JNCF — January 16-20, 2017, Luminy

A brief overwiev of pairings

Razvan Barbulescu

CNRS and IMJ-PRG

Notations

Elliptic curves

- equation (in Edwards form): $x^2 + y^2 = 1 + dx^2y^2$ where $c, d \in K$ and $cd(1 - c^4d) \neq 0$
- group law : $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2+x_2y_1}{c(1+dx_1x_2y_1y_2)}, \frac{y_1y_2-x_1y_2}{c(1-dx_1x_2y_1y_2)})$
- cardinality (Hasse) :

$$|\#\{(x : y : z) \in \mathbb{P}^2(\mathbb{F}_q) : x^2z^2 + y^2z^2 = z^4 + dx^2y^2\} - q| \leq 2\sqrt{q}$$

- scalar product : for any r and P , $[r]P = P + \cdots + P$ (r times)

Finding elliptic curves

Use in cryptography

- Elliptic curves are used in all group-based cryptography : ElGamal, Diffie-Hellman, DSA. They are standardized since 1999.
- Curves are constructed as follows
  - select the good size
  - pick a random prime q of the good size
  - pick random parameters c and d which define a curve E
  - use the Schoof algorithm to compute the cardinality r
  - test primality of r (if desired test primality of $q + 1 - r$)

Pairings

Definition

- E an elliptic curve over a field K
- r an integer
- P(x,y) a point on E so that $[r]P = (0,1)$ (neutral element).
- μ a unit of Φ_r in the algebraic closure of K

$$\begin{array}{rccl} e_{E,r,P,\mu}: & \frac{\mathbb{Z}}{r\mathbb{Z}}P \times \frac{\mathbb{Z}}{r\mathbb{Z}}P & \to & \mu^{\mathbb{Z}/r\mathbb{Z}} \\ & ([a]P,[b]P) & \mapsto & \mu^{ab}. \end{array}$$

Properties of a pairing e

Non-degenerate bilinear map.

Computations of pairings

1. Theorem of Weil (1948): pairings can be defined in terms of divisors, without computing a,b
2. Algorithm of Miller (1985): related to a "fast exponentiation" and has a polynomial complexity

Three-party Diffie-Hellman

Problem

Alice, Bob and Carol use a public elliptic curve E and a pairing e with respect to a point P. Each of the participants broadcast simultaneously an information in a public channel. How can they agree on a common key ?

Joux's protocol (2000)

1. Simultaneously, each participant generates a random integer in $[0, r-1]$ and broadcasts a multiple of P:
   - Alice generates a and computes $[a]P$;
   - Bob generates b and computes $[b]P$;
   - Carol generates c and computes $[c]P$;
2. Simultaneously, each participant computes the pairing of the received information and computes the common key:
   - Alice computes $e([b]P, [c]P)^a$;
   - Bob computes $e([c]P, [a]P)^b$;
   - Carol computes $e([a]P, [b]P)^c$;

Common secret key: μ^{abc}.

Embedding degree

Definition

Given E, K and r the embedding degree is the degree of the extension of K which contains an r-th root of unity.

Pariring friendly elliptic curves

Let q be selected so that the discrete logarithm problem is just hard enough in the elliptic curve. Then

- if k is too large, computations are slow (arithmetic in $\mathbb{F}_{q^k}$)
- if k is too small, the discrete logrithm in $\mathbb{F}_{q^k}$ is too easy and the pairing is not safe.

Key sizes

security (bits)	key size RSA $\log_2(q^k)$	key size ECDSA $\log_2 r \approx \log_2 q$	quotient
80	1024	160	6
128	3072	256	12
256	15360	512	30

We need curves such that

- cardinality $r = c \times \text{prime}$ with $c \leq 10$
- k donné

CM method

Motivation

Theorem of Köblitz and Balusubramanian : a proportion of $1-o(1)$ of the curves defined over $\mathbb{F}_q$ have $k \approx q$.

$\boxed{\text{We cannot take random curves, we must find families}}$

Constructing pairings

Given an embedding degree k we construct a pairing-friendly curve E as follows:

1. find q, r and t subject to the CM equations in next slide; they are
   - $\mathbb{F}_q$ is the field of coefficients
   - E has $q+1-t$ points
   - E has a subgroup of order r.

2. apply the complex method (Morain 1990) to construct a curve E corresponding to q,r,t. The cost is $O(h_D^{2+\epsilon})$ where h_D is the class number of $\mathbb{Q}(\sqrt{D})$ (for a random D, $h_D \simeq \sqrt{D}$).

CM equations

k given but some exceptions are allowed

Two primes q and r and a square-free integer D satisfy the CM conditions if

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Super-singular curves

Idea

Take $t = 0$ and $k = 2$. Indeed,

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$ (true for all r because $\Phi_2(-1) = 0$)
2. $q + 1 - t \equiv 0 \pmod{r}$ (true for any divisor r of $q+1$)
3. $\exists y,\ 4q = Dy^2 + t^2$ (true for any q)

Limits

- if $q = 2$ or $q = 3$ we can have $k \in \{1, 2, 3, 4, 6\}$ (but small characteristic and hence subject to the quasi-polynomial time attack)
- if $q \geq 5$ we has two possibilities
  - $k = 2$ OK
  - $k = 1$ but $q = p^{2s}$ and E or its twist are isomorphic to a pairing of embedding degree 2 defined over p^s $(\mathbb{F}_{(p^{2s})^1 = \mathbb{F}_{(p^s)^2}})$.

Cocks-Pinch

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

Cocks-Pinch

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $Dy^2 + (t-2)^2 \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation

Cocks-Pinch

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod r}$
2. $Dy^2 + (t-2)^2 \equiv 0 \pmod r \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2) \equiv 0(r)$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation
2. select r so that $r \equiv 1 \mod k$ and $(\frac{-D}{r}) = 1$

Cocks-Pinch

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod{r}}$
2. $\cancel{Dy^2 + (t-2)^2 \equiv 0 \pmod{r} \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2)) \equiv 0 \pmod{r}}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation
2. select r so that $r \equiv 1 \mod k$ and $(\frac{-D}{r}) = 1$
3. solve (2) for y

Cocks-Pinch

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod{r}}$
2. $\cancel{Dy^2 + (t-2)^2 \equiv 0 \pmod{r} \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2)) \equiv 0 \pmod{r}}$
3. $\cancel{\exists y,\ 4q = Dy^2 + t^2}$

Method

1. replace (2) by an equivalent equation
2. select r so that $r \equiv 1 \mod k$ and $(\frac{-D}{r}) = 1$
3. solve (2) for y
4. solve (3) for q

Dupont-Enge-Morain

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q+1-t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

Dupont-Enge-Morain

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $a + (t-2)^2 \equiv 0 \pmod{r}$ where $a = Dy^2$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation

Dupont-Enge-Morain

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod r}$
2. $\cancel{a+(t-2)^2 \equiv 0 \pmod r \text{ where } a = Dy^2}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation
2. compute $R(a) = \mathrm{Res}_t(\Phi_k(t-1), a+(t-2)^2)$; enumerate a's and take
   - r a prime factor of $R(a)$
   - compute $\gcd(\Phi_k(t-1) \bmod r, a+(t-2)^2 \bmod r)$ and obtain t if it is linear

Dupont-Enge-Morain

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod r}$
2. $\cancel{a+(t-2)^2 \equiv 0 \pmod r \text{ where } a = Dy^2}$
3. $\cancel{\exists y,\ 4q = Dy^2 + t^2}$

Method

1. replace (2) by an equivalent equation
2. compute $R(a) = \mathrm{Res}_t(\Phi_k(t-1), a+(t-2)^2)$; enumerate a's and take
   - r a prime factor of $R(a)$
   - compute $\gcd(\Phi_k(t-1) \bmod r, a+(t-2)^2 \bmod r)$ and obtain t if it is linear
3. solve (3) for q

Sparse families (e.g. MNT)

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method when $\varphi(k) = 2$ (example when $k = 3$)

Sparse families (e.g. MNT)

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod{r}}$
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method when $\varphi(k) = 2$ (example when $k = 3$)

1. put $r = \Phi_k(t-1)$, which satisfies (1)

Sparse families (e.g. MNT)

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod r}$
2. $\cancel{q+1-t \equiv 0 \pmod r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method when $\varphi(k) = 2$ (example when $k = 3$)

1. put $r = \Phi_k(t-1)$, which satisfies (1)
2. put $q = r + t - 1$, which satisfies (2)

Sparse families (e.g. MNT)

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod r}$
2. $\cancel{q+1-t \equiv 0 \pmod r}$
3. generalized Pell equation (e.g. $X^2 - 3Dy^2 = 24$, where $X = 6x \pm 3$)

Method when $\varphi(k) = 2$ (example when $k = 3$)

1. put $r = \Phi_k(t-1)$, which satisfies (1)
2. put $q = r + t - 1$, which satisfies (2)
3. put $t = t(x)$, t linear, and note that this forces $q = q(x)$, quadratic polynomial q (e.g. $t(x) = -1 \pm 6x$ and $q(x) = 12x^2 - 1$). This transforms (3) into a generalized Pell equation

Sparse families (e.g. MNT)

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod{r}}$
2. $\cancel{q+1-t \equiv 0 \pmod{r}}$
3. ~~generalized Pell equation (e.g. $X^2 - 3Dy^2 = 24$, where $X = 6x \pm 3$)~~

Method when $\varphi(k) = 2$ (example when $k = 3$)

1. put $r = \Phi_k(t-1)$, which satisfies (1)
2. put $q = r + t - 1$, which satisfies (2)
3. put $t = t(x)$, t linear, and note that this forces $q = q(x)$, quadratic polynomial q (e.g. $t(x) = -1 \pm 6x$ and $q(x) = 12x^2 - 1$). This transforms (3) into a generalized Pell equation
4. solve the generalized Pell equation to get y and x, and therefor q

Was generalized by Freeman to $k = 10$, where $\varphi(k) = 4$

Complete families (e.g. BN)

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod r$
2. $q+1-t \equiv 0 \pmod r$
3. $\exists y,\ 4q = Dy^2 + t^2$

Complete families (e.g. BN)

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $Dy^2 + (t-2)^2 \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

1. replace (2) by an equivalent equation

Complete families (e.g. BN)

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod r}$
2. $Dy^2 + (t-2)^2 \equiv 0 \pmod r \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2) \equiv 0(r)$
3. $\exists y,\ 4q = Dy^2 + t^2$

1. replace (2) by an equivalent equation
2.
   - select $r(x) \in \mathbb{Q}[x]$ so that $\mathbb{Q}[x]/r(x)$ which contains a root of $x^2 - D$ and $\Phi_k(x)$
   - take $t = t(x)$ to be such that $t-1$ is a kth root of unity mod $r(x)$

Complete families (e.g. BN)

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod{r}}$
2. $\cancel{Dy^2 + (t-2)^2 \equiv 0 \pmod{r} \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2)) \equiv 0 \pmod{r}}$
3. $\exists y,\ 4q = Dy^2 + t^2$

1. replace (2) by an equivalent equation
2.
   - select $r(x) \in \mathbb{Q}[x]$ so that $\mathbb{Q}[x]/r(x)$ which contains a root of $x^2 - D$ and $\Phi_k(x)$
   - take $t = t(x)$ to be such that $t - 1$ is a kth root of unity mod $r(x)$
3. put $y = t(x)/\sqrt{-D}$ which satisfies (2)

Complete families (e.g. BN)

CM equations

1. $\cancel{\Phi_k(t-1) \equiv 0 \pmod{r}}$
2. $\cancel{Dy^2 + (t-2)^2 \equiv 0 \pmod{r} \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2)) \equiv 0 \pmod{r}}$
3. $\cancel{\exists y,\ 4q = Dy^2 + t^2}$

1. replace (2) by an equivalent equation
2. - select $r(x) \in \mathbb{Q}[x]$ so that $\mathbb{Q}[x]/r(x)$ which contains a root of $x^2 - D$ and $\Phi_k(x)$
   - take $t = t(x)$ to be such that $t - 1$ is a kth root of unity mod $r(x)$
3. put $y = t(x)/\sqrt{-D}$ which satisfies (2)
4. solve (3) for q

Note that we generate a large number of elliptic curves very quickly.

Discrete logarithm problem (DLP)

DLP

Given P and $[a]P$ find P.

Generic algorithm

A combination of Pohlig-Hellman reduction and Pollard's rho solves DLP in a generic group G after $O(\sqrt{r})$ operations, where r is the largest prime factor of $\#G$.

Relation to pairings

A pairing $e : \langle P \rangle \times \langle P \rangle \to K(\mu)$ is safe only if

1. DLP in $E[r]$ is hard; (DLP on elliptic curves) **if** $\log_2 \#G = n$**, cost=**$2^{\frac{n}{2}}$
2. DLP in $K(\mu)$ is hard. (DLP in finite fields) **if** $\log_2 \#K(\mu) = n$**, cost**$\approx \exp(\sqrt[3]{n})$

Types of pairing friendly families

Possible target fields $K(\mu)$:

1. (supersingular) $\mathbb{F}_{2^{4\cdot n}}$ and $\mathbb{F}_{3^{6\cdot n}}$ (fastest)
2. (complete families: BN) $\mathbb{F}_{p^k}$ with p of polynomial form, e.g. $p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$
3. (Pinch-Cocks) arbitrary $\mathbb{F}_{p^k}$ much slower ($log_2 q \approx 2\log_2 r$)

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$7^{5} \bmod p \;=\; 4706 = 2 \cdot 13 \cdot 181$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$
\begin{aligned}
7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\
7^6 \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23
\end{aligned}
$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$\begin{aligned} 7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\ 7^6 \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23 \\ 7^7 \bmod p &= 675 = 3^3 \cdot 5^2 \end{aligned}$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$
\begin{aligned}
7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\
7^6 \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23 \\
7^7 \bmod p &= 675 = 3^3 \cdot 5^2
\end{aligned}
$$

The last relation gives:

$$7 = 3 \log_7 3 + 2 \log_7 5$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$\begin{aligned} 7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\ 7^6 \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23 \\ 7^7 \bmod p &= 675 = 3^3 \cdot 5^2 \\ 7^8 \bmod p &= \ldots \end{aligned}$$

The last relation gives:

$$\begin{aligned} 7 &= 3 \log_7 3 + 2 \log_7 5 \\ 25 &= 8 \log_7 2 + 1 \log_7 3 \\ 42 &= 6 \log_7 2 + 2 \log_7 5. \end{aligned}$$

DLP: an example (2)

Thanks to the Pohlig-Hellman reduction

we do the linear algebra computations modulo $\ell = 11$.

Linear algebra computations

We have to find the unknown $\log_7 2$, $\log_7 3$ and $\lg_7 5$ in the equation

$$\begin{pmatrix} 0 & 3 & 2 \\ 8 & 1 & 0 \\ 6 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} \log_7 2 \\ \log_7 3 \\ \log_7 5 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 25 \\ 42 \end{pmatrix} \mod 11.$$

Conjecture

The matrix obtained by the technique above has maximal rank.

We can drop all conjectures by modifying the algorithm, but this variant is fast and, even if the matrix has smaller rank we can find logs.

Solution

We solve to obtain $\log_7 2 \equiv 0 \mod 11$; $\log_7 3 \equiv 3 \mod 11$ and $\log_7 5 \equiv 10 \mod 11$. For this small example we can also use Pollard's rho method and obtain that

$$\log_7 3 = 8869 \equiv 3 \mod 11.$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$7^3 151 \bmod p \; = \; 3389$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$\begin{aligned} 7^3 151 \bmod p &= 3389 \\ 7^4 151 \bmod p &= 11622 = 2 \cdot 3 \cdot 13 \cdot 149 \end{aligned}$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$\begin{aligned} 7^3 151 \bmod p &= 3389 \\ 7^4 151 \bmod p &= 11622 = 2 \cdot 3 \cdot 13 \cdot 149 \\ 7^5 151 \bmod p &= 8748 = 2^2 \cdot 3^7 \end{aligned}$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$\begin{aligned} 7^3 151 \bmod p &= 3389 \\ 7^4 151 \bmod p &= 11622 = 2 \cdot 3 \cdot 13 \cdot 149 \\ 7^5 151 \bmod p &= 8748 = 2^2 \cdot 3^7 \end{aligned}$$

The discrete logarithms of the two members are equal:

$$5 + \log_7(151) = 2 \log_7 2 + 7 \log_7 3.$$

We find $\log_7(151) \equiv 3 \mod 11$.

Remark

This part of the computations is independent of the relation collection and linear algebra stages. It is called individual logarithm stage.

Small characteristic

The quasi polynomial (B, Gaudry, Joux, Thomé 2014)

- special choice of definition of $\mathbb{F}_{2^n}$ (Joux 2013)
- special choice of smoothness candidates $(aP+b)^q-(aP+b)$
- special smoothness base : $\{P+\lambda \mid \lambda \in \mathbb{F}_{q^2}\}$

Consequences

- $\mathbb{F}_{2^n}$ broken asymptotocally in time $n^{O(\log n)}$
- real-life cryptographic examples of 128 bits of security broken by Granger Kleinjung Zumbragel (2014) in char 2 and by Adj, Menezes Olivieira Rodriguez (2016) in char 3
- since 2013 ENISA standards forbid cryptosystems based on these two cases

The case $\mathbb{F}_{p^n}$ where p has polynomial form

(S)exTNFS

- (TNFS; B, Gaudry, Kleinjung 2015) in NFS replace $\mathbb{Q}$ by a number field of degree a divisor of n
- (exTNFS: Kim and B 2016) combine in TNFS with a method of Joux and Pierrot 2013

(S)exTNFS

- complexity changed from T to $T^{\frac{1}{\sqrt[3]{2}}}$
- key sizes of ENISA repport are incorrect, they must be doubled

The case $\mathbb{F}_{p^n}$ where p is arbitrary

New methods of polynomial selection for NFS

- (Joux Lercier Smart Vercauteren 2006) adapted NFS from $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$ by modifying the polynomial selection
- (B Gaudry Guillevic Morain 2015) proposed a better method : conjugation method (applications of LLL)

exTNFS with conjugation method

- complexity changed from T to $T^{\frac{1}{\sqrt[3]{1.33}}}$
- key sizes of ENISA repport are incorrect, they must be multiplied by 1.33

Conclusion

Summary

property of pairing-friendly curves	attack which exploits it
small $\varphi(k)$	exTNFS for composite k
SNFS q	SNFS variant of exTNFS

Unaffected pairings

1. Cocks-Pinch when $k = 5, 7$, etc (slow)
2. Menezes' $k = 1$ curves (slow)

Quotation

"Is it the beginning of the end of pairings ?" (referee of Crypto 2016)