Pairings at High Security Levels

Michael Naehrig

Eindhoven University of Technology
michael@cryptojedi.org

DoE CRYPTODOC
Darmstadt, 21 November 2011

Pairings are efficient!

- …even at high security levels.
- They are really fast at the 128-bit level,
- and will soon be really fast at 192-bit and 256-bit levels.

A few numbers

openSSL	2048-bit RSA	sign	2.6 ms
		verify	0.08 ms
	4096-bit RSA	sign	18.8 ms
		verify	0.3 ms
	256-bit ECDH		0.7 ms
	256-bit ECDSA	sign	0.2 ms
	256-bit ECDSA	verify	0.8 ms
Beuchat et al. (2010)	optimal ate pairing on a 254-bit BN curve		0.8 ms

single core of an Intel Core i5 650 @ 3.2 GHz running 64-bit Ubuntu 11.10

Aranha et al. (2011) on a similar processor
optimal ate pairing on a 254-bit BN curve: 0.56 ms.

A little ancient history

Pairings on BN curves at roughly 128-bit security

2007	Devigili, Scott, Dahab 32-bit Intel Pentium IV @ 3.0 GHZ	23 ms
2008	Grabher, Großschädl, Page 64-bit Intel Core 2 Duo @ 2.4 GHz	6 ms
2008	Hankerson, Menezes, Scott 64-bit Intel Core 2 @ 2.4 GHz	4.2 ms
2010	N., Niederhagen, Schwabe 64-bit Intel Core 2 Duo @ 2.8 GHz	1.5 ms
2010	Beuchat et al. 64-bit Intel Core i7 @ 2.8 GHz	0.8 ms
2011	Aranha et al. 64-bit AMD Phenom II @ 3.0 GHz	0.5 ms

Why did pairings get so much faster?

- We found better curves,
- we found better functions,
- we got rid of unnecessary computations,
- we learned how to use more of the structure within the involved mathematical objects,
- computers got faster (well, not really),
- we tailored implementations to architecture specific instruction sets,
- we learned how to better choose curve parameters,
- we adjusted parameters and algorithms to the architecture.

A black-box view on pairings

$$e : G_1 \times G_2 \to G_3$$

- G_1 and G_2 are groups (of points on an elliptic curve),
- G_3 is a (multiplicative) group (of finite field elements),
- all groups have prime order r,
- e is bilinear, non-degenerate, efficiently computable

For a real implementation we need more details...

Optimal ate pairings

Typical setting at higher security levels:

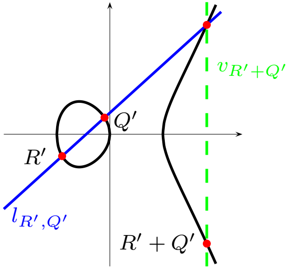
$$e : G_2' \times G_1 \to G_3, \quad (Q', P) \mapsto g_{Q'}(P)^{\frac{q^k-1}{r}}$$

- $G_1 = E(\mathbb{F}_q)[r]$, $G_2' = E'(\mathbb{F}_{q^e})[r]$, $G_3 = \mu_r \subseteq \mathbb{F}_{q^k}^*$,
- $E/\mathbb{F}_q$: 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 $\mathbb{F}_{q^k}^*$.

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 $(q^k - 1)/r$ can use arithmetic in special subgroups of $\mathbb{F}^*_{q^k}$.

Minimal requirements for security

- k should be small, but DLPs must be hard enough.

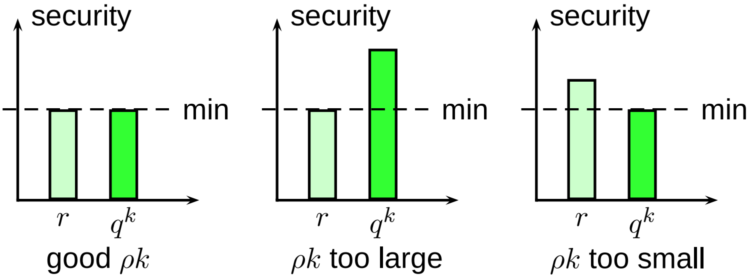
Security level (bits)	EC base point order r (bits)	Extension field size of q^k (bits)		ratio $\rho \cdot k$	
		NIST	ECRYPT	NIST	ECRYPT
112	224	2048	2432	9.1	10.9
128	256	3072	3248	12.0	12.7
192	384	7680	7936	20.0	20.7
256	512	15360	15424	30.0	30.1

NIST/ECRYPT II recommendations

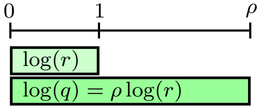
The ρ-value of E is defined as $\rho = \log(q)/\log(r)$.

Balanced security

- If ρk is too large, q^k is larger than necessary.
- If ρk is too small, r is larger than necessary.



- If ρ is too large, q is larger than necessary.



- Still, allowing larger ρ to get smaller k might be worth considering.

Pairing-friendly curves

Supersingular curves have small embedding degree ($k \leq 6$, large char $p > 3$: $k \leq 2$ only).

To find ordinary curves with small embedding degree:
Fix k, find primes r, p and an integer n with the following conditions:

- $n = p + 1 - t$, $|t| \leq 2\sqrt{q}$,
- $r \mid n$,
- $r \mid p^k - 1$,
- $t^2 - 4p = Dv^2 < 0$, $D, v \in \mathbb{Z}$, $D < 0$, $|D|$ small enough to compute the Hilbert class polynomial for $\mathbb{Q}(\sqrt{D})$.

Given such parameters, a corresponding elliptic curve over $\mathbb{F}_p$ can be constructed using the CM method.

Example 1: BN curves

(Barreto-N., 2005)

Find $u \in \mathbb{Z}$ such that

$$\begin{aligned} p = p(u) &= 36u^4 + 36u^3 + 24u^2 + 6u + 1, \\ n = n(u) &= 36u^4 + 36u^3 + 18u^2 + 6u + 1 \end{aligned}$$

are both prime. Then there exists an ordinary elliptic curve

- with equation $E : y^2 = x^3 + b,\ b \in \mathbb{F}_p$,
- $r = n = \#E(\mathbb{F}_p)$ is prime, i. e. $\rho \approx 1$,
- the embedding degree is $k = 12$, i.e. $\rho k \approx 12$,
- $t(u)^2 - 4p(u) = -3(6u^2 + 4u + 1)^2$,
- there exists a twist $E' : y^2 = x^3 + b/\xi$ over $\mathbb{F}_{p^2}$ of degree 6 with $n \mid \#E'(\mathbb{F}_{p^2})$.

Nicely fit the 128-bit security level.

Implementation-friendly BN curves

joint work with P. Barreto, G. Pereira, M. Simplicío

Efficient field arithmetic:

- Choose $p \equiv 3 \pmod 4$, i.e. $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$, $i^2 = -1$. Most efficient version of $\mathbb{F}_{p^2}$.
- Higher-degree extensions:

$$\mathbb{F}_{p^{2j}} = \mathbb{F}_{p^2}[X]/(X^j - \xi), \quad j \in \{2, 3, 6\}.$$

  Choose ξ small, e.g. $\xi = i + 1$. Reductions in extensions are nice.
- Choose p slightly smaller than a multiple of the word size, i.e. 254 instead of 256 bits. Can use lazy reduction techniques in field extensions.

Implementation-friendly BN curves

joint work with P. Barreto, G. Pereira, M. Simplicío

Miller loop and final exponentiation:

- Choose parameter u extremely sparse (in signed binary representation). Final expo profits since main cost is 3 exponentiations with u.
- Choose $6u+2$ (its abs. value $=$ degree of function g) as sparse as possible. Less non-zero entries means less ADD steps in the Miller loop.

Compact representation and twist:

- Choose $b = c^4 + d^6$, $c, d \in \mathbb{F}_p^*$. Then can take $\xi = c^2 + id^3$. This gives field extensions and twist $E' : y^2 = x^3 + (c^2 - id^3)$.
- Get compact generators for G_1 and G_2' by: $(-d^2, c^2)$ and $[2p-n](-di, c)$.

Implementation-friendly BN curves

joint work with P. Barreto, G. Pereira, M. Simplicío

Speed record example curve:

$$u = -(2^{62} + 2^{55} + 1),\ c = 1,\ d = 1$$

All other information is uniquely determined.
Then

- $p \equiv 3 \pmod 4$,
- p has 254 bits,
- $6u + 2 = -(2^{64} + 2^{63} + 2^{57} + 2^{56} + 2^2)$ has weight 5,
- $E : y^2 = x^3 + 2$, $P = (-1, 1)$,
- $\xi = 1 + i$,
- $E' : y^2 = x^3 + (1 - i)$, $Q' = [h](-i, 1)$.

Example 2: BLS curves

Barreto-Lynn-Scott, 2002

If $u \in \mathbb{Z}$, $u \equiv 1 \pmod 3$ such that

$$\begin{aligned} p &= p(u) = (u-1)^2(u^8 - u^4 + 1)/3 + u, \\ r &= r(u) = u^8 - u^4 + 1 \end{aligned}$$

are both prime. Then there exists an ordinary elliptic curve

- with equation $E : y^2 = x^3 + b,\ b \in \mathbb{F}_p$,
- $n = \#E(\mathbb{F}_p) = r \cdot (u-1)^2/3$,
- $\rho \approx 1.25$,
- the embedding degree is $k = 24$, i.e. $\rho k \approx 30$,
- $t(u)^2 - 4p(u) = -3\left((u-1)(2u^4-1)/3\right)^2$,
- there exists a twist $E' : y^2 = x^3 + b/\xi$ over $\mathbb{F}_{p^4}$ of degree 6 with $n \mid \#E'(\mathbb{F}_{p^4})$.

Nicely fit the 256-bit security level.

Implementation-friendly BLS curves

joint work with C. Costello, K. Lauter

Restrict the parameter u to the following congruences mod 72:

u $\pmod{72}$	$p(u)$ $\pmod{72}$	$n(u)$ $\pmod{72}$	E	E'
7	19	12	$y^2 = x^3 + 1$	$y^2 = x^3 \pm 1/v$
16	19	3	$y^2 = x^3 + 4$	$y^2 = x^3 \pm 4v$
31	43	12	$y^2 = x^3 + 1$	$y^2 = x^3 \pm v$
64	19	27	$y^2 = x^3 - 2$	$y^2 = x^3 \pm 2/v$

Efficient field arithmetic:

- $p \equiv 3 \pmod{4}$, i.e. $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$, $i^2 = -1$,
- Can use $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(v)$, $v^2 = -(i+1)$,
- $\mathbb{F}_{p^{24}} = \mathbb{F}_{p^4}(z)$, $z^6 = -v$,
- Choose p slightly smaller than multiple of word size.

Implementation-friendly BLS curves

joint work with C. Costello, K. Lauter

$u \pmod{72}$	$p(u) \pmod{72}$	$n(u) \pmod{72}$	E	E'
7	19	12	$y^2 = x^3 + 1$	$y^2 = x^3 \pm 1/v$
16	19	3	$y^2 = x^3 + 4$	$y^2 = x^3 \pm 4v$
31	43	12	$y^2 = x^3 + 1$	$y^2 = x^3 \pm v$
64	19	27	$y^2 = x^3 - 2$	$y^2 = x^3 \pm 2/v$

Miller loop and final exponentiation:

- Choose u extremely sparse.
- u is the degree in the Miller loop function g, and at the same time used in the final expo, main cost is 9 exponentiations with u.

Compact representation and twist:

- For each congruency class for u, can use fixed small b.
- Twist is automatically determined.

Implementation-friendly BLS curves

joint work with C. Costello, K. Lauter

Nice example curve for the 256-bit level:

$$u = 2^{63} - 2^{47} + 2^{38}, \quad b = 4$$

Then

- $p \equiv 3 \pmod 4$,
- p has 629 bits (10×64), r has 504 bits (8×64),
- $E : y^2 = x^3 + 4$,
- $E' : y^2 = x^3 + 4v$, where $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(v)$.

Thank you for your attention!

- G.C.C.F. Pereira, M.A. Simplicío Jr., M. Naehrig, P.S.L.M. Barreto: *A Family of Implementation-Friendly BN Elliptic Curves*, J. of Systems and Software, Vol. 84(8), pp. 1319–1326, 2011.
- C. Costello, K. Lauter, M. Naehrig: *Attractive Subfamilies of BLS Curves for Implementing High-Security Pairings*, INDOCRYPT 2011, LNCS Vol. 7107, 320–342, 2011.
- `http://www.cryptojedi.org`
- `michael@cryptojedi.org`

There will be a Pairing 2012 conference!

Watch out for the CFP!