Pairing-friendly elliptic curves, design, implementation, and discrete logarithm computations

Diego F. Aranha, Youssef El Housni, Georgios Fotiadis, *Aurore Guillevic*

Aarhus University, Denmark `dfaranha@cs.au.dk`

Consensys, NYC, USA `youssef.elhousni@consensys.net`

Université du Luxembourg, Luxembourg `georgios.fotiadis@uni.lu`

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France `aurore.guillevic@inria.fr`

CAPSULE seminar, Rennes, November 30, 2023

`https://members.loria.fr/AGuillevic/files/talks/23_Rennes.pdf`

Bilinear pairing in cryptography

As a black-box:
$(\mathbb{G}_1, +), (\mathbb{G}_2, +), (\mathbb{G}_T, \cdot)$ three cyclic groups of large prime order r

Bilinear pairing: map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

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 $\langle G_1 \rangle = \mathbb{G}_1$, $\langle G_2 \rangle = \mathbb{G}_2$
3. efficiently computable

Mostly used in practice:

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

Examples of applications

- 1984: idea of identity-based encryption (IBE) 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

...

- Broadcast encryption, re-keying
- aggregate signatures
- zero-knowledge (ZK) proofs
  - non-interactive ZK proofs (NIZK)
  - zk-SNARK (Z-cash, Zexe...)
- tool in isogeny-based post-quantum cryptography, different setting (not in this talk)

Bilinear pairings

Security relies on

- Discrete Log Problem (DLP):

$$\text{given } g, h \in \mathbb{G}, \text{ compute } x \text{ s.t. } g^x = h$$

- Diffie-Hellman Problem (DHP):

$$\text{given } g, g^a, g^b \in \mathbb{G}, \text{ compute } g^{ab}$$

- bilinear DLP and DHP
- pairing inversion problem

Open the black-box: torsion points

Curve25519 : $y^2 = x^3 + \underbrace{486662}_{A} x^2 + x$ over GF(p), $p = 2^{255} - 19$

order $\#E(\mathbb{F}_p) = 8r$, 253-bit prime r

2-torsion points $= \{P \in E,\ 2P = \mathcal{O} \iff y_P = 0\}$

- 2-torsion over $\mathbb{F}_p$: $\{\mathcal{O}, (0,0)\}$
- full 2-torsion over $\mathbb{F}_{p^2}$: $\{\mathcal{O}, (0,0), (\lambda, 0), (\mu, 0)\}$, $x^2 + Ax + 1 = (x - \lambda)(x - \mu)$

Open the black-box: torsion points

Curve25519 : $y^2 = x^3 + \underbrace{486662}_{A} x^2 + x$ over GF(p), $p = 2^{255} - 19$

order $\#E(\mathbb{F}_p) = 8r$, 253-bit prime r

2-torsion points $= \{P \in E,\ 2P = \mathcal{O} \iff y_P = 0\}$

- 2-torsion over $\mathbb{F}_p$: $\{\mathcal{O}, (0,0)\}$
- full 2-torsion over $\mathbb{F}_{p^2}$: $\{\mathcal{O}, (0,0), (\lambda, 0), (\mu, 0)\}$, $x^2 + Ax + 1 = (x - \lambda)(x - \mu)$

For an integer ℓ, the ℓ-torsion $E[\ell]$ has order ℓ^2

- $\#E[2] = 4 \subset E(\mathbb{F}_{p^2})$
- $\#E[4] = 16 \subset E(\mathbb{F}_{p^2})$
- $\#E[8] = 64 \subset E(\mathbb{F}_{p^2})$
- $\#E[r] = r^2 \subset E(\mathbb{F}_{p^k})$, $k = (r-1)/6$ of 250 bits for Curve25519

Pairing-friendly curves should be designed on purpose

In cryptographic setting: $E[r]$ has structure $\mathbb{Z}_r \times \mathbb{Z}_r$ denoted $\mathbb{G}_1 \times \mathbb{G}_2$

128-, resp. 192-bit security level:

- r large prime ~ 256, resp. 384 bits
- $\#E(\mathbb{F}_p) = h \cdot r$, h small **cofactor**, $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$
- $E[r] \subset E(\mathbb{F}_{p^k})$ and $1 \leq k \leq 54$, $\mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$
  k embedding degree
- $\mathbb{G}_T \subset \mathbb{F}_{p^k}^*$ multiplicative subgroup of order r

Usually $\log k \sim \log r$ (Balasubramanian Koblitz [BK98]).

Plain curves (25519, NIST curves) are never pairing-friendly

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

$$e\colon E(\mathbb{F}_p)[r] \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T \subset \mathbb{F}_{p^k}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

$$e\colon E(\mathbb{F}_p)[r] \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T \subset \mathbb{F}_{p^k}^*, \quad e([a]P,[b]Q) = e(P,Q)^{ab}$$

Attacks

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

$$e\colon E(\mathbb{F}_p)[r] \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T \subset \mathbb{F}_{p^k}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

$$\uparrow$$

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

$$e\colon E(\mathbb{F}_p)[r] \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T \subset \mathbb{F}_{p^k}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

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

$$e\colon E(\mathbb{F}_p)[r] \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T \subset \mathbb{F}_{p^k}^*, \quad e([a]P,[b]Q) = e(P,Q)^{ab}$$

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 $\mathbb{F}_{p^k}^*$: **easier, subexponential** $\to$ take a large enough field

Pairing-friendly curves are special

1st ones were *supersingular*, not in this talk.

Ordinary curves:

- 2001: Miyaji–Nakabayashi–Takano curves, $k \in \{3, 4, 6\}$, prime order [MNT01]
- Cocks-Pinch technique
- Barreto–Lynn–Scott curves, $3 \mid k$, $18 \nmid k$ [BLS03]
- Brezing–Weng construction [BW05]
- Freeman $k = 10$ [Fre06], Barreto–Naehrig curves $k = 12$, prime order [BN06]
- Kachisa–Schaefer–Scott curves, $k \in \{8, 16, 18, 32, 36, 40\}$ [KSS08]
- Freeman–Scott–Teske Taxonomy [FST10]
- Scott–G, $k = 54$ [SG18]
- Gasnier–G, $k = 20, 22$ [GG23]

Why Barreto–Naehrig'2005 curves were so popular?

$k = 12,\ j = 0,\ D = -3,$

$$E\colon y^2 = x^3 + b$$

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$
$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

Why Barreto–Naehrig'2005 curves were so popular?

$k = 12,\ j = 0,\ D = -3,$

$$E\colon y^2 = x^3 + b$$

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$
$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

$$\left.\begin{array}{l} x_0 = 2^{62} - 2^{54} + 2^{44} \text{ [NAS}^+\text{08] (Nogami et al.)} \\ x_0 = -(2^{62} + 2^{55} + 1) \text{ [PSNB11] (Pereira et al.)} \\ x_0 = \texttt{0x44e992b44a6909f1} \text{ in Ethereum, s.t. } 2^{28} \mid r - 1 \end{array}\right\} \begin{array}{l} \#E(\mathbb{F}_p) = r \text{ prime order} \\ r \text{ of 254 bits} \end{array}$$

Why Barreto–Naehrig'2005 curves were so popular?

$k = 12,\ j = 0,\ D = -3,$

$$E\colon y^2 = x^3 + b$$

$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$
$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$

$$\left.\begin{array}{l} x_0 = 2^{62} - 2^{54} + 2^{44} \text{ [NAS}^+\text{08] (Nogami et al.)} \\ x_0 = -(2^{62} + 2^{55} + 1) \text{ [PSNB11] (Pereira et al.)} \\ x_0 = \texttt{0x44e992b44a6909f1} \text{ in Ethereum, s.t. } 2^{28} \mid r - 1 \end{array}\right\} \begin{array}{l} \#E(\mathbb{F}_p) = r \text{ prime order} \\ r \text{ of 254 bits} \end{array}$$

$\mathbb{G}_T \subset \mathbb{F}_{p^{12}}$ of $12 \log p \approx 3048$ bits
≈ 3072 bits expected to offer 128 bits of security for RSA and Discrete Log in the 2000's

$\Longrightarrow$ BN curves were the perfect match

Choosing pairing-friendly curves

Pairing-based cryptography needs **secure, efficient, compact** pairing-friendly curves

- secure against discrete log in $E(\mathbb{F}_p)$, $E(\mathbb{F}_{p^k})$, $\mathbb{F}_{p^k}$
- efficient for scalar multiplication in E, exponentiation in $\mathbb{F}_{p^k}$, pairing
- compact: key sizes as small as possible

Which curves are the best options?

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

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

- Special NFS in $\mathbb{F}_{p^k}$: Joux–Pierrot 2013 [JP14]
- Tower NFS (TNFS): Barbulescu–Gaudry–Kleinjung 2015 [BGK15]
- Extended Tower NFS: Kim–Barbulescu [KB16], Kim–Jeong [KJ17], Sarkar–Singh 2016 [SS16]

Use more structure: subfields

Choosing key sizes: Lenstra–Verheul [LV01] extrapolation

Initially for RSA modulus size

For DL in $\mathbb{F}_Q$ of length(Q) bits
n bits of security $\leftrightarrow$ the best (mathematical) attack should take at least 2^n steps

Choosing key sizes: Lenstra–Verheul [LV01] extrapolation

Initially for RSA modulus size

For DL in $\mathbb{F}_Q$ of length(Q) bits
n bits of security $\leftrightarrow$ the best (mathematical) attack should take at least 2^n steps

- fastest Discrete Log computation: with the Number Field Sieve algorithm
- Complexity: $e^{\sqrt[3]{(64/9+o(1))(\ln Q)(\ln\ln Q)^2}}$
- $+o(1)$ not known (or diverges [LG21])

Choosing key sizes: Lenstra–Verheul [LV01] extrapolation

Initially for RSA modulus size

For DL in $\mathbb{F}_Q$ of length(Q) bits
n bits of security $\leftrightarrow$ the best (mathematical) attack should take at least 2^n steps

- fastest Discrete Log computation: with the Number Field Sieve algorithm
- Complexity: $e^{\sqrt[3]{(64/9+o(1))(\ln Q)(\ln\ln Q)^2}}$
- $+o(1)$ not known (or diverges [LG21])
- $Q_{\text{DL-240}} = \text{NextSafePrime}(N_{240}) = N_{240} + 49204$

$$e^{\sqrt[3]{(64/9+0)(\ln Q_{\text{DL-240}})(\ln\ln Q_{\text{DL-240}})^2}} = 2^{77.68}$$

Choosing key sizes: Lenstra–Verheul [LV01] extrapolation

Initially for RSA modulus size

For DL in $\mathbb{F}_Q$ of length(Q) bits
n bits of security $\leftrightarrow$ the best (mathematical) attack should take at least 2^n steps

- fastest Discrete Log computation: with the Number Field Sieve algorithm
- Complexity: $e^{\sqrt[3]{(64/9+o(1))(\ln Q)(\ln\ln Q)^2}}$
- $+o(1)$ not known (or diverges [LG21])
- $Q_{\text{DL-240}} = \text{NextSafePrime}(N_{240}) = N_{240} + 49204$

$$e^{\sqrt[3]{(64/9+0)(\ln Q_{\text{DL-240}})(\ln\ln Q_{\text{DL-240}})^2}} = 2^{77.68}$$

- DL-240 in $2^{67.51}$ operations [BGG$^+$20] $\to 2^{67.51}/2^{77.68} = 2^{-10.17}$

Choosing key sizes: Lenstra–Verheul [LV01] extrapolation

Initially for RSA modulus size

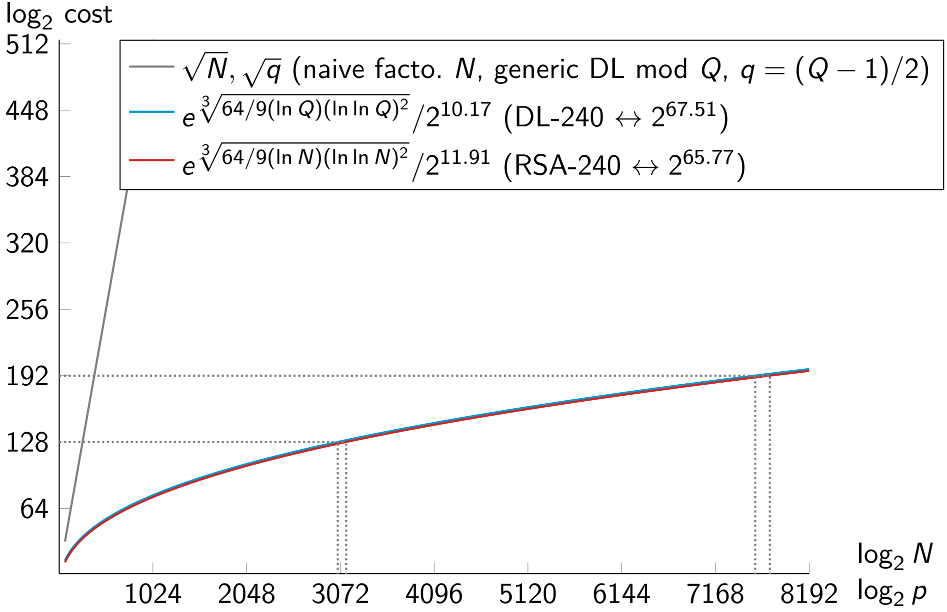
For DL in $\mathbb{F}_Q$ of length(Q) bits
n bits of security $\leftrightarrow$ the best (mathematical) attack should take at least 2^n steps

- fastest Discrete Log computation: with the Number Field Sieve algorithm
- Complexity: $e^{\sqrt[3]{(64/9+o(1))(\ln Q)(\ln \ln Q)^2}}$
- $+o(1)$ not known (or diverges [LG21])
- $Q_{\text{DL-240}} = \text{NextSafePrime}(N_{240}) = N_{240} + 49204$

$$e^{\sqrt[3]{(64/9+0)(\ln Q_{\text{DL-240}})(\ln \ln Q_{\text{DL-240}})^2}} = 2^{77.68}$$

- DL-240 in $2^{67.51}$ operations [BGG+20] $\rightarrow 2^{67.51}/2^{77.68} = 2^{-10.17}$

DL in prime field: Replace unknown $+o(1)$ by scaling factor $2^{-10.17}$



RSA-240: 953 core-years, Intel Xeon Gold 6130 CPUs as a reference (2.1GHz) $\approx 953 \cdot 365.25 \cdot 24 \cdot 60 \cdot 60 \cdot 2.1 \cdot 10^9 \approx 2^{65.77}$

DL-240: 3177 core-years, Intel Xeon Gold 6130 CPUs as a reference (2.1GHz) $\approx 3177 \cdot 365.25 \cdot 24 \cdot 60 \cdot 60 \cdot 2.1 \cdot 10^9 \approx 2^{67.51}$

https://members.loria.fr/AGuillevic/files/Enseignements/UBS/slides.pdf

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

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

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

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

Discrete logarithm in GF(p^6) with Tower-NFS [DGP21]

- $Q = p^6$ of 521 bits, total time 24798 core-hours (2.83 core-years) $\leftrightarrow 2^{57.37}$
- Tower-NFS-Conjugation $e^{\sqrt[3]{(48/9+o(1))(\ln Q)(\ln\ln Q)^2}}$
- $e^{\sqrt[3]{(48/9+0)(\ln Q_{\text{DL-521}})(\ln\ln Q_{\text{DL-521}})^2}} = 2^{58.52}$

DL in non-special $\mathbb{F}_{p^6}$ field: too early to apply Lenstra–Verheul extrapolation

Largest record computations in $\mathbb{F}_{p^k}$ with NFS and its variants[1]

Finite field	Size of p^k	Cost: CPU days	Authors	sieving dim
		Tower-NFS		
$\mathbb{F}_{p^6}$	521	1,033	[DGP21] De Micheli et al.'21	6, Tower
$\mathbb{F}_{p^4}$	512	2244	[Rob22] Robinson'22	4, Tower
		NFS and NFS-HD		
$\mathbb{F}_{p^{12}}$	203	11	[HAKT13, HAKT15]	7
$\mathbb{F}_{p^6}$	423	3,400	[MR20]	3
$\mathbb{F}_{p^5}$	324	386	[GGM17]	3
$\mathbb{F}_{p^4}$	392	510	[BGGM15a]	2
$\mathbb{F}_{p^3}$	593	8,400	[GGM16, GMT16]	2
$\mathbb{F}_{p^2}$	595	175	[BGGM15b]	2
$\mathbb{F}_p$	768	1,935,825	[KDLPS17]	2
$\mathbb{F}_p$	795	1,132,275	[BGGHTZ19]	2

[1] Data extracted from DiscreteLogDB by L.Grémy

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

Simulation tool at `https://gitlab.inria.fr/tnfs-alpha/alpha` from [GS21]

- SageMath
- MIT License

Can select polynomials for (S)TNFS and estimates the running-time
Estimated cost of De Micheli et al. record: 2^{50} (real time: $2^{57.37}$)

We used that tool to estimate the security level in $GF(p^k)$ for many curves

Special Tower NFS

Find two number fields that can be mapped to $\mathbb{F}_{p^k}$ with reduction modulo p
Sharing a subfield $\mathbb{F}_{p^\kappa}$, $1 < \kappa \mid k$

$K_f = K_h[x]/(f_\tau(x))$ $\qquad$ $K_g = K_h[x]/(g_\tau(x))$

$\eta = k/\kappa \leq \deg f$ $\qquad$ $\deg g \geq \eta = k/\kappa$

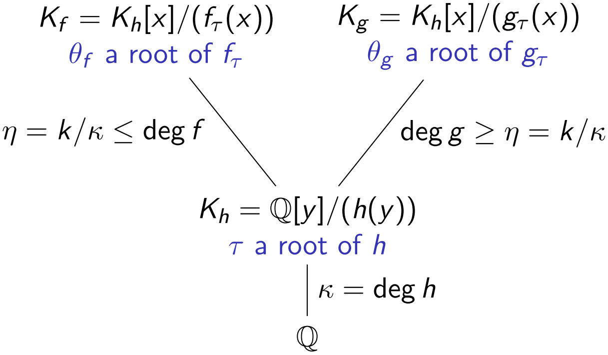
$K_h = \mathbb{Q}[y]/(h(y))$

$\kappa = \deg h$

$\mathbb{Q}$

Special Tower NFS

Find two number fields that can be mapped to $\mathbb{F}_{p^k}$ with reduction modulo p
Sharing a subfield $\mathbb{F}_{p^\kappa}$, $1 < \kappa \mid k$



Special Tower NFS

Find two number fields that can be mapped to $\mathbb{F}_{p^k}$ with reduction modulo p
Sharing a subfield $\mathbb{F}_{p^\kappa}$, $1 < \kappa \mid k$

$K_f = K_h[x]/(f_\tau(x))$ — θ_f a root of f_τ

$K_g = K_h[x]/(g_\tau(x))$ — θ_g a root of g_τ

$\eta = k/\kappa \leq \deg f$

$\deg g \geq \eta = k/\kappa$

$K_h = \mathbb{Q}[y]/(h(y))$ — τ a root of h

$\kappa = \deg h$

$\mathbb{Q}$

- f_τ, g_τ share a common gcd polynomial $\phi_\tau(x)$ irreducible of degree $\eta = k/\kappa$
- θ_f, θ_g map to the same θ_p in $\mathbb{F}_{p^k}$
- h is irreducible modulo p

Special Tower NFS

1. Polynomial selection: choose 3 polynomials h, f, g
2. Relation collection: obtain many smooth norms of
   $\boldsymbol{a} + \boldsymbol{b}\theta_f = (a_0 + a_1\tau + \ldots + a_i\tau^i) + (b_0 + b_1\tau + \ldots + b_i\tau^i)\theta_f$, $\boldsymbol{a} + \boldsymbol{b}\theta_g$
3. Filtering step of the matrix (apply Galois automorphisms if any)
4. Linear algebra
5. Individual discrete logarithm

Are the norms as smooth as integers of the same size?
Bias $\rightarrow \alpha(f), \alpha(g)$
TNFS: $\alpha(h, f), \alpha(h, g)$

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 [BD19]

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
$\rightarrow \alpha(f) < 0$ wanted
$\alpha(f)$ computes the exact number of roots of $f(x)$ mod q^k
for all primes $q < 2000$ (say)
Easy prime $q \nmid \mathrm{disc}(f)$, tricky prime $q \mid \mathrm{disc}(f)$

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 $q \rightarrow$ prime ideal of norm q

Example : Barreto-Naehrig curve, p 254 bits

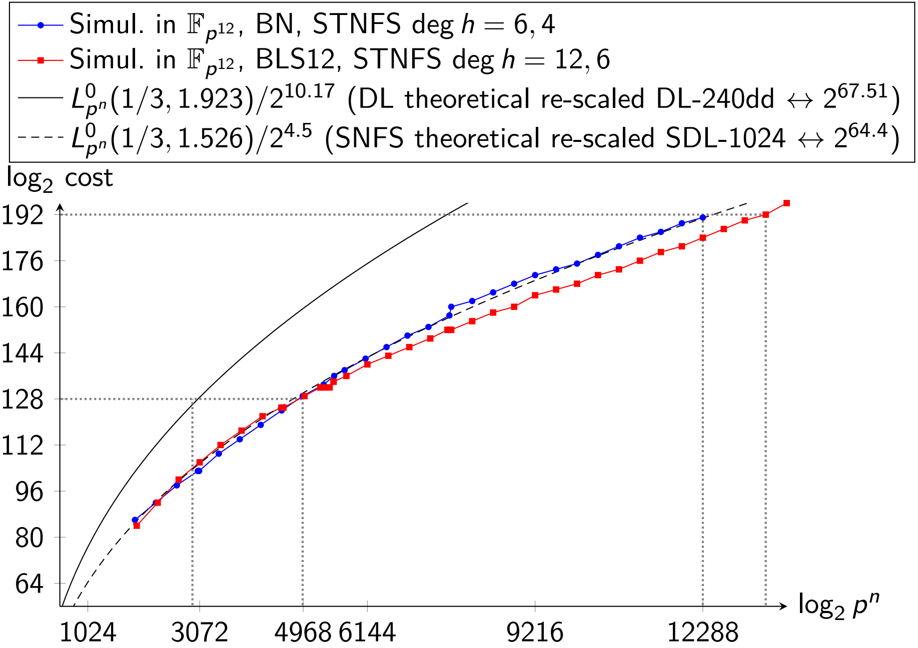
$p = 36s^4 + 36s^3 + 24s^2 + 6s + 1$ where $s = -(2^{62} + 2^{55} + 1)$

$f = 36x^8 + 36yx^6 + 24y^2x^4 + 6y^3x^2 + y^4$

$g = x^2 + sy = x^2 + 4647714815446351873y$

$B = 2000$

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 $h = 6, 4$
Simul. in $\mathbb{F}_{p^{12}}$, BLS12, STNFS deg $h = 12, 6$
$L^0_{p^n}(1/3, 1.923)/2^{10.17}$ (DL theoretical re-scaled DL-240dd $\leftrightarrow 2^{67.51}$)
$L^0_{p^n}(1/3, 1.526)/2^{4.5}$ (SNFS theoretical re-scaled SDL-1024 $\leftrightarrow 2^{64.4}$)
$\log_2$ cost
192
176
160
144
128
112
96
80
64
$\log_2 p^n$
1024
3072
4968
6144
9216
12288

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` [GMT20]
`https://gitlab.inria.fr/smasson/cocks-pinch-variant`
$p = p(s)$ of 446 bits, twist-secure curve
p^k 5352 bits
$h = Y^6 - Y^4 + Y^3 - Y + 1$

$f_y = X^{12} - 2yX^{10} + 2y^3X^6 + y^5X^2 + y^4 - y^3 + y - 1$
$g_y = X^2 - uy = X^2 + 283435675103427088875 53y$
$A = 968,\ B = 2^{68.2}$

Estimated cost: $\approx 2^{132}$

Differences

- Barbulescu–Duquesne [BD19] (curve name, prime field GF(p) bitzise):
  - BN-462 (p^{12}: 5544 bits), BLS12-461 (p^{12}: 5532 bits) for the 128-bit security level
  - BLS24-559 (p^{24} 13416 bits) for the 192-bit security level
- Guillevic–Singh [GS21]:
  - BN-446, BLS12-446 (p^{12} 5352 bits), 64-bit machine-word aligned
  - BLS24-509 (p^{12} 12216 bits)

Differences

- Barbulescu–Duquesne [BD19] (curve name, prime field GF(p) bitzise):
  - BN-462 (p^{12}: 5544 bits), BLS12-461 (p^{12}: 5532 bits) for the 128-bit security level
  - BLS24-559 (p^{24} 13416 bits) for the 192-bit security level
- Guillevic–Singh [GS21]:
  - BN-446, BLS12-446 (p^{12} 5352 bits), 64-bit machine-word aligned
  - BLS24-509 (p^{12} 12216 bits)
- shorter p bitsize, one 64-bit machine-word less $\rightarrow$ faster $\mathbb{F}_p$-multiplication, ratio of $(2s^2 + s)/(2s_0^2 + s_0)$, $s = \lceil p/64 \rceil$ [AFK$^+$13, Sect. 8]
  462-bit $\rightarrow$ 446-bit: $\mathbf{m}_{446} = 0.77\mathbf{m}_{462}$
  559-bit $\rightarrow$ 509-bit: $\mathbf{m}_{509} = 0.8\mathbf{m}_{559}$
- faster pairing, faster group operations, shorter keysizes

Differences

Keysize recommendation difference:
[BD19] assumes there exists *optimal* polynomial h
and the attacker knows how to select it

BLS24
There exists $h(y)$ of degree 24 such that

- $\|h\|_\infty = 1$ i.e. $h_i \in \{0, 1, -1\}$
- h irreducible mod p of a BLS24 curve
- h has cyclic Galois group of order 24

Open problem: *Does it exist? How to find such $h(y)$?*
Ideas are welcome

Ongoing work

Active branches

automorphisms

fab46aea · taking into account special automorphisms for cyclotomic polynomials h. Tested... · 3 weeks ago

master default protected

378f61dd · comment on BLS24 seeds · 1 month ago

Ongoing work

Finding curve seeds of low Hamming weight

```
sage -python -m tnfs.gen.generate_sparse_curve --bls \
    -k 24 -r 254 256 --2NAF --find_all_w_up_to -w 4
cat \
test_vector_sparse_bls24_rnbits_254_256_u_1_4_mod_6_unbits_33_Hw2naf_6.py
test_vector_sparse_bls24 = [
    {'u':-0xeffff000, ... 'label':"-2^32+2^28+2^12 Hw2naf 3"},
```

With high 2-valuation of $p-1$ and $r-1$ for Youssef El Housni

```
sage -python -m tnfs.gen.compute_test_vector_curve --bls \
    -k 24 -r 254 256 --find_all_u --valuation 16
cat \
test_vector_bls24_rnbits_254_256_val2_16_r_prime_pos_u__u_1_4_mod_6.py
# BLS24 curves with seed u = [1, 4] mod 6 s.t. r has 254 to 256 bits
test_vector_BLS24 = [
  {'u':0xe19c0001, 'u_mod_4':1, 'b': 1, 'pnbits':317,'rnbits':255, \
```

Previous work: 128-bit security level

Webpage at
`https://members.loria.fr/AGuillevic/pairing-friendly-curves/`

k	curve	seed	$\log_2 Q$	$\log_2 r$	ρ	bit sec. $GF(p^k)$
		Curves with fast pairing				
12	BN-382	$-(2^{94}+2^{78}+2^{67}+2^{64}+2^{48}+1)$	382	382	1.0	123
12	BN-446	$2^{110}+2^{36}+1$	446	446	1.0	132
12	BLS12-381	$-(2^{63}+2^{62}+2^{60}+2^{57}+2^{48}+2^{16})$	381	254	1.5	126
12	BLS12	see gitlab	440–448	295–300	1.5	132
		Curves with smallest possible $\mathbb{G}_1$ [CDS20]				
13	`BW13-P310`	-0x8b0=-2224	310	267	1.167	140
19	`BW19-P286`	-0x91=-145	286	259	1.111	160
		Curves for SNARK $2^L \mid p-1,\ r-1$				
12	BLS12-377	$2^{63}+2^{58}+2^{56}+2^{51}+2^{47}+2^{46}+1$	377	252	1.5	126
24	BLS24-315	$-2^{32}+2^{30}+2^{22}-2^{20}+1$	315	253	1.25	160

Choosing curves: criteria

- $384 \leq \log_2 r$ for the 192-bit security level
- $12 \leq k$
- adjust $\rho = \log_2 p / \log_2 r$

Lessons learned from the 128-bit short list:

- Too many curve families
- High degree twist is important for fast pairing
- Best curve choice varies from use-cases

Our choices:

→ restrict to $j = 0$ and $3 \mid k$, $6 \mid k$
or $j = 1728$ and $4 \mid k$

→ ρ varies up to 2 (Fotiadis et al. [FK19])

Pre-selected curves

k	curve	seed	$\log p$	$\log r$	ρ	$\log p^k$	secu
16	KSS16	$2^{78} - 2^{76} - 2^{28} + 2^{14} + 2^{7} + 1$	766	605	1.25	12256	194
	FM23	$2^{48} - 2^{44} - 2^{38} + 2^{31}$	765	384	2	12240	196
	AFG16	$-(2^{48} - 2^{44} + 2^{37})$	765	384	2	12240	196
18	KSS18	$2^{80} + 2^{77} + 2^{76} - 2^{61} - 2^{53} - 2^{14}$	638	474	1.33	11484	193
	SG18	$-(2^{63} + 2^{54} + 2^{16})$	638	383	1.66	11484	187
	FM25	$-2^{64} + 2^{33} + 2^{30} + 2^{20} + 1$	768	384	2	13824	197
20	FST 6.4	$-2^{56} + 2^{44} + 1$	670	448	1.5	13400	193
	SG20	$-2^{47} - 2^{45} + 2^{15} + 2^{13}$	670	383	1.75	13400	203
	GG20b	$2^{49} + 2^{46} - 2^{41} + 2^{35} + 2^{30} - 1$	575	379	1.52	11500	196

small $\mathbb{G}_1$

k	curve	seed	$\log p$	$\log r$	ρ	$\log p^k$	secu
21	BLS21	$-2^{32} + 2^{25} + 2^{6} + 2$	511	384	1.33	10731	199
24	BLS24	$-2^{51} - 2^{28} + 2^{11} - 1$	509	409	1.25	12216	193
27	BLS27	$-2^{21} - 2^{19} - 2^{15} + 2^{10} + 2^{4} + 2^{2} + 1$	426	383	1.11	11529	218
28	FST 6.4	$2^{32} - 2^{25} + 2^{22} + 2^{15} + 1$	510	384	1.33	14280	209

Why varying $\rho = \log_2 p / \log_2 r$?

Pairing computation $e(P, Q)$: Miller loop + final exponentiation to $(p^k - 1)/r$

Miller loop: evaluate a function $f_{m,P}$ at point Q [Jou04, Ver10]
Contains a scalar multiplication

$$[m]P \text{ where } \log_2 m \approx \frac{\log_2 r}{\varphi(k)} = \frac{log_2 r}{\deg \Phi_k}$$

Φ_k the k-th cyclotomic polynomial
SageMath: `euler_phi(k)`
$\varphi(12) = 4$, $\varphi(16) = 8$, $\varphi(18) = 6$, $\varphi(20) = 8$, $\varphi(24) = 8$

At fixed k, reducing r gives a faster Miller loop

Pairing: Miller loop and final exponentiation

Algorithm 6.1: $\textsc{MillerFunction}(u, P, Q)$

Input: $E, \mathbb{F}_p, \mathbb{F}_{p^k}$, k even, $P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})[r]$ in affine coord.,
$\pi_p(Q) = [p]Q$, $c \in \mathbb{N}$.

Result: $f = f_{c,Q}(P)$

$f \leftarrow 1$; $R \leftarrow Q$;
for *b from the second most significant bit of c to the least* **do**
  $\ell_0 \leftarrow \ell_{R,R}(P)$; $R \leftarrow [2]R$; // Dbl step, tangent line
  $f \leftarrow f^2$; // $\mathbf{s}_k$
  if $b = 1$ **then**
    $\ell_1 \leftarrow \ell_{R,Q}(P)$; $R \leftarrow R + Q$; // Add step, chord line
    $f \leftarrow f \cdot (\ell_0 \cdot \ell_1)$; // $\mathbf{m}_k +$ sparse-sparse-$\mathbf{m}_k$
  else
    $f \leftarrow f \cdot \ell_0$; // full-sparse-$\mathbf{m}_k$
return f;

Pairing: Miller loop and final exponentiation

Raise to

$$\frac{p^k - 1}{r} = \underbrace{\frac{q^k - 1}{\Phi_k(q)}}_{\text{easy}} \underbrace{\frac{\phi_k(q)}{r}}_{\text{hard}}$$

1st comparison: timing estimates in $\mathbb{F}_p$-multiplications

Estimate the number of multiplications **m** in $\mathbb{F}_p$ needed for

- $\mathbf{m}_k$ multiplication in $\mathbb{F}_{p^k}$
- $\mathbf{s}_k$ squaring in $\mathbb{F}_{p^k}$
- $\mathbf{f}_k$ Frobenius power $x \mapsto x^p$ in $\mathbb{F}_{p^k}$
- $\mathbf{i}_k$ inversion in $\mathbb{F}_{p^k}$
- $\mathbf{s}_k^{\text{cyclo}}$ squaring in the cyclotomic subgroup of $\mathbb{F}_{p^k}^*$ of order $\Phi_k(q)$ (subgroup of norm 1, inversion is free)

Relative cost: multiplication $\mathbf{m}_k$ squaring $\mathbf{s}_k$ Frobenius $\mathbf{f}_k$ inversion $\mathbf{i}_k$ $\mathbb{F}_{p^k}$

k	$\mathbf{m}_k$	$\mathbf{s}_k$	$\mathbf{f}_k$	$\mathbf{s}_k^{\text{cyclo}}$	$\mathbf{i}_k - \mathbf{i}_1$	$\mathbf{i}_k,\ \mathbf{i}_1 = 25\mathbf{m},\ \mathbf{s} = \mathbf{m}$
1	$\mathbf{m}$	$\mathbf{s}$	0		0	$25\mathbf{m}$
2	$3\mathbf{m}$	$2\mathbf{m}$	0	$2\mathbf{s}$	$2\mathbf{m} + 2\mathbf{s}$	$29\mathbf{m}$
3	$6\mathbf{m}$	$2\mathbf{m} + 3\mathbf{s}$ [CH07]	$2\mathbf{m}$		$9\mathbf{m} + 3\mathbf{s}$	$37\mathbf{m}$
4	$9\mathbf{m}$	$2\mathbf{m}_2 = 6\mathbf{m}$	$2\mathbf{m}$	$2\mathbf{s}_2 = 4\mathbf{m}$	$12\mathbf{m} + 2\mathbf{s}$	$39\mathbf{m}$
5	$13\mathbf{m}$	$13\mathbf{s}$ [Mon05]	$4\mathbf{m}$		$48\mathbf{m}$	$73\mathbf{m}$
6	$18\mathbf{m}$	$2\mathbf{m}_2 + 3\mathbf{s}_2 = 12\mathbf{m}$	$4\mathbf{m}$	$6\mathbf{m}$ [GS10]	$34\mathbf{m}$	$59\mathbf{m}$
7	$22\mathbf{m}$	$22\mathbf{s}$	$6\mathbf{m}$		$104\mathbf{m}$	$129\mathbf{m}$
12	$54\mathbf{m}$	$2\mathbf{m}_6 = 36\mathbf{m}$	$10\mathbf{m}$	$6\mathbf{m}_2 = 18\mathbf{m}$	$97\mathbf{m}$	$119\mathbf{m}$
16	$81\mathbf{m}$	$2\mathbf{m}_8 = 54\mathbf{m}$	$14\mathbf{m}$	$2\mathbf{s}_8 = 36\mathbf{m}$	$134\mathbf{m}$	$159\mathbf{m}$
18	$108\mathbf{m}$	$2\mathbf{m}_9 = 72\mathbf{m}$	$16\mathbf{m}$	$6\mathbf{m}_3 = 36\mathbf{m}$	$232\mathbf{m}$	$257\mathbf{m}$
20	$117\mathbf{m}$	$2\mathbf{m}_{10} = 78\mathbf{m}$	$18\mathbf{m}$	$2\mathbf{s}_{10} = 52\mathbf{m}$	$255\mathbf{m}$	$280\mathbf{m}$
21	$132\mathbf{m}$	$110\mathbf{m}$	$20\mathbf{m}$		$393\mathbf{m}$	$418\mathbf{m}$
24	$162\mathbf{m}$	$2\mathbf{m}_{12} = 108\mathbf{m}$	$22\mathbf{m}$	$6\mathbf{m}_4 = 54\mathbf{m}$	$318\mathbf{m}$	$343\mathbf{m}$
27	$216\mathbf{m}$	$153\mathbf{m}$	$26\mathbf{m}$		$511\mathbf{m}$	$536\mathbf{m}$
28	$198\mathbf{m}$	$132\mathbf{m}$	$26\mathbf{m}$	$88\mathbf{m}$	$437\mathbf{m}$	$462\mathbf{m}$

Estimated cost in $\mathbb{F}_p$-multiplications **m** but p varies

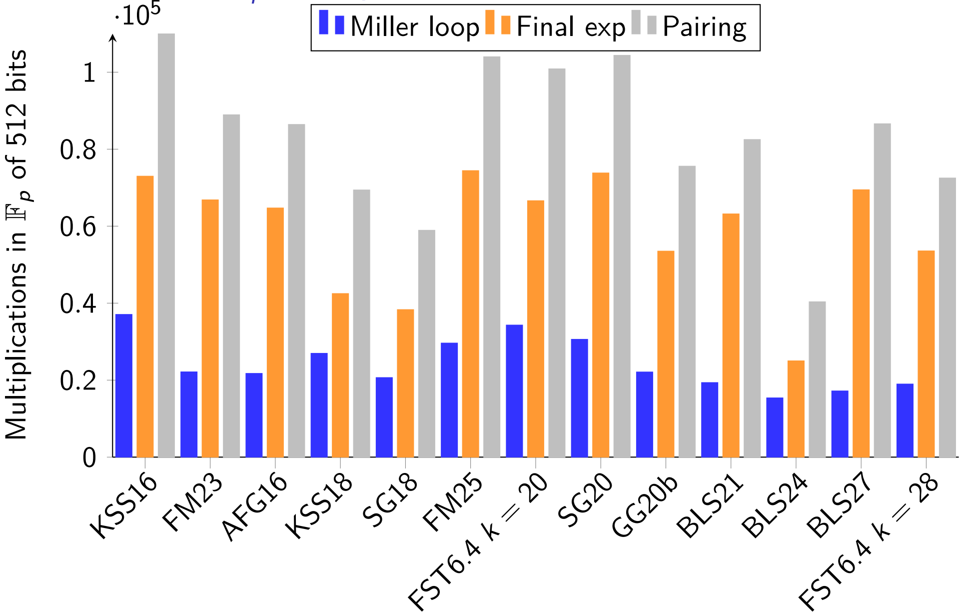
k	curve	p bits	r bits	Miller loop optimal ate	final exp easy	final exp hard	final exp total	pairing total
16	KSS16	766	605	16784**m**	240**m**	32826**m**	33066**m**	49850**m**
	FM23	765	384	10020**m**	255**m**	30024**m**	30279**m**	40299**m**
	AFG16	765	384	9838**m**	255**m**	29067**m**	29322**m**	39160**m**
18	KSS18	638	474	17433**m**	480**m**	27008**m**	27488**m**	44921**m**
	SG18	638	383	13351**m**	480**m**	24308**m**	24788**m**	38139**m**
	FM25	768	384	13410**m**	464**m**	33256**m**	33720**m**	47130**m**
20	FST 6.4	670	448	18416**m**	507**m**	35276**m**	35783**m**	54199**m**
	SG20	670	383	16427**m**	507**m**	39152**m**	39659**m**	56086**m**
	GG20b	575	379	17554**m**	507**m**	42017**m**	42524**m**	60078**m**
21	BLS21	511	384	19321**m**	717**m**	62426**m**	63143**m**	82464**m**
24	BLS24	509	409	15345**m**	658**m**	24310**m**	24968**m**	40313**m**
27	BLS27	426	383	22212**m**	1185**m**	88438**m**	89907**m**	112119**m**
28	FST 6.4	510	384	18940**m**	859**m**	52670**m**	53529**m**	72469**m**

Estimated cost in $\mathbb{F}_p$-multiplications $\mathbf{m}_{512}$, normalized

Rule of thumb Aranha et al. [AFK+13, Sect. 8]

- $\mathbb{F}_p$-elements represented with $\ell = 1 + \lfloor \log_2 p \rfloor$ bits
- packed in $w = \lceil \ell/64 \rceil$ 64-bit machine-words
- Montgomery representation
- $\rightarrow$ $\mathbf{m}$ with reduction in $\mathbb{F}_p$ has complexity $O(2w^2 + w)$
  - $m_{426} = 0.772 m_{512}$
  - $m_{576} = 1.257 m_{512}$
  - $m_{640} = 1.544 m_{512}$
  - $m_{704} = 1.860 m_{512}$
  - $m_{768} = 2.205 m_{512}$

Estimated cost in $\mathbb{F}_p$-multiplications $\mathbf{m}_{512}$, normalized



Other embedding degrees and quadratic twists are not promising

k	curve	p bits	r bits	Miller loop optimal ate	final exp easy	final exp hard	final exp total	pairing total
20	FST 6.4	670	448	18416**m**	507**m**	35276**m**	35783**m**	54199**m**
	SG20	670	383	16427**m**	507**m**	39152**m**	39659**m**	56086**m**
	GG20b	575	379	17554**m**	507**m**	42017**m**	42524**m**	60078**m**
	FST 6.6	527	384	28703**m**	507**m**	37621**m**	38128**m**	66831**m**
22	GG $D = 7$	457	383	41154**m**	789**m**	72352**m**	73141**m**	114295**m**
	FST 6.3	544	420	39707**m**	789**m**	65604**m**	66393**m**	106100**m**
24	BLS24	509	409	15345**m**	658**m**	24310**m**	24968**m**	40313**m**
27	BLS27	426	383	22212**m**	1185**m**	88438**m**	89907**m**	112119**m**

Benchmarks: Timings, clock cycles, RELIC toolkit

https://github.com/relic-toolkit/relic/

Intel Kaby Lake Core i7-7700 CPU machine with 64GB of RAM running single-threaded at 3.6GHz, with Turbo Boost and HT disabled to reduce measurement variability.

k	curve	p bits	r bits	Miller loop optimal ate	final exp	pairing total
16	KSS16	766	605	11855126	26977632	38832758
	AFG16	765	384	7343697	27093958	34443913
18	KSS18	638	474	9327153	15607334	24971803
	SG18	638	383	7135510	13628040	20763550
24	BLS24	509	409	5429826	9670702	15100528

Benchmarks: Timings, clock cycles, RELIC toolkit

https://github.com/relic-toolkit/relic/

Intel Kaby Lake Core i7-7700 CPU machine with 64GB of RAM running single-threaded at 3.6GHz, with Turbo Boost and HT disabled to reduce measurement variability.

Curve	BLS12-381 (ref 128)	KSS16-766	AFG16-765	KSS18-638	SG18-638	BLS24-509
Exp. in $\mathbb{G}_1$	394115	3392210	2210385	1718671	1414755	1066576
Exp. in $\mathbb{G}_2$	843175	18433905	12200469	7450643	6101680	5106474
Exp. in $\mathbb{G}_T$	1202601	13300120	9140193	11748224	9437487	7656674
Hash to $\mathbb{G}_1$	275816	1759828	4269969	1115238	1490162	498829
Hash to $\mathbb{G}_2$	962008	24355512	31849925	8894196	15130315	5804460
Test $P \in \mathbb{G}_1$	254753	3060100	1525930	1808786	1018560	797969
Test $Q \in \mathbb{G}_2$	311478	6880667	2909464	1927367	1663177	1068349
Test $z \in \mathbb{G}_T$	357063	5895541	2280958	2359975	9878582	1294991
Miller Loop	1396749	11855126	7343697	9327153	7135510	5429826
Final Exp	1740115	26977632	27093958	15607334	13628040	9670702
Pairing	3110112	38832758	34443913	24971803	20763550	15100528

Outcomes

- BLS12 is the best at the 128-bit security level
- BLS24 is the best at the 192-bit security level
- Fast Hashing to $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ matters too
- Preprint soon

Thank you.

`https://gitlab.inria.fr/tnfs-alpha/alpha`
`https://gitlab.inria.fr/zk-curves/snark-2-chains`

Bibliography I

Diego F. Aranha, Laura Fuentes-Castañeda, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez.
Implementing pairings at the 192-bit security level.
In Michel Abdalla and Tanja Lange, editors, *PAIRING 2012*, volume 7708 of *LNCS*, pages 177–195. Springer, Heidelberg, May 2013.

Diego F. Aranha, Elena Pagnin, and Francisco Rodríguez-Henríquez.
LOVE a pairing.
In Patrick Longa and Carla Ràfols, editors, *LATINCRYPT 2021*, volume 12912 of *LNCS*, pages 320–340. Springer, Heidelberg, October 2021.

Razvan Barbulescu and Sylvain Duquesne.
Updating key size estimations for pairings.
Journal of Cryptology, 32(4):1298–1336, October 2019.

Razvan Barbulescu, Nadia El Mrabet, and Loubna Ghammam.
A taxonomy of pairings, their security, their complexity.
Cryptology ePrint Archive, Report 2019/485, 2019.
https://eprint.iacr.org/2019/485.

Bibliography II

Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann.
Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment.
In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 62–91. Springer, Heidelberg, August 2020.

Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain.
DL record computation in $\mathrm{GF}(p^4)$ of 392 bits (120dd).
Announcement at the CATREL workshop, October 2nd 2015.
http://www.lix.polytechnique.fr/ guillevic/docs/guillevic-catrel15-talk.pdf.

Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain.
Improving NFS for the discrete logarithm problem in non-prime finite fields.
In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 129–155. Springer, Heidelberg, April 2015.

Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung.
The tower number field sieve.
In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 31–55. Springer, Heidelberg, November / December 2015.

Bibliography III

R. Balasubramanian and Neal Koblitz.
The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone algorithm.
Journal of Cryptology, 11(2):141–145, March 1998.

Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott.
Constructing elliptic curves with prescribed embedding degrees.
In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02*, volume 2576 of *LNCS*, pages 257–267. Springer, Heidelberg, September 2003.

Paulo S. L. M. Barreto and Michael Naehrig.
Pairing-friendly elliptic curves of prime order.
In Bart Preneel and Stafford Tavares, editors, *SAC 2005*, volume 3897 of *LNCS*, pages 319–331. Springer, Heidelberg, August 2006.

Friederike Brezing and Annegret Weng.
Elliptic curves suitable for pairing based cryptography.
Des. Codes Cryptography, 37(1):133–141, 2005.

Rémi Clarisse, Sylvain Duquesne, and Olivier Sanders.
Curves with fast computations in the first pairing group.
In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *CANS 20*, volume 12579 of *LNCS*, pages 280–298. Springer, Heidelberg, December 2020.

Bibliography IV

Jaewook Chung and M. Anwar Hasan.
Asymmetric squaring formulae.
In *18th IEEE Symposium on Computer Arithmetic (ARITH-18 2007), 25-27 June 2007, Montpellier, France*, pages 113–122. IEEE Computer Society, 2007.
https://www.lirmm.fr/arith18/papers/Chung-Squaring.pdf.

Sanjit Chatterjee, Alfred Menezes, and Francisco Rodríguez-Henríquez.
On instantiating pairing-based protocols with elliptic curves of embedding degree one.
IEEE Transactions on Computer, 66(6):1061–1070, 2017.

Régis Dupont, Andreas Enge, and François Morain.
Building curves with arbitrary small MOV degree over finite prime fields.
Journal of Cryptology, 18(2):79–89, April 2005.

Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot.
Lattice enumeration for tower NFS: A 521-bit discrete logarithm computation.
In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 67–96. Springer, Heidelberg, December 2021.

Georgios Fotiadis and Elisavet Konstantinou.
TNFS resistant families of pairing-friendly elliptic curves.
Theoretical Computer Science, 800:73–89, 31 December 2019.

Bibliography V

Georgios Fotiadis and Chloe 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.

David Freeman.
Constructing pairing-friendly elliptic curves with embedding degree 10.
In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *Algorithmic Number Theory, 7th International Symposium, ANTS-VII*, volume 4076 of *LNCS*, pages 452–465, Berlin, Germany, July 23-28 2006. Springer.
https://eprint.iacr.org/2006/026.

David Freeman, Michael Scott, and Edlyn Teske.
A taxonomy of pairing-friendly elliptic curves.
Journal of Cryptology, 23(2):224–280, April 2010.

Jean Gasnier and Aurore Guillevic.
An algebraic point of view on the generation of pairing-friendly curves.
preprint available at https://hal.science/hal-04205681, September 2023.

Bibliography VI

Pierrick Gaudry, Aurore Guillevic, and François 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.

Laurent Grémy, Aurore Guillevic, and François 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.

Aurore Guillevic, François Morain, and Emmanuel Thomé.
Solving discrete logarithms on a 170-bit MNT curve by pairing reduction.
In Roberto Avanzi and Howard M. Heys, editors, *SAC 2016*, volume 10532 of *LNCS*, pages 559–578. Springer, Heidelberg, August 2016.

Aurore Guillevic, Simon Masson, and Emmanuel Thomé.
Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation.
Des. Codes Cryptography, 88:1047–1081, March 2020.

Bibliography VII

Robert Granger and Michael Scott.
Faster squaring in the cyclotomic subgroup of sixth degree extensions.
In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 209–223. Springer, Heidelberg, May 2010.

Aurore Guillevic and Shashank Singh.
On the alpha value of polynomials in the tower number field sieve algorithm.
Mathematical Cryptology, 1(1):1–39, Feb. 2021.

Aurore Guillevic.
A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 535–564. Springer, Heidelberg, May 2020.

Kenichiro Hayasaka, Kazumaro Aoki, Tetsutaro Kobayashi, and Tsuyoshi Takagi.
An experiment of number field sieve for discrete logarithm problem over $\mathrm{GF}(p^{12})$.
In Marc Fischlin and Stefan Katzenbeisser, editors, *Number Theory and Cryptography, Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthdayx*, volume 8260 of *LNCS*, pages 108–120. Springer, 2013.

Bibliography VIII

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

Antoine Joux.
A one round protocol for tripartite Diffie-Hellman.
Journal of Cryptology, 17(4):263–276, September 2004.

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

Taechan Kim and Razvan Barbulescu.
Extended tower number field sieve: A new complexity for the medium prime case.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 543–571. Springer, Heidelberg, August 2016.

Taechan Kim and Jinhyuck Jeong.
Extended tower number field sieve with application to finite fields of arbitrary composite extension degree.
In Serge Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 388–408. Springer, Heidelberg, March 2017.

Bibliography IX

Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott.
Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field.
In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 126–135. Springer, Heidelberg, September 2008.

Aude Le Gluher.
Symbolic Computation and Complexity Analyses for Number Theory and Cryptography.
Phd thesis, Université de Lorraine, Nancy, France, December 2021.
https://hal.univ-lorraine.fr/tel-03564208.

Arjen K. Lenstra and Eric R. Verheul.
Selecting cryptographic key sizes.
Journal of Cryptology, 14(4):255–293, September 2001.

A. Miyaji, M. Nakabayashi, and S. Takano.
New explicit conditions of elliptic curve traces for FR-reduction.
IEICE Transactions on Fundamentals, E84-A(5):1234–1243, 2001.
https://dspace.jaist.ac.jp/dspace/bitstream/10119/4432/1/73-48.pdf.

P. L. Montgomery.
Five, six, and seven-term Karatsuba-like formulae.
IEEE Transactions on Computer, 54:362–369, March 2005.

Bibliography X

Gary McGuire and Oisin Robinson.
A new angle on lattice sieving for the number field sieve, 2020.
https://arxiv.org/abs/2001.10860.

Alfred Menezes, Palash Sarkar, and Shashank Singh.
Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography.
In Raphael C.-W. Phan and Moti Yung, editors, *Mycrypt Conference*, volume 10311 of *LNCS*, pages 83–108, Kuala Lumpur, Malaysia, December 1-2 2016. Springer.

Yasuyuki Nogami, Masataka Akane, Yumi Sakemi, Hidehiro Katou, and Yoshitaka Morikawa.
Integer variable chi-based Ate pairing.
In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 178–191. Springer, Heidelberg, September 2008.

Geovandro C.C.F. Pereira, Marcos A. Simplício, Michael Naehrig, and Paulo S.L.M. Barreto.
A family of implementation-friendly BN elliptic curves.
Journal of Systems and Software, 84(8):1319–1326, 2011.

Oisin Robinson.
An implementation of the extended tower number field sieve using 4d sieving in a box and a record computation in $\mathbb{F}_{p^4}$, 2022.
arXiv:2212.04999 https://arxiv.org/abs/2212.04999.

Bibliography XI

Michael Scott and Aurore Guillevic.
A new family of pairing-friendly elliptic curves.
In Lilya Budaghyan and Francisco Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields*, pages 43–57, Cham, 2018. Springer.

Palash Sarkar and Shashank Singh.
A general polynomial selection method and new asymptotic complexities for the tower number field sieve algorithm.
In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 37–62. Springer, Heidelberg, December 2016.

F. Vercauteren.
Optimal pairings.
IEEE Transactions on Information Theory, 56(1):455–461, Jan 2010.

Complexities $L_{p^k}(\alpha, c) = \exp\Big((c + o(1))(\ln p^k)^\alpha (\ln \ln p^k)^{1-\alpha}\Big)$

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

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