IMHOTEP

AFRICAN JOURNAL OF PURE AND APPLIED MATHEMATICS

Imhotep Mathematical Proceedings
Volume 4, Numéro 1, (2017),
pp. 44 - 50.

Optimal Weil pairing on Elliptic curves with Embedding Degree 15

A. Pecha
Department of Computer Science
and Telecommunications, ENSPM,
University of Maroua. P.O. Box 46
Maroua, Cameroon.
aminap2001@yahoo.fr

Abstract

The aim of our talk is to check that, for the next security level 192-bits, the Aranha's result is still satisfied. In fact, we will construct an optimal Weil pairing over elliptic curves with embedding degree $k = 15$ and compare his efficiency as opposed to the optimal Ate pairing.

Proceedings of the 6th annual workshop on CRyptography, Algebra and Geometry (CRAG-6), 15 - 17 June 2016, University of Bamenda, Bamenda, Cameroon.

http://imhotep-journal.org/index.php/imhotep/
Imhotep Mathematical Proceedings

IMHOTEP - Math. Proc. **4** (2017), 44–50
1608-9324/010044–43, DOI 13.1007/s00009-003-0000

IMHOTEP Mathematical Proceedings

Optimal Weil pairing on Elliptic curves with Embedding Degree 15

A. Pecha

Abstract. The aim of our talk is to check that, for the next security level 192-bits, the Aranha's result is still satisfied. In fact, we will construct an optimal Weil pairing over elliptic curves with embedding degree $k = 15$ and compare his efficiency as opposed to the optimal Ate pairing.

Keywords. Pairing, Elliptic curves.

I. Introduction

In 2005, Koblitz and Menezes [5] examine the efficiency of the Weil pairing as opposed to the Tate pairing and find that for very high security levels such as 192 or 256 bits, the Weil pairing computation is sometimes faster than the Tate pairing. A few times later, in 2006, Granger et al [2] re-examine how one should implement pairings over ordinary elliptic curves for various practical levels of security. They conclude, contrary to prior work, that the Tate pairing is more efficient than the Weil pairing for all such security levels. Optimal Ate and twisted Ate pariring are based on Tate pairing and which are looked at the most efficient pairing. However in 2011, Aranha et al [1] introduce a new optimal Weil pairing tailored for parallel execution. For the current security level 128-bits, their experimental results suggest that the new Weil pairing over Barreto-Naehrig (BN) curves is faster than the optimal Ate pairing.

Communication presentée au 6ème atelier annuel sur la CRyptographie, Algèbre et Géométrie (CRAG-6), 15 - 17 Juin 2016, Université de Bamenda, Bamenda, Cameroun / Paper presented at the 6th annual workshop on CRyptography, Algebra and Geometry (CRAG-6), 15 - 17 June 2016, University of Bamenda, Bamenda, Cameroon.

II. Background on pairing

Definition II.1. *Let $\mathbb{G}_1$, $\mathbb{G}_2$ be the additive groups and $\mathbb{G}_T$ a multiplicative group. A* **pairing** *is a non-degenerate bilinear map of the form $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, i.e. e is linear in each component and there exists $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ such that $e(P, Q) \neq 1$.*

Notation II.2. *We denote by:*

- *$\mathbb{F}_q$ a finite field of characteristic p where $p > 3$ is prime.*
- *E an ordinary elliptic curve defined over $\mathbb{F}_q$.*
  r a large prime divisor of the order of $E(\mathbb{F}_q)$.
- *k the embedding degree with respect to r and q, i.e. the smallest positive integer such that r divides $q^k - 1$.*
- *t a trace of Frobenius.*
- *$\mathcal{O}$ the point at infinity.*
- *μ_r the group of r-th roots of unity in $\mathbb{F}_{q^k}^{\times}$.*
- *$E[r]$ is the set of $r-$torsion points on E.*

Definition II.3. *Let $R \in E(\mathbb{F}_{q^k})$ and $m \in \mathbb{Z}$. A Miller function $f_{m,R}$ of length m is a $\mathbb{F}_{q^k}$-rational function with divisor $(f_{m,R}) = m(R) - ([m]R) - (m-1)\mathcal{O}$.*

Lemma II.4. *Let a and b be non-negative integers, and let $R \in E(\mathbb{F}_{q^k})$. Then*

1. *$f_{a+b,R} = f_{a,R} . f_{b,R} . l_{[a]R,[b]R} / v_{[a+b]R}$, where $l_{[a]R,[b]R}$ is the equation of the line through $[a]R$ and $[b]R$ and $v_{[a+b]R}$ is the corresponding vertical line passing through $[a+b]R$.*
2. *$f_{ab,R} = f_{b,R}^{a} . f_{a,[b]R}$.*

III. Why pairing-friendly elliptic curves?

For randomly generated elliptic curves, we have $k \approx r$, so impossible to compute pairing (because result is in $\mathbb{F}_{q^k}$). Thus for a constructive applications of pairings, we must find the special kind of elliptic curves such that k needs to be small enough, so that the pairing is easy to compute but large enough, so that the DL in $\mathbb{F}_{q^k}^{\times}$ is computationally infeasible.

Definition III.1. *E is* **pairing-friendly** *[3] if the following two conditions hold:*

1. *$r \geq \sqrt{q}$;*
2. *k is less than $log_2(r)/8$.*

Now we assume that $q = p$ is a prime and $k = 15$, so we have $E[r] \subset E(\mathbb{F}_{p^{15}})$. This family of elliptic curves has embedding degree 15 and a ρ-value 1.5 and is parameterized by :

$$\begin{aligned} p &= (x^{12} - 2x^{11} + x^{10} + x^7 - 2x^6 + x^5 + x^2 + x + 1)/3 \\ r &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\ t &= x + 1 \end{aligned} \tag{1}$$

We found a specific value $x = 2^{48} + 2^{41} + 2^9 + 2^8 + 1$ and we obtain $r(x)$ prime of 385 bits and $p(x)$ prime of 575 bits which correspond to parameters for 192-bits security level according to Table.

TABLE 1. Bit sizes of curves parameters and corresponding embedding degrees to obtain commonly desired levels of security.

Security level	Bit length of r	Bit length of q^k	k $\rho \approx 1$	k $\rho \approx 2$
80	160	$960 - 1280$	$6 - 8$	$3 - 4$
128	256	$3000 - 5000$	$12 - 20$	$6 - 10$
192	384	$8000 - 10000$	$20 - 26$	$10 - 13$
256	512	$14000 - 18000$	$28 - 36$	$14 - 18$

IV. Pairing computation

The most common choice is to take the groups:

- $\mathbb{G}_1 = E[r] \cap ker(\pi_p - [1]) = E(\mathbb{F}_p)[r]$;
- $\mathbb{G}_2 = E[r] \cap ker(\pi_p - [p]) \subset E(\mathbb{F}_{p^{15}})[r]$.

where π_p is the p-power Frobenius endomorphism on E.

Definition IV.1. *The* **reduced Tate pairing** *restricted to* $\mathbb{G}_1 \times \mathbb{G}_2$ *is defined as:*

$$e_r : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mu_r, \quad (P, Q) \longmapsto f_{r,P}(Q)^{\frac{p^{15}-1}{r}}.$$

Restricting the Tate pairing to $\mathbb{G}_2 \times \mathbb{G}_1$ *leads to the ate pairing.*

Definition IV.2. *The* **ate pairing** *is defined as*

$$a_T : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r, \quad (Q, P) \mapsto f_{T,Q}(P)^{\frac{(p^{15}-1)}{r}},$$

where $T = t - 1$.

Definition IV.3. *The* **classical Weil pairing** *is defined as*

$$e_W : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T \quad (P, Q) \mapsto (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}.$$

Algorithm IV.4. Miller's algorithm

```
    Inputs: $s \in \mathbb{N}$ and $U, V \in E[r]$ with $U \neq V$
outputs: $f_{s,U}(V)$
Write $s = \sum_{j=0}^{n} s_j 2^j$, with $s_j \in \{0,1\}$ and $s_n = 1$
Set $f \leftarrow 1$ and $R \leftarrow U$
For $j = n-1$ down to $0$ do
    $f \leftarrow f^2 \cdot l_{R,R}(V)/v_{2R}(V)$,
    $R \leftarrow 2R$
    if $s_j = 1$ then
        $f \leftarrow f \cdot l_{R,U}(V)/v_{R+U}(V)$
        $R \leftarrow R + U$,
    end if
end for
return $f$
```

V. optimal pairing

Definition V.1. *Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ be a non degenerate, bilinear pairing with $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = r$, where the field of definition of $\mathbb{G}_T$ is $\mathbb{F}_{q^k}$, then e is called an* **optimal pairing** *if it can be computed in $log_2 r/\varphi(k) + \epsilon(k)$ basic Miller iterations, with $\epsilon(k) \leq log_2 k$.*

Definition V.2. *For a point $R \in E[r]$ and polynomial $h = \sum_{i=0}^{n} h_i z^i \in \mathbb{Z}[z]$ such that $h(s) \equiv 0$ (mod r). The* **extended Miller function** *$f_{s,h,R}$ is a rational function defined as $\prod_{i=0}^{n} f_{h_i, s^i R} \cdot \prod_{i=0}^{n-1} \frac{l_{[s_i+1]R,[h_i s^i]R}}{v_{[s_i R]}}$ where $s_i = \sum_{j=i}^{n} h_j s^j$ with divisor $\sum_{i=0}^{n} h_i [(s^i R) - \mathcal{O}]$.*

Remark V.3. *Note that $f_{s,R} = f_{s,s-x,R}$, with x an integer.*

Due to Vercauteren's optimal pairing framework [1], we have the following theorem.

Theorem V.4. *There exists h such that $|h_i| \leq r^{1/\varphi(k)}$ and $(P, Q) \mapsto f_{p,h,Q}(P)^{(p^k-1)/r}$ is a pairing.*

Remark V.5. *The coefficients h_i can be obtained by finding the shortest vector in the following $\varphi(k)$-dimensional lattice* $\begin{pmatrix} r & 0 & 0 & ... & 0 \\ -q & 1 & 0 & ... & 0 \\ -q^2 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ -q^{\varphi(k)-1} & 0 & 0 & ... & 1 \end{pmatrix}$.

Definition V.6. *According to Aranha's beta Weil pairing framework on elliptic curves with even k, we define: $\theta_{s,h}(P,Q) = \left(\frac{f_{s,h,Q}(P)}{f_{s,h,P}(Q)}\right)^{p^{k/3}-1}$ when $3|k$.*

Theorem V.7. *There exists h such that $|h_i| \leq r^{1/\varphi(k)}$ and $(P,Q) \longmapsto \prod_{i=0}^{e-1} \theta_{p,h}([p^i]P,Q)^{p^{e-1-i}}$ is a pairing.*

The Vercautern approach enabled us to obtain the following optimal function $h(z) = \sum_{i=0}^{5} c_i z^i = x - z \in \mathbb{Z}[z]$ such that $h(p) \equiv 0 \pmod r$ for the elliptic curves with $k = 15$ and according to Theorem V.4 and Theorem V.7, we can define now

Definition V.8. *The* **optimal Ate pairing on elliptic curves with** $k = 15$ *is defined as*

$$e_o : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r, \quad (Q,P) \mapsto f_{x,Q}(P)^{\frac{(p^{15}-1)}{r}}$$

.

Definition V.9. *The* **optimal Weil pairing on elliptic curve with** $k = 15$ *is defined as*

$$\begin{array}{rccl} \beta_{15}: & G_1 \times G_2 & \longrightarrow & \mu_r \\ & (P,Q) & \longmapsto & \left[\prod_{i=0}^{4} \left(\frac{f_{x,[x^i]P}(Q)}{f_{x,Q}([x^i]P)}\right)^{p^{4-i}}\right]^{(p^5-1)(p^3-1)} \end{array}$$

VI. Optimal pairing computation

We denote by M_k, S_k, I_k the cost of multiplication, squaring and Inversion in the field $\mathbb{F}_{p^k}$, for any integer k.

The Miller lite loop $f_{x,P}(Q)$ and full Miller loop $f_{x,Q}(P)$ requires 48 doublings step, 4 additions step, 47 squarings in $\mathbb{F}_{p^{15}}$ and 51 multiplications in $\mathbb{F}_{p^{15}}$.

Definition VI.1. *The* **Optimal ate pairing computation**.

Its computation has two steps: the full Miller loop $f_{x,Q}(P)$ and the final exponentiation which is computed as $\left(f^{p^5-1}\right)^{(p^{10}+p^5+1)/r}$.The overall cost of final exponentiation is $I_1 + 3093M_1 + 24044S_1$.

TABLE 2. Cost of the Miller lite and full Miller loop.

	Miller lite loop	full Miller loop
Aff	$52I_1 + 3491M_1 + 2219S_1$.	$52I_1 + 6299M_1 + 3311S_1$
Proj	$4283M_1 + 2567S_1$	$4911M_1 + 6183S_1$
Proj (mixed add)	$4271M_1 + 2567S_1$	$4803M_1 + 6183S_1$
Jac	$4619M_1 + 2471S_1$	$5319S_1 + 5739M_1$
Jac (mixed add)	$2471S_1 + 4607M_1$	$5319S_1 + 5631M_1$

Definition VI.2. *The* **Optimal Weil pairing computation***.*

We assume that the points $[x]P$, $[x^2]P$, $[x^3]P$ and $[x^4]P$ are precomputed. The cost of the doubling and the addition steps in the Miller's algorithm for $f_{x,[x^{i+1}]P}(Q)$ with $i \in \{1, 2, 3, 4\}$ is the same with $f_{x,P}(Q)$. The ten Miller functions of β Weil pairing defined above can be computed in parallel using 10 *processors. Each processor computes either one Miller lite loop or one full Miller loop and one p^i-frobenius maps ($i \in \{0, 1, 2, 3, 4\}$). The computation of the final step requires* 1 *inversion and* 9 *multiplications in $\mathbb{F}_{p^{15}}$. The final exponentiation cost :* $1I_1 + 1467M_1 + 86S_1$.

VII. Comparisons

Our comparison focuses only on the cost of the operations of optimal ate pairing with the cost of the operations executed by each processor to which is added the final step and the final exponentiation by $(p^5 - 1)(p^3 - 1)$. If we assume that $1S_1 = 1M_1$ and $1I_1 = 10M_1$. We denote by:

: MLite = the cost of the Miller lite loop

: FullM = the cost of full Miller loop

: FS = the cost of the final step

: FE = the cost of the final exponentiation

: Frob = the cost of p-power Frobenius

Conclusion

The optimal weil pairing has the potential speed advantage over the optimal ate pairing due to the absence of an expensive final exponentiation and suitable for parallel execution.

Table 3. Cost comparision of the optimal Ate and β Weil pairing

	MLite+FS+FE+Frob	FullM+FS+FE+Frob	optimal Ate
Aff	$7299M_1$	$11199M_1$	$33966M_1$
Proj	$7919M_1$	$12163M_1$	$38241M_1$
Proj (mixed add)	$7907M_1$	$12055M_1$	$38133M_1$
Jac	$8159M_1$	$12127M_1$	$38205M_1$
Jac (mixed add)	$8147M_1$	$12019M_1$	$38097M_1$

References

[1] Vercauteren F. : *Optimal pairing*, IEEE Transactions on Information Theory, **56**, (2010), 455 – 461.

[2] Aranha D.F., Knapp E., Menezes A. and Rodríguez-Henríquez F.: *Parallelizing the Weil and Tate Pairings.* L. Chen (Ed.): Cryptography and Coding 2011, LNCS 7089, 275-295, (2011). Springer-Verlag Berlin Heidelberg, 2011.

[3] Freeman D., Scott M., and Teske E., *A Taxonomy of Pairing-Friendly Elliptic Curves*, Cryptology ePrint Archive, Report 2006/372, 2006.

[4] Granger R., Page D. and Smart N.P.: *High Security Pairing-Based Cryptography Revisited.* In: Algorithmic Number Theory 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, (2006). Proceedings, 480-494.

[5] Koblitz N. and Menezes A.: *Pairing-Based Cryptography at High Security Levels.* In: Cryptography and Coding, Springer-Verlag LNCS 3796, (2005) 13–36.

A. Pecha
e-mail: aminap2001@yahoo.fr
Department of Computer Science and Telecommunications, ENSPM, University of Maroua. P.O. Box 46 Maroua. Cameroon