A short-list of pairing-friendly curves resistant to Special TNFS at the 128-bit security level

Aurore Guillevic

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

PKC, June 4, 2020

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...)

Bilinear pairings

Rely on

- Discrete Log Problem (DLP):
  given $g, h \in \mathbb{G}$, compute x s.t. $g^x = h$
- Diffie-Hellman Problem (DHP):
  given $g, g^a, g^b \in \mathbb{G}$, compute g^{ab}
- bilinear DLP and DHP
- pairing inversion problem

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

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

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

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

Attacks

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

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

Attacks

- inversion of e : hard problem (exponential)

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

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

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{r})$)

Pairing-based cryptography

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension

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

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{r})$)
- discrete logarithm computation in $\mathbb{F}_{p^n}^*$: **easier, subexponential** $\rightarrow$ take a large enough field

Pairing-friendly curves are special

$E: y^2 = x^3 + ax + b$ over $\mathbb{F}_p$
$\#E(\mathbb{F}_p) = p + 1 - t$ of large prime factor r
discriminant D s.t. $t^2 - 4p = -Dy^2$, D square-free
$r \mid p^n - 1$, $\mathbb{G}_T \subset \mathbb{F}_{p^n}$, n is minimal : **embedding degree**
Tate Pairing: $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
When n is small, the curve is *pairing-friendly*.
This is very rare: usually $\log n \sim \log r$ ([Balasubramanian Koblitz]).

$\mathbb{G}_T \subset p^n$	p^2, p^6	p^3, p^4, p^6	p^{12}	p^{16}	p^{18}	p^{24}
Curve	supersingular	MNT	BN, BLS12	KSS16	KSS18	BLS24

MNT, $n = 6$: variable D,
$p(x) = 4x^2 + 1$, $\#E(\mathbb{F}_p) = r(x) = 4x^2 - 2x + 1$
BN, $n = 12$: $D = -3$, $E: y^2 = x^3 + b$
$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$
$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$

Choosing pairing-friendly curves

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

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

Which curves are the best options?

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

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

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

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

- Special NFS in $\mathbb{F}_{p^n}$: Joux–Pierrot 2013
- Tower NFS (TNFS): Barbulescu–Gaudry–Kleinjung 2015
- Extended Tower NFS: Kim–Barbulescu, Kim–Jeong, Sarkar–Singh 2016

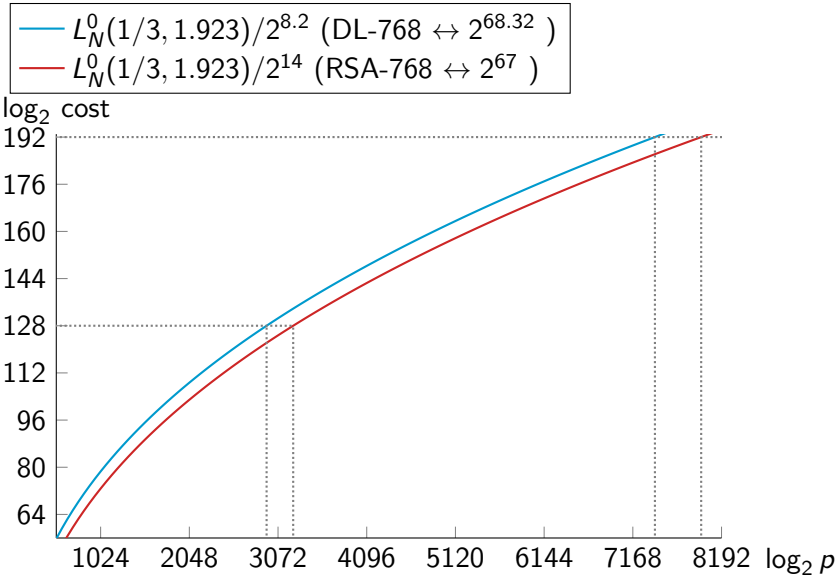
Use more structure: subfields

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

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

medium characteristic $p = L_{p^n}(\alpha_p)$, $1/3 < \alpha_p < 2/3$: $L_{p^n}(1/3, c)$	
$c = (96/9)^{1/3} \simeq 2.201$	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

Lenstra Verheul extrapolation for prime fields



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

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

Largest record computations in $\mathbb{F}_{p^n}$ with NFS[1]

Finite field	Size of p^n	Cost: CPU days	Authors	sieving dim
$\mathbb{F}_{p^{12}}$	203	11	[HAKT13]	7
$\mathbb{F}_{p^6}$	423	3,400	[McGR20]	3
$\mathbb{F}_{p^6}$	422	9,520	[GGMT17]	3
$\mathbb{F}_{p^5}$	324	386	[GGM17]	3
$\mathbb{F}_{p^4}$	392	510	[BGGM15b]	2
$\mathbb{F}_{p^3}$	593	8,400	[GGM16]	2
$\mathbb{F}_{p^2}$	595	175	[BGGM15a]	2
$\mathbb{F}_p$	768	1,935,825	[KDLPS17]	2
$\mathbb{F}_p$	795	1,132,275	[BGGHTZ19]	2

None used TNFS, only NFS and NFS-HD were implemented.

[1] Data extracted from DiscreteLogDB by L.Grémy

Post-STNFS pairing-friendly curves

- FK18 Fotiadis–Konstantinou: new curves based on $L_{p^n}(c)$
- MSS16 Menezes–Sarkar–Singh: opened the black-box of STNFS algorithm
- BD19 Barbulescu–Duquesne: proposed a model of cost, refined keysizes
- FM19 Fotiadis–Martindale: new secure curves based on BD19 cost model
- GS19 G–Singh: improved cost model with α and Murphy's E value
- GMT20 G–Masson–Thomé: variants of Cocks-Pinch curves
- BEG19 Barbulescu–El Mrabet–Ghammam: scanned many possible curves
- This work: applies systematically GS19 cost model
  and revisits BEG19

Brezing–Weng generic construction

$r(x) \leftarrow$ irreducible polynomial s.t.
$K = \mathbb{Q}[x]/(r(x)) \ni \zeta_n$ a primitive n-th root of unity,
and $-D$ is a square in K (e.g. $r(x) \leftarrow \Phi_n(x)$)
$K \leftarrow \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(r(x))$
$a(x) \leftarrow$ a polynomial mapping to $a(\alpha) = \zeta_n$ in K
$e \leftarrow$ integer in $\{1, \ldots, n-1\}$, $\gcd(e, n) = 1$
$t(x) \leftarrow a(x)^e + 1 \bmod r(x)$
$y(x) \leftarrow (t(x) - 2)/\sqrt{-D} \bmod r(x)$
$p(x) \leftarrow (t(x)^2 + Dy(x)^2)/4$
if $p(x)$ is not irreducible return $\perp$
if $p(x)$ does not represent primes return $\perp$
return $(p(x), r(x), t(x), y(x), D)$

Selection criteria

Curves:

- Brezing–Weng, $6 \leq n \leq 21$, $D \in \{1, 2, 3, \ldots, n\}$
- BN, BLS, FK, FM, etc

Security estimate:

- r at least 256 bits
- $3072 \leq p^n \leq 5376 (= 448 \times 12$ for BN, BLS12)
- test all possible *Special* variants of STNFS
  - for even $p(x) = p(-x)$, let $P(x)$: $P(x^2) = p(x)$
  - for palindrome $p(x) = p(1/x)x^d$, let $P(x)$: $P(x + 1/x) = 0 \bmod p(x)$
  - for any $p(x) = a_0 + a_1 x + \ldots + a_d x^d$, let $P_i(x)$: $P(u^i) = p(u)$ for $1 < i \leq d/2$
  - combine the three above
- test all possible *Tower* variants of STNFS: test all subfields $\mathbb{F}_{p^i}$ where $i \mid n$

Key size for pairings: sort-list, 128-bit security level

CP = Cocks–Pinch, BW = Brezing–Weng, BLS = Barreto–Lynn–Scott
FM = Fotiadis–Martindale

n	curve	D	deg $p(x)$	seed u	p bits	p^n bits	r bits	DL cost in $\mathbb{F}_{p^n}$
6	CP	3	4	$2^{128}-2^{124}-2^{69}$ GMT20	672	4028	256	128 GMT20
8	CP	1	8	$2^{64}-2^{54}+2^{37}+2^{32}-4$ GMT20	544	4349	256	131 GMT20
10	FM15	15	14	$2^{32}-2^{26}-2^{17}+2^{10}-1$	446	4460	256	133
11	BW	3	26	-0x1d2a	333	3663	258^+	131
11	BW	11	16	$-2^{26}+2^{21}+2^{19}-2^{11}-2^9-1$	412	4522	256	145
12	BN	3	4	$2^{110}+2^{36}+1$ P11	446	5376	446	132 GS19
12	BLS	3	6	$-(2^{74}+2^{73}+2^{63}+2^{57}+2^{50}+2^{17}+1)$	446	5376	299	132 GS19
12	FM17	3	6	$-2^{72}-2^{71}-2^{36}$ FM19	446	5352	296	136
13	BW	3	28	0x8b0	310	4027	267^+	140
14	BW	3	16	$2^{21}+2^{19}+2^{10}-2^6$	340	4755	256	148
16	KSS16	1	10	$-2^{34}+2^{27}-2^{23}+2^{20}-2^{11}+1$ BD19	330	5280	257	140 GS19
16	KSS16	1	10	$2^{34}-2^{30}+2^{26}+2^{23}+2^{14}-2^5+1$	330	5268	256	140

`https://gitlab.inria.fr/tnfs-alpha/alpha`
`sage/example_curves_short_list.sage`

Key size for pairings: sort-list, 128-bit security level

m multiplication in $\mathbb{F}_p$, **i** inversion in $\mathbb{F}_p$

Curve	bits p	Miller loop	final exp.	total
Cocks–Pinch $k = 6$	672	4601**m**	3871**m**	8472**m**
Cocks–Pinch $k = 8$	544	4502**m**	7056**m**	11558**m**
BN	446	11620**m**	5349**m**	16969**m**
BLS12	446	7805**m**	7723**m**	15528**m**
Fotiadis–Martindale	446	7853**m**	8002**m**	15855**m**
KSS16	339	7691**m**	18235**m**	25926**m**

Brezing–Weng

$k = 11, D = 3, a = 0$	333	29187**m**	$+2\mathbf{i}_{11}$
$k = 11, D = 11, a = 2$	412	25153**m**	$+\mathbf{i}_{11}$
$k = 13, D = 3, a = 0$	310	29919**m**	$+2\mathbf{i}_{13}$
$k = 10, D = 15, a = -3$	446	15784**m**	$+\mathbf{i}_{10} + \mathbf{i}_5$
$k = 14, D = 3, a = 0$	340	16200**m**	$+\mathbf{i}_{14} + \mathbf{i}_7$

`https://gitlab.inria.fr/tnfs-alpha/alpha`
`sage/example_curves_short_list.sage`

Key size for pairings: popular curves

	cost DL 2^{128}		cost DL 2^{192}	
$\mathbb{F}_{p^n}$, curve	$\log_2 p$	$\log_2 p^n$	$\log_2 p$	$\log_2 p^n$
$\mathbb{F}_p$	3072–3200		7400–8000	
$\mathbb{F}_{p^4}$, MNT-4	≈ 1024	≈ 4096	–	–
$\mathbb{F}_{p^6}$, MNT-6	640–672	3840–4032	≈ 1536	≈ 9216
$\mathbb{F}_{p^{12}}$, BN	416–448	4992–5376	≈ 1024	≈ 12288
$\mathbb{F}_{p^{12}}$, BLS	416–448	4992–5376	≈ 1120	≈ 13440
$\mathbb{F}_{p^{12}}$, FM	416–448	4992–5376	≈ 1120	≈ 13440
$\mathbb{F}_{p^{16}}$, KSS	330	5280	≈ 768	≈ 12288
$\mathbb{F}_{p^{18}}$, KSS	348	6264	≈ 640	≈ 11556
$\mathbb{F}_{p^{24}}$, BLS	318	7621	≈ 512	≈ 12202

Many seeds of curves in each family, generate your own curve to suit your needs!
`https://gitlab.inria.fr/tnfs-alpha/alpha`
`sage/tnfs/param/TestVectorSparseSeed.py`

Bibliography I


R. Barbulescu and S. Duquesne.
Updating key size estimations for pairings.
Journal of Cryptology, 32(4):1298–1336, Oct. 2019.
https://ia.cr/2017/334.


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


R. Barbulescu, P. Gaudry, A. Guillevic, and F. 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.


R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain.
Improving NFS for the discrete logarithm problem in non-prime finite fields.
In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 129–155.
Springer, Heidelberg, Apr. 2015.
https://ia.cr/2016/605.

Bibliography II


R. Barbulescu, P. Gaudry, and T. Kleinjung.
The tower number field sieve.
In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 31–55. Springer, Heidelberg, Nov. / Dec. 2015.
https://ia.cr/2015/505.


R. Barbulescu and A. Lachand.
Some mathematical remarks on the polynomial selection in NFS.
Math. Comp., 86(303):397–418, 2017.
https://hal.inria.fr/hal-00954365, https://doi.org/10.1090/mcom/3112.


F. Brezing and A. Weng.
Elliptic curves suitable for pairing based cryptography.
Des. Codes Cryptography, 37(1):133–141, 2005.
https://ia.cr/2003/143.


S. Chatterjee, A. Menezes, and F. Rodríguez-Henríquez.
On instantiating pairing-based protocols with elliptic curves of embedding degree one.
IEEE Transactions on Computer, 66(6):1061–1070, 2017.
https://ia.cr/2016/403.

Bibliography III


G. Fotiadis and E. Konstantinou.
TNFS resistant families of pairing-friendly elliptic curves.
Theoretical Computer Science, 800:73–89, 31 December 2019.
https://ia.cr/2018/1017.


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


D. Freeman, M. Scott, and E. Teske.
A taxonomy of pairing-friendly elliptic curves.
Journal of Cryptology, 23(2):224–280, Apr. 2010.
https://ia.cr/2006/372.


P. Gaudry, A. Guillevic, and F. 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

L. Grémy, A. Guillevic, and F. 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.

L. Grémy, A. Guillevic, F. Morain, and E. Thomé.
Computing discrete logarithms in $\mathbb{F}_{p^6}$.
In C. Adams and J. Camenisch, editors, *SAC 2017*, volume 10719 of *LNCS*, pages 85–105. Springer, Heidelberg, Aug. 2017.
https://hal.inria.fr/hal-01624662.

A. Guillevic, S. Masson, and E. Thomé.
Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation.
Des. Codes Cryptography, pages 1–35, March 2020.
https://hal.inria.fr/hal-02305051.

A. Guillevic, F. Morain, and E. Thomé.
Solving discrete logarithms on a 170-bit MNT curve by pairing reduction.
In R. Avanzi and H. M. Heys, editors, *SAC 2016*, volume 10532 of *LNCS*, pages 559–578. Springer, Heidelberg, Aug. 2016.

Bibliography V


A. Guillevic and S. Singh.
On the alpha value of polynomials in the tower number field sieve algorithm.
Cryptology ePrint Archive, Report 2019/885, 2019.
https://eprint.iacr.org/2019/885.


K. Hayasaka, K. Aoki, T. Kobayashi, and T. Takagi.
An experiment of number field sieve for discrete logarithm problem over GF(p^{12}).
In M. Fischlin and S. Katzenbeisser, editors, *Number Theory and Cryptography*, volume 8260 of *LNCS*, pages 108–120. Springer, 2013.


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


A. Joux and C. Pierrot.
The special number field sieve in $\mathbb{F}_{p^n}$ - application to pairing-friendly constructions.
In Z. Cao and F. Zhang, editors, *PAIRING 2013*, volume 8365 of *LNCS*, pages 45–61. Springer, Heidelberg, Nov. 2014.
https://ia.cr/2013/582.

Bibliography VI


T. Kim and R. Barbulescu.
Extended tower number field sieve: A new complexity for the medium prime case.
In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 543–571. Springer, Heidelberg, Aug. 2016.
https://ia.cr/2015/1027.


T. Kim and J. Jeong.
Extended tower number field sieve with application to finite fields of arbitrary composite extension degree.
In S. Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 388–408. Springer, Heidelberg, Mar. 2017.
https://ia.cr/2016/526.


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


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

Bibliography VII


A. Menezes, P. Sarkar, and S. Singh.
Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography.
In R. C. Phan and M. Yung, editors, *Mycrypt Conference*, volume 10311 of *LNCS*, pages 83–108, Kuala Lumpur, Malaysia, December 1-2 2016. Springer.
https://ia.cr/2016/1102.


P. Sarkar and S. Singh.
A general polynomial selection method and new asymptotic complexities for the tower number field sieve algorithm.
In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 37–62. Springer, Heidelberg, Dec. 2016.
https://eprint.iacr.org/2016/485.


P. Sarkar and S. Singh.
New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields.
In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 429–458. Springer, Heidelberg, May 2016.
https://eprint.iacr.org/2015/944.