\phi_k(p)}$: the first part of the final exponentiation.
- $\frac{\phi_k(p)}{r}$: the hard part of the final exponentiation.
- $\phi_k(p)$ is the cyclotomic polynomial.

Security levels:

Security level	size of r	size of p^k
80	160	1024
128	256	3072
192	384	7680
256	512	15360

Table: Security levels according to NIST

Sommaire

BN (Barreto and Naehrig) elliptic curve

Definition

A BN elliptic curve is an elliptic curve defined over $\mathbb{F}_p$ *by the equation* $E : y^2 = x^3 + b$ *and by the parameter* u *such that:*

$$r(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1 \text{ and } p(u) = r(u) + 6u^2.$$

$$u = -2^{62} - 2^{55} - 1$$

This curve has an embedding degree $\mathbf{k} = \mathbf{12}$.

Optimal Ate on BN

$$\begin{array}{rcl} E(\mathbb{F}_p)[r] \times \Psi_6\left(E'(\mathbb{F}_{p^2})[r]\right) & \longrightarrow & \mathbb{F}^*_{p^{12}} \\ (P, Q) & \longmapsto & e_{BN}(P, Q) \end{array}$$

avec, $e_{BN}(P, Q) = \left((f_{6u+2,Q}(P) l_{[6u+2]Q,\pi(Q)}(P) l_{[6u+2]Q,\pi^2(Q)}(P))\right)^{\frac{p^{12}-1}{r}}$

Comparison before and after **SexTNFS**:

BN Curve	Parameter u	Size of p	Size of p^k
Before **SexTNFS**	$u = -2^{62} - 2^{55} - 1$	256	3072
After **SexTNFS**	$u = 2^{114} + 2^{101} - 2^{14} - 1$	461	5534

Table: BN parameterization

BN curve	Miller loop	Final expo
Parameter u of Nogami *et al.*	6780 M	4364 M+ I (Cyc) 3372 M+ 4I (Com)
Parameter u of Barbulescu and Duquesne	12068 M	7485 M+I (Cyc) 5706+4 I (Com)

Table: Cost of Optimal Ate pairing in BN curves

Sommaire

Is the BN elliptic curve always the most suitable elliptic curve for computing the Optimal Ate pairing for the 128 bits security level?

Others curves

- The BLS12 curve,
- The KSS16 curve,
- The KSS18 curve.

Which curve ?

Results of Barbulescu and Duquesne.

Elliptic curve	Cost Opt Ate (Cyc squaring)	Cost Opt Ate (omp. squaring)
BN	$4399425 + \mathbf{I}$	$3999150 + 4\mathbf{I}$
BLS12	$3600675 + \mathbf{I}$	$3156300 + 6\mathbf{I}$
KSS16	$\mathbf{3155196 + I}$	...
KSS18	$3578212 + \mathbf{I}$	$3298702 + 8\mathbf{I}$

Table: Cost of Opt. Ate pairing on KSS16, BLS12, KSS18 et BN

Sommaire

Our aim:

- Optimizing the computation of Optimal Ate pairing.
- Software implementation of the Optimal Ate pairing in BN, BLS12 and KSS16 curves.
- Concluding.

Definition

Kachisa, Schafer et Scott proposed a family of pairing friendly elliptic curves defined over $\mathbb{F}_p$ *by the equation :*

$$y^2 = x^3 + ax$$

With:

- $r = u^8 + 48u^4 + 625$
- $p = \frac{1}{980}(u^{10}+2u^9+5u^8+48u^6+152u^5+240u^4+625u^2+2398u+3125)$

The choice of the parameter

The parameter proposed by Barbulescu and Duquesne is:

$$u = -2^{34} + 2^{27} - 2^{23} + 2^{20} - 2^{11} + 1$$

This parameter u *is sparse and gives* r *and* p *of sizes 333 and 340 bits.*

Opimal Ate on KSS16

Definition

The Optimal Ate pairing over KSS16 elliptic curve is the following map:

$$\begin{aligned} e_{opt} : E(\mathbb{F}_p)[r] \times \Psi_4(E'(\mathbb{F}_{p^4})[r]) &\longrightarrow \mathbb{F}_{p^{16}} \\ (P, Q) &\longmapsto e_{KSS16}(P, Q) \end{aligned}$$

with

$$e_{KSS16}(P, Q) = \left((f_{u,Q}(P) l_{[u]Q,[p]Q}(P))^{p^3} l_{Q,Q}(P) \right)^{\frac{p^{16}-1}{r}}$$

Ψ_4 is the morphism defined by:

$$\begin{aligned} \Psi_4 : E'\left(\mathbb{F}_{p^4}\right) &\rightarrow E(\mathbb{F}_{p^{16}}) \\ (x, y) &\mapsto (x\zeta^{1/2}, y\zeta^{3/4}). \end{aligned}$$

Optimized Miller algorithm

Input: $P \in G_1, Q \in G_2,\ u = (u_{n-1}, \dots, \dots u_0)$: with $u_{n-1} = 1$
Output: $f_{u,Q}(P) \in \mathbb{F}_{p^k}^*$

$f \leftarrow 1$
$T \leftarrow Q$
For $i = n - 2$ **to** 0 **do**
    $f \leftarrow f^2 \cdot l_{T,T}(P)$
    $T \leftarrow [2]T$
    if $u_i = 1$ **then**
        $f \leftarrow f \cdot l_{T,Q}(P)$
        $T \leftarrow T + Q,$
    end if
    return f
end for

The extension tower of $\mathbb{F}_{p^{16}}$

For KSS-16 curve, $p \equiv 5 \bmod 8$ and $c = 2$ is a quadratic non-residue in $\mathbb{F}_p$, then, the construction of $\mathbb{F}_{p^{16}}$ given as follows:

$$\begin{cases} \mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 - c), \\ \mathbb{F}_{p^4} = \mathbb{F}_{p^2}[\beta]/(\beta^2 - \alpha), \\ \mathbb{F}_{p^8} = \mathbb{F}_{p^4}[\gamma]/(\gamma^2 - \beta), \\ \mathbb{F}_{p^{16}} = \mathbb{F}_{p^8}[\omega]/(\omega^2 - \gamma), \end{cases}$$

Let f be an element of $\mathbb{F}_{p^{16}}$, then

$$f = f_0 + f_1\gamma + f_2\omega + f_3\gamma\omega,$$

with f_0, f_1, f_2 and f_3 elements of $\mathbb{F}_{p^4}$.

Computations in Miller algorithm

In the Miller's algorithm we have to compute:

- $f \leftarrow f^2 \cdot l_{T,T}(P)$,
- $f \leftarrow f \cdot l_{T,Q}(P)$ (also, the computation of $f \leftarrow f \cdot l_{T,-Q}(P)$)

f, $l_{T,T}$, and $l_{T,Q}$ are elements of $\mathbb{F}_{p^{16}}$ **and** $l_{T,T}$, and $l_{T,Q}$ are **two sparse elements**.

Sparse Multiplication

However, thanks to twist property of E', $l_{T,T}$ $l_{T,Q}$ et $l_{T,-Q}$ can be obtained in sparse form which will led us more efficient multiplication called **sparse multiplication**.

Aim: Improving the sparse multiplication.

The Calculation of $l_{T,Q}(P)$

The addition step of Miller algorithm consists in:

- computing $l_{T,Q}(P)$ and updating T; $T + Q = R(x_R, y_R)$,
- Performing the sparse multiplication $f \times l_{T,Q}(P)$.

The line equation passing through T and Q evaluated on P is:

$$l_{T,Q}(P) = y_P + F\omega + E\gamma\omega$$

with:

$$A = \frac{1}{x_{Q'} - x_{T'}}, B = y_{Q'} - y_{T'}, C = AB, D = x_{T'} + x_{Q'},$$
$$x_{R'} = C^2 - D, E = Cx_{T'} - y_{T'}, y_{R'} = E - Cx_{R'}, F = -Cx_P$$

In the addition step of Miller algorithm we have to compute

$$f \times l_{T,Q}(P)$$

So, the computation of

$$l_{T,Q}(P) = y_P + F\omega + E\gamma\omega.$$

$$\times$$

$$f = f_0 + f_1\gamma + f_2\omega + f_3\gamma\omega,$$

$$\Downarrow$$

Sparse multiplication to perform!

$$\Downarrow$$

7-Sparse-Multiplication.

Aim?

How to reduce the cost of the sparse multiplication?

$$l_{T,Q}(P) = y_P - Cx_P\omega + E\gamma\omega$$

Multiplying by y_P^{-1}, we obtain:

$$y_P^{-1} l_{T,Q}(P) = 1 - Cx_P y_P^{-1}\omega + Ey_P^{-1}\gamma\omega,$$

we have:

- y_P^{-1} can be precomputed. Therefore, the overhead calculation of Ey_P^{-1} will cost only 4 $\mathbb{F}_p$-multiplications.
- $y_P^{-1} l_{T,T}(P)$ does not effect the pairing calculation cost.
- $x_P y_P^{-1}$ will be omitted by applying further isomorphic mapping of $P \in G_1$.

Pseudo 8-sparse multiplication

Consider the following isomorphic map between $E(\mathbb{F}_{p^4})$ and $\bar{E}(\mathbb{F}_{p^4})$:

$$\begin{array}{rcl}\Psi : \bar{E}(\mathbb{F}_{p^4})[r] & \longmapsto & E(\mathbb{F}_{p^4})[r], \\ (x, y) & \longmapsto & (z^{-1}x,\ z^{-3/2}y),\end{array}$$

With $\bar{E} : y^2 = x^3 + az^{-2}x$, and $z, z^{-1}, z^{-3/2} \in \mathbb{F}_p$.

Let $\bar{P} = (x_{\bar{P}}, y_{\bar{P}}) = (z^{-1}x_P,\ z^{-3/2}y_P)$, $z =$? verifies $x_{\bar{P}}y_{\bar{P}}^{-1} = 1$

$$\begin{array}{rcl} x_{\bar{P}}y_{\bar{P}}^{-1} & = & 1 \\ z^{-1}x_P(z^{-3/2}y_P)^{-1} & = & 1 \\ z^{1/2}(x_P.y_P^{-1}) & = & 1 \end{array}$$

Ainsi, $z = (x_P^{-1}y_P)^2$.

$\bar{P}(x_{\bar{P}}, y_{\bar{P}}) = (x_P z^{-1}, y_P z^{-3/2}) = (x_P^3 y_P^{-2},\ x_P^3 y_P^{-2})$.

For the same isomorphic map Ψ, we obtain $\bar{Q}$ *in* $\bar{E}$ defined over $\mathbb{F}_{p^{16}}$ by:

$$\bar{Q}(x_{\bar{Q}}, y_{\bar{Q}}) = (z^{-1}x_{Q'}\gamma, z^{-3/2}y_{Q'}\gamma\omega),$$

$\bar{Q}'(x_{\bar{Q}'}, y_{\bar{Q}'})$ is obtained in **quartic twisted curve** $\bar{E}'$ as follows:

$$\begin{aligned}
\bar{E}' : \; y_{\bar{Q}'}^2 &= x_{\bar{Q}'}^3 + a(z^2\beta)^{-1}x_{\bar{Q}'}. \\
\bar{Q}'(x_{\bar{Q}'}, y_{\bar{Q}'}) &= (z^{-1}x_{Q'}, z^{-3/2}y_{Q'}), \\
&= (x_{Q'}x_P^2y_P^{-2}, y_{Q'}x_P^3y_P^{-3}).
\end{aligned}$$

The computation of $l_{T,Q}(P)$

$$y_P^{-1} l_{T,Q}(P) = 1 - C x_P y_P^{-1} \omega + E y_P^{-1} \gamma \omega$$

Now, applying $\bar{P}$ and $\bar{Q}'$, the line evaluation becomes:

$$\begin{aligned} y_{\bar{P}}^{-1} l_{\bar{T}',\bar{Q}'}(\bar{P}) &= 1 - C(x_{\bar{P}} y_{\bar{P}}^{-1})\gamma + E y_{\bar{P}}^{-1} \gamma \omega, \\ \bar{l}_{\bar{T}',\bar{Q}'}(\bar{P}) &= 1 - C\gamma + E(x_P^{-3} y_P^2)\gamma\omega, \end{aligned}$$

where, $x_{\bar{P}} y_{\bar{P}}^{-1} = 1$ and $y_{\bar{P}}^{-1} = z^{3/2} y_P^{-1} = (x_P^{-3} y_P^2)$.

Pseudo 8-sparse multiplication

Doubling Step.

$$\Downarrow$$

The computation of $l_{T,T}(P)$

The doubling step of Miller algorithm consists on :

- computing $l_{T,T}(P)$ and up-dating T.
- Performing the sparse multiplication $f^2.l_{T,T}(P)$.

By the same way, we optimize the sparse multiplication : **Pseudo 8-Sparse multiplication.**

$$\Downarrow$$

More efficient Miller algorithm

Comparison

The following table compares the complexity of Miller's algorithm: **This work** vs Barbulescu et al.'s estimation.

The result of	KSS-16	BN	BLS-12
Barbulescu *et al.*	$7534M_p$	$12068M_p$	$7708M_p$
This work	$7209M_p$	$11114M_p$	$7202M_p$

Table: Complexity comparison of Miller's algorithm

Remark

The Pseudo 8-sparse multiplication is more efficient than the 7-sparse multiplication.

Sommaire

Miller algorithm

The Curve	KSS-16	BN	BLS-12
Miller Algorithm	4.41	7.53	4.91

Table: Comparative results of Miller's Algorithm in [ms].

Final Exponentiation

Curve	KSS-16	BN	BLS-12
Final Exponentiation	17.32	11.65	12.03

Table: Comparative results of Final Exponentiation in [ms].

- BLS12 curve is better than BN curve.
- We found an efficient Miller's loop calculation for KSS-16 than theoretical estimations of previous works.

Merci!