On cycles of pairing-friendly abelian varieties

Maria Corte-Real Santos, Craig Costello, and Michael Naehrig

UCL

Microsoft Research

CRYPTO 2024

Cycles of elliptic curves

$$\#E(\mathbb{F}_p) = q \quad \rightleftharpoons \quad \#E'(\mathbb{F}_q) = p$$

Cycles of pairing-friendly elliptic curves

$\mathbb{F}_{q^n}^{\times}$

$\mathbb{F}_{p^m}^{\times}$

$$\#E(\mathbb{F}_p) = q \quad \rightleftharpoons \quad \#E'(\mathbb{F}_q) = p$$

[BSCT14] Ben-Sasson-Chiesa-Tromer-Virza. *Scalable zero-knowledge via cycles of elliptic curves*. Crypto 2014.

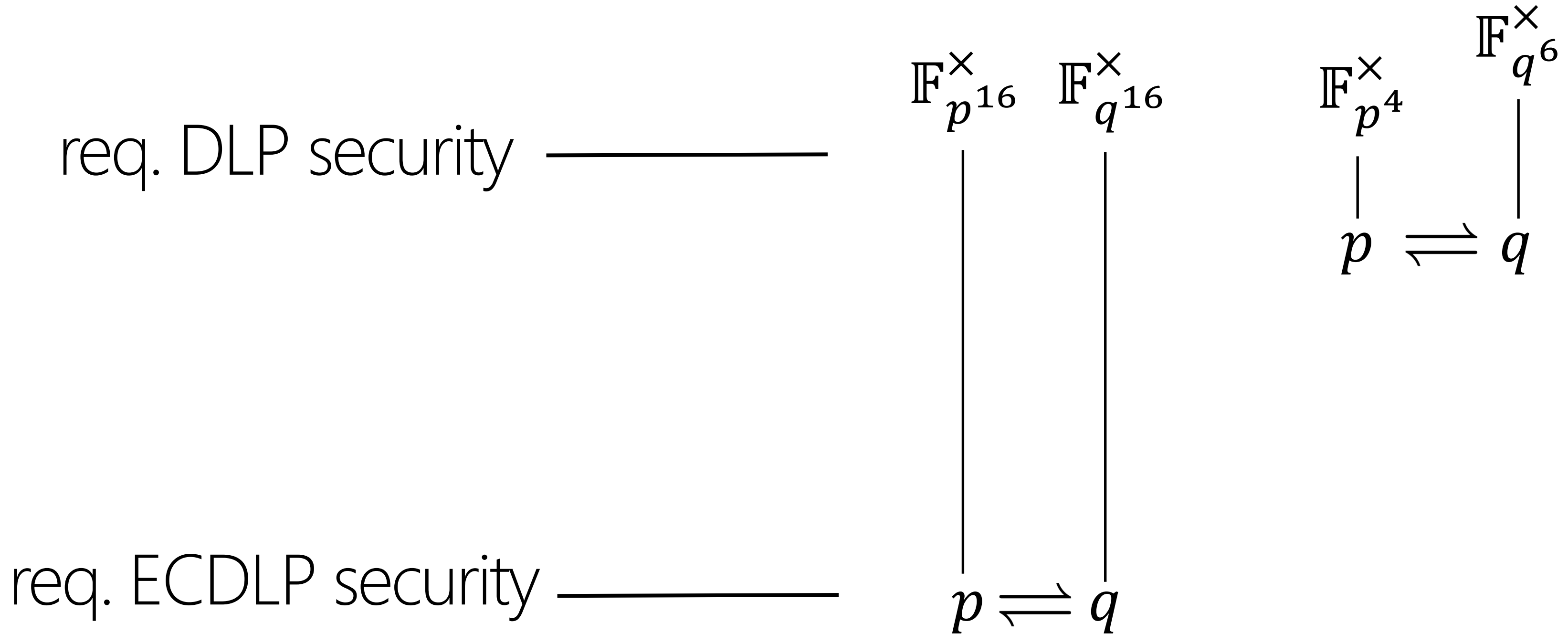
The MNT cycle: $(m, n) = (4, 6)$

$\mathbb{F}_{q^6}^{\times}$

$\mathbb{F}_{p^4}^{\times}$

$\#E(\mathbb{F}_p) = q \quad \rightleftharpoons \quad \#E'(\mathbb{F}_q) = p$

Dream cycles vs. MNT reality



security level	80	112	**128**	192	256
requisite ext. field size	1184	3012	3968	9240	18480
Dream cycles $\boldsymbol{p \approx q}$	160	224	256	384	512
MNT reality $\boldsymbol{p \approx q}$	296	753	992	2310	4620

numbers in table are base-2 log

Pairing-friendly elliptic curve cycles are elusive

- MNT cycles known prior to pairing-based proof popularity [KT08]
- Since then, no new 2-cycle constructions have been found
- Several negative/impossibility results, e.g. [CCW19] & [BJS23]
- [CCW19] explored $q \mid \#E(\mathbb{F}_p) \rightleftharpoons p \mid \#E'(\mathbb{F}_q)$

... but Hasse interval shackles this!

[KT08] Karabina-Teske. *On prime order elliptic curves of embedding degrees k=3, 4 and 6*. ANTS 2008.
[CCW19] Chiesa-Chua-Weidner. *On Cycles of Pairing-Friendly Elliptic Curves*. SIAM J. Appl. Alg. Geom. 2019.
[BJS23] Bellés-Muñoz-Jiménez Urroz-Silva. *Revisiting Cycles of Pairing-Friendly Elliptic Curves*. Crypto 2023.

This work

$$A \rightleftharpoons B$$

Relaxation 1: A and B can be abelian varieties of any dimension

Relaxation 2: $A/\mathbb{F}_{p^u}$ and $B/\mathbb{F}_{q^v}$ defined over ext. field

Relaxation 3: $q \mid \#A(\mathbb{F}_{p^u})$ and $p \mid \#B(\mathbb{F}_{q^v})$ à la [CCW19]

The downsides

$A/\mathbb{F}_{p^u} \rightleftharpoons B/\mathbb{F}_{q^v}$

- Higher-dimensional varieties were/are practically interesting because of the following trade-off: $\#A(\mathbb{F}_p) \approx p^{\mathbf{dim}(A)}$

- But cycles prohibit exploiting this: we can't shrink $\boldsymbol{p}$

- Arithmetic slows drastically as $\mathbf{dim}(A)$ grows

- We cheat with $\boldsymbol{q} = \chi(1)$, with χ char. poly. of $\boldsymbol{p^u}$ - Frobenius on $\boldsymbol{A}$. This forces $\boldsymbol{q} \equiv \mathbf{1} \bmod \boldsymbol{p}$ so B has embedding degree 1

- Can get $\boldsymbol{q}$ twice as large as optimal by boosting the size of $\boldsymbol{v}$, but we could only manage to do this when A has embedding degree $\mathbf{3/2}$

The upsides

$A/\mathbb{F}_{p^u} \rightleftharpoons B/\mathbb{F}_{q^v}$

- Ordinary higher-dimensional pairing-friendly difficult to find, but supersingular easier
- [RS01] give a theorem that allow us to construct supersingular

  $A/\mathbb{F}_{p^u}$ with $\mathbf{dim}(A) = 2^\ell$ and $k = 3 \cdot 2^{\mathrm{dim}(A)-1}$

  identified with trace-zero subgroup of supersingular $E(\mathbb{F}_{p^{2^{\ell+1}\cdot u}})$

- Allows us to get arbitrarily large embedding degree on A; optimal p at any security level
- Construction with p optimal may already be interesting in practice, despite suboptimal $B/\mathbb{F}_{q^v}$

[RS02] Rubin-Silverberg. *Supersingular abelian varieties in cryptography*. CRYPTO 2002.

Questions?

MNT cycle for 128-bit security

p=2564174452218021398507404238251241903258220596409224110423319250106996162690899080468904606298580736776315738820814814278302421133709760747532872876450105952199167994070713491138845449056672200641413433890523759234530066805589807803413266979230902939644302276810096847926508750672520229521632996 2501

q=2564174452218021398507404238251241903258220596409224110423319250106996162690899080468904606298580736776315738820814814278302421133709760747532872876450105952199167994070713491138845449056672200641413433890523759234530066805589807803413266979230902939644302276810096847926508750672520229521632996 2501

$A \rightleftharpoons B$ cycle for 128-bit security

p=115792089237316195423570985008687907853269984665640564039457584007913129633397

$A/\mathbb{F}_{p^2}$ is dimension 4

A has embedding degree 24

q=32317006071311007300714876688669951960444102669715484032130345427524655124267867413720987896876893745686897867069088345691940424302847177637280514465782842327577106464622763061448933322307840184531707045266747760809697747397050381802487119142571586876333102266193111803710989608077767985836336235810117563858143986657795919760172542581506455227183414033575326107046649261051949643037502674639404374312759780842461711599819906372297719593696908291522507051708442221233386826257201030504712294016477126070654232834314348192007782944540304029207265884687704231872519701731455329808130376653722879318888477919293560927281