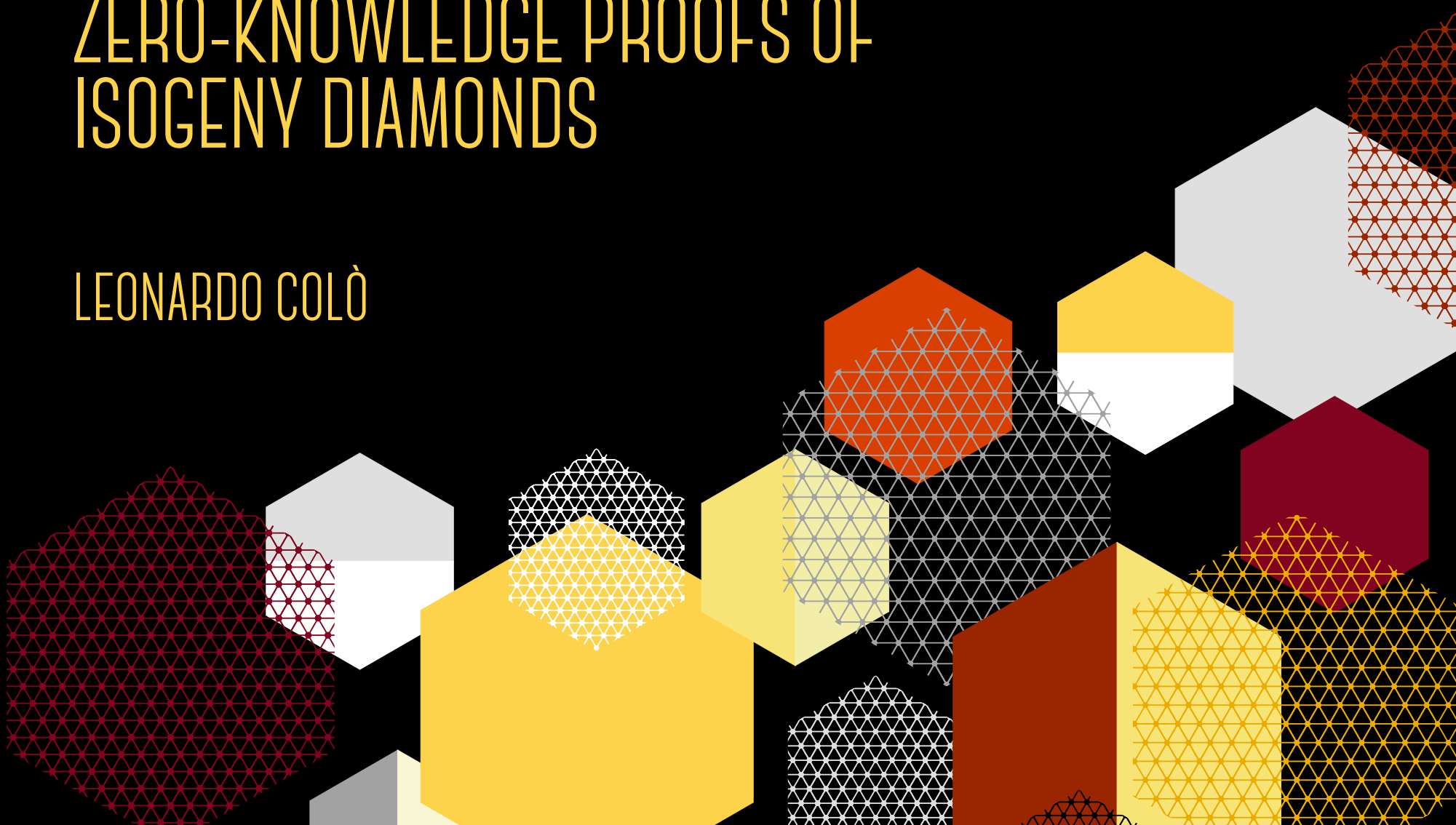
Hamilton, ON, 5 June, 2026

ONTARIO CRYPTO DAYS 2026

UNIVERSITY OF WATERLOO

ZERO-KNOWLEDGE PROOFS OF ISOGENY DIAMONDS

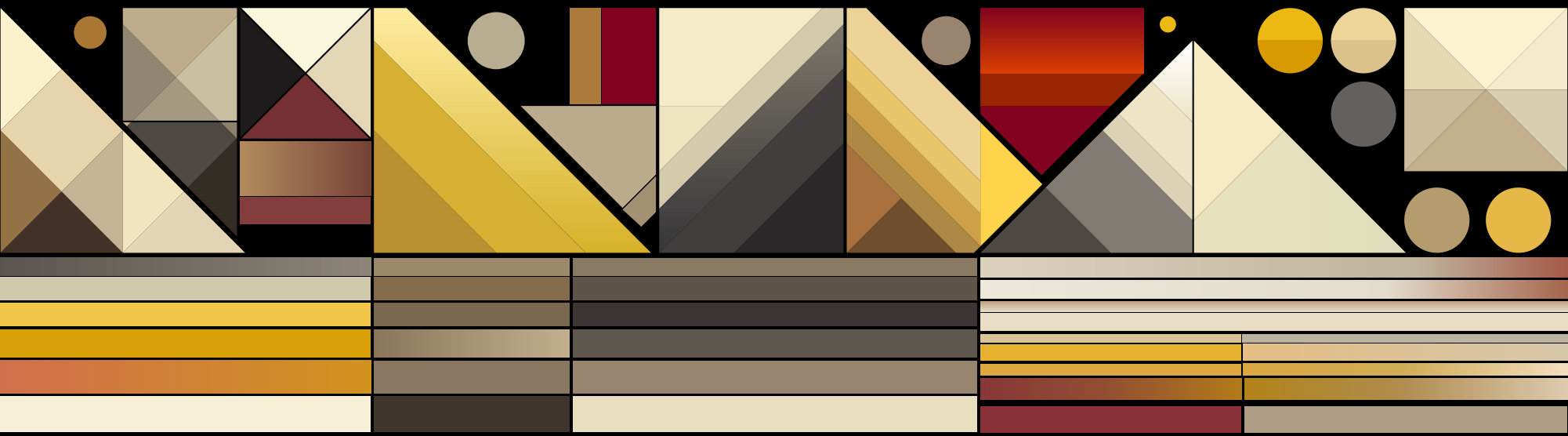
LEONARDO COLÒ



CONTENTS

- Elliptic curves and isogeny graphs.
- Contruction I
- Construction II
- Kani’s theorem and HD-isogenies
- Construction III

ELLIPTIC CURVES & ISOGENY GRAPHS



Elliptic curves

An elliptic curve over a field k (char $\neq 2, 3$):

$$E : y^2 = x^3 + Ax + B, \qquad \Delta = 4A^3 + 27B^2 \neq 0.$$

- Isogeny: non-constant algebraic group morphism $\varphi : E_1 \to E_2$.
- Kernel-theorem: if $\gcd(\deg \varphi, \mathrm{char}(k)) = 1$, then φ is uniquely determined by finite subgroup $\ker \varphi$.
- Dual isogeny and degree multiplication formula: $\widehat{\varphi} \circ \varphi = [\deg \varphi]$.

ISOGENY GRAPHS

L.COLÒ UWAT

Definition

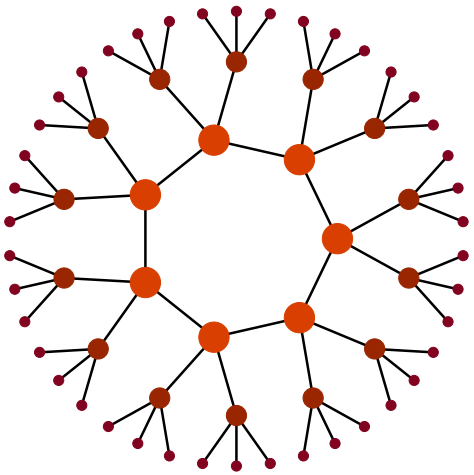
Given an elliptic curve E over k, and a finite set of primes S, we can associate an isogeny graph $G_S(E)$

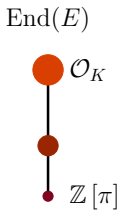
- whose vertices are elliptic curves isogenous to E over $\bar{k}$, and
- whose edges are isogenies of degree $\ell \in S$.

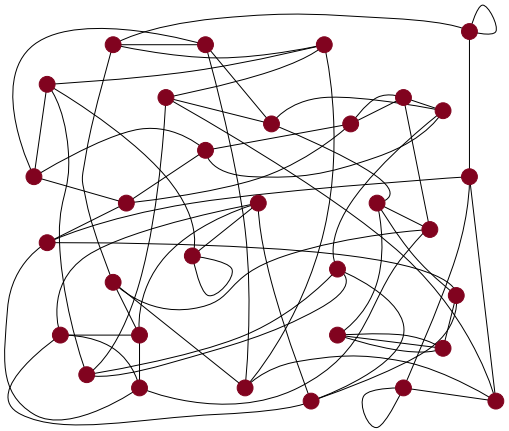
If $S = \{\ell\}$, then we write $G_\ell(E)$, the ℓ-isogeny graph.

The vertices are defined up to $\bar{k}$-isomorphism and the edges from a given vertex are defined up to a $\bar{k}$-isomorphism of the codomain.

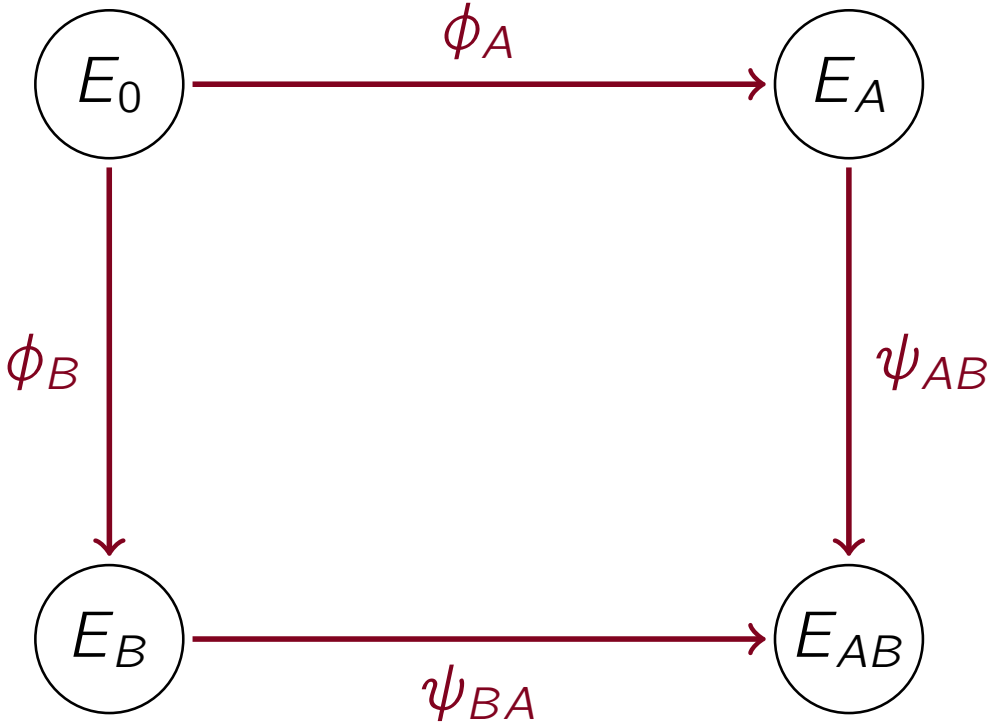
The ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph).







ISOGENY SQUARES



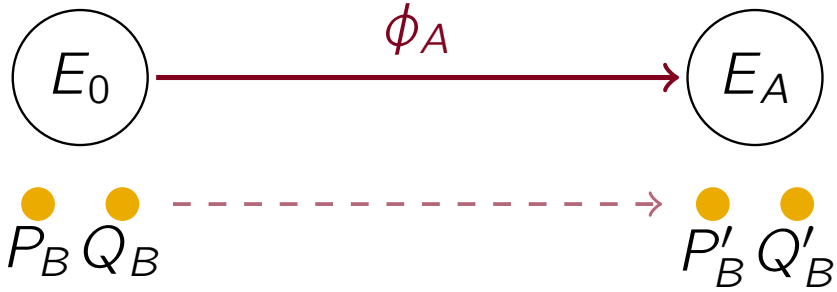
$$\psi_{AB} \circ \phi_A = \psi_{BA} \circ \phi_B$$

$$\ker(\psi_{AB}) = \phi_A(\ker(\phi_B))$$
$$\ker(\psi_{BA}) = \phi_B(\ker(\phi_A))$$

$$\ker(\phi_A) \cap \ker(\phi_B) = \{\mathcal{O}\}$$
$$\gcd(A, B) = 1$$

SIDH & MSIDH

SIDH

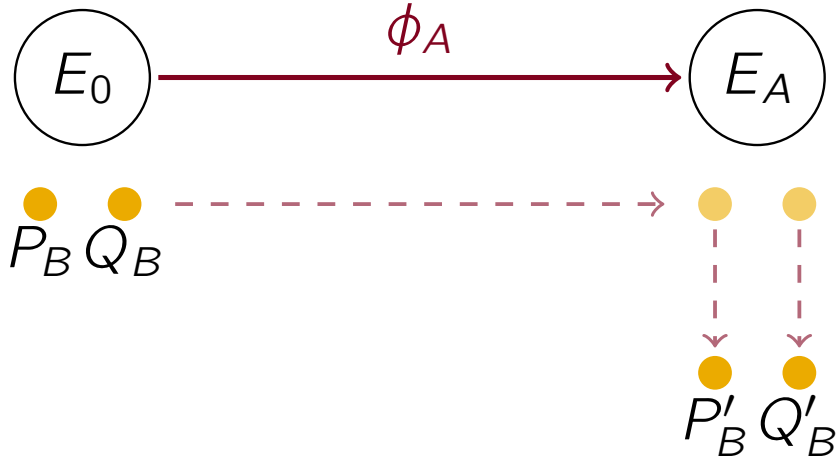


Public Images: $\phi_A(P_B), \phi_A(Q_B)$

$E_0[B] = \langle P_B, Q_B \rangle$

Kani attacks exploit this extra torsion information.

MSIDH

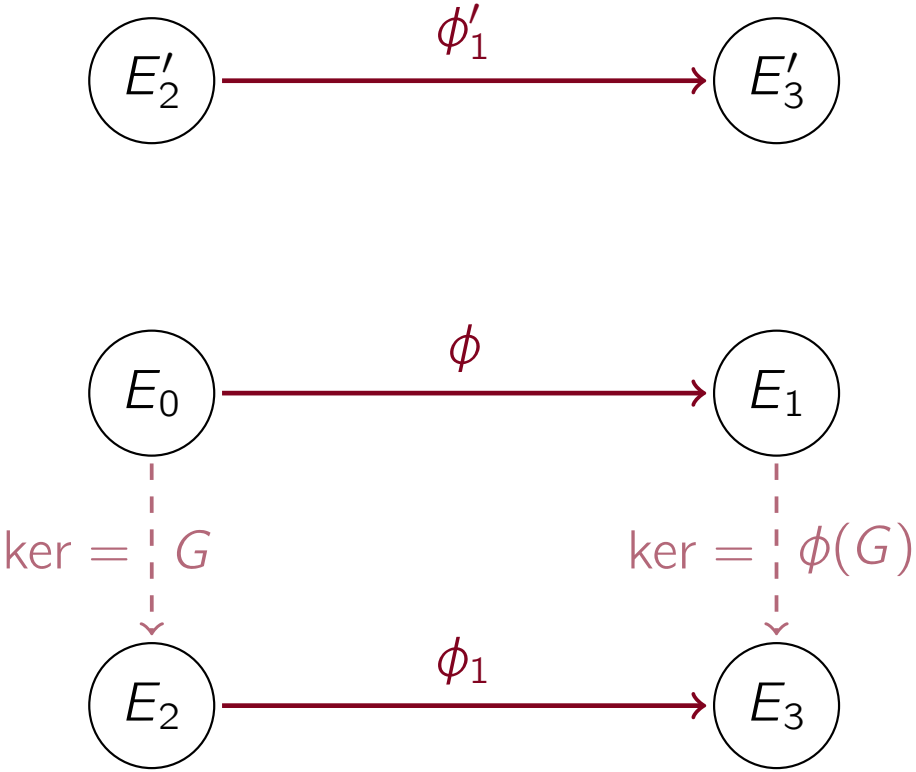


Public: $[\alpha]\phi_A(P_B), [\alpha]\phi_A(Q_B)$

Hidden $\alpha \in (\mathbb{Z}/B\mathbb{Z})^\times$

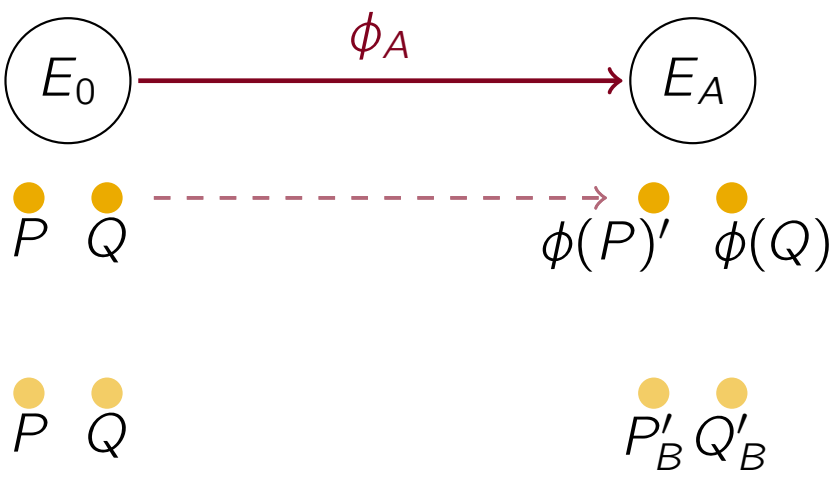
ISOGENY HARDNESS ASSUMPTIONS

DSSP



Distinguish
- genuine pushforward square
- random supersingular isogeny

DLIT

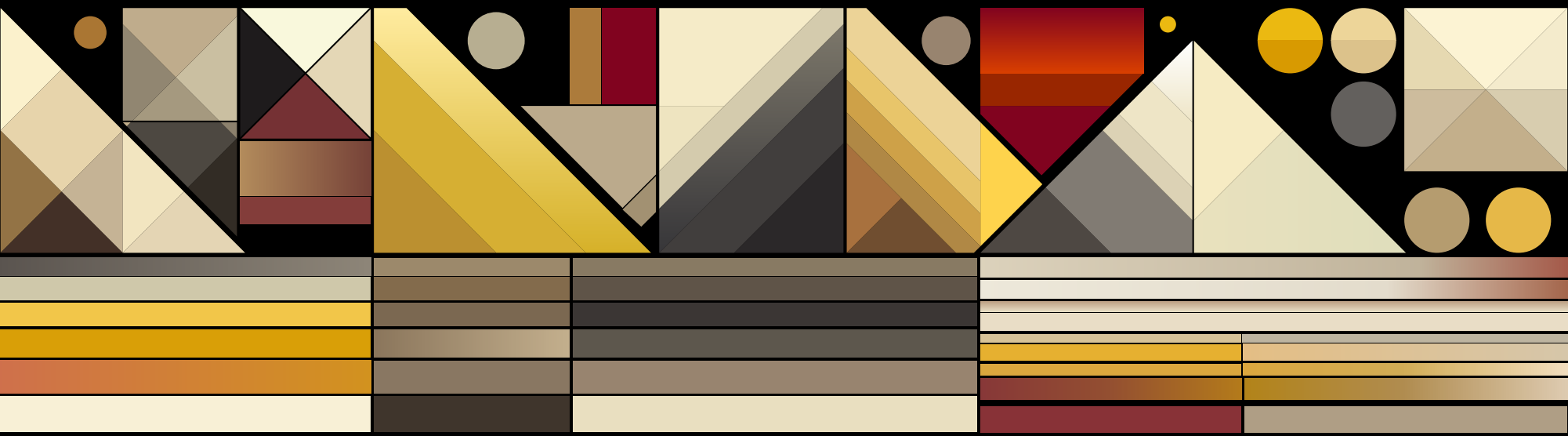


Distinguish
- torsion under a long isogeny
- random torsion (wt pairing)

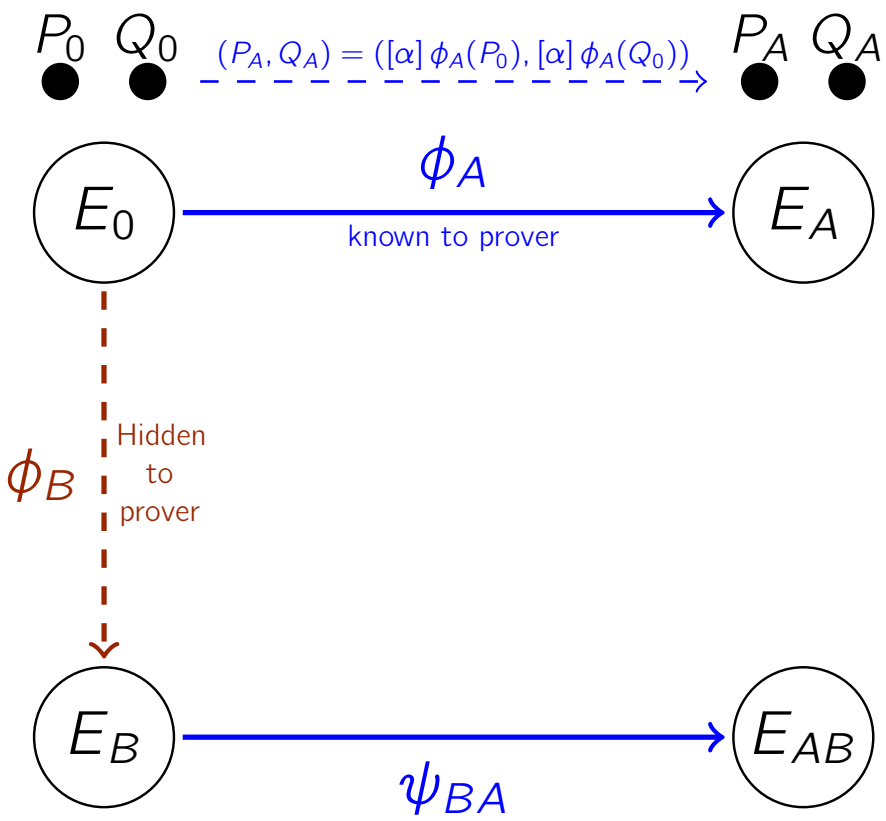
3 DIFFERENT CONSTRUCTIONS

- One knows only the two parallel isogenies in the diagram
  - Windmill-ZKP
- One knows all four isogenies of the diamond.
  - Cube-ZKP
  - Kani-Diamond-ZKP

CONSTRUCTION I: THE WINDMILL



STATEMENT

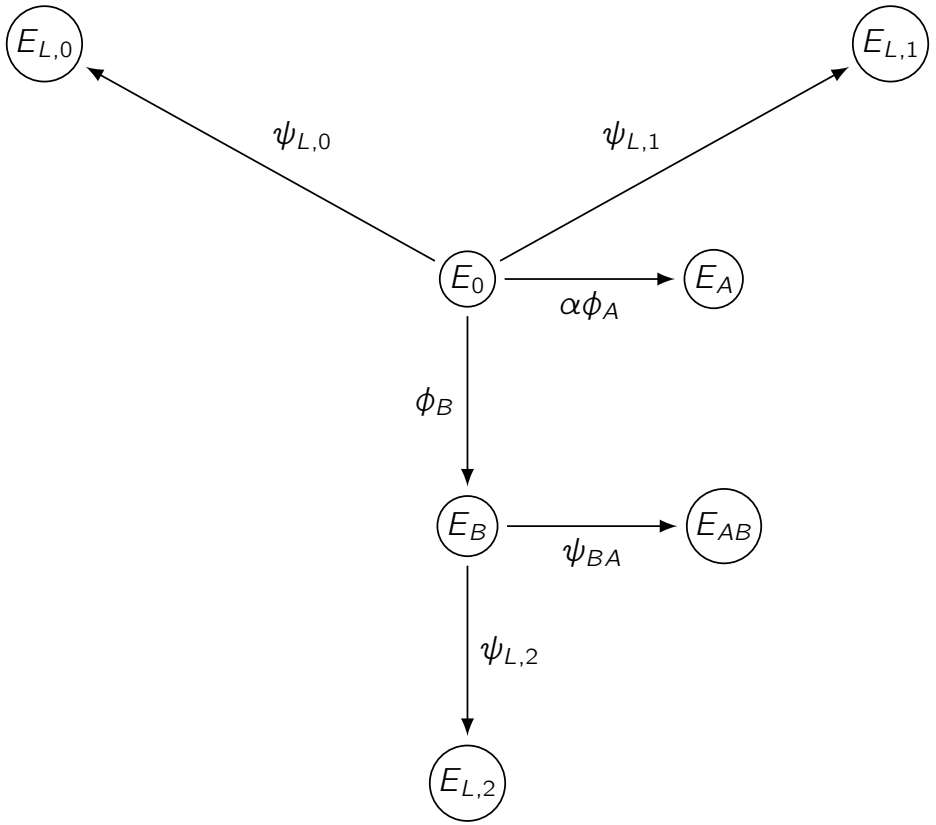


Compatibility condition

The pushforward of ϕ_A along the hidden B direction has codomain E_{AB}

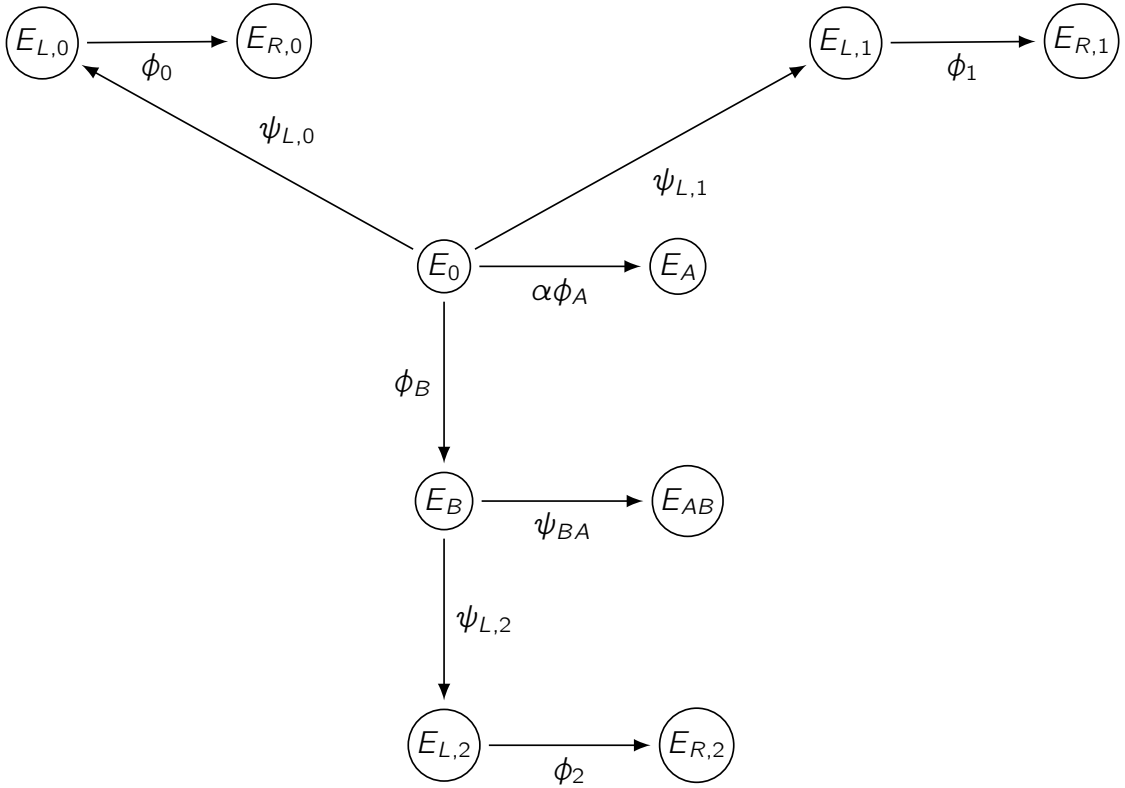
- **Public curves:** E_0, E_A, E_B, E_{AB}
- **Public data:** a basis $E_0[B] = \langle P_0, Q_0 \rangle$ masked images P_A, Q_A on E_A.
- **Witness:** a cyclic A-isogeny ϕ_A a scalar $\alpha \in (\mathbb{Z}/B\mathbb{Z})^\times$.
- **Goal:** Prove that the square is compatible without revealing witnesses.

AUXILIARY ISOGENIES



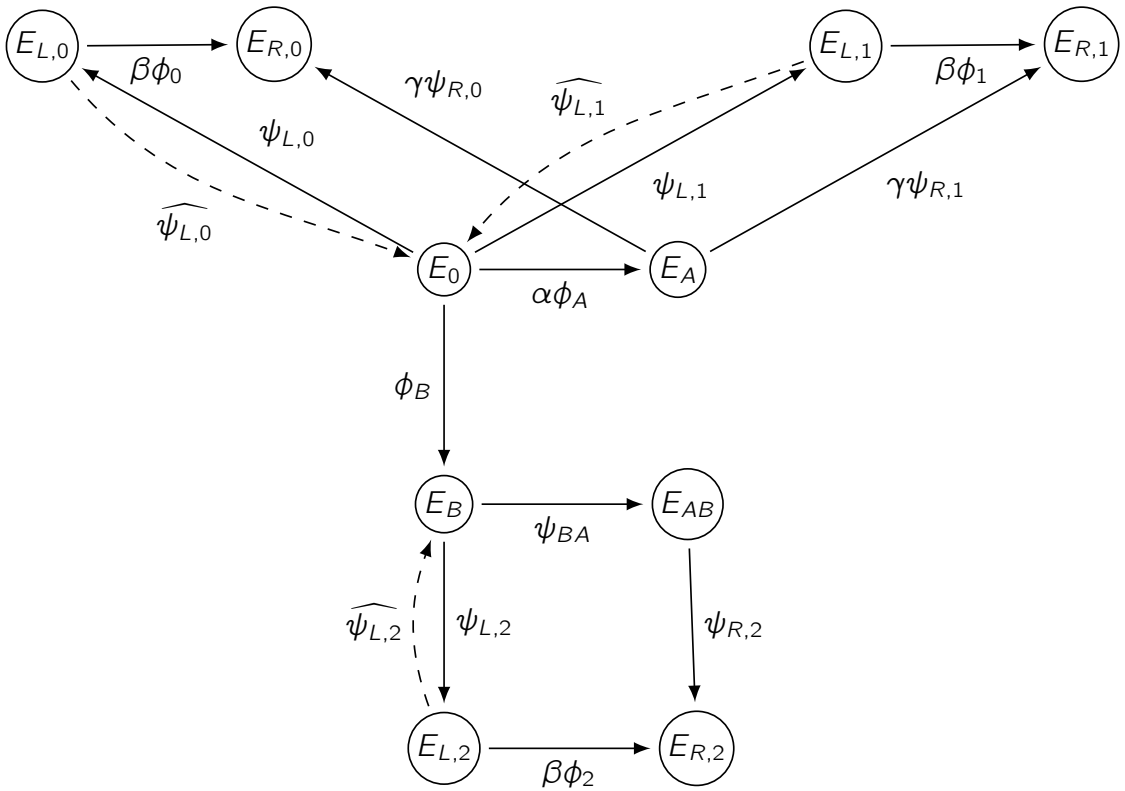
- **Sample B-isogenies**
  $E_0 \to E_{L_0}$, $E_0 \to E_{L_1}$, and $E_B \to E_{L_2}$
- **Choose torsion basis:**
  Pick $E_0[A] = \langle U, V \rangle$
- **Push through:**
  Push U, V through $\psi_{L,0}$, $\psi_{L,1}$, and $\psi_{L,2}$.
- These transposed A-torsion points will describe the pushforward A-isogenies.

PUSH FORWARD



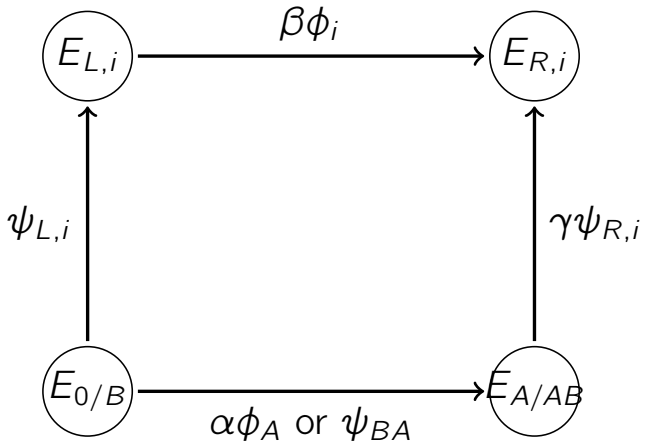
- **Kernel of the witness** find two integers e, f such that $\ker \phi_A = \langle eU + fV \rangle$.
- **Compute pushforwards:** $\phi_i : E_{L,i} \to E_{R,i}$ with $\ker \phi_i = \langle eU_i + fV_i \rangle$
- Each branch is a shadow of the original witness ϕ_A
- These branches will later be opened selectively to the verifier.

TORSION POINTS & MASKING



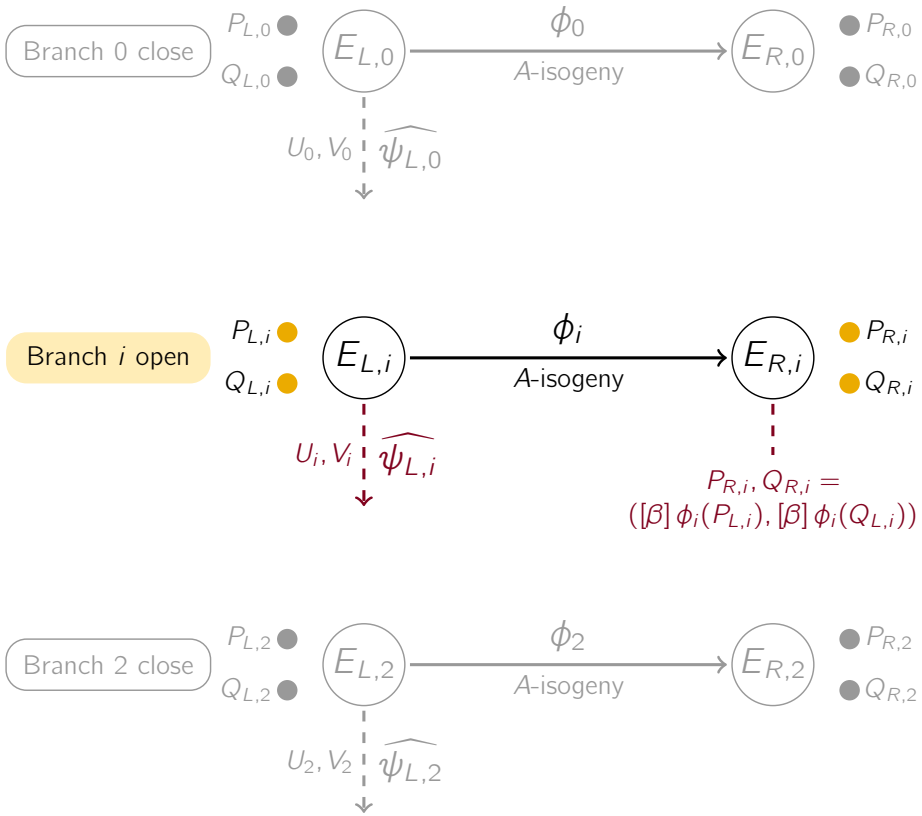
- **Sample B-torsion**
  find B-torsion basis
  $E_{L,i}[B] = \langle P_{L,i}, Q_{L,i} \rangle$
- **Dual**
  find two integers c_i, d_i such that
  $\ker \widehat{\psi_{L,i}} = \langle c_i P_{L,i} + d_i Q_{L,i} \rangle$
- **Map and mask**
  map across ϕ_i and mask by β to obtain
  $P_{R,i} = [\beta]\,\phi_i(P_{L,i})$
  $Q_{R,i} = [\beta]\,\phi_i(Q_{L,i})$
- Compute $\gamma = \alpha^{-1}\beta$

COMMITMENT



- **General data**
  - basis of $E_0[A]$: U, V
  - mask relation γ
- **Left branch data** (Unmasked side.)
  - for each i, we commit to $E_{L,i}$, (U_i, V_i) and $(P_{L,i}, Q_{L,i})$.
- **Right branch data** (Masked side.)
  - for each i, we commit to $E_{R,i}$, and $(P_{R,i}, Q_{R,i})$.
- **Global scalars**
  - e, f, and β.

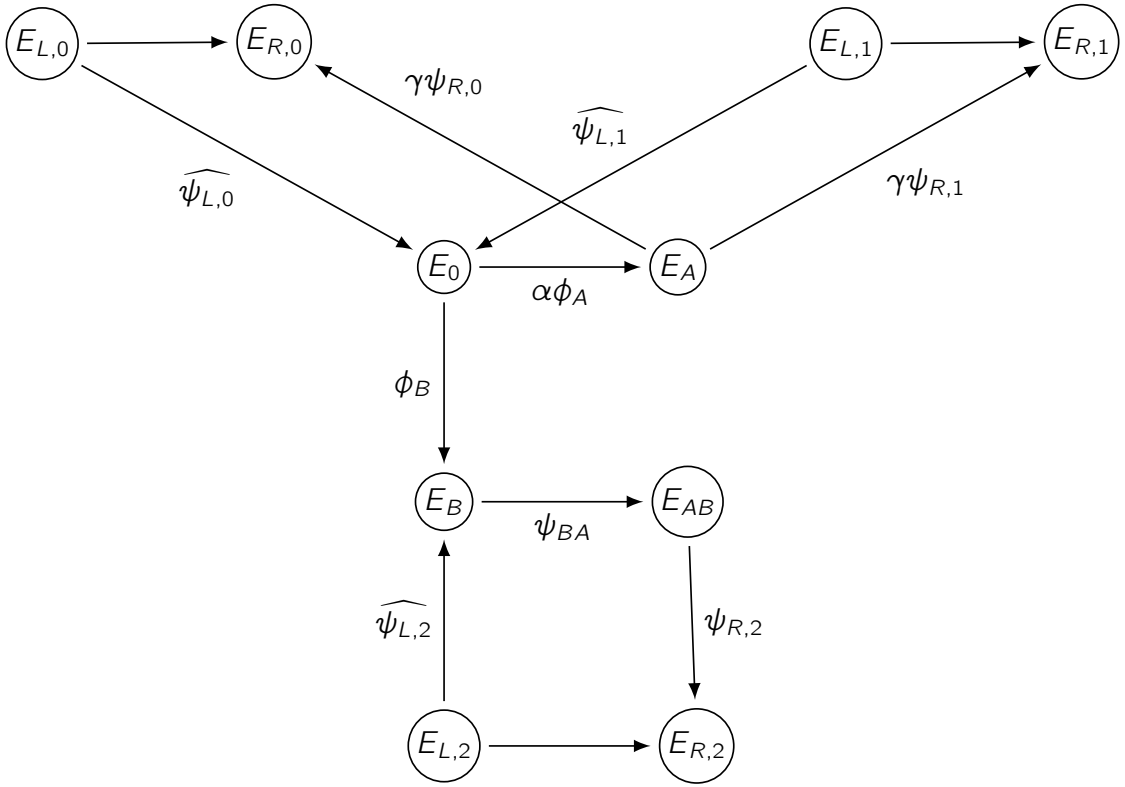
CHALLENGES - THE CASE 0,1,2



Verifier checks:

- Reconstruct $\ker \phi_i = \langle eU_i + fV_i \rangle$
- Build the A-isogeny ϕ_i from $E_{L,i}$
- Check that the codomain is $E_{R,i}$
- Verify $(P_{R,i}, Q_{R,i}) = ([\beta]\,\phi_i(P_{L,i}), [\beta]\,\phi_i(Q_{L,i}))$

CHALLENGES - THE CASE 3,4



Prover reveals

- Describes $\widehat{\psi_{L,i}}$ $\forall i$
- $E_{L,i}$ $\forall i$
- Basis for $E_{L,i}[A]$, $E_{L,i}[B]$ $\forall i$
- U, V basis for $E_0[A]$

Verifier checks

- Codomain of $\psi_{L,i}$ is $E_{L,i}$
- Torsion points images

SECURITY PICTURE

L.COLÒ UWAT

Proposition 1

Windmill-ZKP is correct.

Proposition 2

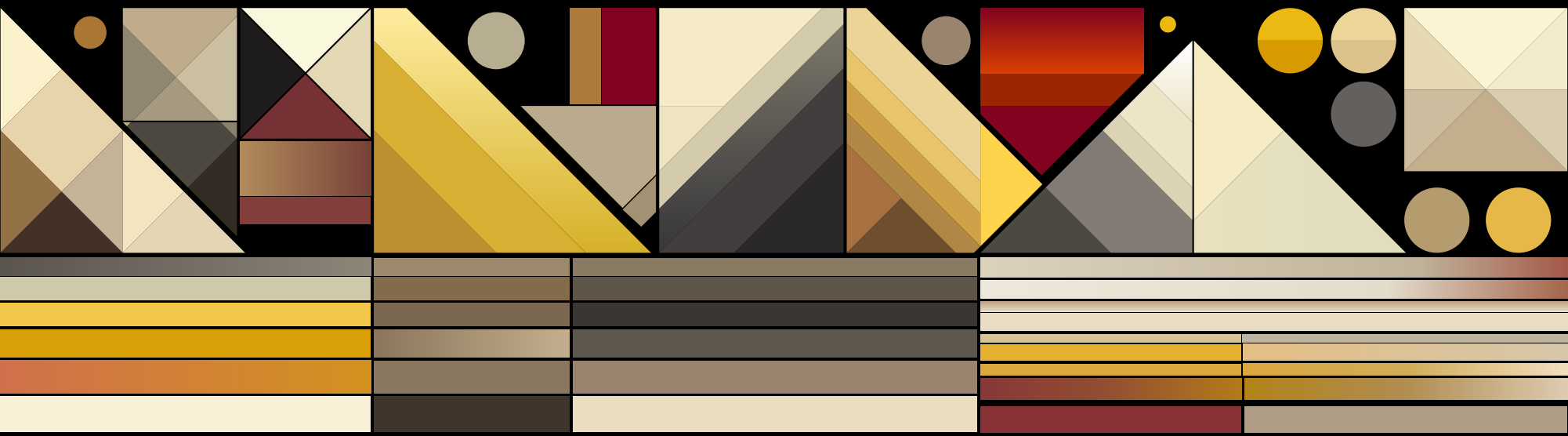
Given that the hash function used is computationally binding, Windmill-ZKP is 5-sound.

- Challenges $0, 1, 2$ certify the A-branch.
- Challenge 3 certify the left-dual data.
- Challenge 4 certify the right-dual data.
- Together they force a single consistent witness

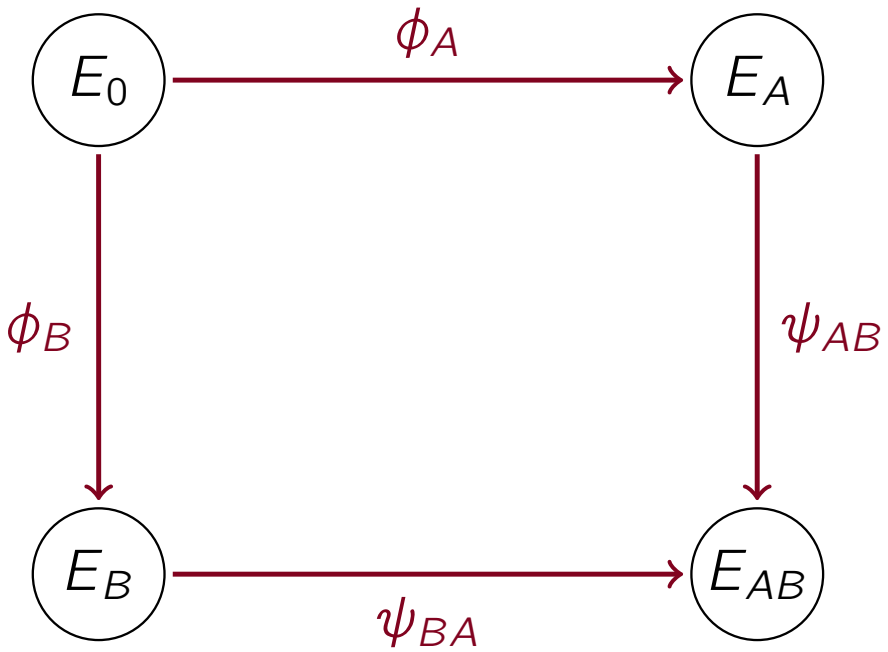
Proposition 3

Given a statistically hiding hash function, Windmill-ZKP is computationally zero-knowledge assuming DSSP is secure for $d = B$ and $N = A$

CONSTRUCTION II: THE CUBE

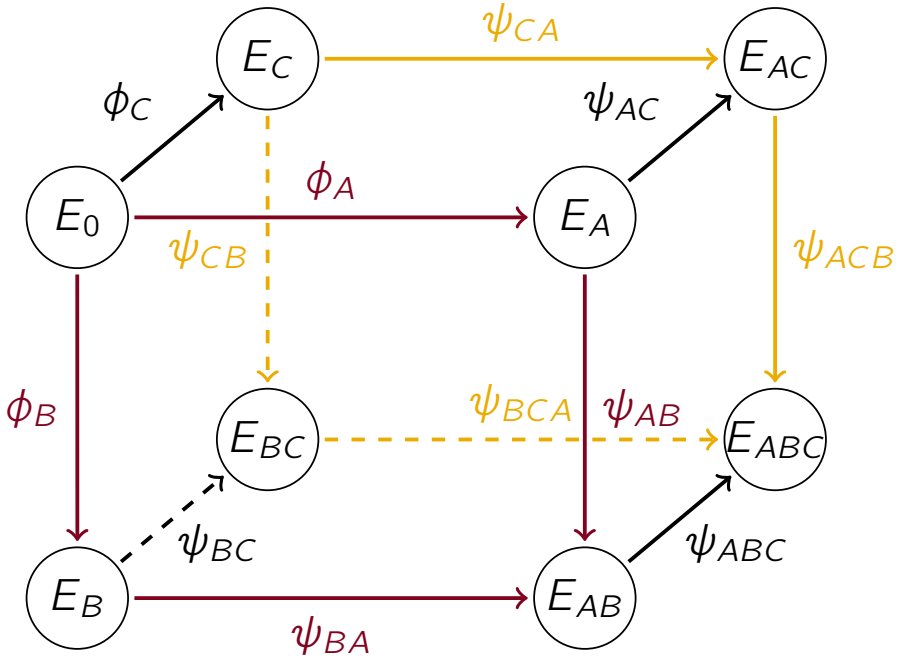


STATEMENT



- **Public curves:** E_0, E_A, E_B, E_{AB}
- **Public data:** Pairwise coprime A, B, C.
- **Witness:**
  a cyclic A-isogeny ϕ_A
  a cyclic B-isogeny ϕ_B
- **Idea**
  Hide the diamond behind a fresh random C-isogeny (translate it through ϕ_C)

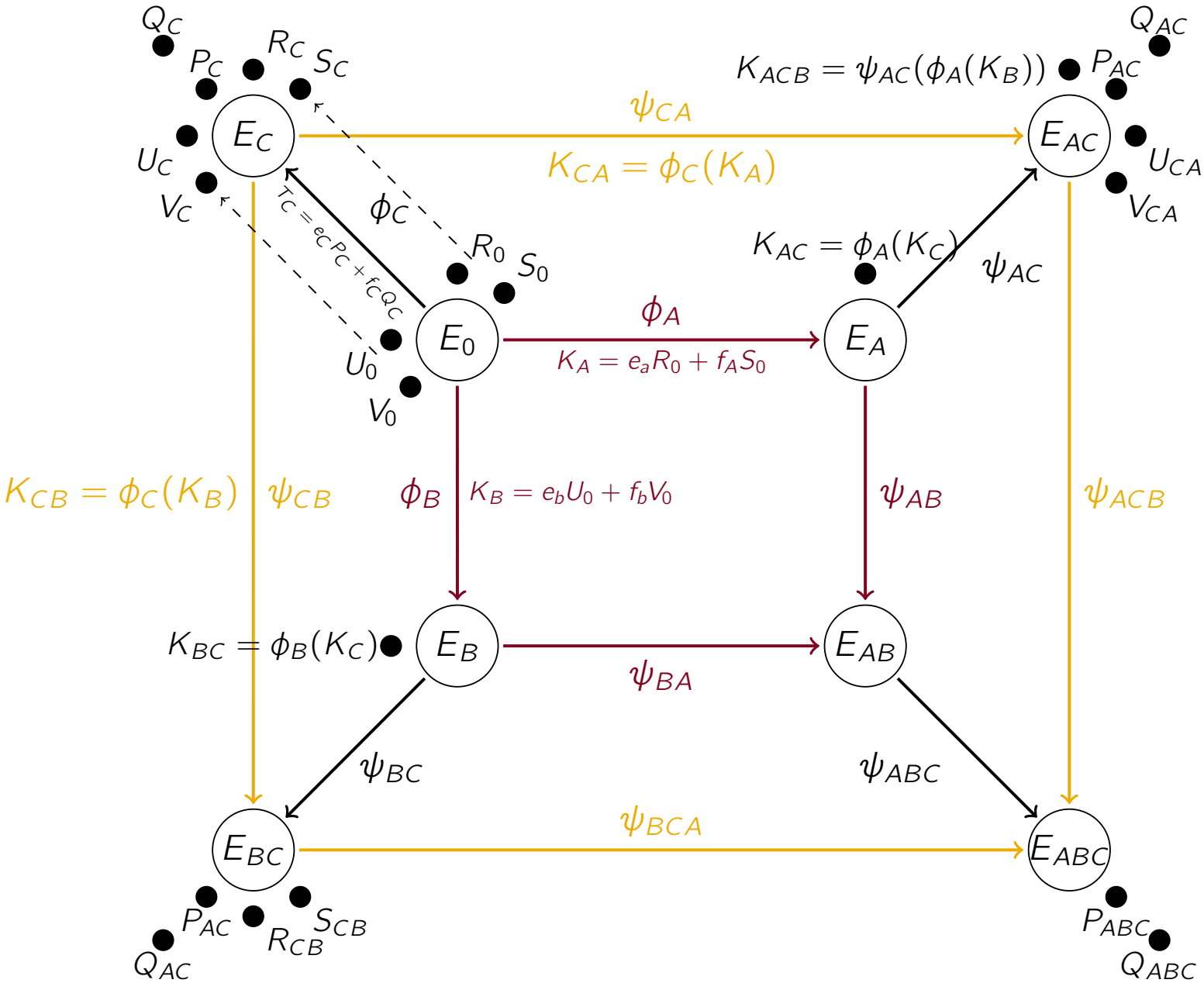
PUSHING THE DIAMOND



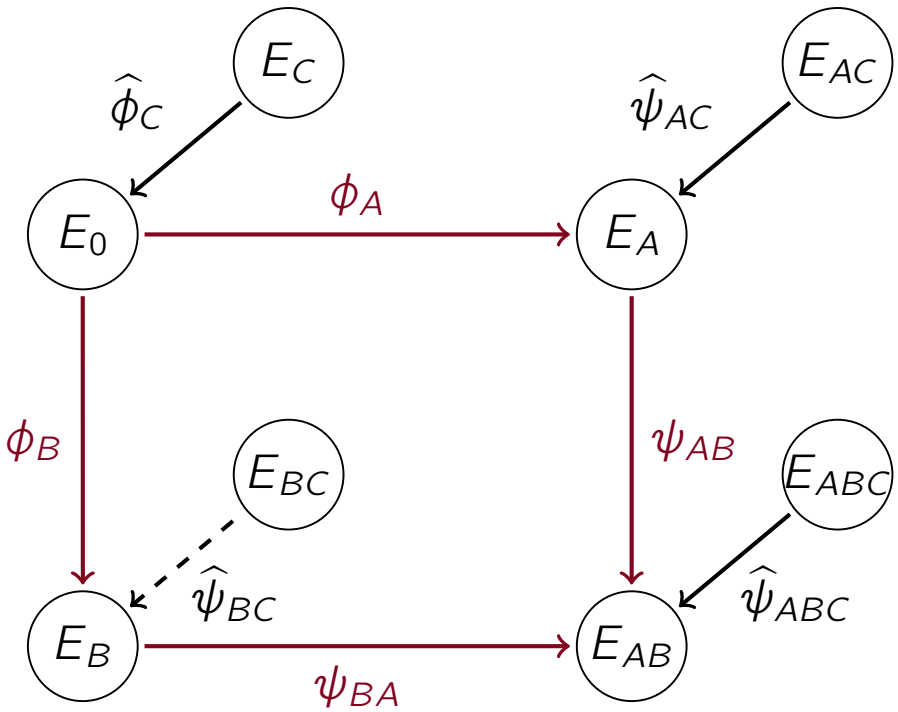
- Sample random cyclic C-isogeny ϕ_C and dual-kernel coordinates $\ker \widehat{\phi_C} = \langle T_C \rangle$
- Transport the A-kernel and B-kernel to E_C to form ψ_{CA} and ψ_{CB}.
- Transport the C-kernel through ϕ_A and ϕ_B to form ψ_{AC} and ψ_{BC}.
- Complete the back square by pushforward to E_{ABC}.

Front face = secret diamond Back face = randomized diamond

COMMITTMENT



CHALLENGES I - CASE 0,1,2,3



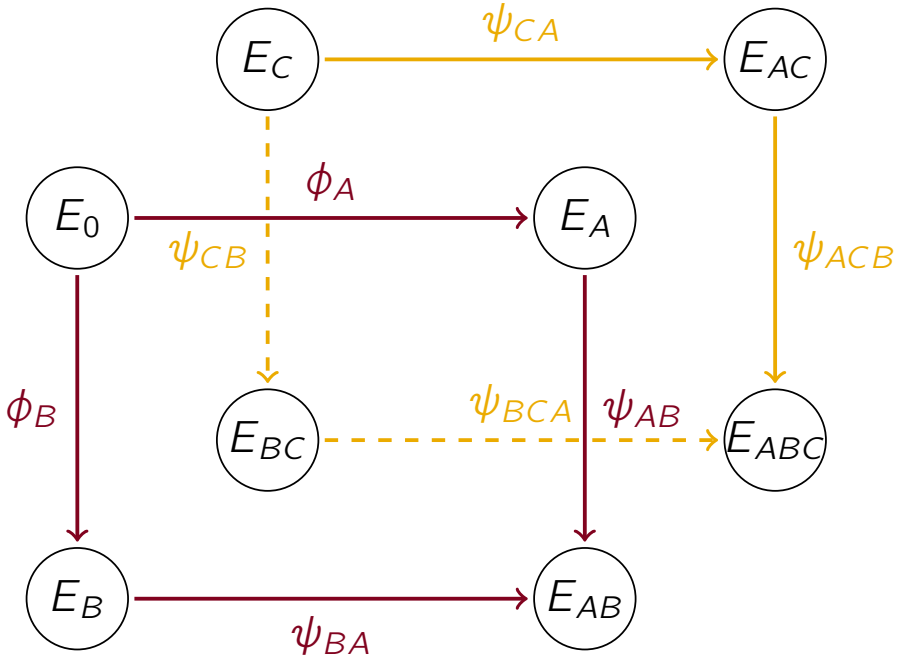
Prover reveals the data describing one of the dual isogenies $\widehat{\phi_C}, \widehat{\phi_{AC}}, \widehat{\phi_{BC}}$ or $\widehat{\phi_{ABC}}$.

- reveals E_{*C}, the basis $E_{*C}[C] = \langle P_*, Q_* \rangle$, the integers e_c, f_C.

Verifiers

- checks committed hashes.
- reconstructs the C-kernel from the committed coordinates.
- check codomain.

CHALLENGES II - CASE 4,5,6,7



Prover reveals the data describing one of the sogenies $\psi_{CA}, \psi_{CB}, \psi_{ACB}$ or ψ_{BCA}.

- opens domain and codomain.
- opens basis for some of the A, B and C torsion for both.

Verifiers

- checks kernel coordinates.
- checks torsion images.

SECURITY PICTURE

Proposition 1

Cube-ZKP is correct.

Proposition 2

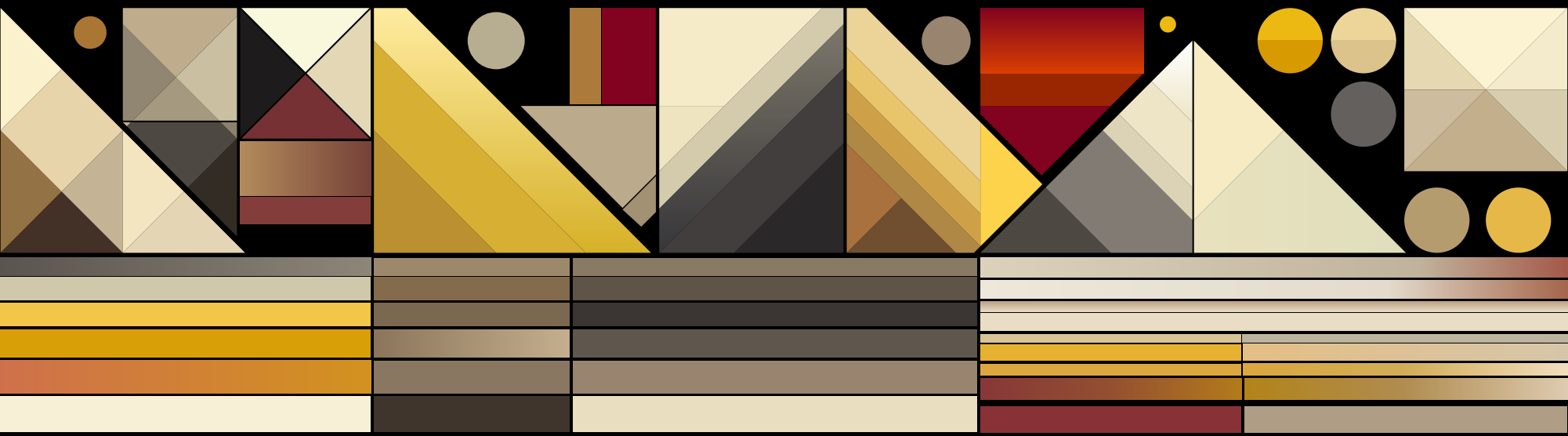
Given that the hash function used is computationally binding, Cube-ZKP is 8-sound.

- Soundness is equivalent to “the cube glues together”: the opened edges force one front diamond.

Proposition 3

Given a statistically hiding hash function, Cube-ZKP is computationally zero-knowledge assuming DSSP is secure for $d = C$ and $N = \max\{A, B\}$

CONSTRUCTION III: KANI



Smooth projective algebraic variety + algebraic group

Principal polarizations

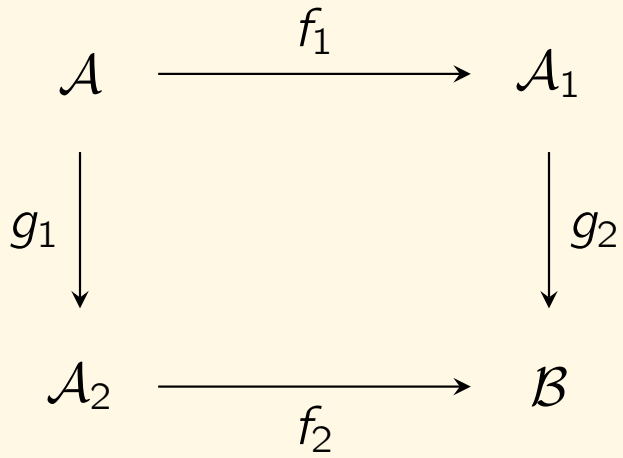
A principally polarized abelian variety (PPAV) is a pair $(\mathcal{A}, \lambda)$, where $\mathcal{A}$ is an abelian variety and $\lambda : \mathcal{A} \to \mathcal{A}^\vee$ is a principal polarization, i.e., an isomorphism to the dual.

Maximally Isotropic subgroups

An isotropic subgroup of $\mathcal{A}[n]$ is a subgroup on which the Weil pairing e_n is trivial.

KANIS THEOREM

Suppose that there is an isogeny diamond as follows:



Then, there is an isogeny $\Psi : \mathcal{A}_1 \times \mathcal{A}_2 \to \mathcal{A} \times \mathcal{B}$ defined by

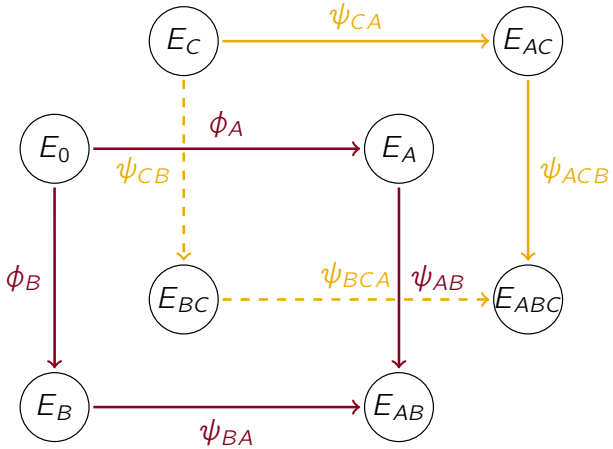
$$\Psi = \begin{pmatrix} \widetilde{f_1} & \widetilde{g_2} \\ -g_1 & f_2 \end{pmatrix}$$

Moreover, we have $\ker \Psi = \langle (f_1(P), g_1(P)) \mid P \in \mathcal{A}[\deg(f_1) + \deg(f_2)] \rangle$.

KANI VARIANT OF THE CUBE: KUBE-ZKP

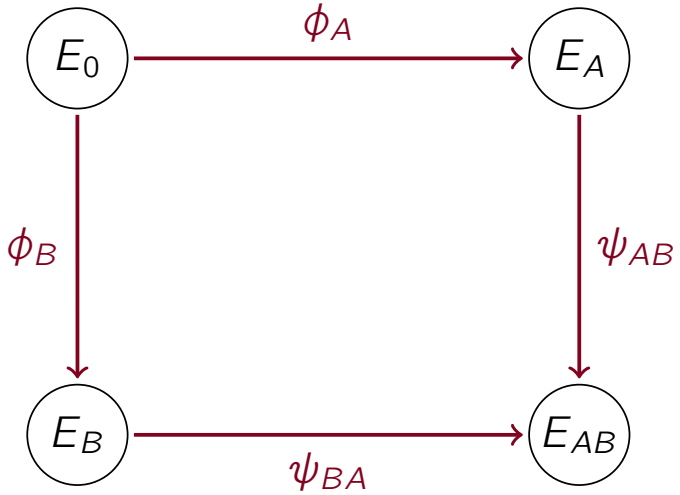
Kube-ZKP collapses the four back-edge challenges of Cube-ZKP into a single one.

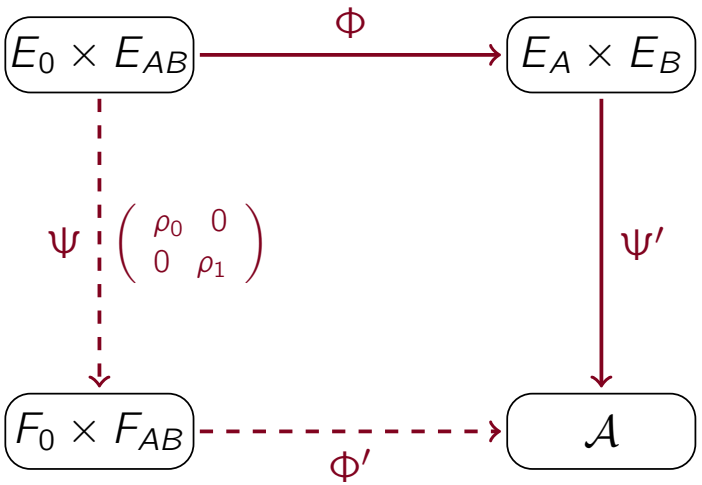
$$\Phi : E_C \times E_{ABC} \longrightarrow E_{AC} \times E_{BC}$$



Property	Kube-ZKP	Kube-ZKP
Challenges	8	5
Back openings	4 edges	1 back square
Front openings	4 edges	4 edges
Transcript length	Longer	Shorter

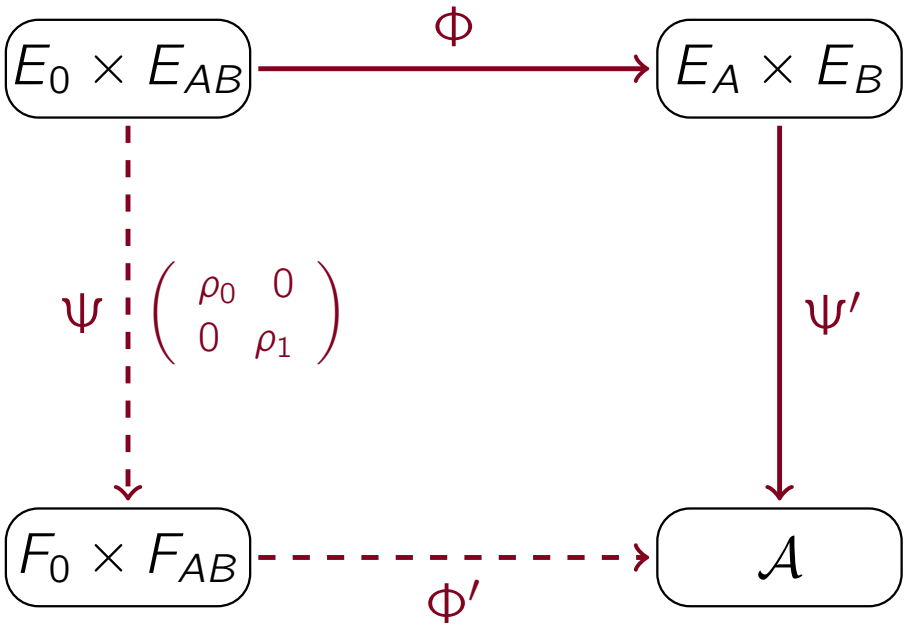
STATEMENT





- **Public curves:** E_0, E_A, E_B, E_{AB}
- **Witness:** the kernel generators of Φ, equivalently the original commuting diamond
- **Idea:**
  prove the diamond by proving one carefully structured 2-dimensional isogeny.

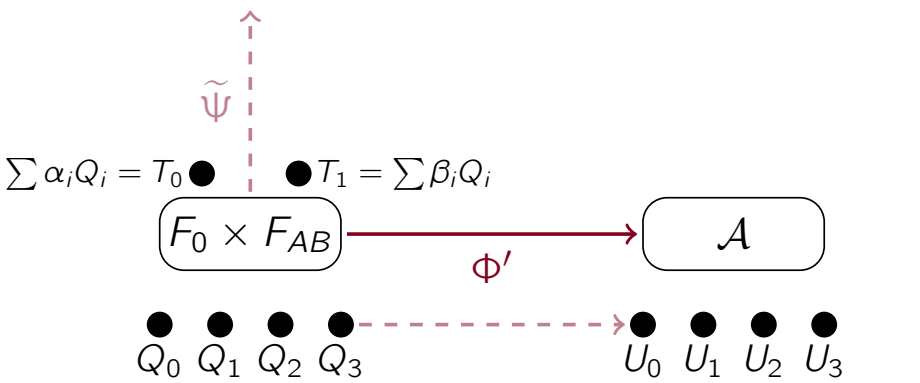
THE AUXILIARY DIAGONAL ISOGENY - THE PUSHFORWARD



- Sample cyclic M-isogenies ρ_0 and ρ_1.
- Form the diagonal isogeny $\Psi = \mathrm{diag}(\rho_0, \rho_1)$:
- Push the kernel forward. Let $(K_0, K_1) \subset (E_0 \times E_{AB})[N]$ be $\ker \Phi$. Compute $K_i' = \Psi(K_i)$ These generate $\ker(\Phi')$.
- The pushforward gives Φ' : and the corresponding map Ψ', completing the diagram.

Structural fact: Pushforward through a diagonal auxiliary map keeps the non-diagonal structure and maximal isotropic nature visible to the verifier.

COMMITTMENT



kernel coefficients
$H(r_{01}, \alpha_i, \beta_i)$

torsion basis
$H(r_{02}, F_0, F_{AB}, Q_i)$

mapped points
$H(r_{12}, \mathcal{A}, U_i)$

kernel of Φ'
$H(r_2, K'_0, K'_1)$

- Sample a random basis of $(F_0, F_{AB})[M]$: $\{Q_0, Q_1, Q_2, Q_3\}$.
- Express the generators $T_0, T_1 \in \ker(\widehat{\Psi})$ in terms of the chosen basis as

$$T_0 = \sum_{i=0}^{3} a_i Q_i, \quad T_1 = \sum_{i=0}^{3} b_i Q_i,$$

- Compute $U_i = \Psi'(Q_i) \in A[M]$.
- Commit to the data.

CHALLENGES

chall = 0: reveal Ψ

Describe the diagonal isogeny $\widetilde{\Psi}$

$$F_0 \times F_{AB} \xrightarrow{\widetilde{\Psi}} E_0 \times E_{AB}$$

What is revealed:
- Basis $Q_i = (Q_{i,0}, Q_{i,AB})$
- Coefficients α_i, β_i

Verifier checks:
- Recover T_0, T_1
- Verify Ψ has ker $\langle T_0, T_1 \rangle$ that is max isotropic
- Verify codomain

chall = 1: reveal Ψ'

Describe the pushed map Ψ'

$$\mathcal{A} \xrightarrow{\widetilde{\Psi'}} E_A \times E_B$$

What is revealed:
- Images $U_i = \Phi'(Q_i) \in \mathcal{A}$
- Coefficients α_i, β_i

Verifier checks:
- Compute $V_0 = \sum \alpha_i U_i$
- Compute $V_1 = \sum \beta_i U_i$
- Verify $\langle V_0, V_1 \rangle$ is max iso
- Verify codomain

chall = 2: reveal Φ'

Describe Φ'

$$F_0 \times F_{AB} \xrightarrow{\Phi'} \mathcal{A}$$

What is revealed:
- Kernel generators K'_0, K'_1
- Source basis Q_i
- Images $U_i = \Phi'(Q_i) \in \mathcal{A}$

Verifier checks:
- Verify $\Phi(Q_i) = U_i$
- Verify $\langle K'_0, K'_1 \rangle$ is max iso
- Verify non-diagonality using the pairing test.

Pairing test (non-diagonality check):

If $K = \langle (P_1, P_2), (Q_1, Q_2) \rangle \subset F_0 \times F_{AB}$ is maximally isotropic, the associated isogeny is diagonal iff $e_N(P_1, Q_1) = 1$ (equivalently $e_N(P_2, Q_2) = 1$)

SECURITY PICTURE

L.COLÒ UWAT

Proposition 1

KaniDiamond-ZKP is correct.

Proposition 2

Given that the hash function used is computationally binding, KaniDiamond-ZKP is 3-sound.

Zero Knowledge

- Challenge 0 is easy to simulate: sample random ρ_0, ρ_1 and construct Ψ honestly.
- Challenge 1 requires simulating Ψ'.
- Challenge 2 requires simulating Φ'.

$$ker(\Phi') = \{(\rho_0([A]P), \rho_1 \circ \psi_{AB} \circ \phi_A(P)) \mid P \in E_0[N]\}$$

COMPARISON

	Cube	Kube	Kani
$p =$	$2^{e_2}3^{e_3}5^{e_5} - 1$	$2^{e_2}3^{e_3} - 1$	$2^{e_2}3^{e_3} - 1$
	-	$e_3 \approx 2e_2$	$3e_2 \approx e_3$
p (in bits)	6λ	6λ	8λ
Repetitions	5.191λ	3.106λ	1.710λ
Prover (2-isogenies)	6λ		
Prover (3-isogenies)	2.52λ	5.04λ	7.56λ
Prover (5-isogenies)	0.86λ		
Prover ((2, 2)-isogenies)		2λ	2λ
Prover ((3, 3)-isogenies)			
Verifier (2-isogenies)	λ		
Verifier (3-isogenies)	0.315λ	4.032λ	2.52λ
Verifier (5-isogenies)	0.215λ		
Verifier ((2, 2)-isogenies)		0.8λ	0.67λ
Verifier ((3, 3)-isogenies)			1.26λ
Proof Size (KB)	118λ	85.2λ	180.5λ

THANK YOU FOR THE ATTENTION

