Nov 12, 2024

Devcon, Bangkok

Elliptic curves and SNARKs: Past, present and future.

Youssef El Housni

Linea

Youssef El Housni

- Cryptographer at Consensys
- Co-maintainer of gnark
- Co-developer of Linea

Linea

I have 2 problems in my life

getting my wife to choose a restaurant

Ethereum supports only BN254 precompiles*

* for now

BN254 precompiles

E(Fp): $y^2=x^3+ax+b$ and r | #E

Operations on E(Fp)[r]:

- Addition:

  P + Q = R

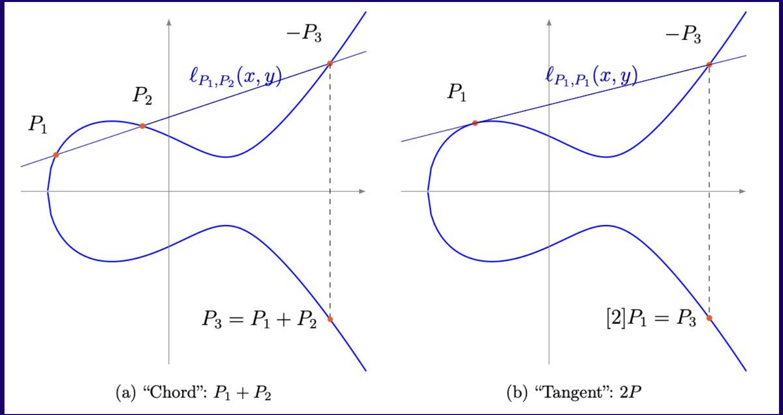
- Scalar multiplication:

  [n]P = P + P + … + P

  (n times)

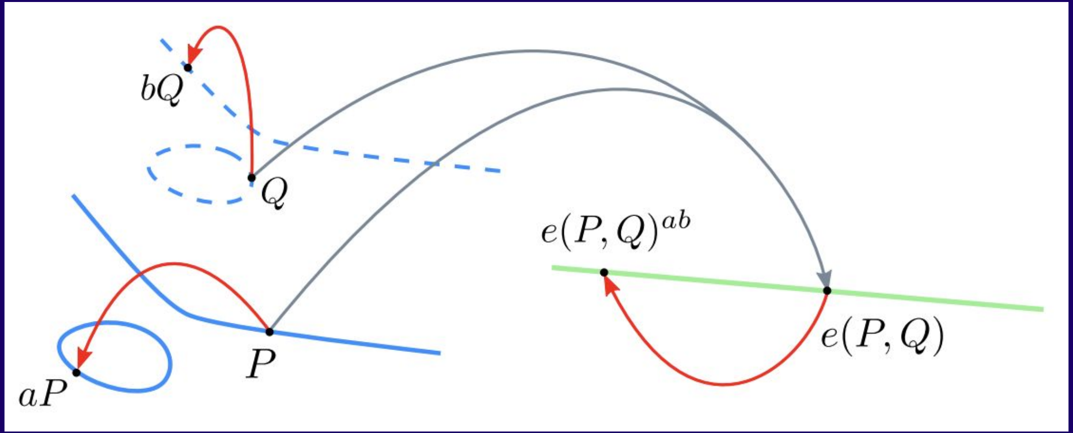
- Pairing product check:

  e(P1, Q1) * … * e(Pn, Qn) == 1



(a) "Chord": $P_1 + P_2$

(b) "Tangent": $2P$



Linea

BN254 precompiles

$E(F_p): y^2=x^3+ax+b$ and $r \mid \#E$

Operations on $E(F_p)[r]$:

- Addition:
  $P + Q = R$
- Scalar multiplication:
  $[n]P = P + P + \ldots + P$
  (n times)
- Pairing product check:
  $e(P1, Q1) * \ldots * e(Pn, Qn) == 1$

Useful for:

SNARK verification

BLS signature verification

Polynomial commitment verification (KZG)

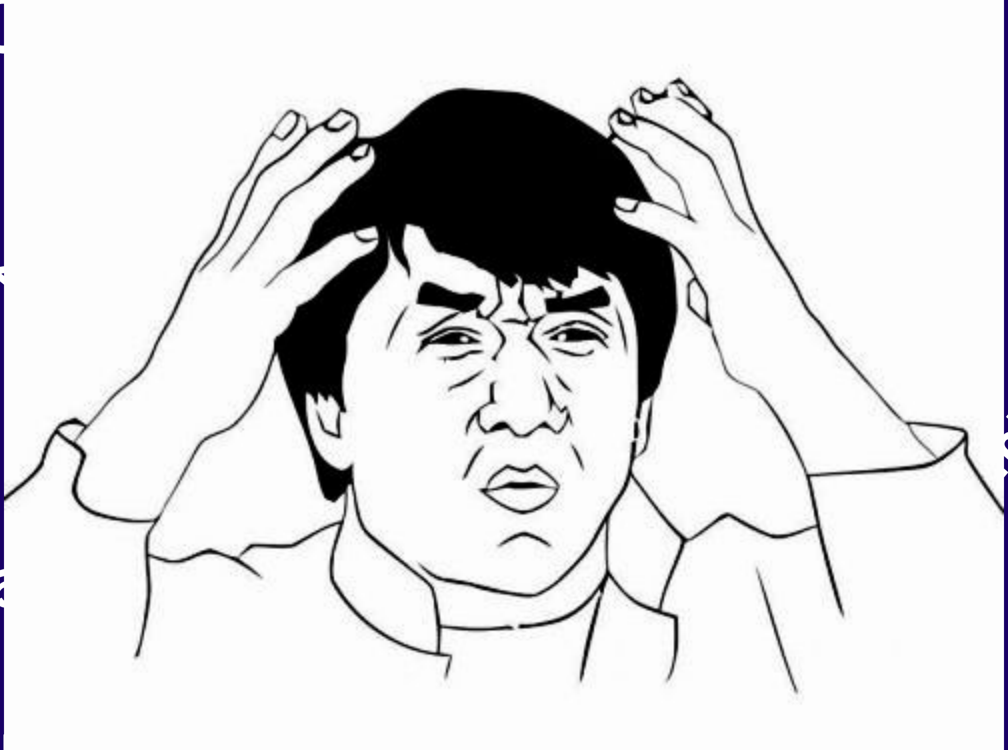
Verkle trie

…

Pluto-Eris

Lollipop-956-451

Many elliptic curves



BN254

secp

BLS12-381

mbedded cycles

MNT4/6 cycle

Ed25

Pasta cycle

Tweedle cycle

Definitions

Past: curves used in SNARKs but not anymore

Present: curves still being used in SNARKs

Future: Curves not used yet and curve likely to continue being used

Many elliptic curves

Pluto-Eris

Lollipop-956-451

Jubjub

Bandersnatch

NIST P-256

secp256k1

BN254

BLS12-381

secq256k1

2-chain

BLS12/BW6

Embedded cycles

MNT4/6 cycle

Ed25519

Grumpkin

Pasta cycle

Tweedle cycle

Many elliptic curves

Non-pairing-friendly curves	Pairing-friendly curves	In-circuit curves
● secp256k1 ● secq256k1 ● Ed25519 ● NIST P-256 ● Pasta cycle ● Tweedle cycle ● -Eris ● Grumpkin	● BN254 ● BLS12-381 ● BLS12-377 ● BW6-761 ● MNT4/6 cycle ● BLS24-317 ● Pluto- ● Lollipop-956-451 ● BLS12-380 + embedded cycle	● Jubjub ● Bandersnatch ● MNT4/6 cycle ● BW6-761 ● Lollipop-956-451 ● Grumpkin ● BLS12-380 + embedded cycle ● Ed25519 + embedded cycle

Non-pairing-friendly curves

SNARK: Bulletproofs, Halo, Nova …

- Ed25519 → Performance
- NIST P-256 → Standard
- secp256k1 → Standard (but not NIST)
- secq256k1 → Recursion + Compatibility w/ secp256k1
- Tweedle cycle → Recursion + Performance
- Pasta cycle → Recursion + More Performance
- Pluto-Eris → Hybrid Recursion
- Grumpkin → Hybrid Recursion + Compatibility w/ Ethereum (BN254)

Pairing–friendly curves

SNARK: Groth16, PlonK, …

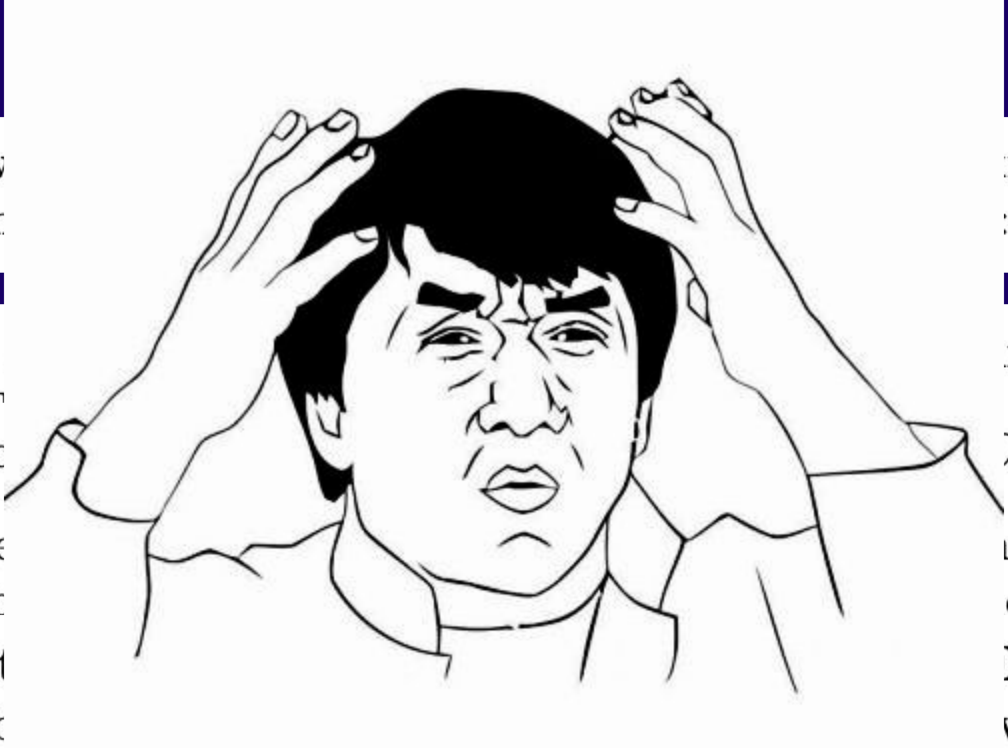
BN254	→	Ethereum (Less secure)
BLS12-381	→	Performance
BLS12-377/BW6-761	→	Performance + 1-Recursion
MNT4/6 cycle	→	∞-Recursion (Unsercure or Slow)
BLS24-317	→	Performance (KZG)
Pluto-Eris	→	Hybrid ∞-Recursion
Lollipop-956-451	→	∞-Recursion
BLS12-380 + embedded cycle	→	Hybrid ∞-Recursion

In-circuit curves

e.g. ECDSA/EdDSA, Bowe-Hopwood hash, Verkle trie, …

- Jubjub → ECC
- Bandersnatch → ECC
- MNT4/6 cycle → ∞-PBC (Unsercure or Slow)
- BW6-761 → 1-PBC
- Lollipop-956-451 → ∞-PBC + ~Succinctness
- Grumpkin → ∞-PBC + Compatibility with Ethereum (BN254)
- BLS12-380 + embedded cycle → ECC + Folding
- Ed25519 + embedded cycle → ECC + Folding + Compatibility with Ed25519

The story so far



[GMR89] Shafi Goldw nowledge com-
plexity of ir 186–208, 1989.

[Kil92] Joe Kilian. ments (extended

[Mic94] Silvio Mic CS, pages 436–453.

[GW11] Craig Ge -interactive argu-
ments fro d Salil P. Vadhan.

[BCCT12] Nir Bit ran Tromer. From
tractab ve arguments of kn
edge, and back again. In Shafi Goldwasser, editor, *ITCS 2012*, pages 326–
ACM, January 2012.

Pairing-based SNARK

[BGN05] Dan Boneh, NF formulas on
ciphertexts. f *LNCS*, pages
325–341. Sp

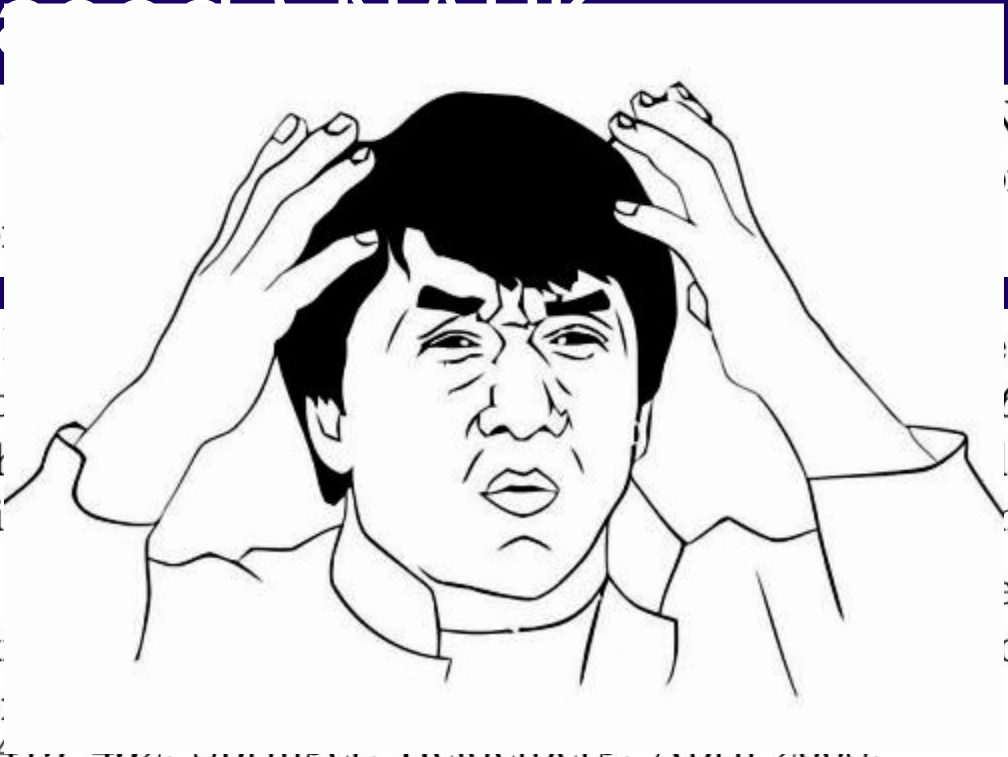
[GOS06] Jens Groth, zaps and new
techniques fo 6, volume 4117

[Gro06] Jens Groth language and
constant si n, editors, *ASI-*

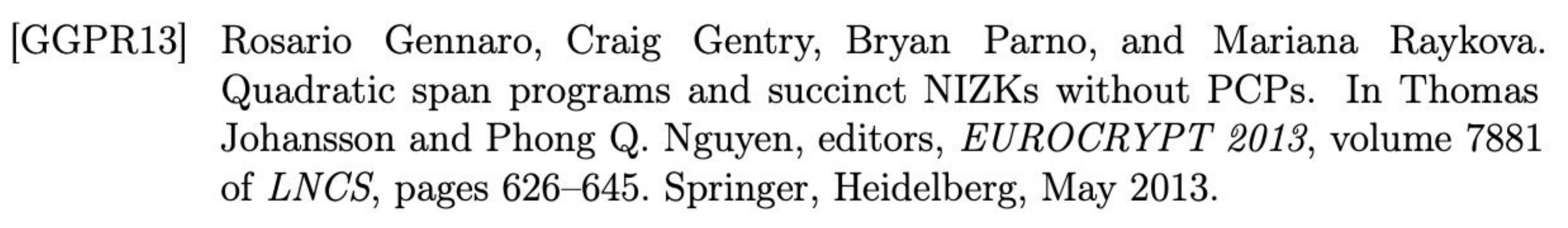
[Gro10] Jens Groth. edge arguments.
In Masayuk of *LNCS*, pages
321–340. Sp

pages 415–432. Springer, Heidelberg, April 2008.

in
N



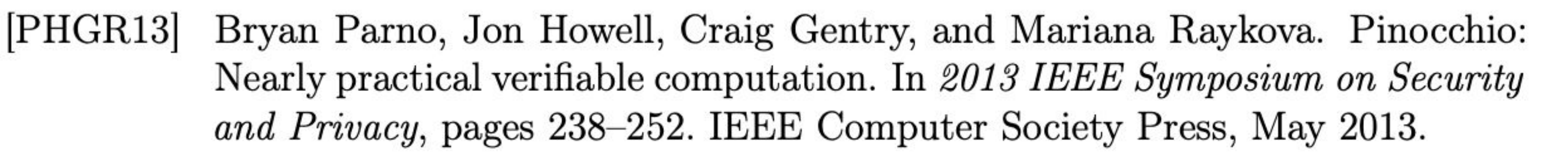
Pairing-friendly curves for SNARKs



[GGPR13] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct NIZKs without PCPs. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 626–645. Springer, Heidelberg, May 2013.

insightful construction of polynomial equations !

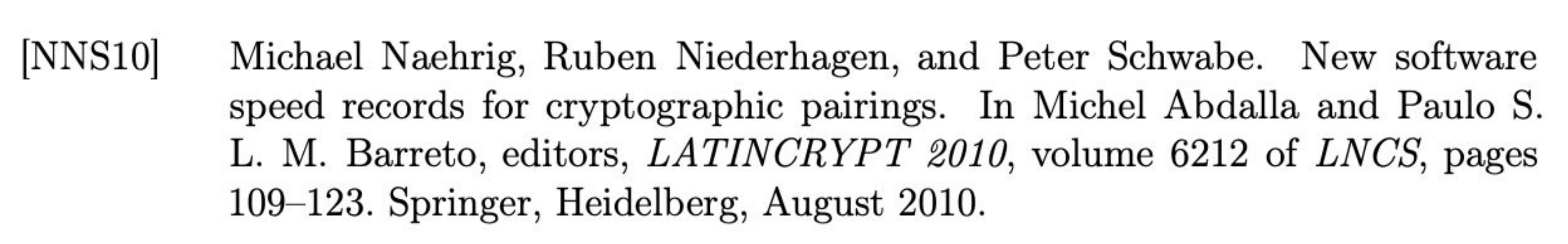
Pairing-friendly curves for SNARKs



[PHGR13] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. Pinocchio: Nearly practical verifiable computation. In *2013 IEEE Symposium on Security and Privacy*, pages 238–252. IEEE Computer Society Press, May 2013.

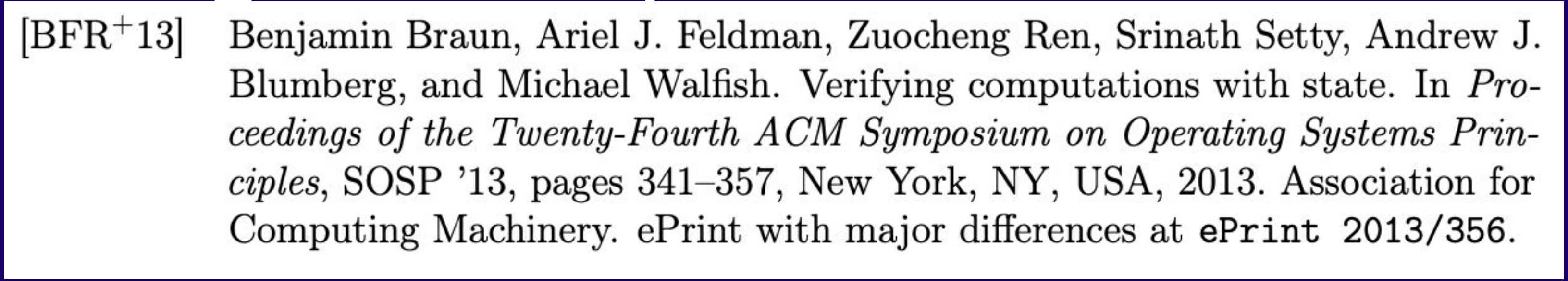
Pinocchio: BN256 curve from [NNS10] with seed 1868033^3 at **128-bit security** and **2-adicity 5**

(proprietary code)



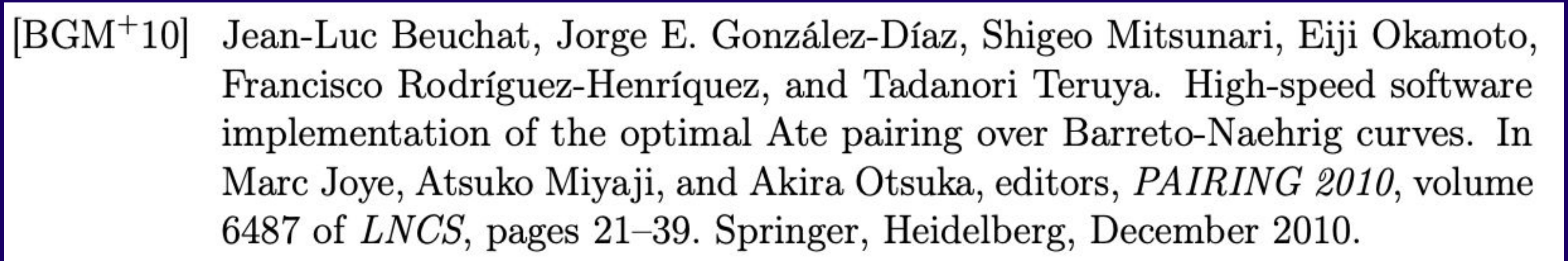
[NNS10] Michael Naehrig, Ruben Niederhagen, and Peter Schwabe. New software speed records for cryptographic pairings. In Michel Abdalla and Paulo S. L. M. Barreto, editors, *LATINCRYPT 2010*, volume 6212 of *LNCS*, pages 109–123. Springer, Heidelberg, August 2010.

Pairing–friendly curves for SNARKs



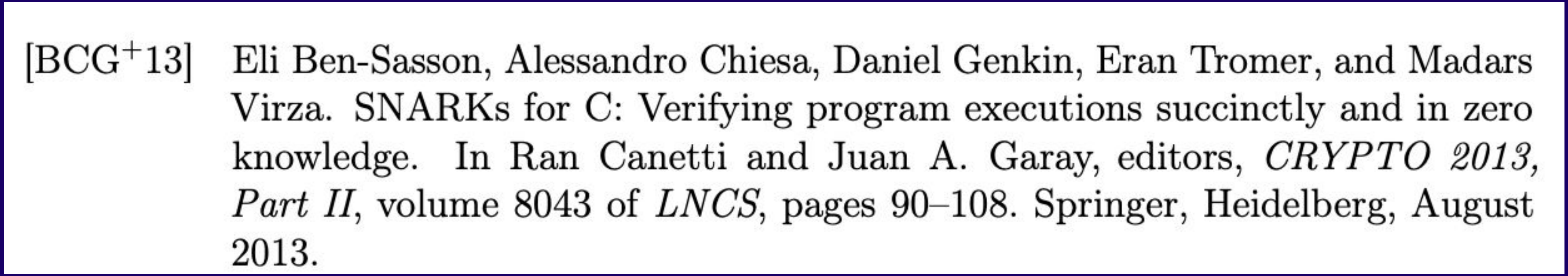
[BFR$^+$13] Benjamin Braun, Ariel J. Feldman, Zuocheng Ren, Srinath Setty, Andrew J. Blumberg, and Michael Walfish. Verifying computations with state. In *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles*, SOSP '13, pages 341–357, New York, NY, USA, 2013. Association for Computing Machinery. ePrint with major differences at ePrint 2013/356.

Pantry: BN254 curve from [BGM+10] with seed 2^62-2^54+2^44 at **128-bit security** and **2-adicity 45** (BSD-style license)



[BGM$^+$10] Jean-Luc Beuchat, Jorge E. González-Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez, and Tadanori Teruya. High-speed software implementation of the optimal Ate pairing over Barreto-Naehrig curves. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *PAIRING 2010*, volume 6487 of *LNCS*, pages 21–39. Springer, Heidelberg, December 2010.

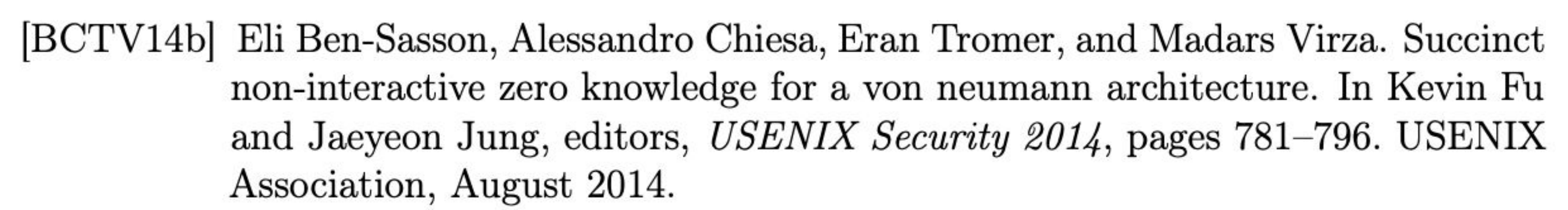
Pairing-friendly curves for SNARKs



[BCG$^+$13] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. SNARKs for C: Verifying program executions succinctly and in zero knowledge. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 90–108. Springer, Heidelberg, August 2013.

Galbraith-McKee-Valença (GMV6-183) curve of twisted Edwards form at **80-bit security** and **2-adicity 31**

Pairing-friendly curves for SNARKs

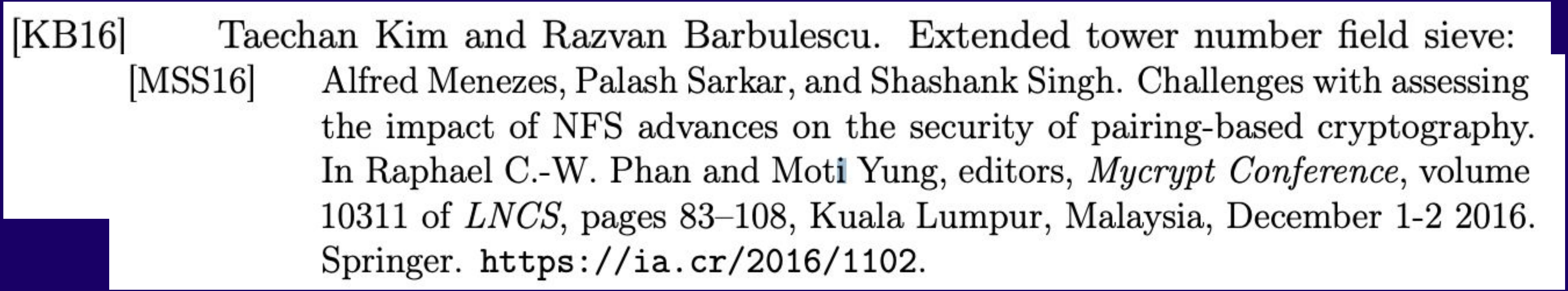


[BCTV14b] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct non-interactive zero knowledge for a von neumann architecture. In Kevin Fu and Jaeyeon Jung, editors, *USENIX Security 2014*, pages 781–796. USENIX Association, August 2014.

BN254 (**Ethereum**) of seed 0x44e992b44a6909f1 at **128-bit security (now 103)** and **2-adicity 28**

(But why not BN254 [BGM+10] with 45 2-adicity?)

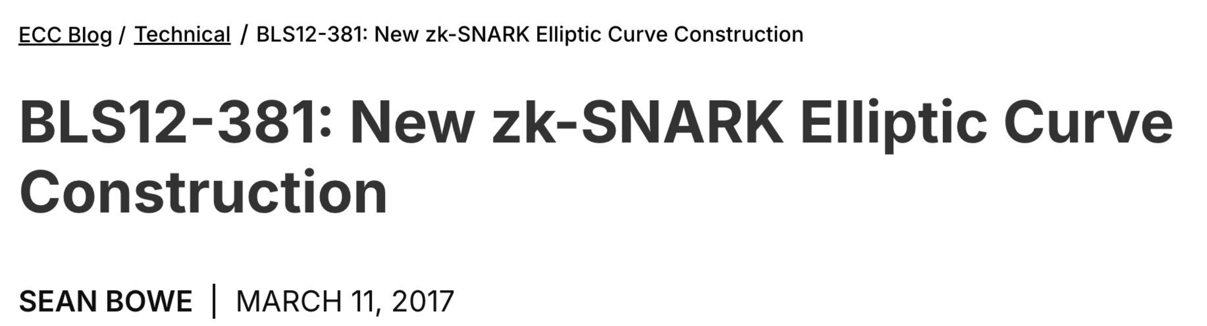
Pairing–friendly curves for SNARKs



[KB16] Taechan Kim and Razvan Barbulescu. Extended tower number field sieve:

[MSS16] 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. `https://ia.cr/2016/1102`.

BLS12 of seed -0xd201000000010000 at **128-bit security** and **2-adicity 32**



ECC Blog / Technical / BLS12-381: New zk-SNARK Elliptic Curve Construction

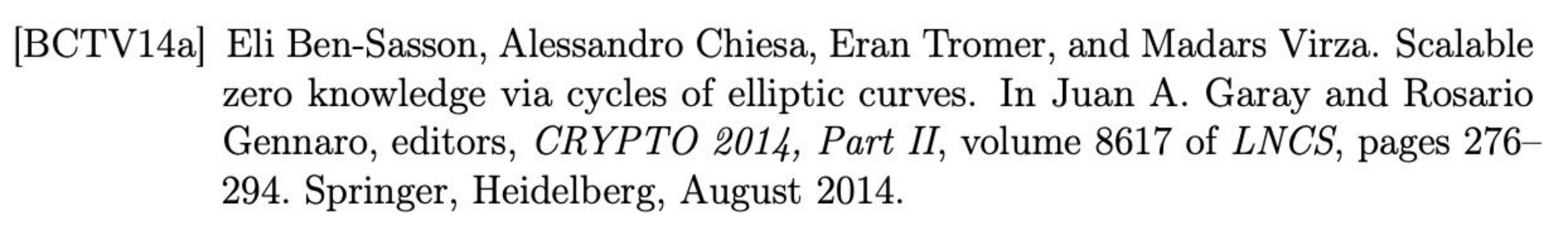
BLS12-381: New zk-SNARK Elliptic Curve Construction

SEAN BOWE | MARCH 11, 2017

Pairing-friendly curves for recursive SNARKs (2-cycle)

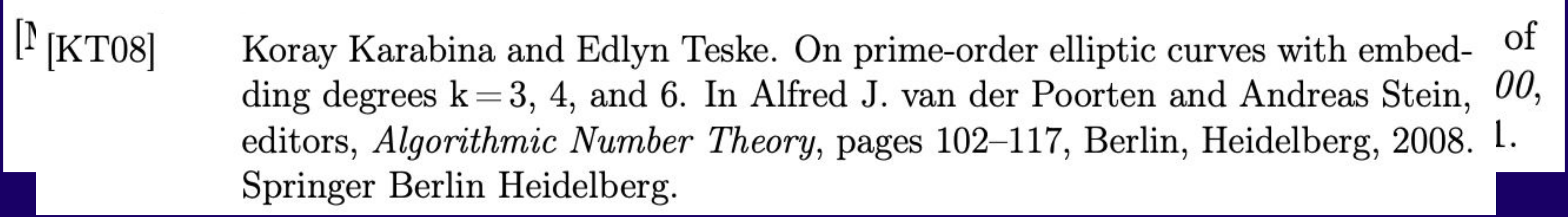
$$\begin{tikzcd}
\boxed{E'(\mathbb{F}_q)} \arrow[d, bend left=60, "\#E(\mathbb{F}_p) = q"] \\
\boxed{E(\mathbb{F}_p)} \arrow[u, bend left=60, "\#E'(\mathbb{F}_q) = p"]
\end{tikzcd}$$

Pairing–friendly curves for recursive SNARKs



[BCTV14a] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Scalable zero knowledge via cycles of elliptic curves. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 276–294. Springer, Heidelberg, August 2014.

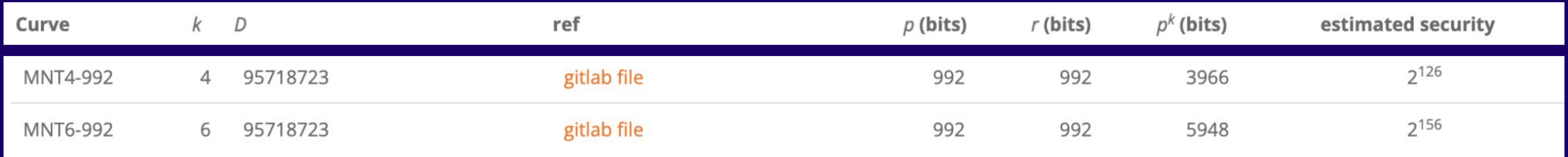
MNT4-298 and MNT6-298 at **80-bit security** of **2-adicity 17**
MNT4-753 and MNT6-753 at **113-bit security** of **2-adicity 30 and 15** *(preprint update 2020)*



[KT08] Koray Karabina and Edlyn Teske. On prime-order elliptic curves with embedding degrees k = 3, 4, and 6. In Alfred J. van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory*, pages 102–117, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

Pairing-friendly curves for recursive SNARKs

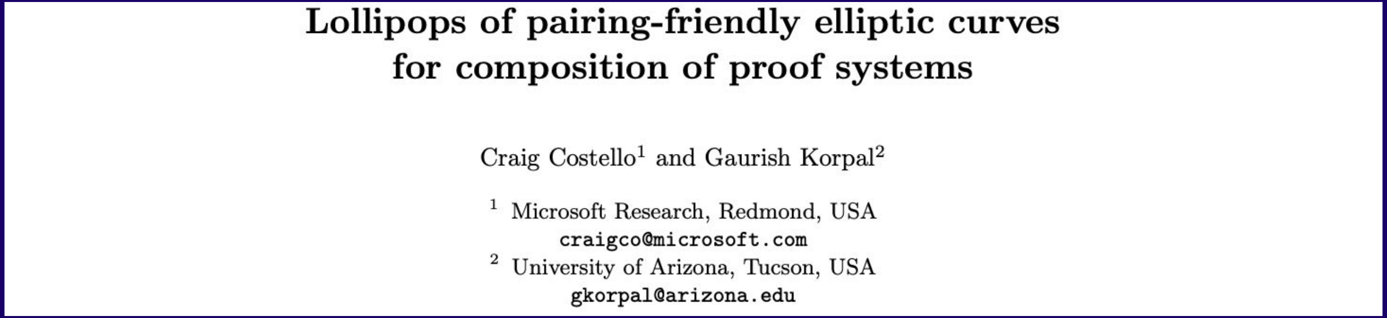
https://members.loria.fr/AGuillevic/pairing-friendly-cuxrves/



Curve	k	D	ref	p (bits)	r (bits)	p^k (bits)	estimated security
MNT4-992	4	95718723	gitlab file	992	992	3966	2^{126}
MNT6-992	6	95718723	gitlab file	992	992	5948	2^{156}

MNT4-992 and MNT6-992 at **128-bit security** of **2-adicity 2**

Pairing–friendly curves for recursive SNARKs



Lollipops of pairing-friendly elliptic curves for composition of proof systems

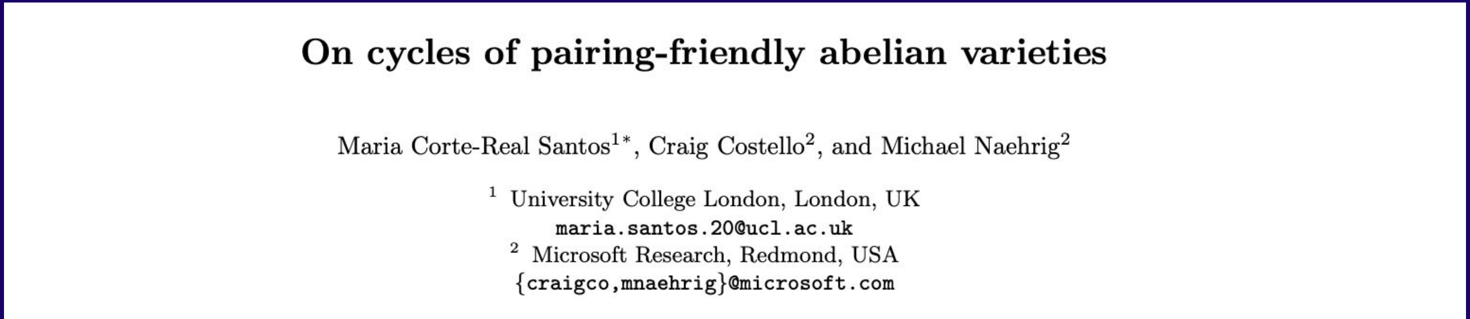
Craig Costello[1] and Gaurish Korpal[2]

[1] Microsoft Research, Redmond, USA
craigco@microsoft.com
[2] University of Arizona, Tucson, USA
gkorpal@arizona.edu

Supersingular MNT-like curves over extensions (2024)

- **High 2-adicity at any security level** but **slow**

Pairing–friendly curves for recursive SNARKs



On cycles of pairing-friendly abelian varieties

Maria Corte-Real Santos[1*], Craig Costello[2], and Michael Naehrig[2]

[1] University College London, London, UK
maria.santos.20@ucl.ac.uk
[2] Microsoft Research, Redmond, USA
{craigco,mnaehrig}@microsoft.com

Pairing-friendly cycles with:

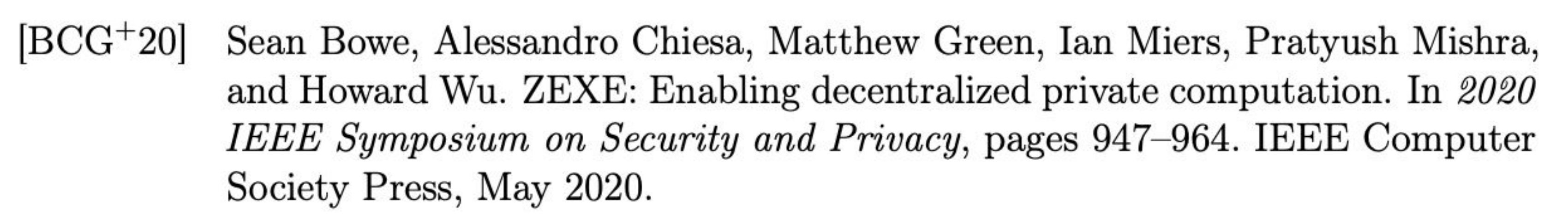
- Ordinary elliptic curves
- Supersingular elliptic curves
- Higher genus curves

but as **slow** as MNT and **early research**

Pairing-friendly curves for recursive SNARKs (2-chain)

$$\begin{tikzcd}
\boxed{E'(\mathbb{F}_q)} \\
\boxed{E(\mathbb{F}_p)} \arrow[u, "\#E'(\mathbb{F}_q) = h \cdot p"']
\end{tikzcd}$$

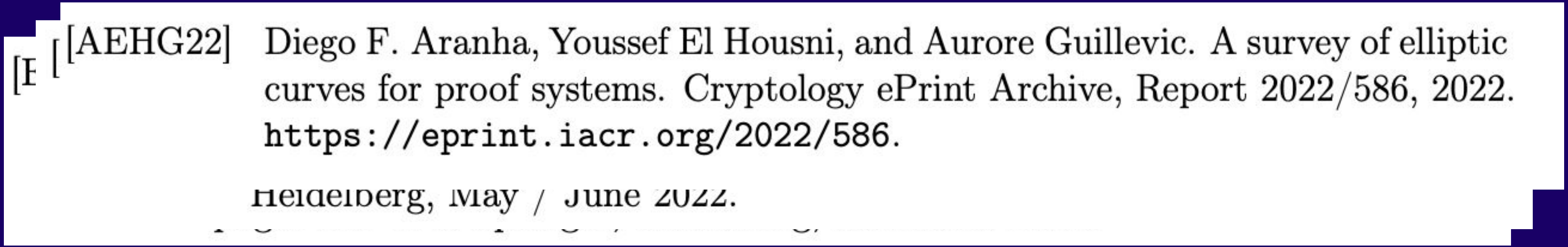
Pairing-friendly curves for recursive SNARKs



[BCG+20] Sean Bowe, Alessandro Chiesa, Matthew Green, Ian Miers, Pratyush Mishra, and Howard Wu. ZEXE: Enabling decentralized private computation. In *2020 IEEE Symposium on Security and Privacy*, pages 947–964. IEEE Computer Society Press, May 2020.

ZEXE:
BLS12-377 at **128-bit security** and **high 2-adicity**
and a CP6-782 curve with **high 2-adicity**

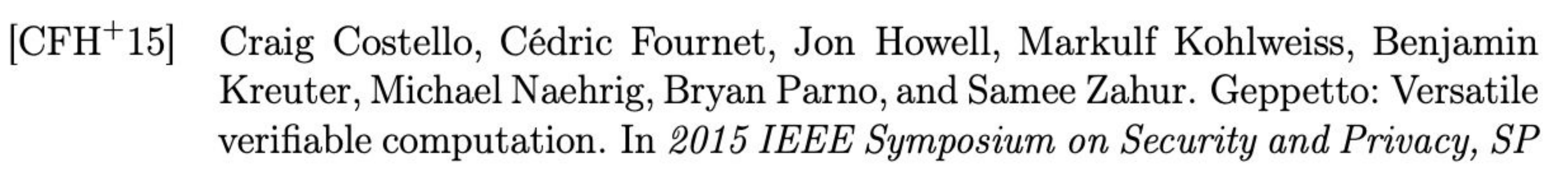
BW6-761 curve with **high 2-adicity + performance**



[E [[AEHG22] Diego F. Aranha, Youssef El Housni, and Aurore Guillevic. A survey of elliptic curves for proof systems. Cryptology ePrint Archive, Report 2022/586, 2022. https://eprint.iacr.org/2022/586.

Heidelberg, May / June 2022.

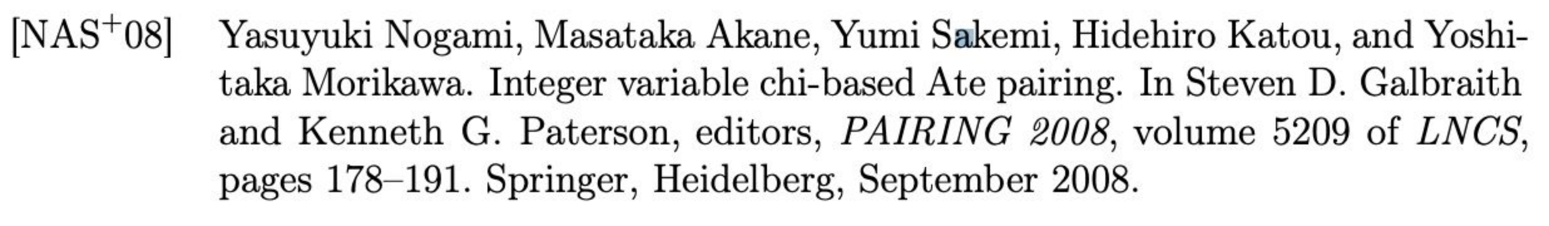
Pairing–friendly curves for recursive SNARKs



[CFH^{+}15] Craig Costello, Cédric Fournet, Jon Howell, Markulf Kohlweiss, Benjamin Kreuter, Michael Naehrig, Bryan Parno, and Samee Zahur. Geppetto: Versatile verifiable computation. In *2015 IEEE Symposium on Security and Privacy, SP*

Gepetto:

BN254 curve from [NAS+08] with seed -2^62-2^55-1 at **128-bit security** and **low 2-adicity** and a BW6-509 curve with **low 2-adicity**

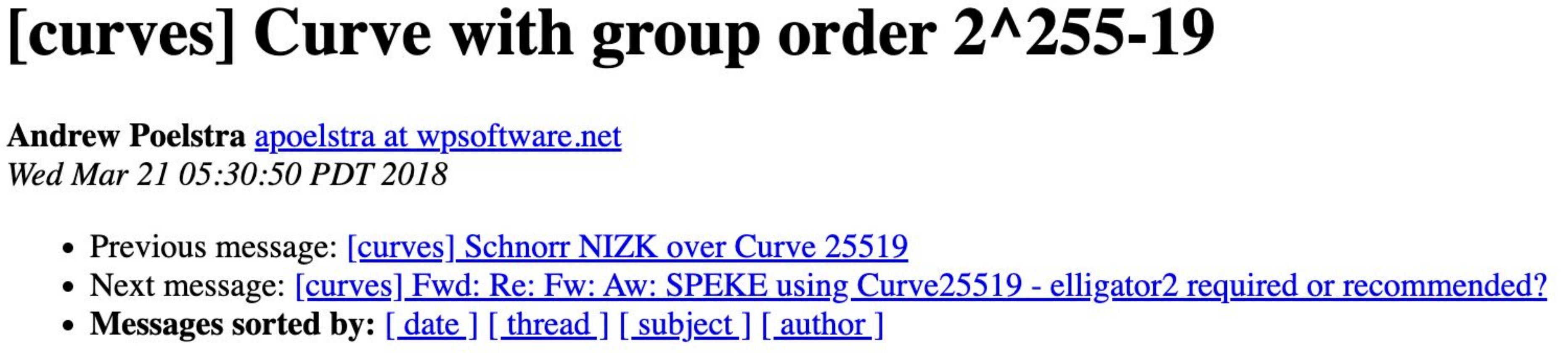


[NAS^{+}08] Yasuyuki Nogami, Masataka Akane, Yumi Sakemi, Hidehiro Katou, and Yoshitaka Morikawa. Integer variable chi-based Ate pairing. In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 178–191. Springer, Heidelberg, September 2008.

Plain curves for recursive SNARKs (2-cycle)

$$\begin{tikzcd}
\boxed{E'(\mathbb{F}_q)} \arrow[d, bend left, "\#E(\mathbb{F}_p) = q"] \\
\boxed{E(\mathbb{F}_p)} \arrow[u, bend left, "\#E'(\mathbb{F}_q) = p"]
\end{tikzcd}$$

Plain curves for recursive SNARKs (2-cycle)

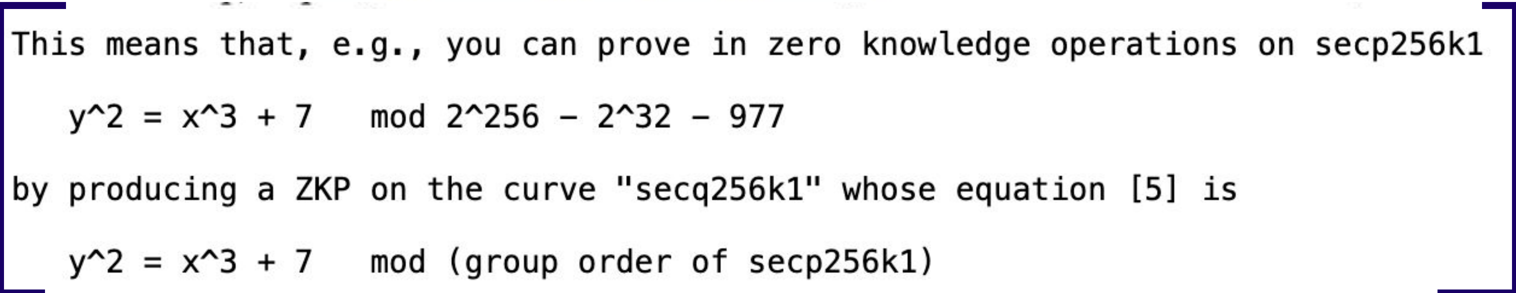


[curves] Curve with group order 2^255-19

Andrew Poelstra apoelstra at wpsoftware.net

Wed Mar 21 05:30:50 PDT 2018

- Previous message: [curves] Schnorr NIZK over Curve 25519
- Next message: [curves] Fwd: Re: Fw: Aw: SPEKE using Curve25519 - elligator2 required or recommended?
- **Messages sorted by:** [date] [thread] [subject] [author]



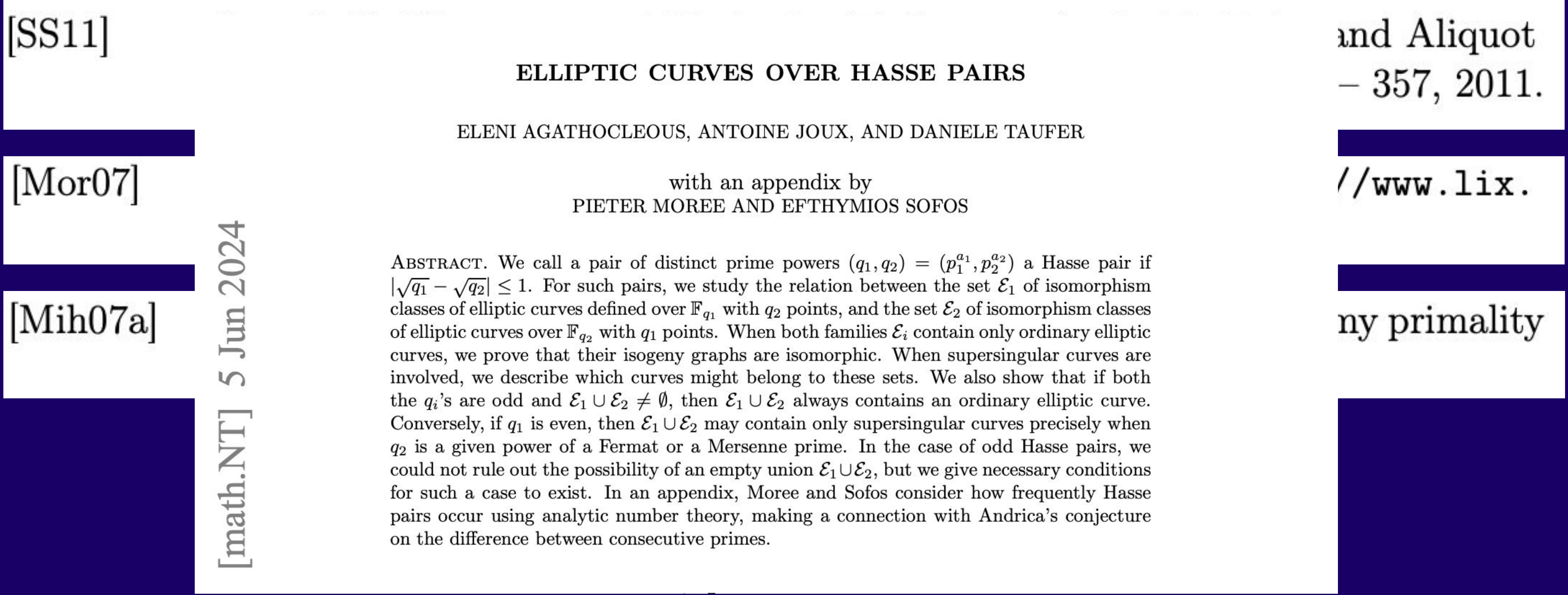
```
This means that, e.g., you can prove in zero knowledge operations on secp256k1

   y^2 = x^3 + 7   mod 2^256 - 2^32 - 977

by producing a ZKP on the curve "secq256k1" whose equation [5] is

   y^2 = x^3 + 7   mod (group order of secp256k1)
```

Plain curves for recursive SNARKs (2-cycle)



[SS11] ınd Aliquot

– 357, 2011.

[Mor07] //www.lix.

[Mih07a] ny primality

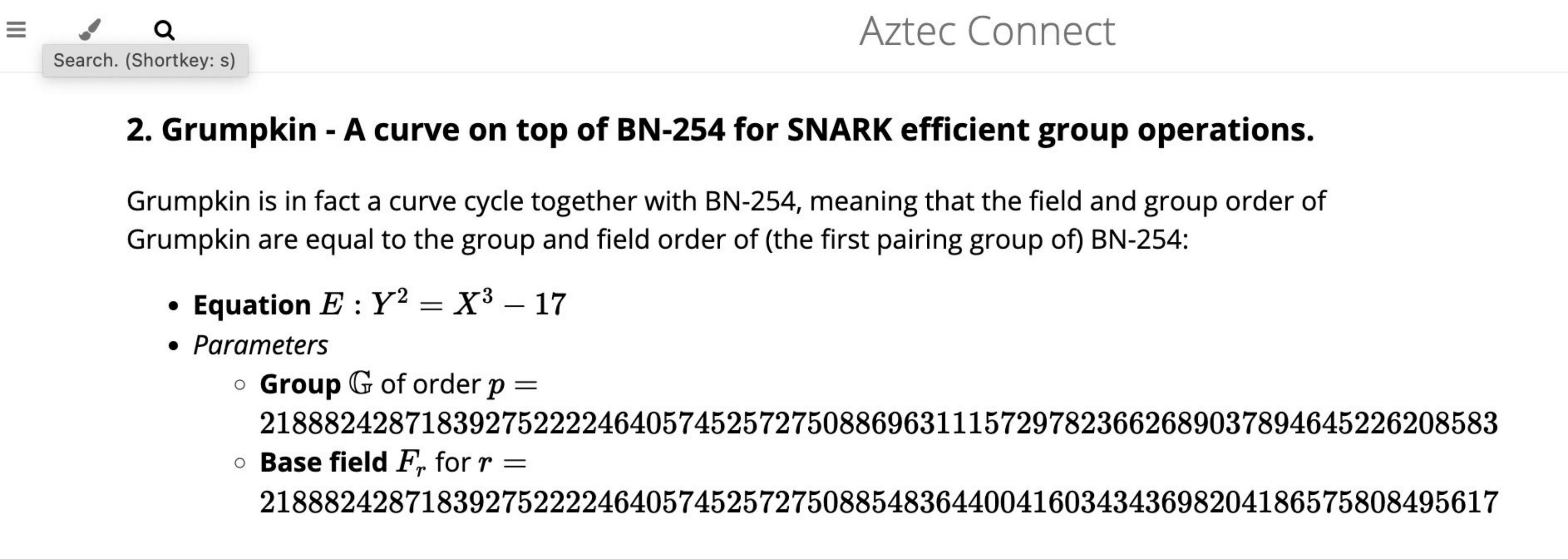
ELLIPTIC CURVES OVER HASSE PAIRS

ELENI AGATHOCLEOUS, ANTOINE JOUX, AND DANIELE TAUFER

with an appendix by
PIETER MOREE AND EFTHYMIOS SOFOS

Abstract. We call a pair of distinct prime powers $(q_1, q_2) = (p_1^{a_1}, p_2^{a_2})$ a Hasse pair if $|\sqrt{q_1} - \sqrt{q_2}| \leq 1$. For such pairs, we study the relation between the set $\mathcal{E}_1$ of isomorphism classes of elliptic curves defined over $\mathbb{F}_{q_1}$ with q_2 points, and the set $\mathcal{E}_2$ of isomorphism classes of elliptic curves over $\mathbb{F}_{q_2}$ with q_1 points. When both families $\mathcal{E}_i$ contain only ordinary elliptic curves, we prove that their isogeny graphs are isomorphic. When supersingular curves are involved, we describe which curves might belong to these sets. We also show that if both the q_i's are odd and $\mathcal{E}_1 \cup \mathcal{E}_2 \neq \emptyset$, then $\mathcal{E}_1 \cup \mathcal{E}_2$ always contains an ordinary elliptic curve. Conversely, if q_1 is even, then $\mathcal{E}_1 \cup \mathcal{E}_2$ may contain only supersingular curves precisely when q_2 is a given power of a Fermat or a Mersenne prime. In the case of odd Hasse pairs, we could not rule out the possibility of an empty union $\mathcal{E}_1 \cup \mathcal{E}_2$, but we give necessary conditions for such a case to exist. In an appendix, Moree and Sofos consider how frequently Hasse pairs occur using analytic number theory, making a connection with Andrica's conjecture on the difference between consecutive primes.

Hybrid curves for recursive SNARKs (2-cycle)



2. Grumpkin - A curve on top of BN-254 for SNARK efficient group operations.

Grumpkin is in fact a curve cycle together with BN-254, meaning that the field and group order of Grumpkin are equal to the group and field order of (the first pairing group of) BN-254:

- **Equation** $E: Y^2 = X^3 - 17$
- *Parameters*
  - **Group** $\mathbb{G}$ of order $p = 21888242871839275222246405745257275088696311157297823662689037894645226208583$
  - **Base field** F_r for $r = 21888242871839275222246405745257275088548364400416034343698204186575808495617$

Lollipops for recursive SNARKs

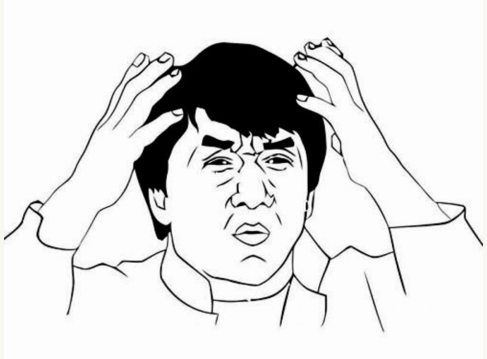
Lollipops of pairing-friendly elliptic curves for composition of proof systems

Craig Costello[1] and Gaurish Korpal[2]

[1] Microsoft Research, Redmond, USA
craigco@microsoft.com
[2] University of Arizona, Tucson, USA
gkorpal@arizona.edu

Linea

Thank you



linea.build
gnark.io

youssef.elhousni@consensys.net
gnark@consensys.net

X: @YoussefElHousn3
TG: @ElMarroqui
GH: @yelhousni