SIAM-AG23: 10 – 14 July 2023, Eindhoven, the Netherlands

3 Minisymposia for cryptographers:

- MS Applications of Algebraic Geometry to Post-Quantum Cryptology
- **MS53, 66, 80 Elliptic Curves and Pairings in Cryptography**
- MS92, 105, 118 Applications of Isogenies in Cryptography

Rank-one tensor completion (SIAGA 1, 2017)

`https://www.win.tue.nl/siam-ag23/index.html`
`https://meetings.siam.org/program.cfm?CONFCODE=AG23`

Practical info

Sessions labelled ECC on your A4-program at the back of your nametag

- Session 1: this session, Wednesday 10:30 – 12:30 Room Audi 1
  live stream at https://videocollege.tue.nl/Mediasite/Channel/siam-2023-event/watch/9f5674a21067410294 1f8614f5d2eba91d
- Session 2: this afternoon, Wednesday 14:00 – 16:00 Room Audi 1
  https://videocollege.tue.nl/Mediasite/Channel/siam-2023-event/watch/e7d29808e57f402a825b23107cf071bb1d
- Session 3: tomorrow, Thursday 10:30 – 12:30 Room Audi 1
  https://videocollege.tue.nl/Mediasite/Channel/siam-2023-event/watch/76dd943096194e8c8391bdac686cd8f91d

Elliptic Curves in Cryptography

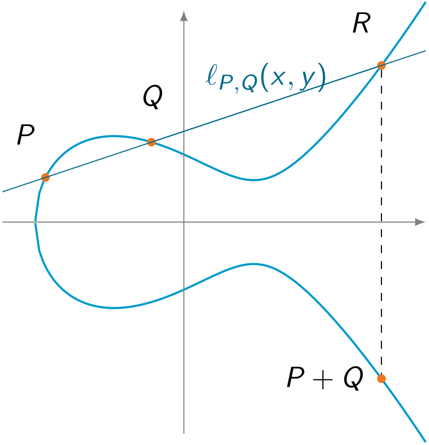
Elliptic curves introduced in 1985 by Miller, Koblitz
Perfect candidates to build a **generic group**
Many curves, usually over prime fields
of sparse binary expansion

- curve 25519 over $GF(2^{255} - 19)$
- NIST-P curves
- Four$\mathbb{Q}$ over $GF(p^2)$, $p = 2^{127} - 1$ Mersenne
- BLS12-381 for pairings ...

Basic crypto operations

Exponentation in a group $\mathbb{G}$ becomes
scalar multiplication

$$m, G \mapsto [m]G = \underbrace{G + G + \ldots + G}_{m \text{ times}}$$



Elliptic curve in Montgomery form and 2-torsion

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

Elliptic curve in Montgomery form and 2-torsion

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

Group operations on curves for crypto

Subgoup membership testing

For curves E over $\mathbb{F}_p$ with a **cofactor** $\#E(\mathbb{F}_p) = h \cdot r$

- Pairings as a new tool by **Dimitri Koshelev** next talk
- Large cofactors for pairings, **Dai Yu**'s talk Session 2

Hashing to a point on the curve

Elligator for curves with $h = 2, 4$,
Wahby–Boneh on the BLS-381 curve and all j-invariant 0 and $p = 1 \bmod 3$ with a $\mathbb{F}_p$-rational small-degree isogeny

- new results by **Jorge Chavez-Saab** just after
- new results by **Dimitri Koshelev** (not in this MS)

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
- attribute-based encryption
  This afternoon, M. Venema, pairing-based ABE
- zero-knowledge (ZK) proofs, non-interactive ZK proofs (NIZK)
  this afternoon, Y. El Housni, pairings in the context of zk-SNARKs
  tomorrow, M. Bellés Muñoz, the quest to finding curves for zk-SNARKs
- tool in isogeny-based post-quantum cryptography, different setting
  (in the other minisymposia, e.g. Giulio's talks MS14)

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

Pairing-friendly curves should be designed on purpose

In cryptographic setting: $E[r]$ has structure $\mathbb{Z}_r \times \mathbb{Z}_r$ denoted $\mathbb{G}_1 \times \mathbb{G}_2$
(remember the 2-torsion points on Curve25519)

128-, resp. 192-bit security level:

- r large prime $\sim$ 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

Finding pairing-friendly curves

Cocks–Pinch method:
Repeat

1. Start from the subgroup prime order r
2. Choose an embedding degree k and check $r \equiv 1 \bmod k$
3. Set $z \equiv \zeta_k \bmod r$
   (take z at random, repeat $z \mapsto z^{(r-1)/k}$ until $\Phi_k(z) = 1 \bmod r$, $z \neq 1$)
4. Set $t = z + 1$ and lift in $\mathbb{Z}$
5. Set $y = (t-2)/\sqrt{-D} \bmod r$ and lift in $\mathbb{Z}$
6. Set $p = (t^2 + Dy^2)/4$

until $p \in \mathbb{Z}$ and p is prime
Variant: lift $t + h_t \cdot r$, $y + h_y \cdot r$ with small h_t, h_y
Drawback: large cofactor $h \approx r$

Pairing-friendly curves are special

1st ones were *supersingular*, again used in post-quantum crypto.

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–Guillevic, $k = 54$ [SG18]
- Gasnier–Guillevic, $k = 20, 22$ (**J. Gasnier, tomorrow**)

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 D-Log in the 2000's

- optimal parameter size, optimal $k = 12$
- prime order: no cofactor clearing, no subgroup membership testing
- $\mathbb{F}_{p^{12}}$ towering easier to implement with Karatsuba

$\implies$ 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?

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

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

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

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

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
- $Q_{\text{DL-240}} = \text{NextSafePrime}(N_{240}) = N_{240} + 49204$

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

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
- $Q_{\text{DL-240}} = \text{NextSafePrime}(N_{240}) = N_{240} + 49204$

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

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

Choosing key sizes: Lenstra–Verheul [LV01] extrapolation

Initially for RSA modulus size

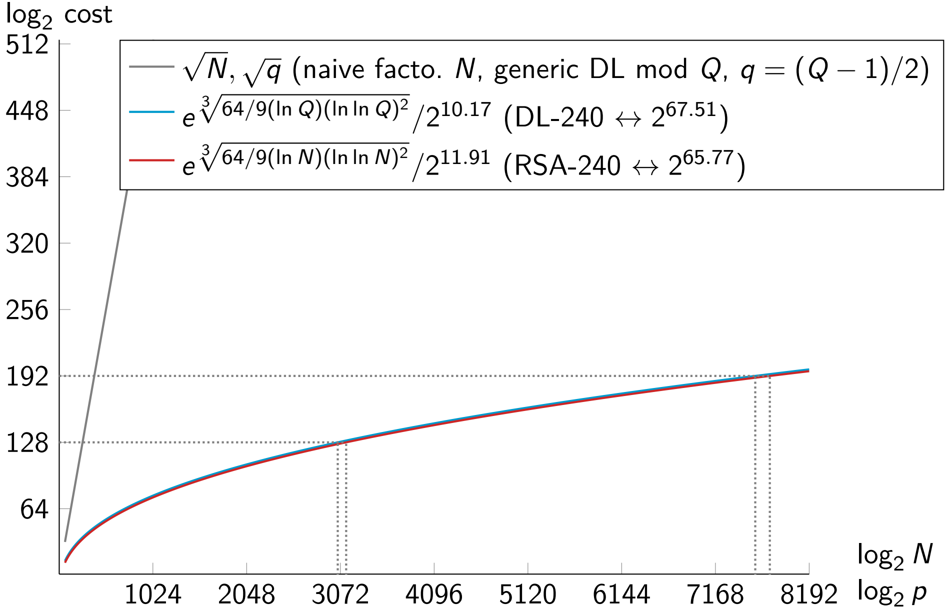
For DL in $\mathbb{F}_Q$ of length(Q) bits
n bits of security $\leftrightarrow$ the best (mathematical) attack should take at least 2^n steps

- 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
- $Q_{\text{DL-240}} = \text{NextSafePrime}(N_{240}) = N_{240} + 49204$

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

- 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) $\approx 3177 \cdot 365.25 \cdot 24 \cdot 60 \cdot 60 \cdot 2.1 \cdot 10^9 \approx 2^{67.51}$

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

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

A short-list of pairing-friendly curves at the 128-bit sec 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

Generating new families, choosing curves

- Cycles of curves for SNARKs, **Marta Bellés Muñoz** tomorrow
- New families of paring-friendly curves **Jean Gasnier** tomorrow
- Fastest pairing-friendly curves at the 192-bit security level **Georgios Fotiadis** tomorrow

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

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

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

- More on pairing computation by **Mike Scott** this afternoon
- Pairing computation on BLS curves of odd k by **Laurian Azebaze Guimagang** this session
- Even shorter Miller loop by **Emmanuel Fouotsa** tomorrow
- Pairings inside circuits by **Youssef El Housni** this afternoon

Bibliography I

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 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 II

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 III

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.

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.

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.

Bibliography IV

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.

Kenichiro Hayasaka, Kazumaro Aoki, Tetsutaro Kobayashi, and Tsuyoshi Takagi.
An experiment of number field sieve for discrete logarithm problem over 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.

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.

Bibliography V

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.

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.

Bibliography VI

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.

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

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.

Bibliography VII

Oisin Robinson.
An implementation of the extended tower number field sieve using 4d sieving in a box and a record computation in fp4, 2022.
arXiv:2212.04999 https://arxiv.org/abs/2212.04999.

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.