Discrete logarithm computation in finite fields $\mathbb{F}_{p^n}$ with NFS variants and consequences in pairing-based cryptography

Aurore Guillevic

Inria Nancy, Caramba team

01/03/2019

Séminaire de cryptographie, Rennes

Joint work with Shashank Singh, IISER Bhopal, India

Asymmetric cryptography

Factorization (RSA cryptosystem)

Discrete logarithm problem (use in Diffie-Hellman, etc)

Given a finite cyclic group $(\mathbf{G}, \cdot)$, a generator g and $h \in \mathbf{G}$, compute x s.t. $h = g^x$.

$\rightarrow$ can invert the exponentiation function $(g, x) \mapsto g^x$?

Common choice of $\mathbf{G}$:

- prime finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (1976)
- characteristic 2 field $\mathbb{F}_{2^n}$
- elliptic curve $E(\mathbb{F}_p)$ (1985)

Discrete log problem

How fast can you invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in \mathbf{G}$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#\mathbf{G}\}$
- naive search, try them all: $\#\mathbf{G}$ tests
- random walk in $\mathbf{G}$, cycle path finding algorithm in a connected graph Floyd $\rightarrow$ Pollard, baby-step-giant-step, $O(\sqrt{\#\mathbf{G}})$ (the cycle path encodes the answer)
- parallel search in each distinct subgroup (Pohlig-Hellman)
- algorithmic refinements

Discrete log problem

How fast can you invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in \mathbf{G}$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#\mathbf{G}\}$
- naive search, try them all: $\#\mathbf{G}$ tests
- random walk in $\mathbf{G}$, cycle path finding algorithm in a connected graph Floyd $\to$ Pollard, baby-step-giant-step, $O(\sqrt{\#\mathbf{G}})$ (the cycle path encodes the answer)
- parallel search in each distinct subgroup (Pohlig-Hellman)
- algorithmic refinements

$\to$ Choose $\mathbf{G}$ of large prime order (no subgroup)

$\to$ complexity of inverting exponentiation in $O(\sqrt{\#G})$

$\to$ security level 128 bits means $\sqrt{\#G} \geq 2^{128}$
analogy with symmetric crypto, keylength 128 bits (16 bytes)

Discrete log problem

How fast can you invert the exponentiation function $(g, x) \mapsto g^x$?

G cyclic group of prime order, complexity $O(\sqrt{\#G})$.

Discrete log problem

How fast can you invert the exponentiation function $(g, x) \mapsto g^x$?

G cyclic group of prime order, complexity $O(\sqrt{\#G})$.

better way?

Discrete log problem

How fast can you invert the exponentiation function $(g, x) \mapsto g^x$?

G cyclic group of prime order, complexity $O(\sqrt{\#G})$.

better way?
$\rightarrow$ Use additional structure of **G**.

Discrete log problem when $\mathbf{G} = (\mathbb{Z}/p\mathbb{Z})^*$

Index calculus algorithm, prequel of the Number Field Sieve algorithm (NFS)

- p prime, $(p-1)/2$ prime, $\mathbf{G} = (\mathbb{Z}/p\mathbb{Z})^*$, gen. g, target h
- get many multiplicative relations in $\mathbf{G}$
  $g^t = g_1^{e_1} g_2^{e_2} \cdots g_i^{e_i} \pmod{p}$, $g, g_1, g_2, \ldots, g_i \in \mathbf{G}$
- find a relation $h = g_1^{e_1'} g_2^{e_2'} \cdots g_i^{e_i'} \pmod{p}$
- take logarithm: linear relations

$$\begin{aligned} t &= e_1 \log_g g_1 + e_2 \log_g g_2 + \ldots + e_i \log_g g_i \pmod{p-1} \\ &\vdots \\ \log_g h &= e_1' \log_g g_1 + e_2' \log_g g_2 + \ldots + e_i' \log_g g_i \pmod{p-1} \end{aligned}$$

- solve a linear system
- get $x = \log_g h$

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

$p = 1019$ prime, $g = 2$, $p - 1 = 2 \times 509$ prime

$$\begin{array}{lll} 2^{909} & = 90 & = 2 \cdot 3^2 \cdot 5 \\ 2^{10} & = 5 & = 5 \\ 2^{848} & = 135 & = 3^3 \cdot 5 \\ 2^{960} & = 12 & = 2^2 \cdot 3 \end{array} \quad \rightarrow \quad \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 1 \\ 0 & 3 & 1 \\ 2 & 1 & 0 \end{bmatrix} \cdot \vec{x} = \begin{bmatrix} 909 \\ 10 \\ 848 \\ 960 \end{bmatrix} \bmod 1018$$

Linear system solving mod 2, mod 509, Chinese remainder th.:
$\log_2 2 = 1$, $\log_2 3 = 958$, $\log_2 5 = 10$.

Target $h = 314$
$g^{372} h = 2^4 \cdot 5^2 \bmod p$
$\log_2 h = 4 + 2 \cdot 10 - 372 \bmod 1018 = 670$

from [15], F. Morain

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

Trick

Multiplicative relations over the **integers**

$g_1, g_2, \ldots, g_i \longleftrightarrow$ small prime integers

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

Trick

Multiplicative relations over the **integers**

$g_1, g_2, \ldots, g_i \longleftrightarrow$ small prime integers

Improvements in the 80's, 90's:

- Multiplicative relations in **number fields**
- Relation collection to get **small** integers to factor
- Better sparse linear algebra
- Independent target h

Coppersmith–Odlyzko–Schroeppel 1986: $\mathbb{Z}[i]$

Idea: enumerate in a clever way the relations
reduce the size of the integers to factor
If $p = 1 \bmod 4$, $\exists\ A$ s.t. $A^2 = -1 \bmod p$.
Let $U/V \equiv A \bmod p$ and $|U|, |V| < \sqrt{p}$ ($p = U^2 + V^2$).

algebraic side	rational side
$f = x^2 + 1$	$g = Vx + U$
$f(U/V) = 0 \bmod p$	$g(U/V) = 0 \bmod p$
$a + bi \in \mathbb{Z}[i]$	$aV + bU \in \mathbb{Z}$
factor in $\mathbb{Z}[i]$	factor in $\mathbb{Z}$
$\to$ factor Norm$(a - bi)$ in $\mathbb{Z}$	
integer $a^2 + b^2 \geqslant 2\max(a, b)$	integer $\geqslant 2\max(a, b)\sqrt{p}$

Enumerate enough (a, b) pairs s.t. $|a|, |b| \ll \sqrt{p}$

Example in $\mathbb{Z}[i]$

$p = 1109 = 1 \bmod 4$, $r = (p-1)/4 = 277$ prime
$p = 22^2 + 25^2$
$\max(|a|, |b|) = A = 20$, $B = 13$ smoothness bound

$\mathcal{F}_r = \{2, 3, 5, 7, 11, 13\}$ primes up to B

Algebraic side: $i^2 = -1$, $(1+i)(1-i) = 2$, $(2+i)(2-i) = 5$, $(2+3i)(2-3i) = 13$

$\mathcal{F}_a = \{-1, i\} \cup \{1+i, 1-i, 2+i, 2-i, 2+3i, 2-3i\}$
"primes" of norm up to B

Example in $\mathbb{Z}[i]$

$a + bi$	$a^2 + b^2$	factor in $\mathbb{Z}[i]$	$aV + bU$	factor in $\mathbb{Z}$
$-17 + 19i$	$650 = 2 \cdot 5^2 \cdot 13$	$-(1 - i)(2 + i)^2(2 - 3i)$	-7	-7
$-11 + 2i$	$125 = 5^3$	$i(2 + i)^3$	-231	$-3 \cdot 7 \cdot 11$
$-6 + 17i$	$325 = 5^2 \cdot 13$	$(2 + i)^2(2 + 3i)$	224	$2^5 \cdot 7$
$-4 + 7i$	$65 = 5 \cdot 13$	$i(2 - i)(2 + 3i)$	54	$2 \cdot 3^3$
$-3 + 4i$	$25 = 5^2$	$-(2 - i)^2$	13	13
$-2 + i$	$5 = 5$	$-(2 - i)$	-28	$-2^2 \cdot 7$
$-2 + 3i$	$13 = 13$	$-(2 - 3i)$	16	2^4
$-2 + 11i$	$125 = 5^3$	$-(2 - i)^3$	192	$2^6 \cdot 3$
$-1 + i$	$2 = 2$	$-(1 - i)$	-3	-3
i	$1 = 1$	i	22	$2 \cdot 11$
$1 + 3i$	$10 = 2 \cdot 5$	$(1 + i)(2 + i)$	91	$7 \cdot 13$
$1 + 5i$	$26 = 2 \cdot 13$	$-(1 - i)(2 - 3i)$	135	$3^3 \cdot 5$
$2 + i$	$5 = 5$	$(2 + i)$	72	$2^3 \cdot 3^2$
$5 + i$	$26 = 2 \cdot 13$	$-i(1 + i)(2 + 3i)$	147	$3 \cdot 7^2$

Example in $\mathbb{Z}[i]$

$$
\begin{array}{ccccccccccccccc}
-1 & i & (1+i) & (1-i) & (2+i) & (2-i) & (2+3i) & (2-3i) & 2 & 3 & 5 & 7 & 11 & 13 & 1/V
\end{array}
$$

$$
M = \begin{bmatrix}
1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 5 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 6 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 3 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 1
\end{bmatrix}
$$

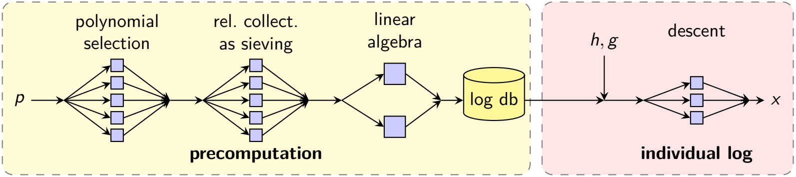
Example in $\mathbb{Z}[i]$

Right kernel mod $(p-1)/4 = 277$:
$\mathbf{v} = (0, 0, 1, 1, 168, 189, 136, 125, 275, 116, 197, 209, 119, 16, 160)$
Virtual logarithms

Target 314, generator $g = 2$
$g^2 \cdot 314 = 147 = 3 \cdot 7^2$
$\log_g 314 = (\log_v 3 + 2\log_v 7 - 2\log_v 2)/\log_v 2 = 8 \bmod (p-1)/4$
$g^8/314 = 354$, $354 = 2^{3(p-1)/4}$ of order 4,
$2^{839} = 314 \bmod p$

$\log_g 314 = 839$

Number Field Sieve today



slide N. Heninger

Latest DL record computation: 768-bit $\mathbb{F}_p$

Kleinjung, Diem, A. Lenstra, Priplata, Stahlke, Eurocrypt'2017.
$p = \lfloor 2^{766} \times \pi \rfloor + 62762$ prime, 768 bits, 232 decimal digits, $p =$

1219344858334286932696341909195796109526657386154251328029
2736561757668709803065055845773891258608267152015472257940
7293588325886803643328721799472154219914818284150580043314
8410869683590659346847659519108393837414567892730579162319

$(p-1)/2$ prime

$f(x) = 140x^4 + 34x^3 + 86x^2 + 5x - 55$

$g(x) = 370863403886416141150505523919527677231932618184100095924x^3$
$-1937981312833038778565617469829395544065255938015920309679x^2$
$-217583293626947899787577441128333027617541095004734736415x$
$+277260730400349522890422618473498148528706115003337935150$

Enumerate ($\sim 10^{12}$) all $f(x)$ s.t. $|f_i| \leqslant 165$
By construction, $|g_i| \approx p^{1/4}$

Latest DL record computation: 768-bit $\mathbb{F}_p$

$\gcd(f, g) = 1$ in $\mathbb{Q}[x]$
$\exists$ root m s.t. $f(m) = g(m) = 0 \pmod p$, $m =$

42902956292319703574889360640139954233871229273731672191 12
87949790195085714269561105202804934131487105126188235866 32
14844974131883926532462067740277566464441832406296509041 12
11026991626107428130330288372525887846431331219647577522 2

Multiplicative relations: for all $|a_i| \leq A \approx 2^{32}$, $\gcd(a_0, a_1) = 1$

- factors $\mathrm{Norm}_f = \mathrm{Resultant}(f, a_0 + a_1 x) \approx 130$ bits, 39 dd
- factors $\mathrm{Norm}_g = \mathrm{Resultant}(g, a_0 + a_1 x) \approx 290$ bits, 87 dd

Linear algebra: square sparse matrix of $23.5 \cdot 10^6$ rows
Total time: 5300 core-years on Intel Xeon E5-2660 2.2GHz

Complexity and key-sizes for cryptography

[Lenstra-Verheul'01] gives RSA key-sizes
Security estimates use

- asymptotic complexity of the best known algorithm (here NFS)
- latest record computation (now 768-bit)
- extrapolation

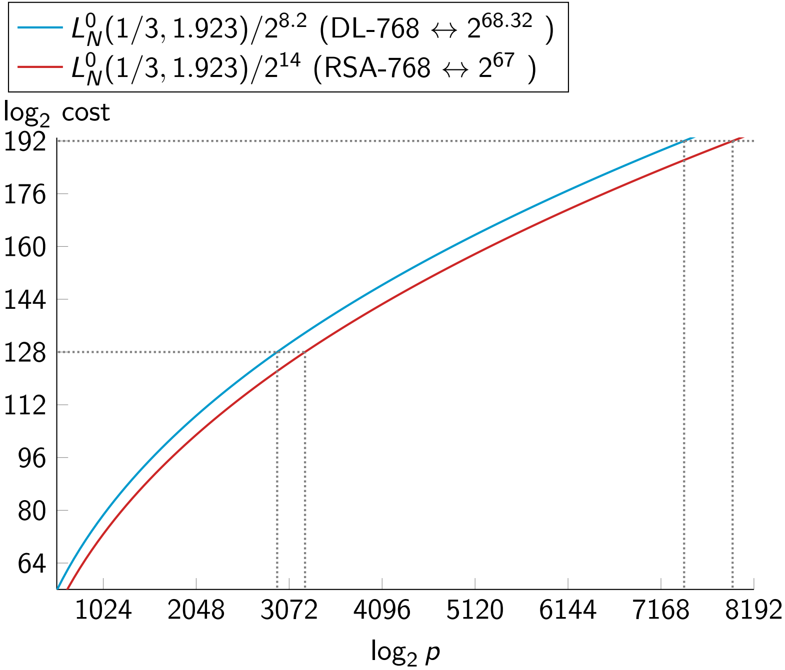
Complexity

Subexponential asymptotic complexity:

$$L_{p^n}(\alpha, c) = e^{(c+o(1))(\log p^n)^\alpha (\log \log p^n)^{1-\alpha}}$$

- $\alpha = 1$: exponential
- $\alpha = 0$: polynomial
- $0 < \alpha < 1$: sub-exponential (including NFS)

1. polynomial selection (precomp., 5% to 10% of total time)
2. relation collection $L_{p^n}(1/3, c)$
3. linear algebra $L_{p^n}(1/3, c)$
4. individual discrete log computation $L_{p^n}(1/3, c' < c)$


$L_N^0(1/3, 1.923)/2^{8.2}$ (DL-768 ↔ $2^{68.32}$)
$L_N^0(1/3, 1.923)/2^{14}$ (RSA-768 ↔ 2^{67})
$\log_2$ cost
192
176
160
144
128
112
96
80
64
1024
2048
3072
4096
5120
6144
7168
8192
$\log_2 p$

Key length

- `keylength.com`
- France: ANSSI RGS B

RSA modulus and prime fields for DL: 3072 to 3200 bits
sub-exponential complexity to invert DL in $\mathbb{F}_p$

Elliptic curves: over prime field of 256 bits (much smaller)
exponential cpx. to invert DL in $E(\mathbb{F}_p)$

Key length

- `keylength.com`
- France: ANSSI RGS B

RSA modulus and prime fields for DL: 3072 to 3200 bits
sub-exponential complexity to invert DL in $\mathbb{F}_p$

Elliptic curves: over prime field of 256 bits (much smaller)
exponential cpx. to invert DL in $E(\mathbb{F}_p)$

Why finite fields in 2019?

because old crypto in $\mathbb{F}_p$ is still in use
cpx $= L_p(1/3, 1.923)$ since 1993: very-well known
because of pairings: $\mathbb{F}_{p^n}$ since 2000

Cryptographic pairing: black-box properties

$(\mathbf{G}_1, +), (\mathbf{G}_2, +), (\mathbf{G}_T, \cdot)$ three cyclic groups of large prime order r
Bilinear Pairing: map $e : \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$

1. bilinear: $e(P_1 + P_2,\ Q) = e(P_1, Q) \cdot e(P_2, Q)$,
   $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. non-degenerate: $e(g_1, g_2) \neq 1$ for $\langle g_1 \rangle = \mathbf{G}_1$, $\langle g_2 \rangle = \mathbf{G}_2$
3. efficiently computable.

Mostly used in practice:

$$e([a]P, [b]Q) = e([b]P, [a]Q) = e(P, Q)^{ab} \ .$$

$\rightsquigarrow$ Many applications in asymmetric cryptography.

Examples of application

- 1984: idea of identity-based encryption formalized by Shamir
- 1999: first practical identity-based cryptosystem of Sakai-Ohgishi-Kasahara
- 2000: constructive pairings, Joux's tri-partite key-exchange
- 2001: IBE of Boneh-Franklin, short signatures Boneh-Lynn-Shacham

Rely on

- Discrete Log Problem (DLP): given $g, h \in \mathbf{G}$, compute x s.t. $g^x = h$ Diffie-Hellman Problem (DHP)
- bilinear DLP and DHP
  Given $\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_T, g_1, g_2, g_T$ and $h \in \mathbf{G}_T$, compute $P \in \mathbf{G}_1$ s.t. $e(P, g_2) = h$, or $Q \in \mathbf{G}_2$ s.t. $e(g_1, Q) = h$
  if $g_T^x = h$ then $e(g_1^x, g_2) = e(g_1, g_2^x) = g_T^x = h$
- pairing inversion problem

Examples of application

Pairings are bilinear maps satisfying DH-like assumptions, and provide

- Identity-based encryption (IBE)
- Broadcast encryption with efficient key distribution and rekeying
- signatures
  - (short) signatures (Boneh–Lynn–Shacham)
  - aggregate signatures
- zero-knowledge (ZK) proofs
  - non-interactive ZK proofs (NIZK)
  - ZK-SNARK (Z-cash)

Multilinear maps are not as efficient as elliptic pairings yet.

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_{p^n})[r] \times E(\mathbb{F}_{p^n})[r] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_{p^n})[r] \times E(\mathbb{F}_{p^n})[r] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_{p^n})[r] \times E(\mathbb{F}_{p^n})[r] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \;:\; E(\mathbb{F}_{p^n})[r] \times E(\mathbb{F}_{p^n})[r] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P,[b]Q) = e(P,Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{r})$)

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_{p^n})[r] \times E(\mathbb{F}_{p^n})[r] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{r})$)
- discrete logarithm computation in $\mathbb{F}_{p^n}^*$: **easier, subexponential** $\rightarrow$ take a large enough field

Pairing-friendly curves are special

$r \mid p^n - 1$, $\mathbf{G}_T \subset \mathbb{F}_{p^n}$, n is minimal : **embedding degree**
Tate Pairing: $e: \ \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$
When n is small i.e. $1 \leqslant n \leqslant 24$, the curve is *pairing-friendly*.
This is very rare: usually $\log n \sim \log r$ ([Balasubramanian Koblitz]).

$\mathbf{G}_T \subset p^n$	p^2, p^6	p^3, p^4, p^6	p^{12}	p^{16}	p^{18}
Curve	supersingular	MNT	BN, BLS12	KSS16	KSS18

MNT, $n = 6$:
$p(x) = 4x^2 + 1, \#E(\mathbb{F}_p) x^2 \mp 2x + 1$
BN, $n = 12$:
$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1,$
$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$

Discrete Log in $\mathbb{F}_{p^n}$

$\mathbb{F}_{p^n}$ much less investigated than $\mathbb{F}_p$ or integer factorization.

- 2000 LUC, XTR cryptosystems: multiplicative subgroup of prime order $r \mid p+1$ of $\mathbb{F}_{p^2}$, $r \mid p^2 - p + 1$ of $\mathbb{F}_{p^6}$
- How fast can we compute DL in $\mathbb{F}_{p^n}$, $n = 2, 6$?
- 2005 [Granger Vercauteren] $L_{p^n}(1/2)$
- 2006 Joux–Lercier–Smart–Vercauteren $L_{p^n}(1/3, 2.423)$ (NFS-HD)
- rising of pairings: what is the security of DL in $\mathbb{F}_{2^n}$,$\mathbb{F}_{3^m}$,$\mathbb{F}_{p^{12}}$?

Special Tower NFS

- Special NFS in $\mathbb{F}_{p^n}$: Joux–Pierrot 2013
- Tower NFS (TNFS): Barbulescu Gaudry Kleinjung 2015
- Extended Tower NFS: Kim–Barbulescu, Kim–Jeong, Sarkar–Singh 2016
- Tower of number fields

Use more structure: subfields

Special Tower NFS

$\mathbb{F}_{p^6}$, subfield $\mathbb{F}_{p^2}$ defined by y^2+1
$g = (g_{00} + g_{01} i) + (g_{10} + g_{11} i)x + (g_{20} + g_{21} i)x^2 \in \mathbb{F}_{p^6}$
Idea: $a_0 + a_1 x \;\rightarrow\; \mathbf{a} = (a_{00} + a_{01} i) + (a_{10} + a_{11} i)x$
Integers to factor are **much smaller**

- factors integer $\mathrm{Norm}_f = \mathrm{Res}(\mathrm{Res}(\mathbf{a}, f_y(x)), y^2+1)$
- factors integer $\mathrm{Norm}_g = \mathrm{Res}(\mathrm{Res}(\mathbf{a}, g_y(x)), y^2+1)$

Res = resultant of polynomials

Complexities

large characteristic $p = L_{p^n}(\alpha),\ \alpha > 2/3$:	
$(64/9)^{1/3} \simeq 1.923$	NFS
special p:	
$(32/9)^{1/3} \simeq 1.526$	SNFS

medium characteristic $p = L_{p^n}(\alpha),\ 1/3 < \alpha < 2/3$:	
$(96/9)^{1/3} \simeq 2.201$	prime n NFS-HD (Conjugation)
$(48/9)^{1/3} \simeq 1.747$	composite n, best case of TNFS: when parameters fit perfectly
special p:	
$(64/9)^{1/3} \simeq 1.923$	NFS-HD+Joux–Pierrot'13
$(32/9)^{1/3} \simeq 1.526$	composite n, best case of STNFS

Estimating key sizes for DL in $\mathbb{F}_{p^n}$

- Latest variants of TNFS (Kim–Barbulescu, Kim–Jeong) seem most promising for $\mathbb{F}_{p^n}$ where n is composite
- We need record computations if we want to extrapolate from asymptotic complexities
- The asymptotic complexities do not correspond to a fixed n, but to a ratio between n and p

Largest record computations in $\mathbb{F}_{p^n}$ with NFS[1]

Finite field	Size of p^n	Cost: CPU days	Authors	sieving dim
$\mathbb{F}_{p^{12}}$	203	11	[HAKT13]	7
$\mathbb{F}_{p^6}$	422	9,520	[GGMT17]	3
$\mathbb{F}_{p^5}$	324	386	[GGM17]	3
$\mathbb{F}_{p^4}$	392	510	[BGGM15b]	2
$\mathbb{F}_{p^3}$	593	8,400	[GGM16]	2
$\mathbb{F}_{p^2}$	595	175	[BGGM15a]	2
$\mathbb{F}_p$	768	1,935,825	[KDLPS17]	2

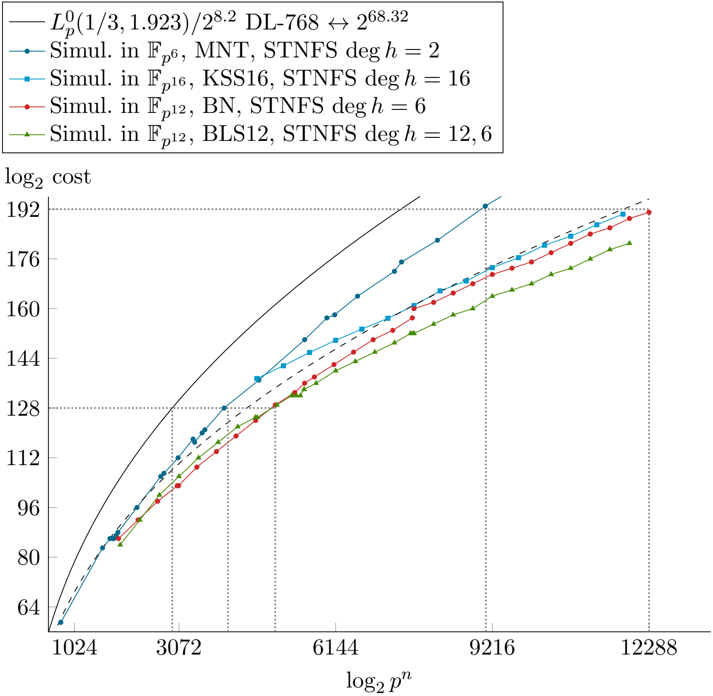
None used TNFS, only NFS and NFS-HD were implemented.

[1] Data extracted from DiscreteLogDB by L.Grémy

Simulation without sieving

Implementation of Barbulescu–Duquesne technique
space: $\mathcal{S} = \{\sum a_{0i} y^i + (\sum a_{1i} y^i) x,\ |a_{ji}| < A\}$
Variants:

- compute $\alpha(f), \alpha(g)$ (w.r.t. subfield)
- select polys f, g with good low $\alpha(f), \alpha(g)$
- Monte-Carlo simulation with 10^6 points in $\mathcal{S}$ taken at random. For each point:
  1. compute its algebraic norm N_f, N_g in each number field
  2. smoothness probability with Dickman-ρ
- Average smoothness probability over the subset of points $\rightarrow$ estimation of the total number of possible relations in $\mathcal{S}$
- dichotomy to approach the best balanced parameters: smoothness bound B, coefficient bound A.


$L_p^0(1/3, 1.923)/2^{8.2}$ DL-768 ↔ $2^{68.32}$
Simul. in $\mathbb{F}_{p^6}$, MNT, STNFS deg $h = 2$
Simul. in $\mathbb{F}_{p^{16}}$, KSS16, STNFS deg $h = 16$
Simul. in $\mathbb{F}_{p^{12}}$, BN, STNFS deg $h = 6$
Simul. in $\mathbb{F}_{p^{12}}$, BLS12, STNFS deg $h = 12, 6$
$\log_2$ cost
192
176
160
144
128
112
96
80
64
1024
3072
6144
9216
12288
$\log_2 p^n$

Key size for pairings

$\mathbb{F}_{p^n}$, curve	cost DL 2^{128}		cost DL 2^{192}	
	$\log_2 p$	$\log_2 p^n$	$\log_2 p$	$\log_2 p^n$
$\mathbb{F}_p$	3072–3200		7400–8000	
$\mathbb{F}_{p^6}$, MNT	640–672	3840–4032	≈ 1536	≈ 9216
$\mathbb{F}_{p^{12}}$, BN	416–448	4992–5376	≈ 1024	≈ 12288
$\mathbb{F}_{p^{12}}$, BLS	416–448	4992–5376	≈ 1120	≈ 13440
$\mathbb{F}_{p^{16}}$, KSS	330	5280	≈ 768	≈ 12288

Future work

- automatic tool (currently developed in Python/SageMath)
- $\mathbb{F}_{p^8}, \mathbb{F}_{p^{15}}, \mathbb{F}_{p^{18}}, \mathbb{F}_{p^{24}}$
- Compare Special-TNFS and TNFS
- $a_0 + a_1 x \rightarrow$ consider $a_0 + a_1 x + a_2 x^2$, $a_i = a_{i0} + a_{i1} y + \ldots$
- Estimate the proportion of duplicate relations (2%, 20%, 60%?)
- How to sieve very efficiently in even dimension 4 to 24 to avoid costly factorization in the relation collection?

Bibliography I

L. Adleman.
A subexponential algorithm for the discrete logarithm problem with applications to cryptography.
In *20th FOCS*, pages 55–60. IEEE Computer Society Press, Oct. 1979.
https://doi.org/10.1109/SFCS.1979.2.

R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain.
DL record computation in GF(p^4) of 392 bits (120dd).
Announcement at the CATREL workshop, October 2nd 2015.
http://www.lix.polytechnique.fr/ guillevic/docs/guillevic-catrel15-talk.pdf.

R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain.
Improving NFS for the discrete logarithm problem in non-prime finite fields.
In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 129–155. Springer, Heidelberg, Apr. 2015.

R. Barbulescu, P. Gaudry, and T. Kleinjung.
The tower number field sieve.
In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 31–55. Springer, Heidelberg, Nov. / Dec. 2015.

Bibliography II

R. Barbulescu and A. Lachand.
Some mathematical remarks on the polynomial selection in NFS.
Math. Comp., 86(303):397–418, 2017.
https://hal.inria.fr/hal-00954365,
https://doi.org/10.1090/mcom/3112.

E. R. Canfield, P. Erdős, and C. Pomerance.
On a problem of Oppenheim concerning "factorisatio numerorum".
Journal of Number Theory, 17(1):1–28, 1983.
https://math.dartmouth.edu/~carlp/PDF/paper39.pdf.

S. Chatterjee, A. Menezes, and F. Rodríguez-Henríquez.
On instantiating pairing-based protocols with elliptic curves of embedding degree one.
IEEE Trans. Computers, 66(6):1061–1070, 2017.

D. Coppersmith.
Fast evaluation of logarithms in fields of characteristic two.
IEEE Transactions on Information Theory, 30(4):587–594, 1984.
http://ieeexplore.ieee.org/document/1056941/,
https://doi.org/10.1109/TIT.1984.1056941.

Bibliography III

D. Coppersmith, A. M. Odlyzko, and R. Schroeppel.
Discrete logarithms in $\mathrm{GF}(p)$.
Algorithmica, 1(1):1–15, 1986.
https://dl.acm.org/citation.cfm?id=6835,
https://doi.org/10.1007/BF01840433.

D. Freeman, M. Scott, and E. Teske.
A taxonomy of pairing-friendly elliptic curves.
Journal of Cryptology, 23(2):224–280, Apr. 2010.

P. Gaudry, A. Guillevic, and F. Morain.
Discrete logarithm record in GF(p^3) of 592 bits (180 decimal digits).
Number Theory list, item 004930, August 15 2016.
https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;ae418648.1608.

D. M. Gordon.
Discrete logarithms in $\mathrm{GF}(p)$ using the number field sieve.
SIAM Journal on Discrete Mathematics, 6(1):124–138, 1993.
https://www.ccrwest.org/gordon/log.pdf.

Bibliography IV

L. Grémy, A. Guillevic, and F. Morain.
Discrete logarithm record computation in GF(p^5) of 100 decimal digits using NFS with 3-dimensional sieving.
Number Theory list, item 004981, August 1st 2017.
https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;68019370.1708.

L. Grémy, A. Guillevic, F. Morain, and E. Thomé.
Computing discrete logarithms in $\mathbb{F}_{p^6}$.
In C. Adams and J. Camenisch, editors, *SAC 2017*, volume 10719 of *LNCS*, pages 85–105. Springer, Heidelberg, Aug. 2017.

A. Guillevic and F. Morain.
Pairings for Engineers, chapter 9 – Discrete Logarithms, pages 203–242.
CRC Press Taylor and Francis group, Spring 2016.
N. ElMrabet and M. Joye (eds),
https://www.crcpress.com/Guide-to-Pairing-Based-Cryptography/El-Mrabet-Joye/p/book/9781498729505,
https://hal.inria.fr/hal-01420485v2.

A. Guillevic, F. Morain, and E. Thomé.
Solving discrete logarithms on a 170-bit MNT curve by pairing reduction.
In R. Avanzi and H. M. Heys, editors, *SAC 2016*, volume 10532 of *LNCS*, pages 559–578. Springer, Heidelberg, Aug. 2016.

Bibliography V

K. Hayasaka, K. Aoki, T. Kobayashi, and T. Takagi.
An experiment of number field sieve for discrete logarithm problem over $GF(p^{12})$.
In M. Fischlin and S. Katzenbeisser, editors, *Number Theory and Cryptography*, volume 8260 of *LNCS*, pages 108–120. Springer, 2013.

K. Hayasaka, K. Aoki, T. Kobayashi, and T. Takagi.
A construction of 3-dimensional lattice sieve for number field sieve over $\mathbb{F}_{p^n}$.
Cryptology ePrint Archive, Report 2015/1179, 2015.
http://eprint.iacr.org/2015/1179.

A. Joux, R. Lercier, N. Smart, and F. Vercauteren.
The number field sieve in the medium prime case.
In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 326–344. Springer, Heidelberg, Aug. 2006.

T. Kim and R. Barbulescu.
Extended tower number field sieve: A new complexity for the medium prime case.
In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 543–571. Springer, Heidelberg, Aug. 2016.

Bibliography VI

T. Kleinjung, C. Diem, A. K. Lenstra, C. Priplata, and C. Stahlke.
Computation of a 768-bit prime field discrete logarithm.
In J. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 185–201. Springer, Heidelberg, Apr. / May 2017.

M. Kraitchik.
Théorie des Nombres.
Gauthier–Villars, 1922.

M. Kraitchik.
Recherches sur la Théorie des Nombres.
Gauthier–Villars, 1924.

H. Lenstra and C. Pomerance.
A rigorous time bound for factoring integers.
J. Amer. Math. Soc., 5(3):483–516, 1992.

D. V. Matyukhin.
Effective version of the number field sieve for discrete logarithms in the field $\mathrm{GF}(p^k)$ (in Russian).
Trudy po Discretnoi Matematike, 9:121–151, 2006.

Bibliography VII

K. S. McCurley.
The discrete logarithm problem.
In C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, pages 49–74. AMS, 1990.
http://www.mccurley.org/papers/dlog.pdf.

A. Menezes, P. Sarkar, and S. Singh.
Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography.
In R. C. Phan and M. Yung, editors, *Mycrypt Conference, Revised Selected Papers*, volume 10311 of *LNCS*, pages 83–108, Kuala Lumpur, Malaysia, December 1-2 2016. Springer.

C. Pomerance.
Fast, rigorous factorization and discrete logarithm algorithms.
In D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, editors, *Discrete algorithms and complexity*, pages 119–143, Orlando, Florida, 1987. Academic Press.
https://math.dartmouth.edu/~carlp/disclog.pdf.

Bibliography VIII

P. Sarkar and S. Singh.
A general polynomial selection method and new asymptotic complexities for the tower number field sieve algorithm.
In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 37–62. Springer, Heidelberg, Dec. 2016.

P. Sarkar and S. Singh.
New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields.
In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 429–458. Springer, Heidelberg, May 2016.

O. Schirokauer.
Discrete logarithms and local units.
Philos. Trans. Roy. Soc. London Ser. A, 345(1676):409–423, 1993.
http://rsta.royalsocietypublishing.org/content/345/1676/409,
http://doi.org/10.1098/rsta.1993.0139.

A. E. Western and J. C. P. Miller.
Tables of Indices and Primitive Roots, volume 9 of *Royal Society Mathematical Tables*.
Cambridge University Press, 1968.