BN curves revisited

Michael Naehrig

Technische Universiteit Eindhoven
michael@cryptojedi.org

Workshop on
Computational aspects of elliptic and hyperelliptic curves
Leuven, 28 October 2009

Notation

Take an elliptic curve E over $\mathbb{F}_q$ (of characteristic $p > 3$) with

- $n = \#E(\mathbb{F}_q) = q + 1 - t, \quad |t| \leq 2\sqrt{q}$,
- $r \mid n$ a large prime divisor of n ($r \nmid q$, $r \geq \sqrt{q}$),
- and embedding degree $k > 1$.

The embedding degree of E w.r.t. r is the smallest integer k with

$$r \mid q^k - 1.$$

Then

- k is the order of q modulo r,
- r-th roots of unity $\mu_r \subseteq \mathbb{F}_{q^k}^*$,
- $E[r] \subseteq E(\mathbb{F}_{q^k})$.

The Tate pairing

The Tate pairing

$$\begin{aligned} t_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/[r]E(\mathbb{F}_{q^k}) &\longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r, \\ (P, Q) &\longmapsto f_{r,P}(\mathcal{D}_Q). \end{aligned}$$

is a non-degenerate, bilinear map, where

- $f_{r,P}$ is a function with divisor $(f_{r,P}) = r(P) - r(\mathcal{O})$,
- $\mathcal{D}_Q \sim (Q) - (\mathcal{O})$ is a divisor with support disjoint from $\{\mathcal{O}, P\}$.

For $P \in E(\mathbb{F}_q)[r]$, we have $t_r(P, P) = 1$, take $Q \notin \langle P \rangle$.

The reduced Tate pairing

Assume $r^2 \nmid \#E(\mathbb{F}_q)$. The reduced Tate pairing is

$$\begin{aligned} t_r : G_1 \times G_2 &\rightarrow G_3, \\ (P, Q) &\mapsto f_{r,P}(Q)^{\frac{q^k-1}{r}} \end{aligned}$$

for cyclic groups (of prime order r)

- $G_1 = E(\mathbb{F}_{q^k})[r] \cap \ker(\phi_q - [1]) = E(\mathbb{F}_q)[r]$,
- $G_2 = E(\mathbb{F}_{q^k})[r] \cap \ker(\phi_q - [q])$,
- $G_3 = \mu_r \subset \mathbb{F}_{q^k}^*$.

We have $E(\mathbb{F}_{q^k})[r] = G_1 \oplus G_2$, and ϕ_q is the q-power Frobenius on E, $\phi_q(x, y) = (x^q, y^q)$.

Miller's algorithm (k even)

Input: $P \in G_1, Q \in G_2, r = (r_m, \ldots, r_0)_2$

Output: $t_r(P,Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}}$

$R \leftarrow P$, $f \leftarrow 1$

for $(i \leftarrow m-1;\ i \geq 0;\ i--)$ **do**

  $f \leftarrow f^2 \cdot l_{R,R}(Q)$

  $R \leftarrow [2]R$

  if $(r_i = 1)$ **then**

    $f \leftarrow f \cdot l_{R,P}(Q)$

    $R \leftarrow R + P$

  end if

end for

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

return f

Specific parameters for crypto

- k should be small,
- DLPs must be hard in all three groups G_1, G_2, and G_3,
- for efficiency reasons balance the security.

Security level (bits)	Extension field size of q^k (bits)	EC base point order r (bits)	ratio $\rho \cdot k$
	G_3	G_1, G_2	
80	1248	160	7.8
112	2432	224	10.9
128	3248	256	12.7
192	7936	384	20.7
256	15424	512	30.1

ECRYPT II recommendations (2009), $\rho = \log(q)/\log(r)$.

Pairing-friendly curves

Fix a suitable value for k and find primes r, p and a number n with the following conditions:

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

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

BN curves

(Barreto-N., 2005)

If $u \in \mathbb{Z}$ 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 $k = 12$.

BN curves are ideal for the 128-bit security level.

BN curves

Let Φ_k be the k-th cyclotomic polynomial. Then

- k is the embedding degree of E w.r.t. r,
- iff $r \mid \Phi_k(t-1)$.

Galbraith, McKee, Valença:

$$\Phi_{12}(6x^2) = n(x)n(-x),$$

with $n(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.

- Choose $n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$, $t(u) = 6u^2 + 1$.
- Then $p(u) = n(u) + t(u) - 1$,
- $t^2 - 4p(u) = -3(6u^2 + 4u + 1)^2$.

Distribution of prime pairs

(Bateman-Horn conjecture, 1962)

For large $N \in \mathbb{N}$, we heuristically expect the number of positive integers u with $1 \leq u \leq N$ for which $p(u), n(u)$ are both prime to be

$$Q(N) = \frac{C}{16} \int_2^N \frac{1}{(\log u)^2} du,$$

where

$$C = \prod_q \left[\left(1 - \frac{1}{q}\right)^{-2} \left(1 - \frac{w(q)}{q}\right) \right],$$

the product is taken over all primes q, and $w(q)$ is the number of solutions of $p(x)n(x) \equiv 0 \pmod{q}$.

Distribution of prime pairs

Heuristics

u_1	$u_2 - u_1 + 1$	$R(I)$	$\lfloor Q(I) \rfloor$	$r_I \cdot 10^2$	bits
1	72621324	250565	277429	0.34503	≤ 109
448869734239	4008033	5794	6142	0.14456	160
114911668072285	9977856	9952	10501	0.09974	192
29417389567148395	13774482	10011	10567	0.07268	224
7530851732698370160	17949966	10097	10481	0.05625	256
1927898043575355590045	22521445	9961	10343	0.04423	288
493541899155296768986804	27819263	10127	10311	0.03640	320
126346726183755979948643811	34034872	10109	10394	0.02970	352
32344761903041530875525863096	40428318	10048	10349	0.02485	384

- $R(I)$: number of prime pairs $(p(u), n(u))$ where $u \in I = [u_1, u_2]$,
- $Q(I)$: estimate for $R(I)$ from Bateman-Horn,
- $r_I = R(I)/(u_2 - u_1 + 1)$

“Constructing” BN curves

For a given desired bitsize of p and n

1. choose integers u of suitable size until $p(u)$ and $n(u)$ are prime and have the desired bitsize,
2. choose $b \in \mathbb{F}_p$, and a point $(x, y) \in \mathbb{F}_p^2$ on the curve $y^2 = x^3 + b$ until $[n](x, y) = \mathcal{O}$.

We can restrict to u with special properties in first step:

- e.g. u odd, then $p \equiv 3 \mod 4$,
- or u with very low Hamming weight, s.t. n has low Hamming weight.

Second step is done to choose the twist with the right order (out of 6 possibilities).

Nice properties

- Curve arithmetic is very efficient, since parameter $a = 0$ in curve equation $E : y^2 = x^3 + ax + b$.
- Often can choose $P = (1, 2) \in G_1$ ($E : y^2 = x^3 + 3$).
- Have efficient endomorphisms: e.g. if $Q \in G_2$ then

$$\phi_p(Q) = [6u^2]Q.$$

  Can use Gallant-Lambert-Vanstone or Galbraith-Scott methods.

Using twists of degree 6

There exists a twist $E'/\mathbb{F}_{p^2}$ of degree 6 with

- $n \mid E'(\mathbb{F}_{p^2})$,
- isomorphism

$$\psi : E' \to E, (x', y') \mapsto (\xi^{1/3}x', \xi^{1/2}y'),$$

where $E' : y^2 = x^3 + b/\xi$.

Thus we can represent G_2 by

$$G_2' = E'(\mathbb{F}_{p^2})[n]$$

and $\psi : G_2' \to G_2$ is a group isomorphism.

The R-ate pairing on BN curves

- The ate pairing (Hess, Smart, Vercauteren)

$$a_T : G_2 \times G_1 \to G_3,\ (Q, P) \mapsto f_{T,Q}(P)^{(q^k-1)/r}$$

  comes from the Tate pairing on $G_2 \times G_1$, has shorter loop ($T = t - 1$) in Miller's algorithm.
- The R-ate pairing (Lee, Lee, Park)

$$R(Q,P) = \left(f_{a,Q}(P)(f_{a,Q}(P)l_{[a]Q,Q}(P))^p \cdot l_{\phi_p([a]Q+Q),[a]Q}(P)\right)^{(p^{12}-1)/n},$$

  has even shorter loop ($a = 6u + 2$).

What about the prime field arithmetic?

- Improving the arithmetic in $\mathbb{F}_p$ improves the whole pairing computation.
- Can we use the special form of p to make things faster?

What about the prime field arithmetic?

- Improving the arithmetic in $\mathbb{F}_p$ improves the whole pairing computation.
- Can we use the special form of p to make things faster?
- Yes, see Fan, Vercauteren, Verbauwhede (improve modular multiplication in hardware).

What about the prime field arithmetic?

- Improving the arithmetic in $\mathbb{F}_p$ improves the whole pairing computation.
- Can we use the special form of p to make things faster?
- Yes, see Fan, Vercauteren, Verbauwhede (improve modular multiplication in hardware).

The following is work in progress with P. Schwabe (TU/e).
...there is no "real" implementation yet
to see how efficient it is.

Arithmetic modulo p

(Following ideas in Bernstein's Curve25519 paper)

Consider the ring

$$R = \mathbb{Z}[x] \cap \overline{\mathbb{Z}}[\sqrt{6}ux].$$

and the element

$$\begin{aligned} P &= 36u^4x^4 + 36u^3x^3 + 24u^2x^2 + 6ux + 1 \\ &= (\sqrt{6}ux)^4 + \sqrt{6}(\sqrt{6}ux)^3 + 4(\sqrt{6}ux)^2 + \sqrt{6}(\sqrt{6}ux) + 1. \end{aligned}$$

Then $P(1) = p$ and

- $R \to \mathbb{F}_p,\ F \mapsto F(1) \mod p$,
- $R/(P) \to \mathbb{F}_p,\ F + (P) \mapsto F(1) \mod p$

are ring homomorphisms.

Arithmetic modulo p

Representing integers

Represent $f \in \mathbb{F}_p$ by a polynomial $F \in R$ as

$$\begin{aligned} F &= f_0 + f_1\sqrt{6}(\sqrt{6}ux) + f_2(\sqrt{6}ux)^2 + f_3\sqrt{6}(\sqrt{6}ux)^3 \\ &= f_0 + f_1(6ux) + f_2(6u^2x^2) + f_3(36u^3x^3) \end{aligned}$$

such that $F(1) = f$.

$$f \leftrightarrow [f_0, f_1, f_2, f_3]$$

Arithmetic modulo p

Multiplication

$$
\begin{aligned}
f = & \quad f_0 + f_1\sqrt{6}(\sqrt{6}ux) + f_2(\sqrt{6}ux)^2 + f_3\sqrt{6}(\sqrt{6}ux)^3, \\
g = & \quad g_0 + g_1\sqrt{6}(\sqrt{6}ux) + g_2(\sqrt{6}ux)^2 + g_3\sqrt{6}(\sqrt{6}ux)^3
\end{aligned}
$$

Then

$$
\begin{aligned}
fg &= h_0 + h_1\sqrt{6}(\sqrt{6}ux) + h_2(\sqrt{6}ux)^2 + h_3\sqrt{6}(\sqrt{6}ux)^3 \\
&+ h_4(\sqrt{6}ux)^4 + h_5\sqrt{6}(\sqrt{6}ux)^5 + h_6(\sqrt{6}ux)^6
\end{aligned}
$$

$$
\begin{aligned}
h_0 &= f_0g_0 \\
h_1 &= f_0g_1 + f_1g_0 \\
h_2 &= f_0g_2 + 6f_1g_1 + f_2g_0 \\
h_3 &= f_0g_3 + f_1g_2 + f_2g_1 + f_3g_0 \\
h_4 &= 6f_1g_3 + f_2g_2 + 6f_3g_1 \\
h_5 &= f_2g_3 + f_3g_2 \\
h_6 &= 6f_3g_3
\end{aligned}
$$

Arithmetic modulo p

Degree reduction

Reduce modulo P:

$$
\begin{aligned}
(\sqrt{6}ux)^6 &= -\sqrt{6}(\sqrt{6}ux)^5 - 4(\sqrt{6}ux)^4 - \sqrt{6}(\sqrt{6}ux)^3 - (\sqrt{6}ux)^2 \\
\sqrt{6}(\sqrt{6}ux)^5 &= -6(\sqrt{6}ux)^4 - 4\sqrt{6}(\sqrt{6}ux)^3 - 6(\sqrt{6}ux)^2 - \sqrt{6}(\sqrt{6}ux) \\
(\sqrt{6}ux)^4 &= -\sqrt{6}(\sqrt{6}ux)^3 - 4(\sqrt{6}ux)^2 - \sqrt{6}(\sqrt{6}ux) - 1
\end{aligned}
$$

$$
\begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \end{bmatrix}
\rightarrow
\begin{bmatrix} h_0 \\ h_1 \\ h_2 - h_6 \\ h_3 - h_6 \\ h_4 - 4h_6 \\ h_5 - h_6 \\ 0 \end{bmatrix}
\rightarrow
\begin{bmatrix} h_0 \\ h_1 - (h_5 - h_6) \\ h_2 - h_6 - 6(h_5 - h_6) \\ h_3 - h_6 - 4(h_5 - h_6) \\ h_4 - 4h_6 - 6(h_5 - h_6) \\ 0 \\ 0 \end{bmatrix}
\cdots
\begin{bmatrix} h_0 - h_4 + 6h_5 - 2h_6 \\ h_1 - h_4 + 5h_5 - h_6 \\ h_2 - 4h_4 + 18h_5 - 3h_6 \\ h_3 - h_4 + 2h_5 + h_6 \\ 0 \\ 0 \\ 0 \end{bmatrix}
$$

Hm...

- To reduce coefficients need to reduce mod $6u$ and u.
- When p has 256 bits, $6u$ is larger than 64 bits.
- Probably no advantage over Montgomery multiplication/reduction.

Arithmetic modulo p

Now assume $u = v^3$ for some $v \in \mathbb{Z}$. Let $\delta = \sqrt[6]{6}$, then

$$(\delta v x)^3 = \sqrt{6} u x^3.$$

Consider

$$R = \mathbb{Z}[x] \cap \overline{\mathbb{Z}}[\delta v x].$$

and the element

$$\begin{aligned} P &= 36u^4x^{12} + 36u^3x^9 + 24u^2x^6 + 6ux^3 + 1 \\ &= 36v^{12}x^{12} + 36v^9x^9 + 24v^6x^6 + 6v^3x^3 + 1 \\ &= (\delta v x)^{12} + \delta^3(\delta v x)^9 + 4(\delta v x)^6 + \delta^3(\delta v x)^3 + 1. \end{aligned}$$

Arithmetic modulo p

Representing integers with 12 coefficients

Let $\alpha = \delta v x$.
Represent $f \in \mathbb{F}_p$ by a polynomial $F \in R$ as

$$\begin{aligned} F &= f_0 + f_1\delta^5\alpha + f_2\delta^4\alpha^2 + f_3\delta^3\alpha^3 + f_4\delta^2\alpha^4 + f_5\delta\alpha^5 \\ &+ f_6\alpha^6 + f_7\delta^5\alpha^7 + f_8\delta^4\alpha^8 + f_9\delta^3\alpha^9 + f_{10}\delta^2\alpha^{10} + f_{11}\delta\alpha^{11} \\ &= f_0 + f_1(6vx) + f_2(6v^2x^2) + f_3(6v^3x^3) \\ &+ f_4(6v^4x^4) + f_5(6v^5x^5) + f_6(6v^6x^6) + f_7(36v^7x^7) \\ &+ f_8(36v^8x^8) + f_9(36v^9x^9) + f_{10}(36v^{10}x^{10}) + f_{11}(36v^{11}x^{11}) \end{aligned}$$

such that $F(1) = f$.

$$f \leftrightarrow [f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}]$$

Arithmetic modulo p

Multiplying integers with 12 coefficients

Multiplication of two elements

$$\begin{aligned} f &\leftrightarrow [f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}] \\ g &\leftrightarrow [g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_{10}, g_{11}] \end{aligned}$$

gives 23 coefficients. Reduce the degree of the polynomial via

$$\begin{aligned} (\delta v x)^{12} &= -\delta^3(\delta v x)^9 - 4(\delta v x)^6 - \delta^3(\delta v x)^3 - 1, \\ \delta^5(\delta v x)^{13} &= -6\delta^2(\delta v x)^{10} - 4\delta^5(\delta v x)^7 - 6\delta^2(\delta v x)^4 - \delta^5(\delta v x), \\ &\vdots \\ \delta^2(\delta v x)^{22} &= -\delta^5(\delta v x)^{19} - 4\delta^2(\delta v x)^{16} - \delta^5(\delta v x)^{13} - \delta^2(\delta v x)^{10}. \end{aligned}$$

Arithmetic modulo p

Advantages

We hope it will be efficient (on 64-bit processor) since

- coefficients fit in double precision floating-point numbers,
- even after multiplication,
- even after degree reduction,
- we allow negative numbers as well,
- coefficient reduction can be done by multiplying floating point numbers,
- can use SIMD instructions, i.e. do two such multiplications per cycle.

Arithmetic modulo p

Advantages

We hope it will be efficient (on 64-bit processor) since

- coefficients fit in double precision floating-point numbers,
- even after multiplication,
- even after degree reduction,
- we allow negative numbers as well,
- coefficient reduction can be done by multiplying floating point numbers,
- can use SIMD instructions, i.e. do two such multiplications per cycle.

Now we need a good implementation to check ...

Thanks for your attention

- Database and web interface to get and compute parameters of BN curves:

  http://www.ti.rwth-aachen.de/research/cryptography/bncurves.php
- C-Implementation of several pairings on BN curves: http://www.cryptojedi.org/crypto

michael@cryptojedi.org