Sparse Multiplication for Pairing with Sextic Twist

Kazuma Ikesaka

Information Security Lab.
Okayama University, Japan

2nd progress meeting
November 28th, 2024

Contents

Contents

Background

- Pairing on Elliptic Curve
  - A map with special properties of bilinear and non-degenerate.
  - Based on the difficulties of solving FFDLP and ECDLP.
  - Enable innovative protocols

    e.g., ID-based cryptography and zk-SNARKs.
  - Efficient pairing implementation is an inseparable topic for practical uses in cryptographic protocols.

Background

- Attacking Methods for Pairing
  - Tower of Number Field Sieve (TNFS)[KB16]
  - Special Tower of Number Field Sieve (STNFS)[BD19]

The resistance against TNFS and STNFS is important.

- [Gui20] list STNFS-secure pairing-friendly curves.
- Elliptic curves with a sextic twist are one of the efficient STNFS-secure pairing-friendly curves.

[KB16] : Taechan Kim and Razvan Barbulescu. "Extended tower number field sieve: A new complexity for the medium prime case". In: *Annual international cryptology conference*. Springer. 2016, pp. 543–571

[BD19] : Razvan Barbulescu and Sylvain Duquesne. "Updating key size estimations for pairings". In: *Journal of cryptology* 32.4 (2019), pp. 1298–1336

[Gui20] : Aurore Guillevic. "A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level". In: *IACR international conference on public-key cryptography*. Springer. 2020, pp. 535–564

Background

- Pairing on Elliptic Curve
  - Carried out by two steps, Miller loop and final exponentiation.

$$e(P,Q) = \underbrace{f(P,Q)}_{\text{Miller loop}}{}^{\overbrace{(p^k-1)/r}^{\text{Final exponentiation}}}$$

- In this work, we aim to reduce the cost for Miller loop.

Background

Our Objective

Reduce the cost for Miller loop for pairing on elliptic curve with sextic twist.

- Elliptic curve with sextic twist is one of the efficient STNFS-secure pairing-friendly curves.
- Construct a new efficient algorithm to compute Miller loop.
- In particular, we focus on constructing a new sparse multiplication.

Contents

Extention Field

- Let p be a prime number and m be a positive integer.
- The finite field $\mathbb{F}_{p^m}$ is an extension field of $\mathbb{F}_p$.
- The extension field $\mathbb{F}_{p^m}$ is defined as follows:

$$\mathbb{F}_{p^m} = \mathbb{F}_p[x]/(f(x)),$$

where $f(x)$ is an irreducible polynomial of degree m over $\mathbb{F}_p$.

Extention Field with $m = 12$

- A tower of extension fields for $m = 12$ is defined as follows:

$$\mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 + 1)$$
$$\mathbb{F}_{p^6} = \mathbb{F}_{p^2}[\beta]/(\beta^3 - (\alpha + 1))$$
$$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[\gamma]/(\gamma^2 - \beta)$$

- The relation between α, β, and γ is as follows:

$$\gamma^6 = \beta^3 = \alpha + 1, \alpha^2 = -1.$$

- Ex. $X \in \mathbb{F}_{p^{12}}$ is represented as follows.

$$X = x_0 + x_1\alpha + x_2\beta + x_3\alpha\beta + x_4\beta^2 + x_5\alpha\beta^2 + x_6\gamma + x_7\gamma\alpha$$
$$+x_8\beta\gamma + x_9\alpha\beta\gamma + x_{10}\beta^2\gamma + x_{11}\alpha\beta^2\gamma, \text{where } x_i \in \mathbb{F}_p.$$

Elliptic Curves on Finite Field

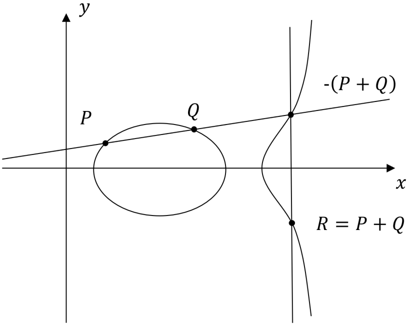
- An elliptic curve over $\mathbb{F}_{p^m}$ is defined as follows:

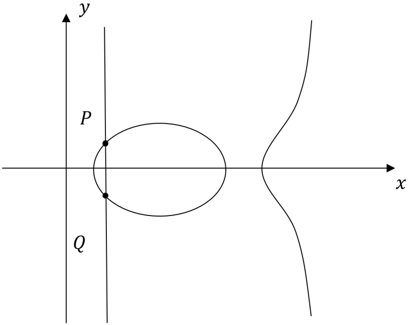
$$E/\mathbb{F}_{p^m} : y^2 = x^3 + ax + b.$$

- Note that a and b are elements over $\mathbb{F}_p$ and they satisfy $4a^3 + 27b^2 \neq 0$.
- A set of rational points $E(\mathbb{F}_{p^m})$ performs an additive group with the infinity point $\mathcal{O}$ as the unity of the group.

Elliptic Curves on Finite Field

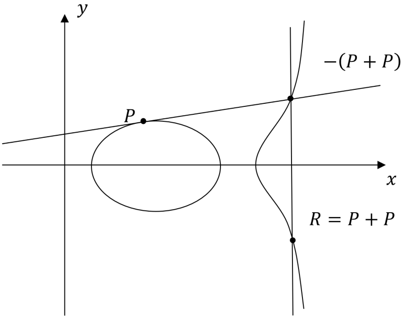
- ECA (Elliptic Curve Addition)

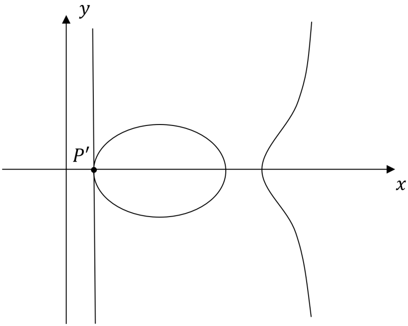




Elliptic Curves on Finite Field

- ECD (Elliptic Curve Doubling)





Elliptic Curves on Finite Field

- For a positive integer s, a point multiplication endomorphism is defined by

$$[s] : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q), P \mapsto P + P + \cdots + P$$

which involves $(s-1)$-times additions.

- Let π_p be the Frobenius endomorphism defined as follows:

$$\pi_p : E \to E : (x, y) \mapsto (x^p, y^p),$$

A Family of Curves

- Parameters of E are given as follows:
  - p : a characteristic of $\mathbb{F}_p$,
  - r : a large prime factor of group order $n = \#E(F_p)$,
  - t : an integer $t = p + 1 - n$, a Frobenius trace of $E(F_p)$,
  - k : the smallest integer satisfying $(p^k - 1)/r$, an embedding degree with respect to r.
- The set of curves specified by the polynomials $p(x), r(x), t(x) \in \mathbb{Q}[x]$ is called a family of curves.

Pairings on Elliptic Curve

- We define base-field and trace-zero subgroup of $E[r]$ defined as follows:

$$\begin{cases} \mathbb{G}_1 & = & E[r] \cap \ker(\pi_p - [1]) \\ \mathbb{G}_2 & = & E[r] \cap \ker(\pi_p - [p]). \end{cases}$$

- Pairing on Elliptic Curve
  - Carried out by two steps, Miller loop and final exponentiation.

$$e(P, Q) = \underbrace{f_{s,Q}(P)}_{\text{Miller loop}}{}^{\overbrace{(p^k - 1)/r}^{\text{Final exponentiation}}} \qquad P \in \mathbb{G}_1, Q \in \mathbb{G}_2$$

- In this work, we focus on Miller loop.

Miller's Algorithm

Alg 1 Miller's algorithm

Input: $s, P \in \mathbb{G}_1, Q \in \mathbb{G}_2$;
Output: $f_{s,Q}(P)$;

$f \leftarrow 1, T \leftarrow Q$;
for $i = \lfloor \log_2(s) \rfloor - 1$ **downto** 1; **do**
  $f \leftarrow f^2 \cdot l_{T,T}(P),\ T \leftarrow [2]T$; ▷ DBL
  if $s[i] = 1$; **then**
    $f \leftarrow f \cdot l_{T,Q}(P),\ T \leftarrow T + Q$; ▷ ADD
  else if $s[i] = -1$; **then**
    $f \leftarrow f \cdot l_{T,-Q}(P),\ T \leftarrow T - Q$; ▷ SUB
return f;

- Let $l_{P,Q}$ be a line function on E, which intersects points $P \in E(\mathbb{F}_p), Q \in E(\mathbb{F}_{p^{12}})$.
- The count of iterations depends on the bit length of $s \in \mathbb{Z}$.

Contents

Sextic Twist

- A sextic twist of E is defined as follows:

$$E' : y^2 = x^3 + bz \mapsto E : y^2 = x^3 + b(z = \alpha + 1,\ \text{QNR, CNR})$$

$$\psi : Q'(x', y') \mapsto Q(z^{\frac{1}{3}}x', z^{\frac{1}{2}}y')$$

$$\psi : Q'(x', y') \mapsto Q((0, x', 0, 0, 0, 0), (0, 0, 0, y', 0, 0))$$

- Note that $Q' \in EF_{p^2}$ and $Q \in EF_{p^{12}}$.

Miller's Algorithm

Alg 2 Miller's algorithm

Input: $s, P \in \mathbb{G}_1, Q' \in \mathbb{G}'_2$;
Output: $f_{s,Q'}(P)$;
$f \leftarrow 1, T \leftarrow Q'$;
for $i = \lfloor \log_2(s) \rfloor - 1$ **downto** 1; **do**
  $f \leftarrow f^2 \cdot l_{T,T}(P),\ T \leftarrow [2]T$; ▷ DBL
  if $s[i] = 1$; **then**
    $f \leftarrow f \cdot l_{T,Q'}(P),\ T \leftarrow T + Q'$; ▷ ADD
  else if $s[i] = -1$; **then**
    $f \leftarrow f \cdot l_{T,-Q'}(P),\ T \leftarrow T - Q'$; ▷ SUB
return f;

- Let $l_{P,Q'}$ be a line function on E', which intersects points $P \in E(\mathbb{F}_p)$, $Q' \in E(\mathbb{F}_{p^2})$.
- The count of iterations depends on the bit length of $s \in \mathbb{Z}$.

Sparse Form

- Thanks to the sextic twist, the result of the line function $l_{P,Q'} \in \mathbb{F}_{p^2}$
- The shape of $l_{P,Q'}$ is as follows:

$$l_{P,Q'}(P) = x_0 + x_3\gamma + x_4\beta\gamma$$

- In other words, it has 7 zero as coefficients, and it is called a 7-sparse form.
- By multiplicating x_0^{-1}, we get following pseudo 8-sparse form:

$$l_{P,Q'}(P) = 1 + a_3\gamma + a_4\beta\gamma$$

Contents

Multiplication of two pseudo 8-sparse elements

- Let a and b be pseudo 8-sparse elements in $\mathbb{F}_{p^{12}}$ as follows:

$$a = 1 + a_3\gamma + a_4\beta\gamma$$

$$b = 1 + b_3\gamma + b_4\beta\gamma$$

- The result of multiplication $c = a \cdot b$ is obtained with following coefficients:

$$c_0 = 1 + (1+\alpha) \cdot a_4 \cdot b_4 \qquad c_3 = a_3 + b_3$$

$$c_1 = a_3 \cdot y_3 \qquad c_4 = a_4 + b_4$$

$$c_2 = a_3 b_4 + a_4 b_3 \qquad c_5 = 0$$

Multiplication of two pseudo 8-sparse elements

- Coefficients of c are obtained by following formulas:

$$t_0 = a_3 \cdot b_3 \qquad c_1 = t_0$$

$$t_1 = a_4 \cdot b_4 \qquad c_2 = s_1 \cdot s_2 - t_0 - t_1$$

$$s_0 = a_3 + a_4 \qquad c_3 = s_1$$

$$s_1 = b_3 + b_4 \qquad c_4 = s_2$$

$$c_0 = 1 + (1 + \alpha) \cdot t_1$$

- As a result, it costs 3 m_2, and its result has 2 zero coefficients.
- Note that m_i is a multiplication in $\mathbb{F}_{p^i}$.

Multiplication of two 2-sparse elements in $\mathbb{F}_{p^{12}}$

- Let a and b be 2-sparse elements in $\mathbb{F}_{p^{12}}$ as follows:

$$a = a_0 + a_1\beta + a_2\beta^2 + a_3\gamma + a_4\beta\gamma \qquad = A_0 + A_1\gamma$$

$$b = b_0 + b_1\beta + b_2\beta^2 + b_3\gamma + b_4\beta\gamma \qquad = B_0 + B_1\gamma$$

- The result of multiplication $c = a \cdot b$ is obtained as follows:

$$c = c_0 + c_1\beta + c_2\beta^2 + c_3\gamma + c_4\beta\gamma + c_5\beta^2\gamma = C_0 + C_1\gamma$$

$$T_0 = A_0 \cdot B_0 \qquad S_1 = B_0 + B_1$$

$$T_1 = A_1 \cdot B_1 \qquad C_0 = T_0 + \beta \cdot T_1$$

$$S_0 = A_0 + A_1 \qquad C_1 = S_0 \cdot S_1 - T_0 - T_1$$

Multiplication of two 2-sparse elements in $\mathbb{F}_{p^{12}}$

- Let a and b be 2-sparse elements in $\mathbb{F}_{p^{12}}$ as follows:

$$a = a_0 + a_1\beta + a_2\beta^2 + a_3\gamma + a_4\beta\gamma \qquad = A_0 + A_1\gamma$$

$$b = b_0 + b_1\beta + b_2\beta^2 + b_3\gamma + b_4\beta\gamma \qquad = B_0 + B_1\gamma$$

- The result of multiplication $c = a \cdot b$ is obtained as follows:

$$c = c_0 + c_1\beta + c_2\beta^2 + c_3\gamma + c_4\beta\gamma + c_5\beta^2\gamma = C_0 + C_1\gamma$$

$T_0 = A_0 \cdot B_0 \leftarrow$ Normal m_6

$T_1 = A_1 \cdot B_1 \leftarrow$ 2-sparse $\times$ 2-sparse

$S_0 = A_0 + A_1$

$S_1 = B_0 + B_1$

$C_0 = T_0 + \beta \cdot T_1$

$C_1 = S_0 \cdot S_1 - T_0 - T_1 \leftarrow$ Normal m_6

Multiplication of two 2-sparse elements in $\mathbb{F}_{p^6}$

- Let a' and b' be 2-sparse elements in $\mathbb{F}_{p^6}$ as follows:

$$a' = a'_0 + a_1\beta$$
$$b' = b'_0 + b_1\beta$$

- The result of multiplication $c' = a' \cdot b'$ is obtained as follows:

$$c' = c'_0 + c'_1\beta + c'_2\beta^2$$

$$t_0 = a_3 \cdot b_3$$
$$t_1 = a_4 \cdot b_4$$
$$s_0 = a_3 + a_4$$
$$s_1 = b_3 + b_4$$

$$c'_0 = t_0$$
$$c'_1 = s_0 \cdot s_1 - t_0 - t_1$$
$$c'_2 = t_1$$

- As a result, it costs 3 m_2.

Multiplication of two 2-sparse elements in $\mathbb{F}_{p^{12}}$

- The result of multiplication $c = a \cdot b$ is obtained as follows:

$$c = c_0 + c_1\beta + c_2\beta^2 + c_3\gamma + c_4\beta\gamma + c_5\beta^2\gamma = C_0 + C_1\gamma$$

$T_0 = A_0 \cdot B_0 \leftarrow$ Normal m_6

$T_1 = A_1 \cdot B_1 \leftarrow$ 2-sparse $\times$ 2-sparse

$S_0 = A_0 + A_1$

$S_1 = B_0 + B_1$

$C_0 = T_0 + \beta \cdot T_1$

$C_1 = S_0 \cdot S_1 - T_0 - T_1 \leftarrow$ Normal m_6

- As a result, it costs 2 m_6 and 3 m_2.

Quick Summary

- The cost for each multiplication is summarized in Table 2.

Table 1: Caluculation cost for each multiplication

Multiplication Type in $\mathbb{F}_{p^{12}}$	Costs
m_{12}	$54m_1$
m_{8s}	$10m_2 = 30m_1$
$m_{8s,8s}$	$3m_2 = 9m_1$
$m_{2s,2s}$	$2m_6 + 3m_2 = 45m_1$

- Note that $m_{is}, m_{is,is}$ are a pseudo i-sparse multiplication and multiplication of two i-sparse form elements.

Applying to Miller's algorithm

- Handle with 4 steps in Miller's algorithm as one set.
  - Store the output of a line function 4 times denoted as l_0, l_1, l_2, l_3.
  - Caluculate $l_0 \cdot l_1$ and $l_2 \cdot l_3 \leftarrow 2m_{8s,8s}$.
  - Caluculate $l_0 \cdot l_1 \cdot l_2 \cdot l_3 \leftarrow m_{2s,2s}$.
  - Malutiply $l_0 \cdot l_1 \cdot l_2 \cdot l_3$ to $f \leftarrow m_{12}$.
- In total, our proposed method costs $2m_{8s,8s} + m_{2s,2s} + m_{12} = 117m_1$ to multiply 4 line function results.

Comparsion with Previous Work

- If we apply pesudo 8-sparse multiplication to Miller's algorithm naively, the cost is $4m_{8s} = 120$.

Table 2: Caluculation cost to multiply 4 line function results

	Costs
Previous One	$117m_1$
Our Proposal	$120m_1$

Contents

Conclusion

- We proposed a new efficient algorithm to compute Miller loop for pairing on elliptic curve with sextic twist.
- In particular, we focused on constructing a new sparse multiplication with embedding degree 12.
- Our proposed method costs $117m_1$ to multiply 4 line function results and $3m_1$ are reduced from previous algorithm.

Future Works

- Implemant the proposed method and evaluate the performance.
- Apply the strategy to quadratic twist.
- Apply our proposed method to higher embedding degree.