An Analysis of Affine Coordinates for Pairing Computation

Michael Naehrig

Microsoft Research
mnaehrig@microsoft.com

joint work with

Kristin Lauter and Peter Montgomery
Microsoft Research

Pairing 2010, Yamanaka Hot Spring, Ishikawa, Japan
13 December 2010

Optimal ate pairings

To efficiently implement pairing-based protocols (at reasonably high security), one could choose a pairing

$$e : G_2' \times G_1 \to G_3, \quad (Q', P) \mapsto g_{Q'}(P)^{\frac{q^k-1}{r}}$$

- $G_1 = E(\mathbb{F}_q)[r]$, $G_2' = E'(\mathbb{F}_{q^e})[r]$, $G_3 = \mu_r \subseteq \mathbb{F}_{q^k}^*$,
- $E/\mathbb{F}_q$: elliptic curve, r prime, $r \mid \#E(\mathbb{F}_q)$, $\mathrm{char}(\mathbb{F}_q) > 3$,
- with small (even) embedding degree k,

$$r \mid q^k - 1, \quad r \nmid q^i - 1 \text{ for } i < k,$$

- $E'/\mathbb{F}_{q^e}$: twist of E of degree $d \mid k$, $e = k/d$, $r \mid \#E'(\mathbb{F}_{q^e})$,
- μ_r: group of r-th roots of unity in $\mathbb{F}_{q^k}^*$,
- $g_{Q'}$: function depending on Q' with coefficients in $\mathbb{F}_{q^k}^*$.

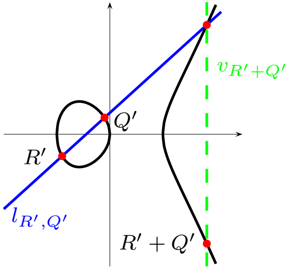
Possible choices for pairing-friendly curves

$$E : y^2 = x^3 + ax + b \text{ over } \mathbb{F}_q, \quad q \text{ prime}$$

Freeman, Scott, Teske: A taxonomy of pairing-friendly elliptic curves

security	construction	curve	k	d	e
128	BN (Ex. 6.8)	$a = 0$	12	6	2
	Ex. 6.10	$b = 0$	8	4	2
	Freeman (5.3)	$a, b \neq 0$	10	2	5
	Constr. 6.7+	$a, b \neq 0$	12	2	6
192	BN (Ex. 6.8)	$a = 0$	12	6	2
	KSS (Ex. 6.12)	$a = 0$	18	6	3
	KSS (Ex. 6.11)	$b = 0$	16	4	4
	Constr. 6.3+	$a, b \neq 0$	14	2	7
256	Constr. 6.6	$a = 0$	24	6	4
	Constr. 6.4	$b = 0$	28	4	7
	Constr. 6.24+	$a, b \neq 0$	26	2	13

Components of the pairing algorithm



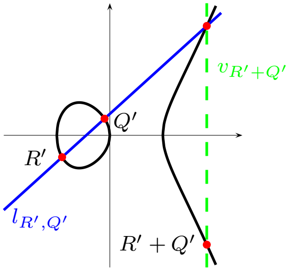
Pairings are computed with Miller's algorithm.

- Miller loop builds functions for $g_{Q'}(P)$ from DBL/ADD steps.

DBL	ADD	computation
$l_{R',R'}(P)$	$l_{R',Q'}(P)$	coefficients in $\mathbb{F}_{q^e}$, eval. at $P \in E(\mathbb{F}_q)$
$R' \leftarrow [2]R'$	$R' \leftarrow R' + Q'$	curve arith. $E(\mathbb{F}_{q^e})$
$f \leftarrow f^2 \cdot l_{R',R'}(P)$	$f \leftarrow f \cdot l_{R',Q'}(P)$	general squaring, special mult. in $\mathbb{F}_{q^k}$

- Final exponentiation to the power $(q^k - 1)/r$ needs arithmetic in the special subgroup μ_r of $\mathbb{F}_{q^k}^*$.

Choosing coordinates for pairings



- affine coordinates: ($\mathbb{F}_{q^e} = \mathbb{F}_q(\alpha)$)
  $R' + Q'$ and $l_{R',Q'}(P)$

$$\begin{aligned}
\lambda' &= (y_{R'} - y_{Q'})/(x_{R'} - x_{Q'}), \\
x_{R'+Q'} &= \lambda'^2 - x_{R'} - x_{Q'}, \\
y_{R'+Q'} &= \lambda'(x_{R'} - x_{R'+Q'}) - y_{R'}, \\
l_{R',Q'}(P) &= y_P - \alpha\lambda' x_P + \alpha^3(\lambda' x_{Q'} - y_{Q'}).
\end{aligned}$$

- DBL/ADD steps in affine coords need one inversion in $\mathbb{F}_{q^e}$,
- projective coordinates avoid the inversion by doing more of the other operations,
- finite field inversion in prime field $\mathbb{F}_q$ very expensive,
- for plain ECC over $\mathbb{F}_q$: projective always better,
- current speed records for pairings at 128-bit security level: projective formulas.

Affine vs. projective

$ab \neq 0$, $d = 2$, $e = k/2$

Cost for computing $[2]R'$, $l_{R',R'}(P)$ and $R' + Q'$, $l_{R',Q'}(P)$ resp.

	coord.	$\mathbf{M}_q$	$\mathbf{I}_{q^e}$	$\mathbf{M}_{q^e}$	$\mathbf{S}_{q^e}$	$\mathbf{add}_{q^e}$
DBL	affine	$k/2$	1	3	2	10
	proj.	$-$	$-$	3	11	23
ADD	affine	$k/2$	1	3	1	8
	proj.	$-$	$-$	8	6	23

Cost to avoid the inversion (assuming $\mathbf{S}_{q^e} \approx 0.8\mathbf{M}_{q^e}$):

- DBL: $9\mathbf{S}_{q^e} + 13\mathbf{add}_{q^e} - (k/2)\mathbf{M}_q > 6\mathbf{M}_{q^e}$
- ADD: $5\mathbf{M}_{q^e} + 5\mathbf{S}_{q^e} + 15\mathbf{add}_{q^e} - (k/2)\mathbf{M}_q > 8\mathbf{M}_{q^e}$

Affine vs. projective

$a = 0$, $d = 6 \mid k$

Cost for computing $[2]R'$, $l_{R',R'}(P)$ and $R' + Q'$, $l_{R',Q'}(P)$ resp.

	coord.	$\mathbf{M}_q$	$\mathbf{I}_{q^e}$	$\mathbf{M}_{q^e}$	$\mathbf{S}_{q^e}$	$\mathbf{add}_{q^e}$
DBL	affine	$k/6$	1	3	2	9
	proj.	$k/3$	$-$	2	7	21
ADD	affine	$k/6$	1	3	1	7
	proj.	$k/3$	$-$	11	2	8

Cost to avoid the inversion (assuming $\mathbf{S}_{q^e} \approx 0.8\mathbf{M}_{q^e}$):

- DBL: $(k/6)\mathbf{M}_q + 5\mathbf{S}_{q^e} + 12\mathbf{add}_{q^e} - 1\mathbf{M}_{q^e} > 3\mathbf{M}_{q^e}$
- ADD: $(k/6)\mathbf{M}_q + 8\mathbf{M}_{q^e} + 1\mathbf{S}_{q^e} + 1\mathbf{add}_{q^e} > 8\mathbf{M}_{q^e}$

Affine vs. projective

- If extra cost to avoid inversions $<$ cost to compute inversions $\Longrightarrow$ projective coordinates are the better choice.
- It all depends on the cost $\mathbf{I}_{q^e}$, or rather on the ratio

$$\mathbf{R}_{q^e} = \mathbf{I}_{q^e}/\mathbf{M}_{q^e}.$$

- For q prime, $\mathbf{I}_q >> \mathbf{M}_q$.

How large is $\mathbf{R}_{q^e}$? How small can it be made in pairing implementations?
Note:

- Pairings based on the ate pairing usually have $e > 1$, at least for higher security levels.
- Often, multiple pairings or products of pairings need to be computed.

Extension field inversions

Quadratic extension:

- $\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha)$ with $\alpha^2 = \omega \in \mathbb{F}_q^*$,
- $$\frac{1}{b_0 + b_1\alpha} = \frac{b_0 - b_1\alpha}{b_0^2 - b_1^2\omega} = \frac{b_0}{b_0^2 - b_1^2\omega} - \frac{b_1}{b_0^2 - b_1^2\omega}\alpha,$$
- $b_0^2 - b_1^2\omega = N(b_0 + b_1\alpha) \in \mathbb{F}_q$,
- compute inversion in $\mathbb{F}_{q^2}$ by inversion in $\mathbb{F}_q$ and some other operations

$$\mathbf{I}_{q^2} \leq \mathbf{I}_q + 2\mathbf{M}_q + 2\mathbf{S}_q + \mathbf{M}_{(\omega)} + \mathbf{sub}_q + \mathbf{neg}_q.$$

- Assume $\mathbf{M}_{q^2} \geq 3\mathbf{M}_q$ and $\mathbf{I}_{q^2} \leq \mathbf{I}_q + 6\mathbf{M}_q$ to get

$$\mathbf{R}_{q^2} = \mathbf{I}_{q^2}/\mathbf{M}_{q^2} \leq (\mathbf{I}_q/3\mathbf{M}_q) + 2 = \mathbf{R}_q/3 + 2.$$

Extension field inversions

Degree-ℓ extension:

- generalization of Itoh-Tsujii inversion,
- standard way for inversion in optimal extension fields,
- assume $\mathbb{F}_{q^\ell} = \mathbb{F}_q(\alpha)$ with $\alpha^\ell = \omega \in \mathbb{F}_q^*$,
- with $v = (q^\ell - 1)/(q-1) = q^{\ell-1} + \cdots + q + 1$, compute

$$\beta^{-1} = \beta^{v-1} \cdot \beta^{-v},$$

- for $\beta \in \mathbb{F}_{q^\ell}$, $\beta^v = N(\beta) \in \mathbb{F}_q$.

$$\mathbf{R}_{q^\ell} \leq \mathbf{R}_q / M(\ell) + C(\ell)$$

ℓ	2	3	4	5	6	7
$1/M(\ell)$	$1/3$	$1/6$	$1/9$	$1/13$	$1/17$	$1/22$
$C(\ell)$	3.33	4.17	5.33	5.08	6.24	6.05

Simultaneous inversions

Montgomery's n-th trick...

- Idea: To invert a_1 and a_2, compute $a_1 a_2$, then $(a_1 a_2)^{-1}$ and

$$a_1^{-1} = a_2 \cdot (a_1 a_2)^{-1}, \quad a_2^{-1} = a_1 \cdot (a_1 a_2)^{-1},$$

  replace $2\mathbf{I}$ by $1\mathbf{I} + 3\mathbf{M}$.

- In general for s inversions at once: compute $c_i = a_1 \cdot \cdots \cdot a_i$ for $2 \le i \le s$, then c_s^{-1} and

$$\begin{aligned} a_s^{-1} &= c_s^{-1} \cdot c_{s-1}, & c_{s-1}^{-1} &= c_s^{-1} \cdot a_s, \\ a_{s-1}^{-1} &= c_{s-1}^{-1} \cdot c_{s-2}, & c_{s-2}^{-1} &= c_{s-1}^{-1} \cdot a_{s-1}, \quad \ldots \end{aligned}$$

  replace $s\mathbf{I}$ by $1\mathbf{I} + 3(s-1)\mathbf{M}$.

- Average $\mathbf{I}/\mathbf{M}$ is

$$(s\mathbf{I})/(s\mathbf{M}) = \mathbf{I}/(s\mathbf{M}) + 3(s-1)/s \le \mathbf{R}/s + 3.$$

Affine coordinates for pairings

Affine coordinates can be better than projective

- if the used implementation has small $\mathbf{R}_q = \mathbf{I}_q / \mathbf{M}_q$,
- for ate pairings whenever e is large,
  - at high security levels (when k is large),
  - when high-degree twists are not being used ($d = 2$),
- for computing several pairings (or products of several pairings) at once on different point pairs.

Pairings based on Microsoft Research's bignum

optimal ate pairing on BN curves

Pairing implementation uses MSR bignum for

- base field arithmetic ($\mathbb{F}_p$) with Montgomery multiplication,
- extension fields based on MSR bignum field extensions,
- field inversions use norm trick as described before.

MSR bignum + pairings

- is a C implementation (with a little bit of assembly for mod mul in case of 256-bit prime fields),
- is not restricted to specific security level, curves, or processors,
- works under 32-bit and 64-bit Windows.

Pairings based on Microsoft Research's bignum

field arithmetic performance

Fields over 256-bit BN prime field with

- $p \equiv 3 \pmod 4$, i.e. $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$, $i^2 = -1$.

Timings on a 3.16 GHz Intel Core 2 Duo E8500, 64-bit Windows 7

	M		**S**		**I**		**I/M**
	cyc	μs	cyc	μs	cyc	μs	
$\mathbb{F}_p$	414	0.13	414	0.13	9469	2.98	22.87
$\mathbb{F}_{p^2}$	2122	0.67	1328	0.42	11426	3.65	5.38
$\mathbb{F}_{p^6}$	18544	5.81	12929	4.05	40201	12.66	2.17
$\mathbb{F}_{p^{12}}$	60967	19.17	43081	13.57	103659	32.88	1.70

Pairings based on Microsoft Research's bignum

pairings on a 256-bit BN curve

Timings on a 3.16 GHz Intel Core 2 Duo E8500,
64-bit Windows 7

operation	CPU cycles	time
Miller loop	7,572,000	2.36 ms
optimal ate pairing	14,838,000	4.64 ms
20 opt. ate at once (per pairing)	14,443,000	4.53 ms
product of 20 opt. ate (per pairing)	4,833,000	1.52 ms
EC scalar mult in G_1	2,071,000	0.64 ms
EC scalar mult in G_2'	8,761,000	2.74 ms