Higher-dimensional abelian varieties for public-key cryptography

Maria Corte-Real Santos

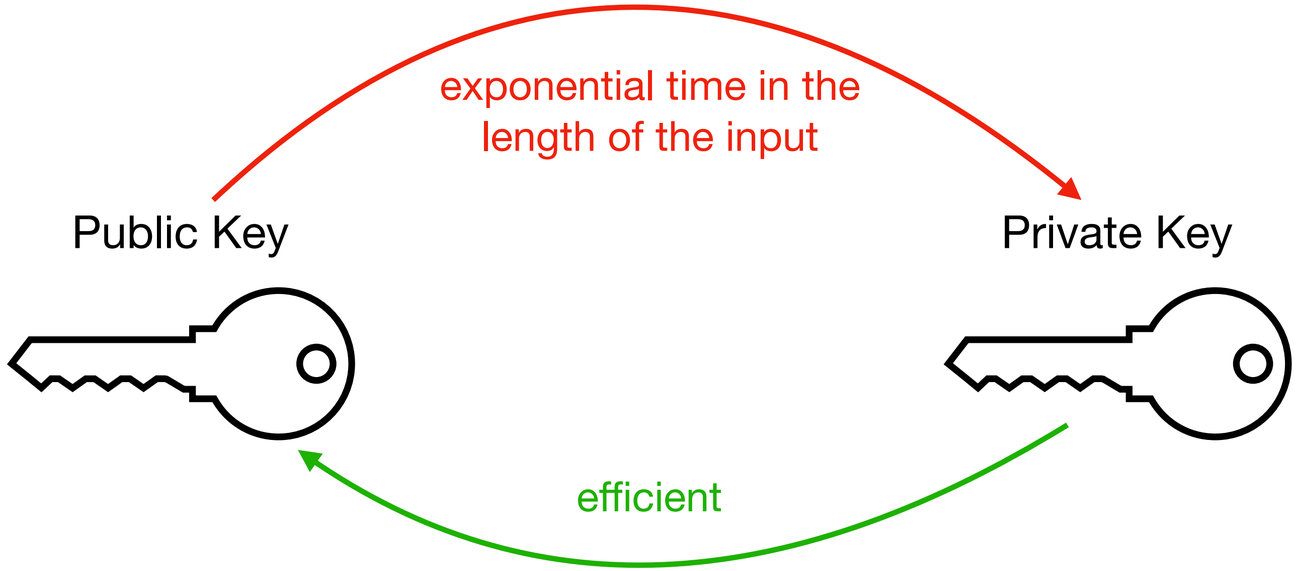
- Since Jan ’25: Postdoc at ENS de Lyon (France)
- Dec ’24: PhD at University College London (United Kingdom)
- August ’20: MMath at University of Cambridge (United Kingdom)

Higher-dimensional abelian varieties for public-key cryptography

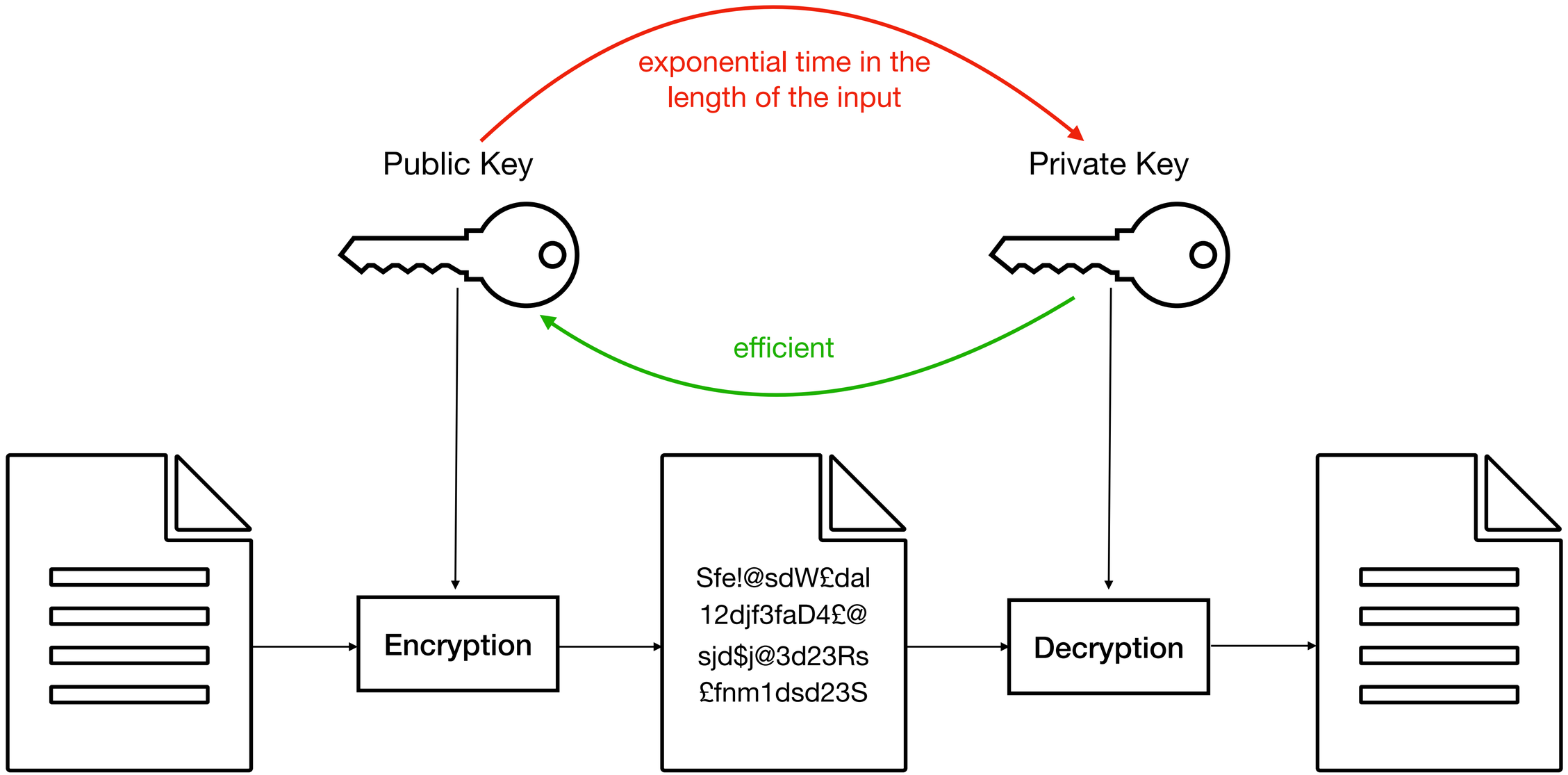
Maria Corte-Real Santos

- Since Jan ’25: Postdoc at ENS de Lyon (France)
- Dec ’24: PhD at University College London (United Kingdom)
- August ’20: MMath at University of Cambridge (United Kingdom)

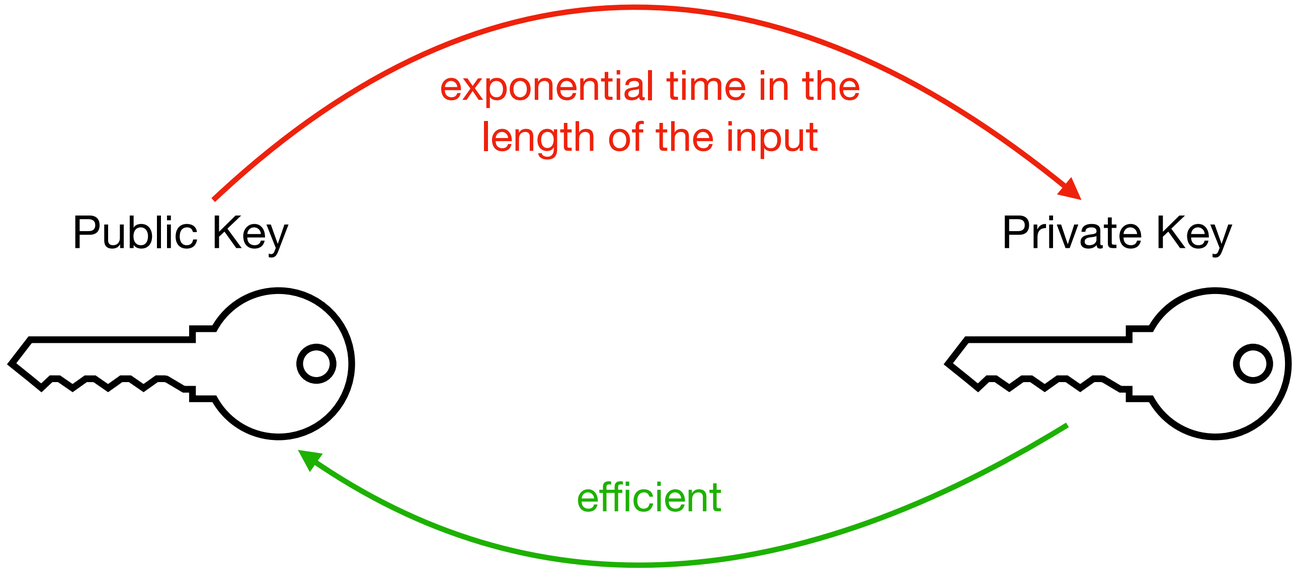
Public key cryptography



Public key cryptography



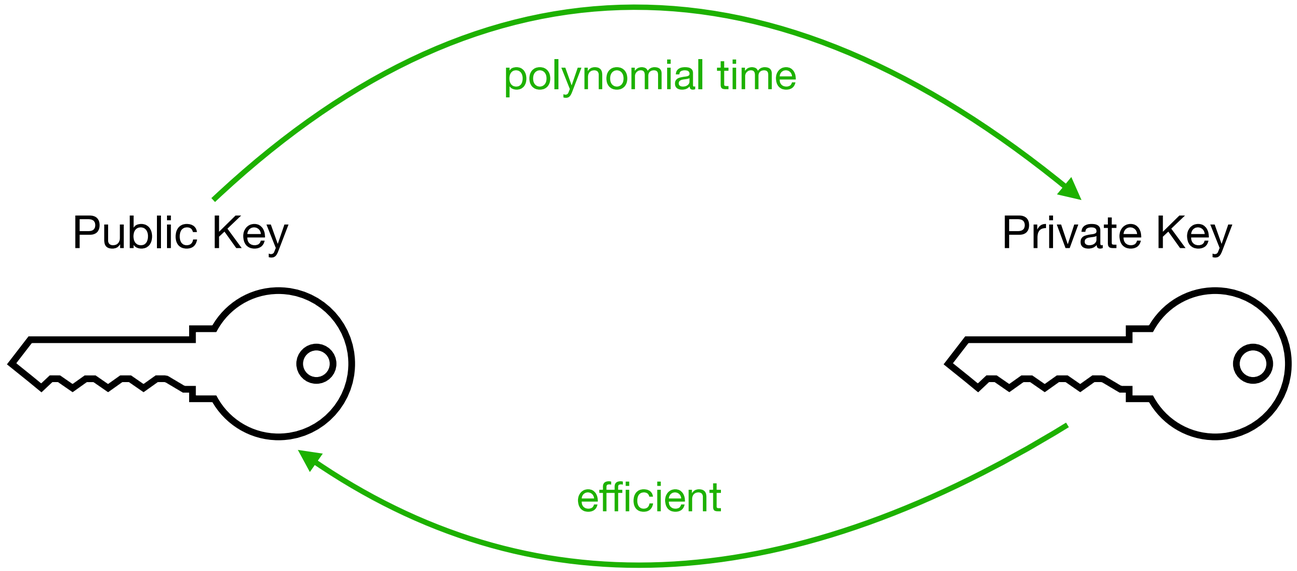
Public key cryptography



Classical hard problems:

- The discrete logarithm problem
- Integer factorisation

Public key cryptography



Classical hard problems:

- The discrete logarithm problem
- Integer factorisation

These are easy to solve for **quantum computers** (shown by Shor in 1995).

Post-quantum candidate: isogenies

Public

Supersingular elliptic curves

$E_1, E_2 / \bar{\mathbb{F}}_p$

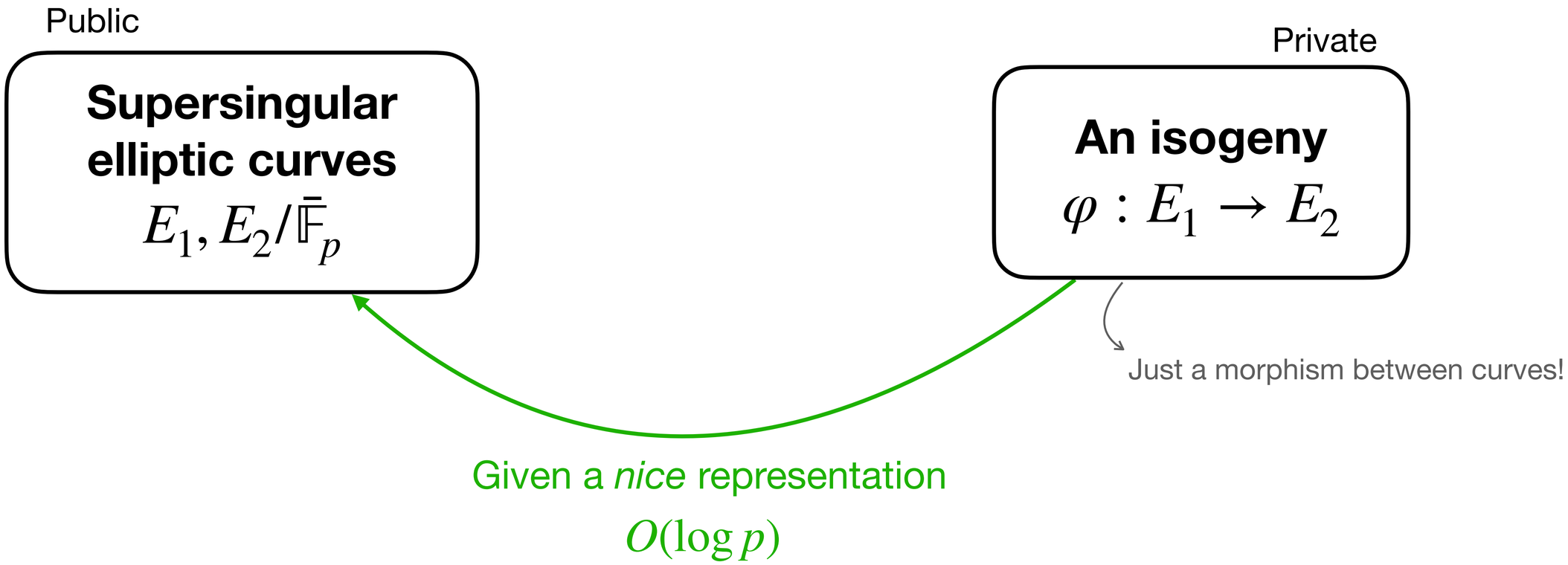
Private

An isogeny

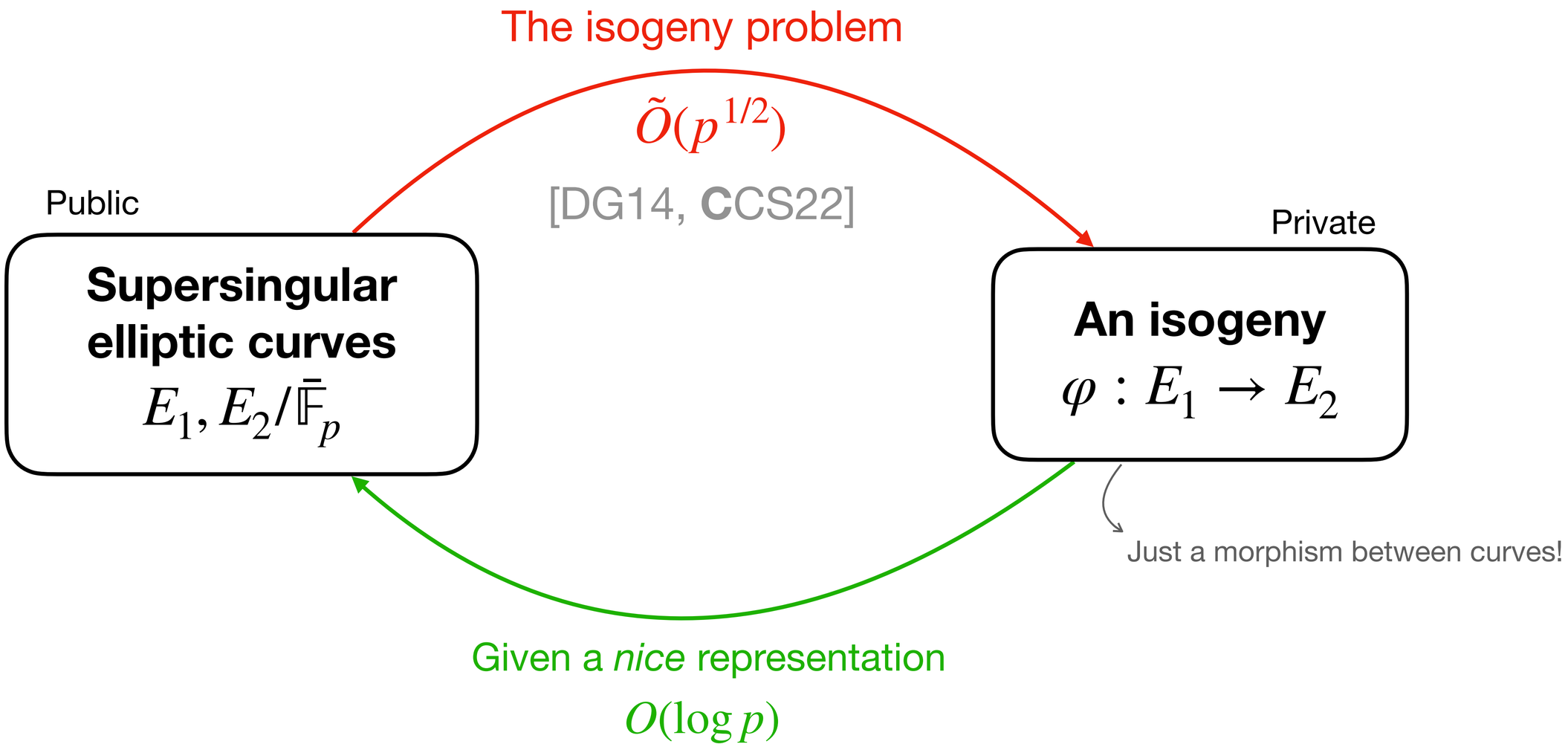
$\varphi : E_1 \to E_2$

Just a morphism between curves!

Post-quantum candidate: isogenies



Post-quantum candidate: isogenies



Hard problems in isogeny-based cryptography

The isogeny problem: Given supersingular elliptic curves E_1, E_2 defined over $\bar{\mathbb{F}}_p$, compute an isogeny $\varphi : E_1 \to E_2$

Hard problems in isogeny-based cryptography

The isogeny problem: Given supersingular elliptic curves E_1, E_2 defined over $\bar{\mathbb{F}}_p$, compute an isogeny $\varphi : E_1 \to E_2$

The endomorphism ring problem: Given a supersingular elliptic curve E defined over $\bar{\mathbb{F}}_p$, compute the endomorphism ring $\mathrm{End(E)}$.

Hard problems in isogeny-based cryptography

The isogeny problem: Given supersingular elliptic curves E_1, E_2 defined over $\bar{\mathbb{F}}_p$, compute an isogeny $\varphi : E_1 \to E_2$

[Wes22]

The endomorphism ring problem: Given a supersingular elliptic curve E defined over $\bar{\mathbb{F}}_p$, compute the endomorphism ring $\mathrm{End(E)}$.

Hard problems in isogeny-based cryptography

The endomorphism ring problem: Given a supersingular elliptic curve E defined over $\bar{\mathbb{F}}_p$, compute the endomorphism ring $\mathrm{End(E)}$.

Hard problems in isogeny-based cryptography

The endomorphism ring problem: Given a supersingular elliptic curve E defined over $\bar{\mathbb{F}}_p$, compute the endomorphism ring $\mathrm{End}(\mathrm{E})$.

Underlies the security of **SQIsign**

Hard problems in isogeny-based cryptography

The endomorphism ring problem: Given a supersingular elliptic curve E defined over $\bar{\mathbb{F}}_p$, compute the endomorphism ring $\mathrm{End}(\mathrm{E})$.

Underlies the security of **SQIsign**

Contributions:

- A member of the submission team to the NIST post-quantum standardisation competition, now in Round 2
- Improving the efficiency without compromising security

[BBC**C**+23, **C**EMR24, **C**EMR24, B**C**EI+25, **C**K26]

Best early career award at Eurocrypt 2024

Hard problems in isogeny-based cryptography

The endomorphism ring problem: Given a supersingular elliptic curve E defined over $\bar{\mathbb{F}}_p$, compute the endomorphism ring $\mathrm{End}(\mathrm{E})$.

Underlies the security of **SQIsign**

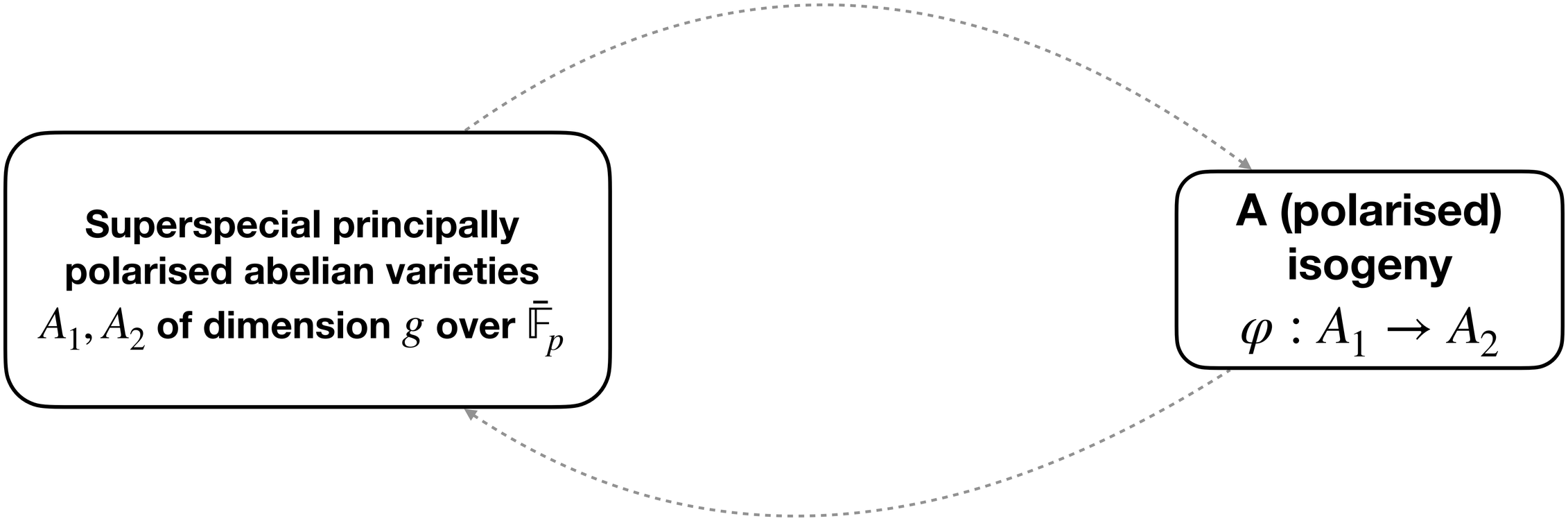
Contributions:

- A member of the submission team to the NIST post-quantum standardisation competition, now in Round 2
- Improving the efficiency without compromising security

  [BBC**C**+23, **C**EMR24, **C**EMR24, B**C**EI+25, **C**K26]
- Implementations of algorithms in Python, SageMath, Magma, C and C++

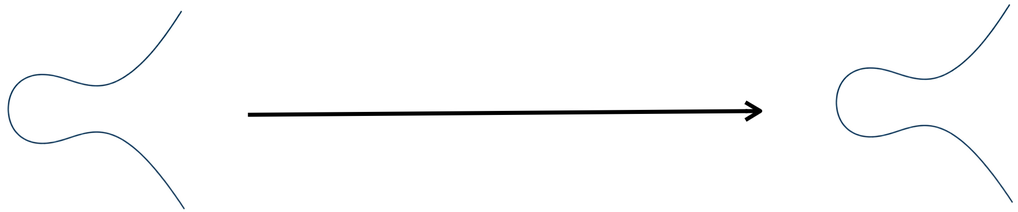
Moving to higher dimensions

Moving to higher dimensions

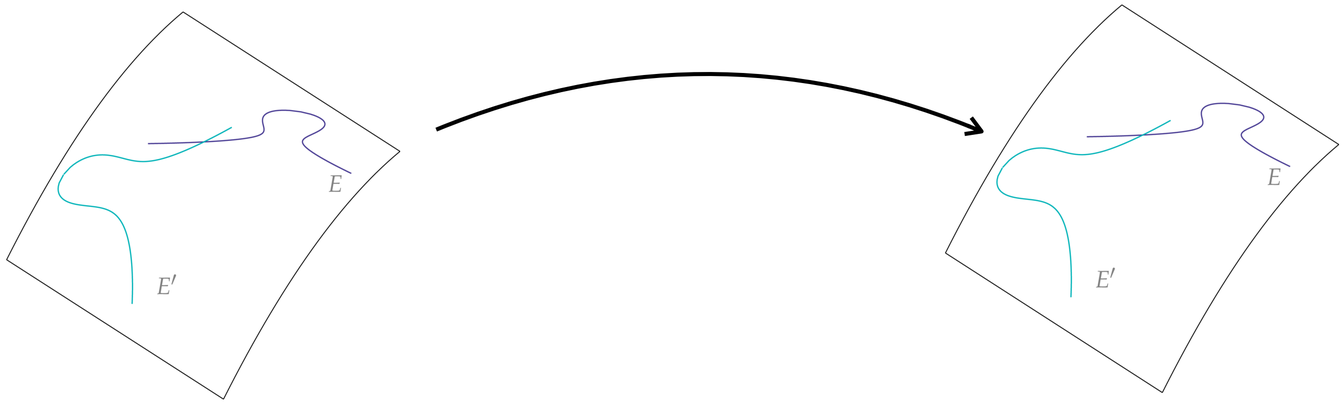


Why?

The one-dimensional isogeny of **any degree**

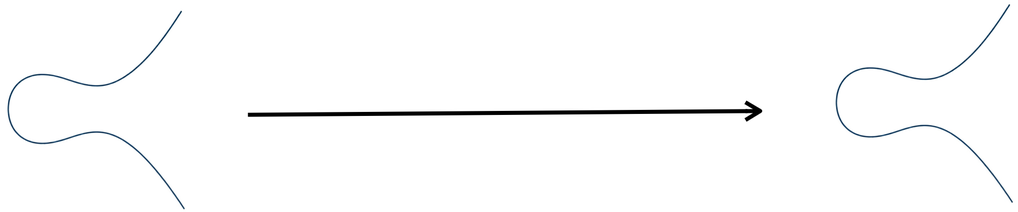


can be embedded into a higher-dimensional isogeny of **controlled degree**

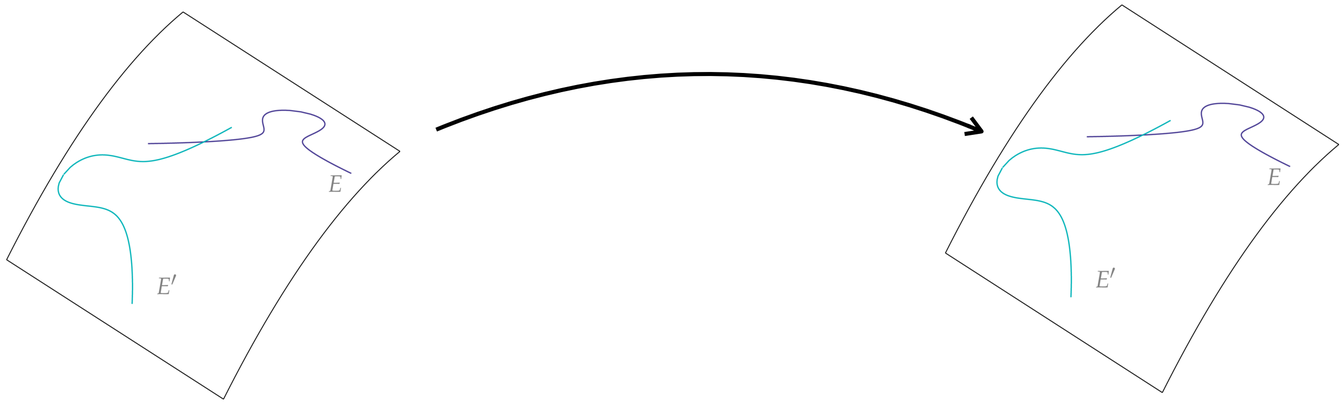


Why?

The one-dimensional isogeny of **any degree**



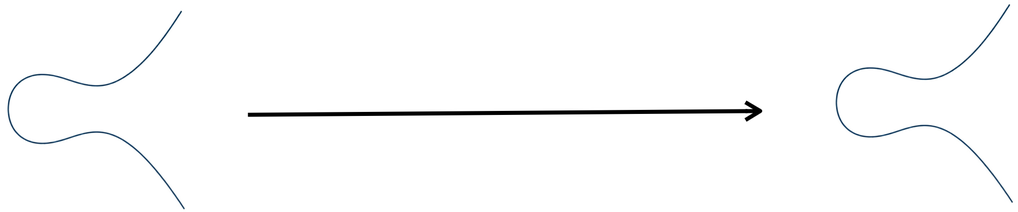
can be embedded into a higher-dimensional isogeny of **controlled degree**



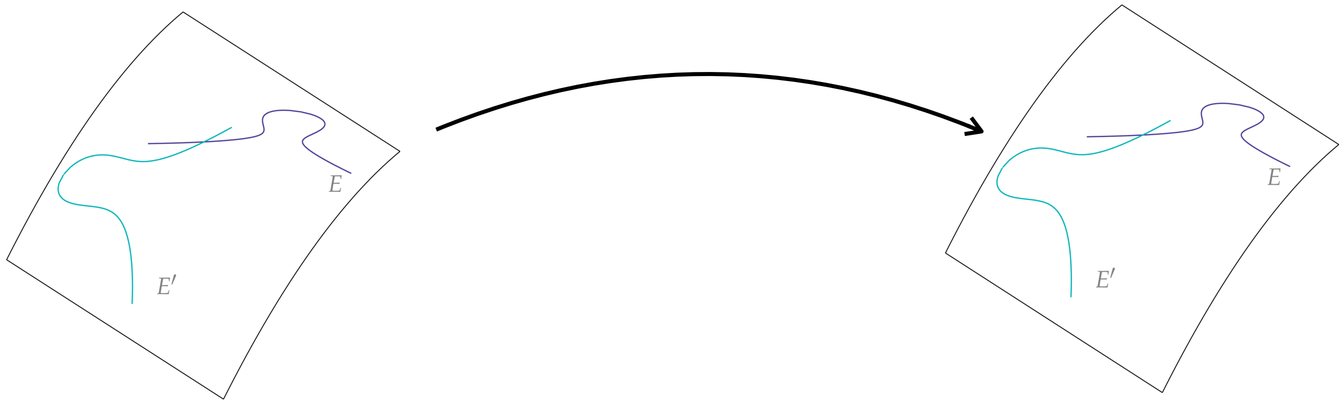
Higher dimensional isogenies are crucial to understand the **security** of the isogeny problem in dimension 1 [CD23, MMPP+23, Rob23].

Why?

The one-dimensional isogeny of **any degree**



can be embedded into a higher-dimensional isogeny of **controlled degree**



Higher dimensional isogenies are crucial to understand the **security** of the isogeny problem in dimension 1 [CD23, MMPP+23, Rob23].

They are also used to improve **computations** in dimension 1 (e.g., [B**C**EI+25, BBC**C**+25])

Research Questions

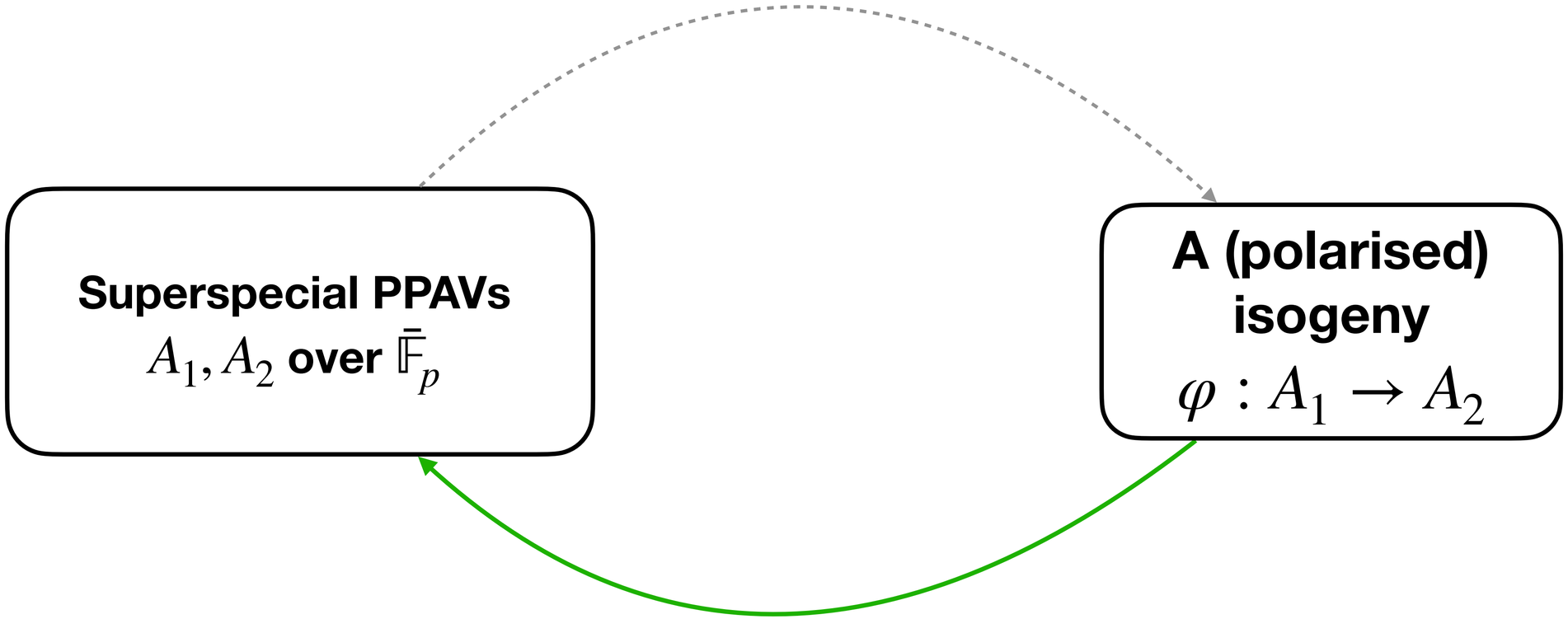
Expanding the computational toolbox

1. Efficient computation of higher dimensional isogenies

   Informed by joint works with Costello and Smith (2024) and Flynn (2025)

2. New tools for higher-dimensional representations

Moving to higher dimensions



Research Questions

Expanding the computational toolbox

1. Efficient computation of higher dimensional isogenies

   Informed by joint works with Costello and Smith (2024) and Flynn (2025)

2. New tools for higher-dimensional representations

Exploring the foundations

3. Study the hardness of the isogeny problem in higher dimensions

   Informed by joint works with Costello and Frengley (2024, 2025)

Research Questions

Expanding the computational toolbox

1. Efficient computation of higher dimensional isogenies

   Informed by joint works with Costello and Smith (2024) and Flynn (2025)

2. New tools for higher-dimensional representations

Exploring the foundations

3. Study the hardness of the isogeny problem in higher dimensions

   Informed by joint works with Costello and Frengley (2024, 2025)

4. Study relationships between the underlying hard problems

Recall in dimension 1

Recall in dimension 1

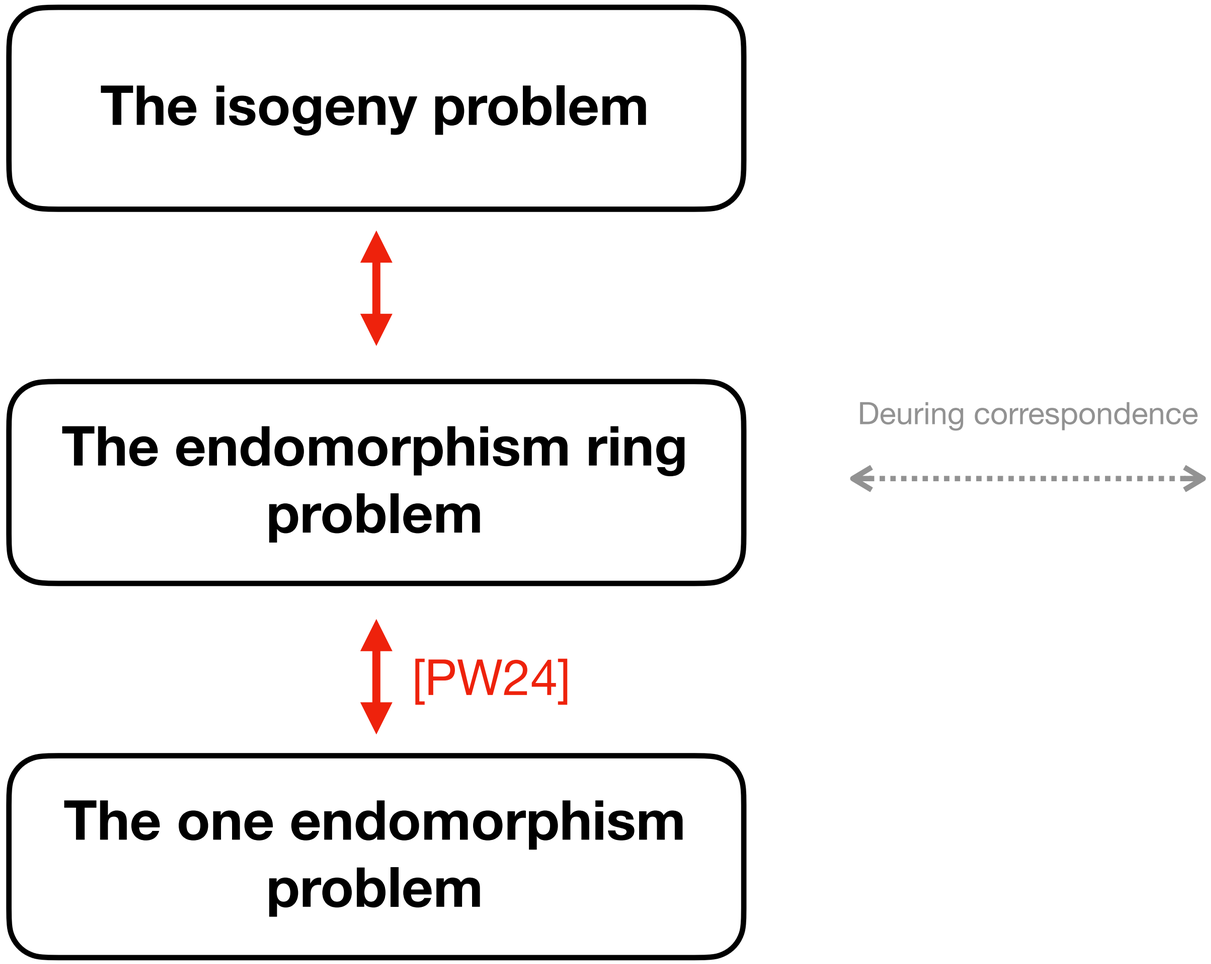
The isogeny problem

Recall in dimension 1

The isogeny problem

The endomorphism ring problem

Recall in dimension 1



Deuring correspondence

Recall in dimension 1

The isogeny problem

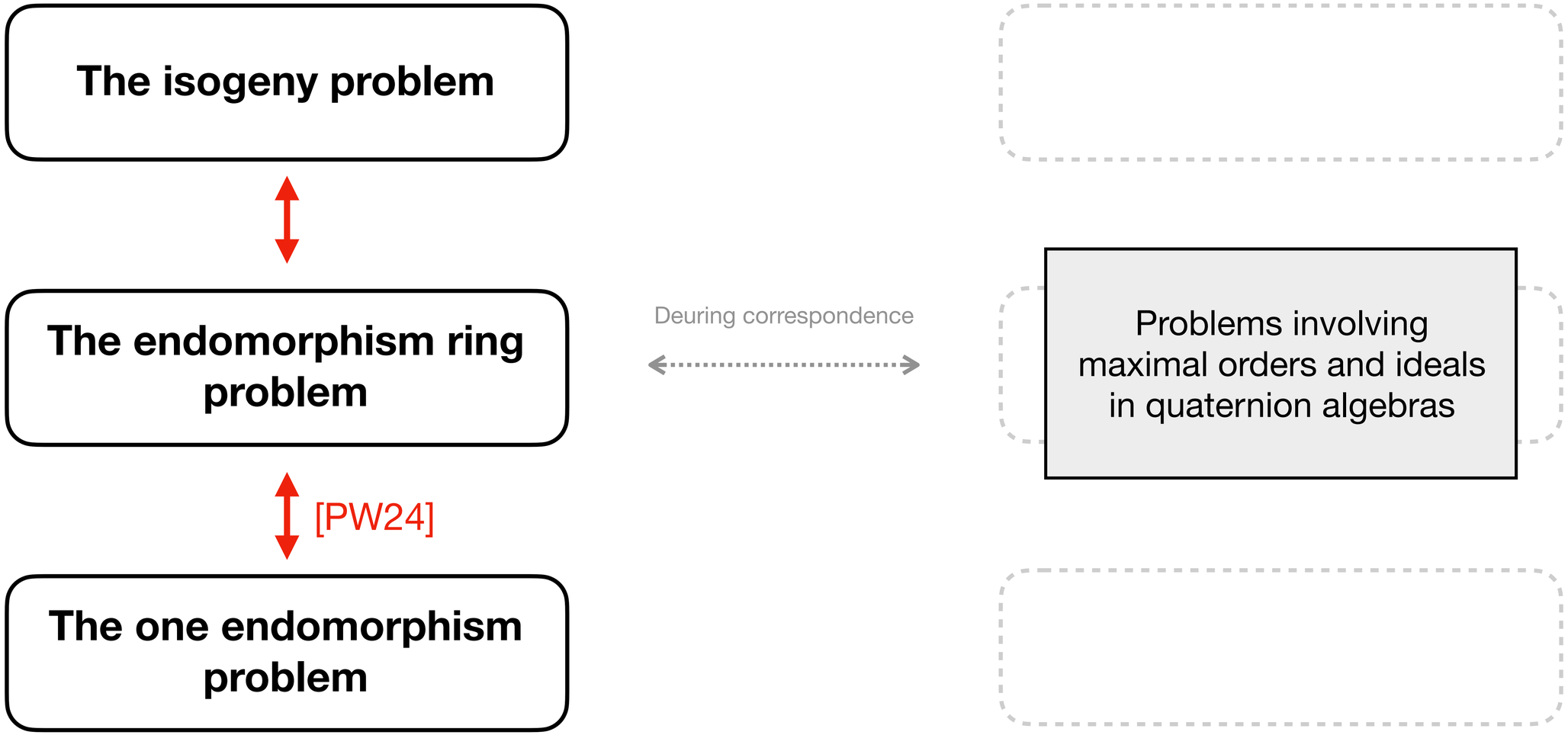
The endomorphism ring problem

Deuring correspondence

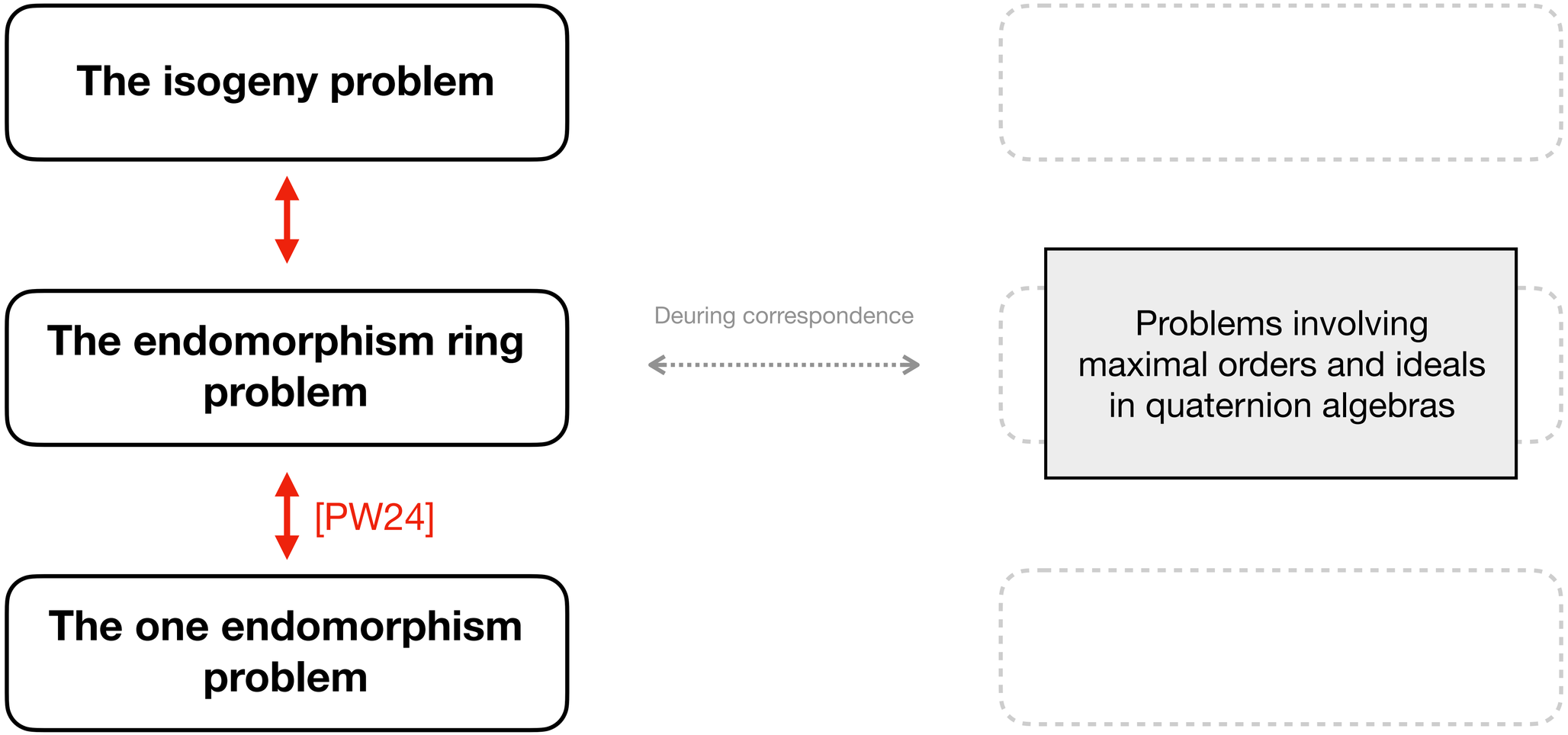
[PW24]

The one endomorphism problem

Recall in dimension 1



Recall in dimension 1



Relationships studied in depth in e.g., [EHLM+18, W22, PW24, HW25]

Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension

Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension

The isogeny problem

Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension

The isogeny problem

The endomorphism ring problem

Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension

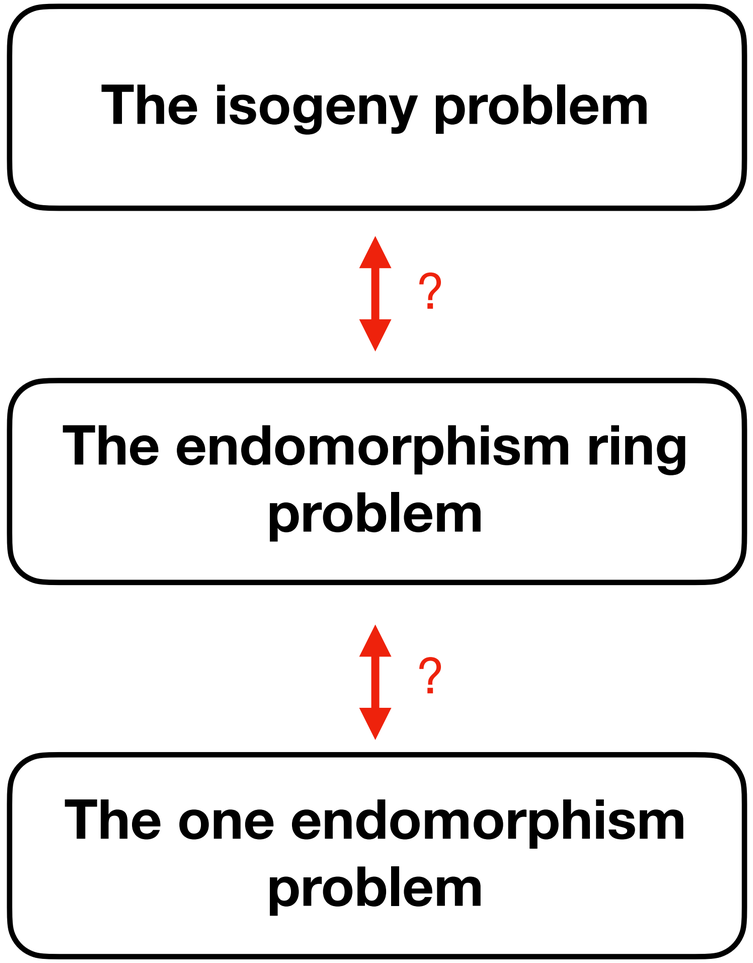
The isogeny problem

The endomorphism ring problem

The one endomorphism problem

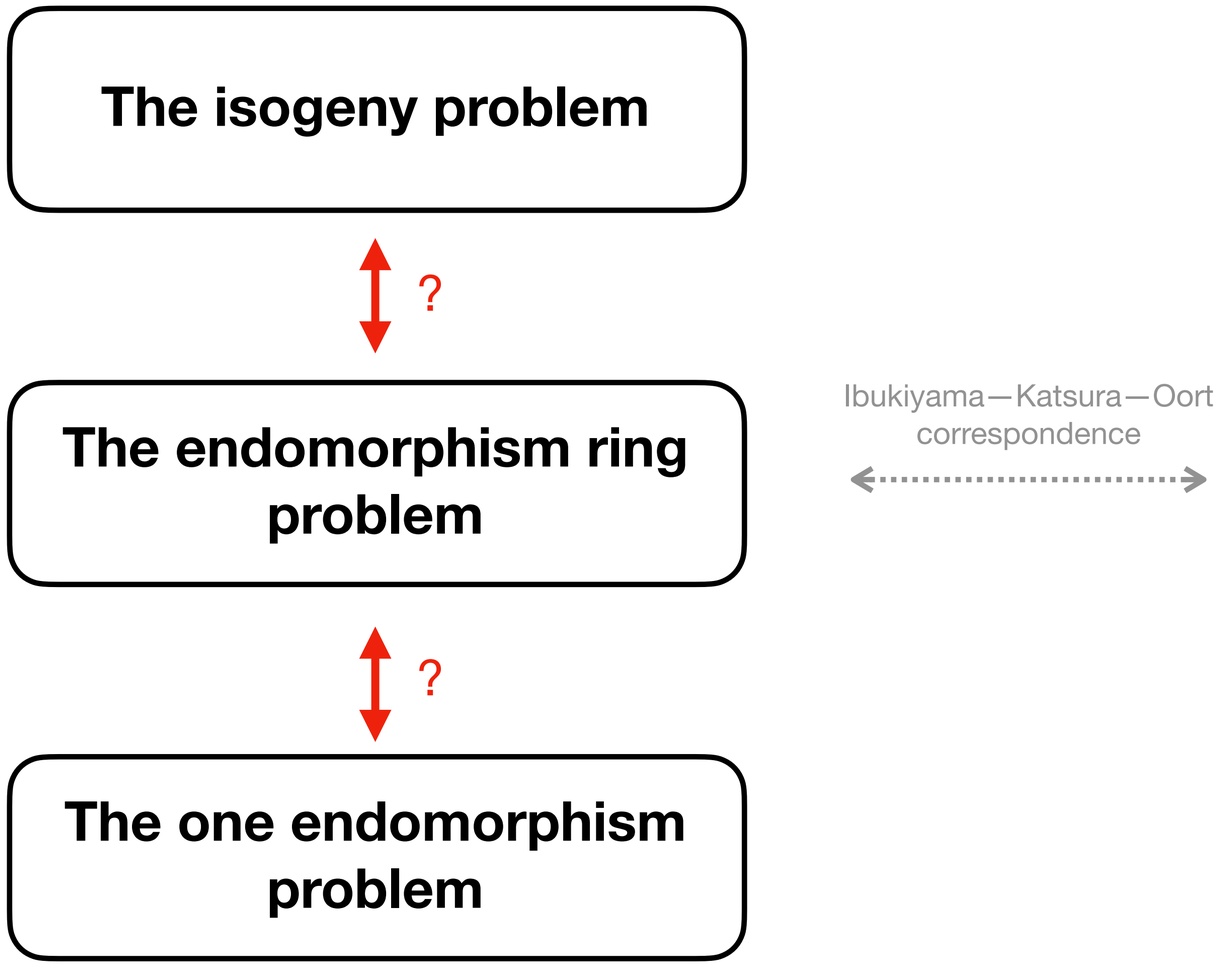
Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension



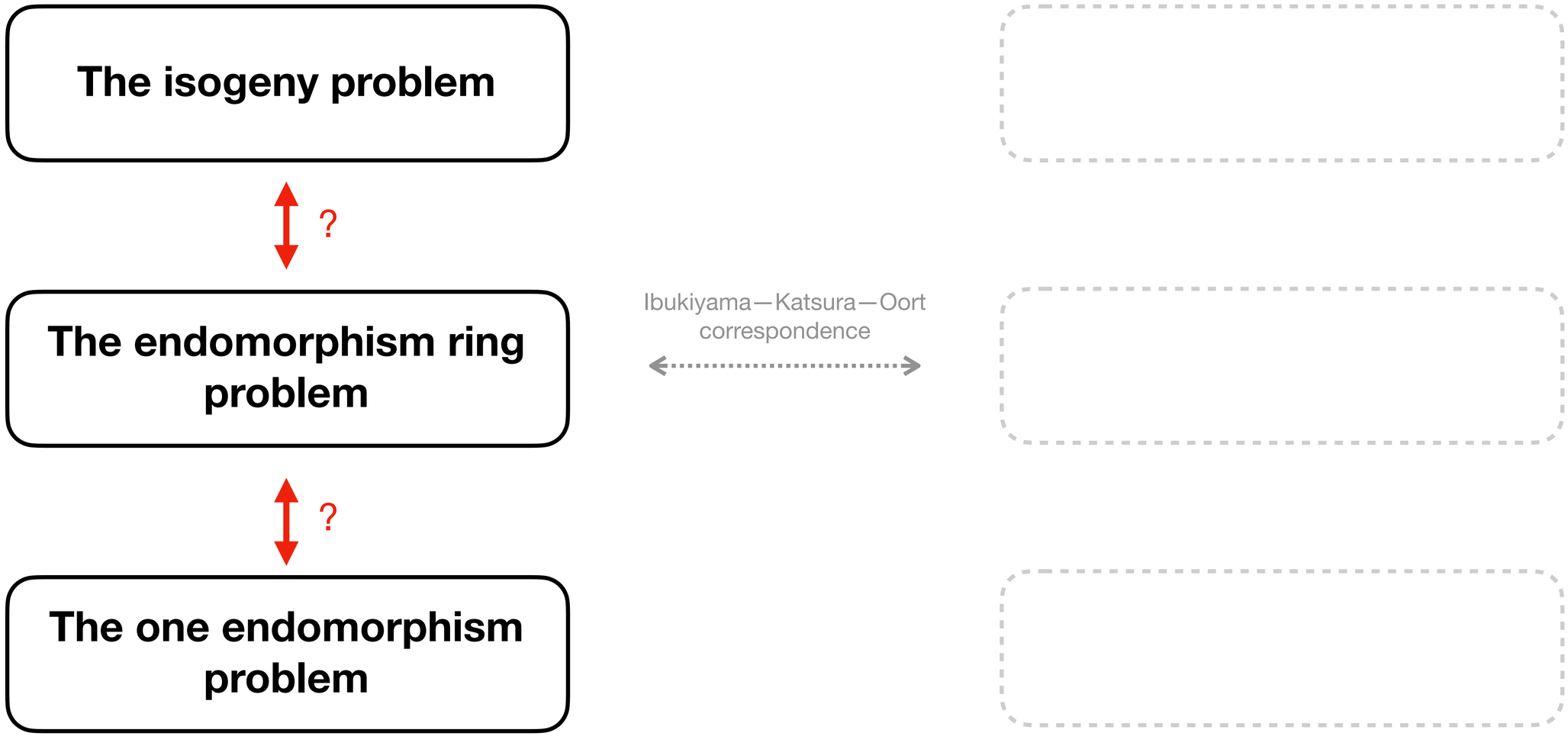
Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension



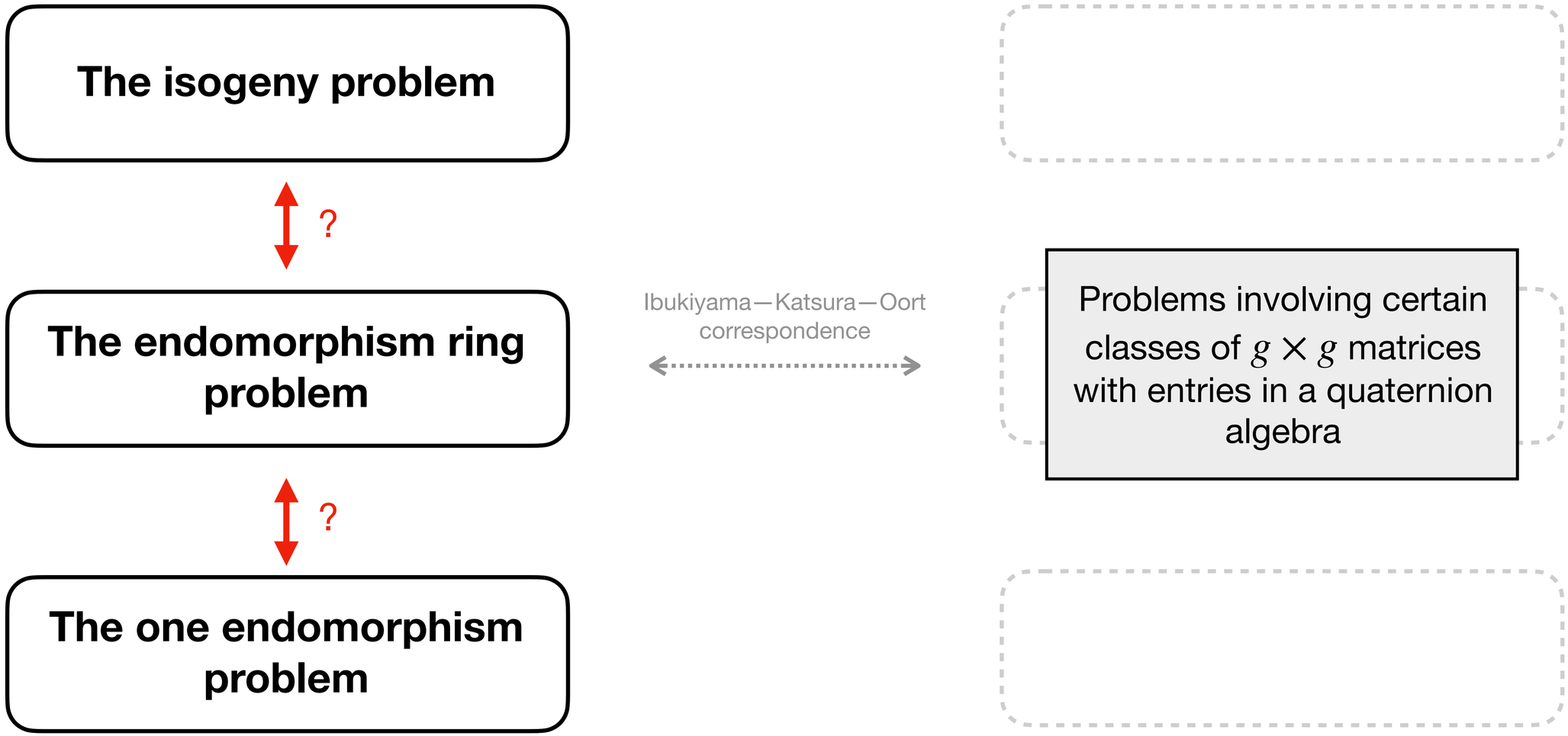
Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension



Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension



Hard problems in higher-dimensions

All the problems we've discussed naturally generalise to higher dimension

The isogeny problem

?

The endomorphism ring problem

Ibukiyama—Katsura—Oort correspondence

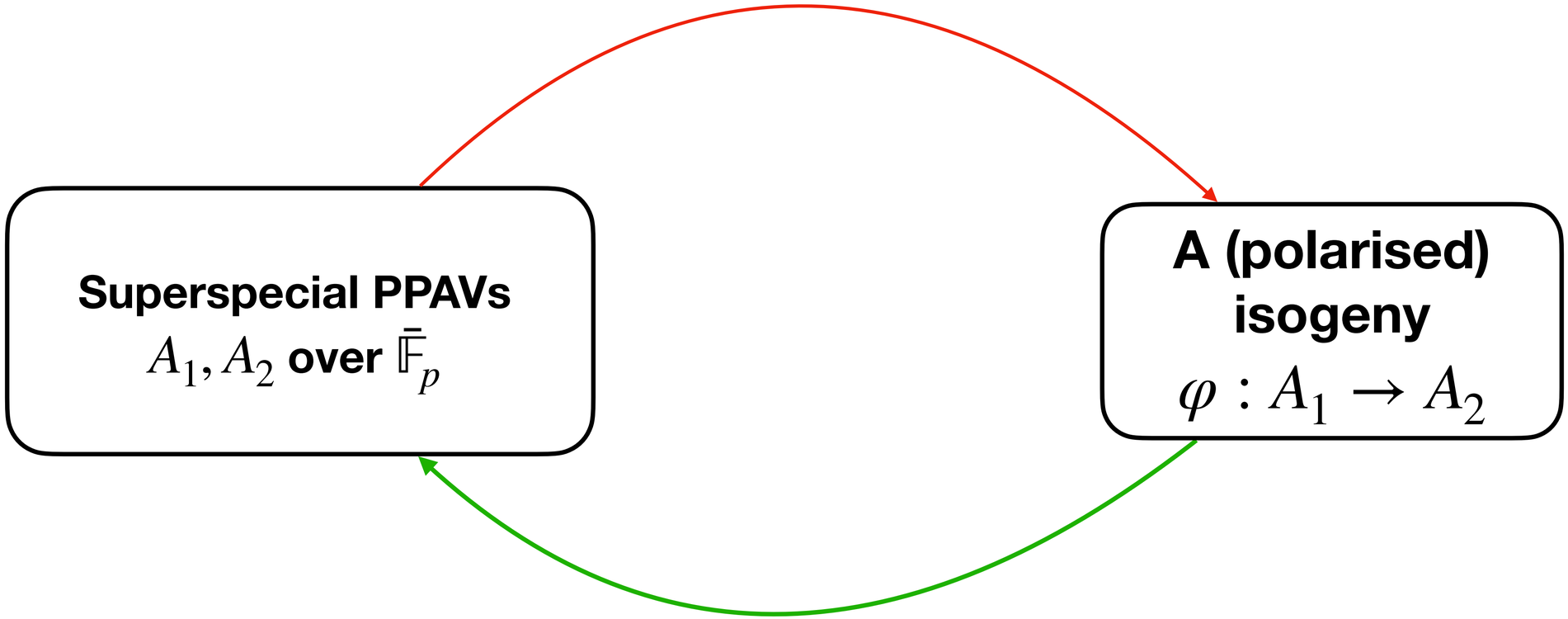
Problems involving certain classes of $g \times g$ matrices with entries in a quaternion algebra

?

The one endomorphism problem

I aim to build the landscape of these problems in dimension $g \geq 2$.

Moving to higher dimensions



Higher-dimensional abelian varieties for public-key cryptography

PROJECT GOALS

Expanding the computational toolbox

1. Improve the efficiency of computing higher dimensional isogenies
2. Build more tools for higher-dimensional representations

Exploring the foundations

3. Study the hardness of the isogeny problem in higher dimensions
4. Study relationships between the underlying hard problems

INTEGRATION INTO LABS

1. Équipe de Théorie des Nombres de l'UMPA, Lyon
2. Équipe Théorie des Nombres de l'IMB, Bordeaux
3. Équipe de Groupe Arithmétique, Géométrie, Logique et Représentations de l'I2M, Marseille

UPDATES

1. PEPS JCJC 2026: awarded 2000€
2. New publication '*Return of the Kummer: a toolbox for genus 2 cryptography*'

Merci!

My (joint) works referenced

[BBCC+25] A. Basso, G. Borin, W. Castryck, M. Corte-Real Santos, R. Invernizzi, A. Leroux, L. Maino, F. Vercauteren, B. Wesolowski. “PRISM: Simple And Compact Identification and Signatures From Large Prime Degree Isogenies”. In Public- Key Cryptography - PKC 2025, pages 300-332. Springer, 2025. **Best paper award.**

[BCEI+25] G. Borin, M. Corte-Real Santos, J. K. Eriksen, R. Invernizzi, M. Mula, S. Schaeffler, F. Vercauteren. “Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies”. In Advances in Cryptology — Asiacrypt 2025, pages 174-205. Springer, 2025.

[CCS22] M. Corte-Real Santos, C. Costello, and J. Shi. “Accelerating the Delfs–Galbraith Algorithm with Fast Subfield Root Detection”. In Advances in Cryptology - CRYPTO 2022, pages 285-314. Springer, 2022.

[CEMR24] M. Corte-Real Santos, J. K. Eriksen, M. Meyer, and K. Reijnders. “AprèsSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing”. In Advances in Cryptology - EUROCRYPT 2024, pages 63-93. Springer, 2024. **Best early career paper award.**

My (joint) works referenced

[CCF24] M. Corte-Real Santos, C. Costello, and S. Frengley. “An Algorithm for Efficient Detection of (N,N)-Splittings and Its Application to the Isogeny Problem in Dimension 2”. In Public-Key Cryptography - PKC 2024, pages 157-189. Springer, 2024. **Best paper award.**

[CF25] M. Corte-Real Santos, and E. V. Flynn. “Isogenies on Kummer Surfaces”. Mathematics of Computation 94. American Mathematical Society, 2025.

[CCS25] M. Corte-Real Santos, C. Costello, and B. Smith. “Efficient (3, 3)-isogenies on fast Kummer surfaces”. Research in Number Theory 11, 25. Springer Nature, 2025. Presented at the Sixteenth Algorithmic Number Theory Symposium (ANTS XVI).

[CCF24] M. Corte-Real Santos, C. Costello, and S. Frengley. “Efficient Algorithms for the Detection of (N,N)-Splittings and Endomorphisms”. Journal of Cryptology 39, 2. Springer Nature, 2026

Other works referenced

[CD23] W. Castryck and T. Decru. “An Efficient Key Recovery Attack on SIDH”. In Advances in Cryptology — EUROCRYPT 2023, pages 423-447. Springer, 2023.

[DG24] C. Delfs and S. D. Galbraith. “Computing isogenies between supersingular elliptic curves over Fp”. In: DCC 78.2 (2016), pages 425–440.

[EHLM+18] K. Eisenträger, S. Hallgren, K. E. Lauter, T. Morrison, and C. Petit. “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions”. In Advances in Cryptology — EUROCRYPT 2018, pages 329-368. Springer, 2018.

[HW25] A. Herlédan Le Merdy and B. Wesolowski. “Unconditional foundations for supersingular isogeny-based cryptography”. In Theory of Cryptology — TCC 2025, pages 266-297. Springer, 2025.

Other works referenced

[MMPP+23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. “A Direct Key Recovery Attack on SIDH”. In Advances in Cryptology — EUROCRYPT 2023, pages 448-471. Springer, 2023.

[PW24] A. Page and B. Wesolowski. “The Supersingular Endomor- phism Ring and One Endomorphism Problems are Equivalent”. In Advances in Cryptology — EUROCRYPT 2024, pages 388-417. Springer, 2024.

[Rob23] D. Robert. “Breaking SUCH in Polynomial Time”. In Advances in Cryptology — EUROCRYPT 2023, pages 472-503. Springer, 2023.

[Wes22] B. Wesolowski. “The supersingular isogeny path and endomorphism ring problems are equivalent”. FOCS 2022, pages 1100-1111. IEEE Computer Society Press, 2022.

Why me?

Experience

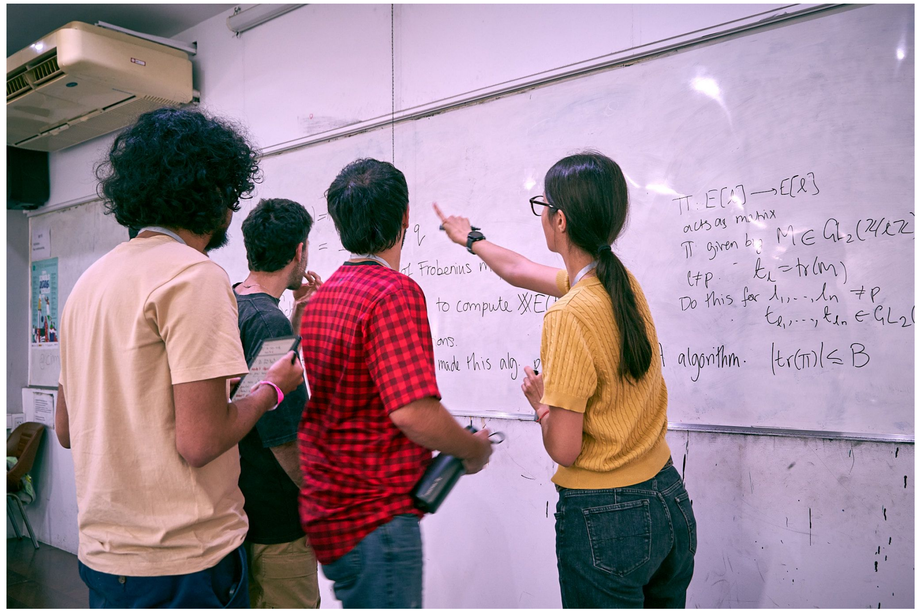
- Multiple publications on computational aspects of higher dimensional abelian varieties (e.g., MathComp, ANTS, CRYPTO).
- 2 Best Paper awards, and 1 Best Early-Career Paper award.

International Network

- PhD in the United Kingdom, now working in France
- Internship at Microsoft Research, Seattle
- Ongoing collaborations with researchers throughout France, Europe, USA, and Australia.

Active in the community

- Invited lecturer at a CIMPA school
- Co-organiser of an online seminar series (200+ members)
- Collegial Council member of the Women and Allies in Cryptography Association.



Credit: Annamaria Iezzi