Constructing Efficient & STNFS–Secure Pairings

Georgios Fotiadis

Applied Security & Information Assurance (APSIA) Group
APSIA Quantum Lab
https://wwwen.uni.lu/snt/people/georgios_fotiadis
georgios.fotiadis@uni.lu, gfotiadis.crypto@gmail.com

Caramba Research Seminar
February 16, 2021

UNIVERSITÉ DU LUXEMBOURG
Interdisciplinary Centre for Security Reliability & Trust (SnT)

History

[2001–2015] Golden age:

- 2000: Joux one round tripartite key-exchange [Jou00].
- 2001: Boneh–Franklin ID-based encryption [BF01].
- 2001: Boneh–Lynn–Shacham short BLS signatures [BLS01].
- Building block for privacy–related protocols (ZKPs).
- ...

In market:

- Trusted Platform Module (TPM)
- Blockchain (ZCash, Ethereum, ...)

Clouds on the horizon:

1. Large–scale quantum computer (nothing we can do).
2. Improved DLP attacks on extension fields $\mathbb{F}_{p^{ab}}$ [KB16] (can tackle this).

...but what is a pairing?

A bilinear map:

$$\boxed{e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T} \quad \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T : \text{ cyclic groups of order } r$$

s.t. $\quad e(g^a, h^b) = e(g, h)^{ab} = e(g^b, h^a) \qquad$ (bilinearity property)

Basic requirements:

- Security: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ have a hard DLP (roughly of same complexity).
- Formula: Miller's algorithm for efficient computation of e.

In practice:

- $\mathbb{G}_1, \mathbb{G}_2$: subgroups of elliptic curves $E(\mathbb{F}_{p^k})$.
- $\mathbb{G}_1, \mathbb{G}_2$: subgroups of Jacobians of genus 2 curves $J(\mathbb{F}_{p^k})$.
- $\mathbb{G}_T$: subgroup of $\mathbb{F}_{p^k} \Rightarrow k$ is called the embedding degree.

Pairings in Cryptography

Efficiency:

- efficient finite field operations: squaring & multiplication.
- efficient elliptic curve operations: point doubling & addition.
- efficient 2–dimensional Jacobian operations: doubling & addition (headache)

Pairing types:

- Type I (symmetric): $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ (Weil, ...).
- Type II (asymmetric): $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (Tate, twisted ate, ...).
- Type III (asymmetric): $\mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T$ (ate, optimal ate, ...).

Elliptic curves

For a prime p an elliptic curve E over $\mathbb{F}_p$ is defined as:

$$\boxed{E/\mathbb{F}_p : y^2 = x^3 + ax + b} \qquad a, b \in \mathbb{F}_p$$

$\mathbb{F}_p$-rational points $E(\mathbb{F}_p)$:

- Order: $\#E(\mathbb{F}_p) = p + 1 - t$ (t: trace of Frobenius)
- Prime r divides $\#E(\mathbb{F}_p) \implies \#E(\mathbb{F}_p) = hr$ (h: cofactor)
- CM–discriminant: square–free $D > 0$ s.t.

$$\boxed{4p - t^2 = Dy^2} \quad \text{(CM–equation)}$$

Pairing–friendly elliptic curves

Embedding degree:

- Smallest $k > 0$ s.t.

$$\boxed{r \mid (p^k - 1) \Leftrightarrow \Phi_k(t-1) \equiv 0 \bmod r}$$

- Large k s.t. DLP is hard in $\mathbb{F}_{p^k}$.
- Small k for efficient squaring/multiplication in $\mathbb{F}_{p^k}$.

Pairing–friendly elliptic curve:

- Has small k (e.g. $k \leq 30$).
- Has $\rho = \log p / \log r$ (approximately) equal to 1.
- They are very rare! (usually $\log k \approx \log r$).
- Specialized algorithms needed for their construction.

Pairing–friendly elliptic curve constructions

Two main constructions:

1. $(p, t, r) \leftarrow \textsc{CocksPinch}(k, D, \lambda)$ [FST10]
2. $(p(x), t(x), r(x)) \leftarrow \textsc{BrezingWeng}(k, D, \lambda)$ [BW05]

Brezing–Weng is most common:

- $(p(x), t(x), r(x))$: complete family of pairing–friendly elliptic curves.
- Extract a member from family $(p, r, t) = (p(u), r(u), t(u))$, for some $u \in \mathbb{Z}$.
- Such p is called special (derived from evaluation of polynomial).
- Two well–known families for $k = 12$ and $D = 3$: Barreto–Naehrig (BN12), Barreto–Lynn–Scott (BLS12).
- Additional families for $k = 16, D = 1$ and $k = 18, D = 3$: Kachisa–Schaefer–Scott (KSS16), Kachisa–Schaefer–Scott (KSS18).

Popular examples (better suited for 128–bit security)

Barreto–Naehrig (BN12) family: $k = 12$, $D = 3$, $\rho = 1$

$$\begin{aligned} r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1 \\ t(x) &= 6x^2 + 1 \\ p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \end{aligned}$$

Barreto–Lynn–Scott (BLS12) family: $k = 12$, $D = 3$, $\rho = 1.5$

$$\begin{aligned} r(x) &= \Phi_{12}(x) = x^4 - x^2 + 1 \\ t(x) &= x \\ p(x) &= (x-1)^2(x^4 - x^2 + 1)/3 + x \end{aligned}$$

Currently used in practice:

- BN12–254: ($\log p = \log r = 254$) in TPM2.0, Ethereum.
- BLS12–381: ($\log p = 381, \log r = 254$) in ZCash.

Popular examples (better suited for 192–bit security)

Kachisa–Schaefer–Scott (KSS16) family: $k = 16$, $D = 1$, $\rho = 1.25$

$$r(x) = x^8 + 48x^4 + 625$$
$$t(x) = (2x^5 + 41x + 35)/35$$
$$p(x) = (x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125)/980$$

Kachisa–Schaefer–Scott (KSS18) family: $k = 18$, $D = 3$, $\rho = 1.333$

$$r(x) = (x^6 + 37x^3 + 343)/343$$
$$t(x) = (x^4 + 16x + 7)/7$$
$$p(x) = (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 1763x + 2401)/21$$

Many alternative Brezing–Weng families by Freeman–Scott–Teske [FST10].

Security

$$\mathbb{G}_1 \subset E(\mathbb{F}_p)[r], \quad \mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r], \quad \mathbb{G}_T \subset \mathbb{F}_{p^k} \qquad (\#\mathbb{G}_1 = \#\mathbb{G}_2 = \#\mathbb{G}_T = r)$$

Security in $\mathbb{G}_1, \mathbb{G}_2$ (Pollard-ρ): $O(\sqrt{r})$.

- r large prime factor of $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_{p^k})$.

$$[a]P \in E(\mathbb{F}_p) \longrightarrow \boxed{\text{Pollard–}\rho} \longrightarrow a \in (\mathbb{Z}/r\mathbb{Z})^\times$$

$$[b]Q \in E(\mathbb{F}_{p^k}) \longrightarrow \boxed{\text{Pollard–}\rho} \longrightarrow b \in (\mathbb{Z}/r\mathbb{Z})^\times$$

Security in $\mathbb{G}_T$ (NFS variants): harder to give estimates.

$$g^a \in \mathbb{F}_{p^k} \longrightarrow \boxed{\text{NFS variants}} \longrightarrow a \in (\mathbb{Z}/r\mathbb{Z})^\times$$

Security in target group

Asymptotic complexity of DLP in $\mathbb{F}_{p^k}$:

$$\boxed{L_{p^k}[c] = \exp\left[(c+o(1))\left(\ln p^k\right)^{1/3}\left(\ln\ln p^k\right)^{2/3}\right]}$$

For special primes p (e.g. Brezing–Weng curves):

- prime k: $c = 1.923$.
- composite k: $c = 1.526$, Kim–Barbulescu STNFS [KB16] (dropped from 1.923).
- BN12–254 security in $\mathbb{F}_{p^{12}}$: 110–bits, BLS12–381 security in $\mathbb{F}_{p^{12}}$: 130–bits.
- ...but asymptotic complexity is not accurate!

Better estimates for STNFS complexity:

1. $SecLev(\mathbb{F}_{p^k}) \leftarrow \textsc{Simulator}\mathrm{BD}(k, u, p(x))$ in [BD19] (SageMath)
2. $SecLev(\mathbb{F}_{p^k}) \leftarrow \textsc{Simulator}\mathrm{GMT}(k, u, p(x))$ in [GMT20] (SageMath) [1]
   $\Rightarrow$ sec. lev. BN12–254: 103–bits, sec. lev. BLS12–381: 126–bits.

[1] Available at: https://gitlab.inria.fr/tnfs-alpha/alpha/tree/master/sage

STNFS-Secure Curves

We need to update key sizes:

1. Barbulescu–Duquesne:
   - Increase BN12 and BLS12 parameters [BD19] until they are secure.
   - Barbulescu–El Mrabet–Ghammam: New key sizes for older curves [BEMG19]. Freeman–Scott–Teske (FST) curves [FST10].

2. Guillevic–Masson–Thomé:
   - Use Cocks–Pinch curves [GMT20] (examples for $k = 5, 6, 7, 8$).
   - STNFS does not apply to non-special primes p.
   - Less efficient examples.
   - Best example GMT8–544 curve for 128–bits security.

3. Fotiadis–Konstantinou:
   - New Brezing–Weng families using $L_{p^k}[c]$ [FK18, FK19].
   - Fotiadis–Martindale:
     Optimal members of Fotiadis–Konstantinou families [FM19].
     Use SIMULATORBD to estimate security level in $\mathbb{F}_{p^k}$.

New Brezing–Weng curves

Construction of Fotiadis–Konstantinou (FK12) family for $k = 12, D = 3, \rho = 1.5$:

$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1 \qquad \text{(BN12 polynomial)}$$
$$t(x) = -6x^2 + 1$$
$$p(x) = 1728x^6 + 2160x^5 + 1548x^4 + 756x^3 + 240x^2 + 54x + 7$$

Two optimal Fotiadis–Martindale examples:

Curve	seed u	$\log r$	$\log p$	$k \log p$	sec. in $\mathbb{F}_{p^{12}}$ [2]	ρ
FM12–398	$-2^{64} - 2^{63} - 2^{11} - 2^{10}$	264	398	4776	127	1.5
FM12–446	$-2^{72} - 2^{71} - 2^{36}$	296	446	5352	133	1.5

[2] Security in $\mathbb{F}_{p^{12}}$ using SimulatorBD (better estimates with SimulatorGMT).

New Brezing–Weng curves

Fotiadis–Martindale curves at 128–bit security [FM19]

Label	k	D	$\deg(r)$	$\deg(p)$	$\log(p)$	$k\log(p)$	ρ
1	8	1	4	8	760	6080	2
2	8	1	4	8	760	6080	2
3	8	2	4	8	768	6144	2
4	8	3	8	16	512	4906	2
5	8	1	4	8	752	6016	2
6	8	1	4	8	704	5632	2
7	8	1	4	8	752	6016	2
8	8	1	4	8	752	6016	2
9	8	1	8	16	512	4096	2
10	9	3	6	12	624	5616	2
11	9	3	6	12	516	4644	2
12	9	3	6	12	512	4608	2
13	10	1	8	14	448	4480	1.75
14	10	5	8	14	448	4480	1.75
15	10	15	8	14	448	4480	1.75
16	10	1	8	14	448	4480	1.75
17	12	3	4	6	384	4608	1.5
18	12	2	8	14	448	5376	1.75
19	12	3	4	6	444	5328	1.5
20	12	3	4	6	480	5760	1.5

Pairing computation: Tate pairing

Algorithm 1: TatePairing($P \in E(\mathbb{F}_p)[r], Q \in E(\mathbb{F}_{p^k})[r], r = (1, r_{n-1}, \ldots, r_1, r_0)_2$)

1: $f \leftarrow 1$; $R \leftarrow P$ //Miller loop: steps 2–5
2: **for** $i = \lfloor \log_2(r) \rfloor - 1, \ldots, 0$ **do**
3: $\quad (R, f) \leftarrow$ DblStep(R, P, Q, f)
4: $\quad$ **if** $r_i = 1$ **then**
5: $\quad\quad (R, f) \leftarrow$ AddStep(R, P, Q, f)
6: $f \leftarrow$ FinalExp(f) //f to exponent $(p^k - 1)/r$
7: **return** f

DblStep(R, P, Q, f)

1: $R \leftarrow [2]R$
2: $h_{R,R}(Q) = l_{R,R}(Q)/v_R(Q)$
3: $f \leftarrow f^2 \cdot h_{R,R}(Q)$

AddStep(R, P, Q, f)

1: $R \leftarrow R + P$
2: $h_{R,P}(Q) = l_{R,P}(Q)/v_R(Q)$
3: $f \leftarrow f \cdot h_{R,P}(Q)$

$$\mathbf{C}_{\text{Tate}} = \underbrace{(\log_2(r) - 1)\mathbf{C}_{\text{DblStep}} + (h_{\text{wt}}(r) - 1)\mathbf{C}_{\text{AddStep}}}_{\text{Miller loop}} + \mathbf{C}_{\text{FinalExpo}}$$

Pairing computation: Improving efficiency

Reduce iterations in Miller's loop:

- Optimal ate pairing [Ver09]: $\log_2(r)/\varphi(k)$ iterations instead of $\log_2(r)$.
- Vercauteren: $\log_2(r)/\varphi(k)$ the shortest loop we can have (conjecture).

Optimal ate is a type III pairing: $\mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T$

- High degree twists to reduce complexity in DBLSTEP & ADDSTEP.
- Most operations in $\mathbb{F}_{p^{k/\delta}}$, where $\delta \mid k$ s.t. E^t degree δ twist of E.
- Point in Jacobian coordinates as in [GMT20]:

$$\begin{array}{rcl} \text{Jacobian coordinates} & \to & \text{affine coordinates} \\ (X, Y, Z, Z^2) & \to & (X/Z^2, Y/Z^3) \end{array}$$

- Most efficient examples today use the optimal ate pairing.

Pairing computation: Improving efficiency

Improve the final exponentiation:

- Split exponent $(p^k - 1)/r$ into "easy part" and "hard part".

$$(p^k - 1)/r = \underbrace{(p^k - 1)/\Phi_k(p)}_{\text{"easy part"}} \times \underbrace{\Phi_k(p)/r}_{\text{"hard part"}}$$

- See e.g. Aranha et al. [AFCK$^+$12] for details, or Scott et al. [SBC$^+$09].
- In the case of Brezing–Weng curves:
  Hard part: $\deg(p) - 1$ exponentiations of size $\approx (\log_2(r)/\varphi(k))$.
- Larger k implies larger $\deg(p)$, hence more expensive final exponentiation.

Optimal ate pairings in practice

For seed u s.t. $(p, t, r) = (p(u), t(u), r(u))$ and $\log_2(u) \approx \log_2(r)/\varphi(k)$:

- BLS12 curves:

$$\mathbf{C}_{\mathrm{OptAte}} = \underbrace{(\log_2(u) - 1)\mathbf{C}_{\mathrm{DBLSTEP}} + (h_{\mathrm{wt}}(u) - 1)\mathbf{C}_{\mathrm{ADDSTEP}}}_{\text{Miller loop}} + \mathbf{C}_{\mathrm{FINALEXPO}}$$

  Require minimum $\log_2(u)$ and $h_{\mathrm{wt}}(u)$.

- FM12 curves for $T = 6u + 2$:

$$\mathbf{C}_{\mathrm{OptAte}} = \underbrace{(\log_2(T) - 1)\mathbf{C}_{\mathrm{DBLSTEP}} + (h_{\mathrm{wt}}(T) - 1)\mathbf{C}_{\mathrm{ADDSTEP}}}_{\text{Miller loop}} + \mathbf{C}_{\mathrm{EXTRAMULT}}$$
$$+ \mathbf{C}_{\mathrm{FINALEXPO}}$$

  Require minimum $\log_2(T), h_{\mathrm{wt}}(T)$ and minimum $\log_2(u), h_{\mathrm{wt}}(u)$.

STNFS–Secure pairings at 128–bit security [Gui20, PKC'2020]

Curve	$\log p$	$\log r$	$\log p^k$	sec. $\mathbb{F}_{p^k}$	ρ	Miller loop	Final exp.	time (ms) [3]
GMT6	672	256	4028	128	2.625	4601**m**	3871**m**	1.53
GMT8	544	256	4349	131	2.125	4502**m**	7056**m**	1.49
BN12	446	446	5376	132	1	11620**m**	5349**m**	1.44
BLS12	446	299	5376	132	1.5	7805**m**	7723**m**	1.32
FM12	446	296	5352	136	1.5	7853**m**	8002**m**	1.35
KSS16	339	256	5424	140	1.32	7691**m**	18235**m**	1.69
BN12	254	254	3048	103	1	6820**m**	3585**m**	0.33

A. Guillevic (https://members.loria.fr/AGuillevic/pairing-friendly-curves/):

> *"For efficient non–conservative pairings, choose BLS12-381 (or any other BLS12 curve or Fotiadis-Martindale curve of roughly 384 bits), for conservative but still efficient, choose a BLS12 or a Fotiadis-Martindale curve of 440 to 448 bits."*

[3] Aranha's Relic library: time for one $\mathbb{F}_p$–mult. (**m**) based on number of 64–bit words of p (https://github.com/relic-toolkit/relic).

STNFS–Secure pairings at 128–bit security (Non–Conservative)

Curve	seed u	$\log p$	$\log r$	$\log p^k$	ρ	Miller loop	Final exp.	time (ms)
BN12	$-2^{62}-2^{55}-1$	254	254	3048	1	6820**m**	3585**m**	0.33
BLS12	$-2^{63}-2^{62}-2^{60}-2^{57}-2^{48}-2^{16}$	381	254	4572	1.5	6625**m**	6673**m**	0.86
FM12	$-2^{61}-2^{60}-2^{28}-1$	381	252	4572	1.5	6863**m**	7732**m**	0.95
FM12	$-2^{62}+2^{56}+2^{2}+1$	383	254	4596	1.5	6962**m**	7732**m**	0.96
FM12	$-2^{63}-2^{14}-2^{12}$	389	258	4668	1.5	7061**m**	7462**m**	1.23
FM12	$-2^{64}-2^{63}-2^{11}-2^{10}$	398	265	4776	1.5	7061**m**	7912**m**	1.27

Discussion:

- BLS12–381 and FM12–381 seem to be acceptable options.
- Moving to BLS12–446 or FM12–446 implies less efficient protocols.
- Security levels in $\mathbb{F}_{p^k}$ depend on further improvements of (S)TNFS variants.
- FM12 curves need more study.

Pairings at 192–bit security

Two main approaches:

1. Use BN12 or BLS12 with adjusted parameters.
   Guillevic–Singh [GS19]:

Curve	$\log_2(p)$	$\log_2(p^k)$
BN12	1022	12264
BLS12	1150	13800
FM12	1150	13800

2. Increase the embedding degree k.
   Known examples: KSS16–766, KSS18–638, BLS24–512
   New families reported in [FK19] and new curves in [FM19]:

Label	k	D	$\deg(r)$	$\deg(p)$	$\log(p)$	$k\log(p)$	ρ
21	15	3	8	16	784	11760	2
22	15	3	8	16	768	11520	2
23	16	1	8	16	768	12288	2
24	16	1	8	16	768	12288	2
25	18	3	6	12	792	14256	2
26	18	3	6	12	768	13824	2
27	20	1	8	12	648	12960	1.5

Two Fotiadis–Konstantinou families

Fotiadis–Konstantinou (FK16) family for $k = 16$, $D = 1$, $\rho = 2$:

$$r(x) = \Phi_{16}(x) = x^8 + 1$$
$$t(x) = x^8 + x + 2$$
$$p(x) = (x^{16} + x^{10} + 5x^8 + x^2 + 4x + 4)/4$$

Fotiadis–Konstantinou (FK18) family for $k = 18$, $D = 3$, $\rho = 2$:

$$r(x) = \Phi_{18}(x) = x^6 - x^3 + 1$$
$$t(x) = x^6 - x^4 - x^3 + 2$$
$$p(x) = (3x^{12} - 3x^9 + x^8 - 2x^7 + 7x^6 - x^5 - x^4 - 4x^3 + x^2 - 2x + 4)/3$$

Fotiadis–Martindale: Two curve examples [FM19]

- FM16–766 with seed $u = 2^{48} + 2^{28} + 2^{26}$.
- FM18–768 with seed $u = -2^{64} - 2^{35} + 2^{11} - 1$.

Pairings at 192–bit security

Curve	$\log p$	$\log r$	$\log p^k$	ρ	Miller loop	Final exp.	Total
BN12	1022	1022	12264	1.000	25760**m**	10533**m**	36293**m**
BLS12	1150	768	13800	1.497	19425**m**	14353**m**	33778**m**
KSS16	766	605	12255	1.266	16944**m**	32896**m**	49840**m**
FM16	766	384	12255	1.995	10331**m**	28981**m**	39312**m**
KSS18	638	474	11477	1.346	16408**m**	25816**m**	42224**m**
FM18	768	384	13824	2.000	13412**m**	24896**m**	38308**m**

For larger k:

- More expensive final exponentiation.
- Shorter Miller loops + smaller prime p.
- FM16–766 & FM18–768 faster than KSS16–766.
- The best example for 192–bit security seems to be KSS18–638 (smaller p).
- Is there a family with $k = 18$ and $\rho = 1.667$?
- Interested to see how BLS24–512 compares to the above.

Measuring Optimal Curves

Condition $\rho = 1$ may not be sufficient for security & efficiency:

- Sometimes it is necessary to increase p without affecting r.
  $\Rightarrow$ hence larger ρ might be better for specific k.
- e.g. $k = 12$: BLS12–446 and FM12–446 more efficient than BN12–446.
- e.g. $k = 16$: FM16–766 more efficient than KSS16–766.

Additionally define the τ–value: $\tau = \log(\sqrt{r})/n$:

- n: the estimated security level in $\mathbb{F}_{p^k}$ ($n = \textsc{Simulator}\mathrm{GMT}(k, u, p(x))$).
- $\tau = 1 \Rightarrow$ the security level in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ is the same.

Curve	BN12–446	BLS12–446	FM12–446
τ–value	1.7	1.1	1.1

Conclusion & Future Work

Pairing-friendly curves with prime embedding degree:

- e.g. [GMT20] for $k = 5, 7$: best example GMT7–512 ($\approx 3\times$BLS12–446).
- Most speedups used for composite k do not apply.

Pairing implementation:

- Optimization of finite field multiplication for specific primes.
- Parallel/side–channel resistant implementations.

Explore further FM12, FM16, FM18 curves.

- e.g. hashing in $\mathbb{G}_1$ or $\mathbb{G}_2$ in BLS signatures with FM12 curves.

Pairings on genus 2 hyperelliptic curves (work under review):

- Best case scenario: examples close to elliptic curves, but slightly worse.
  e.g. for 192–bit security: Ihsii16–671 with 52778**m** [Ish18].
- Need further improvement for doubling & addition in Jacobian.
- Doubling & addition using Fan et al. coordinate system [FGJ08].

Thank you!

Georgios Fotiadis

Applied Security & Information Assurance (APSIA) Group
APSIA Quantum Lab
https://wwwen.uni.lu/snt/people/georgios_fotiadis
georgios.fotiadis@uni.lu, gfotiadis.crypto@gmail.com

@giofotiadis

Université du Luxembourg
Interdisciplinary Centre for Security Reliability & Trust (SnT)

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'2012*, pages 177–195. Springer, 2012.

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

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

Dan Boneh and Matt Franklin.
Identity-based encryption from the Weil pairing.
In *CRYPTO'2001*, pages 213–229. Springer, 2001.

References II

Dan Boneh, Ben Lynn, and Hovav Shacham.
Short signatures from the Weil pairing.
In *ASIACRYPT'2001*, pages 514–532. Springer, 2001.

Friederike Brezing and Annegret Weng.
Elliptic Curves Suitable for Pairing Based Cryptography.
Designs, Codes and Cryptography, 37(1):133–141, 2005.

Xinxin Fan, Guang Gong, and David Jao.
Efficient Pairing Computation on Genus 2 Curves in Projective Coordinates.
In *SAC'2008*, pages 18–34. Springer, 2008.

Georgios Fotiadis and Elisavet Konstantinou.
Generating Pairing-Friendly Elliptic Curve Parameters using Sparse Families.
Journal of Mathematical Cryptology, 12(2):83–99, 2018.

References III

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.

David Freeman, Michael Scott, and Edlyn Teske.
A Taxonomy of Pairing-Friendly Elliptic Curves.
Journal of Cryptology, 23(2):224–280, 2010.

Aurore Guillevic, Simon Masson, and Emmanuel Thomé.
Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation.
Designs, Codes and Cryptography, pages 1–35, 2020.

References IV

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.

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.

Masahiro Ishii.
Pairings on Hyperelliptic Curves with Considering Recent Progress on the NFS Algorithms.
In *Mathematical Modelling for Next-Generation Cryptography*, pages 81–96. Springer, 2018.

Antoine Joux.
A one round protocol for tripartite Diffie–Hellman.
In *ANTS'2000*, pages 385–393. Springer, 2000.

References V

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.

Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J Dominguez Perez, and Ezekiel J Kachisa.
On the final exponentiation for calculating pairings on ordinary elliptic curves.
In *PAIRING'2009*, pages 78–88. Springer, 2009.

Frederik Vercauteren.
Optimal pairings.
IEEE Transactions on Information Theory, 56(1):455–461, 2009.