A Short-List of Pairing-Friendly Curves Resistant to the Special TNFS at 192-Bit Security Level

Diego F. Aranha [1] **Georgios Fotiadis** [2] Aurore Guillevic [3]

[1]Aarhus University, Denmark. Email: `dfaranha@cs.au.dk`

[2]Université du Luxembourg, Luxembourg. Email: `georgios.fotiadis@uni.lu`

[3]Université de Lorraine, CNRS, Inria, LORIA, Nancy, France. Email: `aurore.guillevic@inria.fr`

SIAM Conference on Applied Algebraic Geometry (AG23)
Elliptic Curves and Pairings in Cryptography
July 13, 2023

Motivation

Research on pairings vs future Quantum computers.

- Pairings are **not Quantum Resistant**.
- Quantum computers will become reality in **5 to 10 years** (?)
- Research on PQC and Classical Crypto **should continue in parallel**.
- Transition to PQC will require **PQC** + **Classical Crypto** to coexist.
- Some crypto applications **we cannot do**, or **cannot do well** with PQC yet.
- Pairings are useful in PQC (**isogeny-based crypto**).

Why 192-bit security?

- For long-term security: offer the option for **higher levels of security**.
- Landscape for 128-bit security is clear $\rightarrow$ **BLS12 curves dominate**.
- For 192-bit security it is **not clear** which curves are optimal.
- Some works for 192-bit security: [AFCK+13], [FK19], [BEMG19], [Gui20].

Pairings at 128-bit security

k	curve	seed	$\log_2 \mathbf{p}$	$\log_2 \mathbf{r}$	ρ	sec. lev.
		curves with efficient pairing computation				
12	BN-382	$-(2^{94}+2^{78}+2^{67}+2^{64}+2^{48}+1)$	382	382	1.000	123
12	BN-446	$2^{110}+2^{36}+1$	446	446	1.000	132
12	BLS12-381	$-(2^{63}+2^{62}+2^{60}+2^{57}+2^{48}+2^{16})$	381	255	1.500	126
12	BLS12	Aurore's Gitlab	440-448	295-300	1.500	132
12	FK12-381	$-(2^{61}+2^{60}+2^{28}+1)$	381	252	1.500	126
12	FK12-446	$-(2^{72}+2^{71}+2^{36})$	446	296	1.500	133
		curves with small $\mathbb{G}_1$ [CDS20]				
13	BW13-P310	$-\mathtt{0x8b0} = -2224$	310	267	1.167	140
19	BW19-P286	$-\mathtt{0x91} = -145$	286	259	1.111	160
		curves for SNARKs				
12	BLS12-377	$2^{63}+2^{58}+2^{56}+2^{51}+2^{47}+2^{46}+1$	377	252	1.500	126
24	BLS24-315	$-2^{32}+2^{30}+2^{22}-2^{20}+1$	315	253	1.250	160

Lessons learned from 128-bit pairings

- Many sources (**different families/seeds**) for pairing-friendly elliptic curves.
- Many papers **before** and **after** the improved TNFS attacks [KB16].
- **High degree twists** are important for fast pairing.
- Optimal curve selection depends on the **protocol/use case requirements**.
  Other things matter besides the pairing computation.
- Extending BN12 or BLS12 to 192-bit security is **not optimal** [GS19].

  BLS12 needs to go to **1150-bit prime field** for 193-bit security.

  BN12 needs to go to **1022-bit prime field** for 191-bit security.

  Higher embedding degrees are needed!

Pairings at 192-bit security: selection criteria

- At least 192-bit security in $\mathbb{G}_1, \mathbb{G}_2 \implies \log_2 r \geq 384$-bits.
- Look at embedding degrees $k > 12$.
- The size of $\mathbb{G}_T \subset \mathbb{F}_{p^k}^*$ varies: depends on k and $\rho = \log_2 p / \log_2 r$.
- Take into account **improved TNFS attacks** [KB16] in $\mathbb{F}_{p^k}$ for composite k.
  Estimate key sizes with Aurore's simulator[1].
- Use curves that admit **high degree twists**: 6, 4, 3 $\implies$ focus on composite k.
- Restrict to j-invariant $j = 0$ and $3 \mid k$, $6 \mid k$, or $j = 1728$ and $4 \mid k$.
- The ρ should be close to 1.
  This is not always optimal $\Rightarrow$ Look at ρ up to 2.

[1]Simulation tool in SageMath under MIT license: https://gitlab.inria.fr/tnfs-alpha/alpha

Why higher ρ can be helpful?

Miller-loop cost (Tate pairing):

$$\mathbf{C}_{\text{MILLER}} = (\log_2 r - 1)\mathbf{C}_{\text{DBLSTEP}} + (h_{\text{wt}}(r) - 1)\mathbf{C}_{\text{ADDSTEP}}$$

- The ρ-value is: $\rho = \log_2 p / \log_2 r$.
- For some curves we need to increase p to resist TNFS attacks [KB16].
- Then r is increased as well (without really needing it) $\Rightarrow$ increased $\mathbf{C}_{\text{MILLER}}$.
- **Solution**: Increase $\rho \Rightarrow$ increase p without affecting r.
- Beneficial also for membership testing.

However... for pairing-friendly families $(p(x), t(x), r(x))$: $\rho = \deg p(x) / \deg r(x)$.

- Increasing ρ affects final exp (more exponentiations by the seed u).
- Increasing ρ affects hashing to $\mathbb{G}_1$, $\mathbb{G}_2$.

Needs for pairing-based protocols

Efficient pairing computation.

- Short Miller loop + few addition steps + efficient final exp. formulas.

Efficient exponentiation in $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$.

- Scalar multiplication in $E(\mathbb{F}_p), E'(\mathbb{F}_{p^{k/d}})$, where d is the degree of the twist.
- Exponentiation in $\mathbb{F}_{p^k}$.

Efficient hashing to $\mathbb{G}_1$, $\mathbb{G}_2$.

- See yesterday's talks by **Jorge Chavez-Saab** on Swiftec and **Yu Dai**.
- New results by **Dimitri Koshelev** [Kos22a, Kos22b].

Efficient membership testing in $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$.

- See yesterday's talks by **Dimitri Koshelev** and **Yu Dai**.

Efficient cofactor clearing.

- Wahby–Boneh for perfect square cofactor [WB19].
- Gallant–Lambert–Vanstone (GLV) otherwise [GLV01].

Existing families for 192-bit security

Barreto–Lynn–Scott (BLS) curves [BLS03] $\longrightarrow$ **BLS21**, **BLS24** and **BLS28**.

Kachisa–Schaefer–Scott (KSS) curves [KSS08] $\longrightarrow$ **KSS16** and **KSS18**.

Freeman–Scott–Teske (FST) curves [FST10] $\longrightarrow$ **FST 6.4** for $k = 28$.

Scott-Guillevic (SG) curves [SG18] $\longrightarrow$ **SG18** and **SG20**.

Fotiadis–Konstantinou (FK) curves [FK19]:

- Fotiadis–Martindale **FM23** curve for $k = 16$ [FM19]
- Fotiadis–Martindale **FM25** curve for $k = 18$ [FM19]

Gasnier–Guillevic (GG) curves $\longrightarrow$ **GG20b**

- See last talk of the session by **Jean Gasnier**.

New family for $k = 16$

Aranha–Fotiadis–Guillevic (AFG16)

$$\begin{aligned} p(x) &= (x^{16} + 2x^{13} + x^{10} + 5x^8 + 6x^5 + x^2 + 4)/4 \\ r(x) &= \Phi_{16}(x) = x^8 + 1 \\ t(x) &= x^8 + x^5 + 2 \end{aligned}$$

with $\rho = 2$ and $\#E(\mathbb{F}_p) = h(x)r(x)$ with $h(x) = (x^4 + x)^2/4$.

Interesting features:

- Cofactor is perfect square $\Rightarrow$ **fast cofactor clearing**.
- $\sqrt{h(x)}$ divides $p(x) - 1 \Rightarrow$ the **trick of Wahby–Boneh** applies [WB19].
- For $P \in E(\mathbb{F}_p)$, the point $Q = [(x^4 + x)/2]P$ has order r.

Instantiation of families for 192-bit security

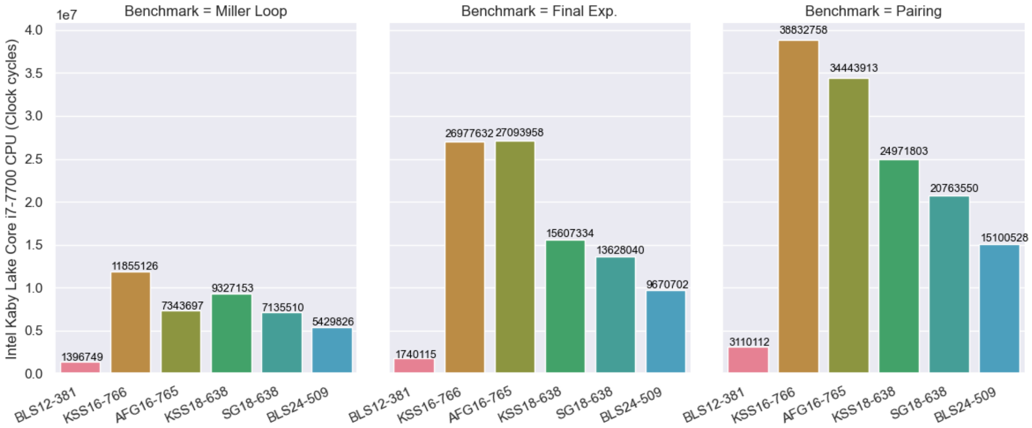
k	curve	seed	$\log_2 p$	$\log_2 r$	$k \log_2 p$	ρ	sec. lev.
16	KSS16	$2^{78} - 2^{76} - 2^{28} + 2^{14} + 2^7 + 1$	766	605	12256	1.250	194
	FM23	$2^{48} - 2^{44} - 2^{38} + 2^{31}$	765	384	12240	2.000	196
	AFG16	$-2^{48} + 2^{44} - 2^{37}$	765	384	12240	2.000	196
18	KSS18	$2^{80} + 2^{77} + 2^{76} - 2^{61} - 2^{53} - 2^{14}$	638	474	11484	1.333	193
	SG18	$-(2^{63} + 2^{54} + 2^{16})$	638	383	11484	1.666	187
	FM25	$-2^{64} + 2^{33} + 2^{30} + 2^{20} + 1$	768	384	13824	2.000	197
20	FST 6.4	$-2^{56} + 2^{44} + 1$	670	448	13400	1.500	193
	SG20	$-2^{47} - 2^{45} + 2^{15} + 2^{13}$	670	383	13400	1.750	203
	GG20b	$2^{49} + 2^{46} - 2^{41} + 2^{35} + 2^{30} - 1$	575	379	11500	1.520	196
		curves with small $\mathbb{G}_1$					
21	BLS21	$-2^{32} + 2^{25} + 2^6 + 2$	511	384	10731	1.333	199
24	BLS24	$-2^{51} - 2^{28} + 2^{11} - 1$	509	409	12216	1.250	193
27	BLS27	$-2^{21} - 2^{19} - 2^{15} + 2^{10} + 2^4 + 2^2 + 1$	426	383	11529	1.111	218
28	FST 6.4	$2^{32} - 2^{25} + 2^{22} + 2^{15} + 1$	510	384	14280	1.333	209

Theoretical comparison

k	curve	p bits	r bits	Miller loop optimal ate	final exp easy	final exp hard	final exp total	total pairing
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**	24308**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**	≈50000**m**	≈50000**m**	≈70000**m**
21	BLS21	511	384	19321**m**	717**m**	62426**m**	62426**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**

Selected curves for RELIC implementation: **KSS16**, **AFG16**, **KSS18**, **SG18**, **BLS24**.

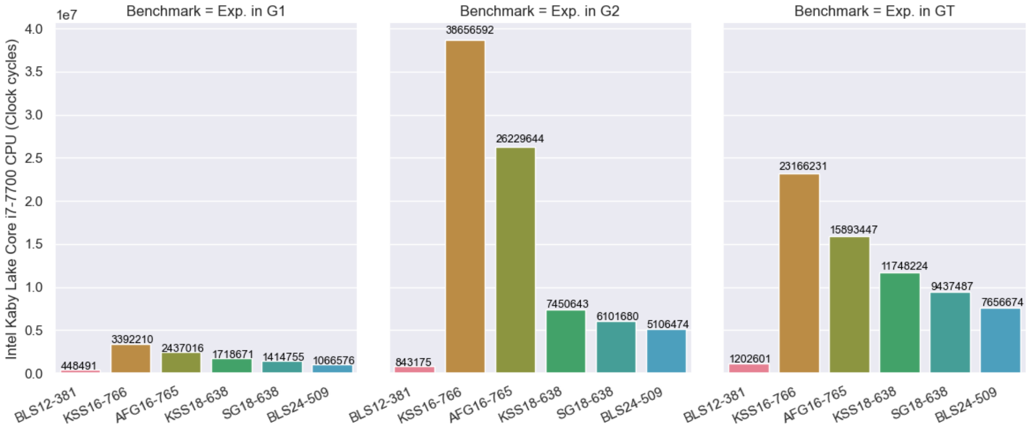
Execution time – pairing computation



Conclusion.

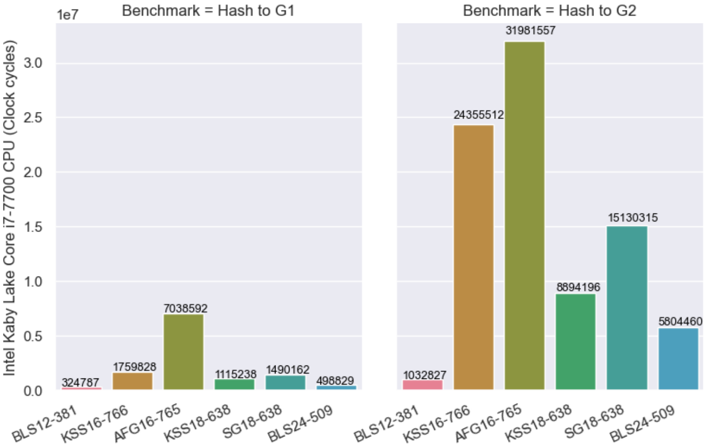
- BLS24-509 has: faster Miller loop and faster final exponentiation.
- *BLS12-381 targets 128-bit security. It is only for reference comparison.

Execution time – exponentiation in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$



Gallant–Lambert–Vanstone (**GLV**) for $\mathbb{G}_1$ [GLV01].
Galbraith–Lin–Scott (**GLS**) for $\mathbb{G}_2$ [GLS11]

Execution time – hashing to $\mathbb{G}_1, \mathbb{G}_2$ + cofactor clearing



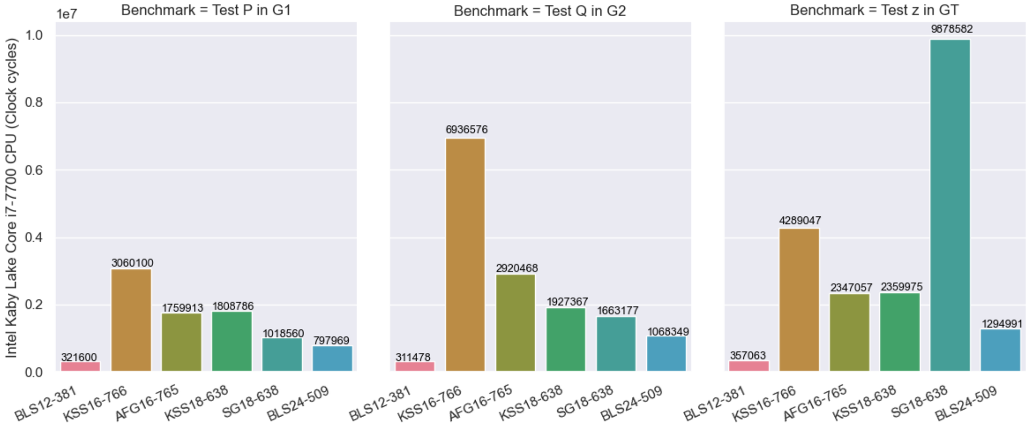
When $p \equiv 1 \bmod 3, j = 0$:

- **SwiftEC** for $\mathbb{G}_1$, $\mathbb{G}_2$ [CSRHT22].
- BLS12, KSS18, SG18, BLS24.

When $j = 1728$:

- KSS16, AFG16.
- **Koshelev** for $\mathbb{G}_2$ [Kos22a].
- **SwiftEC** for $\mathbb{G}_1$ [CSRHT22].

Execution time – subgroup membership testing[2]



$\mathbb{G}_1$: BLS12/KSS18/SG18/BLS24 (**GLV**)–KSS16/AFG16 (**Yu Dai et al.** [DLZZ23]).
$\mathbb{G}_2$: BLS12/KSS18/SG18/BLS24 (**GLS**)–KSS16/AFG16 (**Yu Dai et al.** [DLZZ23]).

[2]Credit to Mónica P. Arenas for the plots.

Conclusions

- **BLS12-381** is the best candidate at 128-bit security.
- **BLS24-509** is the best candidate at 192-bit security.
  Additional seeds for SNARKS at 192-bit security:
  https://gitlab.inria.fr/tnfs-alpha/alpha/-/tree/master
- **BLS48** is the best candidate at 256-bit security?
- Pre-print will be available soon.
- PoC implementation for all curves in SageMath.
- Optimized implementation using RELIC toolkit available at:
  https://github.com/relic-toolkit
- See also Aurore's talk for more info:
  https://members.loria.fr/AGuillevic/files/talks/23_Roscoff.pdf

Thank you!

References I

Diego F Aranha, Laura Fuentes-Castaneda, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez.
Implementing pairings at the 192-bit security level.
In *Pairing-Based Cryptography–Pairing 2012: 5th International Conference, Cologne, Germany, May 16-18, 2012, Revised Selected Papers 5*, pages 177–195. Springer, 2013.

Razvan Barbulescu, Nadia El Mrabet, and Loubna Ghammam.
A Taxonomy of Pairings, their Security, their Complexity.
Cryptology ePrint Archive, Report 2019/485, 2019.

Paulo SLM Barreto, Ben Lynn, and Michael Scott.
Constructing elliptic curves with prescribed embedding degrees.
In *Security in Communication Networks: Third International Conference, SCN 2002 Amalfi, Italy, September 11–13, 2002 Revised Papers 3*, pages 257–267. Springer, 2003.

Rémi Clarisse, Sylvain Duquesne, and Olivier Sanders.
Curves with fast computations in the first pairing group.
In *CANS'2020*, pages 280–298. Springer, 2020.

References II

- Jorge Chávez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi.
  Swiftec: Shallue-van de woestijne indifferentiable function to elliptic curves: Faster indifferentiable hashing to elliptic curves.
  In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 63–92. Springer, 2022.
- Yu Dai, Kaizhan Lin, Chang-An Zhao, and Zijian Zhou.
  Fast subgroup membership testings for g 1, g 2 and gt on pairing-friendly curves.
  Designs, Codes and Cryptography, pages 1–26, 2023.
- Georgios Fotiadis and Elisavet Konstantinou.
  TNFS Resistant Families of Pairing-Friendly Elliptic Curves.
  Journal of Theoretical Computer Science, 800:73–89, 2019.
- Georgios Fotiadis and Chloe Martindale.
  Optimal TNFS-secure Pairings on Elliptic Curves with Composite Embedding Degree.
  Cryptology ePrint Archive, Report 2019/555, 2019.

References III

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

Steven D Galbraith, Xibin Lin, and Michael Scott.
Endomorphisms for faster elliptic curve cryptography on a large class of curves.
Journal of cryptology, 24(3):446–469, 2011.

Robert P Gallant, Robert J Lambert, and Scott A Vanstone.
Faster point multiplication on elliptic curves with efficient endomorphisms.
In *Annual International Cryptology Conference*, pages 190–200. Springer, 2001.

Aurore Guillevic and Shashank Singh.
On the alpha value of polynomials in the tower number field sieve algorithm.
Cryptology ePrint Archive, Report 2019/885, 2019.

References IV

Aurore Guillevic.
A Short-List of Pairing-Friendly Curves Resistant to Special TNFS at the 128-bit Security Level.
In *PKC'2020*, pages 535–564. Springer, 2020.

Taechan Kim and Razvan Barbulescu.
Extended tower number field sieve: A new complexity for the medium prime case.
In *CRYPTO'2016*, pages 543–571. Springer, 2016.

Dmitrii Koshelev.
The most efficient indifferentiable hashing to elliptic curves of j-invariant 1728.
Journal of Mathematical Cryptology, 16(1):298–309, 2022.

Dmitrii Koshelev.
Optimal encodings to elliptic curves of j-invariants 0, 1728.
SIAM Journal on Applied Algebra and Geometry, 6(4):600–617, 2022.

References V

Ezekiel J Kachisa, Edward F Schaefer, and Michael Scott.
Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field.
In *Pairing'2008*, pages 126–135. Springer, 2008.

Michael Scott and Aurore Guillevic.
A new family of pairing-friendly elliptic curves.
In *WAIFI 2018*, pages 43–57. Springer, 2018.

Riad S. Wahby and Dan Boneh.
Fast and simple constant-time hashing to the BLS12-381 elliptic curve.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2019(4):154–179, 2019.