Efficient Computation of $(3^n, 3^n)$-isogenies

AfricaCrypt 2023, Sousse

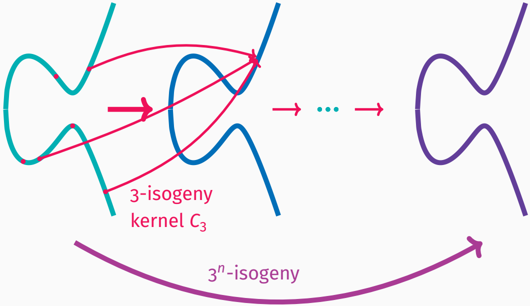
Thomas Decru[1] & Sabrina Kunzweiler[2]

July 21st, 2023

[1]imec-COSIC, KU Leuven, België
[2]Inria, IMB, Bordeaux, France

What are $(3^n, 3^n)$-isogenies?

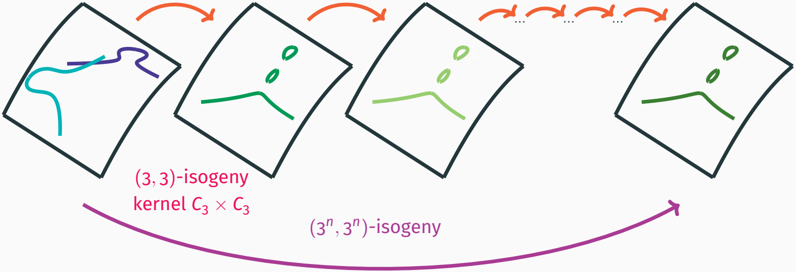
Dimension 1: Elliptic curves



- 3^n-isogeny: chain of 3-isogenies, kernel $K \cong C_{3^n}$.

What are $(3^n, 3^n)$-isogenies?

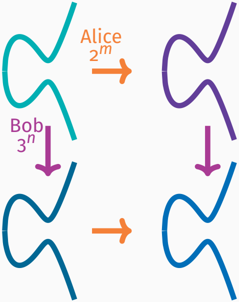
Dimension 2: Principally polarized abelian surfaces (p.p.a.s.)



- $(3^n, 3^n)$-isogeny: chain of $(3, 3)$-isogenies, kernel $K \cong C_{3^n} \times C_{3^n}$

Why are $(3^n, 3^n)$-isogenies interesting (for crypto)?

SIDH



EuroCrypt 2023:

- Key recovery attack on SIDH (Castryk-Decru; Maino-Martindale-Panny-Pope-Wesolowski; Robert)
- Algorithmic prerequisite: isogeny computations in higher dimension.

Retrieving Bob's secret

▷ based on $(2^m, 2^m)$-isogenies

▷ 9 sec (SIKEp217) - 1 h (SIKEp751)

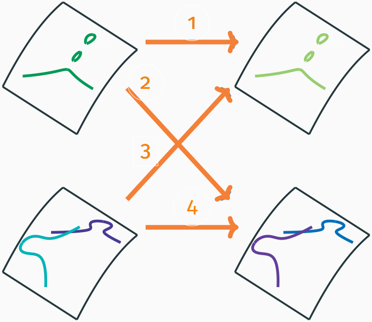
Retrieving Alice's secret

▷ based on $(3^n, 3^n)$-isogenies

▷ timing: **?**

State-of-the-art of $(3,3)$-formulae

Four types of $(3,3)$-isogenies

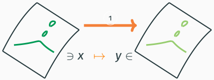


1. Generic:
   ✓ Explicit Formulae [Bruin-Flynn-Testa '14]
   ✗ Non-optimized (37.500 mult. for point evaluation)
2. Splitting and 3. Gluing:
   ✓ Compact parametrization [Bröker, Howe, Lauter, Stevenhagen '15]
   ✗ Explicit maps only on the level of curves (not surfaces)
4. Product:
   ✗ not explicitly discussed anywhere

Our Contributions

Generic Case (1.):

BFT provide a three-parameter (r, s, t) parametrization.



Isogeny evaluation $x \mapsto y$ with $x = (x_1, x_2, x_3, x_4)$ is represented by matrix multiplication:[1]

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} a_1 & \dots & a_{20} \\ \vdots & & \vdots \\ d_1 & \dots & d_{20} \end{pmatrix} \cdot \begin{pmatrix} x_4^3 \\ x_4^2 x_3 \\ \vdots \\ x_1^3 \end{pmatrix}$$

Formulae for the matrix entries in terms of r, s, t are known, but expensive!

Tricks for simplifying the formulae:

- Find 282 (at most quartic) relations among matrix entries and curve coefficients.
- Formulate the problem as a Mixed Integer Linear Program (MILP).

[1]Technical remark: Computations are done on the Kummer surface.

Our Contributions

Example: Matrix entry a_5 (coefficient of $x_3^2 x_4$)

```
(4) * (r^6*s^4*t^2 + r^6*s^4*t - 9*r^5*s^4*t^2 + 3*r^4*s^4*t^3 -
r^3*s^4*t^4 + r^6*s^4 + 2*r^6*s^3*t - 9*r^5*s^4*t + 39*r^4*s^4*t^2 -
29*r^3*s^4*t^3 + 18*r^2*s^4*t^4 - 6*r*s^4*t^5 + s^4*t^6 - r^6*s^3 -
9*r^5*s^3*t + 3*r^4*s^4*t + 3*r^4*s^3*t^2 - 29*r^3*s^4*t^2 -
2*r^3*s^3*t^3 + 9*r^2*s^4*t^3 - 3*r*s^4*t^4 + r^6*s^2 + 39*r^4*s^3*t -
r^3*s^4*t - 57*r^3*s^3*t^2 + 18*r^2*s^4*t^2 + 51*r^2*s^3*t^3 -
3*r*s^4*t^3 - 21*r*s^3*t^4 + s^4*t^4 + 4*s^3*t^5 - 3*r^4*s^3 -
3*r^4*s^2*t - 28*r^3*s^3*t + 33*r^2*s^3*t^2 - 6*r*s^4*t^2 -
18*r*s^3*t^3 + 2*s^3*t^4 + 3*r^4*s^2 + r^3*s^3 - 28*r^3*s^2*t +
15*r^2*s^3*t + 48*r^2*s^2*t^2 - 15*r*s^3*t^2 + s^4*t^2 - 27*r*s^2*t^3
+ 5*s^3*t^3 + 6*s^2*t^4 - 3*r^4*s + 2*r^3*s*t + 21*r^2*s^2*t -
3*r*s^3*t - 24*r*s^2*t^2 + 2*s^3*t^2 + 5*s^2*t^3 + 15*r^2*s*t -
9*r*s^2*t - 15*r*s*t^2 + 6*s^2*t^2 + 4*s*t^3 + r^3 - 9*r*s*t + s^2*t +
4*s*t^2 - 3*r*t + 2*s*t + t^2 + t)
```

Original formula with r, s, t.

$\Rightarrow$

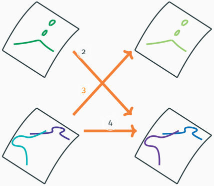
$$\boxed{4(f_6\Delta - g_6).}$$

New formula with curve coefficients $f_0, \ldots, f_6$, $g_0, \ldots, g_6$.

In total: Our new formulae reduce the number of multiplications by 94 %. ✓

Our Contributions

All other cases (2.-4.):



✓ We derive compact and explicit formulae on the level of Kummer surfaces, Jacobians or elliptic curves (as needed).

Code https://github.com/KULeuven-COSIC/3_3_isogenies

- Implementation of our formulae and the resulting algorithm to compute $(3^n, 3^n)$-isogenies in magma.
- Symbolic verification of our results.

Applications

Cryptanalysis

- SIDH attack: We can now also retrieve Alice's secret key!
  Only 11 seconds for SIKEp751 parameters.

New Protocols

- 2-dimensional CGL hash function.
- Constructive use of the SIDH attack, such as:
  FESTA, SQISign-HD, ...

Thank you!