Faster Beta Weil Pairing on BLS Pairing Friendly Curves with Odd Embedding Degree.

Laurian Azebaze Guimagang
azebazelaurian@yahoo.fr

UNIVERSITE DE YAOUNDE I
UNIVERSITY OF YAOUNDE I

SIAM AG23 at Eindhoven

Registration & travel support for this presentation was provided by the SIAM.

Outline

1. Introduction
2. β-Weil Pairing
   2.1. Analyse the β-Weil Pairing
   2.2. New formula of the β-Weil Pairing
   2.3. Application on BLS-27 curves
   2.4. Suitable method for the evaluation
3. Conclusion

Definition 1 (Pairing). A pairing is a non degenerate bilinear map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3 : (Q, P) \longmapsto e(P, Q)\ .$$

- Bilinearity
  $e(P_1 + P_2, Q_1) = e(P_1, Q_1) \cdot e(P_2, Q_1)$ and
  $e(P_1, Q_1 + Q_2) = e(P_1, Q_1) \cdot e(P_1, Q_2)$;
- non-degeneracy
  if $e(P, Q) = 1_{\mathbb{G}_3}$ for all $P \in \mathbb{G}_1$, implies $Q = \mathcal{O}_{\mathbb{G}_2}$ and
  if $e(P, Q) = 1_{\mathbb{G}_3}$ for all $Q \in \mathbb{G}_2$, implies $P = \mathcal{O}_{\mathbb{G}_1}$;
- computability, e can be efficiently computed.

- Weil Pairing introduced by André Weil in 1940 to study the arithmetic on elliptic curves and Abelian varieties.
  The Weil pairing is defined as :

$$\begin{array}{rcl} e_W : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] & \longrightarrow & \mu_r \\ (P, Q) & \longmapsto & (-1)^r \dfrac{f_{r,P}(Q)}{f_{r,Q}(P)}. \end{array}$$

- There exist many variants of Weil pairing
  - α-Weil pairing by D.F. Aranha et *al* 2011,
  - β-Weil pairing by D.F. Aranha et *al.* 2012, Fouotsa et *al.* 2019,
  - ω-Weil pairing by C. Zhao et *al.* 2011.

- Weil pairings are suitable for parallel evaluation.

- Tate pairing introduced by John Tate in 1958.
  The Tate pairing

$$\begin{array}{rcl} e_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] & \longrightarrow & \mu_r \\ (P, Q) & \longmapsto & f_{r,P}(Q)^{(q^k-1)/r}. \end{array}$$

- There exist many variants of Tate pairing
  - Ate pairing due to F. Hess et *al.* 2006,
  - Optimal Ate pairing due to Vercauteren 2010,
  - superoptimal pairing due to Q.Y. Feng et *al.* 2013.
  - $\cdots$.

Faster algorithm to compute $f_{r,P}(Q)$ (V. Miller 1985)

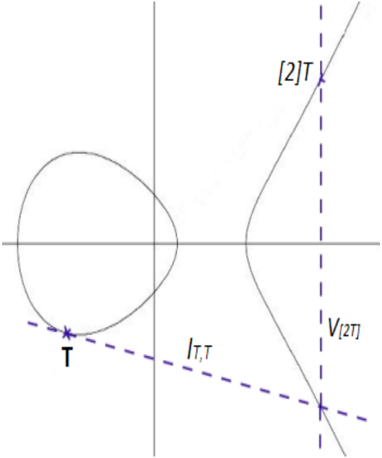
$$f_{1,P} = 1, \qquad f_{i+j,P} = f_{i,P} \cdot f_{j,P} \cdot \frac{l_{[i]P,[j]P}}{\mathcal{V}_{[i+j]T}}$$

Algorithm 1: Miller loop

Input: $r = s_n 2^n + \sum_{i=0}^{n-1} s_i 2^i$, P, Q
Output: $f_{r,P}(Q)$

$f \leftarrow 1,$
$T \leftarrow P,$
for i *from* $n-1$ *down to* 0 **do**
  $f \leftarrow f^2 . \frac{l_{T,T}(Q)}{\mathcal{V}_{[2]T}(Q)}, \qquad T \leftarrow [2]T$
  if $s_i = 1$ **then**

return f.



Algorithm 2: Miller loop

Input: $r = s_n 2^n + \sum_{i=0}^{n-1} s_i 2^i$, P, Q

Output: $f_{r,P}(Q)$

$f \leftarrow 1$,

$T \leftarrow P$,

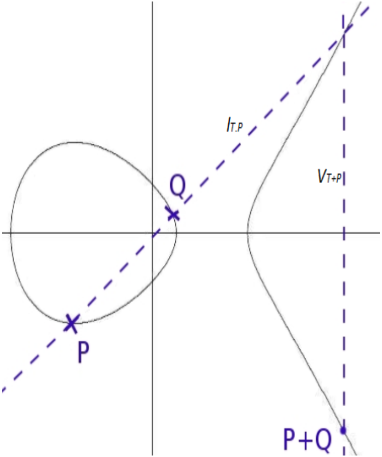
for i *from* $n-1$ *down to* 0 **do**

  $f \leftarrow f^2 . \frac{l_{T,T}(Q)}{\mathcal{V}_{[2]T}(Q)}$, $T \leftarrow [2]T$

  if $s_i = 1$ **then**

    $f \leftarrow f . \frac{l_{T,P}(Q)}{\mathcal{V}_{T+P}(Q)}$, $T \leftarrow T + P$

return f.



The security of pairing based protocol depends :

→ on DLP over elliptic curve.

→ on DLP over finite field $\mathbb{F}^*_{q^k}$.

- **T. Kim and R. Barbulescu., Extended tower number field sieve : A new complexity for the medium prime case.** August 14-18, 2016, Proceedings, Part I, volume 9814 of Lecture Notes in Computer Science, pages 543–571. Springer, 2016.

Where the finite field $\mathbb{F}_{q^k}$ verify the conditions

- $q = exp(c\log(Q)^l(\log(\log(Q)))^{1-l})$ with $c > 0$ and $\frac{1}{3} < l < \frac{2}{3}$,
- $k = a \times b$ with $gcd(a, b) = 1$.

They provided some practical examples for $k = 6$ and $k = 12$ (see that k is even)
We focus your studies on Elliptic Curves with odd embedding degree as an alternative for the security of pairing based protocols.

Theorem – Fouotsa E. and Pecha A. and EL Mrabet N.[6],

Let $h(x) = \sum_{i=0}^{w} h_i x^i$ in $\mathbb{Z}[x]$ and $m = h(p)/r$ such that $m \nmid r$.
The $\beta-$Weil pairing is defined as follows :

$$\beta_k : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left[\prod_{i=0}^{e-1} \left(\frac{f_{p,h,Q}([p^i]P)}{f_{p,h,[p^i]P}(Q)} \right)^{p^{e-1-i}} \right]^{p^l-1}, \tag{1}$$

for $e = \frac{k}{d}$ and $mkq^{k-1} \not\equiv ((q^k - 1)/r).\sum_{i=0}^{l} ic_i q^{i-1} \mod r$.

Lemma.

1. *Elimination of the exponents : which come from the remarks that for any $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$:*

$$f_{p,h,P}^{p^i}(Q) = f_{p,h,P}(\pi_{p^i}(Q)) \quad \text{and} \quad f_{p,h,Q}^{p^i}(P) = f_{p,h,\pi_{p^i}(Q)}(P).$$

2. *Elimination of the denominators.*

For all $a \in \mathbb{Z}$ and any k, we obtain the following two relations :

$$(i) \quad f_{a,P}^{-1} = f_{a,-P}.\mathcal{V}_{[a]P}.\mathcal{V}_P^{-a}$$

$$(ii) \quad f_{p,h,P}^{-1} = f_{p,h,-P}.\prod_{j=0}^{w} \mathcal{V}_{[p^j]P}^{-h_j}$$

Theorem – Azebaze L., Fouotsa E., Pecha A., El Mrabet N. [1]

For every elliptic curves the new formula of β-Weil pairing is given as follows
$\beta_k(P, Q) =$

$$\boxed{\left(\prod_{i=0}^{e-1} f_{p,h,\pi_{p^{\delta_i}}(Q)}([p^i]P) \cdot f_{p,h,[p^i]\overline{P}}(\pi_{p^{\delta_i}}(Q)) \cdot \prod_{j=0}^{w} \mathcal{V}_{[p^{i+j}]P}^{-h_j}(\pi_{p^{\delta_i}}(Q))\right)^{p^l-1}},$$

where $\overline{P} = -P$ and $\delta_i = e - 1 - i$.

Remark : For k even we found the result of **K. Kinoshita and K. Suzuki, Accelerating Beta Weil pairing with precomputation and multi-pairing techniques.** September 2-4, 2020, Proceedings, volume 12231 of Lecture Notes in Computer Science, pages 261–281. Springer, 2020.

Corollary – Azebaze L., Fouotsa E., Pecha A., El Mrabet N. [1]

For BLS curves of embedding degrees $k = 9, 15$ and 27, the polynomial $h(z)$ for the extended Miller's function yields

$$h(z) = x - z, \quad \textit{then} \quad f_{p,h,P} = f_{x,P}$$

then

$$\boxed{\beta_k(P, Q) = \left(\prod_{i=0}^{e-1} f_{x,Q_i}(P_i) \cdot f_{-x,P_i}(Q_i) \cdot \mathcal{V}_{P_{i+1}}(Q_i) \right)^{p^l - 1}}, \qquad (2)$$

where $P_i = [p^i]P$ and $Q_i = \pi_{p^{\delta_i}}(Q)$.

Barreto–Lynn–Scott curves [2]
Parameters of BLS−27 elliptic curve

$$\begin{aligned} r &= \frac{1}{3}(x^{18}+x^{9}+1), \\ p &= \frac{1}{3}(x-1)^2(x^{18}+x^{9}+1)+x, \\ t &= x+1 \end{aligned}$$

To rich 256-bit level of security,

$$x = -2^{51}-2^{31}-2^{21}-2^{8}-2^{4}.$$

This curve admit twists of degree three which enable

- denominator elimination technique,
- computation to be done in subfields.
- Also it is a suitable choice for computing product of pairings (by X. Zhang et *al.* 2012).

β-Weil pairing in $E(\mathbb{F}_{p^{27}})$

$$\beta_k(P,Q) =$$

$$\Big[f_{x,\pi_{p^8}(Q)}(P)\cdot f_{-x,P}(\pi_{p^8}(Q))\cdot f_{x,\pi_{p^5}(Q)}(P_3)\cdot f_{-x,P_3}(\pi_{p^5}(Q))\cdot f_{x,\pi_{p^2}(Q)}(P_6)$$
$$\cdot f_{-x,P_6}(\pi_{p^2}(Q))\cdot \mathcal{V}_{P_1}(\pi_{p^8}(Q))\cdot \mathcal{V}_{P_4}(\pi_{p^5}(Q))\cdot \mathcal{V}_{P_7}(\pi_{p^2}(Q))$$
$$\cdot f_{x,\pi_{p^7}(Q)}(P_1)\cdot f_{-x,P_1}(\pi_{p^7}(Q))\cdot f_{x,\pi_{p^4}(Q)}(P_4)\cdot f_{-x,P_4}(\pi_{p^4}(Q))\cdot f_{x,\pi_{p}(Q)}(P_7)$$
$$\cdot f_{-x,P_7}(\pi_{p}(Q))\cdot \mathcal{V}_{P_2}(\pi_{p^7}(Q))\cdot \mathcal{V}_{P_5}(\pi_{p^4}(Q))\cdot \mathcal{V}_{P_8}(\pi_{p}(Q))$$
$$\cdot f_{x,\pi_{p^6}(Q)}(P_2)\cdot f_{-x,P_2}(\pi_{p^6}(Q))\cdot f_{x,\pi_{p^3}(Q)}(P_5)\cdot f_{-x,P_5}(\pi_{p^3}(Q))\cdot f_{x,Q}(P_8)$$
$$\cdot f_{-x,P_8}(Q)\cdot \mathcal{V}_{P_3}(\pi_{p^6}(Q))\cdot \mathcal{V}_{P_6}(\pi_{p^3}(Q))\cdot \mathcal{V}_{P_9}(Q)\Big]^{p^9-1}.$$

consists to **compute and store** line functions of the Miller function $f_{s,Q}$ or $f_{s,P}$.

-

Algorithm 3: CSL : Compute and Store Line functions [8]

Input: $R \in \mathbb{G}_1$ (or $R \in \mathbb{G}_2$), integer s
Output: An array g of $\lfloor log_2 s \rfloor + HW(s) - 1$ line functions and sR.
$HW(s)$ is the hamming weight of s

$T \leftarrow R$ and $j \leftarrow 1$
for $i \leftarrow \lfloor log_2 s \rfloor - 1$ *to 0* **do**
  $g[j] \leftarrow \ell_{T,T}$, $T \leftarrow 2T$, $j \leftarrow j + 1$
  if $i{-}th$ *bit of* $s = \pm 1$ **then**
    $g[j] \leftarrow \ell_{T,R}$, $T \leftarrow T + R$, $j \leftarrow j + 1$
return g, T.

- **Algorithm 4:** EPM : Evaluate Product of e-Multi-functions

Input: $\left[(g_0, P_0), \ldots, (g_{e-1}, P_{e-1}), (h_0, Q_0), \ldots, (h_{e-1}, Q_{e-1})\right]$

$s = \sum_{i=0}^{n} l_i 2^i$, where $l_i \in \{-1, 0, 1\}$ and $l_n \neq 0$

$h_i's$ are the precomputed line functions from $f_{s,\overline{P}_i}$

$g_i's$ are the precomputed line functions from f_{s,Q_i}

Output: $\prod_{i=0}^{e-1}\left(f_{s,Q_i}([p^i]P) f_{s,P_i}(Q_i)\right)$,

$f \leftarrow 1$,

for *j from $n-1$ down to 0* **do**

  $f \leftarrow f^2$

  for *i from $e-1$ down to 0* **do**

    $f \leftarrow f . \prod_{i=0}^{e-1} g_i[j](P_i).h_i[j](Q_i)$

  if $l_j = \pm 1$ **then**

    for *i from $e-1$ down to 0* **do**

      $f \leftarrow f . \prod_{i=0}^{e-1} g_i[j](P_i).h_i[j](Q_i)$

return f.

Parallel computation of the proposed β−Weil pairing.

For parallel computation using 3 processors, $\beta_{27}(P,Q)$ can be regarded as

$$\beta_{27}(P,Q) = (X^{p^2} \cdot Y^p \cdot Z)^{p^9-1},$$

where

$$\begin{aligned}
X &= f_{x,\pi_{p^6}(Q)}(P) \cdot f_{-x,P}(\pi_{p^6}(Q)) \cdot f_{x,\pi_{p^3}(Q)}(P_3) \cdot f_{-x,P_3}(\pi_{p^3}(Q)) \cdot f_{x,Q}(P_6) \\
&\quad \cdot f_{-x,P_6}(Q) \cdot H_1, \\
Y &= f_{x,\pi_{p^6}(Q)}(P_1) \cdot f_{-x,P_1}(\pi_{p^6}(Q)) \cdot f_{x,\pi_{p^3}(Q)}(P_4) \cdot f_{-x,P_4}(\pi_{p^3}(Q)) \cdot f_{x,Q}(P_7) \\
&\quad \cdot f_{-x,P_7}(Q) \cdot H_2, \\
Z &= f_{x,\pi_{p^6}(Q)}(P_2) \cdot f_{-x,P_2}(\pi_{p^6}(Q)) \cdot f_{x,\pi_{p^3}(Q)}(P_5) \cdot f_{-x,P_5}(\pi_{p^3}(Q)) \cdot f_{x,Q}(P_8) \\
&\quad \cdot f_{-x,P_8}(Q) \cdot H_3
\end{aligned}$$

and

$$\begin{aligned}
H_1 &= \mathcal{V}_{P_1}(\pi_{p^6}(Q)) \cdot \mathcal{V}_{P_4}(\pi_{p^3}(Q)) \cdot \mathcal{V}_{P_7}(Q), \\
H_2 &= \mathcal{V}_{P_2}(\pi_{p^6}(Q)) \cdot \mathcal{V}_{P_5}(\pi_{p^3}(Q)) \cdot \mathcal{V}_{P_8}(Q), \\
H_3 &= \mathcal{V}_{P_3}(\pi_{p^6}(Q)) \cdot \mathcal{V}_{P_6}(\pi_{p^3}(Q)) \cdot \mathcal{V}_{P_9}(Q).
\end{aligned}$$

Comparison between optimal Ate pairings, the original $\beta-$Weil pairing and the proposed $\beta-$Weil pairing.

Table 1 – Theoretical cost of the optimal Ate pairings, the original $\beta-$Weil pairing and the proposed $\beta-$Weil pairing.

curve	pairing	Serial computation	Parallel computation (with 3 processors)
BLS-27	Optimal Ate	$176881M + 56I$	$156301M + 20I$
	original $\beta-$Weil pairing	$475463M + 497I$	$162251M + 166I$
	Proposed $\beta-$Weil pairing	$261608M + 64I$	$103030M + 64I$

- For serial computation, the theoretical cost of the proposed β-Weil pairing is 44.78% more benefit than the original β-Weil pairing.
- For parallel computation, the theoretical cost of the proposed β-Weil pairing is faster than Optimal Ate.

- **Azebaze G.L., Fouotsa, E., El Mrabet N., and Pecha N.A., Faster Beta Weil Pairing on BLS Pairing Friendly Curves with Odd Embedding Degree.** Math. Comput. Sci. 16, 13. Springer Birkhäuser, (2022). https ://doi.org/10.1007/s11786-022-00531-w

Accelerating the β-Weil pairing

- $\rightarrow$ Generalise the β-Weil pairing formula given by Kinoshita et *al.*
- $\rightarrow$ Simplify the formula and makes it to be suitable for parallel execution
- $\rightarrow$ Provide efficient algorithm for his evaluation

[1] L.G. Azebaze, E. Fouotsa, N. El Mrabet, and A. Pecha.
Faster beta weil pairing on BLS pairing friendly curves with odd embedding degree.
Math. Comput. Sci., 16(2) :13. Springer Birkhäuser, 2022.

[2] P.S.L.M. Barreto, B. Lynn, and M. Scott.
Constructing elliptic curves with prescribed embedding degrees.
In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers*, volume 2576 of *Lecture Notes in Computer Science*, pages 257–267. Springer, 2002.

[3] D. Boneh and M.K. Franklin.
Identity-based encryption from the weil pairing.
In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 213–229, 2001.

[4] Q.Y. Feng, T.C. Ming, G. Baoan, and X.M. Zhi.
Super-optimal pairings.
In *Mechanical Engineering, Materials and Energy II*, volume 281 of *Applied Mechanics and Materials*, pages 127–133. Trans Tech Publications Ltd, 3 2013.

[5] G. Fotiadis and E. Konstantinou.

TNFS resistant families of pairing-friendly elliptic curves.
Theoretical Compututer Science, 800 :73–89. Elsevier, 2019.

[6] E. Fouotsa, A. Pecha, and N. El Mrabet.
Beta Weil pairing revisited.
Afrika Matematika., 30 :371–388. Springer, 2019.

[7] A. Joux.
A one round protocol for tripartite diffie-hellman.
In *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, volume 1838, pages 385–394, 2000.

[8] K. Kinoshita and K. Suzuki.
Accelerating Beta Weil pairing with precomputation and multi-pairing techniques.
In Kazumaro Aoki and Akira Kanaoka, editors, *Advances in Information and Computer Security - 15th International Workshop on Security, IWSEC 2020, Fukui, Japan, September 2-4, 2020, Proceedings*, volume 12231 of *Lecture Notes in Computer Science*, pages 261–281. Springer, 2020.

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

I would like to thank you for your attention.

I would also like to thank the organizers for inviting me to deliver this presentation.