CAEN – June 20-22, 2018, Caen

An overview of the discrete logarithm in finite fields

Razvan Barbulescu
CNRS and IMJ-PRG

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}.

Multi-linear maps

Applications

- Zero-knowledge proof;
- identity based encryption;
- short signature;
- etc.

Mathematical realization

- lattice-based maps
- elliptic curve pairings
  - in 2000 it was proposed by Sakai, Ohgishi and Kasahara and later by Joux, and key sizes were proposed based on a hypothesis;
  - in 2012 the NIST studied them for standardization and in 2013 Boneh, Franklin and Joux received the Gödel prize;
  - between 2013 and 2016 there were attacks which invalidated the key sizes;
  - currently, key sizes are being updated and new implementations are proposed.

Multi-linear maps

Applications

- Zero-knowledge proof;
- identity based encryption;
- short signature;
- etc.

Mathematical realization

- ~~lattice-based maps~~
- elliptic curve pairings
  - in 2000 it was proposed by Sakai, Ohgishi and Kasahara and later by Joux, and key sizes were proposed based on a hypothesis;
  - in 2012 the NIST studied them for standardization and in 2013 Boneh, Franklin and Joux received the Gödel prize;
  - between 2013 and 2016 there were attacks which invalidated the key sizes;
  - currently, key sizes are being updated and new implementations are proposed.

Security

Pairings security

The security of pairings based cryptosystems relies on the difficulty of

- elliptic curves discrete logarithms;
- finite fields discrete logarithm.

Embedding degree

If a paring is such that

$$E_1/\mathbb{F}_Q[r] \times E_2/\mathbb{F}_Q[r] \to (\mathbb{F}_{Q^n})^*$$

then n is called the embedding degree. If Q is prime and $n > 1$ then it is a different problem than behind DSA;

$\boxed{\text{Required: DLP(curve over } \mathbb{F}_p\text{)} \approx \text{DLP(finite field } \mathbb{F}_{p^k}\text{)}}$

Discrete logarithm

Definition

Given g and g^x, find x if possible (here G is a known group of known order).

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

Cryptographic sizes before 2018

Key sizes

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

Pairings

- discrete log problem over elliptic curves (DSA) must be as hard as discrete log 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 $n = 12$.

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

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

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

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

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.

Chronology of DLP in finite fields

Index Calculus

- $\mathbb{F}_p$, 1977, Adleman
- $\mathbb{F}_{2^n}$, 1982, Hellman Reyneri, use polynomials instead of numbers
- $\mathbb{F}_{p^n}$, 1994, Hellman for $n = 2$ then Adleman DeMarrais, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$.

NFS and FFS

- $\mathbb{F}_p$, 1990, Gordon / Schirokauer
- $\mathbb{F}_{2^n}$, 1994, Adleman, use polynomials instead of numbers
- $\mathbb{F}_{p^n}$,
  - 2000, Schirokauer, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$ (rehabilitated in 2015 by B., Gaudry and Kleinjung).
  - 2006, Joux Lercier Smart Vercauteren, modify polynomial selection (JLSV)
  - 2016, Kim and B., combiner TNFS and JLSV: exTNFS

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?

Cost of algorithms of the Index Calculus family

where norms' size is

- p in Index Calculus;
- $B^3 p^{\frac{1}{2}}$ for Gaussian integers (complexity $L_p(\frac{1}{2})$);
- $B^{d+1} p^{\frac{1}{d}}$ for NFS in $\mathbb{F}_p$ (complexity $L_p(\frac{1}{3})$);
- norms product for NFS in $\mathbb{F}_{p^n}$ when $n > 1$

Norms' product

If $f = f_d x^d + \cdots + f_1 x + f_0$ then

$$|\,\mathrm{N}_f(a + b\alpha_f)| = |f_d a^d + \cdots + f_1 a b^{d-1} + f_0 b^d| \leq (d+1) B^d \|f\|\,.$$

The bit size of the norm's product is very well approximated by $(\deg f + \deg g) + \log_2 \|f\| + \log_2 \|g\|\,.$

The polynomial selection task

Fix $\deg f$ and $\deg g$ as small as possible (or try all possibilities, in practice the optimal choices are ≤ 10, then find f and g of small coefficients.
Intuitively in favor of the hypothesis of 2000 : when $k \geq 2$ we have the extra condition $\min(\deg f, \deg g) \geq n$ which makes the task harder.

The idea of Joux Lercier Smart Vercauteren

Polynomial selection

Select f and g which have a common ~~root~~ factor φ of degree n modulo p.

$$\begin{tikzcd}
 & a - bx \in \mathbb{Z}[x] \arrow[dl] \arrow[dr] & \\
\mathbb{Z}[x]/\langle f(x)\rangle \arrow[dr] & & \mathbb{Z}[x]/\langle g(x)\rangle \arrow[dl] \\
 & \mathbb{F}_p[t]/\langle \varphi \rangle \simeq \mathbb{F}_{p^n} &
\end{tikzcd}$$

The idea of Joux Lercier Smart Vercauteren

Polynomial selection

Select f and g which have a common ~~root~~ factor φ of degree n modulo p.

$$\begin{tikzcd}
& a-bx\in\mathbb{Z}[x] \arrow[dl, "\text{mod } f"'] \arrow[dr, "\text{mod } g"] & \\
\mathbb{Z}[x]/\langle f(x)\rangle \arrow[dr, "\begin{array}{c}\text{mod } p\\ \text{mod } \varphi\end{array}"'] & & \mathbb{Z}[x]/\langle g(x)\rangle \arrow[dl, "\begin{array}{c}\text{mod } p\\ \text{mod } \varphi\end{array}"] \\
& \mathbb{F}_p[t]/\langle\varphi\rangle \simeq \mathbb{F}_{p^n} &
\end{tikzcd}$$

JLSV in practice

Modifications

The only modification is the polynomial selection (done in sage or magma) and the fact that in the sieve we have two non-linear polynomials.

- the implementation of Joux and Lercier was so even for $\mathbb{F}_p$;
- CADO-NFS supports two non-linear polynomials since 2014).

Records

- 2006, Joux Lercier Smart Vercauteren, $\mathbb{F}_{p^3}$, 120dd.
- 2014, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^2}$, 180dd.
- 2015, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^4}$, 120dd.
- 2015, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^3}$ and again Guillevic, Thomé, Morain (2016) 156dd.
- 2017, Gremy, Guillevic Morain and Thomé, $\mathbb{F}_{p^6}$ using $3d$ sieving (Gremy implemented it in the nfs-hd branch of CADO-NFS since 2016) 132dd

Important tool

Theorem (Lenstra, Lenstra, Lovasz)

Let $M \in \mathcal{M}_n(\mathbb{Z})$ define a lattice. Then one can compute in polynomial time a vector of euclidean norm less than $2^{\frac{n-1}{4}} |\det M|^{\frac{1}{n}}$.

Corollary (rational reconstruction (also called continued fractions))

For any integer a and prime p one can compute two integers u and v so that

$$a \equiv \frac{u}{v} \mod p$$

and $|u|, |v| \leq 2^{\frac{1}{4}} \sqrt{p}$.

Polynomial selection : GJL

Lattice

Let $\varphi \in \mathbb{F}_p[x]$ be a polynomial of degree n.
For a parameter D consider the subgroup of $\mathbb{Z}^D$ defined by the rows of

$$M(p,\varphi,D) = \begin{bmatrix} p &&&&& \\ & \ddots &&&& \\ && p &&& \\ \varphi_0 & \cdots & \varphi_n & 1 && \\ & \ddots && \ddots & \ddots & \\ && \varphi_0 & \cdots & \varphi_n & 1 \end{bmatrix} \begin{array}{l} \left.\vphantom{\begin{array}{c} p \\ \ddots \\ p \end{array}}\right\} \deg \varphi = n \\ \left.\vphantom{\begin{array}{c} \varphi_0 \\ \ddots \\ \varphi_0 \end{array}}\right\} D+1-n \end{array}$$

JLSV$_2$ algorithm

1. Take random $f \in \mathbb{Z}[x]$ of degree $D+1$ with a factor of degree n modulo p.
2. Set $g \in \mathbb{Z}[x]$ to have the same coefficients as the shortest vector in the LLL-reduced basis of the lattice defined by $M(p,\varphi,D)$.

justification: The LLL algorithm cannot return $f = g$ because g is too large.

Polynomial selection : JLSV$_1$

Raw variant

1. Select $f \in \mathbb{Z}[x]$ of degree n irreducible modulo p;
2. Set $g = f + p$.

information theory: f and g are optimal.

Practical variant

1. Take $f_0, f_1 \in \mathbb{Z}[x]$ so that $\deg f_0 = n$ and $\deg f_1 < n$.
2. Take $a \geq 2^{\frac{1}{4}}\sqrt{p}$ as small as possible so that $f := f_0 + af_1$ is irreducible modulo p.
3. Compute the rational reconstruction $a \equiv u/v \mod p$ and set $g := vf_0 + uf_1$.

justification: LLL cannot return $a/1$ as rational reconstruction.

Polynomial selection : Conjugation (part I)

Idea

- $\sqrt{3}$ in $\mathbb{F}_p$ has a representative which is larger than $2^{\frac{1}{4}}p^{\frac{1}{2}}$ so the LLL theorem cannot return the rational reconstruction

$$\sqrt{3} \equiv \sqrt{3}/1 \mod p.$$

- A polynomial $f_0 + \sqrt{3}f_1$ is not allowed but we can **conjugate** it to obtain $(f_0 + \sqrt{3}f_1)(f_0 - \sqrt{3}f_1) = f_0^2 - 3f_1^2 \in \mathbb{Z}[x]$.

Conjugation algorithm

1. Take $f_0, f_1 \in \mathbb{Z}[x]$ so that $\deg f_0 = n$ and $\deg f_1 < n$.
2. Take $a < p$ non-square so that $\sqrt{a}$ exists in $\mathbb{F}_p$ and $\varphi := f_0 + \sqrt{a}f_1$ is irreducible modulo p.
3. Set $\varphi = f_0^2 - af_1^2$.
4. Compute the rational reconstruction $\sqrt{a} \equiv \frac{u}{v} \mod p$ and set $g := vf_0 + uf_1$.

justification: f and g share the factor φ modulo p.

Polynomial selection : Conjugation (part II)

Example

Discrete logarithm in $\mathbb{F}_{p^2}$ of 180 decimal digits Consider DLP in $\mathbb{F}_{p^2}$ where $p = \lfloor \pi \cdot 10^{89} \rfloor + 14905741$

- GJL : $f = x^4 + x - 1$ and
$$\begin{aligned} g \; = \; & 55947346946240760948788499410380792946617500 4x^3 \\ & +79866641850329856433972092304608878381464121x^2 \\ & +52391486839645529970296074400426159302999066x \\ & -14098507812691843454410733515032134952661662 0. \end{aligned}$$
- Conjugation : $f = x^4 + 1$ and
$$\begin{aligned} g \; = \; & 4482250772492864335651609658288283036183624 74x^2 \\ & -29606109908476368046927513730655796265782462 3x \; ; \\ & 448225077249286433565160965828828303618362474. \end{aligned}$$

$$\boxed{\mathbb{F}_{p^2} \text{ (Conjugation) was 160 times faster than } \mathbb{F}_p \text{ (GJL)}}$$

Domain of application

- $N_f = E^{2n}$ and $N_g = E^n (p^n)^{\frac{1}{2n}}$ instead of $E^d N^{\frac{1}{d+1}}$ and $EN^{\frac{1}{d+1}}$ for the prime case;
- When $n = \frac{1}{12}^{\frac{-1}{3}} \left(\frac{\log p^n}{\log \log p^n}\right)^{\frac{1}{3}}$ the complexity is $L_{p^n}(1/3, \sqrt[3]{48/9})$ instead of $\geq L_{p^n}(1/3, \sqrt[3]{64/9})$.

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 ~~$\mathbb{F}_p$~~

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 $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

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

Relation collection

Reminder of NFS

Enumerate pairs (a, b) in $\mathbb{Z} \times \mathbb{Z}$ without common divisors such that $F(a, b)$ and $G(a, b)$ are B-smooth for a parameter B.

TNFS

- Enumerate pairs (a, b) in $\mathbb{Z}[\iota] \times \mathbb{Z}[\iota]$ without common divisors such that $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(F(a, b))$ and $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(G(a, b))$ are B-smooth for the same parameter B as in NFS.
- In particular for the first example, we enumerate $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ and search those where

$$(\mathrm{Re} F(a, b))^2 + (\mathrm{Im} F(a, b))^2 \text{ and } (\mathrm{Re} G(a, b))^2 + (\mathrm{Im} G(a, b))^2$$

are B-smooth.

Relation collection

Reminder of NFS

Enumerate pairs (a, b) in $\mathbb{Z} \times \mathbb{Z}$ without common divisors such that $F(a, b)$ and $G(a, b)$ are B-smooth for a parameter B.

TNFS

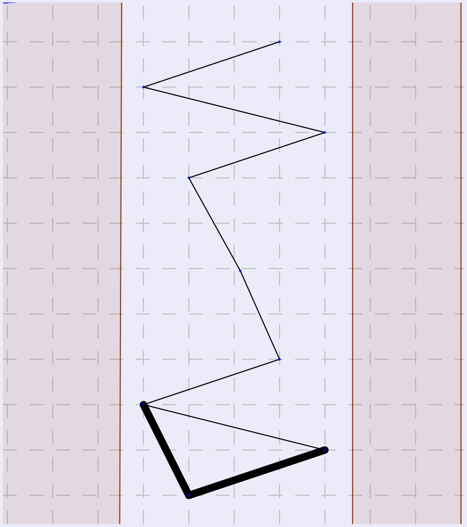
- Enumerate pairs (a, b) in $\mathbb{Z}[\iota] \times \mathbb{Z}[\iota]$ without common divisors such that $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(F(a, b))$ and $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(G(a, b))$ are B-smooth for the same parameter B as in NFS.
- In particular for the first example, we enumerate $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ and search those where
$$(\mathrm{Re} F(a, b))^2 + (\mathrm{Im} F(a, b))^2 \text{ and } (\mathrm{Re} G(a, b))^2 + (\mathrm{Im} G(a, b))^2$$
are B-smooth.

$\boxed{\text{We collect smooth values of polynomials with } 2n\text{-variables.}}$

Pollard's Lattice sieve (1/2)

Lattice sieve (theory 1993) : Franke-Kleinjung (algo 2009)

Given a lattice, find the next point in a tight lane.



In dimension 2 (classical NFS) one can find the next point in $\mathcal{O}(1)$ operations because only 3 vectors, called transition vectors, can occur as differences. In practice lattice sieve is 20 times faster than line sieve.

Sieving in higher dimension (NFS-HD)

- Hayasaka, Aoki, Kobayashi, Takagi 2015 : 3D sieving;
- Grémy 2016 : 3D sieving (hybrid between 2D and 3D) available in the nfs-hd branch of CADO-NFS;
- Grémy 2018 : 4D sieving.

The question of implementing 6D, 8D etc is open.

Plan of the lecture

- JLSV's idea: from $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$
- Schirokauer's idea: from $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$
- Pairings
- Pairing-friendly curves
- Consequences
- Updating key sizes (joint work with S. Duquesne)

CM method

Difference with constructiong curves for ECDSA

The embedding degree has probability less than $1/q$ to be ≤ 20.

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 to construct a curve E so that. 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. $\exists y,\ 4q = Dy^2 + t^2$

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. ~~$\Phi_k(t-1) \equiv 0 \pmod{r}$~~
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. ~~$\Phi_k(t-1) \equiv 0 \pmod{r}$~~
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)
2. put $q = r + t - 1$, which satisfies (2)

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

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

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

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

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

1. replace (2) by an equivalent equation

Complete families (e.g. BN)

CM equations

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

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

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

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

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

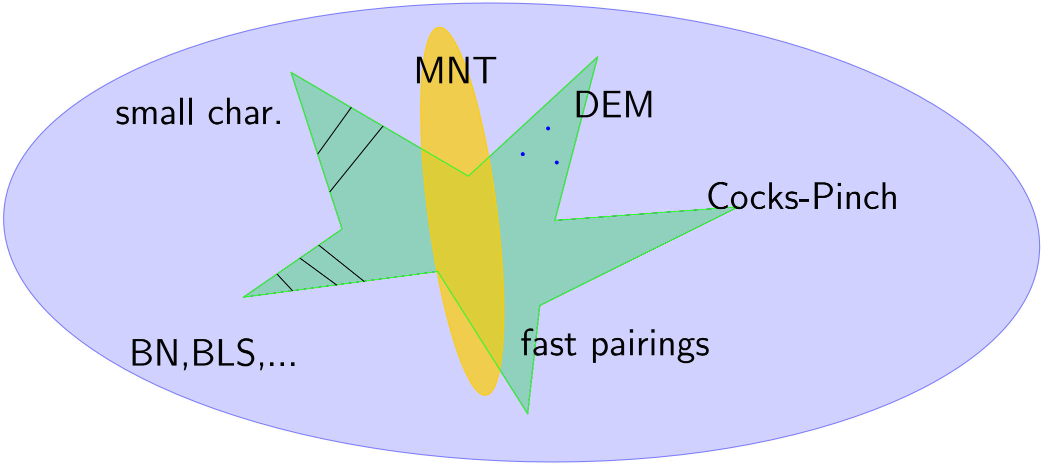
1. ~~$\Phi_k(t-1) \equiv 0 \pmod{r}$~~
2. ~~$Dy^2 + (t-2)^2 \equiv 0 \pmod{r} \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2)) \equiv 0 \pmod{r}$~~
3. ~~$\exists y,\ 4q = Dy^2 + t^2$~~

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

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

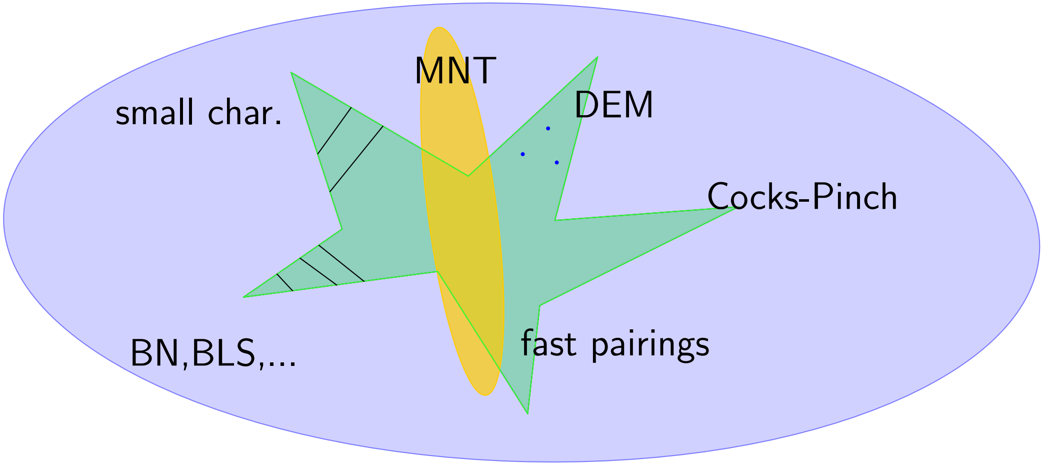
Note that we generate a large number of elliptic curves very quickly.

Summary



- Pinch-Cocks constructs all the fast pairings, but it is never in the fast case.
- Sparse families (e.g. MNT) construct many pairings but $k = 2$ and they are not fast for the ≥ 80 bits of security.
- Dupond-Enge-Morain offers a very small number of pairings, which might be target of subsequent attacks, impossible to tune them to be faster in practice.

Summary



- Pinch-Cocks constructs all the fast pairings, but it is never in the fast case.
- Sparse families (e.g. MNT) construct many pairings but $k = 2$ and they are not fast for the ≥ 80 bits of security.
- Dupond-Enge-Morain offers a very small number of pairings, which might be target of subsequent attacks, impossible to tune them to be faster in practice.

We are left with small char and parametrized families (e.g. BN, BLS).

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

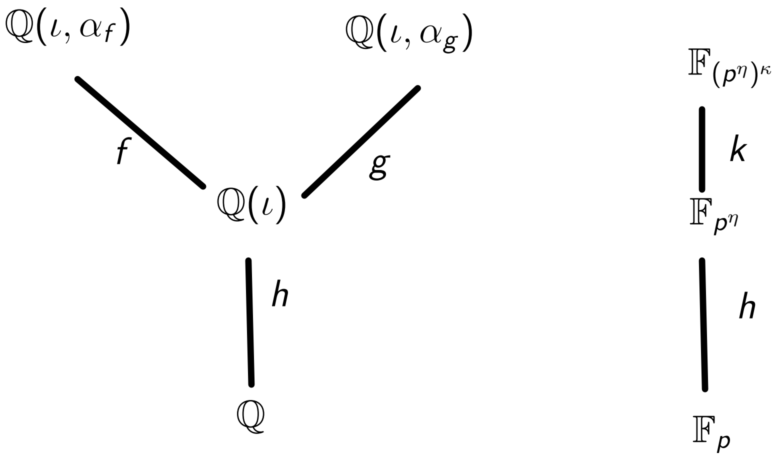
$$N = f(m)$$

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

Consequences

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

The extended TNFS (Kim B. 2016)


$\mathbb{Q}(\iota,\alpha_f)$
$\mathbb{Q}(\iota,\alpha_g)$
f
g
$\mathbb{Q}(\iota)$
h
$\mathbb{Q}$
$\mathbb{F}_{(p^\eta)^\kappa}$
k
$\mathbb{F}_{p^\eta}$
h
$\mathbb{F}_p$

exTNFS algorithm

constraints: $n = \eta\kappa$ with $\gcd(\eta,\kappa) = 1$

1. select h as in TNFS for $\mathbb{F}_{p^\eta}$;
2. select f and g as for $\mathbb{F}_{p^\kappa}$; put $k = \gcd(f \bmod p, g \bmod p)$;
3. continue the algorithm as for TNFS.

exTNFS diagram

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

Explication

k is irreducible over $\mathbb{F}_p$ and, since $\gcd(\eta,\kappa)=1$, it is automatically irreducible over $\mathbb{F}_{p^\eta}$.

exTNFS diagram

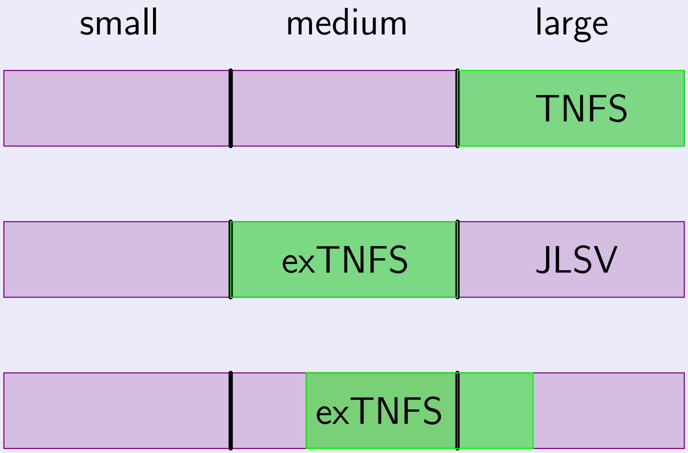
$$\begin{tikzcd}
 & a - bx \in \mathbb{Z}[\iota][x] \arrow[dl, "\text{mod } f"] \arrow[dr, "\text{mod } g"'] & \\
\mathbb{Z}[\iota][x]/\langle f(x)\rangle \arrow[dr, "\substack{\text{mod } p\\ \text{mod } k}"] & & \mathbb{Z}[\iota][x]/\langle g(x)\rangle \arrow[dl, "\substack{\text{mod } p\\ \text{mod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

Explication

k is irreducible over $\mathbb{F}_p$ and, since $\gcd(\eta, \kappa) = 1$, it is automatically irreducible over $\mathbb{F}_{p^\eta}$.

exTNFS with Conjugation

From Kim to Barbulescu



exTNFS with Conjugation method

- idea: exTNFS can be used to extend to the left any case of NFS
- complexity: the best case of NFS is when $p = L_{p^n}(1/3, 12^{\frac{1}{3}})$ and one uses the Conjugation method

Theorem

If $n = \eta\kappa$, $\gcd(\eta, \kappa) = 1$ *and* $\kappa = 12^{-\frac{1}{3}}$ *then DLP can be solved in time* $L_{p^n}(1/3, \sqrt[3]{48/9})$.

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

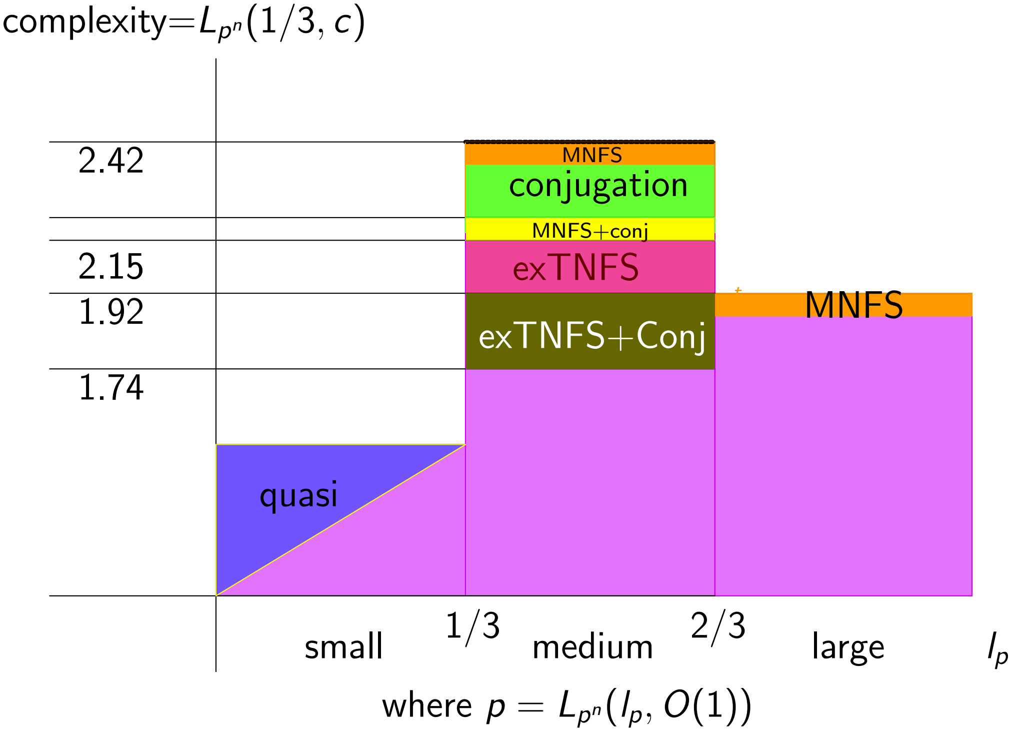
The product of norms, which must be small, has size

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

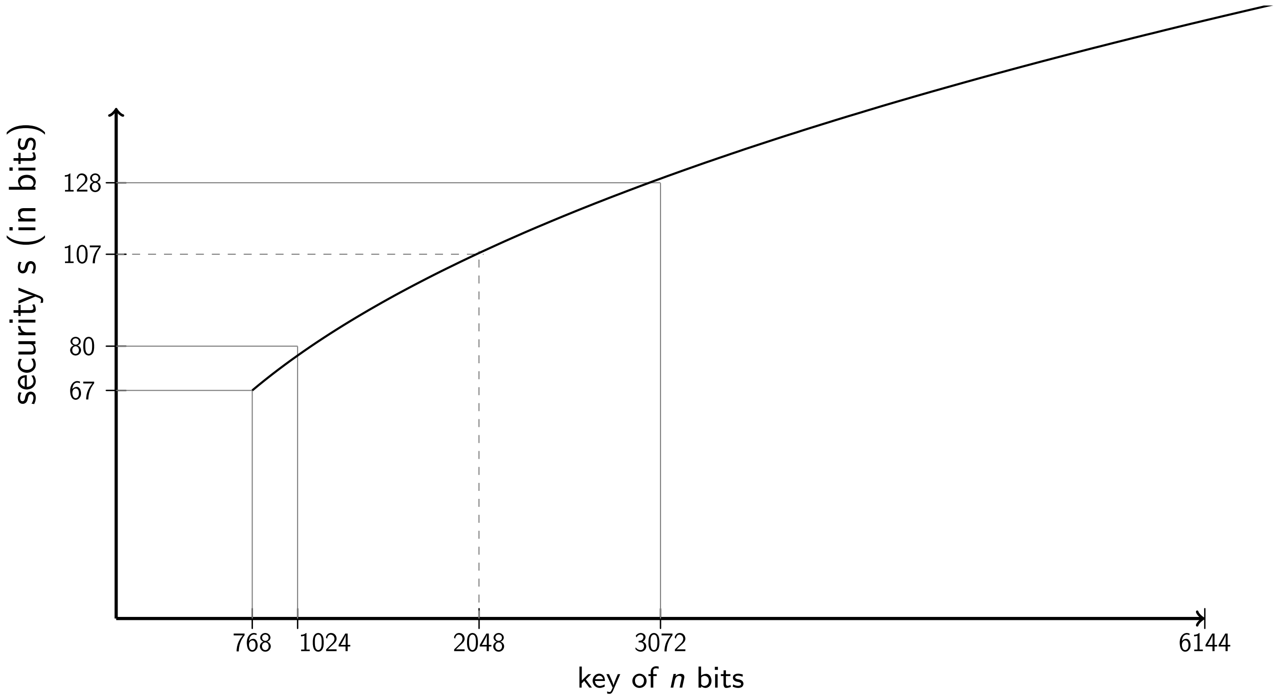
where E and Q are given.

$\boxed{\text{Due to exTNFS We replace } n \text{ by one of its divisors.}}$

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



Size of keys for RSA (naive computation)



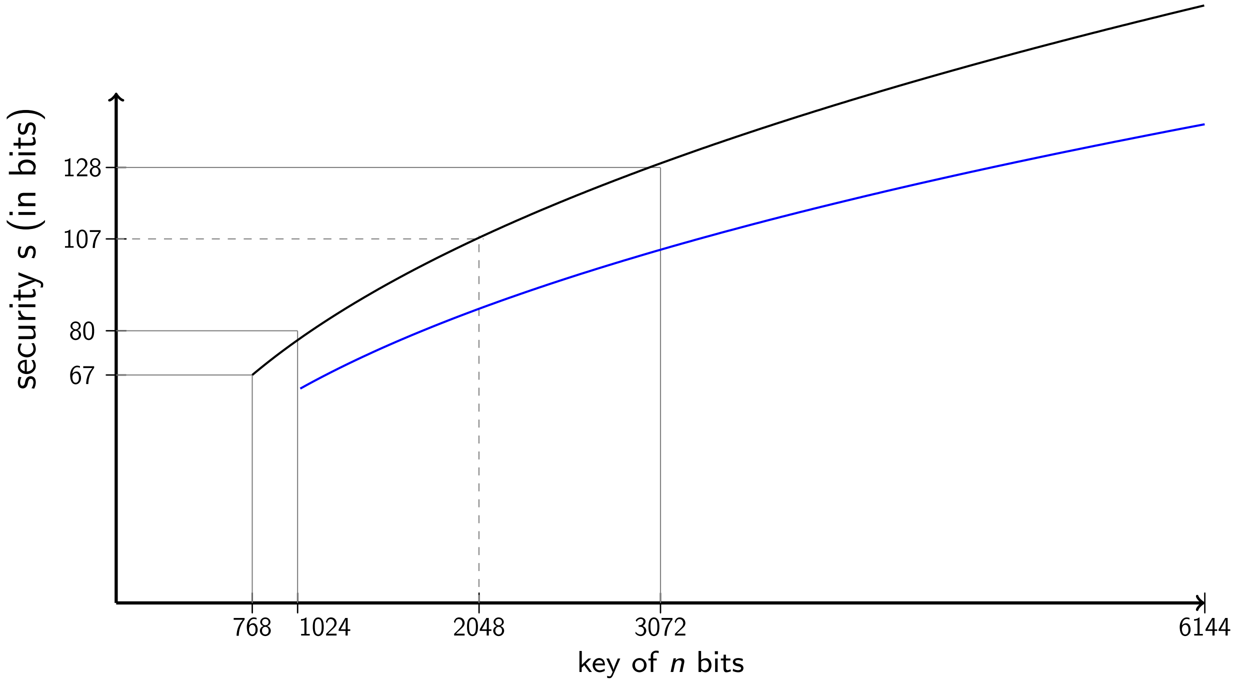
Extrapolation formula (based on the RSA-768 record)

$$2^s = 2^{67}\frac{L_{2^n}[64]}{L_{2^{768}}[64]}$$

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)

y



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

$$2^s = 2^{63}\frac{L_{2^n}[32]}{L_{2^{768}}[32]}$$

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

Size of keys for SNFS (naive computation)

Cost

$$\text{cost} = \frac{2B}{\mathcal{A}\log B}\,\rho\left(\frac{\log_2(N_f)}{\log_2 B}\right)^{-1}\rho\left(\frac{\log_2(N_g)}{\log_2 B}\right)^{-1} + 2^7\frac{B^2}{\mathcal{A}^2(\log B)^2(\log_2 B)^2},$$

where $\mathcal{A}$ can be upper bounded by $\eta\kappa/\gcd(\eta,\kappa)$.

Litterature records

record	$\log_2 E$	$\log_2$(cost of sieve)	$\log_2 B$	$\log_2$(cost of lin.alg)	$\log_2(c_{\text{sieve}})$	$\log_2(c_{\text{lin.alg}})$
SNFS-1039 (factor)	31.0	63.0	38	63.0	1	1
NFS-768 (factor)	33.0	66.5	40	64.5	0.5	-2
FFS-809	27.0	57.5	28	55.0	3.5	2
SNFS-1024 (DLP)	31.5	64.5	31	63.5	1.5	2
NFS-768 (DLP)	35.0	68.0	36	66.0	-2	-4

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. The fastest families of pairings are all affected, BLS12 became the best in place of BN
2. future work with Nadia El Mrabet and Kamel Mohamed to update keysizes for more exotic families of pairings.