x-Superoptimal Pairings on Elliptic Curves with Embedding Degrees 13 and 19.

Emmanuel FOUOTSA
**The University of Bamenda
Cameroon**

Participation Supported by :

European Mathematical Society
Committee for Developing Countries

Inria
CARAMBA Team

Registration and Travel support for thispresentation was provided by:

siam
Society for Industrial and Applied Mathematics

2023 SIAM Conference on Applied Algebraic Geometry (AG23) July 10 – 14, 2023,
Eindhoven, The Netherlands

Outline

1. Introduction

2. Security of pairings

3. Pairings
    - 3.1. Optimal Ate pairing
    - 3.2. Super-optimal pairing

4. Application on BW-13 curve
    - 4.1. x-superoptimal pairing on BW-13 curve
    - 4.2. Fast Evaluation of x-superoptimal pairing

5. Conclusion

INTRODUCTION

The Tate pairing

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

Algorithm 1: Miller loop

```
Input: $r = s_n 2^n + \sum_{i=0}^{n-1} s_i 2^i$, where $s_i \in \{0,1\}$
Output: $f_{r,P}(Q)$
$f \leftarrow 1$,
$T \leftarrow P$,
for $i$ from $n-1$ down to $0$ do
    $f \leftarrow f^2 . \frac{l_{T,T}(Q)}{\mathcal{V}_{[2]T}(Q)}$,    $T \leftarrow [2]T$                ▷ DOUBLE STEP
    if $s_i = 1$ then
        $f \leftarrow f . \frac{l_{T,P}(Q)}{\mathcal{V}_{T+P}(Q)}$,    $T \leftarrow T + P$        ▷ ADDITION STEP
return $f$.
```

INTRODUCTION :

- Pairings have first been studied in mathematical research areas such as
  - ▷ algebraic geometry and
  - ▷ number theory
- In 1993 the MOV attack, named after Menezes, Okamoto, and Vanstone, uses pairing to convert discrete log problem in ECC to one in finite field.
  - ▷ Best algorithms to solve DLP in elliptic curve is in $O(\sqrt{n})$.
  - ▷ In $\mathbb{F}_{p^k}$ there are sub-exponential complexity.
  - ▷ The attack is only efficient for small k.
- Pairing are used to ameliorate existent protocols.
  - → Joux's one round tripartite key exchange
  - → Construct verifiable delay functions

INTRODUCTION

- To create new protocols.
  - → Identity based encryption (IBE)
  - → Compress public keys in key exchange (Isogeny-based encryption)
  - → Ring signatures
- Practical importance of pairings
  - → Zcash cryptocurrency
  - → Electronic voting
  - → Internet of Things (IoT)

Security of pairings

The security of pairing based protocol depends :

→ on DLP over E

→ on DLP over $\mathbb{F}_{q^k}^*$

- T. Kim and R. Barbulescu., **Extended tower number field sieve : A new complexity for the medium prime case.** In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I, volume 9814 of Lecture Notes in Computer Science, pages 543–571. Springer, 2016.
- A. 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, Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part II, volume 12111 of Lecture Notes in Computer Science, pages 535–564. Springer, 2020.

BN curve are no more valid. Some elliptic curves resistant to these attacks have been constructed namely

- Aurifeuillean curves,
- BLS curves and
- BW curves.

Types of pairings

- Weil pairing (By Weil 1940). The new variants today α-Weil, β-Weil and ω-Weil pairings
- Tate pairing (by Tate 1958). New variant today Ate pairing, optimal Ate,...

Let

- E an elliptic curve over $\mathbb{F}_q$,
- r a large prime factor of $\#E(\mathbb{F}_q)$,
- k the smallest positive integer such that r divides $q^k - 1$.

OPTIMAL ATE PAIRING

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

Theorem 1 *([Ver10]). Let $\lambda = mr$ with $r \nmid m$ and write $\lambda = \sum_{i=0}^{n} c_i p^i$ then*

$$a_{op} : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_3, (Q, P) \longmapsto \left(\prod_{i=0}^{n} f^{p^i}_{c_i,Q}(P) \cdot \prod_{i=0}^{n} \frac{l_{[s_{i+1}]Q,[c_i p^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{\frac{p^k-1}{r}}$$

with $s_i = \sum_{j=i}^{n} c_j p^j$,

- $r/(q^k - 1)$, then $\phi_k(p) = 0 \mod r$, and there exists c_i's such that $c_0 r = \sum_{i=1}^{\Phi(k)-1} c_i p^i$
- Find c_i's with LLL applied to

$$L = \begin{bmatrix} r & 0 & 0 & \dots & 0 \\ -p & 1 & 0 & \dots & 0 \\ -p^2 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ -p^{\varphi(k)-1} & 0 & 0 & \dots & 1 \end{bmatrix}.$$

- Find short vector $(c_0, \dots, c_{\varphi(k)-1})$ with $|c_i| \leq r^{1/\varphi(k)}$.

OPTIMAL ATE PAIRING

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

***Theorem 2** ([Ver10]).*

$$a_{op} : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_3, (Q, P) \longmapsto \left(\prod_{i=0}^{n} f_{c_i,Q}^{p^i}(P) \cdot \prod_{i=0}^{n} \frac{l_{[s_{i+1}]Q,[c_i p^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{\frac{p^k-1}{r}}$$

- $|c_i| \leq r^{1/\varphi(k)}$.
- The computation of $f_{c_i,Q}$ requires at most $\frac{\log_2(r)}{\varphi(k)}$ iterations in the Miller algorithm
- One can't do better : Optimal Pairing
- Except there exists an efficient computable endomorphism over E than the Frobenius : Superoptimal

Let

- $E/\mathbb{F}_q : y^2 = x^3 + b$
- $q \equiv 1 \mod 3$
- $\phi : (x, y) \longmapsto (\xi x, y)$ where ξ is the primitive cube root of unity in $\mathbb{F}_q^\star$.
- $Spec(\phi) = \{\lambda, \mu\}$ integer such that r divides $q^k - 1$.
- $\psi = \pi_q \circ \phi$ and $Spec(\psi) = \{\lambda, \omega = q\mu\}$
- If $gcd(3, k) = 1$ then,
- ω is a primitive $3k$-th root of unity in $\mathbb{F}_r$ and $r/(\omega^{3k} - 1)$.
- Set $G_1 = E(\mathbb{F}_q)[r] \cap (\phi^2 - [\mu])$ and $G_2 = E(\mathbb{F}_{q^k})[r] \cap (\phi^2 - [\lambda])$

Superoptimal pairing

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.

Theorem 3*. Yang Feng et al. [FMBZ13] Let*

- $\#E(\mathbb{F}_q) = cr = \sum_{i=0}^{n} a_i\omega^i = h(\omega), \quad a_{n+1} = 0$ *and*
- $r^2 \nmid (\omega^{3k} - 1)$,

then there exists a bilinear pairing

$$\begin{aligned} a_{sup} : \mathbb{G}_2 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (Q, P) &\mapsto \left(\prod_{j=0}^{n} \prod_{i=0}^{2} \left[f_{a_j,Q}^{\omega^j}(\phi^{2i}(P)) \cdot \frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} \right]^{\lambda^i} \right)^{\frac{p^k-1}{r}} . \quad (1) \end{aligned}$$

Where

$$h^{(j)} = \sum_{i=0}^{j} a_i\omega^i.$$

Let $h'(\omega) = \sum_{j=1}^{n} ja_j\omega^{j-1}$.

Moreover, $a_{sup}(.,.)$ *is non-degenerate if and only if*

$$r \nmid [3kh(\omega) - (\omega^{3k} - 1)\omega h'(\omega)].$$

Construction of a_i's

$$r/(\omega^{3k}-1) \Longrightarrow \Phi_{3k}(\omega) = 0 \mod r$$

and therefore there exists a_i's such that

$$a_0 r = \sum_{i=1}^{\varphi(3k)-1} a_i \omega^i .$$

The a_i's is obtained by finding short vectors in the following $\varphi(3k)$-dimensional lattice

$$M = \begin{bmatrix} r & 0 & 0 & \dots & 0 \\ -\omega & 1 & 0 & \dots & 0 \\ -\omega^2 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ -\omega^{\varphi(3k)-1} & 0 & 0 & \dots & 1 \end{bmatrix} .$$

By the theorem of Minkowski $|a_i| \leq r^{\frac{1}{\varphi(3k)}}$.

The length of a_i's is

$$\frac{\log_2(r)}{\varphi(3k)} \quad i.e. \quad \frac{1}{2} \cdot \frac{\log_2(r)}{\varphi(k)} .$$

So, the Miller loop length is the half of that of optimal pairings.

R. Clarisse, S. Duquesne, and O. Sanders., Curves with fast computations in the first pairing group. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings, volume 12579 of Lecture Notes in Computer Science, pages 280–298. Springer, 2020.

curve recommended for ring signature : $BW13$

The curve $BW13$ is an elliptic curve with embedding degree $k = 13$ and parametrized by the polynomials

- $q(x) = (\frac{1}{3}) * (x+1)^2(x^{26} - x^{13} + 1) - x^{27}$,
- $r(x) = \Phi_{78}(x)$ and
- $t(x) = -x^{14} + x + 1$.
- For the seed $x = -2059$ recommended by [DZZZ21], the corresponding elliptic curve is given as $Y^2 = X^3 - 17$ and the bit length of the prime p is 310.

Application on BW-13 curve

***Lemma 4**. Let the endomorphism $\phi : (x, y) \longmapsto (\xi x, y)$ with ξ a primitive third root of unity, such that $\phi(P) = \lambda P$ in $\mathbb{G}_1$ for $\lambda \in \mathbb{Z}/r\mathbb{Z}$ then* $\lambda = \dfrac{t - f - 2}{2f} \mod r$ *where, $Df^2 = t^2 - 4p$ with $D = -3$ and $\mu = \lambda^2$.*

For this curve the eigenvalue

$$\lambda = -x^{13} \quad \textit{and} \quad \mu = \lambda^2 = x^{26}.$$

Application on BW-13 curve

By using the function LLL in MAGMA $V2.26-8$ calculator, we obtain a short vector

$$[x,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0].$$

$$a_0 = x, \quad a_{14} = 1 \quad \mathit{and} \quad a_i = 0 \quad \textbf{otherwise so,} \quad h(\omega) = x + \omega^{14}.$$

Corollary 5. *The superoptimal pairing on the curves $BW13-P310$ gives*

$$\boxed{a_{sup}(Q,P) = \left(f_{|x|,Q}(P)\cdot f^{\lambda}_{|x|,Q}(\phi^2(P))\cdot f^{\mu}_{|x|,Q}(\phi(P))\right)^{-\frac{p^k-1}{r}}.} \tag{2}$$

Proof

$$\prod_{j=0}^{n}\prod_{i=0}^{2}\left[f^{\omega^j}_{a_j,Q}(\phi^{2^i}(P))\right]^{\lambda^i} = \prod_{i=0}^{2}\left[f^{\omega^0}_{x,Q}(\phi^{2^i}(P))\cdot f^{\omega^{14}}_{1,Q}(\phi^{2^i}(P))\right]^{\lambda^i} = \prod_{i=0}^{2}\left[f_{x,Q}(\phi^{2^i}(P))\right]^{\lambda^i}. \tag{3}$$

For every i and $1 \leq j \leq 12$,

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,[0]Q}(\phi^{2i}(P))}{v_{[x]Q}(\phi^{2i}(P))} = \frac{v_{[x]Q}(\phi^{2i}(P))}{v_{[x]Q}(\phi^{2i}(P))} = 1. \tag{4}$$

For every i and $j = 13$ since, $h(\omega) = 0 \mod r$ then $[x + \omega^{14}]Q = \mathcal{O}$ and $[\omega^{14}]Q = -[x]Q$,

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,[\omega^{14}]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,-[x]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} \equiv v_{[x]Q}(\phi^{2i}(P)),$$

this is because $v_{[x+\omega^{14}]Q}(\phi^{2i}(P))$ will be sent to 1 during the final exponentiation.
For every i and $j = 14$,

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x+\omega^{14}]Q,[0]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} = \frac{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} = 1$$

Thus,

$$a_{sup}(Q,P) = \left(\prod_{j=0}^{n}\prod_{i=0}^{2}\left[f_{a_j,Q}^{\omega^j}(\phi^{2i}(P)) \cdot \frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}\right]^{\lambda^i}\right)^{\frac{p^k-1}{r}} \quad (5)$$

$$= \left(\prod_{i=0}^{2}\left[f_{x,Q}(\phi^{2i}(P)) \cdot v_{[x]Q}(\phi^{2i}(P))\right]^{\lambda^i}\right)^{\frac{p^k-1}{r}} \quad (6)$$

Application on BW-13 curve

Since $x < 0$, $x = -|x|$ and $f_{x,Q} = f^{-1}_{|x|,Q} \cdot f_{-1,[|x|]Q} = f^{-1}_{|x|,Q} \cdot v^{-1}_{[x]Q}$. Therefore Equation 6 yields :

$$a_{sup}(Q,P) = \left(\prod_{i=0}^{2} \left[f^{-1}_{|x|,Q}(\phi^{2i}(P)) \right]^{\lambda^i} \right)^{\frac{p^k-1}{r}}.$$

Also, $\lambda^2 = \mu$, then,

$$a_{sup}(Q,P) = \left(f_{|x|,Q}(P) \cdot f^{\lambda}_{|x|,Q}(\phi^2(P)) \cdot f^{\mu}_{|x|,Q}(\phi(P)) \right)^{-\frac{p^k-1}{r}}.$$

Lower the cost of the inner exponent

The Lemma 6 eliminates the exponentiation by μ whereas Lemma 7 transforms the exponentiation by $x\lambda$ into $p-x$.

Lemma 6. *For any $f \in \mathbb{F}^*_{p^k}$,*

$$\boxed{f^{\mu\frac{p^k-1}{r}} = f^{(-1-\lambda)\frac{p^k-1}{r}}}$$

- Since,

$$r/(1+\lambda+\mu) \quad \textit{and} \quad f \in \mathbb{F}^*_{p^k} \quad \textit{then,} \quad f^{(1+\lambda+\mu)\frac{p^k-1}{r}} = 1.$$

So, $f^{\mu\cdot\frac{p^k-1}{r}} = f^{(-1-\lambda)\cdot\frac{p^k-1}{r}}$. ■

Lemma 7. *For any $f \in \mathbb{F}^*_{p^k}$ and $\lambda = -x^{13}$*

$$\boxed{f^{(x\lambda)\frac{p^k-1}{r}} = f^{(p-x)\frac{p^k-1}{r}}.}$$

- - $|E(\mathbb{F}_p)| = p+1-t = p+1-(-x^{14}+x+1) = p-x\lambda-x.$
  - for $r/(p-x\lambda-x)$, $f^{(p-x\lambda-x)\frac{p^k-1}{r}} = 1$. So, $f^{(x\lambda)\frac{p^k-1}{r}} = f^{(p-x)\frac{p^k-1}{r}}$.

■

Theorem 8. *If the* $\gcd(x, r) = 1$, *we derive a new pairing called* x*-superoptimal pairing defined as*

$$a^{x}_{sup}(Q, P) = \left(\left(f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))\right)^{x} \cdot \left(f_{|x|,Q}(\phi^2(P)) \cdot f^{-1}_{|x|,Q}(\phi(P))\right)^{p}\right)^{-\frac{p^k-1}{r}} . \quad (7)$$

It is a non-degenerate bilinear pairing on $BW13 - P310$.

- Let
$$A = f_{|x|,Q}(P), \quad B = f_{|x|,Q}(\phi^2(P)) \quad and \quad C = f_{|x|,Q}(\phi(P))$$
  - $a_{sup}(Q, P) = \left(A \cdot B^{\lambda} \cdot C^{\mu}\right)^{-\frac{p^k-1}{r}}$
  - from Lemma 6, $a_{sup}(Q, P) = \left(A \cdot B^{\lambda} \cdot C^{-1-\lambda}\right)^{\frac{1-p^k}{r}} = \left(A \cdot C^{-1} \cdot (B \cdot C^{-1})^{\lambda}\right)^{\frac{1-p^k}{r}}$
  - by raising to the power x and using Lemma 7, we then obtain $a^{x}_{sup}(Q, P) = \left((A \cdot C^{-1})^{x} \cdot (B \cdot C^{-1})^{p-x}\right)^{\frac{1-p^k}{r}} = \left((A \cdot B^{-1})^{x} \cdot (B \cdot C^{-1})^{p}\right)^{\frac{1-p^k}{r}}$.

■

x-SUPEROPTIMAL PAIRING : ADDING LINE

$$a^{x}_{sup}(Q,P) = \left(\left(f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^{2}(P)) \right)^{-x} \cdot \left(f^{-1}_{|x|,Q}(\phi^{2}(P)) \cdot f_{|x|,Q}(\phi(P)) \right)^{p} \right)^{\frac{p^{k}-1}{r}} .$$

In Jacobian coordinates the quadruple (X, Y, Z, Z^2) represents the affine point $(X/Z^2; Y/Z^3)$. This saves inversions and multiplications.

Algorithm 2: ADDING LINE Given $S, Q \in \mathbb{G}_2$, compute $S + Q$ and the evaluation of the lines (SQ) at $P, \phi(P)$ and $\phi^2(P)$ in $\mathbb{G}_1$

```
$(X, Y, Z, Z_2) \leftarrow S$, $(x_Q, y_Q) \leftarrow Q$, $(x_P, y_P) \leftarrow P$,
$t_1 \leftarrow x_Q \cdot Z_2 - X$, $t_2 \leftarrow y_Q \cdot Z \cdot Z_2 - Y$, $t_3 \leftarrow t_1^2$, $t_4 \leftarrow t_1 \cdot t_3$, $t_5 \leftarrow X \cdot t_3$,
$\mathbf{X} \leftarrow t_2^2 - (t_4 + 2t_5)$, $\mathbf{Y} \leftarrow t_2 \cdot (t_5 - \mathbf{X}) - Y \cdot t_4$, $\mathbf{Z} \leftarrow Z \cdot t_1$,
$\lambda_d \leftarrow \mathbf{Z}$, $t_6 \leftarrow \lambda_d \cdot (y_P - y_Q)$,
$\lambda_n \leftarrow t_6 - t_2 \cdot (x_P - x_Q)$,
$\lambda_{n1} \leftarrow t_6 - t_2 \cdot (x_{\phi(P)} - x_Q)$,
$\lambda_{n2} \leftarrow t_6 - t_2 \cdot (x_{\phi^2(P)} - x_Q)$
return $S = (X, Y, Z, Z^2), \lambda_n, \lambda_{n1}, \lambda_{n2}$
```

$$C_{ADDLINE} = 11M_k + 3S_k$$

x-SUPEROPTIMAL PAIRING : DOUBLING LINE

Algorithm 3: DOUBLING LINE Given $S \in \mathbb{G}_2$, compute $[2]S$ and the evaluation of the tangent S mapped at $P, \phi(P)$ and $\phi^2(P)$ in $\mathbb{G}_1$

```
$(X, Y, Z, Z_2) \leftarrow S$, $(x_P, y_P) \leftarrow P$;
$t_1 \leftarrow Y^2$, $t_2 \leftarrow 4X \cdot t_1$
if $a = -3u^2$ for a small $u \in \mathbb{F}_p$ then
    $t_3 \leftarrow 3(X - uZ_2) \cdot (X + uZ_2)$
else
    $t_3 \leftarrow 3X^2 + a \cdot Z_2^2$
$\mathbf{X} \leftarrow t_3^2 - 2t_2$, $\mathbf{Y} \leftarrow t_3 \cdot (t_2 - \mathbf{X}) - 8t_1^2$, $\mathbf{Z} \leftarrow Z \cdot 2Y$,
$\lambda_d \leftarrow \mathbf{Z}.Z_2$, $t_4 \leftarrow \lambda_d \cdot y_P - 2t_2$,
$\lambda_n \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_P - X)$,
$\lambda_{n1} \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_{\phi(P)} - X)$,
$\lambda_{n2} \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_{\phi^2(P)} - X)$
return $S = (X, Y, Z, Z^2), \lambda_n, \lambda_{n1}, \lambda_{n2}$
```

$$C_{DLINE} = 7M_k + 6S_k + 4kM$$

x-superoptimal pairing : VERTICAL LINE

Algorithm 4: VERTICAL LINE Compute the line through S and $-S$ evaluated at $P, \phi(P)$ and $\phi^2(P)$ in $\mathbb{G}_1$

```
$(X, Y, Z, Z_2) \leftarrow S$
$(x_P, y_P) \leftarrow P$
$\mu_n = Z_2 \cdot x_P - X$
$\mu_{n1} = Z_2 \cdot x_{\phi(P)} - X$
$\mu_{n2} = Z_2 \cdot x_{\phi^2(P)} - X$
return $\mu_n, \mu_{n1}, \mu_{n2}$
```

$$C_{VerLINE} = 3kM$$

Algorithm 5 evaluates $f = f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $g = f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$ at ones using the multifunction technique this saves squarings.

x-superoptimal pairing on BW-13 curve

Algorithm 5: Miller Loop for faster x-superoptimal pairing.

```
Input: $|x| = 2^n + \sum_{i=0}^{n-1} s_i 2^i$, where $s_i \in \{0, -1, 1\}$, $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^k})$
Output: $[x]Q$, the functions $f = f_{|x|,Q}(P) \cdot f_{|x|,Q}^{-1}(\phi^2(P))$ and
        $g = f_{|x|,Q}^{-1}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$.
$(n_f, d_f, n_g, d_g) \leftarrow (1, 1, 1, 1)$; $S \leftarrow Q$
for $i$ from $n-1$ down to $0$ do
    $(\lambda_n, \lambda_{n1}, \lambda_{n2}) \leftarrow l_{S,S}(P)$, $S \leftarrow [2]S$                ▷ DOUBLE LINE
    $(\mu_n, \mu_{n1}, \mu_{n2}) \leftarrow v_S(P)$,                                   ▷ VERTICAL LINE
    $(n_f, d_f) \leftarrow (n_f^2 \lambda_n \mu_{n2}, d_f^2 \mu_n \lambda_{n2})$ , $(n_g, d_g) \leftarrow (n_g^2 \mu_{n2} \lambda_{n1}, d_g^2 \lambda_{n2} \mu_{n1})$ ▷ UPDATE 1
    if $s_i = \pm 1$ then
        $(\lambda_n, \lambda_{n1}, \lambda_{n2}) \leftarrow l_{S,[s_i]Q}(P)$, $S \leftarrow S + [s_i]Q$      ▷ ADDITION LINE
        $(\mu_n, \mu_{n1}, \mu_{n2}) \leftarrow v_S(P)$,                               ▷ VERTICAL LINE
        $(n_f, d_f) \leftarrow (n_f \lambda_n \mu_{n2}, d_f \mu_n \lambda_{n2})$ , $(n_g, d_g) \leftarrow (n_g \mu_{n2} \lambda_{n1}, d_g \lambda_{n2} \mu_{n1})$ ▷
         UPDATE 2
return $f = n_f d_f^{-1}$ and $g = n_g d_g^{-1}$
```

$$
\begin{aligned}
C \quad = \quad & (\log_2(x) - 1)\big(C_{DBLINE} + C_{VerLINE}\big) + (\log_2(x) - 2)C_{UPDATE1} \\
& + (HW_{2-NAF}(x) - 1)\big(C_{ADDLINE} + C_{VerLINE} + C_{UPDATE2}\big). \qquad (8)
\end{aligned}
$$

Cost evaluation of the x-superoptimal pairing on BW-13 curve

- From the seed $x = -2^{11} - 2^7 - 2^5 - 2^4$,
- we compute $f = f_{|x|,Q}(P) \cdot f_{|x|,Q}^{-1}(\phi^2(P))$ and $g = f_{|x|,Q}^{-1}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$
- by executing 10 double line, 10 update1, 3 addition line, 3 update2 and 13 vertical line steps.
- From [DZZZ21], $M_{13} = S_{13} = 66M$ and $I_{13} = 350M + I$. Hence,

$$\begin{aligned} C &= 10[(7M_{13} + 6S_{13} + 4 \times 13M) + (3 \times 13M)] + 9[8M_{13} + 4S_{13}] \\ &\quad + 3[(11M_{13} + 3S_{13}) + (3 \times 13M) + 8M_{13}] \\ &= 21091M. \end{aligned}$$

- The last step consists to compute $(n_f \cdot d_f^{-1})^{-x} \cdot (n_g \cdot d_g^{-1})^p$ at cost of
- 3 multiplications, 2 inversions, 1 p-Frobenius and 1 exponentiation by $-x$ in $\mathbb{F}_{p^{13}}$.
- For the cost of
$$3M_{13} + 2I_{13} + 1F_p + 1E_x = 1834M + 2I.$$
- The total cost of the Miller loop is then $22925M + 2I$.

Table 1 – Comparison. The cost of the Miller loop for the optimal Ate pairing are found in [DZZZ21] for the curve $BW13-P310$. Whereas for the curve $BW19-P286$ we refer to [CDS20] for these costs.

Curve	Pairing	Miller loop
$BW13-P310$	optimal Ate [DZZZ21] superoptimal x-superoptimal	$27074M+2I$ $68871M+3I$ $22925M+2I$
$BW19-P286$	Optimal Ate [CDS20] superoptimal x-superoptimal	$35991M+2I_{19}$ $79657M+3I_{19}$ $21688M+2I_{19}$

Conclusion

We bring out a new variant of the superoptimal pairing (the x-superoptimal pairing) on BW-13 and BW-19 curves by :

- ⋆ reducing certain costly exponents.

To compute the x-superoptimal pairing, we used :

- The idea of Guillevic which consists to evaluate the numerators and the denominators of each double step and addition step separately. This highly reduce the inverse operation.

→ The x-superoptimal pairing constructed is the power of the superoptimal pairing.

→ The Miller loop of the x-superoptimal pairing is about 27.3% and 49% faster than the one of the optimal ate pairing on $BW13 - P310$ and $BW19 - P286$ respectively.

→ The x-superoptimal pairing obtained is then easy for implementation and suitable for ring signature.

Master and PhD programs in Cryptography and Cybersecurity : www.uniba.cm

- Seed Fund : Free University of Bruxelles with Christophe Petit
- Teaching and Projects (Online, Visit to Cameroon....)
- Supervision of Master or PhD Theses
- Talks to our seminar...

IACR Event

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

iacr

Springer

IACR Event

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

i c a r

Springer

IACR Event

Program Chairs
Christophe Petit, ULB
Serge Vaudenay, EPFL

General Chairs
Emmanuel Fouotsa, UBa
Boris Tako Fouotsa, EPFL

IACR Event

Program Chairs
Christophe Petit, ULB
Serge Vaudenay, EPFL

General Chairs
Emmanuel Fouotsa, UBa
Boris Tako Fouotsa, EPFL

AFRICACRYPT 2024
Douala, Cameroon

[CDS20] R. Clarisse, S. Duquesne, and O. Sanders.
Curves with fast computations in the first pairing group.
In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings*, volume 12579 of *Lecture Notes in Computer Science*, pages 280–298. Springer, 2020.

[DZZZ21] Y. Dai, Z. Zhou, F. Zhang, and C. Zhao.
Software implementation of optimal pairings on elliptic curves with odd prime embedding degrees.
IACR Cryptol. ePrint Arch., 1162, 2021.

[FMBZ13] 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.

[Ver10] F. Vercauteren.
Optimal pairings.
IEEE Transactions on Information Theory, 56(1) :455–461, 2010.

Bedankt voor uw aandacht ! ! !