Analysis of Optimum Pairing Products at High Security Levels

Xusheng Zhang[†] and Dongdai Lin[‡]

† Institute of Software, Chinese Academy of Sciences
‡ Institute of Information Engineering, Chinese Academy of Sciences

INDOCRYPT 2012
Indian Statistical Institute, Kolkata

Dec 12, 2012

Outline

Bilinear pairing on elliptic curve

- Bilinear Pairing is very important in **encryption**, **signature** ...
- **Elliptic Curve Pairing** is a very simple model.
  - Weil: $e(P,Q) = f_{r,D_{\boldsymbol{P}}}(D_Q)/f_{r,D_{\boldsymbol{Q}}}(D_P)$
  - Tate: $t(P,Q) = f_{r,D_{\boldsymbol{P}}}(D_Q)^{(q^{\boldsymbol{k}}-1)/r}$
- Many pairings in Tate family could be chosen.
  - Symmetric: eta pairing
  - **Asymmetric**: ate, optimal ate pairing
- Special elliptic (pairing-friendly) curves are preferred.
  - Supersingular curve
  - Parameterized **ordinary curve**: BN, BLS, KSS curves ...

Fast pairing on elliptic curve

For an order-r pairing on elliptic curve

$$e : E(\mathbb{F}_q)[r] \times E[r] \cap \ker(\pi_q - q) \to \mu_r \subset \mathbb{F}_{q^k}$$

- Choosing good parameters.
  - Prime r insures ECC security.
  - $\mathbb{F}_{q^k}$ insures MOV security.
  - $\rho = \log q / \log r$ is close to 1.
- Miller's algorithm is widely used.
  - Doubling or addition formulas: even embedding degree k, **high-degree twist** ...
  - Miller loop length: $\lceil \log r / \varphi(k) \rceil$ (**optimal**)
- Choosing Weil family or Tate family?
  - Weil's optimal **loop length** could be **larger** than Tate's.
  - Weil's **Miller formulas** could be more **expansive** than Tate's.
  - But Weil's **final exponentiation** is **much easier** than Tate's. (Fortunately **cyclotomic squaring** could be used for Tate's.)

Fast pairing on elliptic curve

For an order-r pairing on elliptic curve

$$e : E(\mathbb{F}_q)[r] \times E[r] \cap \ker(\pi_q - q) \to \mu_r \subset \mathbb{F}_{q^k}$$

- Choosing good parameters.
  - Prime r insures ECC security.
  - $\mathbb{F}_{q^k}$ insures MOV security.
  - $\rho = \log q / \log r$ is close to 1.
- Miller's algorithm is widely used.
  - Doubling or addition formulas: even embedding degree k, **high-degree twist** ...
  - Miller loop length: $\lceil \log r / \varphi(k) \rceil$ (**optimal**)
- Choosing Weil family or Tate family?
  - Weil's optimal **loop length** could be **larger** than Tate's.
  - Weil's **Miller formulas** could be more **expansive** than Tate's.
  - But Weil's **final exponentiation** is **much easier** than Tate's. (Fortunately **cyclotomic squaring** could be used for Tate's.)

Fast pairing on elliptic curve

For an order-r pairing on elliptic curve

$$e : E(\mathbb{F}_q)[r] \times E[r] \cap \ker(\pi_q - q) \to \mu_r \subset \mathbb{F}_{q^k}$$

- Choosing good parameters.
  - Prime r insures ECC security.
  - $\mathbb{F}_{q^k}$ insures MOV security.
  - $\rho = \log q / \log r$ is close to 1.
- Miller's algorithm is widely used.
  - Doubling or addition formulas: even embedding degree k, **high-degree twist** ...
  - Miller loop length: $\lceil \log r / \varphi(k) \rceil$ (**optimal**)
- Choosing Weil family or Tate family?
  - Weil's optimal **loop length** could be **larger** than Tate's.
  - Weil's **Miller formulas** could be more **expansive** than Tate's.
  - But Weil's **final exponentiation** is **much easier** than Tate's. (Fortunately **cyclotomic squaring** could be used for Tate's.)

Optimum choices

So the optimum choice is optimal ate pairing with sextic twist!

When computing pairing product, what's the optimum choice? Notice Miller iteration is more important. So need to balance the loop length and the twist degree.

- 128-bit security: recommended $k\rho = 12$
  - Single: BN ($k = 12$, $\rho = 1$) optimal pairing
  - Product: BN optimal pairing
- 192-bit security: recommended $k\rho = 21\frac{1}{3}$
  - Single: BLS12 ($k = 12$, $\rho = 1.5$) ate pairing
  - Product: ?
- 256-bit security: recommended $k\rho = 30$
  - Single: BLS24 ($k = 24$, $\rho = 1.25$) ate pairing
  - Product: ?

Optimum choices

So the optimum choice is optimal ate pairing with sextic twist!

When computing pairing product, what's the optimum choice? Notice **Miller iteration** is more important. So need to balance the loop length and the twist degree.

- 128-bit security: recommended $k\rho = 12$
  - Single: BN ($k = 12$, $\rho = 1$) optimal pairing
  - Product: BN optimal pairing
- 192-bit security: recommended $k\rho = 21\frac{1}{3}$
  - Single: BLS12 ($k = 12$, $\rho = 1.5$) ate pairing
  - Product: ?
- 256-bit security: recommended $k\rho = 30$
  - Single: BLS24 ($k = 24$, $\rho = 1.25$) ate pairing
  - Product: ?

Optimum choices

So the optimum choice is optimal ate pairing with sextic twist!

When computing pairing product, what's the optimum choice? Notice **Miller iteration** is more important. So need to balance the loop length and the twist degree.

- 128-bit security: recommended $k\rho = 12$
  - Single: BN ($k = 12$, $\rho = 1$) optimal pairing
  - Product: BN optimal pairing
- 192-bit security: recommended $k\rho = 21\frac{1}{3}$
  - Single: BLS12 ($k = 12$, $\rho = 1.5$) ate pairing
  - Product: KSS16 ($k = 16$, $\rho = 1.5$) optimal pairing
- 256-bit security: recommended $k\rho = 30$
  - Single: BLS24 ($k = 24$, $\rho = 1.25$) ate pairing
  - Product: BLS27 ($k = 27$, $\rho = 1.111$) ate pairing

Outline

Review Miller's algorithm

Input: $r = \sum_{j=0}^{L} s_j 2^j$, $s_j \in \{0, 1\}$
Output: $f_{r,P}(Q)^{(q^k-1)/r}$

1: $R \leftarrow P$; $f \leftarrow 1$
2: **for** $j = L - 1..0$ **do**
3: $\quad f \leftarrow f^2 \cdot l_{R,R}(Q)/v_{2R}(Q)$
4: $\quad R \leftarrow 2R$
5: $\quad$ **if** $s_j = 1$ **then**
6: $\quad\quad f \leftarrow f \cdot l_{R,P}(Q)/v_{R+P}(Q)$
7: $\quad\quad R \leftarrow R + P$
8: **return** $f^{(q^k-1)/r}$.

- Expand in 2-adic
- Denominator elimination method
- Expand in 2-NAF

Review Miller's algorithm

Input: $r = \sum_{j=0}^{L} s_j 2^j$, $s_j \in \{0, 1\}$
Output: $f_{r,P}(Q)^{(q^k-1)/r}$

1: $R \leftarrow P$; $f \leftarrow 1$
2: **for** $j = L - 1..0$ **do**
3: $\quad f \leftarrow f^2 \cdot l_{R,R}(Q)$
4: $\quad R \leftarrow 2R$
5: $\quad$ **if** $s_j = 1$ **then**
6: $\quad\quad f \leftarrow f \cdot l_{R,P}(Q)$
7: $\quad\quad R \leftarrow R + P$
8: **return** $f^{(q^k-1)/r}$.

- Expand in 2-adic
- Denominator elimination method
- Expand in 2-NAF

Review Miller's algorithm

Input: $r = \sum_{j=0}^{L} s_j 2^j$, $s_j \in \{-1, 0, 1\}$
Output: $f_{r,P}(Q)^{(q^k-1)/r}$

1: $R \leftarrow P$; $f \leftarrow 1$
2: **for** $j = L - 1..0$ **do**
3: $\quad f \leftarrow f^2 \cdot l_{R,R}(Q)$
4: $\quad R \leftarrow 2R$
5: $\quad$ **if** $s_j = 1$ **then**
6: $\quad\quad f \leftarrow f \cdot l_{R,P}(Q)$
7: $\quad\quad R \leftarrow R + P$
8: $\quad$ **if** $s_j = -1$ **then**
9: $\quad\quad f \leftarrow f \cdot \overline{l_{-R,P}(Q)}$
10: $\quad\quad R \leftarrow R - P$
11: **return** $f^{(q^k-1)/r}$.

- Expand in 2-adic
- Denominator elimination method
- Expand in 2-NAF

Curves only with cubic twist

Some curves only with cubic twist might have **faster Miller iteration** (due to larger $\varphi(k)/k$, e.g. $k = 9, 27$).

Denominator elimination method

- ☹ Classic method is invalid

$$v_R(S) = x_S - x_R \notin \mathbb{F}_{p^{k'}} \ (k' \mid k)$$

- ☺ A substituted method by Lin *et al.*

$$f_{R_1,R_2}(S) = \frac{l_{R_1,R_2}}{v_{R_3}}(S) \sim l_{R_1,R_2}(S)(x_S^2 + x_{R_3}x_S + x_{R_3}^2)$$

- ☺☺ New method

$$f_{R_1,R_2}(S) = \frac{l_{R_1,R_2}}{v_{R_3}}(S) \sim x_S^2 + x_{R_3}x_S + x_{R_3}^2 - \lambda(y_S - y_{R_3})$$

Curves only with cubic twist

Some curves only with cubic twist might have **faster Miller iteration** (due to larger $\varphi(k)/k$, e.g. $k = 9, 27$).

Denominator elimination method

- ☹ Classic method is invalid

$$v_R(S) = x_S - x_R \notin \mathbb{F}_{p^{k'}} \ (k' \mid k)$$

- ☺ A substituted method by Lin *et al.*

$$f_{R_1,R_2}(S) = \frac{l_{R_1,R_2}}{v_{R_3}}(S) \sim l_{R_1,R_2}(S)(x_S^2 + x_{R_3}x_S + x_{R_3}^2)$$

☺☺ New method

$$f_{R_1,R_2}(S) = \frac{l_{R_1,R_2}}{v_{R_3}}(S) \sim x_S^2 + x_{R_3}x_S + x_{R_3}^2 - \lambda(y_S - y_{R_3})$$

Ate-like Miller iteration function

Use the cubic twist

- Affine Miller iteration function

$$f_{DBL(R_1)}(P') = x_3^2 + \frac{3x_1^2}{2y_1}(y_3 - y_{P'}) + x_3 x_P \omega^2 + x_P^2 \omega^4$$

$$f_{ADD(R_1,Q')}(P') = x_3^2 + \frac{y_2 - y_1}{x_2 - x_1}(y_3 - y_{P'}) + x_3 x_P \omega^2 + x_P^2 \omega^4$$

- Projective Miller iteration function

$$\begin{aligned} & F_{DBL(R_1)}(P') \\ = \; & X_3^2 + 12X_1^2 Y_1^2 (Y_3 - Z_3 y_{P'}) + 2X_3 Z_3 (\frac{x_P}{2}\omega^2) + Z_3^2 (x_P^2 \omega^4) \\ & F_{ADD(R_1,Q')}(P') \\ = \; & X_3^2 - Z_1 Z_2 (Z_1 X_2 - X_1 Z_2)^2 (Z_1 Y_2 - Y_1 Z_2)(Y_3 - Z_3 y_{P'}) \\ & + 2X_3 Z_3 (\frac{x_P}{2}\omega^2) + Z_3^2 (x_P^2 \omega^4) \end{aligned}$$

Operations for ate-like Miller formulas with cubic twist

Affine ADD

$A = (x_2 - x_1)^{-1},\ B = A \cdot (y_2 - y_1),\ x_3 = B^2 - x_1 - x_2,\ y_3 = B \cdot (x_2 - x_3) - y_2,$
$t_3 = x_3^2,\ C = B \cdot (y_3 - y_{P'}),\ D = t_3 + C,\ E = x_3 \cdot x_P.$

Affine DBL

$A = 3t_1,\ B = 2y_1,\ C = B^{-1},\ D = A \cdot C,\ x_3 = D^2 - 2x_1,\ y_3 = D \cdot (x_1 - x_3) - y_1,$
$t_3 = x_3^2,\ E = D \cdot (y_3 - y_{P'}),\ F = t_3 + E,\ G = x_3 \cdot x_P.$

Projective mADD

$A = X_1 \cdot Z_2,\ B = Y_1 \cdot Z_2,\ C = Z_1 \cdot Z_2,\ D = A - Z_1 \cdot X_2,\ E = B - Z_1 \cdot Y_2,\ F = D^2,$
$G = E^2,\ H = D \cdot F,\ I = F \cdot A,\ J = H + C \cdot G - 2I,\ K = C \cdot F \cdot E,\ X_3 = D \cdot J,$
$Y_3 = E \cdot (I - J) - H \cdot B,\ Z_3 = C \cdot H,\ T_3 = X_3^2,\ U_3 = Z_3^2,\ L = (X_3 + Z_3)^2 - T_3 - U_3,$
$M = Z_3 \cdot y_{P'},\ L_0 = T_3 - K \cdot (Y_3 - M),\ L_1 = L \cdot (x_P/2),\ L_2 = U_3 \cdot (x_P^2).$

Projective DBL

$A = Y_1^2,\ B = 3b \cdot U_1,\ C = (X_1 + Y_1)^2 - T_1 - A,\ D = (Y_1 + Z_1)^2 - A - U_1,\ E = 3B,$
$X_3 = C \cdot (A - E),\ Y_3 = (A + E)^2 - 3(2B)^2,\ Z_3 = 4A \cdot D,\ T_3 = X_3^2,\ U_3 = Z_3^2,$
$F = (X_3 + Z_3)^2 - T_3 - U_3,\ G = 3C^2,\ H = Z_3 \cdot y_{P'},\ L_0 = G \cdot (Y_3 - H) + T_3,$
$L_1 = F \cdot (x_P/2),\ L_2 = U_3 \cdot (x_P^2).$

Costs for ate-like Miller formulas with cubic twist

$3 \mid k$	coord.	$\mathbf{M}_1$	$\mathbf{I}_{k/3}$	$\mathbf{M}_{k/3}$	$\mathbf{S}_{k/3}$	$\mathbf{M}_{(.)}$
DBL	$\mathcal{P}$ Costello *et al.*	k	–	6	7	$1\mathbf{M}_{(b)}$
DBL	$\mathcal{P}$	k	–	3	9	$1\mathbf{M}_{(3b)}$
DBL	$\mathcal{A}$	$k/3$	1	3	2	–
mADD	$\mathcal{P}$ Costello *et al.*	k	–	13	3	–
mADD	$\mathcal{P}$	k	–	12	5	–
ADD	$\mathcal{A}$	$k/3$	1	3	2	–
BDL+mADD	$\mathcal{P}$ Costello *et al.*	$2k$	–	19	10	$1\mathbf{M}_{(b)}$
BDL+mADD	$\mathcal{P}$	$2k$	–	15	14	$1\mathbf{M}_{(3b)}$

- Projective formulas are a **little** faster than the previous ones.
- Affine formulas might be **much** faster than these projective ones.

Affine vs. Projective

- Lauter *et al.* showed at **high security levels**, affine ate-like Miller formulas could be faster than projective ones.
  (**Idea**: the **inversion-to-multiplication ratio** in larger extension field could be lower.)
- In our case of ate-like pairing computation, the inversion-to-multiplication ratio $\mathbf{R}_{k/3} = \frac{\mathbf{I}_{k/3}}{\mathbf{M}_{k/3}}$ is still low.

k	$\mathbf{I}_{k/3}$	$\mathbf{M}_{k/3}$	$\mathbf{R}_{k/3}$
9	$\mathbf{I}_1 + 11\mathbf{M}_1$ (Karatsuba, $\mathbf{M}_1 \approx 0.8\mathbf{S}_1$)	$6\mathbf{M}_1$ (Karatsuba)	$\mathbf{R}_3 \leq 18.5$ ($\mathbf{R}_1 \leq 100$)
27	$\mathbf{I}_1 + 75\mathbf{M}_1$ (Karatsuba, $\mathbf{M}_1 \approx 0.8\mathbf{S}_1$)	$36\mathbf{M}_1$ (Karatsuba)	$\mathbf{R}_9 \leq 4.86$ ($\mathbf{R}_1 \leq 100$)

From the previous cost comparison, our new affine formulas are better than the projective ones when $\mathbf{R}_{k/3} \leq 5.6$.

Outline

Barreto-Lynn-Scott 27 curve

BLS27: $E(r(z), t(z), p(z)), y^2 = x^3 + b$

$$\begin{cases} r(z) = \frac{1}{3}(z^{18} + z^9 + 1), \\ t(z) = z + 1, \\ p(z) = \frac{1}{3}(z-1)^2(z^{18} + z^9 + 1) + z. \end{cases}$$

- Extension field can be constructed easily.

$$\mathbb{F}_{p^{27}} = \mathbb{F}_p[t]/\langle t^{27} - 2\rangle, \text{ if } (z-1)/3 \text{ is odd}$$
$$\mathbb{F}_{p^{27}} = \mathbb{F}_p[t]/\langle t^{27} - 3\rangle, \text{ two-thirds of even } (z-1)/3$$

- Ate pairing is optimal.

$$f_{z,Q'}(P')^{(p^{27}-1)/r}$$

- Final Exp. can be computed without using addition chains.

$$(p^{27}-1)/r = (p^9-1)((z-1)^2(p^9 + z^9 + 1)(\sum_{i=0}^{8} z^i p^{8-i}) + 3)$$

Barreto-Lynn-Scott 27 curve

BLS27: $E(r(z), t(z), p(z)), y^2 = x^3 + b$

$$\begin{cases} r(z) = \frac{1}{3}(z^{18} + z^9 + 1), \\ t(z) = z + 1, \\ p(z) = \frac{1}{3}(z-1)^2(z^{18} + z^9 + 1) + z. \end{cases}$$

- Extension field can be constructed easily.

$$\mathbb{F}_{p^{27}} = \mathbb{F}_p[t]/\langle t^{27} - 2\rangle, \text{ if } (z-1)/3 \text{ is odd}$$
$$\mathbb{F}_{p^{27}} = \mathbb{F}_p[t]/\langle t^{27} - 3\rangle, \text{ two-thirds of even } (z-1)/3$$

- Ate pairing is optimal.

$$f_{z,Q'}(P')^{(p^{27}-1)/r}$$

- Final Exp. **but** lacks cyclotomic squarings!

$$(p^{27}-1)/r = (p^9-1)((z-1)^2(p^9 + z^9 + 1)(\sum_{i=0}^{8} z^i p^{8-i}) + 3)$$

Comparison at 256-bit security level

- Suggested curve choices:
  $E : y^2 = x^3 - 2$, where $z = 2^{28} + 2^{27} + 2^{25} + 2^8 - 2^3$, $r(z)$ has a 516-bit prime factor. and $p(z)$ is a 573-bit prime.

- Estimated Cost ($\mathbf{m}_{640} \approx 1.228\mathbf{m}_{576}$, $\mathbf{m}_{576} \approx 1.257\mathbf{m}_{512}$, $\mathbf{m}_{576} \approx 0.8\mathbf{s}_{576}$)

Pairing	ML+FS		FE	Total	
(coord.)	Full Sq.	others		n	
BLS27	$5832\mathbf{m}_{573}$	$14897\mathbf{m}_{573}$	$116625\mathbf{m}_{573}$	1	$34\mathbf{i}_{573} + 137355\mathbf{m}_{573}$
ate		$+33\mathbf{i}_{573}$	$+\mathbf{i}_{573}$	26	$859\mathbf{i}_{573} + 509779\mathbf{m}_{573}$
$(\mathcal{A})$				30	$991\mathbf{i}_{573} + 569367\mathbf{m}_{573}$
BLS24	$6804\mathbf{m}_{640}$	$14493\mathbf{m}_{640}$	$30596\mathbf{m}_{640}$	1	$77\mathbf{i}_{640} + 63724\mathbf{m}_{576}$
ate		$+67\mathbf{i}_{640}$	$+10\mathbf{i}_{640}$	26	$1752\mathbf{i}_{640} + 508649\mathbf{m}_{576}$
$(\mathcal{A})$				30	$2020\mathbf{i}_{640} + 579837\mathbf{m}_{576}$

Outline

Kachisa-Schaefer-Scott 16 curve

KSS16: $E(r(z), t(z), p(z)), y^2 = x^3 + ax$

$$\begin{cases} r(z) = z^8 + 48z^4 + 625, \\ t(z) = \frac{1}{35}(2z^5 + 41z + 35), \\ p(z) = \frac{1}{980}(z^{10} + 2z^9 + 5z^8 + 48z^6 + 152z^5 \\ \qquad +240z^4 + 625z^2 + 2398z + 3125) \end{cases}$$

- Optimal ate pairing can be constructed by using Vercauteren's method.

Lemma

Let $E(t(z), r(z), p(z))$ be a complete family of P-F curves with embedding degree $k > 1$. Then, there exist $m(z) \in \mathbb{Q}[z]$ and $c_i(z) \in \mathbb{Z}[z]$, so that $m(z)r(z) = \sum_{i=0}^{\varphi(k)-1} c_i(z)p(z)^i$, where $\deg c_0(z) = 1$ and $\deg c_i(z) = 0$.

- Final exponentiation seems complicated.

Kachisa-Schaefer-Scott 16 curve

KSS16: $E(r(z), t(z), p(z)), y^2 = x^3 + ax$

$$\begin{cases} r(z) = z^8 + 48z^4 + 625, \\ t(z) = \frac{1}{35}(2z^5 + 41z + 35), \\ p(z) = \frac{1}{980}(z^{10} + 2z^9 + 5z^8 + 48z^6 + 152z^5 \\ \qquad +240z^4 + 625z^2 + 2398z + 3125) \end{cases}$$

- Optimal ate pairing can be constructed by using Vercauteren's method.

$$a_{opt}(Q, P) = \left(\left(\underline{f_{z,Q}(P) \cdot l_{[z]Q,[p]Q}(P)} \right)^{p^3} \cdot l_{Q,Q}(P) \right)^{857500(p^{16}-1)/r}$$

- Final exponentiation seems complicated.

$$857500(p^{16} - 1)/r = (p^8 - 1) \sum_{i=0}^{7} c_i(z) p^i$$

Kachisa-Schaefer-Scott 16 curve

KSS16: $E(r(z), t(z), p(z)), y^2 = x^3 + ax$

$$\begin{cases} r(z) = z^8 + 48z^4 + 625, \\ t(z) = \frac{1}{35}(2z^5 + 41z + 35), \\ p(z) = \frac{1}{980}(z^{10} + 2z^9 + 5z^8 + 48z^6 + 152z^5 \\ \qquad +240z^4 + 625z^2 + 2398z + 3125) \end{cases}$$

- Optimal ate pairing can be constructed by using Vercauteren's method.

$$a_{opt}(Q, P) = \left(\underline{(f_{z,Q}(P) \cdot l_{[z]Q,[p]Q}(P))^{p^3}} \cdot l_{Q,Q}(P) \right)^{857500(p^{16}-1)/r}$$

- Final exponentiation seems complicated.

$$857500(p^{16} - 1)/r = (p^8 - 1) \sum_{i=0}^{7} c_i(z) p^i$$

Kachisa-Schaefer-Scott 16 curve

- Decomposed the final exp. by using special addition chains.

$$
\begin{aligned}
c_0 &= -11(z^4A + 27z^3B + 28) + 19A, \\
c_1 &= 5(3z^3A + 44z^2B), \\
c_2 &= 25(z^2A + 38zB), \\
c_3 &= -125(zA + 24B), \\
c_4 &= -(2z^4A + 55z^3B) + 84A, \\
c_5 &= -5(4z^3A + 117z^2B), \\
c_6 &= 25(2z^2A + 41zB), \\
c_7 &= 125 \cdot 7B
\end{aligned}
$$

where $A = z^3 \cdot B + 56$ and $B = (z+1)^2 + 4$.

Comparison at 192-bit Security Level

- Suggested curve choices:
  $E : y^2 = x^3 - 3x$, where $z = 2^{49} + 2^{26} + 2^{15} - 2^7 - 1$, $r(z)$ has a 377-bit prime factor, and $p(z)$ is a 481-bit prime.

- Estimated Cost ($\mathbf{m}_{640} \approx 1.544\mathbf{m}_{512}$, $\mathbf{m}_{512} \approx 1.744\mathbf{m}_{384}$)

Pairing (coord.)	ML+FS		FE	Total	
	Full Sq.	others		n	
KSS16 opt-ate ($\mathcal{P}$)	$2592\mathbf{m}_{481}$	$7616\mathbf{m}_{481}$	$22330\mathbf{m}_{481}$ $+\mathbf{i}_{481}$	1	$\mathbf{i}_{481} + 32538\mathbf{m}_{481}$
				2	$\mathbf{i}_{481} + 40154\mathbf{m}_{481}$
				7	$\mathbf{i}_{481} + 78234\mathbf{m}_{481}$
BLS12 ate ($\mathcal{P}$)	$3816\mathbf{m}_{640}$	$7049\mathbf{m}_{640}$	$8464\mathbf{m}_{640}$ $+6\mathbf{i}_{640}$	1	$6\mathbf{i}_{640} + 29843\mathbf{m}_{512}$
				2	$6\mathbf{i}_{640} + 40728\mathbf{m}_{512}$
				7	$6\mathbf{i}_{640} + 95146\mathbf{m}_{512}$
KSS18 opt-ate ($\mathcal{P}$)	$4158\mathbf{m}_{508}$	$9544\mathbf{m}_{508}$	$23821\mathbf{m}_{508}$ $+8\mathbf{i}_{508}$	1	$8\mathbf{i}_{508} + 37523\mathbf{m}_{508}$
				2	$8\mathbf{i}_{508} + 47067\mathbf{m}_{508}$
				7	$8\mathbf{i}_{508} + 94787\mathbf{m}_{508}$

Outline

Summary

- New fast Miller formulas only with cubic twist.
  - Affine formulas (more efficient at high security levels).
  - Projective formulas.
- Improvements of pairing computations on KSS16 and BLS27. Specially, when computing pairing product
  - KSS16 optimal ate pairing is preferred at 192-bit security level.
  - BLS27 ate pairing might be better at 256-bit security level.

Further work ...

- Accelerate the final exp. computation for BLS27 ate pairing ? (cyclotomic squaring or cubing)
- Fast pairing on other curves only with cubic twist ?
  e.g. Supersingular curve $E/\mathbb{F}_{p^{2m}}$ with $k = 3$ (We have done)

Summary

- New fast Miller formulas only with cubic twist.
  - Affine formulas (more efficient at high security levels).
  - Projective formulas.
- Improvements of pairing computations on KSS16 and BLS27. Specially, when computing pairing product
  - KSS16 optimal ate pairing is preferred at 192-bit security level.
  - BLS27 ate pairing might be better at 256-bit security level.

Further work ...

- Accelerate the final exp. computation for BLS27 ate pairing ? (cyclotomic squaring or cubing)
- Fast pairing on other curves only with cubic twist ?
  e.g. Supersingular curve $E/\mathbb{F}_{p^{2m}}$ with $k = 3$ (**We have done**)

Thank you for your attention !

Any questions, please email to "xszhang.is@gmail.com"