基于并发架构的SM9算法高效实现.

10.14.

Multiplication embedding:

- $X_{\mathbb{F}_q}$ be a curve.
- $Q \in X$ of degree m.
- $G = P_1 + \cdots + P_n$.
- D a divisor.

$$\mathbb{F}_{q^k} = \mathbb{F}_q[x]_{\leq k-1} \xrightarrow{\{x_1 \cdots x_n\}} \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]_{2k-2} \mapsto g(\alpha) =$$

$$\alpha = f_\alpha(\omega) \qquad a_i = f_\alpha \cdot f_\beta(P_i) \qquad \sum \prod_{j \neq i} \frac{x - x_i}{x_j - x_i} a_i$$

$$\beta = f_\beta(\omega) \qquad (a_1, \ldots, a_n) \qquad \| \; g(x)$$

$$\mathbb{F}_{q^k} \xrightarrow{\psi} \mathbb{F}_q^{2k-2} \xrightarrow{\phi} \mathbb{F}_{q^k}$$

$$\alpha \mapsto f_\alpha(x) \mapsto \vec{a} = (f_\alpha(x_1) \cdots f_\alpha(x_n)) \mapsto f_\alpha(x) \mapsto f_\alpha(\omega)$$

$$\alpha \cdot \beta \mapsto f_\alpha \cdot f_\beta \mapsto \vec{ab} \mapsto f_{ab}(x) \mapsto f_{ab} = f_\alpha \cdot f_\beta(\omega)$$

$$n \geq 2k-2$$

$$\phi(\psi(\alpha) * \psi(\beta)) = \alpha \cdot \beta$$

Newton interpolation:

$\mathbb{F}_{p^{12}}$:

$\mathbb{F}_{p^2} = \mathbb{F}_p(u)$. $u^2+2=0$

$\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(v)$. $v^2-u=0$

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^4}(w)$. $w^3-v=0$.

$\mathbb{F}_{p^2} = \mathbb{F}_p(u)$. $u^2+5=0$

$\mathbb{F}_{p^6} = \mathbb{F}_{p^2}(v)$. $v^3-u=0$

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}(w)$ $w^2-v=0$

$f^{\frac{p^{12}-1}{r}} = f^{p^6-1} \cdot \frac{p^6+1}{r}$

$m = f^{p^6-1}$, $m^{p^6+1} = 1 \Rightarrow m^{p^6} = \bar{m} = m^{-1}$.

R-ate Pairing: (优化一，点加的顺序)

- $E: y^2 = x^3 + b$ defined over $\mathbb{F}_p$

  $E': y^2 = x^3 + \beta b$, $\beta \in \mathbb{F}_{p^2}$, $\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$

  since $(\beta^{-1/3}x)^3 + b = \beta^{-1}x^3 + b = \beta^{-1}(x^3 + \beta b) = (\beta^{-1/2}y)^2$

Then $\varphi: E' \longrightarrow E$; $(x, y) \longmapsto (\beta^{-1/3}x, \beta^{-1/2}y)$ d.o. $\mathbb{F}_{p^{12}}$

$\hat{\varphi}: E \to E'$; $(x, y) \mapsto (\beta^{1/3}x, \beta^{1/2}y)$ $(\beta^{1/3}x_Q \quad \beta^{1/2}y_Q)$

R-ate Pairing: $R_{6t+2}(P, Q) = \left[f_{6t+2, Q}(P) \cdot l_{(6t+2)Q, \pi_p(Q)}(P) \cdot l_{(6t+2)Q + \pi_p(Q), -\pi_{p^2}(Q)}(P) \right]^{\frac{p^{12}-1}{r}}$

Input: $P \in E(\mathbb{F}_p)$, $Q \in E'(\mathbb{F}_{p^2})$

Output: $f \in \mathbb{F}_{p^{12}}$

① $6t+2 = a = \sum_{i=0}^{l} a_i \cdot 2^i$, $a_l = 1$

② $Q = \varphi(Q')$, $T = Q'$, $f = 1$ $T/\mathbb{F}_{p^2}$

③ Loop for $i = l-1$ to 0 do

{ 1) $f = f^2 \cdot g_{T,T}(P)$, $T = [2]T$

2) if $a_i = 1$, $f = f \cdot g_{T,Q}(P)$, $T = T + Q$

④ $Q_1 = \pi_p(Q)$, $Q_2 = \pi_{p^2}(Q)$ compute

1) $f = f \cdot g_{T,Q_1}(P)$, $T = T + Q_1$

2) $f = f \cdot g_{T,Q_2}(P)$, $T = T + Q_2$

⑤ output: $f^{\frac{p^{12}-1}{r}}$

② $T' = Q'$, $Q = \varphi(Q')$

③ loop

1) $T = \varphi(T')$ $f = f^2 \cdot g_{T,T}(P)$ $T = [2]T'$

2) if $a_i = 1$, $T = \varphi(T')$, $f = f \cdot g_{T,Q}(P)$, $T' = T + Q'$ $\mathbb{F}_{p^2}$

④ $Q_1 = \pi_p(Q)$, $Q_2 = \pi_{p^2}(Q)$ $T = \varphi(T')$

1) the same

2)

优化 1.1 (加减法)

Optimal Ate Pairing on BN-curves

Input: $P \in G_1$, $Q \in G_2$

Output: $a_{opt}(Q, P)$ $\quad \psi(Q') = Q$, $Q' \in E'(\mathbb{F}_{p^2})[r]$

Write $s = 6t+2 = \sum_{i=0}^{l-1} s_i \cdot 2^i$, $s_i \in \{-1, 0, 1\}$

$T = Q$, $f = 1$

for $i = l-2$ to 0 do

$f = f^2 \cdot l_{T,T}(P)$, $T = 2T$

if $s_i = -1$ then

$f = f \cdot l_{T,-Q}(P)$; $T = T - Q$

else if $s_i = 1$ then

$f = f \cdot l_{T,Q}(P)$; $T = T + Q$

end if

end for

$Q_1 = \pi_p(Q)$; $Q_2 = \pi_{p^2}(Q)$

$f = f \cdot l_{T,Q_1}(P)$; $T = T + Q_1$

$f = f \cdot l_{T,-Q_2}(P)$, $T = T - Q_2$

return $f^{\frac{p^{12}-1}{r}}$

$T' = Q'$, $f = 1$

$T = \psi(T')$

$f = f^2 \cdot l_{T,T}(P)$, $T' = 2T'$

if $s_i = -1$ then

$T = \psi(T')$

$f = f \cdot l_{T,Q}(P)$ $T' = T' + Q'$

end if

end for

$Q_1 = \pi_p(Q)$ $Q_2 = \pi_{p^2}(Q)$, $T = \psi(T')$

$f = f \cdot l_{T,Q_1}(P)$ $T = T + Q_1$

$f = f \cdot l_{T,-Q_2}(P)$ $T = T - Q_2$

$V/\mathbb{F}_{p^2}$ $x^2 - u = 0$ $\quad u \in \mathbb{F}_{p^2}$ $\quad u^{p^2} = u$, $u^p \neq u$

V^{p^2} $\quad (V^{p^2})^2 - u = (V^2 - u)^{p^2}$

$V^p / \mathbb{F}_p$ $\quad x^2 = u$, $x^4 = u^2 = -2$, $x^4 + 2 = 0$

V, V^p, V^{p^2}, V^{p^3}, $V^{p^4} = V$

$V \cdot V^{\frac{p-1}{2}}$

$(-2)^{\frac{1}{4}} \cdot \pm 1$

$(-1)^{\frac{1}{2}} = u^{\frac{p-1}{2}}$

$u^{p-1} = -1$

$u^p = -u$

优化二：模幂运算：

$$f^{\frac{p^{12}-1}{r}} = f^{\frac{(p^6-1)(p^6+1)}{r}} = f^{\frac{(p^6-1)(p^2+1)(p^4-p^2+1)}{r}}$$

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}(v)$

$$\begin{cases} m = f^{p^6-1} \\ s = m^{p^2+1} \\ \vdots \\ z = s^{\frac{p^4-p^2+1}{r}} \end{cases} \checkmark$$

$\mathbb{F}_{p^{12}}$

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}(u)$, $u^2+2=0$ 2

$\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(v)$, $v^2-u=0$ 2

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^4}(w)$, $w^3-v=0$ 3

$\mathbb{F}_p$ ↓ $\mathbb{F}_{p^2}$

$m^{p^6+1} = 1 \Rightarrow \bar{m} = m^{-1}$ $\left(s^{-1} = (m^{-1})^{(p^2+1)} = m^{p^6 \cdot (p^2+1)} \right)$

$\mathbb{F}_{p^2} = \mathbb{F}_p(u)$ $(a+bu)^p = a^p + b^p u^p = a - bu = \overline{a+bu}$ ✓

$\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(v)$ $(c+dv)^{p^2} = c + dv^{p^2} = c - dv = \overline{c+dv}$

$$(c+dv)^p = c^p + d^p v^p = \bar{c} + \bar{d} \cdot v \cdot (-1)^{\frac{p-1}{2}} = \bar{c} + \bar{d} \cdot u^{\frac{p-1}{2}} \cdot v$$

$$= \bar{c} + \bar{d} (u^{\frac{p-1}{6}})^3 v$$

$fr = u^{\frac{p-1}{6}}$ $(u^{p-1} = -1)$

$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^4}(w)$:

$$(e+fw+gw^2)^p = e^p + f^p w^p + g^p (w^p)^2$$

$$= e^p + f^p \cdot fr \cdot w + g^p \cdot fr^2 \cdot w^2 \checkmark \quad fr = u^{\frac{p-1}{6}}$$

① $m = f^{p^6-1} = f^{p^6} \cdot f^{-1} = \bar{f} \cdot f^{-1}$

② $s = m^{p^2} \cdot m = (m^p)^p \cdot m$, moreover $m^{-1} = \bar{m} = m^{p^6}$

③ assume $\frac{p^4-p^2+1}{r} = \lambda_3(t) \cdot p^3 + \lambda_2(t) \cdot p^2 + \lambda_1(t) \cdot p^1 + \lambda_0(t)$

then $\lambda_3 = 1$, $\lambda_2 = 6t^2+1$, $\lambda_1 = -36t^3-18t^2-12t+1$, $\lambda_0 = -36t^3-30t^2-18t-2$

$$s^{\frac{p^4-p^2+1}{r}} = s^{p^3+\lambda_2 p^2+\lambda_1 p^1+\lambda_0}$$

hard-part $= s^{p^3} \cdot s^{6t^2 \cdot p^2 + p^2} \cdot s^{-36t^3 \cdot p - 18t^2 \cdot p - 12t \cdot p + p} \cdot s^{-36t^3-30t^2-18t-2}$

$$= s^{p^3} \cdot s^{p^2} \cdot s^{p} \cdot (s^{-1})^2 \cdot \left[(s^{t^2})^{p^2}\right]^6 \cdot \left[(s^{-1})^{36t^3}\right]^p \cdot \left[(s^{-1})^{18t^2}\right]^p \cdot (s^{-1})^{12tp}$$

$$\cdot (s^{-1})^{36t^3} \cdot (s^{-1})^{30t^2} \cdot (s^{-1})^{18t}$$

□

优化3. 预计算与存储.

f^r

$r = R^7 \| R^6 \| \cdots \| R^0$, R^i 为 32bit. $i \in \{0, \cdots, 7\}$ $32 \times 8 = 256$ bits

R^7	R_{31}^7	R_{30}^7	$\cdots$	R_0^7 $\in 2^{224}$
R^6	R_{31}^6	R_{30}^6	$\cdots$	R_0^6 $\in 2^{6\cdot 32}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
R^0	R_{31}^0	R_{30}^0		R_0^0 $\in 1 \sim 2^{32}$

$a_{31}^7 \quad \cdots \quad a_0^7 \to a_7$

$\vdots$

$a_{31}^1 \quad \cdots \quad a_1^0 \to a_1$

$a_{31}^0 \quad \cdots \quad a_0^0 \to a_0$

$a = (a_0 \cdots a_7)$ $a_i \in \{0,1\}$ $r_0 2^0 + r_1 \cdot 2^{32} + r_2 \cdot 2^{32\cdot 2} + \cdots + r_7 2^{32\cdot 7}$

$256 = 32 \cdot 8 = 2^5 \cdot 2^3 = 2^8$

$$g^r = g^{\left[R_{31}^7 \cdot 2^{255} + R_{30}^7 \cdot 2^{254} + \cdots + R_0^7 \cdot 2^{224} + R_{31}^6 \cdot 2^{223} + R_{30}^6 \cdot 2^{232} + \cdots + R_0^6 \cdot 2^{192} + \cdots + R_{31}^1 \cdot 2^{63} + R_{30}^1 \cdot 2^{63} + \cdots + R_0^1 \cdot 2^{32} + R_{31}^0 \cdot 2^{31} + R_{30}^0 \cdot 2^{30} + \cdots + R_0^0 \cdot 1\right]}$$

$i = 31$ to 0

$w = w^2$

$\vec{R_i} = a$, $g^a = g^{a_7 \cdot 2^{224} + \cdots + a_0}$

$w = g \cdot w$

g_{31}

$\xleftarrow{2}$

$g_{31}^2 \cdot g_{30}$

$\xleftarrow{2}$

$g_{31}^4 \cdot g_{30}^2 \cdot g_{29}$

$\xleftarrow{\cdots}$

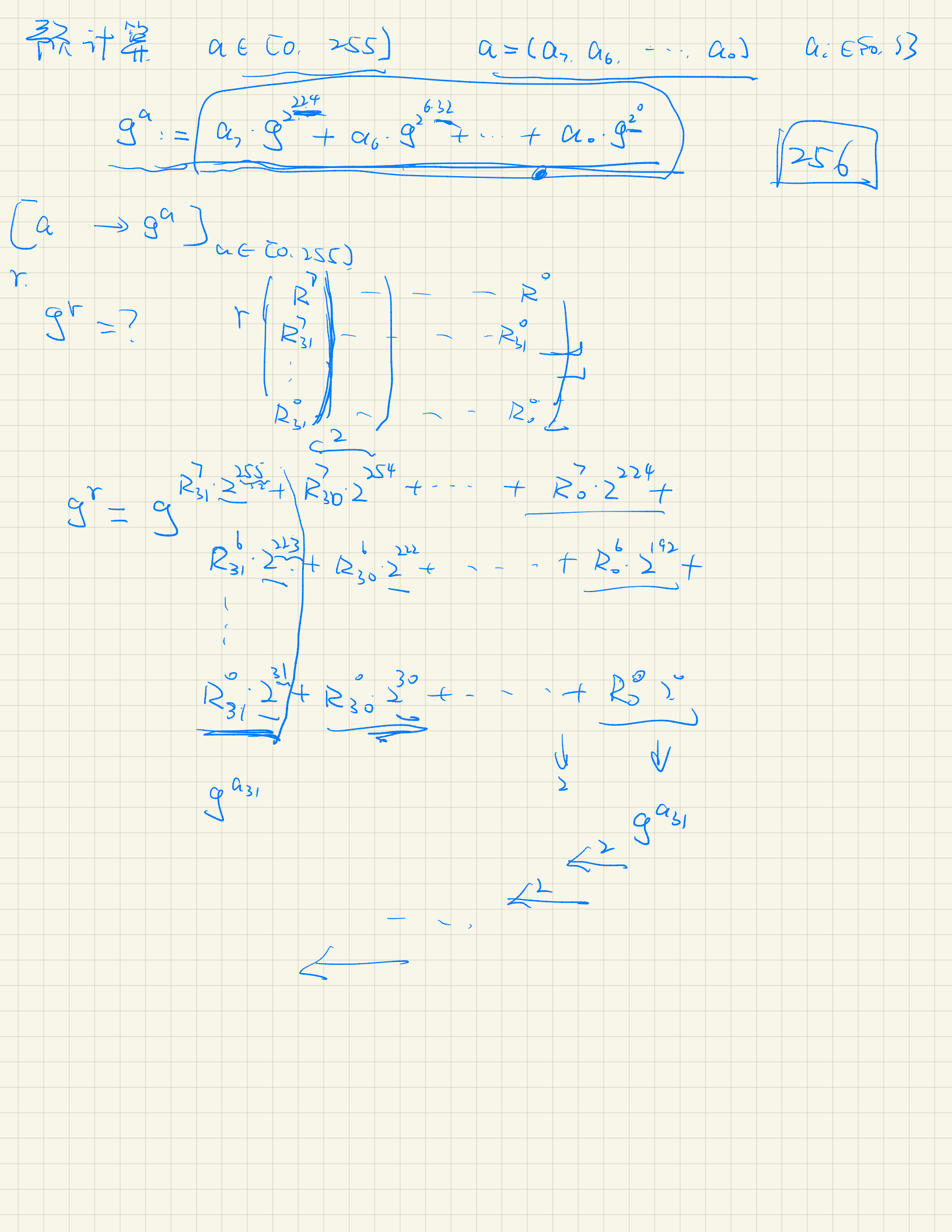
$g_{31}^{31} \quad g_{30}^{30} \quad \cdots \quad g_1 \quad g_0$

预计算 & 存储.

g^a $a \in [0, 2^{256}]$

all

$a_7 g^{2^{224}} + \cdots + a_0 g^2$


累计算
$a \in [0, 255]$
$a = (a_7, a_6, \cdots, a_0)$
$a_i \in \{0, 1\}$
$g^a := a_7 \cdot g^{2^{224}} + a_6 \cdot g^{2^{192}} + \cdots + a_0 \cdot g^{2^0}$
256
$[a \to g^a]_{a \in [0, 255]}$
r.
$g^r = ?$
$r = (R_{31}^7 \| \cdots \| R_0^7, \cdots, R_{31}^0 \| \cdots \| R_0^0)$
2
$g^r = g^{R_{31}^7 \cdot 2^{255} + R_{30}^7 \cdot 2^{254} + \cdots + R_0^7 \cdot 2^{224} +}$
$R_{31}^6 \cdot 2^{223} + R_{30}^6 \cdot 2^{222} + \cdots + R_0^6 \cdot 2^{192} +$
$R_{31}^0 \cdot 2^{31} + R_{30}^0 \cdot 2^{30} + \cdots + R_0^0 \cdot 2^0$
$g^{a_{31}}$
2
$g^{a_{31}}$
2
2

2022.10.1.

主题：例会讨论.

1. 对 SM9 相关理论和代码的了解程度

① 程序实现：C语言 库的调用.

高并发特点指的是什么？应该怎么利用.

② 理论部分：加速 Miller 算法.

- 1.2.1. Miller 生成次数.
- 1.2.2. 配对友好型曲线的选择
- 1.2.3. 有限域上运算的加速.

- t 的选取
- 6t+2 → 生成次数 ← 每一步的有限域操作. (eg: doub. p, ...)
- 有限域 F_{p^n} 上的运算
- 高阶模乘次数.

2. 下一阶段的安排. 10.26 ~ 10.28.

会后讨论 (10.8)：寻找突破点

10.13 } 解决
10.20 }
10.25 } 文档整理.

Content: 2022.09.28.

① Elliptic curve over finite field.

② Pairings: Weil Pairing
Tate Pairing
Ate Pairing
R-ate pairing.

- $\mathbb{F}_p$: finite prime field of characteristic p
- $\mathbb{F}_{p^m} := \mathbb{F}_p[x]/(f(x))$ $\deg f = m$ & f is irr. over $\mathbb{F}_p[x]$
- Elliptic curve E defined over $\mathbb{F}_{p^m}$:

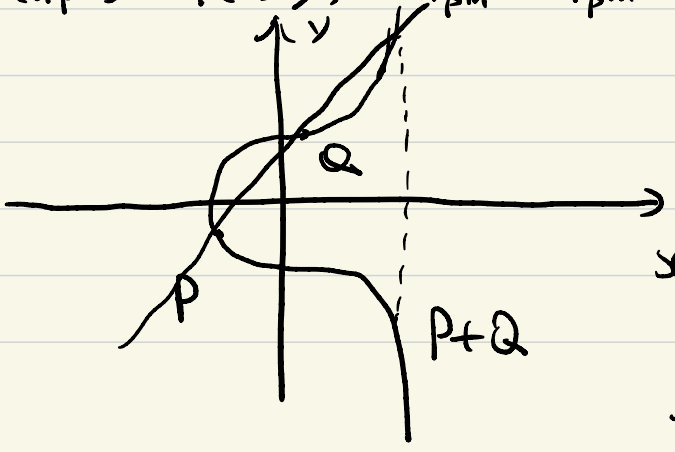
E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_1 \cdots a_6 \in \mathbb{F}_{p^m}$

NON-singular: $\begin{cases} \frac{\partial f(x,y)}{\partial x} = 0 \\ \frac{\partial f(x,y)}{\partial y} = 0 \\ f(x,y) = 0 \end{cases}$ has no solutions in $\overline{\mathbb{F}}_p^2$

Short Weistrass form: ($p \geq 5$)

$y^2 = x^3 + ax + b$ $\quad \Delta = 27b^2 + 4a^3 \neq 0$

$E(\mathbb{F}_{p^m}) = \{(x,y) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$



$(E(\mathbb{F}_{p^m}), +)$ is a finite group

$\#E(\mathbb{F}_{p^m}) = |E(\mathbb{F}_{p^m})|$

$= p^m + 1 - t$ $\quad |t| \leq 2p^{m/2}$

$t = tr(\pi)$, $\pi : \overline{E} \to \overline{E}$, $(x,y) \mapsto (x^{p^m}, y^{p^m})$

Point addition formula:

$P=(x_P, y_P)$ $Q=(x_Q, y_Q)$ $P+Q=(x_{P+Q}, y_{P+Q})$

If $P \neq Q$ & $Q=-P$

$$\begin{cases} y-y_P = \frac{y_Q-y_P}{x_Q-x_P}(x-x_P) = \lambda(x-x_P) \\ y^2 = x^3+ax+b \end{cases} \Rightarrow \begin{cases} x_3 = \lambda^2 - x_P - x_Q \\ y_3 = \lambda(x_P - x_3) - y_P \end{cases}$$

If $P=Q$

$$\begin{cases} y-y_P = \frac{3x_P^2+a}{2y_P}(x-x_P) = \lambda(x-x_P) \\ y^2 = x^3+ax+b \end{cases} \Rightarrow \begin{cases} x_3 = \lambda^2 - 2x_1 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

Scalar multiplication (多倍点) $[u]P$

$u = \sum_{i=0}^{\ell-1} u_i \cdot 2^i$, $u_i \in \{0,1\}$ $[u]P = \sum_{i=0}^{\ell-1} [u_i 2^i]P$

Input: P, u

Output: $Q=[u]P$

a) $Q=O=\infty$

b) for $j=\ell-1$ to 0

1) $Q=2Q$

2) $u_j=1$ $Q=Q+P$

c) output Q

$= [2^{\ell-1}]P + [u_{\ell-2}2^{\ell-2}]P + \cdots + [u_0]P$

$= 2^{\ell-2}(2P + u_{\ell-2}P) + u_{\ell-3}2^{\ell-3}$

$= 2^{\ell-3}(\quad)$

$Q_j^e = 2Q_j^s + u_j P$

$Q_0^e = 2Q_0^s + u_0 P$

$= 2(2Q_1^s + u_1 P) + u_0 P$

$= 2(2(2Q_2^s + u_2 P) + u_1 P) + u_0 P$

$= 2(\cdots 2(2Q_{\ell-1}^s + u_{\ell-1}P)\cdots + u_1 P) + u_0 P$

$= P + u_{\ell-2}$

Extended algorithm:

加减法 \ 滑动窗口法

order $= N$

[Pairing] $e : (G_1, +) \times (G_2, +) \longrightarrow (G_t, \cdot)$

$$\begin{cases} e(aP, bQ) = e(P, Q)^{ab} \\ e(P, Q) \neq 1 \\ \text{efficient computation.} \end{cases}$$

Preliminaries:

Divisors: $\mathrm{Div}(E) = \{ \sum_{P_i \in E(\bar{F}_q)} a_i (P_i) \mid \text{all but finitely many } a_i = 0 \}$

$$\sum a_i (P_i) + \sum b_i (P_i) = \sum (a_i + b_i)(P)$$

$\Rightarrow (\mathrm{Div}(E), +)$ is a group.

$\deg(D) = \sum a_i < +\infty$ $\quad \mathrm{Div}^0(E) = \{ D \mid \deg(D) = 0 \}$

divisors of a function: $\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P)$ [Principal divisor.]

then $\deg(\mathrm{div}(f)) = 0$.

a divisor $D = \sum a_i (P_i)$ is a Principal divisor iff $\begin{cases} \sum a_i = 0 \\ \sum [a_i] P_i = \infty \end{cases}$

Specially, assume $P, Q \in E[N] := \{ R \in E(\bar{F}_q) \mid [N]R = \infty \}$

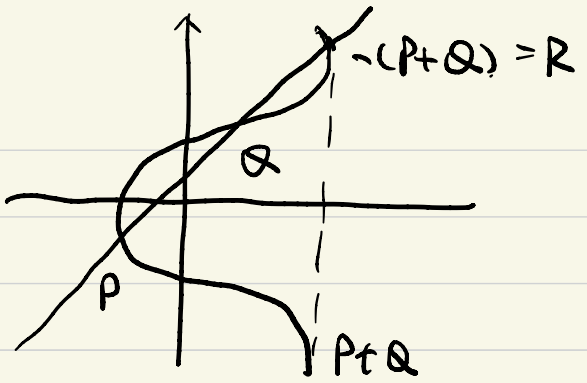
then $D = N(P) - N(\infty)$ is a Principal divisor.

We assume $\mathrm{div}(f_P) = N(P) - N(\infty) \sim N(P) - ([N]P) - (N-1)(\infty)$

$\mathrm{div}(f_Q) = N(Q) - N(\infty)$

(0:1:0)

An example



$x = a$

$Y - Y_P Z = \lambda (X - X_P Z)$

$(0:1:0)$

$f = y - y_P - \lambda(x - x_P)$ $\quad$ $div(f) = (P) + (Q) + (R) - 3(\infty)$

$f(P) = f(Q) = f(R) = 0$ $\quad$ $f(S) = Y_S - Y_P - \lambda(X_S - X_P)$

Weil Pairing: Let $G_1 \leq E(\mathbb{F}_q)[N]$ be a subgroup of order N.

$e_N : G \times G \longrightarrow \mu_N = \langle \zeta_N \rangle \subseteq \mathbb{F}_{q^k}^*$. k: embedding degree

$N \mid q^k - 1$

$$e_N(P, Q) = \frac{f_P(Q+S) \,/\, f_P(S)}{f_Q(P-S) \,/\, f_Q(-S)}$$ For any $S \in E(\mathbb{F}_q) \setminus \langle P \rangle$.

How to compute f_P or f_Q ?

$\frac{f_P(DQ+S)}{f_P(S)}$

Let $h_{P,Q} = \begin{cases} \dfrac{Y - Y_P - \lambda(X - X_P)}{X + X_P + x_Q - \lambda^2 - a_1\lambda - a_2}, & \lambda \neq \infty \\ X - X_P, & \lambda = \infty \end{cases}$

$\frac{g_{P,Q}}{g_{P+Q}}$

$div(h_{P,Q}) = (P) + (Q) + (R) - 3(\infty) - (R) - (P+Q) + 2(\infty)$

$= (P) + (Q) - (P+Q) - (\infty)$

Miller algorithm: $N = \varepsilon_0 + \varepsilon_1 \cdot 2 + \varepsilon_2 \cdot 2^2 + \cdots + \varepsilon_t \cdot 2^t$.

(1) Set $T = P$ and $f = 1$

(2) loop $i = t-1$ to 0.

Set $f = f^2 \cdot h_{T,T}$

Set $T = 2T$

If $\varepsilon_i = 1$

Set $f = f \cdot h_{T,P}$

Set $T = T + P$

End if

End loop.

$h_{V,V} = \frac{g_{V,V}}{g_{2V}}$

$f = f^2 \cdot \frac{g_{V,V}}{g_{2V}}$

$\varepsilon_i = 1$ $\quad h_{T,P} = \frac{g_{T,P}}{g_{T+P}}$

$f =$

(3) Return f. $T = [N]P$

Proof: [$f = f_p$] $\quad div(h_{T,T}) = 2(T) - (2T) - (\infty)$

$div(h_{T,P}) = (T) + (P) - (T+P) - (\infty)$

$T_i^{end} = 2T_i^s + \varepsilon_i P$

$f_i^{end} = (f_i^s)^2 \cdot h_{T_i^s, T_i^s} \cdot h_{2T_i^s, P}^{\varepsilon_i}$

$\Rightarrow div(f_i^{end}) = 2\, div(f_i^s) + div(h_{T_i^s, T_i^s}) + \varepsilon_i\, div(h_{2T_i^s, P})$

$= 2div(f_i^s) + 2(T_i^s) - (2T_i^s) - (\infty) + \varepsilon_i [(2T_i^s) + (P) - (2T_i^s + P) - (\infty)]$

$= 2div(f_i^s) + 2(T_i^s) - (T_i^{end}) + \varepsilon_i (P) - (1+\varepsilon_i)(\infty)$

$\Rightarrow div(f_{i+1}^s) = 2div(f_i^s) + 2(T_i^s) - (T_{i+1}^s) + \varepsilon_i (P) - (1+\varepsilon_i)(\infty)$

$\Rightarrow div(f_{i-1}^s) - 2div(f_i^s) = 2(T_i^s) - (T_{i-1}^s) + \varepsilon_i (P) - (1+\varepsilon_i)(\infty)$

$T_{i-1}^S - 2T_i^S = \varepsilon_i P$

$= T_{-1}^S = 2T_0^S + \varepsilon_0 P$

$= \varepsilon_0 P + 2T_0^S - 2^2 T_1^S + 2^2 T_1^S - 2^3 T_2^S + \cdots + 2^{t+1} T_{t+1}^S - 2^{t+1} T_{t+1}^S$

$\Rightarrow T_0^{end} = \varepsilon_0 P + 2T_1^S = \varepsilon_0 P + \left\{ \sum_{i=1}^{t+1} 2^i (T_{i-1}^S - 2T_i^S) + 2^{t+1} T_{t+1}^S \right.$

$= \varepsilon_0 P + \sum_{i=1}^{t+1} 2^i \cdot \varepsilon_i P + 2^{t+1} \cdot T_{t+1}^S \quad (T_{t+1} = P \quad \varepsilon_{t+1} = 1)$

$= \sum_{i=0}^{t+1} 2^i \varepsilon_i P = [N]P$

$dN(f_0^{end}) = 2\, dN(f_0^S) + 2(T_0^S) - (T_0^{end}) + \varepsilon_0(P) - (1+\varepsilon_0)(\infty)$

$= \left[\sum_{i=1}^{t+1} 2^i \left(dN(f_{i-1}^S) - 2\, dN(f_i^S) \right) \right] + 2(T_0^S) - (NP)$

$+ \varepsilon_0 P - (1+\varepsilon_0)(\infty)$

$= \left[\sum_{i=1}^{t+1} 2^i \left(2(T_{i-1}^S) - (T_{i-1}^S) + \varepsilon_i(P) - (1+\varepsilon_i)(\infty) \right) \right]$

$+ 2(T_0^S) - (NP) + \varepsilon_0(P) - (1+\varepsilon_0)(\infty)$

$= 2^{t+1}(T_{t+1}^S) + \sum_{i=0}^{t+1} 2^i \varepsilon_i(P) - \sum_{i=0}^{t+1} 2^i (1+\varepsilon_i)(\infty) - (NP)$

$= N(P) - (N-1)(\infty) - (NP)$

$h_{T,T} = \frac{g_{T,T}}{g_{2T}}$

$h_{T,P} = \frac{g_{T,P}}{g_{T+P}}$

Tate-Pairing:

$div(f_P) = N(P) - ([N-1]P) - N(\infty)$ $\quad f_P^r = f_P$

$div(f_P^r) = N(P) - ([N-1]P) - N(\infty) = div(f_P^r)$

$G_1 = E(\mathbb{F}_q)[r]$, $G_2 = \langle Q \rangle \subseteq E(\mathbb{F}_{q^k})[r]$, $G_3 = \mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^N$

$e: G_1 \times G_2 \to \mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^N$ $\xrightarrow{(\cdot)^{\frac{q^k-1}{N}}}$ μ_N

$(P, Q) \mapsto e(P, Q) = \dfrac{f_{P,N}(Q+U)}{f_{P,N}(U)}$ mod $(\mathbb{F}_{q^k}^*)^N$

$\forall\, U \in E(\mathbb{F}_{q^k})$

$P \neq Q + U$

$U \neq -\infty$.

$div(f_P') = N(R+P) - N(R) - r(R)$

$R \notin \{P, \infty\}$

Reduced tate Pairing $e(P,Q) = f_{P,N}(Q)^{\frac{q^k-1}{N}}$

$= \left(\dfrac{f_{P,N}(Q)}{f_{P,N}'(\infty)}\right)^{\frac{q^k-1}{N}} = (f_{P,N}'(Q))^{\frac{q^k-1}{N}}$

Ate-pairing:

Notations: $\pi_q: E \to E;\ (x, y) \mapsto (x^q, y^q)$

$\hat{\pi}_q$

then $\hat{\pi}_q \circ \pi_q = [q]$

$\pi_q \cdot \hat{\pi}_q$: $x^2 - tx + [q] = 0 \mod r$

$= (x-1)(x-q)$

$\hat{\pi}_q + \pi_q = t$

$G_2 \times G_1 \to$ Ate Pairing: $G_1 = E[r] \cap \ker(\pi_q - 1) \subseteq E(\mathbb{F}_q)$

$G_2 = E[r] \cap \ker(\pi_q - [q]) \subseteq E(\mathbb{F}_{q^k})$

Ate: $G_2 \times G_1 \to \mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^r$

$(Q, P) \mapsto f_{Q, t-1}(P)^{\frac{q^k-1}{r}}$

$G_1 \times G_2$ — Ate Pairing. something similarly.

R-ate "R" for ratio.

$P, Q \in E(\mathbb{F}_{q^k})[r]$. $A = aB + b$

$$R_{A,B}(P,Q) = f_{aB,P}(Q)\, f_{b,P}(Q) \cdot g_{[aB]P,\,[b]P}(Q)$$

$$\tilde{e}(P,Q)^{L_1} = f_{A,P}(Q)^{M_1}$$

$$\tilde{e}(P,Q)^{L_2} = f_{B,P}(Q)^{M_2}$$

$M = \mathrm{lcm}(M_1, M_2)$. $M = d_1 M_1 = d_2 M_2$ $L = d_1 L_1 - a d_2 L_2$.

If $r \mid L$. R-ate is nondegenerate and

$$\tilde{e}(P,Q)^{L} = R_{A,B}(P,Q)^{M}$$

一生代价为 $\log(r^{1/\varphi(k)})$

$\frac{g_{[aB]Q,\,[b]Q} - f_{[aB]Q} + f_{[b]Q} + (\infty)}{g_{[A]Q}}$

$A = aB + b$

$$\mathrm{div}(f_{Q,A}) = \mathrm{div}(f_{Q,aB+b}) = (aB+b)(Q) - ([aB+b]Q) - (aB+b-1)(\infty)$$

$$= (aB)Q + b(Q) - ([aB]Q) - (aB-1)\infty + ([b]Q) - (b-1)\infty$$

$$= \mathrm{div}(f_{Q,aB}) + \mathrm{div}(f_{Q,b}) + \mathrm{div}(g_{[aB]Q,\,[b]P}) - \mathrm{div}(g_{[A]Q})$$

$$= \mathrm{div}(f_{Q,B}^{a}) + \mathrm{div}(f_{[B]Q,a}) + \mathrm{div}(f_{Q,b}) + \mathrm{div}(g_{[aB]Q,\,[b]P}) - \cdots$$

$\Rightarrow$

$$f_{Q,A}(P) = \frac{f_{Q,B}^{a}(P) \cdot f_{[B]Q,a}(P) \cdot f_{Q,b}(P) \cdot g_{[aB]Q,\,[b]P}(P)}{g_{[A]Q}(P)}$$

$\frac{q^k - 1}{r}$

$$R_{A,B}(P,Q) := \left(\frac{f_{Q,A}(P)}{f_{Q,B}^{a}(P)}\right)^{\frac{q^k-1}{r}} = \left[\frac{f_{[B]Q,a}(P) \cdot f_{Q,b}(P) \cdot g_{[aB]Q,\,[b]P}(P)}{g_{[A]Q}(P)}\right]^{\frac{q^k-1}{r}}$$

$f_{Q,a}(P)$ ·

Not for all (A, B), $R_{A,B}$ is non-degenerate.

If $(f_{Q,A}(P))^{\frac{q^k-1}{r}\cdot M_1} = e_r(Q,P)$

$(f_{Q,B}(P))^{\frac{q^k-1}{r}\cdot M_2} = e_r(Q,P)$

Let $M = \mathrm{lcm}(M_1, M_2)$. $m = \frac{M}{M_1}\cdot L_1 - \frac{M}{M_2}\cdot L_2 \cdot a$ $(r \nmid m)$

then $e_r^m(Q,B) = R_{A,B}(Q,P)^M$

Four cases of (A, B)

(SM9. R-ate.) ✓

BN-curve: for ordinary elliptic curve. $E: y^2 = x^3 + b$.

& $k=12$ for prime r. $q^k \equiv 1 \pmod r$

$q^{12} \equiv 1 \pmod r$

$$\begin{cases} q(t) = 36t^4 + 36t^3 + 24t^2 + 6t + 1 \\ r(t) = 36t^4 + 36t^3 + 18t^2 + 6t + 1 \\ tr(t) = 6t^2 + 1 \end{cases}$$

$$\begin{cases} \#E(\mathbb{F}_{q(t)}) = q(t) + 1 - tr(t) \\ r \mid \#E(\mathbb{F}_{q(t)}) \end{cases}$$

Sextic twisted curve $E'/\mathbb{F}_{q^2}: y^2 = x^3 + \beta b$. $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$

$\beta \notin \mathbb{F}_{q^2}^3$ nor $\mathbb{F}_{q^2}^2$

$\phi_6: E \to E'$ is an isomorphism defined over $\mathbb{F}_{q^{2\cdot 6}}$

$(x, y) \mapsto \left(\frac{1}{\sqrt[3]{\beta}}x, \frac{1}{\sqrt{\beta}}y\right)$

$\mathbb{F}_{q^{2\cdot 6}} = \mathbb{F}_{q^{12}}$ $\mathbb{F}_{q^{2\cdot 6}}$

$\beta \in \mathbb{F}_{q^2}$ $\nearrow 3$ $\nearrow 2$.

$R_a(Q,P) =$ F_a

$\sqrt[3]{\beta}$

$E/\pi_q \xrightarrow[(t)]{\text{Bezout}} E'/\pi_{q'}$ isomorphism

(,) $\mathbb{F}_q$-

$x_q(x, y) = (x^q, y^q)$