The higher-dimensional picture

And its role in isogeny-based cryptography

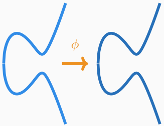
Sabrina Kunzweiler

June 13th, 2024

Inria Bordeaux, IMB, France

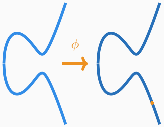
Isogeny-based cryptography

Candidate for post-quantum cryptography based on the hard problem of finding isogenies

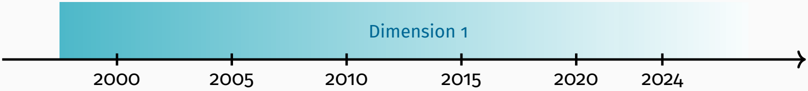


Isogeny-based cryptography

Candidate for post-quantum cryptography based on the hard problem of finding isogenies

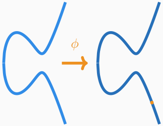


Dimensions in isogeny-based crypto

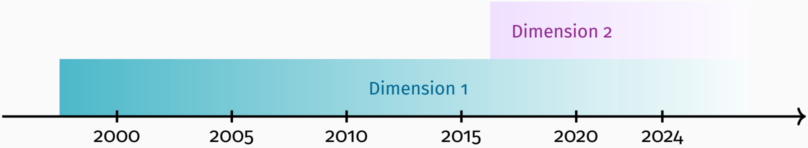


Isogeny-based cryptography

Candidate for post-quantum cryptography based on the hard problem of finding isogenies

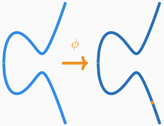


Dimensions in isogeny-based crypto

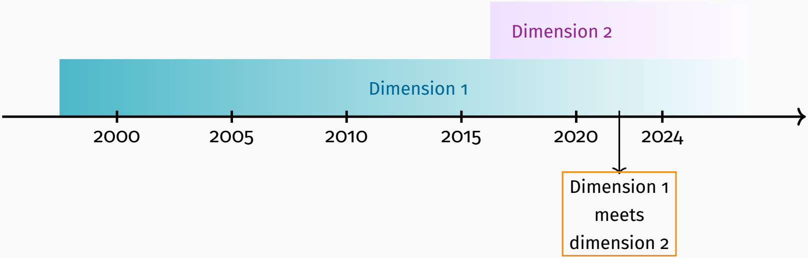


Isogeny-based cryptography

Candidate for post-quantum cryptography based on the hard problem of finding isogenies

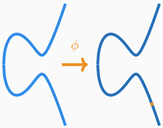


Dimensions in isogeny-based crypto

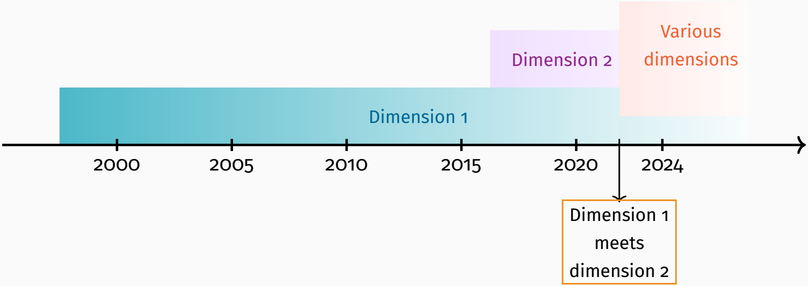


Isogeny-based cryptography

Candidate for post-quantum cryptography based on the hard problem of finding isogenies



Dimensions in isogeny-based crypto



The 1-dimensional picture

Elliptic curves

An **Elliptic Curve** E over $\mathbb{F}_{p^k}$
is defined by an equation

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

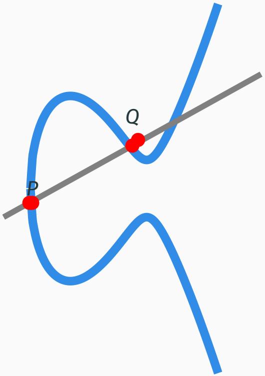
where $4a^3 + 27b^2 \neq 0$.

Elliptic curves

An **Elliptic Curve** E over $\mathbb{F}_{p^k}$ is defined by an equation

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

where $4a^3 + 27b^2 \neq 0$.



Points of E form an additive group.

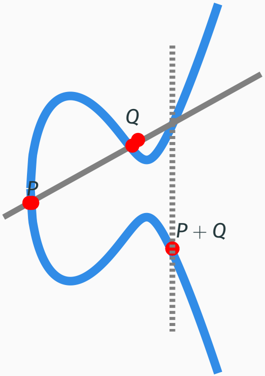
- Can compute $P + Q$ for points $P, Q \in E(\mathbb{F}_{p^k})$.

Elliptic curves

An **Elliptic Curve** E over $\mathbb{F}_{p^k}$ is defined by an equation

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

where $4a^3 + 27b^2 \neq 0$.



Points of E form an additive group.

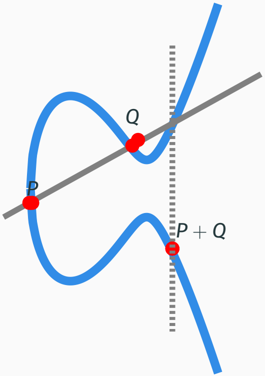
- Can compute $P + Q$ for points $P, Q \in E(\mathbb{F}_{p^k})$.

Elliptic curves

An **Elliptic Curve** E over $\mathbb{F}_{p^k}$ is defined by an equation

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

where $4a^3 + 27b^2 \neq 0$.



Points of E form an additive group.

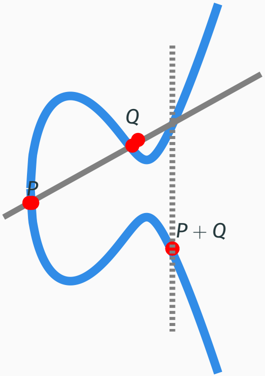
- Can compute $P + Q$ for points $P, Q \in E(\mathbb{F}_{p^k})$.
- Can compute $m \cdot P$ for a point $P \in E(\mathbb{F}_{p^k})$ and $m \in \mathbb{Z}$.

Elliptic curves

An **Elliptic Curve** E over $\mathbb{F}_{p^k}$ is defined by an equation

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

where $4a^3 + 27b^2 \neq 0$.



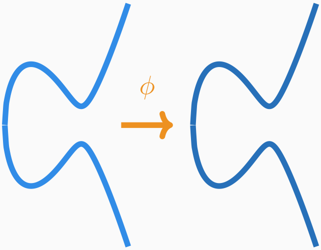
Points of E form an additive group.

- Can compute $P + Q$ for points $P, Q \in E(\mathbb{F}_{p^k})$.
- Can compute $m \cdot P$ for a point $P \in E(\mathbb{F}_{p^k})$ and $m \in \mathbb{Z}$.

$\Rightarrow$ **One-way function:** $m \mapsto m \cdot P$ for some fixed $P \in E(\mathbb{F}_{p^k})$.

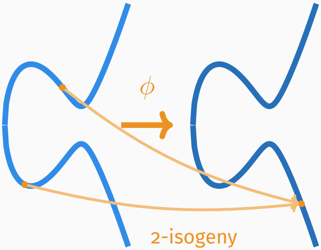
⚠ not a post-quantum one-way function

Isogenies



An **isogeny** $\phi : E \to E'$ is a (special) map between elliptic curves.

Isogenies

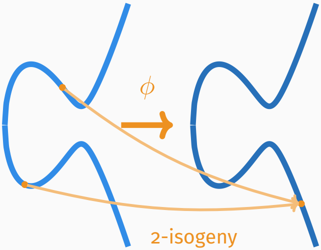


An **isogeny** $\phi : E \to E'$ is a (special) map between elliptic curves.

An N**-isogeny** is an isogeny $\phi : E \to E'$ with kernel $K \simeq \mathbb{Z}/N\mathbb{Z}$.

- Complexity: $O(N)$ (Vélu) or $\tilde{O}(\sqrt{N})$ ($\sqrt{\text{é}}$lu)

Isogenies



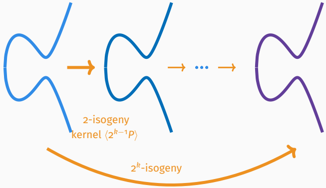
An **isogeny** $\phi : E \to E'$ is a (special) map between elliptic curves.

An N**-isogeny** is an isogeny $\phi : E \to E'$ with kernel $K \simeq \mathbb{Z}/N\mathbb{Z}$.

- Complexity: $O(N)$ (Vélu) or $\tilde{O}(\sqrt{N})$ ($\sqrt{\text{élu}}$)

Smooth-degree isogenies

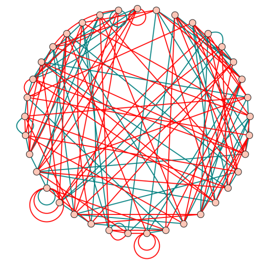
- Composition of small degree isogenies
- E.g. for $N = 2^k$ in time $O(k \log(k))$.



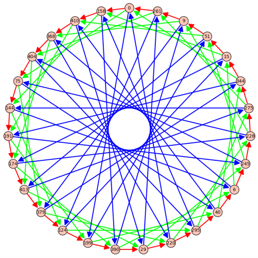
Isogeny graphs

- **Vertices**: elliptic curves (E).
- **Edges**: ℓ-isogenies with $\ell \in \{\ell_1, \ldots, \ell_n\}$ (E)—(E').

Two typical graphs



supersingular curves over $\mathbb{F}_{p^2}$
$\ell \in \{2, 3\}$, $p = 431$



supersingular curves over $\mathbb{F}_p$
$\ell \in \{3, 5, 7\}$, $p = 419$.

Isogenies as one-way functions

Setup Fix an elliptic curve E,
in an $\{\ell_1, \ldots, \ell_n\}$-isogeny graph with efficient navigation.

Isogeny one-way function

Input bit-string	$\rightsquigarrow$	path in the graph E — … — E'	$\rightsquigarrow$	Output E'

No polynomial quantum attacks are known.

Key exchange based on isogenies

Setup
Fix a starting curve E.

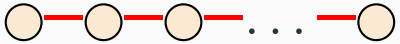
Key exchange based on isogenies

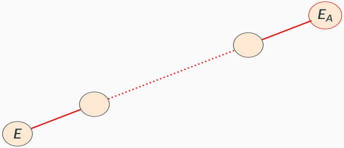
Setup

Fix a starting curve E.

Secret paths

Alice:





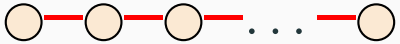
Key exchange based on isogenies

Setup

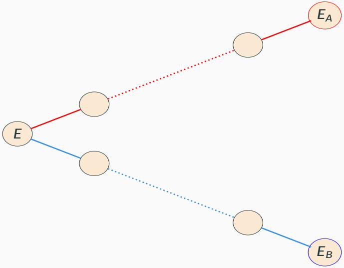
Fix a starting curve (E).

Secret paths

Alice:



Bob:



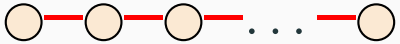
Key exchange based on isogenies

Setup

Fix a starting curve (E).

Secret paths

Alice:

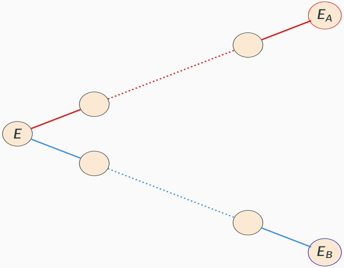


Bob:

Exchange

Alice $\xrightarrow{E_A}$ Bob

$\xleftarrow{E_B}$



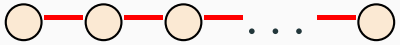
Key exchange based on isogenies

Setup

Fix a starting curve (E).

Secret paths

Alice:



Bob:

Exchange

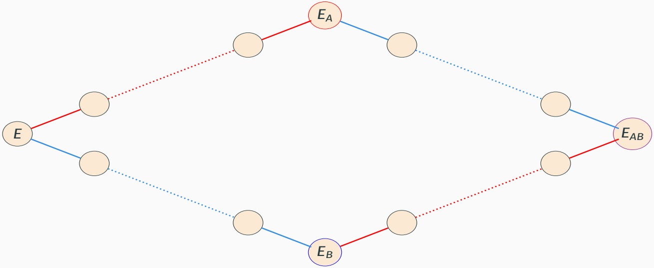
Alice $\xrightarrow{E_A}$ Bob

$\xleftarrow{E_B}$

Shared key

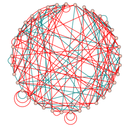
repeating* the path,

$\rightarrow$ (E_{AB})



(*) It is not obvious how to repeat a path with a different starting vertex, so that the paths commute.

Isogeny-based primitives in dimension 1



1997
Couveignes

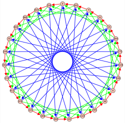
Hard homogeneous space
Group-action based cryptography
$\rightarrow$ DH key exchange with isogenies.

2006
Rostovtsev, Stolbunov

Public-key cryptosystem based on isogenies
Independent discovery of Couveigne's (unpublished) ideas.

2009
Charles, Goren, Lauter

CGL hash function Cryptographic hash functions from expander graphs.



2011
de Feo, Jao

SIDH
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies

2018,
Castryck, Lange, Martindale, Panny, Renes

CSIDH:
an efficient post-quantum commutative group action

2020
de Feo, Kohel, Leroux, Petit, Wesolowski

SQISign:
compact post-quantum signatures from quaternions and isogenies

The 2-dimensional picture

What are 2-dimensional elliptic curves ?

An elliptic curve

- is a 1-dimensional variety

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \subset \mathbb{P}^2.$$

- equipped with a group structure.

What are 2-dimensional ~~elliptic curves~~ principally polarized abelian varieties?

An elliptic curve

- is a 1-dimensional variety

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \subset \mathbb{P}^2.$$

- equipped with a group structure.

It is a principally polarized abelian variety (p.p.a.v.) of dimension 1.

What are 2-dimensional ~~elliptic curves~~ principally polarized abelian varieties?

An elliptic curve

- is a 1-dimensional variety

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \subset \mathbb{P}^2.$$

- equipped with a group structure.

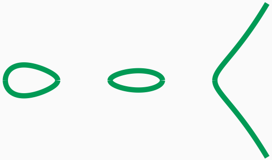
It is a principally polarized abelian variety (p.p.a.v.) of dimension 1.

How to construct a p.p.a.v. of dimension 2?

$1 + 1 = 2$:
product of elliptic curves
$E_1 \times E_2$

$2 = 2$: Irreducible p.p.a.v of dimension 2

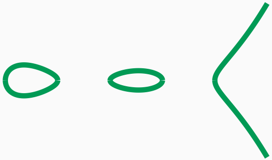
Genus-2 curve $C : y^2 = f(x),$ with $\deg(f) \in \{5, 6\}.$



$y^2 = x(x^2 - 1)(x^2 - 4)$

$2 = 2$: Irreducible p.p.a.v of dimension 2

Genus-2 curve $C : y^2 = f(x), \text{ with } \deg(f) \in \{5, 6\}$.

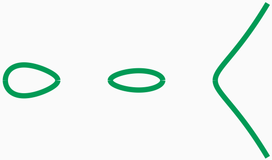


$y^2 = x(x^2 - 1)(x^2 - 4)$

⚠ Points on C do not form a group.

$2 = 2$: Irreducible p.p.a.v of dimension 2

Genus-2 curve $C : y^2 = f(x)$, with $\deg(f) \in \{5, 6\}$.

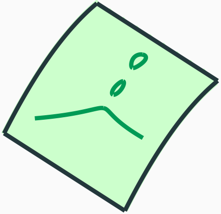


⚠ Points on C do not form a group.

$y^2 = x(x^2 - 1)(x^2 - 4)$

The **Jacobian of** C, $Jac(C)$, is a principally polarized abelian surface.

- Complicated as a variety (e.g. defined by 72 polynomials in $\mathbb{P}^{15}$).
- Easy description of $D \in Jac(C)$: $D = (P, Q)$ with P, Q points of C.



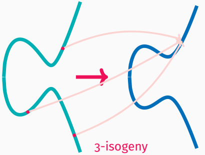
Isogenies in dimension 2

dimension 1

N-isogeny $\phi : E \to E'$ surjective morphism with $\ker(\phi) \simeq \mathbb{Z}/N\mathbb{Z}$.

dimension 2

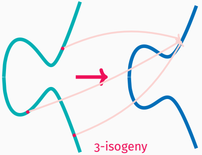
(N, N)-isogeny surjective morphism $\phi : A \to A'$ has isotropic[1] $\ker(\phi) \simeq (\mathbb{Z}/N\mathbb{Z})^2$



[1] Weil pairing is trivial.

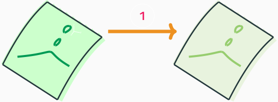
dimension 1

N-isogeny $\phi : E \to E'$ surjective morphism with $\ker(\phi) \simeq \mathbb{Z}/N\mathbb{Z}$.



dimension 2

(N, N)-isogeny surjective morphism $\phi : A \to A'$ has isotropic[1] $\ker(\phi) \simeq (\mathbb{Z}/N\mathbb{Z})^2$

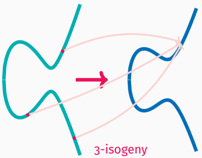


[1]Weil pairing is trivial.

Isogenies in dimension 2

dimension 1

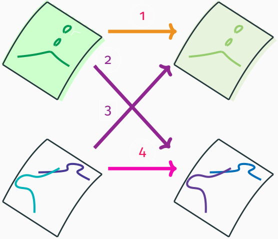
N-isogeny $\phi : E \to E'$ surjective morphism with $\ker(\phi) \simeq \mathbb{Z}/N\mathbb{Z}$.



all isogenies are generic

dimension 2

(N, N)-isogeny surjective morphism $\phi : A \to A'$ has isotropic[1] $\ker(\phi) \simeq (\mathbb{Z}/N\mathbb{Z})^2$



4 isogeny types:

1. generic
2. splitting
3. gluing
4. product

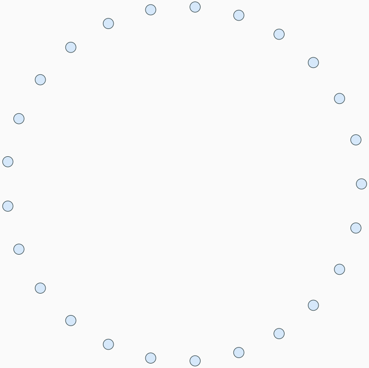
[1] Weil pairing is trivial.

Isogeny graphs in dimension 2

Vertices: p.p. abelian surfaces

○ $E \times E'$

(vey inaccurate) sketch of an isogeny graph



$\ell = 2$, $p = 53$

generically, the graph is 15-regular (for $\ell = 2$)

[a] More details on Slide 15

Isogeny graphs in dimension 2

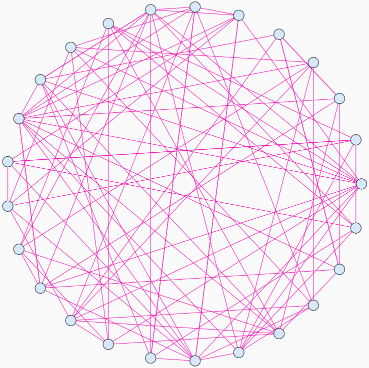
Vertices: p.p. abelian surfaces

 $E \times E'$

Edges: (ℓ, ℓ)-isogenies with

$\ell \in \{\ell_1, \ldots, \ell_n\}$

(vey inaccurate) sketch of an isogeny graph



$\ell = 2$, $p = 53$

generically, the graph is 15-regular

(for $\ell = 2$)

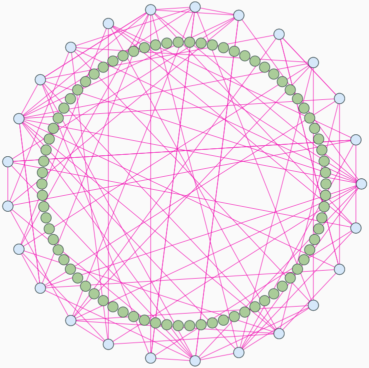
[a] More details on Slide 15

Vertices: p.p. abelian surfaces

 $E \times E'$  $Jac(C)$

Edges: (ℓ, ℓ)-isogenies with $\ell \in \{\ell_1, \ldots, \ell_n\}$

(vey inaccurate) sketch of an isogeny graph



$\ell = 2$, $p = 53$

generically, the graph is 15-regular (for $\ell = 2$)

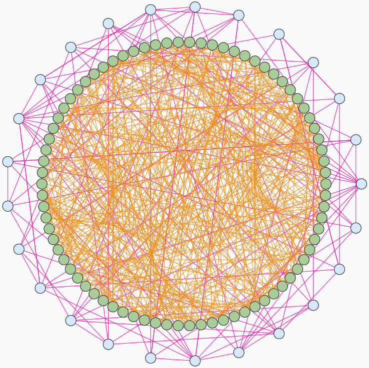
[a] More details on Slide 15

Vertices: p.p. abelian surfaces

$E \times E'$ $Jac(C)$

Edges: (ℓ, ℓ)-isogenies with $\ell \in \{\ell_1, \ldots, \ell_n\}$

(vey inaccurate) sketch of an isogeny graph



$\ell = 2$, $p = 53$

generically, the graph is 15-regular (for $\ell = 2$)

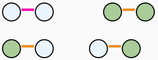
[a] More details on Slide 15

Isogeny graphs in dimension 2

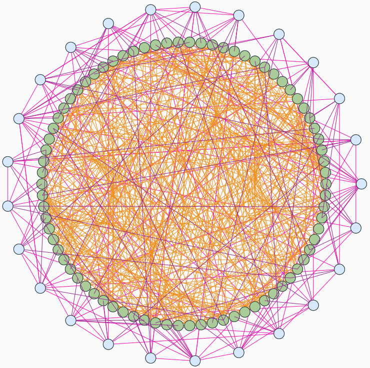
Vertices: p.p. abelian surfaces

○ $E \times E'$ ● $Jac(C)$

Edges: (ℓ,ℓ)-isogenies with $\ell \in \{\ell_1, \dots, \ell_n\}$



(vey inaccurate) sketch of an isogeny graph



$\ell = 2$, $p = 53$

generically, the graph is 15-regular (for $\ell = 2$)

[a] More details on Slide 15

Isogeny graphs in dimension 2

Vertices: p.p. abelian surfaces

$E \times E'$ $Jac(C)$

Edges: (ℓ, ℓ)-isogenies with

$\ell \in \{\ell_1, \dots, \ell_n\}$

Key features

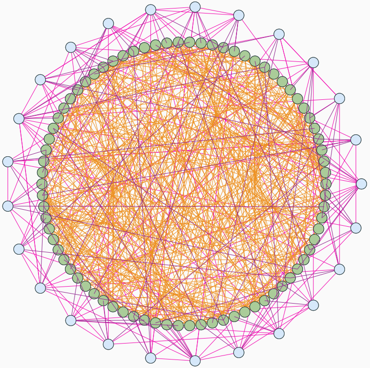
- # $\gg$ #;
- For small ℓ, we can navigate efficiently. [a]
- Finding a path

  is hard

[a] More details on Slide 15

(vey inaccurate) sketch of an isogeny graph



$\ell = 2$, $p = 53$

generically, the graph is 15-regular

(for $\ell = 2$)

Generalization of 1-dimensional crypto to dimension 2

Isogeny-based primitives in dimension 1

- 1997, Couveignes: CRS key exchange
- 2006, Rostovtsev, Stolbunov: CRS key exchange
- 2009, Charles, Goren, Lauter: CGL hash function
- 2011, de Feo, Jao: SIDH key exchange
- 2018, Castryck, Lange, Martindale, Panny, Renes: CSIDH key exchange
- 2020, de Feo, Kohel, Leroux, Petit, Wesolowski: SQISign

Generalization of 1-dimensional crypto to dimension 2

2018
Takashima

Efficient algorithms for isogeny sequences and their cryptographic applications
First generalization of the CGL hash function

2020
Castryck, Decru, Smith

Hash functions from superspecial genus-2 curves using Richelot isogenies
Repair of Takashima's hash function

Isogeny-based primitives in dimension 1

1997 Couveignes — CRS key exchange

2006 Rostovtsev, Stolbunov — CRS key exchange

CGL hash function — 2009 Charles, Goren, Lauter

SIDH key exchange — 2011 de Feo, Jao

2018, Castryck, Lange, Martindale, Panny, Renes — CSIDH key exchange

SQISign — 2020 de Feo, Kohel, Leroux, Petit, Wesolowski

Generalization of 1-dimensional crypto to dimension 2

2018 Takashima

Efficient algorithms for isogeny sequences and their cryptographic applications
First generalization of the CGL hash function

2019 Flynn, Ti

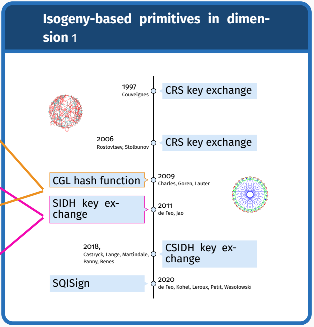
Genus two isogeny cryptography
First generalization of the SIDH key exchange (G2SIDH)

2020 Castryck, Decru, Smith

Hash functions from superspecial genus-2 curves using Richelot isogenies
Repair of Takashima's hash function

2021, Kunzweiler, Ti, Weitkämper

Secret keys in genus-2 SIDH
Improvement of the G2SIDH protocol



Generalization of 1-dimensional crypto to dimension 2

2018
Takashima

Efficient algorithms for isogeny sequences and their cryptographic applications
First generalization of the CGL hash function

2019
Flynn, Ti

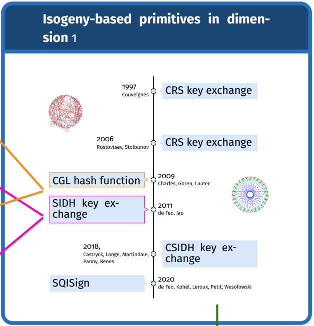
Genus two isogeny cryptography
First generalization of the SIDH key exchange (G2SIDH)

2020
Castryck, Decru, Smith

Hash functions from superspecial genus-2 curves using Richelot isogenies
Repair of Takashima's hash function

2021, Kunzweiler, Ti, Weitkämper

Secret keys in genus-2 SIDH
Improvement of the G2SIDH protocol

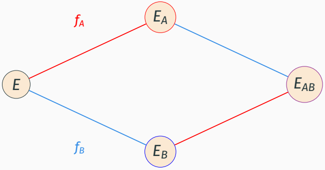


open problem

Dimension 2 meets dimension 1

Kani's Lemma (1997)

Isogeny diamond
(dimension 1)



d_A-isogeny f_A and d_B-isogeny f_B

$\Leftrightarrow$

Product isogeny
(dimension 2)

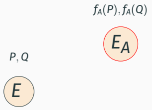
$(d_A + d_B, d_A + d_B)$-isogeny F

$d_A + d_B$ interpolation data of f_A, f_B $\Rightarrow$ kernel of F

The attacks on Supersingular Isogeny Diffie-Hellman (SIDH)

Kani's lemma serves as a key ingredient for attacking the isogeny one-way function **with torsion point information**.

Setting Given E, E_A and interpolation data $P, Q, f_A(P), f_A(Q)$ with $\langle P, Q \rangle = E[d_A + d_B]$, find f_A.

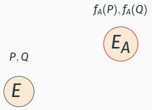


The attacks on Supersingular Isogeny Diffie-Hellman (SIDH)

Kani's lemma serves as a key ingredient for attacking the isogeny one-way function **with torsion point information**.

Setting Given E, E_A and interpolation data $P, Q, f_A(P), f_A(Q)$ with $\langle P, Q \rangle = E[d_A + d_B]$, find f_A.

Idea (Castryck-Decru, Maino-Martindale-Panny-Pope-Wesolowski, Robert)



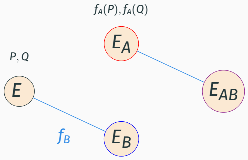
The attacks on Supersingular Isogeny Diffie-Hellman (SIDH)

Kani's lemma serves as a key ingredient for attacking the isogeny one-way function **with torsion point information**.

Setting Given E, E_A and interpolation data $P, Q, f_A(P), f_A(Q)$ with $\langle P, Q \rangle = E[d_A + d_B]$, find f_A.

Idea (Castryck-Decru, Maino-Martindale-Panny-Pope-Wesolowski, Robert)

1. Construct f_B to obtain an isogeny diamond.



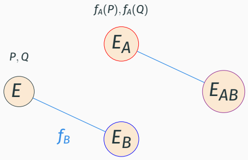
The attacks on Supersingular Isogeny Diffie-Hellman (SIDH)

Kani's lemma serves as a key ingredient for attacking the isogeny one-way function **with torsion point information**.

Setting Given E, E_A and interpolation data $P, Q, f_A(P), f_A(Q)$ with $\langle P, Q\rangle = E[d_A + d_B]$, find f_A.

Idea (Castryck-Decru, Maino-Martindale-Panny-Pope-Wesolowski, Robert)

1. Construct f_B to obtain an isogeny diamond.
2. Use Kani to obtain a product isogeny F.



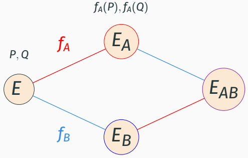
The attacks on Supersingular Isogeny Diffie-Hellman (SIDH)

Kani's lemma serves as a key ingredient for attacking the isogeny one-way function **with torsion point information**.

Setting Given E, E_A and interpolation data $P, Q, f_A(P), f_A(Q)$ with $\langle P, Q\rangle = E[d_A + d_B]$, find f_A.

Idea (Castryck-Decru, Maino-Martindale-Panny-Pope-Wesolowski, Robert)

1. Construct f_B to obtain an isogeny diamond.
2. Use Kani to obtain a product isogeny F.
3. Recover f_A from F.



Computational aspects of the attacks

$d_A + d_B \in \{2^n, 3^m\} \Rightarrow$ need $(2,2)$- and $(3,3)$-isogenies

Computational aspects of the attacks

$d_A + d_B \in \{2^n, 3^m\} \Rightarrow$ need $(2,2)$- and $(3,3)$-isogenies

$(2,2)$**-isogenies** $\rightarrow$ attack Bob's secret.

- Original implementations: Richelot isogenies
- Explicit formulas in Mumford/Kummer coordinates (Kunzweiler '2022)
- Explicit formulas in theta coordinates (Dartois-Maino-Pope-Robert '2023).

Computational aspects of the attacks

$d_A + d_B \in \{2^n, 3^m\} \Rightarrow$ need $(2,2)$- and $(3,3)$-isogenies

$(2,2)$**-isogenies** $\rightarrow$ attack Bob's secret.

- Original implementations: Richelot isogenies
- Explicit formulas in Mumford/Kummer coordinates (Kunzweiler '2022)
- Explicit formulas in theta coordinates (Dartois-Maino-Pope-Robert '2023).

$(3,3)$**-isogenies** $\rightarrow$ attack Alice's secret.

- First implementation (Decru-Kunzweiler '2023) optimizing formulas by Bruin-Flynn-Testa (2014)
- Formulas in theta coordinates (Costello-Santos-Smith '2024)

More dimensions!

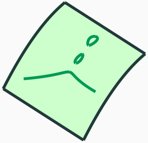
The 3-dimensional picture(s)

dimension 1
(abelian curves)

elliptic curve

dimension 2
(abelian surfaces)

product of elliptic curves



Jacobian of a genus-2 curve

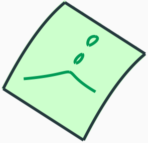
The 3-dimensional picture(s)

dimension 1
(abelian curves)

elliptic curve

dimension 2
(abelian surfaces)

product of elliptic curves



Jacobian of a genus-2 curve

dimension 3
(abelian threefolds)

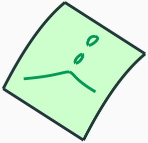
The 3-dimensional picture(s)

dimension 1
(abelian curves)

elliptic curve

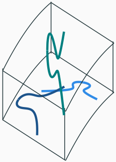
dimension 2
(abelian surfaces)

product of elliptic curves



Jacobian of a genus-2 curve

dimension 3
(abelian threefolds)

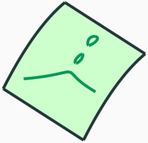


dimension 1
(abelian curves)

elliptic curve

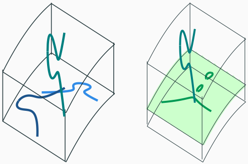
dimension 2
(abelian surfaces)

product of elliptic curves



Jacobian of a genus-2 curve

dimension 3
(abelian threefolds)



products

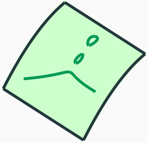
The 3-dimensional picture(s)

dimension 1
(abelian curves)

elliptic curve

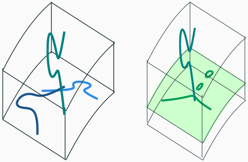
dimension 2
(abelian surfaces)

product of elliptic curves

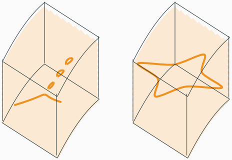


Jacobian of a genus-2 curve

dimension 3
(abelian threefolds)



products



Jacobians of genus-3 curves

Why do we need more dimensions in cryptography?

1. **for cryptanalysis**: The unconditional poly-time attack on SIDH (Robert) requires working in dimension 8.

Why do we need more dimensions in cryptography?

1. **for cryptanalysis**: The unconditional poly-time attack on SIDH (Robert) requires working in dimension 8.

$\Rightarrow$ new tool: HD representations!

HD representations

Any N-isogeny $f : E \to E'$ (of elliptic curves) has an efficient representation in dimension $d \in \{2, 4, 8\}$.
$\Rightarrow$ Evaluation in $O(\log^c(N))$ for some constant c.

Why do we need more dimensions in cryptography?

1. **for cryptanalysis**: The unconditional poly-time attack on SIDH (Robert) requires working in dimension 8.

$\Rightarrow$ new tool: HD representations!

HD representations

Any N-isogeny $f : E \to E'$ (of elliptic curves) has an efficient representation in dimension $d \in \{2, 4, 8\}$.
$\Rightarrow$ Evaluation in $O(\log^c(N))$ for some constant c.

2. **for constructive applications:**

- SQISignHD
- SQISign2D $\times 3$
- FESTA, QFESTA
- IS-CUBE
- POKE
- SCALLOP-HD
- HD VRF
- CLAPOTIS

since 2022!

Computations in arbitrary dimensions

A: principally polarized abelian variety of dimension g.

- ✗ Dimension $g > 3$: A generically not the Jacobian of a curve.
- ✓ The Kummer variety $K = A/\langle \pm 1 \rangle$ has a nice representation:

$$\theta : K \to \mathbb{P}^{2^g - 1}$$

given by theta coordinates.

Computations in arbitrary dimensions

A: principally polarized abelian variety of dimension g.

- ✗ Dimension $g > 3$: A generically not the Jacobian of a curve.
- ✓ The Kummer variety $K = A/\langle \pm 1 \rangle$ has a nice representation:

$$\theta : K \to \mathbb{P}^{2^g - 1}$$

  given by theta coordinates.

$\phi : A \to A'$: an $(\ell, \ldots, \ell)$-isogeny of p.p.a.v.

Computations in arbitrary dimensions

A: principally polarized abelian variety of dimension g.

- ✗ Dimension $g > 3$: A generically not the Jacobian of a curve.
- ✓ The Kummer variety $K = A/\langle \pm 1 \rangle$ has a nice representation:

$$\theta : K \to \mathbb{P}^{2^g - 1}$$

given by theta coordinates.

$\phi : A \to A'$: an $(\ell, \ldots, \ell)$-isogeny of p.p.a.v.

- $\ell = 2$: Algorithm by Robert (2023) in any dimension.
  - ✓ Implementations by Dartois, Maino, Pope, Robert ($g = 2$) and Dartois ($g = 4$)
  - ✗ dimensions $g = 3$ and $g > 4$ missing.
- $\ell \neq 2$ prime: Algorithms by Cosset, Lubicz, Robert in $\tilde{O}(\ell^g)$.
  - ✗ not yet optimized for crypto applications.

Conclusion

Exciting time for higher dimensions in isogeny-based cryptography.

What's next?

- Optimize higher dimensional computations.
- More applications of HD-representations.
- Exploit the full structure of higher dimensional isogeny graphs.
- Better understanding of higher dimensional isogeny graphs.

Conclusion

Exciting time for higher dimensions in isogeny-based cryptography.

What's next?

- Optimize higher dimensional computations.
- More applications of HD-representations.
- Exploit the full structure of higher dimensional isogeny graphs.
- Better understanding of higher dimensional isogeny graphs.

Thanks for your attention!