Faster Pairing Computations on Curves with High-Degree Twists

Craig Costello

craig.costello@qut.edu.au
Queensland University of Technology

PKC 2010

Joint work with Tanja Lange and Michael Naehrig

Applications of Pairings

The power of pairings: $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$

$$e(aP, bQ) = e(P, Q)^{ab} = e(bP, aQ) \in \mathbb{G}_T$$

Bilinearity has brought us...

- ID-based encryption
- ID-based key agreement
- short signatures
- group signatures
- ring signatures
- certificateless encryption
- hierarchical ID-based encryption
- attribute-based encryption
- searchable encryption
- non-interactive proof systems
- ... + many more (e.g. see the proceedings)

Motivation

Elliptic curves: many high-level optimizations thoroughly explored

loop shortening, endomorphism rings, group choices and representations, friendly curves, and many more tricks...

AS FOR THIS WORK...

- Standard (Weierstrass) representation $E : y^2 = x^3 + ax + b$
- Optimal curve constructions produce curves with $a = 0$ or $b = 0$ (high-degree twists also demand either constraint)
- Want to minimize field operations for pairing computations on these special shaped curves
- Tate and ate formulas haven't always been compatible
- Previously: special curve models don't necessarily allow for ate pairing computation (Edwards, $y^2 = x^3 + c^2$, etc)
- Improve and collect all required explicit formulae (records) together

Group choices as Frobenius eigenspaces

The embedding degree k

Must form a degree k field extension of $\mathbb{F}_q$ to find two order r subgroups

$$\mathbb{G}_1 = E[r] \cap \ker(\phi_q - [1]) = E(\mathbb{F}_q)[r], \qquad \text{(the base field)}$$

$$\mathbb{G}_2 = E[r] \cap \ker(\phi_q - [q]) \subseteq E(\mathbb{F}_{q^k})[r], \qquad \text{(the full extension field)}$$

The elements of $\mathbb{G}_2$ are much bigger than the elements of $\mathbb{G}_1$ (e.g. $k = 12$)

$P \in \mathbb{G}_1$: $(341746248540, 710032105147)$

$Q \in \mathbb{G}_2$: $(502478767360 * t^{11} + 1034075074191 * t^{10} + 342970860051 * t^9 + 225764301423 * t^8 + 205398279920 * t^7 + 182600014119 * t^6 + 860891557473 * t^5 + 435210764901 * t^4 + 1043922075477 * t^3 + 566889113793 * t^2 + 150949917087 * t + 21392569319, 654337640030 * t^{11} + 744622505639 * t^{10} + 1092264803801 * t^9 + 895826335783 * t^8 + 529466169391 * t^7 + 550511036767 * t^6 + 985244799144 * t^5 + 554170865706 * t^4 + 194564971321 * t^3 + 969736450831 * t^2 + 579122687888 * t + 581111086076)$

The twisted curve

- Original curve is $E(\mathbb{F}_q) : y^2 = x^3 + ax + b$
- Twisted curve is $E'(\mathbb{F}_{q^{k/d}})$: $y^2 = x^3 + a\omega^4 x + b\omega^6$, $\omega \in \mathbb{F}_{q^k}$
- Possible degrees of twists are $d \in \{2, 3, 4, 6\}$
- $d > 2$ requires $a = 0$ or $b = 0$
- Twist $\Psi : E' \to E : (x', y') \to (x'/\omega^2, y'/\omega^3)$ induces $\mathbb{G}_2' = E'(\mathbb{F}_{q^{k/d}})[r]$ so that $\Psi : \mathbb{G}_2' \to \mathbb{G}_2$
- Instead of working with $Q \in \mathbb{G}_2$, a lot of work can be done with $Q' \in \mathbb{G}_2'$ defined over subfield $\mathbb{F}_{q^e} = \mathbb{F}_{q^{k/d}}$

$P \in \mathbb{G}_1$: $(341746248540, 710032105147)$
$Q \in \mathbb{G}_2' = \Psi^{-1}(\mathbb{G}_2)$:

$((917087150949 * t + 25693192139) \cdot \omega^2, (878885791226 * t + 860765811110) \cdot \omega^3)$

Tate vs. ate pairings

Tate pairing

$$e_r : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r, \ (P, Q) \mapsto f_{r,P}(Q)^{\frac{q^k-1}{r}}.$$

Ate pairing

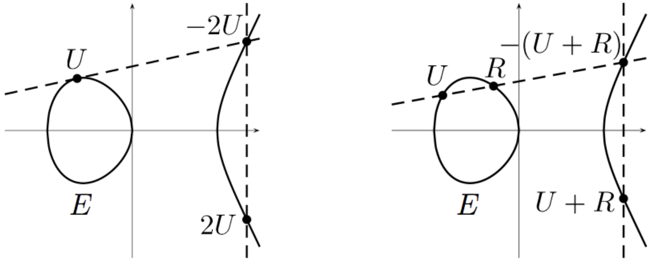
$$a_T : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r, \ (Q, P) \mapsto f_{T,Q}(P)^{\frac{q^k-1}{r}}.$$

- Pairings require the computation of Miller functions $f_{m,R}(S)$
- Function $f_{m,R}$ is of degree m
- Constructions require $\lfloor \log_2 m \rfloor$ iterations of Miller's algorithm
- Most of the work is done in the first argument
- Tate needs $\lfloor \log_2 r \rfloor$ iters, ate needs $\lfloor \log_2 T \rfloor$ iters, $T \ll r$
- Trade-off is that more work in ate is done in larger field $(\mathbb{G}_2')$

Miller's algorithm to compute $f_{m,R}(S)$

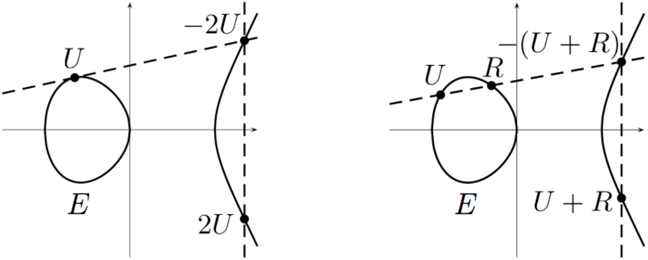
$m = (m_{l-1}, \ldots, m_1, m_0)_2$ initialize: $U = R$, $f = 1$

1. for $i = l - 2$ to 0 do
   a. i. Compute $f_{\mathrm{DBL}(U)}$ in the doubling of U
      ii. $U \leftarrow [2]U$ //(DBL)
      iii. $f \leftarrow f^2 \cdot f_{\mathrm{DBL}(U)}(S)$
   b. if $m_i = 1$ then
      i. Compute $f_{\mathrm{ADD}(U,R)}$ in the addition of $U + R$
      ii. $U \leftarrow U + R$ //(ADD)
      iii. $f \leftarrow f \cdot f_{\mathrm{ADD}(U,R)}(S)$
2. $f \leftarrow f^{(q^k-1)/r}$.



Weierstrass curves for fast pairings

- Want to minimize effort of computing doubling $U \leftarrow [2]U$ and $f_{\mathrm{DBL}(U)}$ together (analogous for addition)
- Miller functions $f_{\mathrm{DBL}} = l_{\mathrm{DBL}}/v_{\mathrm{DBL}}$ and $f_{\mathrm{ADD}} = l_{\mathrm{ADD}}/v_{\mathrm{ADD}}$ are inherent in doubling and addition formulae
- Weierstrass (cubic) elliptic curves give natural combination of point operations and **line** computations



Roles of arguments in Miller's algorithm

1. for $i = l - 2$ to 0 do
   - a.
     - i. Compute $f_{\mathrm{DBL}(U)}$ in the doubling of U
     - ii. $U \leftarrow [2]U$, //(DBL)
     - iii. $f \leftarrow f^2 \cdot f_{\mathrm{DBL}(U)}(S)$,
   - b. if $m_i = 1$ then
     - i. Compute $f_{\mathrm{ADD}(U,R)}$ in the addition of $U + R$
     - ii. $U \leftarrow U + R$ //(ADD)
     - iii. $f \leftarrow f \cdot f_{\mathrm{ADD}(U,R)}(S)$
2. $f \leftarrow f^{(q^k-1)/r}$.

- Step (iii): same complexity regardless of Tate or ate pairing. Operations are in full extension field (costly) $\mathbb{F}_{q^k}$
- Steps (i) and (ii): depend entirely on first argument R
- $R \in \mathbb{F}_q$ for Tate... large k means (iii) dominates complexity
- $R \in \mathbb{F}_{q^e}$ for ate... complexities of (i) and (ii) grow at same rate as (iii) as k grows

Compatible Tate and ate formulas

- Tate pairing keeps U on the same curve throughout entire computation
- Ate pairing twists U back and forth $U \leftrightarrow U'$ between E and E'
- Formulas for pairing computation derived assuming same curve equation... okay if E and E' both covered by curve equation
- **Not okay** if E and E' don't both agree with equation (Edwards, $y^2 = x^3 + c^2$, etc)

a.
  i. Compute $f_{\mathrm{DBL}(U')}$ in the doubling of U' — $U' \in \mathbb{G}_2' \subset E'$
  ii. $U' \leftarrow [2]U'$, — $U' \in \mathbb{G}_2' \subset E'$
  iii. $f \leftarrow f^2 \cdot f_{\mathrm{DBL}(U)}(S)$ — $S \in E$, $U = \Psi(U') \in \mathbb{G}_2 \subset E$

b. if $m_i = 1$ then
  i. Compute $f_{\mathrm{ADD}(U',R)}$ in the addition of $U' + R$ — $U' \in \mathbb{G}_2' \subset E'$
  ii. $U' \leftarrow U' + R$ — $U' \in \mathbb{G}_2' \subset E'$
  iii. $f \leftarrow f \cdot f_{\mathrm{ADD}(U,R)}(S)$ — $S \in E$, $U = \Psi(U') \in \mathbb{G}_2 \subset E$

Ate pairing entirely on the twist

Thm 1+ Corr 2: **Compute** $a_T(Q', P')$ **instead of** $a_T(\Psi(Q'), P)$
(make twisted curve E' the curve under which the formulas are derived)

a. i. Compute $f_{\mathrm{DBL}(U')}$ in the doubling of U' — $U' \in \mathbb{G}_2' \subset E'$
   ii. $U' \leftarrow [2]U'$, — $U' \in \mathbb{G}_2' \subset E'$
   iii. $f \leftarrow f^2 \cdot f_{\mathrm{DBL}(U')}(S')$ — $U', S' \in \mathbb{G}_2' \subset E'$

b. if $m_i = 1$ then
   i. Compute $f_{\mathrm{ADD}(U',R')}$ in the addition of $U + R$ — $U' \in \mathbb{G}_2' \subset E'$
   ii. $U' \leftarrow U' + R'$ — $U' \in \mathbb{G}_2' \subset E'$
   iii. $f \leftarrow f \cdot f_{\mathrm{ADD}(U',R')}(S')$ — $U', S' \in \mathbb{G}_2' \subset E'$

Consequences...

- Computationally no different but allows Tate formulas (derived over one curve) to be applied to ate pairing
- Ate pairing now available on Edwards curves, $y^2 = x^3 + c^2$, etc.
- Analogous Tate-ate operation counts simplified on all curve shapes

Curve shapes and twists

- Fastest explicit formulas involves looking for best coordinates (curve representation and projection)
- Simplest (computable) expressions for projectified combination of point operations and line computations
- Prioritize **doublings** !!! (additions are rare)
- Different degree twists require curves of different shapes

i. $d = 2$ quadratic twists: $y^2 = x^3 + ax + b$, but $a = 0$ or $b = 0$ are almost always optimal constructions anyway (compatible with $d = 4, 6$ formulas)

ii. $d = 3$ cubic twists: $y^2 = x^3 + b$ (Section 6)

iii. $d = 4$ quartic twists: $y^2 = x^3 + ax$ (Section 4)

iv. $d = 6$ sextic twists: $y^2 = x^3 + b$ (Section 5)

Quartic twists and $y^2 = x^3 + ax$

- Affine formulas for $(x_3, y_3) = [2]U = [2](x_1, y_1)$ simplify to

$$x_3 = \lambda^2 - 2x_1,$$
$$y_3 = \lambda(x_1 - x_3) - y_1, \qquad \text{where } \lambda = (3x_1^2 + a)/(2y_1).$$

- Success with **weight-(1,2)** coordinates: $(x, y) = (X/Z,\ Y/Z^2)$
- Projective doubling $(X_3 : Y_3 : Z_3) = [2](X_1 : Y_1 : Z_1)$

$$X_3 = (X_1^2 - aZ_1^2)^2,$$
$$Y_3 = 2Y_1(X_1^2 - aZ_1^2)((X_1^2 + aZ_1^2)^2 + 4aZ_1^2X_1^2),$$
$$Z_3 = 4Y_1^2.$$

  Costs $1\mathbf{m} + 6\mathbf{s} + 1\mathbf{d}_a$ (Current fastest in the EFD!!)
- Formulas for line computation

$$f'_{\mathrm{DBL}(U)}(S) = -2(3X_1^2Z_1 + aZ_1^3) \cdot x_S + (4Y_1Z_1) \cdot y_S + 2(X_1^3 - aZ_1^2X_1).$$

  Additional cost of $1\mathbf{m} + 2\mathbf{s}$
- **NEW RECORD**: $2\mathbf{m} + 8\mathbf{s} + 1\mathbf{d}_a$
- Previous record: $1\mathbf{m} + 11\mathbf{s} + 1\mathbf{d}_a$ (Jacobian coorindates), Ionica and Joux + Arene *et al.*

Sextic twists and $y^2 = x^3 + b$

- Affine formulas for $(x_3, y_3) = [2]U = [2](x_1, y_1)$ simplify to

$$x_3 = \lambda^2 - 2x_1,$$
$$y_3 = \lambda(x_1 - x_3) - y_1, \qquad \text{where } \lambda = 3x_1^2/(2y_1).$$

- Success with homogeneous **projective** coordinates
- Projective doubling $(X_3 : Y_3 : Z_3) = [2](X_1 : Y_1 : Z_1)$

$$X_3 = 2X_1Y_1(Y_1^2 - 9bZ_1^2),$$
$$Y_3 = Y_1^4 + 18bY_1^2Z_1^2 - 27b^2Z_1^4,$$
$$Z_3 = 8Y_1^3Z_1.$$

- Formulas for line computation

$$f'_{\mathrm{DBL}(U)}(S) = 3X_1^2 \cdot x_S - 2Y_1Z_1 \cdot y_S + 3bZ_1^2 - Y_1^2.$$

- **NEW RECORD**: $2\mathbf{m} + 7\mathbf{s} + 1\mathbf{d}_b$
- Previous record: $3\mathbf{m} + 8\mathbf{s} + 1\mathbf{d}_b$ (Jacobian coordinates), Arene *et al.*

Cubic twists and $y^2 = x^3 + b$

- Cubic twists require special treatment (denominator elimination non-standard)
- Affine line must be multiplied $f'_{\mathrm{ADD}(U,R)}(S) = l_{\mathrm{ADD}(U,R)}(S) \cdot (x_S^2 + x_S x_{U+R} + x_{U+R}^2)$
- Success with homogeneous **projective** coordinates
- $f''_{\mathrm{DBL}(U)}(S) = X_1^2(Y_1^2 - 9bZ_1^2) \cdot x_S + 4X_1Y_1^2Z_1 \cdot x_S^2$
  $-6X_1^3Y_1 \cdot y_S + (Y_1^2 - bZ_1^2)(Y_1^2 + 9bZ_1^2).$
- **NEW RECORD**: $k\mathbf{m}_1 + 6\mathbf{m} + 7\mathbf{s} + 1\mathbf{d}_b$
- Previous record: $2k\mathbf{m}_1 + 8\mathbf{m} + 9\mathbf{s} + 1\mathbf{d}_b$ (also homog. projective), El Mrabet. *et al.*

Comparisons with previous best formulas...

Curve Curve order Twist deg.	Best Coord.	DBL ADD mADD	Prev. best Coord.	DBL ADD mADD
$y^2 = x^3 + ax$ - $d = 2, 4$	This work weight-1,2	$(2k/d)\mathbf{m}_1 + 2\mathbf{m} + 8\mathbf{s} + 1\mathbf{d}_a$ $(2k/d)\mathbf{m}_1 + 12\mathbf{m} + 7\mathbf{s}$ $(2k/d)\mathbf{m}_1 + 9\mathbf{m} + 5\mathbf{s}$	Ionica & Joux + Arene *et al.* Jacobian	$(2k/d)\mathbf{m}_1 + 1\mathbf{m} + 11\mathbf{s} + 1\mathbf{d}_a$ $(2k/d)\mathbf{m}_1 + 10\mathbf{m} + 6\mathbf{s}$ $(2k/d)\mathbf{m}_1 + 7\mathbf{m} + 6\mathbf{s}$
$y^2 = x^3 + c^2$ $3 \mid \#E$ $d = 2, 6$	This work + prev homog.	$(2k/d)\mathbf{m}_1 + 3\mathbf{m} + 5\mathbf{s}$ $(2k/d)\mathbf{m}_1 + 14\mathbf{m} + 2\mathbf{s} + 1\mathbf{d}_c$ $(2k/d)\mathbf{m}_1 + 10\mathbf{m} + 2\mathbf{s} + 1\mathbf{d}_c$	Costello *et al.* homog.	$(2k/d)\mathbf{m}_1 + 3\mathbf{m} + 5\mathbf{s}$ $(2k/d)\mathbf{m}_1 + 14\mathbf{m} + 2\mathbf{s} + 1\mathbf{d}_c$ $(2k/d)\mathbf{m}_1 + 11\mathbf{m} + 2\mathbf{s} + 1\mathbf{d}_c$
$y^2 = x^3 + b$ $3 \nmid \#E$ $d = 2, 6$	This work + prev homog.	$(2k/d)\mathbf{m}_1 + 2\mathbf{m} + 7\mathbf{s} + 1\mathbf{d}_b$ $(2k/d)\mathbf{m}_1 + 14\mathbf{m} + 2\mathbf{s}$ $(2k/d)\mathbf{m}_1 + 10\mathbf{m} + 2\mathbf{s}$	Arene *et al.* Jacobian	$(2k/d)\mathbf{m}_1 + 3\mathbf{m} + 8\mathbf{s}$ $(2k/d)\mathbf{m}_1 + 10\mathbf{m} + 6\mathbf{s}$ $(2k/d)\mathbf{m}_1 + 7\mathbf{m} + 6\mathbf{s}$
$y^2 = x^3 + b$ - $d = 3$	This work homog.	$k\mathbf{m}_1 + 6\mathbf{m} + 7\mathbf{s} + 1\mathbf{d}_b$ $k\mathbf{m}_1 + 16\mathbf{m} + 3\mathbf{s}$ $k\mathbf{m}_1 + 13\mathbf{m} + 3\mathbf{s}$	El Mrabet *et al.* homog.	$2k\mathbf{m}_1 + 8\mathbf{m} + 9\mathbf{s} + 1\mathbf{d}_b$ *ADD/mADD* *not reported*

- Also $\mathbf{m}_k + \mathbf{s}_k$ in each doubling entry ($\mathbf{m}_k$ for addition)
- Cubic twists faster by over 4 field operations per standard iteration
- Quartic twists faster by 2 field operations per standard iteration
- Sextic twists faster by 2 field operations per standard iteration

Tate and ate operation counts...

k	Const.	$\varphi(k)$	ρ	d	$m_{opt} : T_e : r$ (log)	Tate : ate $\mathbf{s} = \mathbf{m}$	Tate : ate $\mathbf{s} = 0.8\mathbf{m}$	$a_{m_{opt}}$ vs. η_{T_e}
4	6.4	2	2.000	4	1 : 1 : 2	30 : 30	26.6 : 26.6	Even
6	6.6	2	2.000	6	1 : 1 : 2	40 : 41	36 : 36.6	η_{T_e} (1.02)
8	6.10	4	1.500	4	3 : 3 : 4	68 : 88	61 : 77.8	η_{T_e} (1.3)
9	6.6	6	1.333	3	1 : 3 : 6	72 : 124	65.6 : 112	$a_{m_{opt}}$ (1.7)
12	6.8	4	1.000	6	1 : 2 : 4	103 : 121	92.6 : 107.8	$a_{m_{opt}}$ (1.7)
16	6.11	8	1.250	4	1 : 4 : 8	180 : 260	162.2 : 229.4	$a_{m_{opt}}$ (2.8)
18	6.12	6	1.333	6	1 : 3 : 6	165 : 196	148.6 : 176	$a_{m_{opt}}$ (2.5)
24	6.6	8	1.250	6	1 : 4 : 8	286 : 359	258 : 319.4	$a_{m_{opt}}$ (3.2)
27	6.6	18	1.111	3	1 : 9 : 18	290 : 602	263.6 : 542	$a_{m_{opt}}$ (4.4)
32	6.13	16	1.125	4	1 : 8 : 16	512 : 772	461.8 : 680.2	$a_{m_{opt}}$ (5.3)
36	6.14	12	1.167	6	1 : 6 : 12	471 : 597	424.6 : 531	$a_{m_{opt}}$ (4.7)
48	6.6	16	1.125	6	1 : 8 : 16	834 : 1069	752 : 950.2	$a_{m_{opt}}$ (6.2)

- Number of base field $\mathbb{F}_q$ multiplications per iteration
- Optimal loop lengths assumed to give Tate/ate comparison for Miller loop
- Tate speedup is only significant for small embedding degrees
- Faster formulas improve ate by speedup consistently for all k