Bordeaux — November 22, 2016

A brief overwiev of pairings

Razvan Barbulescu
CNRS and IMJ-PRG

Plan of the lecture

- Pairings
- Pairing-friendly curves
- Progress of NFS attacks
- Consequences

Definition

Definition

Let r be an integer, E an elliptic curve with coefficients in a field K, P a point on E with coefficients in K so that $[r]P = 0$ (where $[r]P := P + \cdots + P = 0$, r times). Given μ a solution of $\mu^r = 1$ in an extension of K, the pairing of $E \times E$ with respect to r, P and μ is the map

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

Properties of a pairing e

1. $e([\lambda]P, Q) = e(P, Q)^{\lambda} = e([\lambda]Q, P)$
2. $e([a]P, [b_1]P + [b_2]P) = e([a]P, [b_1]P) \cdot e([a]P, [b_2]P)$
3. if a is such that $e([a]P, [b]P) = 1$ for all b then $a = 0$.

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

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}.

Discrete logarithm

Definition

Given a finite group G generated by an element P of order r, we call discrete logarithm of P^a (or $[a]P$ in additive notation) in base P the integer $a \in [0, r-1]$. The discrete logarithm problem (DLP) consists of computing the discrete logarithm of any element.

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**$\approx \exp(\sqrt[3]{N})$

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:

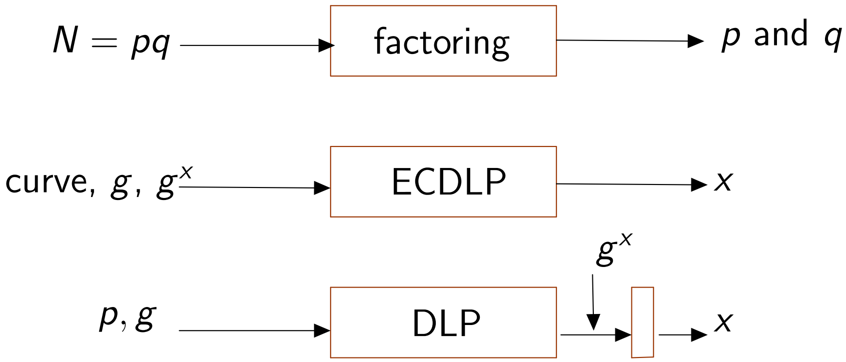
$$5 + \log_7(151) = 2 \log_7 2 + 7 \log_7 3.$$

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.

Comparison among cryptographic primitives



- **elliptic curves:** can be hard-coded without loss of security
- **finite fields:** if hard-coded, an attacker can do precomputations, so the cost of DLP becomes equal to that of individual logarithm.

LogJam

Records and precise estimations

bitsize	common part	possible for	individual logarithm
512	7.7 core-years	everybody	10 min
768	4.5k core-years	academic level	2 days
1024	35M core-years	state level	30 days

LogJam

Records and precise estimations

bitsize	common part	possible for	individual logarithm
512	7.7 core-years	everybody	10 min
768	$4.5k$ core-years	academic level	2 days
1024	$35M$ core-years	state level	30 days

When default parameters are given

Among the servers using 512-bit primes (Table 1 Logjam paper):

- 82% used the same prime;
- 10% more used a second prime;
- 8% others used a total of 463 primes.

Similar proportions occur for 1024 and 2048-bit primes, and ECDSA.

Pairings are vulnerable to LogJam so we must produce pairing-friendly curves on the fly.

Computing pairings

Some algorithms for Tate-Lichtenbaum

- Miller (see Miller 1986)
- Ate (see Barreto-Galbraith-O hEigeataigh and Scott 2007)
- Eta (see Hess, Smart and Vercauteren 2006)

Cost

Depending on the each curve but it grows with

- $\log_2 r$,
- $\log_2(q^k)$.

Cryptographic sizes

A priori key sizes

security (bits)	key size RSA	key size ECDSA	quotient
80	1024	160	6
128	3072	256	12
256	15360	512	30

Pairings

- DLP over elliptic curves (ECDSA) must be as hard as DLP in $\mathbb{F}_{p^n}$ (RSA under the assumption that it is as hard as factoring);
- most important cases: $2 \leq n \leq 30$;
- very fast construction (Barreto-Naehrig) at $n = 12$.

Plan of the lecture

- Pairings
- Pairing-friendly curves
- Progress of NFS attacks
- Consequences

Embedding degree

Definition

The embedding degree of a curve E defined over $\mathbb{F}_q$ with respect to an integer r is the smallest integer k so that r divides $q^k - 1$.

Random curves have large embedding degree

- Parings allow to reduce the DLP on a curve of cardinality $\approx q$ to the DLP in the finite field $\mathbb{F}_{q^k}$.
- Balasubramanian and Köblitz 1998 : For random curves $k \approx q$. Hence even if DLP in finite fields was polynomial time it wouldn't be enough to break DLP on curves.

Definition

A curve E defined over $\mathbb{F}_q$ is pairing-friendly with respect to a prime r if

- $r > \sqrt{q}$;
- $k < (\log_2 r)/8$

Embedding degree

Definition

The embedding degree of a curve E defined over $\mathbb{F}_q$ with respect to an integer r is the smallest integer k so that r divides $q^k - 1$.

Random curves have large embedding degree

- Parings allow to reduce the DLP on a curve of cardinality $\approx q$ to the DLP in the finite field $\mathbb{F}_{q^k}$.
- Balasubramanian and Köblitz 1998 : For random curves $k \approx q$. Hence even if DLP in finite fields was polynomial time it wouldn't be enough to break DLP on curves.

Definition

A curve E defined over $\mathbb{F}_q$ is pairing-friendly with respect to a prime r if

- $r > \sqrt{q}$;
- $k < (\log_2 r)/8$

$\boxed{\text{We must construct pairing-friendly curves.}}$

CM method

Constructing pairings

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

1. Find three integers q, r and t subject to the CM equations in next slide; The three integers will be so that
   - $\mathbb{F}_q$ is the field of coefficients;
   - E has $q+1-t$ points;
   - E has a subgroup of order r.
2. Apply the complex method to construct a curve E of parameters q, r and 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

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)

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 have 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 $\left(\frac{-D}{r}\right) = 1$
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 $\left(\frac{-D}{r}\right) = 1$
3. solve (2) for y
4. solve (3) for q

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

Limits

We have no control on the size of q. We would like $r \approx q$ but we have $q = \frac{1}{4}(\text{small} + (\text{random residue of } r)^2) \approx r^2$.

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

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

Limits

Very few integers a are such that $R(a) \approx 2^{256}$ and both E and its twist are secure, e.g. for $k = 16$ and $D = 3$ there are only $a = 39193, 61815$.

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. ~~$\Phi_k(t-1) \equiv 0 \pmod r$~~
2. ~~$q+1-t \equiv 0 \pmod r$~~
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

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

Limits

- If $\varphi(k) > 4$ then the plane curve that we obtain has genus ≥ 2 and by Faltings' theorem it has a finit set of solutions.
- The cases $\varphi(k) \leq 4$ imply $k = 2, 3, 4, 6, 8, 10$ which are less than the value required by pairings. (Rmk: Freeman worked the case $k = 10$).

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. $\exists y,\ 4q = Dy^2 + t^2$

Method

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. $\exists y,\ 4q = Dy^2 + t^2$

Method

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. $\exists y,\ 4q = Dy^2 + t^2$

Method

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. $\exists y,\ 4q = Dy^2 + t^2$

Method

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. $\cancel{\exists y,\ 4q = Dy^2 + t^2}$

Method

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.

Limits

q has a polynomial form. In the case of factoring this is a vulnerability.

Plan of the lecture

- Pairings
- Pairing-friendly curves
- Progress of NFS attacks
- Consequences

The number field sieve(NFS): diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

$$
\begin{tikzcd}
 & a - bx \in \mathbb{Z}[x] \arrow[dl] \arrow[dr] & \\
\mathbb{Z}[x]/\langle f(x) \rangle \arrow[dr] & & \mathbb{Z}[x]/\langle g(x) \rangle \arrow[dl] \\
 & \mathbb{Z}/p\mathbb{Z} &
\end{tikzcd}
$$

The number field sieve(NFS): diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

$$\begin{tikzcd}
 & a - bx \in \mathbb{Z}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\mathbb{Z}[\alpha_f] \arrow[dr, "\alpha_f \mapsto m"'] & & \mathbb{Z}[\alpha_g] \arrow[dl, "\alpha_g \mapsto m"] \\
 & \mathbb{Z}/p\mathbb{Z} &
\end{tikzcd}$$

The NFS algorithm for $\mathbb{F}_p$

$F(a,b) = \sum_{i=0}^{d} f_i a^i b^{d-i}$ where $d = \deg f$ and $G(a,b) = g_1 a + g_0 b$.

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ which have a common root modulo p;

2: (Sieve) Collect relatively prime pairs (a,b) such that $F(a,b)$ and $G(a,b)$ are B-smooth (for a parameter B);

3: Write a linear equation for each pair (a,b) found in the Sieve stage.

4: (Linear algebra) Solve the linear system to find (virtual) logarithms of the prime ideals of norm less than B;

5: (Individual logarithm) Write $\log_t s$ in terms of the previously computed logs.

Why is the polynomial selection important?

Size of norms

- If E^2 is the cost of the relation collection, then we sieve all pairs a, b so that $|a|, |b| \leq E$.
- $|F(a,b)| = |\sum_{i=0}^{d} f_i a^i b^{d-i}| \leq E^d \|f\|$ and $|G(a,b)| = |g_1 a + g_0 b| \leq E\|g\|$.
- If we reduce $\|f\|$ and $\|g\|$ we can reduce the work.

Polynomial selection: Base-m method

Put $m = \lfloor p^{\frac{1}{d+1}} \rfloor$ and write $p = p_d m^d + p_{d-1} m^{d-1} + \cdots p_1 m + p_0$ in base m and put

- $f = p_d x^d + \cdots + p_1 x + p_0$;
- $g = x - m$.

The special number field sieve (SNFS)

Example: when factoring $N = 2^{1039} - 1$ the polynomial selection is easy

- $d = 4,\ m = 2^{260},\ f = x^4 - 2$
- $d = 5,\ m = 2^{208},\ f = x^5 - 2$
- $d = 6,\ m = 2^{173},\ f = 2x^6 - 1$

Definition: an integer N is d-SNFS

for an absolute constant A if there exists $f \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}$ so that

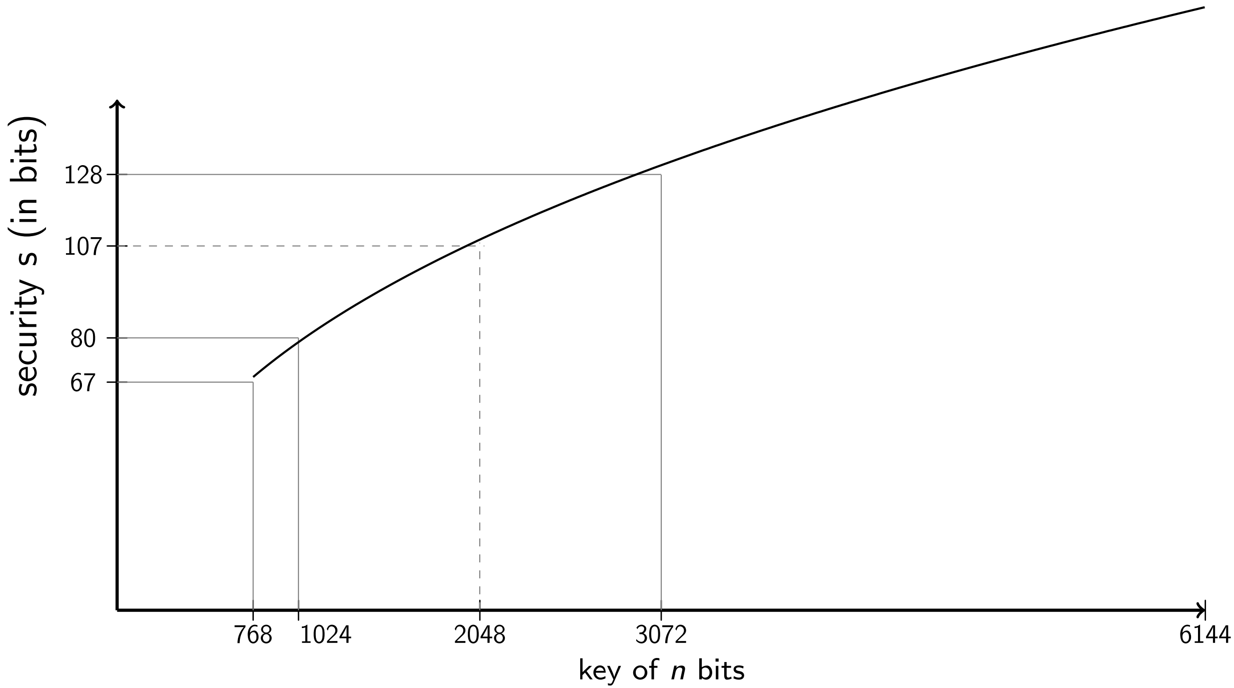
$$N = f(m)$$

and $\|f\| \leq A$. Note that $|m| \leq N^{\frac{1}{d}} = (N^{\frac{1}{d+1}})^{1+o(1)}$.

Consequences

When we run NFS with $\|f\| = O(1)$ we say that we run SNFS because the complexity is reduced.

Size of keys for RSA (naive computation)

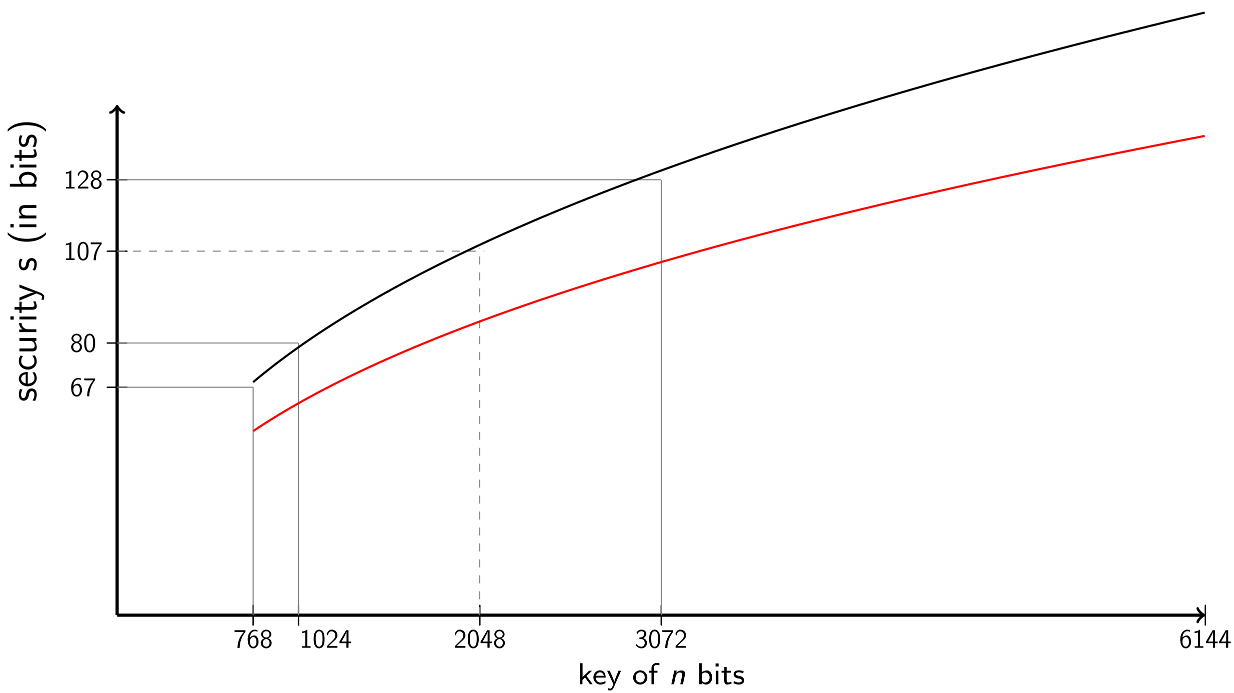


Extrapolation formula (based on the RSA-768 record)

$$2^s = 2^{-8} L_{2^n}[64]$$

where $L_N[c] = \exp((\frac{c}{9})^{\frac{1}{3}}(\log_e N)^{\frac{1}{3}}(\log_e(\log_e N))^{\frac{2}{3}})$

Size of keys for SNFS (naive computation)



Extrapolation formula (based on factoring $2^{1039} - 1$)

$$2^s = 2^{-7} L_{2^n}[32]$$

where $L_N[c] = \exp((\frac{c}{9})^{\frac{1}{3}}(\log_e N)^{\frac{1}{3}}(\log_e(\log_e N))^{\frac{2}{3}})$

Chronology: adapting SNFS from factoring to pairings

Index Calculus

- $\mathbb{F}_p$, '77, Adleman
- $\mathbb{F}_{2^n}$, '82, Hellman Reyneri, use polynomials instead of numbers
- $\mathbb{F}_{p^n}$, '94, Adleman DeMarrais, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$.

NFS and FFS

- $\mathbb{F}_p$, '90, Gordon / Schirokauer
- $\mathbb{F}_{2^n}$, '94, Adleman, use polynomials instead of numbers
- $\mathbb{F}_{p^n}$,
  - '00, Schirokauer, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$ (TNFS).
  - '06, Joux Lercier Smart Vercauteren, modify polynomial selection (JLSV)
  - new, Kim Barbulescu, combiner TNFS and JLSV: exTNFS

Joux, Lercier, Smart, Vercauteren

NFS for DLP in $\mathbb{F}_{p^n}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Joux, Lercier, Smart, Vercauteren

NFS for DLP in $\mathbb{F}_{p^n}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common ~~root~~ $\cancel{m}$ factor $\varphi(x)$ modulo $p$which is irreducible of degree n.

$$
\begin{tikzcd}
 & a - bx \in \mathbb{Z}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\mathbb{Z}[\alpha_f] \arrow[dr, "\bmod p\mathcal{O}_{\mathbb{Q}(\alpha_f)}"'] & & \mathbb{Z}[\alpha_g] \arrow[dl, "\bmod p\mathcal{O}_{\mathbb{Q}(\alpha_g)}"] \\
 & (\mathbb{Z}[x]/\langle p\mathbb{Z})/\langle\varphi\rangle &
\end{tikzcd}
$$

Joux-Pierrot's SNFS when $n \geq 1$

Method when $p = \Pi(u)$

1. Enumerate polynomials S of degree $\leq n-1$ until $x^n + S(x) - u$ is irreducible modulo p;
2. return $g = x^n + S(x) - u$ and $f = \Pi(x^n + S(x))$

Correction: $f(x) - p = \Pi(x^n + S(x)) - \Pi(u) = (x^n + S(x) - u)(\cdots)$.

Size of norms

The product of norms, which must be small, has size

$$E^{n(d+1)} Q^{\frac{1}{nd}},$$

where E and Q are given.

$\boxed{\text{Difficulty in practice: optimal only when } nd \approx 8.}$

TNFS diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

$$\begin{tikzcd}
 & a - bx \in \mathbb{Z}[x] \arrow[dl] \arrow[dr] & \\
\mathbb{Z}[x]/\langle f(x)\rangle = \mathbb{Z}[\alpha_f] \arrow[dr] & & \mathbb{Z}[x]/\langle g(x)\rangle = \mathbb{Z}[\alpha_g] \arrow[dl] \\
 & \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p &
\end{tikzcd}$$

TNFS diagram

NFS for DLP in $\cancel{\mathbb{F}_p}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree k such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

$$\begin{tikzcd}
 & a - bx \in \cancel{\mathbb{Z}}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\cancel{\mathbb{Z}}[x]/\langle f(x)\rangle = \cancel{\mathbb{Z}}[\alpha_f] \arrow[dr, "\alpha_f \mapsto m"'] & & \cancel{\mathbb{Z}}[x]/\langle g(x)\rangle = \cancel{\mathbb{Z}}[\alpha_g] \arrow[dl, "\alpha_g \mapsto m"] \\
 & \cancel{\mathbb{Z}}/p\cancel{\mathbb{Z}} \simeq \cancel{\mathbb{F}_p} &
\end{tikzcd}$$

TNFS diagram

NFS for DLP in $\mathbb{F}_{p^k}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree k such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

$$\begin{tikzcd}
& a - bx \in \mathbb{Z}[\iota][x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\mathbb{Z}[\iota][x]/\langle f(x) \rangle = \mathbb{Z}[\iota][\alpha_f] \arrow[dr, "\alpha_f \mapsto m"'] & & \mathbb{Z}[\iota][x]/\langle g(x) \rangle = \mathbb{Z}[\iota][\alpha_g] \arrow[dl, "\alpha_g \mapsto m"] \\
& \mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k} &
\end{tikzcd}$$

TNFS diagram

NFS for DLP in $\mathbb{F}_{p^k}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree k such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

$$
\begin{tikzcd}
 & a - bx \in \mathbb{Z}[\iota][x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\mathbb{Z}[\iota][x]/\langle f(x) \rangle = \mathbb{Z}[\iota][\alpha_f] \arrow[dr, "\alpha_f \mapsto m"'] & & \mathbb{Z}[\iota][x]/\langle g(x) \rangle = \mathbb{Z}[\iota][\alpha_g] \arrow[dl, "\alpha_g \mapsto m"] \\
 & \mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k} &
\end{tikzcd}
$$

$$\boxed{\text{STNFS: if } p = P(u) \text{ we have } f = P}$$

exTNFS diagram

$$\begin{tikzcd}[column sep=small]
 & a - bx \in \mathbb{Z}[\iota][x] \arrow[dl] \arrow[dr] & \\
\mathbb{Z}[\iota][x]/\langle f(x)\rangle \arrow[dr] & & \mathbb{Z}[\iota][x]/\langle g(x)\rangle \arrow[dl] \\
 & (\mathbb{Z}[\iota]/p\mathbb{Z}[\iota])[t]/\langle k(t)\rangle \simeq \mathbb{F}_{p^{\eta\kappa}} &
\end{tikzcd}$$

Explanation

- TNFS as if $n = \eta$
- Joux-Pierrot as if $n = \kappa$ (any other method when p is not SNFS)

$$\boxed{\text{SexTNFS: when } p = P(u) \text{ we take } f = P(x^\eta).}$$

exTNFS diagram

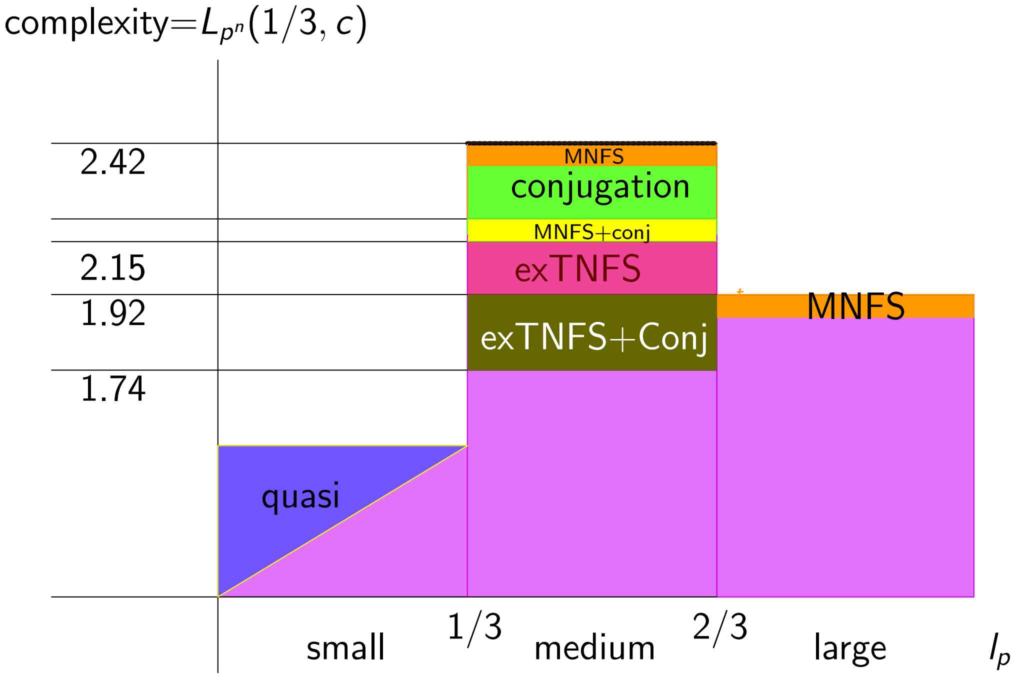
$$
\begin{tikzcd}
 & a - bx \in \mathbb{Z}[\iota][x] \arrow[dl, "\text{mod } f"'] \arrow[dr, "\text{mod } g"] & \\
\mathbb{Z}[\iota][x]/\langle f(x)\rangle \arrow[dr, "\substack{\text{mod } p\\ \text{mod } k}"'] & & \mathbb{Z}[\iota][x]/\langle g(x)\rangle \arrow[dl, "\substack{\text{mod } p\\ \text{mod } k}"] \\
 & (\mathbb{Z}[\iota]/p\mathbb{Z}[\iota])[t]/\langle k(t)\rangle \simeq \mathbb{F}_{p^{\eta\kappa}} &
\end{tikzcd}
$$

Explanation

- TNFS as if $n = \eta$
- Joux-Pierrot as if $n = \kappa$ (any other method when p is not SNFS)

$\boxed{\text{SexTNFS: when } p = P(u) \text{ we take } f = P(x^\eta).}$

DLP in $\mathbb{F}_{p^n}$ when p is not SNFS but n is composite with good factors



where $p = L_{p^n}(l_p, O(1))$

Plan of the lecture

- Pairings
- Pairing-friendly curves
- Progress of NFS attacks
- **Consequences**

Complete families (e.g. BN)

SNFS

- The complexity has been revised from $L[64]$ to $L[32]$ where $L_N[c] = \exp((\frac{c}{9})^{\frac{1}{3}}(\log_e N)^{\frac{1}{3}}(\log_e(\log_e N))^{\frac{2}{3}})$
- If $L_{Q^{\text{new}}}[32] = L_{Q^{\text{old}}}[64]$ then we obtain $\log_2 Q^{\text{new}} = (2 + o(1)) \log_2 Q^{\text{old}}$.
- Hence, if q is SNFS we must double the key size $\log_2(q^k)$. Since k is fixed in thes families, we must increase q (and r).

It is a consequence of the starting idea

The first step of the construction of pairing-friendly curves of this type is to set r and t to be SNFS, then we set q as an expression of r and t.

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
2. Menezes' $k = 1$ curves