On cycles of pairing-friendly abelian varieties

Based on joint work with Craig Costello and Michael Naehrig

Maria Corte-Real Santos
ENS Lyon and CNRS

Motivation

Pairing-based proof systems

- Our motivation comes from *non-interactive zero-knowledge proofs*.

Pairing-based proof systems

- Our motivation comes from *non-interactive zero-knowledge proofs*.
- In 2014, Ben-Sasson, Chiesa, Tromer and Virza realised efficient pairing-based zk-SNARKs with *recursive composition* of proofs.

Pairing-based proof systems

- Our motivation comes from *non-interactive zero-knowledge proofs*.
- In 2014, Ben-Sasson, Chiesa, Tromer and Virza realised efficient pairing-based zk-SNARKs with *recursive composition* of proofs.
- The core ingredient are *cycles of pairing-friendly elliptic curves*.

$$
\begin{tikzcd}
\mathbb{F}_{p^k}^{\times} & \mathbb{F}_{p^{k'}}^{\times} \\
E/\mathbb{F}_p \arrow[u] \arrow[r, bend left] & E'/\mathbb{F}_q \arrow[u] \arrow[l, bend left]
\end{tikzcd}
$$

Pairing-friendly cycles of elliptic curves

Definition [Ben-Sasson, Chiesa, Tromer, Virza '14]

A *(2-)cycle of pairing-friendly elliptic curves* is a pair of elliptic curves

$$E/\mathbb{F}_p \quad \text{and} \quad E'/\mathbb{F}_q$$

such that

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

and E, E' are pairing-friendly.

Pairing-friendly cycles of elliptic curves

Definition [Ben-Sasson, Chiesa, Tromer, Virza '14]

A *(2-)cycle of pairing-friendly elliptic curves* is a pair of elliptic curves

$$E/\mathbb{F}_p \quad \text{and} \quad E'/\mathbb{F}_q$$

such that

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

and E, E' are pairing-friendly.

$$\begin{tikzcd} E/\mathbb{F}_p \arrow[r, bend left] & E'/\mathbb{F}_q \arrow[l, bend left] \end{tikzcd}$$

Main example of a cycle

Example: 2-cycle of Miyaji, Nakabayashi and Takano (MNT) curves

$$(k, k') = (4,6)$$

$$\begin{tikzcd}
\mathbb{F}_{p^4}^{\times} & \mathbb{F}_{q^6}^{\times} \\
\#E(\mathbb{F}_p) = q \arrow[u] \arrow[r, bend left] & \#E'(\mathbb{F}_q) = p \arrow[u] \arrow[l, bend left]
\end{tikzcd}$$

Search for new cycles

- MNT cycles known prior to pairing-based proof popularity [Karabina, Teske ’08]

Search for new cycles

- MNT cycles known prior to pairing-based proof popularity [Karabina, Teske '08]
- Since then, no new 2-cycle constructions have been found

Search for new cycles

- MNT cycles known prior to pairing-based proof popularity [Karabina, Teske '08]
- Since then, no new 2-cycle constructions have been found
- Several negative/impossibility results

Search for new cycles

- MNT cycles known prior to pairing-based proof popularity [Karabina, Teske ’08]
- Since then, no new 2-cycle constructions have been found
- Several negative/impossibility results
    - Chiesa, Chia, Weidner ’19

Search for new cycles

- MNT cycles known prior to pairing-based proof popularity [Karabina, Teske '08]
- Since then, no new 2-cycle constructions have been found
- Several negative/impossibility results
    - Chiesa, Chia, Weidner '19
    - Bellés-Muñoz, Jiménez Urroz, Silva '23

Search for new cycles

- MNT cycles known prior to pairing-based proof popularity [Karabina, Teske '08]
- Since then, no new 2-cycle constructions have been found
- Several negative/impossibility results
    - Chiesa, Chia, Weidner '19
    - Bellés-Muñoz, Jiménez Urroz, Silva '23
- Chiesa, Chia, Weidner explored

$$q \mid \#E(\mathbb{F}_p) \qquad p \mid \#E'(\mathbb{F}_q)$$

... but Hasse interval shackles this!

Search for new cycles

- MNT cycles known prior to pairing-based proof popularity [Karabina, Teske '08]
- Since then, no new 2-cycle constructions have been found
- Several negative/impossibility results
    - Chiesa, Chia, Weidner '19
    - Bellés-Muñoz, Jiménez Urroz, Silva '23
- Chiesa, Chia, Weidner explored $q \mid \#E(\mathbb{F}_p) \quad p \mid \#E'(\mathbb{F}_q)$

... but Hasse interval shackles this!

To overcome these impossibility results, previous works relax *pairing-friendly* or look at *2-chains*.

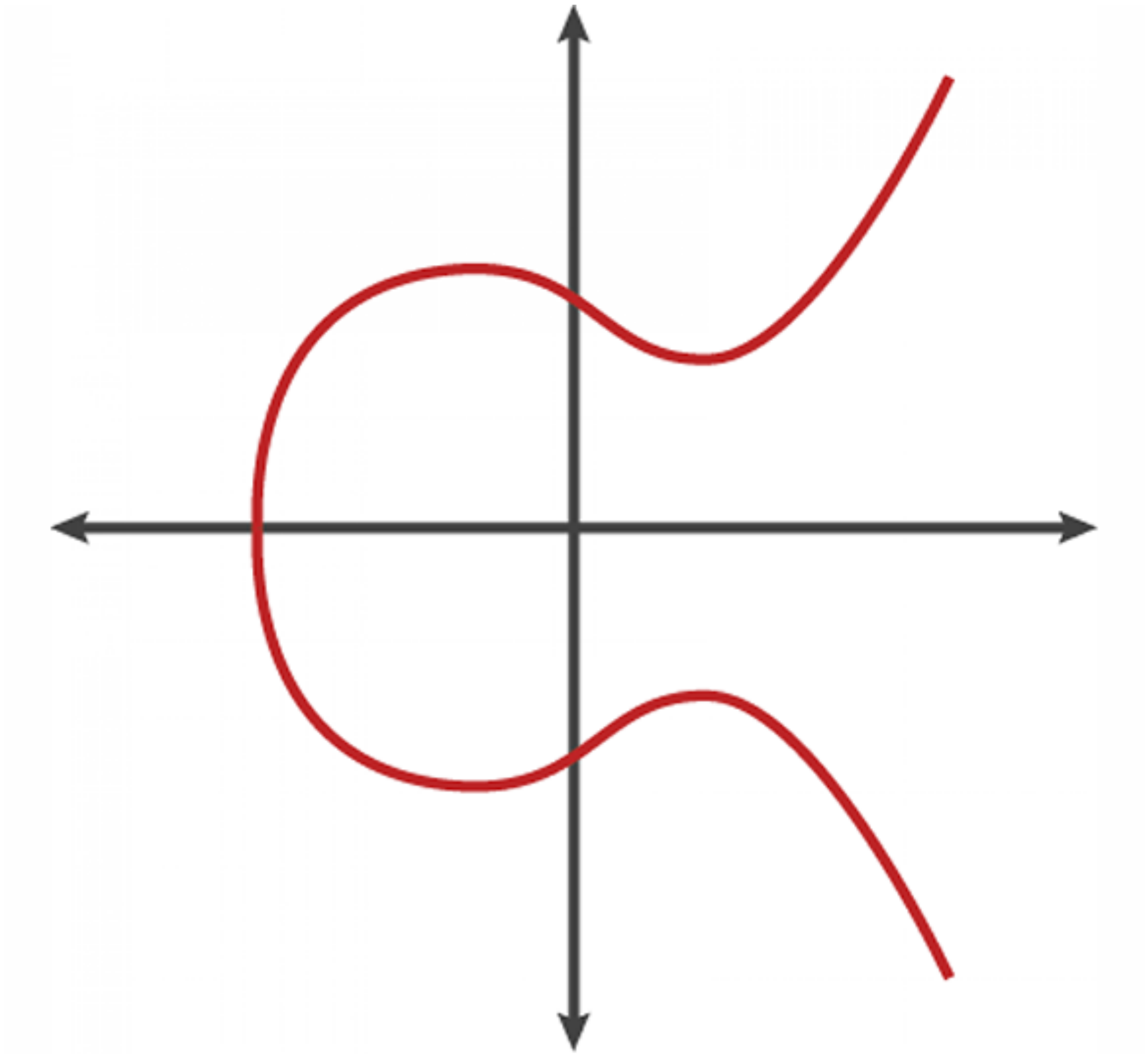
(Short) Preliminaries

Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ ($q = p^{\bullet}, p \neq 2,3$) is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.



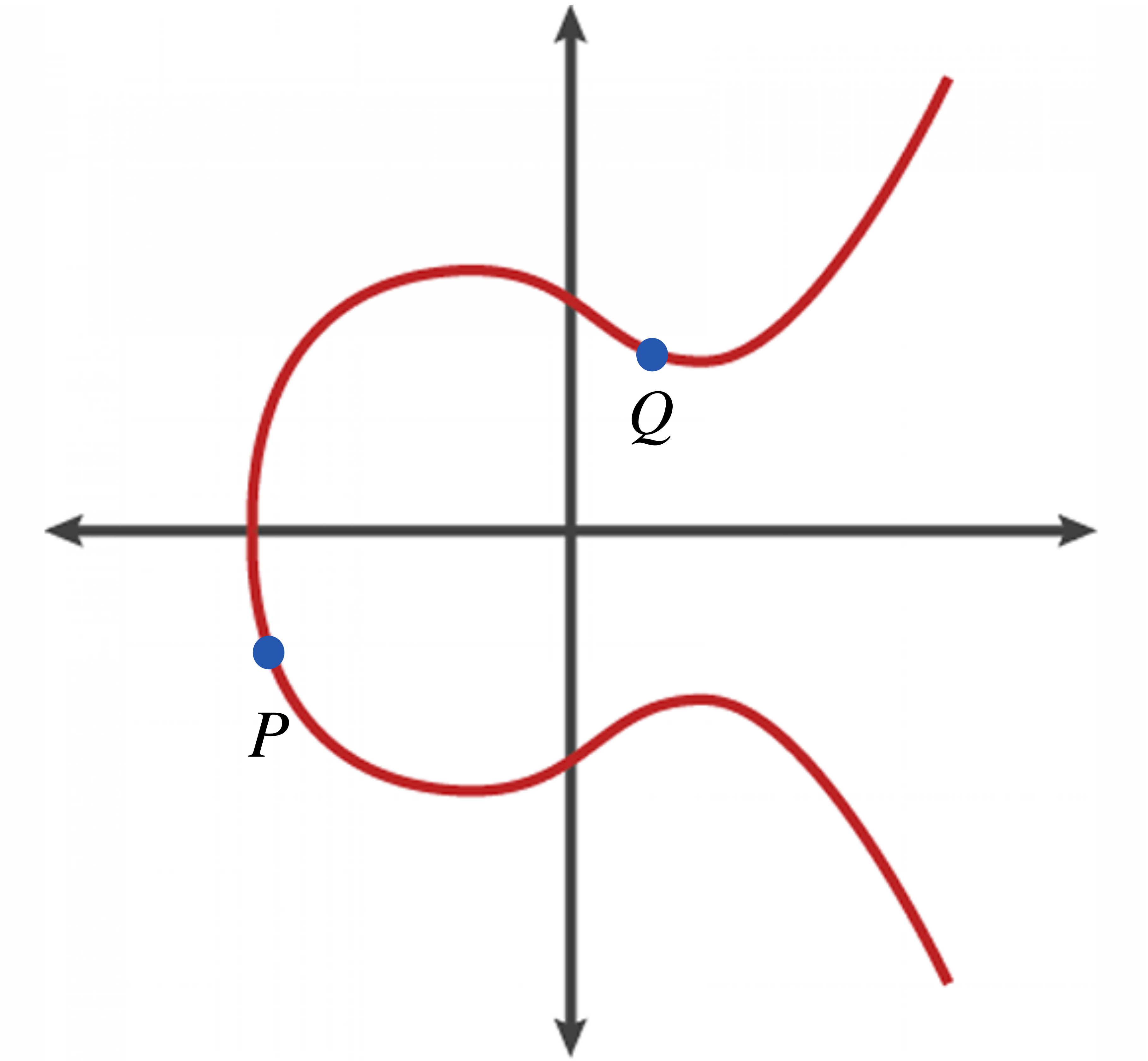
Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ ($q = p^{\bullet}, p \neq 2{,}3$) is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.

Elliptic curves form a group $E(\mathbb{F}_q)$ under **addition of poi**



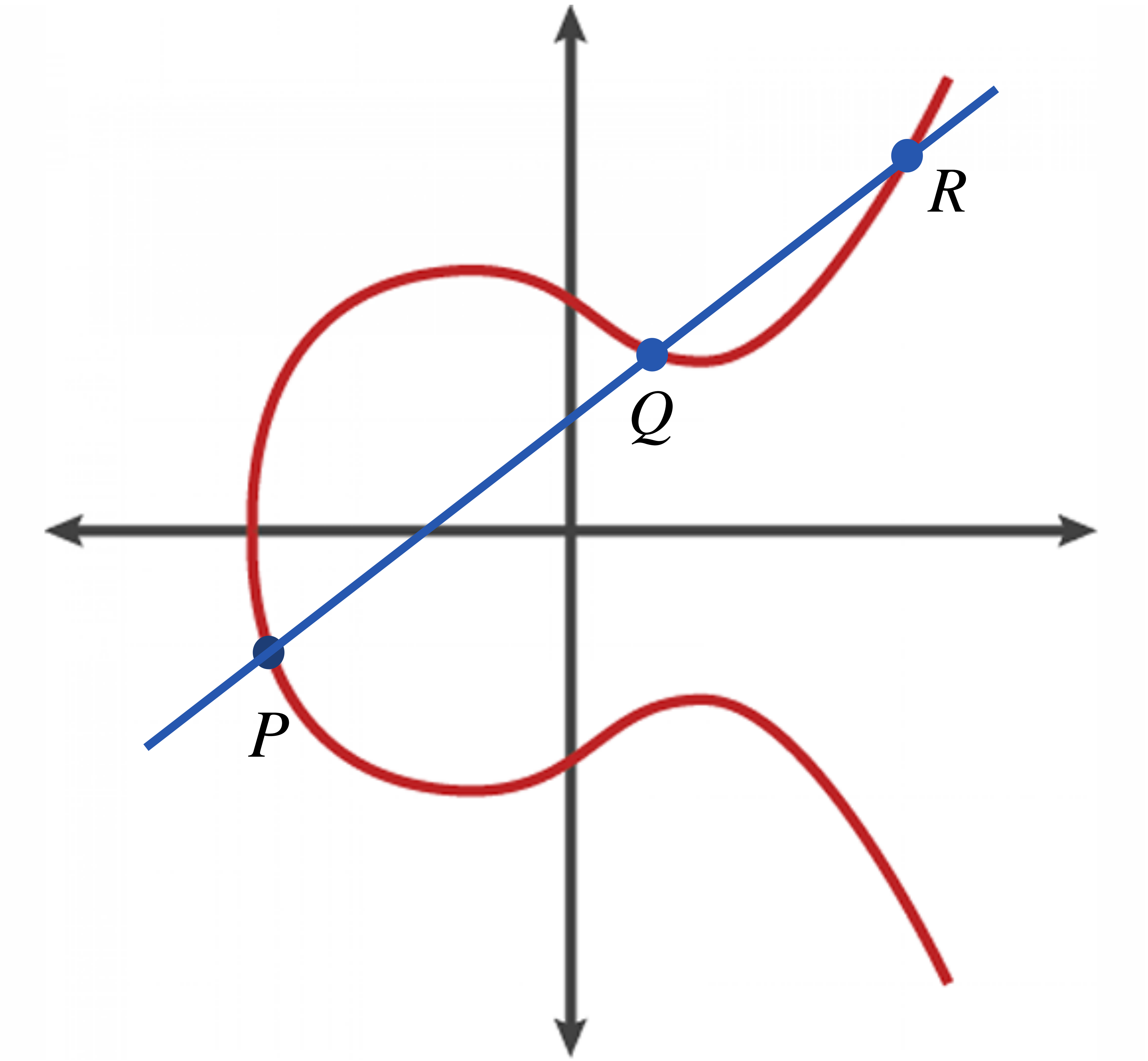
Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ $(q = p^{\bullet}, p \neq 2{,}3)$ is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.

Elliptic curves form a group $E(\mathbb{F}_q)$ under **addition of poi**



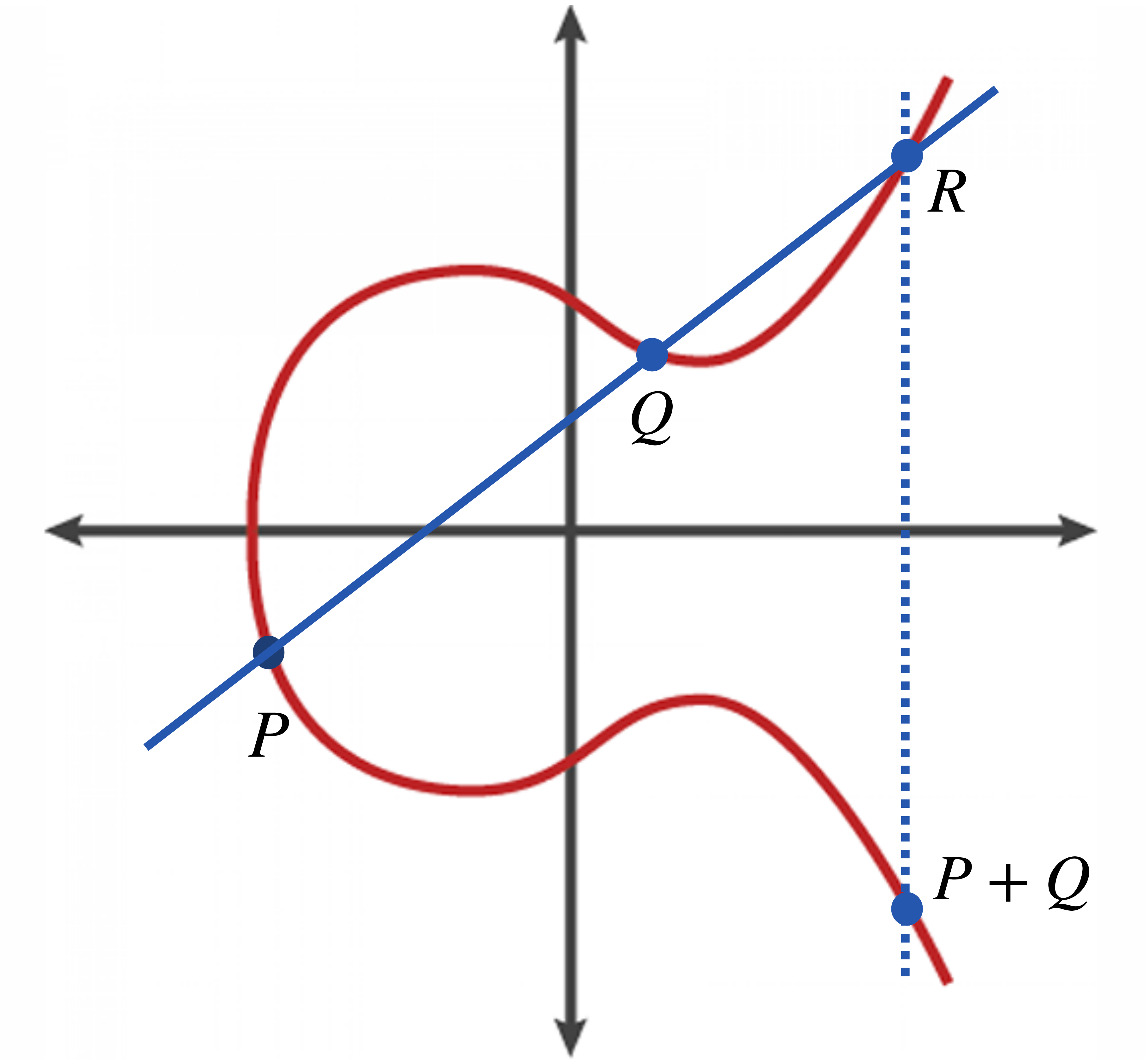
Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ ($q = p^{\bullet}, p \neq 2,3$) is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.

Elliptic curves form a group $E(\mathbb{F}_q)$ under **addition of poi**



Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ $(q = p^\bullet, p \neq 2,3)$ is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.

Elliptic curves form a group $E(\mathbb{F}_q)$ under **addition of points**. Identity is denoted $\mathcal{O}$.

Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ ($q = p^{\bullet}, p \neq 2,3$) is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.

Elliptic curves form a group $E(\mathbb{F}_q)$ under **addition of points**. Identity is denoted $\mathcal{O}$.

Another useful operation is **scalar multiplication**:

For $a \in \mathbb{Z}$ and point $P \in E(\mathbb{F}_q)$, $[a]P = P \underbrace{+ \ldots +}_{a} P$

Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ ($q = p^\bullet, p \neq 2{,}3$) is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.

Elliptic curves form a group $E(\mathbb{F}_q)$ under **addition of points**. Identity is denoted $\mathcal{O}$.

Another useful operation is **scalar multiplication**:

For $a \in \mathbb{Z}$ and point $P \in E(\mathbb{F}_q)$, $[a]P = P \underbrace{+ \ldots +}_{a} P$

The **order** of the point is the smallest positive $n \in \mathbb{Z}$ such that $[n]P = \mathcal{O}$.

$E(\mathbb{F}_q)[n]$ is the subgroup of n-torsion points (points whose order divides n).

Elliptic Curves for Cryptography

An **elliptic curve** E over finite field $\mathbb{F}_q$ ($q = p^\bullet, p \neq 2,3$) is a smooth curve

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$.

Elliptic curves form a group $E(\mathbb{F}_q)$ under **addition of points**. Identity is denoted $\mathcal{O}$.

Another useful operation is **scalar multiplication**:

For $a \in \mathbb{Z}$ and point $P \in E(\mathbb{F}_q)$, $[a]P = P \underbrace{+ \ldots +}_{a} P$

The **order** of the point is the smallest positive $n \in \mathbb{Z}$ such that $[n]P = \mathcal{O}$

An elliptic curve is **supersingular** if $E(\bar{\mathbb{F}}_q)$ has no points of order p, otherwise **ordinary**.

Abelian varieties

Elliptic curves E

Abelian varieties

Elliptic curves E $\longrightarrow$ Principally polarised abelian varieties A

Pairings

A pairing is a non-degenerate bilinear map

(additive) group
of prime order ℓ

$$e : G_1 \times G_2 \to G_T$$

(additive) group
of prime order ℓ

(multiplicative) group
of prime order ℓ

Pairings

A pairing is a non-degenerate bilinear map

$$e : G_1 \times G_2 \to G_T$$

Non-degenerate: $e(P_1, P_2) = 1_{G_T}$ for all $P_2 \in G_2$ if and only if $P_1 = 0_{G_1}$

$e(P_1, P_2) = 1_{G_T}$ for all $P_1 \in G_1$ if and only if $P_2 = 0_{G_2}$

Bilinear: For all $P_1, Q_1 \in G_1$ and $P_2, Q_2 \in G_2$ we have

$$e(P_1 + Q_1, P_2) = e(P_1, P_2)e(Q_1, P_2) \text{ and } e(P_1, P_2 + Q_2) = e(P_1, P_2)e(P_1, Q_2)$$

Pairings

For an elliptic curve, the ℓ-Weil pairing (for prime ℓ with ℓ-torsion defined over $\mathbb{F}_{p^u}$) is the pairing

$$e : E(\mathbb{F}_{p^u})[\ell] \times E(\mathbb{F}_{p^u})[\ell] \to \mu_\ell \subseteq \mathbb{F}_{p^{uk}}^\times$$

where k is the *embedding degree with respect to* ℓ: the smallest natural number k such that $\ell \mid (p^u)^k - 1$.

Pairings

For an elliptic curve, the ℓ-Weil pairing (for prime ℓ with ℓ-torsion defined over $\mathbb{F}_{p^u}$) is the pairing

$$e : E(\mathbb{F}_{p^u})[\ell] \times E(\mathbb{F}_{p^u})[\ell] \to \mu_\ell \subseteq \mathbb{F}_{p^{uk}}^\times$$

where k is the *embedding degree with respect to* ℓ: the smallest natural number k such that $\ell \mid (p^u)^k - 1$.

For **security**, we need the DLP to be hard in $\mathbb{F}_{p^{uk}}^\times$ so we want to maximise the embedding degree (while the pairing still be efficiently computable).

We also need ℓ to be large enough so that the ECDLP is hard in $E(\mathbb{F}_{p^u})[\ell]$; best attack is generic and runs in $O(\sqrt{l})$.

Pairings

For an elliptic curve, the ℓ-Weil pairing (for prime ℓ with ℓ-torsion defined over $\mathbb{F}_{p^u}$) is the pairing

$$e : E(\mathbb{F}_{p^u})[\ell] \times E(\mathbb{F}_{p^u})[\ell] \to \mu_\ell \subseteq \mathbb{F}_{p^{uk}}^\times$$

where k is the *embedding degree with respect to ℓ*: the smallest natural number k such that $\ell \mid (p^u)^k - 1$.

Paring friendly with respect to q

$$\begin{tikzcd} E/\mathbb{F}_p \arrow[r, bend left] & E'/\mathbb{F}_q \arrow[l, bend left] \end{tikzcd}$$

Paring friendly with respect to p

Abelian varieties

Elliptic curves $\longrightarrow$ Principally polarised abelian varieties

We can generalise the ℓ-Weil pairing for principally polarised abelian varieties.

Abelian varieties

Elliptic curves $\longrightarrow$ Principally polarised abelian varieties

We can generalise the ℓ-Weil pairing for principally polarised abelian varieties.

Embedding Degree

Abelian varieties

Elliptic curves $\longrightarrow$ Principally polarised abelian varieties

We can generalise the ℓ-Weil pairing for principally polarised abelian varieties.

Embedding Degree $\longrightarrow$

Cryptographic Exponent

For large enough ℓ, the *cryptographic exponent* c_A of A is such that $(p^u)^{c_A} = p^r$, with r the smallest integer such that $\ell \mid p^r - 1$.

Abelian varieties

Elliptic curves $\longrightarrow$ Principally polarised abelian varieties

We can generalise the ℓ-Weil pairing for principally polarised abelian varieties.

Embedding Degree $\longrightarrow$

When $u > 1$, r can be smaller than uk

Cryptographic Exponent

For large enough ℓ, the *cryptographic exponent* c_A of A is such that $(p^u)^{c_A} = p^r$, with r the smallest integer such that $\ell \mid p^r - 1$.

Abelian varieties

Elliptic curves $\longrightarrow$ Principally polarised abelian varieties

We can generalise the ℓ-Weil pairing for principally polarised abelian varieties.

Embedding Degree $\longrightarrow$ **Cryptographic Exponent**

For large enough ℓ, the *cryptographic exponent* c_A of A is such that $(p^u)^{c_A} = p^r$, with r the smallest integer such that $\ell \mid p^r - 1$.

Captures the ratio between the field of definition of A and where the ℓ-Weil pairing is defined.

Abelian varieties

Elliptic curves $\longrightarrow$ Principally polarised abelian varieties

We can generalise the ℓ-Weil pairing for principally polarised abelian varieties.

Embedding Degree $\longrightarrow$

Cryptographic Exponent

For large enough ℓ, the *cryptographic exponent* c_A of A is such that $(p^u)^{c_A} = p^r$, with r the smallest integer such that $\ell \mid p^r - 1$.

Remark: the larger the cryptographic exponent is, the smaller p^u can be chosen, making arithmetic in the field of definition more efficient while still ensuring DLP security in the finite field group.

The *Ideal* Situation

The ideal situation

A 2-cycle of two prime order elliptic curves, both of which have (the same) embedding degree that balances the ECDLP and DLP securities of all groups involved.

The ideal situation

A 2-cycle of two prime order elliptic curves, both of which have (the same) embedding degree that balances the ECDLP and DLP securities of all groups involved.

$$
\begin{tikzcd}
\mathbb{F}_{p^k}^{\times} & \mathbb{F}_{q^{k'}}^{\times} \\
\#E(\mathbb{F}_p) = q \arrow[u] \arrow[r, bend left] & \#E'(\mathbb{F}_q) = p \arrow[u] \arrow[l, bend left]
\end{tikzcd}
$$

The ideal situation

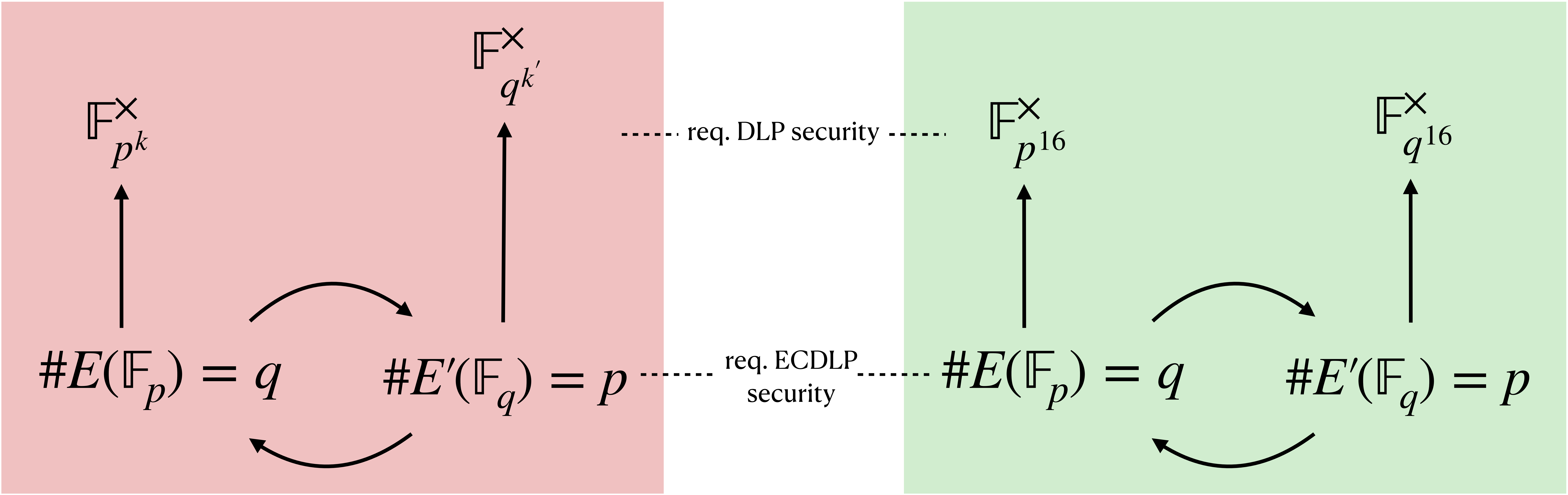
A 2-cycle of two prime order elliptic curves, both of which have (the same) embedding degree that balances the ECDLP and DLP securities of all groups involved.

$$\begin{tikzcd}
\mathbb{F}_{p^k}^{\times} & & \mathbb{F}_{q^{k'}}^{\times} \\
\#E(\mathbb{F}_p) = q \arrow[u] \arrow[rr, bend left] & & \#E'(\mathbb{F}_q) = p \arrow[u] \arrow[ll, bend left]
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbb{F}_{p^{16}}^{\times} & & \mathbb{F}_{q^{16}}^{\times} \\
\#E(\mathbb{F}_p) = q \arrow[u] \arrow[rr, bend left] & & \#E'(\mathbb{F}_q) = p \arrow[u] \arrow[ll, bend left]
\end{tikzcd}$$

The ideal situation

A 2-cycle of two prime order elliptic curves, both of which have (the same) embedding degree that balances the ECDLP and DLP securities of all groups involved.



The ideal situation

A 2-cycle of two prime order elliptic curves, both of which have (the same) embedding degree that balances the ECDLP and DLP securities of all groups involved.

Security level	**80**	**112**	**128**
Req. ext. field size	1184	3012	3968
Dream cycles $p \approx q$	160	224	256
MNT reality $p \approx q$	296	753	992

$$\begin{tikzcd}
\mathbb{F}_{p^{16}}^{\times} & \mathbb{F}_{q^{16}}^{\times} \\
\#E(\mathbb{F}_p) = q \arrow[u] \arrow[r, bend left] & \#E'(\mathbb{F}_q) = p \arrow[u] \arrow[l, bend left]
\end{tikzcd}$$

Overview

Our generalisation

We instead consider **pairing-friendly cycles of abelian varieties**. We say

$$A/\mathbb{F}_{p^u} \quad \text{and} \quad B/\mathbb{F}_{q^v}$$

form a cycle if $q \mid \#A(\mathbb{F}_{p^u})$ and $p \mid \#B(\mathbb{F}_{q^v})$ and A, B are pairing-friendly with respect to q, p (respectively).

Differences:

(i) A and B can be abelian varieties of any dimension

(ii) A and B can be defined over extension fields

(iii) p and q need only divide the respective group orders of B and A

High-level strategy

Choices and Restrictions

1) A **and** B **are simple**: i.e., not isomorphic to a product of lower dimensional abelian varieties

Choices and Restrictions

1) A **and** B **are simple**: i.e., not isomorphic to a product of lower dimensional abelian varieties

2) A **is supersingular of dimension** $g \geq 1$: exploiting existing constructions of supersingular pairing-friendly abelian varieties of dimension ≥ 1 (e.g., Galbraith, Pujolàs, Ritzenthaler, Smith '09)

Choices and Restrictions

1) A **and** B **are simple**: i.e., not isomorphic to a product of lower dimensional abelian varieties

2) A **is supersingular of dimension** $g \geq 1$: exploiting existing constructions of supersingular pairing-friendly abelian varieties of dimension ≥ 1 (e.g., Galbraith, Pujolàs, Ritzenthaler, Smith '09)

3) $A(\mathbb{F}_{p^u})$ **is of prime order** q: alongside supersingularity, this implies $q \equiv 1 \bmod p$, which means that B is pairing-friendly with respect to p; but, this forces $c_B = 1$.

Choices and Restrictions

1) A **and** B **are simple**: i.e., not isomorphic to a product of lower dimensional abelian varieties

2) A **is supersingular of dimension** $g \geq 1$: exploiting existing constructions of supersingular pairing-friendly abelian varieties of dimension ≥ 1 (e.g., Galbraith, Pujolàs, Ritzenthaler, Smith '09)

3) $A(\mathbb{F}_{p^u})$ **is of prime order** q: alongside supersingularity, this implies $q \equiv 1 \bmod p$, which means that B is pairing-friendly with respect to p; but, this forces $c_B = 1$.

4) B **is of dimension** 1: as $c_B = 1$, having B as an elliptic curve allows the most straightforward construction of a cycle with most efficient arithmetic.

Choices and Restrictions

1) A **and** B **are simple**: i.e., not isomorphic to a product of lower dimensional abelian varieties

2) A **is supersingular of dimension** $g \geq 1$: exploiting existing constructions of supersingular pairing-friendly abelian varieties of dimension ≥ 1 (e.g., Galbraith, Pujolàs, Ritzenthaler, Smith '09)

3) $A(\mathbb{F}_{p^u})$ **is of prime order** q: alongside supersingularity, this implies $q \equiv 1 \bmod p$, which means that B is pairing-friendly with respect to p; but, this forces $c_B = 1$.

4) B **is of dimension** 1: as $c_B = 1$, having B as an elliptic curve allows the most straightforward construction of a cycle with most efficient arithmetic.

To counter: find large v such that v is the smallest integer with $B[p] \subseteq B(\mathbb{F}_{q^v})$

Security

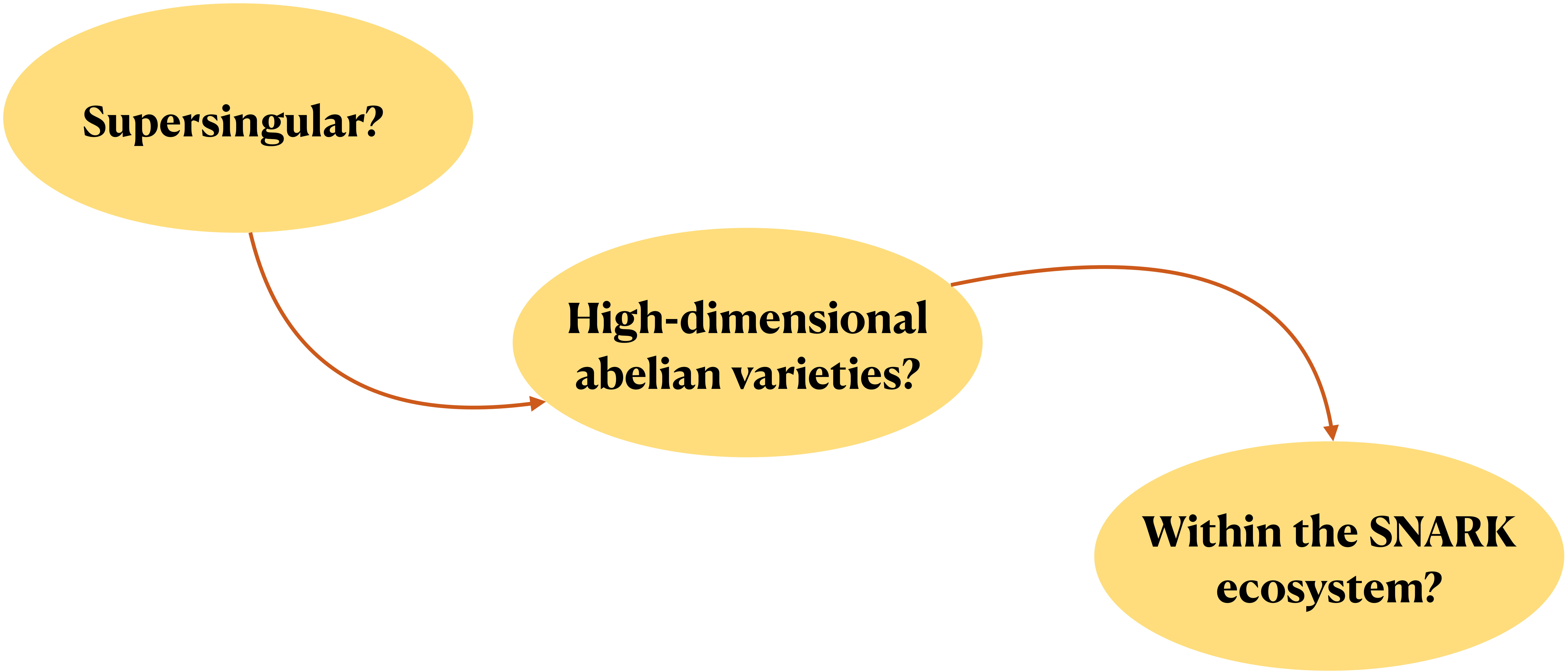
Supersingular?

Security

Supersingular?

High-dimensional abelian varieties?

Security


Supersingular?
High-dimensional abelian varieties?
Within the SNARK ecosystem?

Towards optimal cycles

Recall: An optimal cycle for λ-bit security would be one where

- $p \approx q \approx 2^{2\lambda}$
- q-Weil pairing of A map into an extension field large enough to achieve λ-bits of security against state-of-the-art DLP attacks.
- Likewise for the p-Weil pairing of B

Towards optimal cycles

Recall: An optimal cycle for λ-bit security would be one where

- $p \approx q \approx 2^{2\lambda}$
- q-Weil pairing of A map into an extension field large enough to achieve λ-bits of security against state-of-the-art DLP attacks.
- Likewise for the p-Weil pairing of B

This work: Give constructions of A where $p \approx 2^{2\lambda}$ is indeed as small as possible. With our choices and restrictions, we cannot pair this with an "optimal" B… but there is not negative result saying they cannot exist.

Constructions

Constructions

Let's focus on two constructions...

First construction

$p \equiv 2 \bmod 3$, $u = 2u'$ with u' even such that $q = p^u - p^{u/2} + 1$ is prime

- supersingular elliptic curve defined over $\mathbb{F}_{p^u}$
- $\#A(\mathbb{F}_{p^u}) = q$
- cryptographic exponent $c_A = 3$ w.r.t. q

Proposition 2 gives the explicit construction.

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

First construction

$p \equiv 2 \bmod 3$, $u = 2u'$ with u' even such that $q = p^u - p^{u/2} + 1$ is prime

- supersingular elliptic curve defined over $\mathbb{F}_{p^u}$
- $\#A(\mathbb{F}_{p^u}) = q$
- cryptographic exponent $c_A = 3$ w.r.t. q

Proposition 2 gives the explicit construction.

$$A/\mathbb{F}_{p^u} \qquad B/\mathbb{F}_{q^2}$$

$p > 3$ prime, u even such that $q = p^u + p^{u/2} + 1$ is prime

- supersingular elliptic curve defined over $\mathbb{F}_{q^2}$
- $p \,|\, \#B(\mathbb{F}_{q^2})$
- cryptographic exponent $c_B = 1$ w.r.t. p

Proposition 5 gives the explicit construction.

Example #1

$p = 2^{160} - 44159$

$\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ with $\alpha^2 = 3$

$\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\beta)$ with $\beta^2 = \alpha$

$q = p^4 - p^2 + 1 \approx 2^{640}$

$$\begin{tikzcd}
\mathbb{F}_{p^{12}}^{\times} \ \text{1920-bit field} & \mathbb{F}_{q^2}^{\times} \ \text{1280-bit field} \\
A/\mathbb{F}_{p^4} : y^2 = x^3 + (\alpha + \beta) \arrow[u] \arrow[r, bend left] & B/\mathbb{F}_{q^2} : y^2 = x^3 + ax + b \arrow[u] \arrow[l, bend left]
\end{tikzcd}$$

$a, b \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$

Summary of constructions

Target security	MNT cycle				This work					
	p	q	p^k	$q^{k'}$	$\dim(A)$	p	p^u	q	$(p^u)^{c_A}$	q^v
80	298	298	1192	1788	1	**160**	640	640	1920	1280
112										
128										

Second construction

Let $g = 2^\ell$ with $\ell \geq 0$. Let $u = 2u'$ with u' odd and $q = p^{ug} - p^{ug/2} + 1$ prime.

- supersingular abelian variety over $\mathbb{F}_{p^u}$ of dimension g
- $\#A(\mathbb{F}_{p^u}) = q$
- cryptographic exponent $c_A = 3 \cdot 2^{g-1}$ w.r.t. q

Theorem 4 gives the explicit construction. In particular, there is a natural identification of $A(\mathbb{F}_{p^u})$ with a subgroup of $E(\mathbb{F}_{p^{ur}})$ with $r = 2g$ and E as in Proposition 1. Relies heavily on work by Rubin and Silverberg.

$$\begin{tikzcd} A/\mathbb{F}_{p^u} \arrow[r, bend left] & B/\mathbb{F}_{q^v} \arrow[l, bend left] \end{tikzcd}$$

Second construction

Let $g = 2^\ell$ with $\ell \geq 0$. Let $u = 2u'$ with u' odd and $q = p^{ug} - p^{ug/2} + 1$ prime.

- supersingular abelian variety over $\mathbb{F}_{p^u}$ of dimension g
- $\#A(\mathbb{F}_{p^u}) = q$
- cryptographic exponent $c_A = 3 \cdot 2^{g-1}$ w.r.t. q

$$
\begin{tikzcd}
A/\mathbb{F}_{p^u} \arrow[r, bend left] & B/\mathbb{F}_{q^v} \arrow[l, bend left]
\end{tikzcd}
$$

Theorem 4 gives the explicit construction. In particular, there is a natural identification of $A(\mathbb{F}_{p^u})$ with a subgroup of $E(\mathbb{F}_{p^{ur}})$ with $r = 2g$ and E as in Proposition 1. Relies heavily on work by Rubin and Silverberg.

the trace-zero subvariety

Second construction

As before....

Let $g = 2^\ell$ with $\ell \geq 0$. Let $u = 2u'$ with u' odd and $q = p^{ug} - p^{ug/2} + 1$ prime.

- supersingular abelian variety over $\mathbb{F}_{p^u}$ of dimension g
- $\#A(\mathbb{F}_{p^u}) = q$
- cryptographic exponent $c_A = 3 \cdot 2^{g-1}$ w.r.t. q

$$A/\mathbb{F}_{p^u} \quad \rightleftarrows \quad B/\mathbb{F}_{q^2}$$

$p > 3$ prime, u even such that $q = p^{ug} - p^{ug/2} + 1$ is prime

- supersingular elliptic curve defined over $\mathbb{F}_{q^2}$
- $p \,|\, \#B(\mathbb{F}_{q^2})$
- cryptographic exponent $c_B = 1$ w.r.t. p

Theorem 4 gives the explicit construction. In particular, there is a natural identification of $A(\mathbb{F}_{p^u})$ with a subgroup of $E(\mathbb{F}_{p^{ur}})$ with $r = 2g$ and E as in Proposition 1. Relies heavily on work by Rubin and Silverberg.

Proposition 5 gives the explicit construction.

Example #2

$p = 2^{160} - 44159$

$\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ with $\alpha^2 = 3$

$g = 2$

$q = p^4 - p^2 + 1 \approx 2^{640}$

$$
\begin{tikzcd}
\mathbb{F}_{p^{12}}^{\times} \text{ 1920-bit field} & \mathbb{F}_{q^2}^{\times} \text{ 1280-bit field} \\
A/\mathbb{F}_{p^2} \text{ of dimension 2} \arrow[u] \arrow[r, bend left] & \begin{array}{c} B/\mathbb{F}_{q^2} : y^2 = x^3 + ax + b \\ a, b \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q \end{array} \arrow[u] \arrow[l, bend left]
\end{tikzcd}
$$

Summary of constructions

Target security	MNT cycle				This work					
	p	q	p^k	$q^{k'}$	$\dim(A)$	p	p^u	q	$(p^u)^{c_A}$	q^v
80	298	298	1192	1788	1 2	**160** **160**	640 320	640 640	1920 1920	1280 1280

Summary of constructions

Target security	MNT cycle				This work					
	p	q	p^k	$q^{k'}$	$\dim(A)$	p	p^u	q	$(p^u)^{c_A}$	q^v
80	298	298	1192	1788	1 2	**160** **160**	640 320	640 640	1920 1920	1280 1280
112	753	753	3012	4517	1 2	**224** **377**	1792 754	1792 1508	5376 4512	3584 3012
128	992	992	3966	5948	1 2 4	2048 1024 **512**	2048 1024 **512**	2048 2048 2048	6144 6144 12288	4096 4096 4096

Future work

Future work

For finding such *relaxed* 2-cycles, Costello and Korpal study the following necessary condition:

Future work

For finding such *relaxed* 2-cycles, Costello and Korpal study the following necessary condition:

Definition: Primes with (k, k')-order reciprocity

The prime numbers p and q have (k, k')-order reciprocity if

- $\mathrm{ord}_q(p) = k$
- $\mathrm{ord}_p(q) = k'$

Future work

For finding such *relaxed* 2-cycles, Costello and Korpal study the following necessary condition:

Definition: Primes with (k, k')-order reciprocity

The prime numbers p and q have (k, k')-order reciprocity if

- $\mathrm{ord}_q(p) = k$
- $\mathrm{ord}_p(q) = k'$

(k, k') will correspond to the embedding degrees.

Future work

Example:

- The prime pair $(p, q) = (620461, 15493)$ is such that $(k, k') = (12, 12)$

Future work

Example:

- The prime pair $(p, q) = (620461, 15493)$ is such that $(k, k') = (12, 12)$
- We cannot have $q = \#E(\mathbb{F}_p)$ and $p = \#E'(\mathbb{F}_q)$. Indeed, the Hasse bound for $E'/\mathbb{F}_q$ is $15246 \leq \#E'(\mathbb{F}_q) \leq 15742$.

Future work

Example:

- The prime pair $(p, q) = (620461, 15493)$ is such that $(k, k') = (12, 12)$
- We cannot have $q = \#E(\mathbb{F}_p)$ and $p = \#E'(\mathbb{F}_q)$. Indeed, the Hasse bound for $E'/\mathbb{F}_q$ is $15246 \leq \#E'(\mathbb{F}_q) \leq 15742$.
- Allowing cofactors and/or extension fields? Still doesn't quite work:
    - $hq = \#E(\mathbb{F}_p)$ and $h'p = \#E'(\mathbb{F}_{q^2})$
    - Such an E exists with $h = 40$, but no multiple of p in the Hasse interval for $E'/\mathbb{F}_{q^2}$

Future work

Example:

- The prime pair $(p, q) = (620461,15493)$ is such that $(k, k') = (12,12)$
- We cannot have $q = \#E(\mathbb{F}_p)$ and $p = \#E'(\mathbb{F}_q)$. Indeed, the Hasse bound for $E'/\mathbb{F}_q$ is $15246 \leq \#E'(\mathbb{F}_q) \leq 15742$.
- Allowing cofactors and/or extension fields? Still doesn't quite work:
  - $hq = \#E(\mathbb{F}_p)$ and $h'p = \#E'(\mathbb{F}_{q^2})$
  - Such an E exists with $h = 40$, but no multiple of p in the Hasse interval for $E'/\mathbb{F}_{q^2}$
- We need higher dimensions:
  - $C/\mathbb{F}_q : y^2 = x^6 + 6611x^5 + 13858x^4 + 6818x^3 + 5652x^2 + 10423x + 1795$ ordinary, $\#J_C(\mathbb{F}_q) = 383 \cdot p$
  - $E/\mathbb{F}_p : y^2 = x^3 + 30984x + 426966$ ordinary, $\#E(\mathbb{F}_p) = 40 \cdot q$

Future work

In light of this, they pose some open questions:

Future work

In light of this, they pose some open questions:

1. Is (620461,15493) the only prime pair with (12,12)-order reciprocity?

Future work

In light of this, they pose some open questions:

1. Is (620461,15493) the only prime pair with (12,12)-order reciprocity?
2. Are there any fixed values of (k, k') with $\min(k, k') > 4$ for which that are an infinite number of primes with (k, k')-order reciprocity?

Future work

In light of this, they pose some open questions:

1. Is (620461,15493) the only prime pair with (12,12)-order reciprocity?
2. Are there any fixed values of (k, k') with $\min(k, k') > 4$ for which that are an infinite number of primes with (k, k')-order reciprocity?
3. Are there any fixed values of (k, k') with $\min(k, k') > 2$ for which that are no primes with (k, k')-order reciprocity?

Conclusions

- We generalise the definition of cycles of pairing-friendly elliptic curves.
- We make certain choices to restrict our attention to a subset of possible cycles.
- We exhibit the interest of this framework by presenting new constructions.

Conclusions

- We generalise the definition of cycles of pairing-friendly elliptic curves.
- We make certain choices to restrict our attention to a subset of possible cycles.
- We exhibit the interest of this framework by presenting new constructions.

- Can we relax some of these restrictions to find better cycles?
- How do these cycles perform in practice?

Conclusions

- We generalise the definition of cycles of pairing-friendly elliptic curves.
- We make certain choices to restrict our attention to a subset of possible cycles.
- We exhibit the interest of this framework by presenting new constructions.

- Can we relax some of these restrictions to find better cycles?
- How do these cycles perform in practice?

Published at CRYPTO 2024
(eprint 2024/869)