Pairing-Friendly Curves and Tower Number Field Sieve Algorithm

Aurore Guillevic

Inria Nancy, France

10/07/2019

SIAM-AG Bern, Switzerland

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 we 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 $\mathbb{F}_{2^n}$ ($\approx$ 1979)
- elliptic curve $E(\mathbb{F}_p)$ (1985)

Discrete log problem

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

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \dots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms
- independent search in each distinct subgroup + CRT (Pohlig-Hellman)

Discrete log problem

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

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms
- independent search in each distinct subgroup + CRT (Pohlig-Hellman)

$\rightarrow$ choose G of large prime order (no subgroup)

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

$\rightarrow$ security level 128 bits means $\sqrt{\#G} \geq 2^{128}$
take $\#G = 2^{256}$
analogy with symmetric crypto, keylength 128 bits (16 bytes)

Discrete log problem

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

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms
- independent search in each distinct subgroup + CRT (Pohlig-Hellman)

→ choose G of large prime order (no subgroup)

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

→ security level 128 bits means $\sqrt{\#G} \geq 2^{128}$
take $\#G = 2^{256}$
analogy with symmetric crypto, keylength 128 bits (16 bytes)

Use additional structure of G if any.

Number Field: Toy example with $\mathbb{Z}[i]$

If $p = 1 \bmod 4$, $\exists\ U, V$ s.t. $p = U^2 + V^2$
and $|U|, |V| < \sqrt{p}$
$U/V \equiv m \mod p$ and $m^2 + 1 = 0 \mod p$

Define a map from $\mathbb{Z}[i]$ to $\mathbb{Z}/p\mathbb{Z}$

$$\begin{aligned} \phi\colon \mathbb{Z}[i] &\to \mathbb{Z}/p\mathbb{Z} \\ i &\mapsto m \bmod p \text{ where } m = U/V,\ m^2 + 1 = 0 \bmod p \end{aligned}$$

ring homomorphism $\phi(a + bi) = a + bm$

$$\phi(\underbrace{a + bi}_{\substack{\text{factor in} \\ \mathbb{Z}[i]}}) = a + bm = (a + b\ \underbrace{U/V}_{=m}) = (\underbrace{aV + bU}_{\text{factor in } \mathbb{Z}})V^{-1} \mod p$$

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

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

Rational side

$\mathcal{F}_{\text{rat}} = \{2, 3, 5, 7, 11, 13\}$ primes up to B
$g(x) = Vx - U$

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

Rational side

$\mathcal{F}_{\text{rat}} = \{2, 3, 5, 7, 11, 13\}$ primes up to B
$g(x) = Vx - U$

Algebraic side: think about the complex number in $\mathbb{C}$

$-i(1+i)^2 = 2,\ (2+i)(2-i) = 5,\ (2+3i)(2-3i) = 13$
$\mathcal{F}_{\text{alg}} = \{1+i, 2+i, 2-i, 2+3i, 2-3i\}$
"primes" of norm up to B
$f(x) = x^2 + 1$

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

Rational side

$\mathcal{F}_{\text{rat}} = \{2, 3, 5, 7, 11, 13\}$ primes up to B
$g(x) = Vx - U$

Algebraic side: think about the complex number in $\mathbb{C}$

$-i(1+i)^2 = 2$, $(2+i)(2-i) = 5$, $(2+3i)(2-3i) = 13$
$\mathcal{F}_{\text{alg}} = \{1+i, 2+i, 2-i, 2+3i, 2-3i\}$
"primes" of norm up to B
$f(x) = x^2 + 1$

Units

$\mathcal{U}_{\text{alg}} = \{-1, i, -i\}$

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

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

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

$M =$

2	3	5	7	11	13	$\frac{1}{V}$	-1	i	$1+i$	$2+i$	$2-i$	$2+3i$	$2-3i$
0	0	0	0	0	0	0	1	2	0	0	0	0	0
0	0	0	1	0	0	1	1	1	1	2	0	0	1
0	1	0	1	1	0	1	1	1	0	3	0	0	0
5	0	0	1	0	0	1	0	0	0	2	0	1	0
1	3	0	0	0	0	1	0	1	0	0	1	1	0
0	0	0	0	0	1	1	1	0	0	0	2	0	0
2	0	0	1	0	0	1	0	0	0	0	1	0	0
4	0	0	0	0	0	1	1	0	0	0	0	0	1
6	1	0	0	0	0	1	1	0	0	0	3	0	0
0	1	0	0	0	0	1	1	1	1	0	0	0	0
1	0	0	0	1	0	1	0	1	0	0	0	0	0
0	0	0	1	0	1	1	0	0	1	1	0	0	0
0	3	1	0	0	0	1	0	1	1	0	0	0	1
3	2	0	0	0	0	1	0	0	0	1	0	0	0
0	1	0	2	0	0	1	1	1	1	0	0	1	0

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

$M =$

2	3	5	7	11	13	$\frac{1}{V}$	-1	i	$1+i$	$2+i$	$2-i$	$2+3i$	$2-3i$
							1	2					
			1			1	1	1	1	2			1
	1		1	1		1	1	1		3			
5			1			1				2		1	
1	3					1		1			1	1	
					1	1	1				2		
2			1			1					1		
4						1	1						1
6	1					1	1				3		
	1					1	1	1	1				
1				1		1		1					
			1		1	1			1	1			
	3	1				1		1	1				1
3	2					1				1			
	1		2			1	1	1	1			1	

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

$M =$

2	3	5	7	11	13	$\frac{1}{V}$	-1	i	$1+i$	$2+i$	$2-i$	$2+3i$	$2-3i$
							-1	-2					
			1			1	-1	-1	-1	-2			-1
	1		1	1		1	-1	-1		-3			
5			1			1				-2		-1	
1	3					1		-1			-1	-1	
					1	1	-1				-2		
2			1			1					-1		
4						1	-1						-1
6	1					1	-1				-3		
	1					1	-1	-1	-1				
1				1		1		-1					
			1		1	1			-1	-1			
	3	1				1		-1	-1				-1
3	2					1				-1			
	1		2			1	-1	-1	-1			-1	

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

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{139, 84, 233, 68, 201}_{\text{algebraic side}})$$

Logarithms (in some basis)

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

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{139, 84, 233, 68, 201}_{\text{algebraic side}})$$

Logarithms (in some basis)

Rational side: logarithms of $\{2, 3, 5, 7, 11, 13\}$ in basis 2

$\boldsymbol{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

$\rightarrow$ order 4 subgroup

$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

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

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{139, 84, 233, 68, 201}_{\text{algebraic side}})$$

Logarithms (in some basis)

Rational side: logarithms of $\{2, 3, 5, 7, 11, 13\}$ in basis 2

$\boldsymbol{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

$\to$ order 4 subgroup

$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Target 314, generator $g = 2$

$314 = -20/7 \bmod p = -2^2 \cdot 5/7$

$$\begin{aligned} \log_g 314 &= \log_g -1 + 2\log_g 2 + \log_g 5 - \log_g 7 \\ &= (p-1)/2 + 2 + 594 - 311 = 839 \bmod p - 1 \end{aligned}$$

$2^{839} = 314 \bmod p$

Number Field Sieve

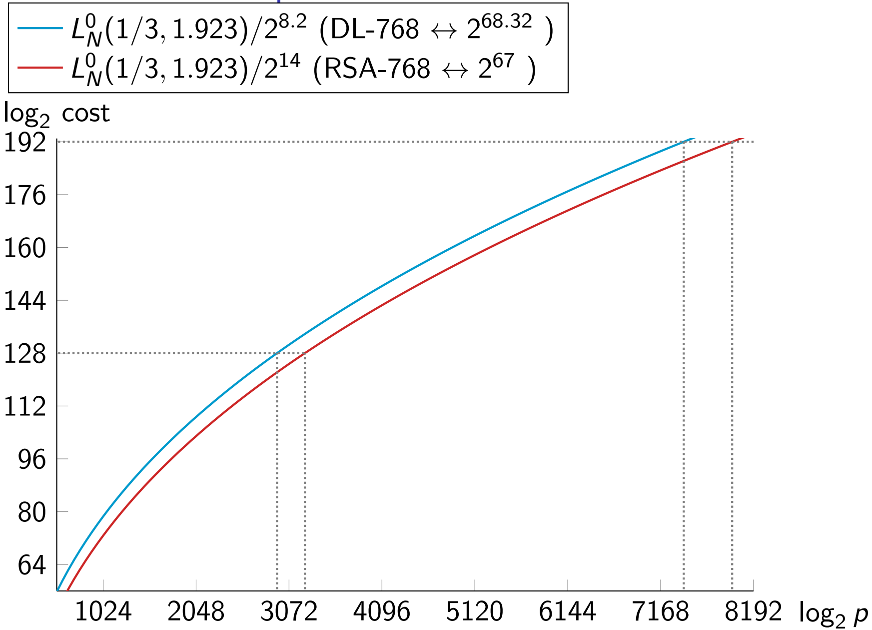
Since 1993 (Gordon, Schirokauer):

$$L_p(1/3, c) = e^{(c+o(1))(\log p)^{1/3}(\log\log p)^{2/3}}$$

- polynomial selection
- **relation collection** $L_p(1/3, 1.923)$
  sieve to enumerate efficiently (a, b) pairs
- **sparse linear algebra** $L_p(1/3, 1.923)$
  compute right kernel mod prime ℓ, block-Wiedemann alg.
- individual discrete logarithm

Latest record computation: 768-bit prime p, $\ell = (p-1)/2$ prime
Kleinjung, Diem, A. Lenstra, Priplata, Stahlke, Eurocrypt'2017
Total time: 5300 core-years on Intel Xeon E5-2660 2.2GHz

Lenstra Verheul extrapolation



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
(identity-based encryption, short signatues, NIZK, ZK-SNARK...)

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

Attacks

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

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.

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

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.

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

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, the curve is *pairing-friendly*.
This is very rare: usually $\log n \sim \log r$ ([Balasubramanian Koblitz]).

Barreto-Naehrig (BN), $n = 12$:
$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$
$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$
$D = -3$, $j = 0$, $\mathbf{G}_T \subset \mathbb{F}_{p^{12}}$

p is special

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

$\mathbb{F}_{p^n}$ much less investigated than $\mathbb{F}_p$ or integer factorization.
Much better results in pairing-related fields

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

$\mathbb{F}_{p^n}$ much less investigated than $\mathbb{F}_p$ or integer factorization.
Much better results in pairing-related fields

- 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

$\mathbb{F}_{p^{2k}}$, subfield $\mathbb{F}_{p^2}$ defined by $y^2 + 1$
Idea: $a + bx$ in NFS $\rightarrow$ $(a_0 + a_1 i) + (b_0 + b_1 i)x$ in TNFS
Integers to factor are **much smaller**

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

Res = resultant of polynomials

Special Tower NFS

$\mathbb{F}_{p^{2k}}$, subfield $\mathbb{F}_{p^2}$ defined by $y^2 + 1$
Idea: $a + bx$ in NFS $\rightarrow$ $(a_0 + a_1 i) + (b_0 + b_1 i)x$ in TNFS
Integers to factor are **much smaller**

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

Res = resultant of polynomials
$p = p(s)$ is special

Special Tower NFS

$\mathbb{F}_{p^{2k}}$, subfield $\mathbb{F}_{p^2}$ defined by $y^2 + 1$
Idea: $a + bx$ in NFS $\rightarrow$ $(a_0 + a_1 i) + (b_0 + b_1 i)x$ in TNFS
Integers to factor are **much smaller**

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

Res = resultant of polynomials
$p = p(s)$ is special

Index calculus in the 80's: implemented *before* complexity known
TNFS: complexity known, no implementation

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

Ranking polynomials: Murphy's α and E

B. A. Murphy, 1999
Input: irreducible polynomials f, g, $p \mid \mathrm{Res}(f, g)$

- $\alpha(f)$: bias in smoothness between norms and integers
  $\alpha(f), \alpha(g) < 0$ wanted
- $E(f, g, B_f, B_g, \text{area})$: estimation of the yield of polynomials
  B_f, B_g smoothness bounds of f, g sides
  How many relations would (f, g) produce?
- Rank many (f_i, g_i), choose the best pair

Ranking polynomials: Murphy's α and E

B. A. Murphy, 1999
Input: irreducible polynomials f, g, $p \mid \mathrm{Res}(f, g)$

- $\alpha(f)$: bias in smoothness between norms and integers
  $\alpha(f), \alpha(g) < 0$ wanted
- $E(f, g, B_f, B_g, \text{area})$: estimation of the yield of polynomials
  B_f, B_g smoothness bounds of f, g sides
  How many relations would (f, g) produce?
- Rank many (f_i, g_i), choose the best pair

Generalization to the TNFS setting:

- $\alpha(h, f)$, $\alpha(h, g)$
  SageMath & Magma code, generalization from `cado-nfs` α
  (Bai, Gaudry, Hanrot, Thomé, Zimmermann)
- Monte-Carlo simulation for Murphy's E

Simulation without sieving

Polynomial selection: for many pairs (f, g)

- compute $\alpha(h, f), \alpha(h, g)$ (w.r.t. subfield) **bias in smoothness**
- select polys f, g with negative bias $\alpha(f), \alpha(g)$ if possible

- **Monte-Carlo** simulation with 10^6 random samples from $\mathcal{S} = \{(a_0 + a_1 y + \ldots + a_d y^d) + (b_0 + b_1 y + \ldots + b_d y^d)x, \ |a_i|, |b_j| < A\}$
  For each sample:
  1. compute its algebraic norm N_f, N_g in each number field
  2. smoothness probability (N_f, α_f), (N_g, α_g) with Dickman-ρ

- Average smoothness probability of samples
  $\rightarrow$ estimation of the total number of possible relations in $\mathcal{S}$
  $\rightarrow$ **Murphy's E for TNFS**

Simulation without sieving

Polynomial selection: for many pairs (f, g)

- compute $\alpha(h, f), \alpha(h, g)$ (w.r.t. subfield) **bias in smoothness**
- select polys f, g with negative bias $\alpha(f), \alpha(g)$ if possible
- **Monte-Carlo** simulation with 10^6 random samples from $\mathcal{S} = \{(a_0 + a_1 y + \ldots + a_d y^d) + (b_0 + b_1 y + \ldots + b_d y^d)x, \ |a_i|, |b_j| < A\}$
  For each sample:
  1. compute its algebraic norm N_f, N_g in each number field
  2. smoothness probability (N_f, α_f), (N_g, α_g) with Dickman-ρ
- Average smoothness probability of samples
  $\rightarrow$ estimation of the total number of possible relations in $\mathcal{S}$
  $\rightarrow$ **Murphy's E for TNFS**

dichotomy to approach the best balanced parameters

smoothness bound B, coefficient bound A.

$\rightarrow$ refinement of Barbulescu–Duquesne technique [BD18]

Murphy's α function

$\alpha(f)$ for NFS estimates the bias in smoothness

Algebraic norms in $K_f = \mathbb{Q}[x]/(f(x))$ of $\log_2 N_f$ bits have same smoothness proba as integers of $\log_2 N_f + \alpha(f)/\log(2)$ bits
$\to \alpha(f) < 0$ wanted
$\alpha(f)$ computes the exact number of roots of $f(x) \bmod \ell^k$ for all primes $\ell < 2000$ (say)
Easy prime $\ell \nmid \mathrm{disc}(f)$, tricky prime $\ell \mid \mathrm{disc}(f)$

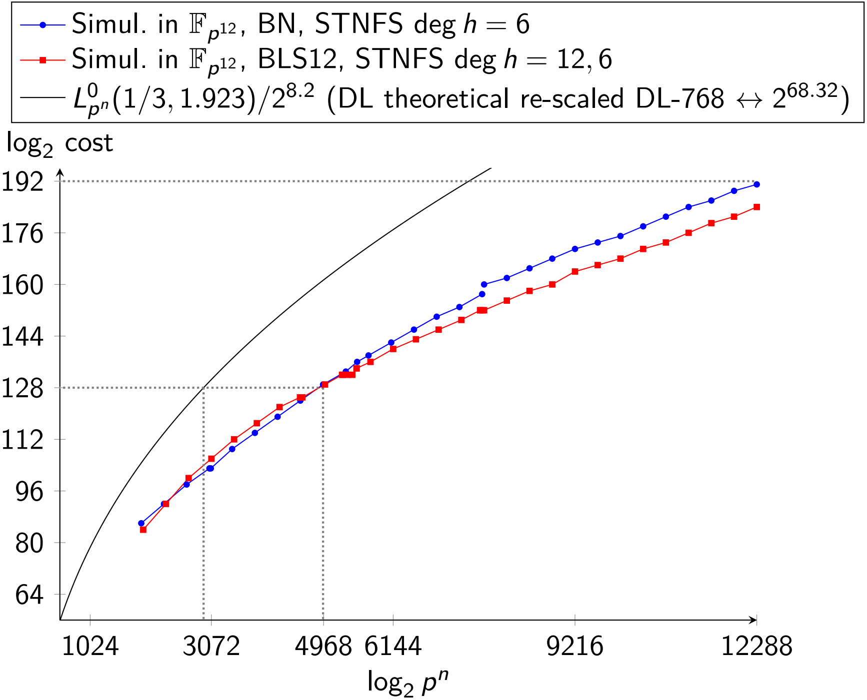
Implementation for TNFS

Reverse-engineering of
`cado-nfs/polyselect/{auxiliary.c,alpha.sage}`
Magma and SageMath
`https://gitlab.inria.fr/tnfs-alpha/alpha`
Same algorithm, prime $\ell \to$ prime ideal $\mathfrak{l}$

Example : Barreto-Naehrig curve, p 254 bits

$p = 36s^4 + 36s^3 + 24s^2 + 6s + 1$ where $s = -(2^{62} + 2^{55} + 1)$
$f = 36x^8 + 36yx^6 + 24y^2x^4 + 6y^3x^2 + y^4$
$g = x^2 + sy = x^2 + 4647714815446351873y$
$B = 2000$

h	$1/\zeta_{K_h}(2)$	$\alpha(h, f, B)$	$\alpha(h, g, B)$	$\alpha_f + \alpha_g$
$y^6 + y^5 - y^2 - y - 1$	0.953	2.042	2.479	4.521
$y^6 - y^4 + y^3 + y^2 - 1$	0.917	1.288	1.740	3.028
$y^6 + y^3 + y^2 - y - 1$	0.917	2.419	2.876	5.295
$y^6 + y^5 - y^3 + y - 1$	0.909	0.278	2.357	2.636
$y^6 + y^5 + y^4 + y^3 + y^2 + y - 1$	0.883	2.341	2.033	4.374
$y^6 + y^4 + y^3 + y - 1$	0.867	0.899	2.526	3.425
$y^6 + y^4 + y^2 + y + 1$	0.836	1.955	1.141	3.095
$y^6 + y^5 + y^2 - y + 1$	0.763	0.891	1.264	2.155
$y^6 + y^5 - y^4 + y^3 + y^2 + y - 1$	0.756	0.956	1.177	2.133
$y^6 + y^5 + y - 1$	0.736	1.925	2.108	4.032
$y^6 + y^5 + y^3 - y^2 + y - 1$	0.732	1.729	2.099	3.828
$y^6 + y^3 + y - 1$	0.728	−0.250	1.191	0.941
$y^6 + y^3 - y + 1$	0.720	1.605	1.348	2.952
$y^6 + y^3 + y^2 + 1$	0.718	1.151	1.294	2.445
$y^6 - y^4 + y^3 - y^2 - y - 1$	0.710	0.406	2.278	2.684
$y^6 + y^5 - y^3 + y^2 - y + 1$	0.697	1.572	0.818	2.390
$y^6 + y^4 + y + 1$	0.679	1.319	1.683	3.002


Simul. in $\mathbb{F}_{p^{12}}$, BN, STNFS deg $h = 6$
Simul. in $\mathbb{F}_{p^{12}}$, BLS12, STNFS deg $h = 12, 6$
$L^0_{p^n}(1/3, 1.923)/2^{8.2}$ (DL theoretical re-scaled DL-768 $\leftrightarrow 2^{68.32}$)
$\log_2$ cost
192
176
160
144
128
112
96
80
64
1024
3072
4968
6144
9216
12288
$\log_2 p^n$

Numerical example: BLS12-446 bits

$p(x) = (x-1)^2(x^4 - x^2 + 1)/3 + x$
$r(x) = x^4 - x^2 + 1$
$s = -(2^{74} + 2^{73} + 2^{63} + 2^{57} + 2^{50} + 2^{17} + 1)$
seed with `enumerate_sparse_T.sage` [G. Masson Thomé]
`https://gitlab.inria.fr/smasson/cocks-pinch-variant`
$p = p(s)$ of 446 bits, twist-secure subgroup-secure curve
p^k 5352 bits

$h = Y^6 - Y^4 + Y^3 - Y + 1$
$f_y = X^{12} - 2yX^{10} + 2y^3X^6 + y^5X^2 + y^4 - y^3 + y - 1$
$g_y = X^2 - uy = X^2 + 28343567510342708887553y$

$A = 968,\ B = 2^{68.2}$
Estimated cost: $\approx 2^{132}$

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
$\mathbb{F}_{p^{18}}$, KSS	348	6264	≈ 640	≈ 11520
$\mathbb{F}_{p^{24}}$, BLS			≈ 512	≈ 12288

- BN-382 and BLS12-381 $\approx 2^{123}$
- BN-446 and BLS12-446 $\approx 2^{132}$
- BN-462 and BLS12-461 $\approx 2^{135}$

Other curves:

- Fotiadis-Martindale [FM19] $k = 12$ with $r = r_{BN}$ like BLS12
- modified Cocks-Pinch with $k = 8$ and $\rho = 2.125$ [GMT19]

Future work

- automatic tool (currently developed in Python/SageMath)
- Compare Special-TNFS, TNFS and SNFS
- $a_0 + a_1 x \to$ consider $a_0 + a_1 x + a_2 x^2$, $a_i = a_{i0} + a_{i1} y + \ldots$
- Estimate the proportion of duplicate relations due to units (2%, 20%, 60%?)
- How to sieve very efficiently in even dimension 4 to 24 to avoid costly factorization in the relation collection?
- Record computation in $\mathbb{F}_{p^6}$

Code available at
`https://gitlab.inria.fr/tnfs-alpha/alpha`

Preprint available very soon

Thank you for your attention.

Bibliography I

S. Bai.
Polynomial Selection for the Number Field Sieve.
Phd thesis, Australian National University, Australia, September 2011.
http://maths.anu.edu.au/~brent/pd/Bai-thesis.pdf.

S. Bai, R. P. Brent, and E. Thomé.
Root optimization of polynomials in the number field sieve.
Math. Comp., 84(295):2447–2457, 2015.
https://hal.inria.fr/hal-00919367,
https://doi.org/10.1090/S0025-5718-2015-02926-3.

R. Barbulescu and S. Duquesne.
Updating key size estimations for pairings.
Journal of Cryptology, Jan 2018.
https://hal.archives-ouvertes.fr/hal-01534101v2.

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.

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.

G. Fotiadis and C. Martindale.
Optimal TNFS-secure pairings on elliptic curves with composite embedding degree.
Cryptology ePrint Archive, Report 2019/555, 2019.
https://eprint.iacr.org/2019/555.

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

Bibliography III

A. Guillevic, S. Masson, and E. Thomé.
Cocks-pinch curves of embedding degrees five to eight and optimal ate pairing computation.
Cryptology ePrint Archive, Report 2019/431, 2019.
https://eprint.iacr.org/2019/431.

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.

A. Joux and C. Pierrot.
The special number field sieve in $\mathbb{F}_{p^n}$ - application to pairing-friendly constructions.
In Z. Cao and F. Zhang, editors, *PAIRING 2013*, volume 8365 of *LNCS*, pages 45–61. Springer, Heidelberg, Nov. 2014.

Bibliography IV

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.

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.

A. K. Lenstra and E. R. Verheul.
Selecting cryptographic key sizes.
Journal of Cryptology, 14(4):255–293, Sept. 2001.

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.
https://bookstore.ams.org/psapm-42/,
http://www.mccurley.org/papers/dlog.pdf.

Bibliography V

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.
http://eprint.iacr.org/2016/1102.

B. A. Murphy.
Polynomial selection for the number field sieve integer factorisation algorithm.
Phd thesis, Australian National University, Australia, 1999.
http://maths-people.anu.edu.au/~brent/pd/Murphy-thesis.pdf.

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.