SQIsign2D: an introduction

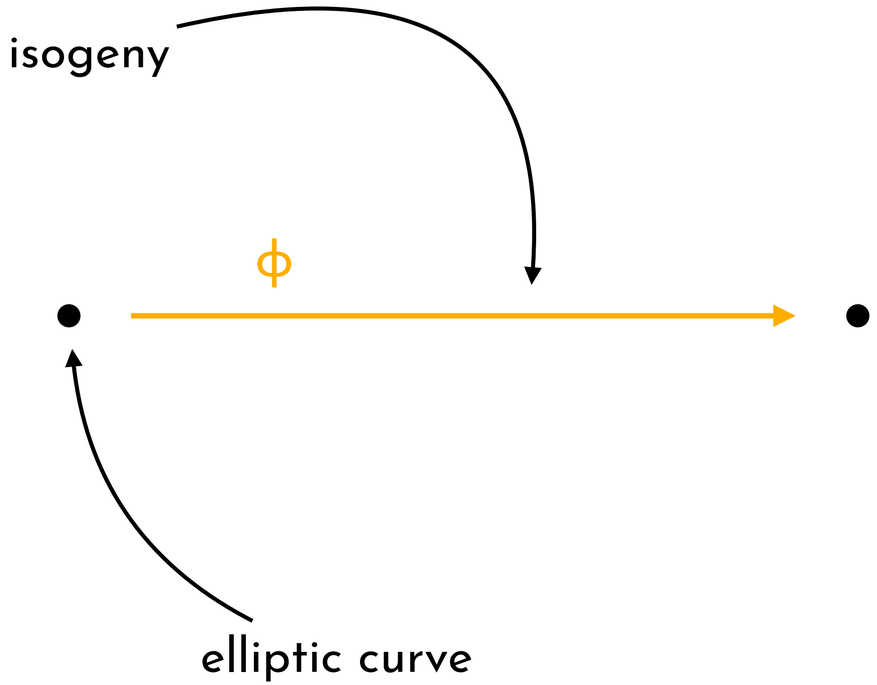
Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski

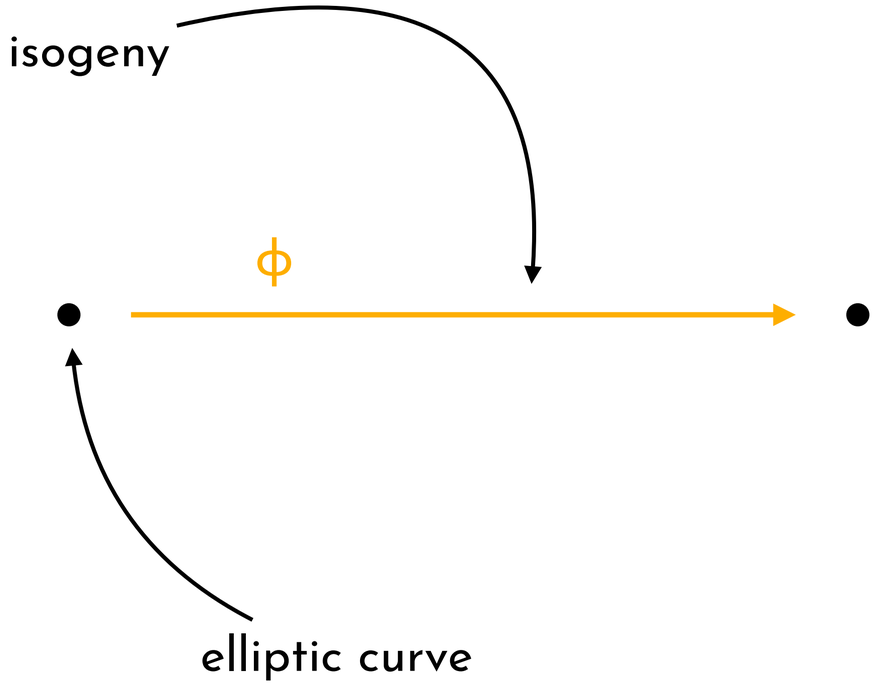
Max Duparc, Tako Boris Fouotsa

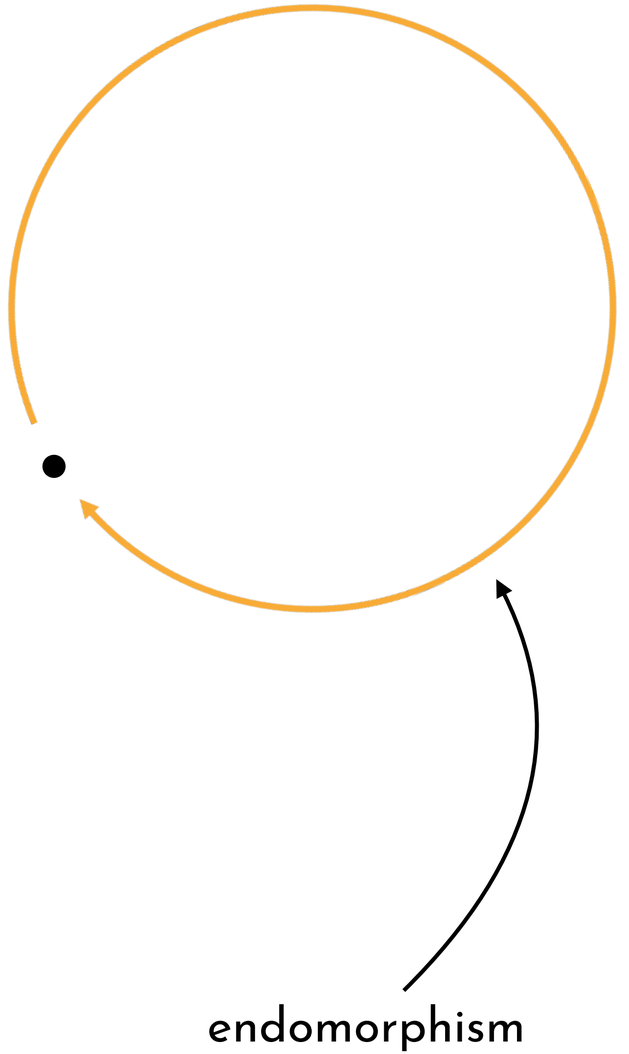
Kohei Nakagawa, Hiroshi Onuki, Wouter Castryck, Mingjie Chen, Riccardo Invernizzi, Gioella Lorenzon, Frederik Vercauteren

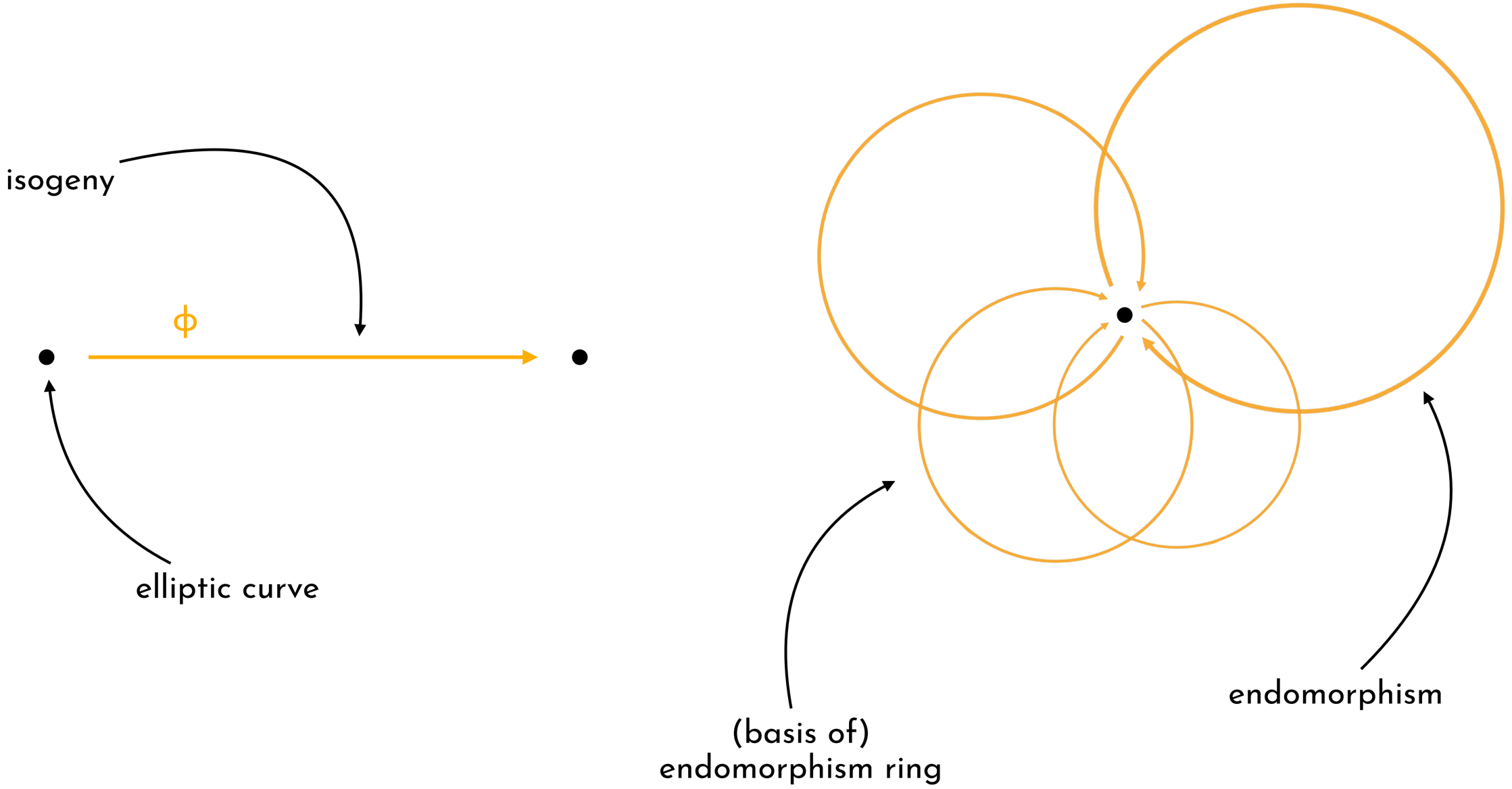
Asiacrypt 2024

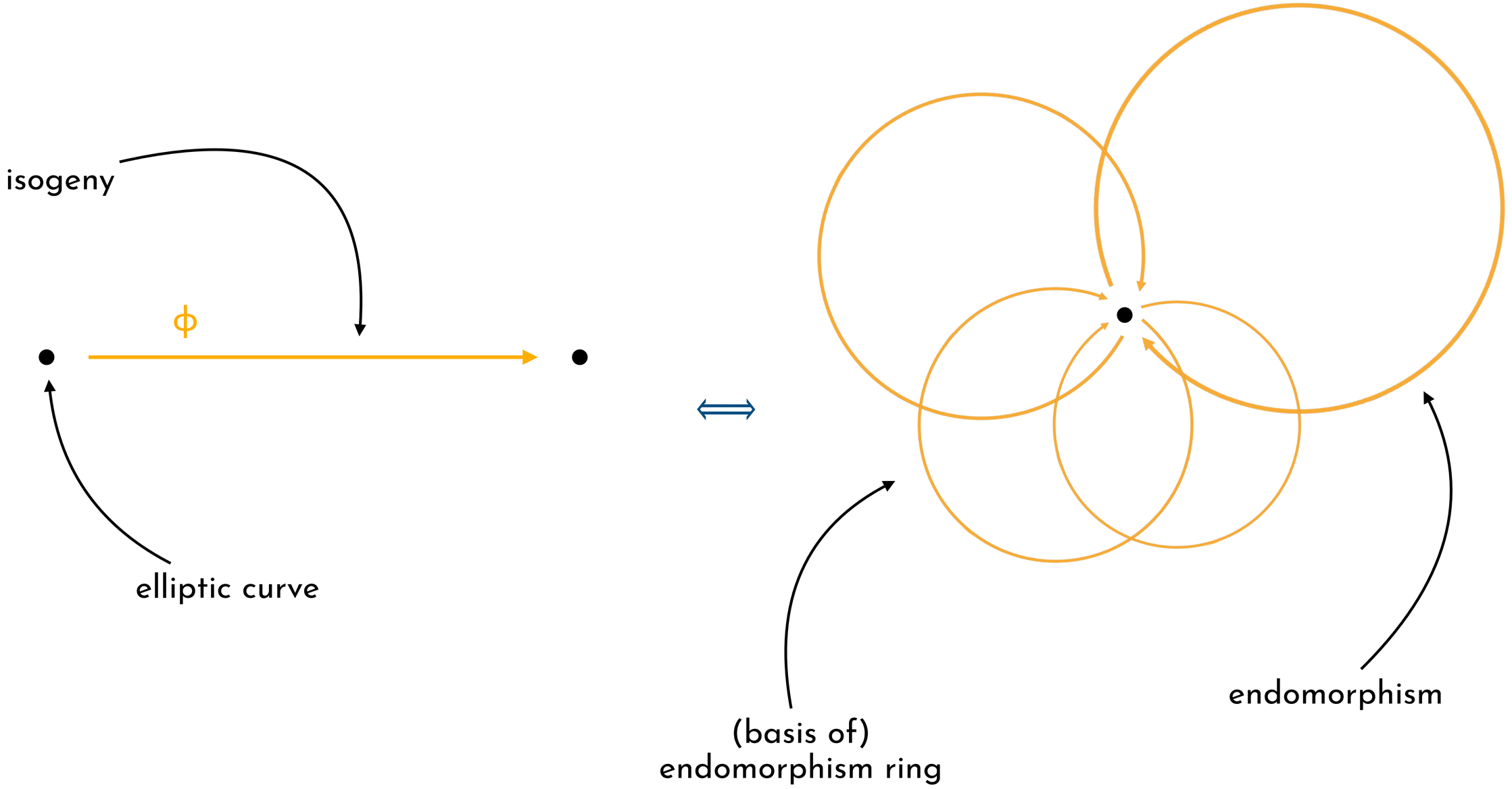
10th December 2024

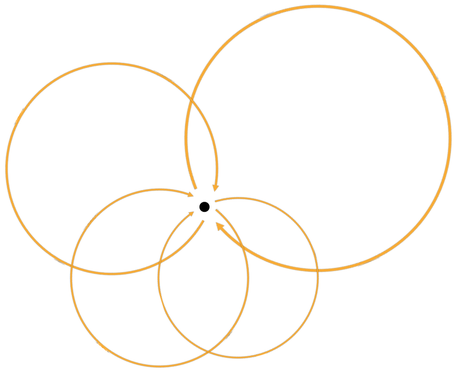

isogeny
ϕ
elliptic curve

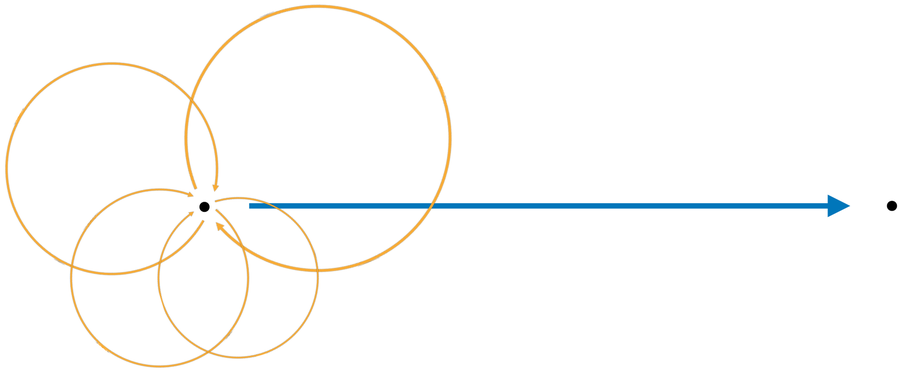

isogeny
ϕ
elliptic curve

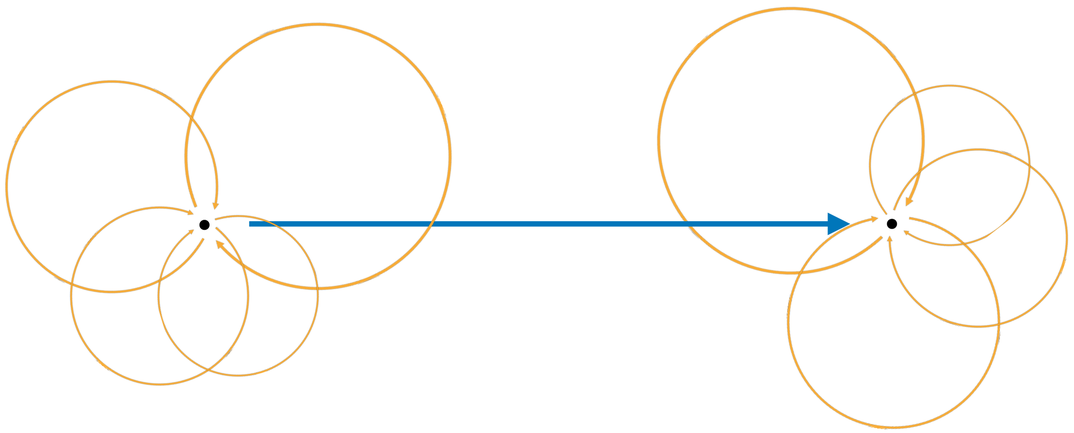

endomorphism

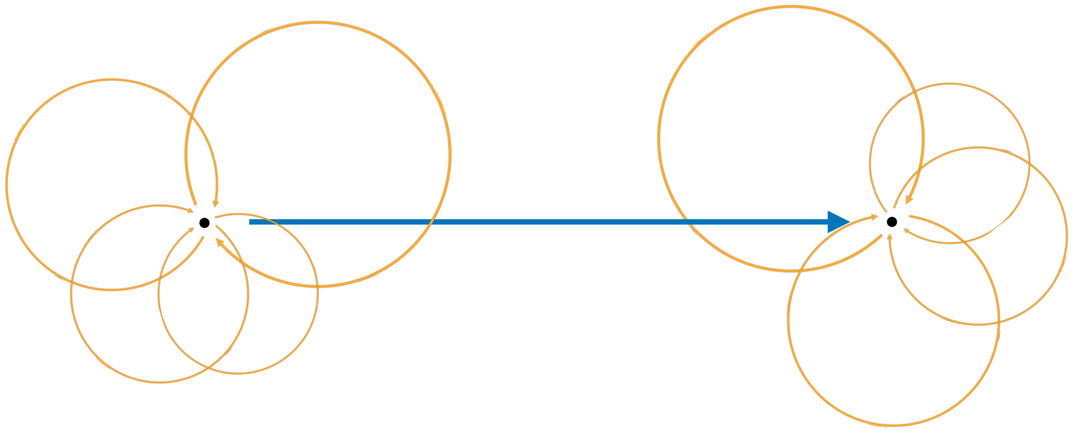

isogeny
ϕ
elliptic curve
(basis of)
endomorphism ring
endomorphism


isogeny
ϕ
elliptic curve
⟺
(basis of)
endomorphism ring
endomorphism

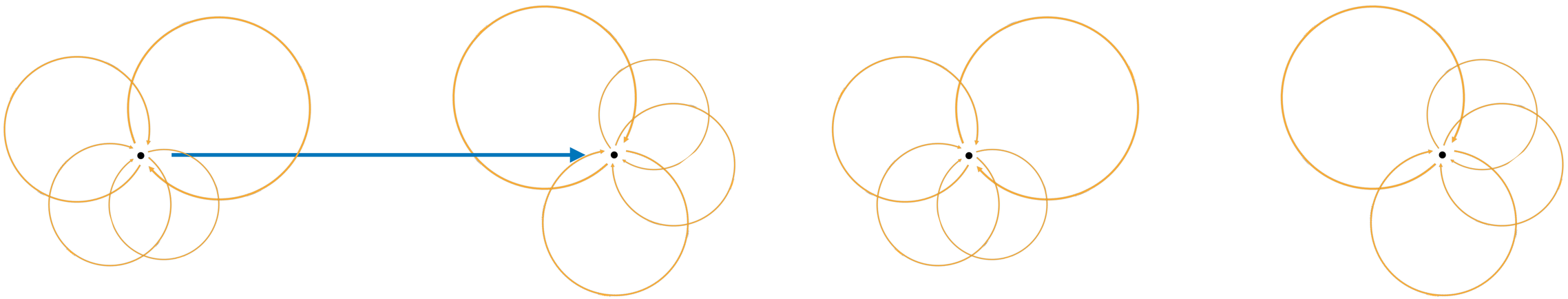




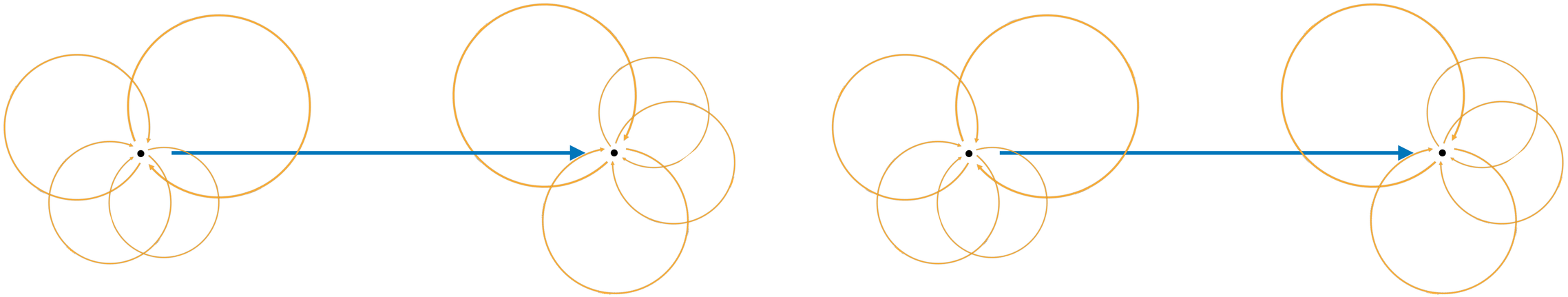




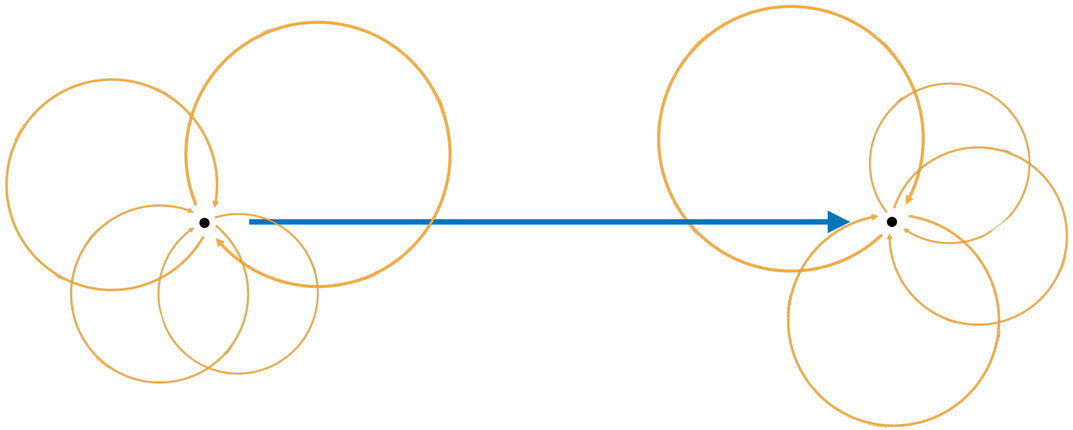
isogenies “carry”
knowledge of the
endomorphism ring



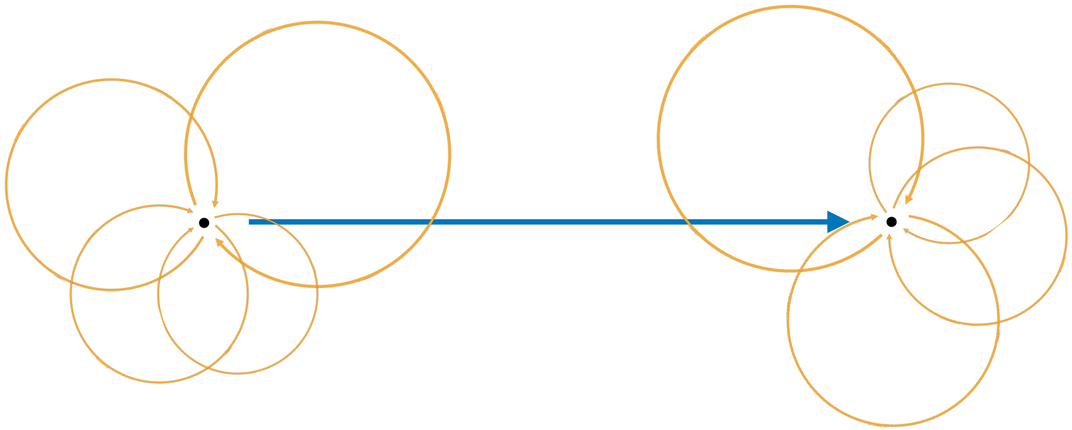
isogenies “carry” knowledge of the endomorphism ring



isogenies “carry” knowledge of the endomorphism ring

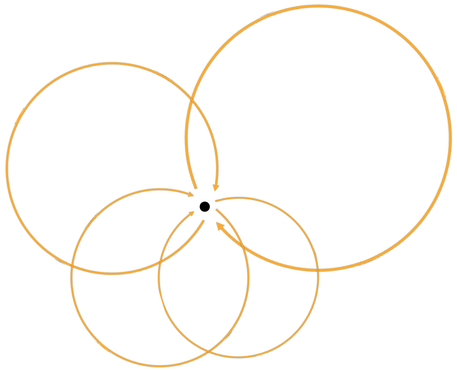


isogenies “carry”
knowledge of the
endomorphism ring

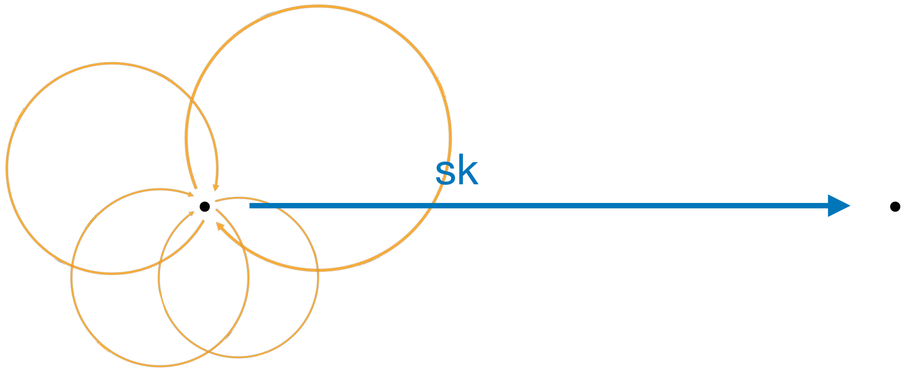


knowldege of
endomorphism rings
enable isogeny finding

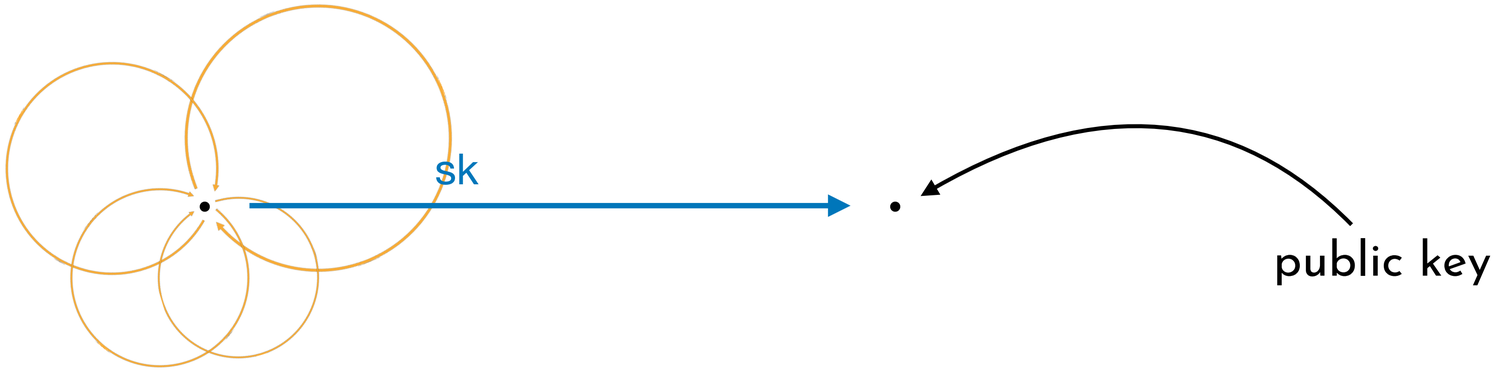
SQIsign – ID protocol



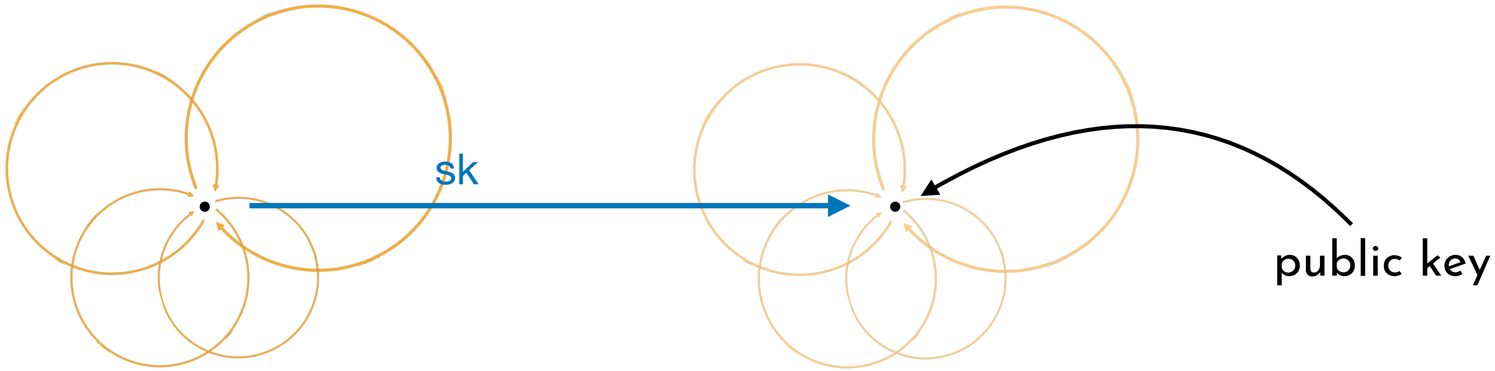
SQIsign – ID protocol



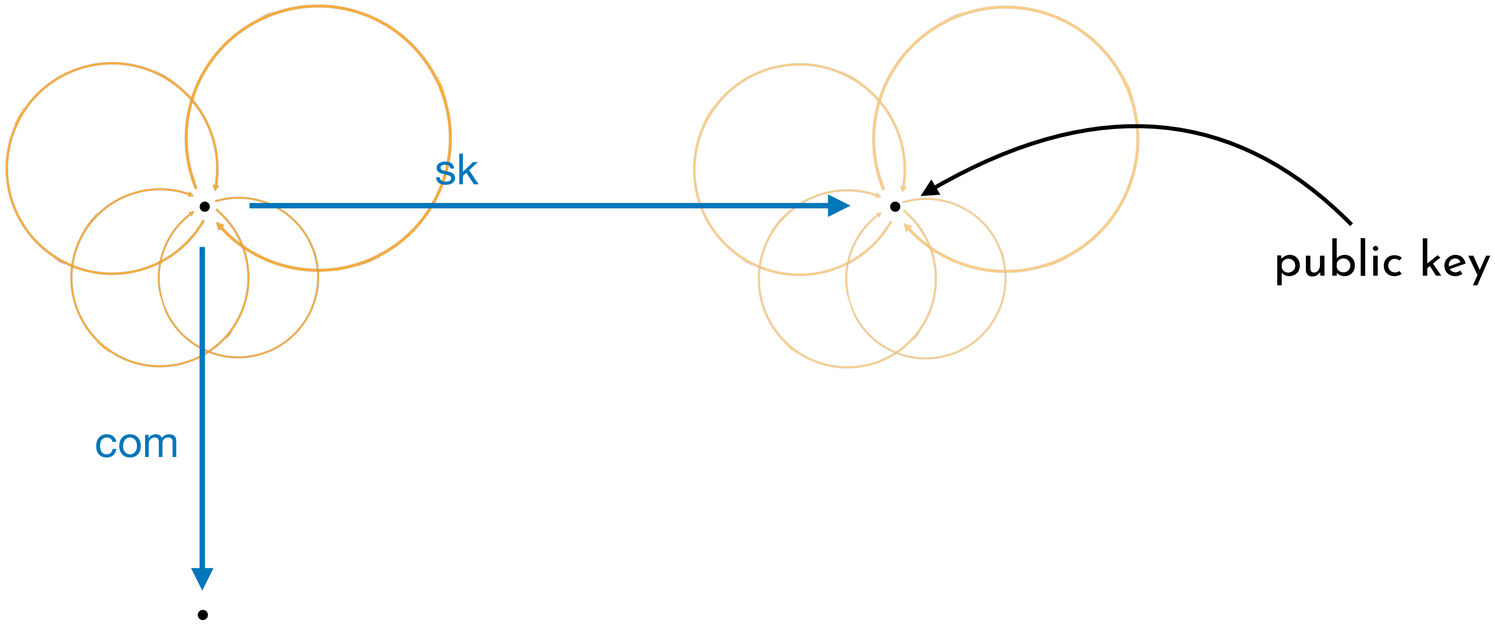
SQIsign – ID protocol



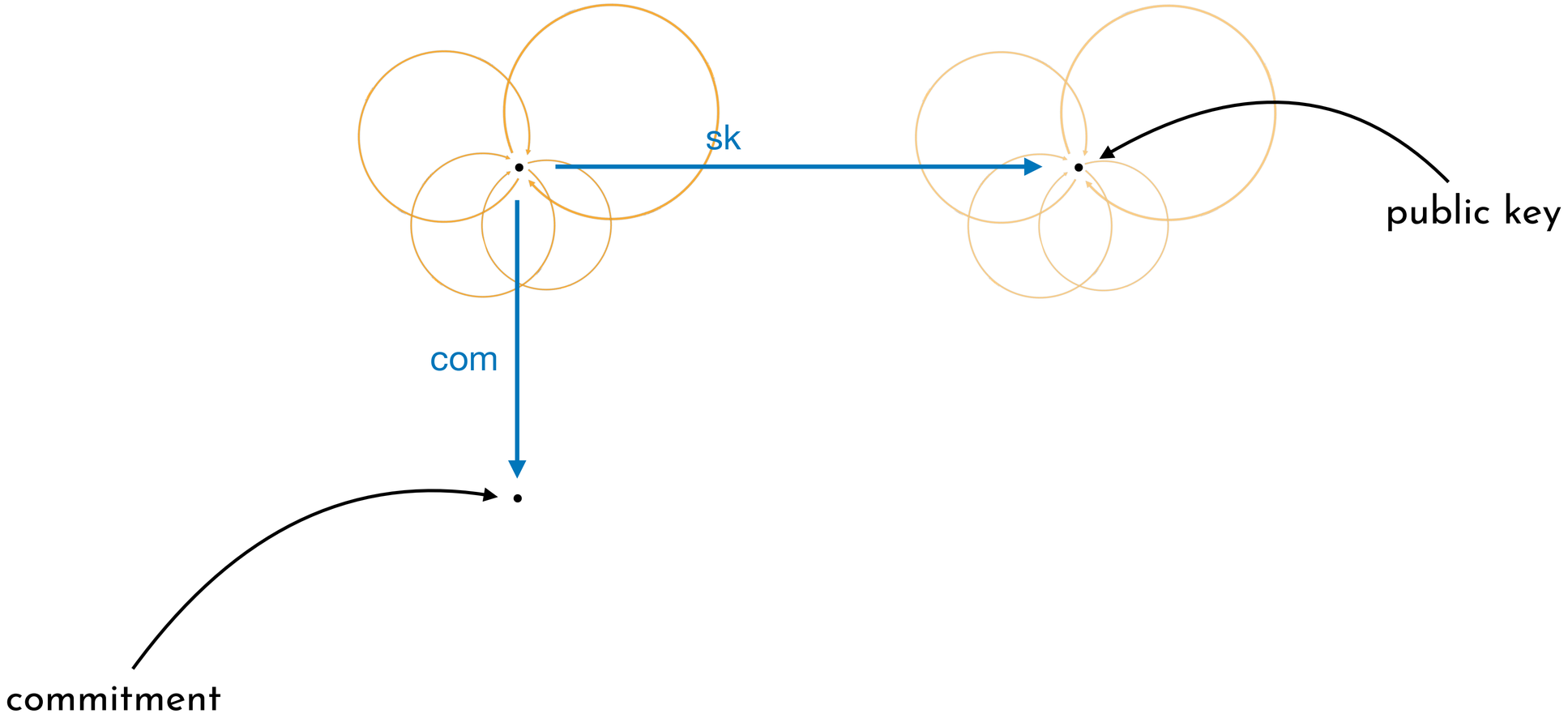
SQIsign – ID protocol



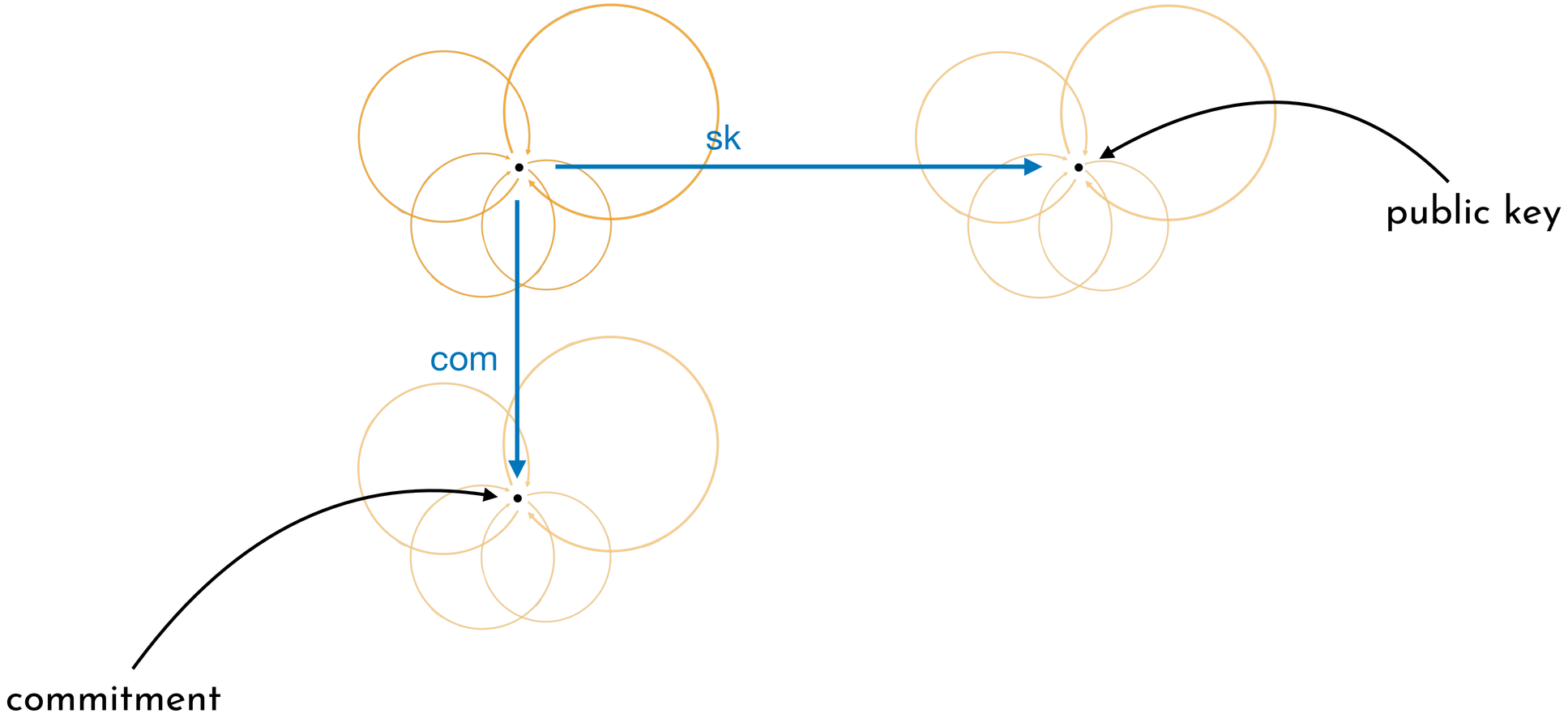
SQIsign – ID protocol



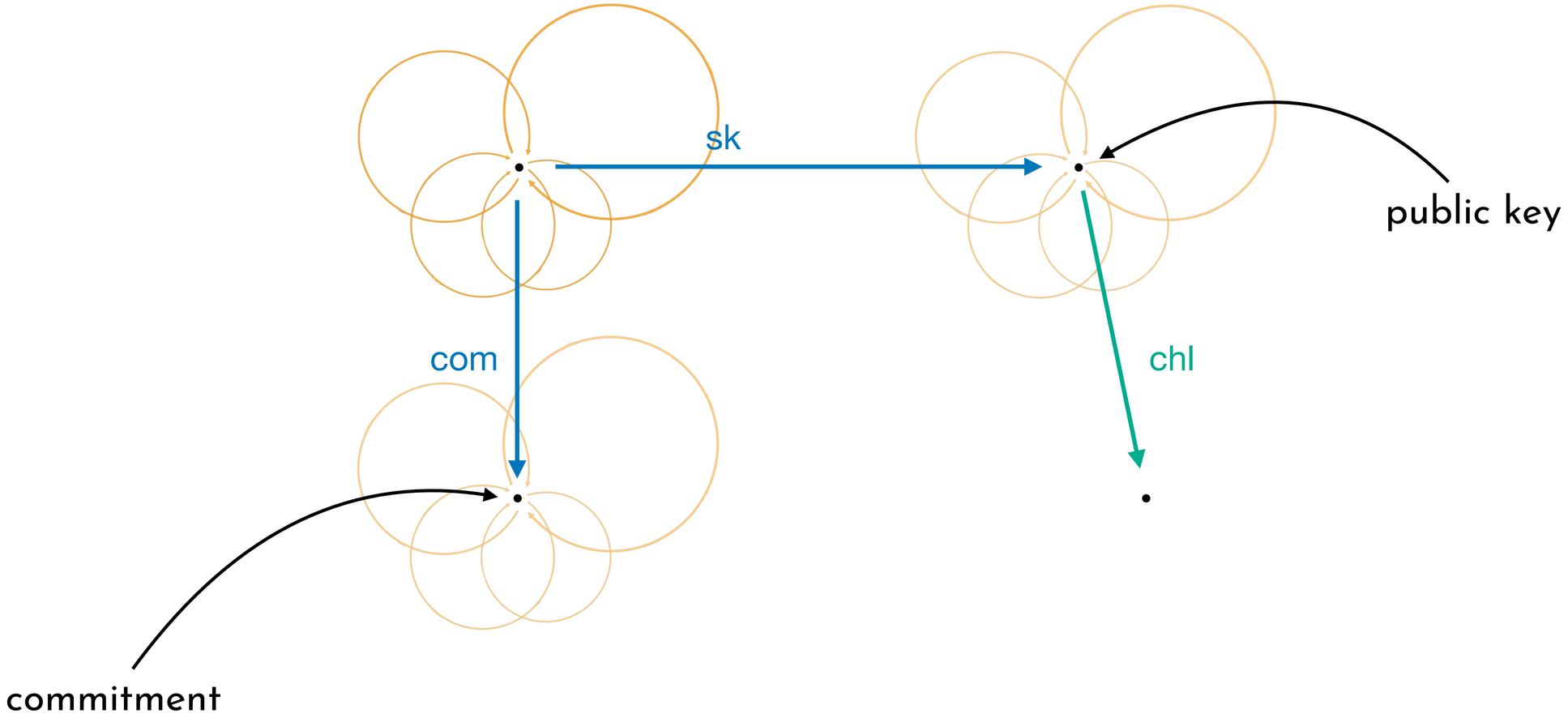
SQIsign – ID protocol



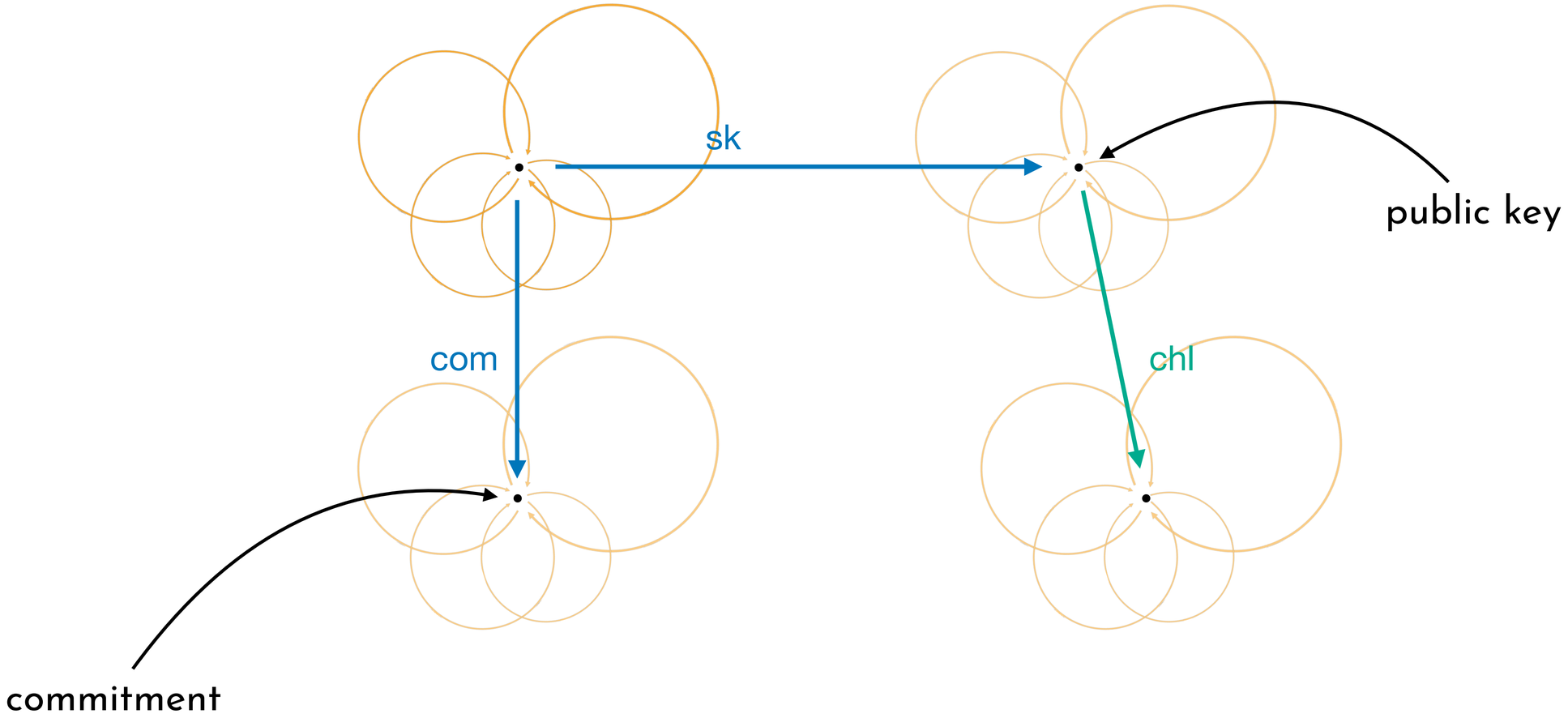
SQIsign – ID protocol



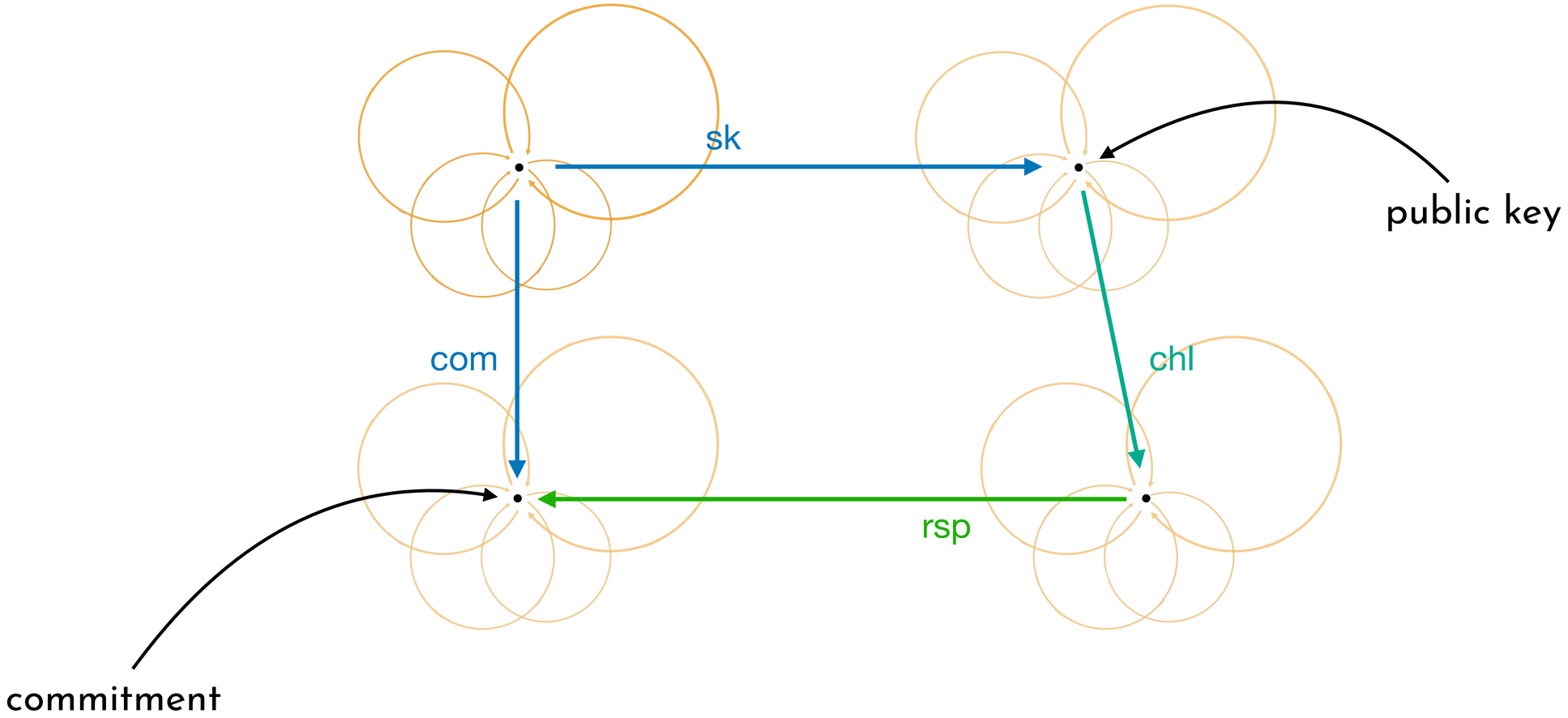
SQIsign – ID protocol



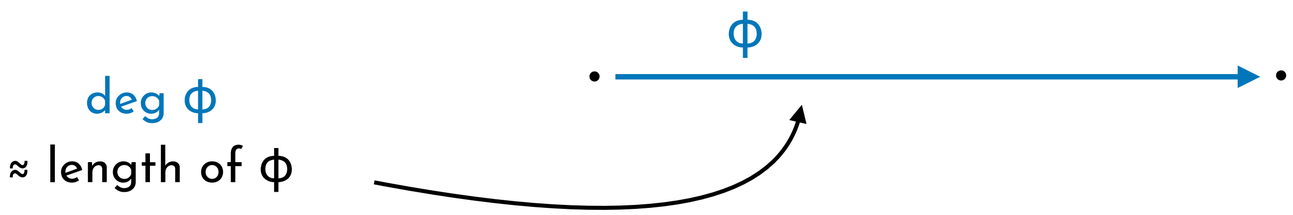
SQIsign – ID protocol



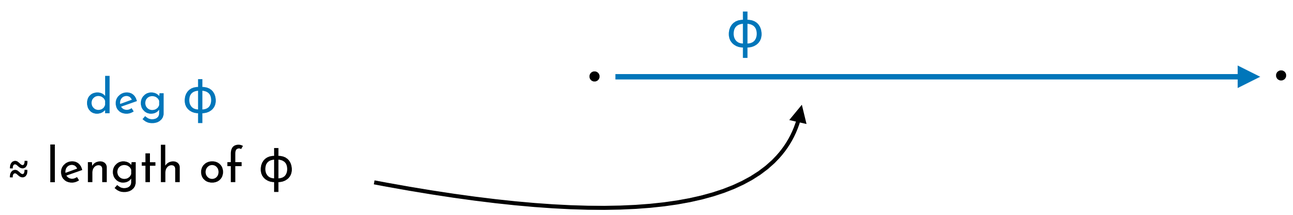
SQIsign – ID protocol



How do we represent isogenies?

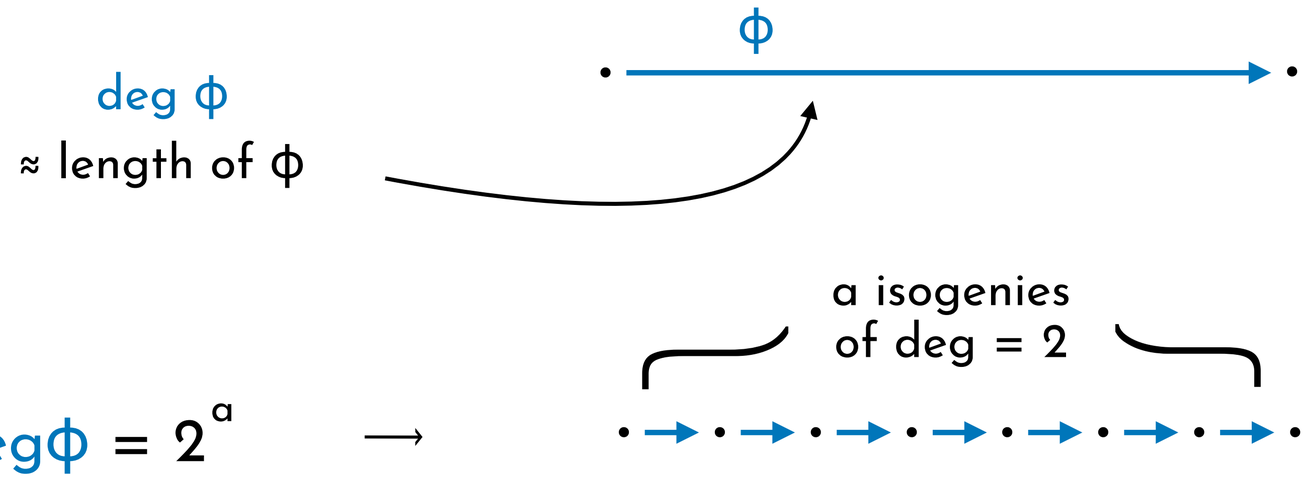


How do we represent isogenies?

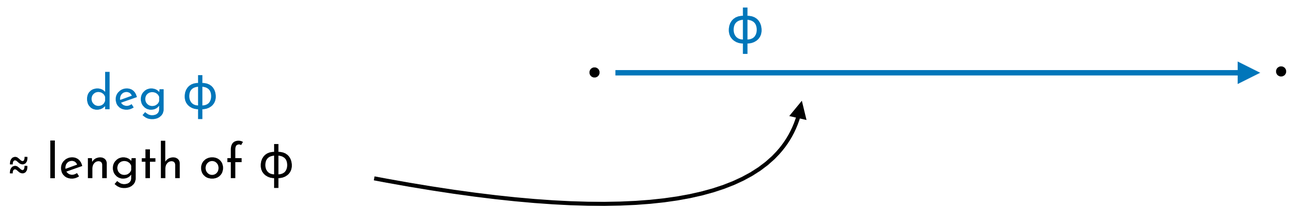


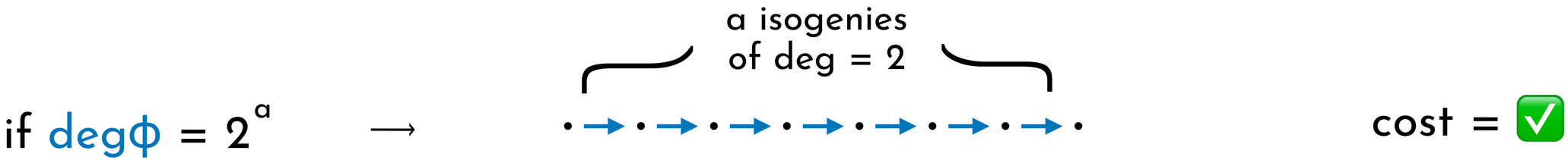
if $\deg\phi = 2^a$

How do we represent isogenies?

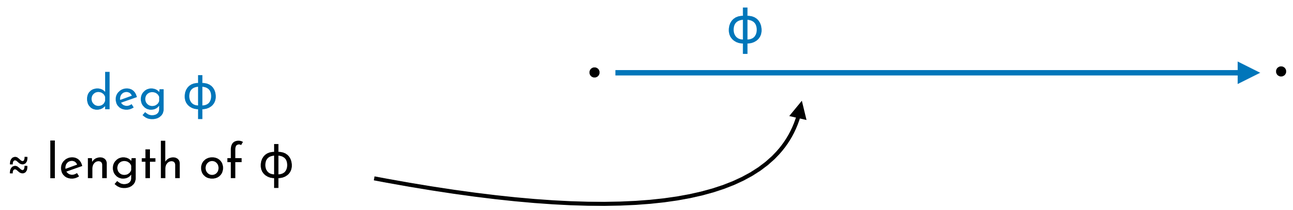


How do we represent isogenies?

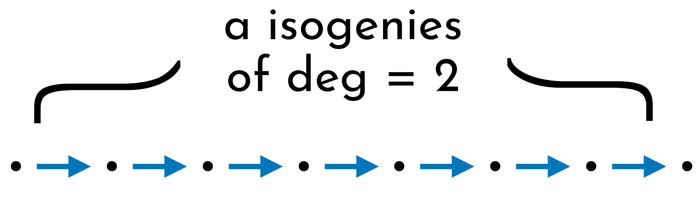




How do we represent isogenies?



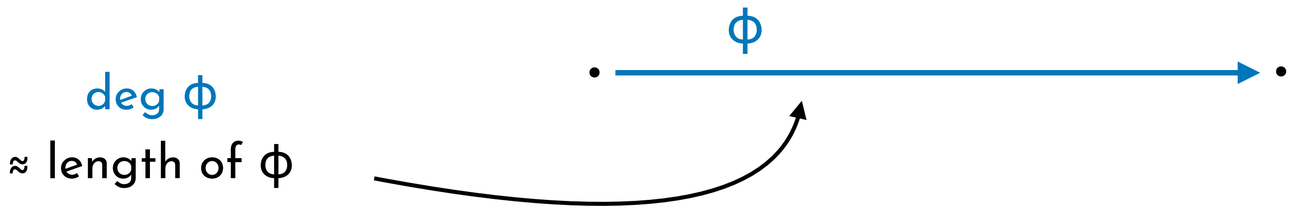
if $\deg\phi = 2^a$ ⟶



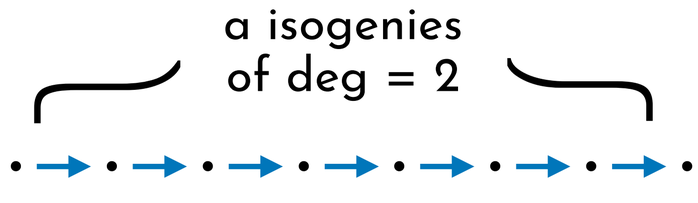
cost = ✅

if $\deg\phi$ = prime

How do we represent isogenies?



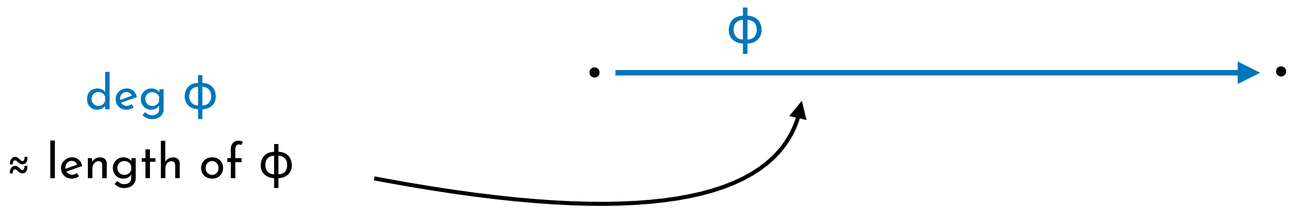
if $\deg\phi = 2^a$ ⟶

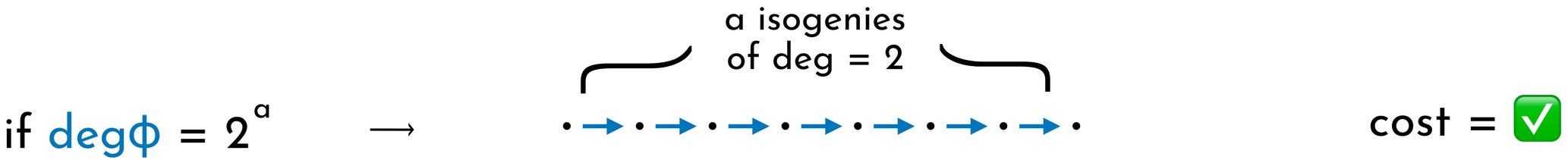


cost = ✅

if $\deg\phi$ = prime ???

How do we represent isogenies?

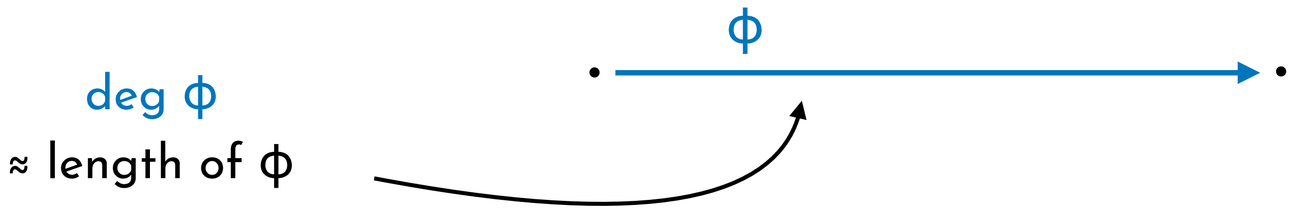


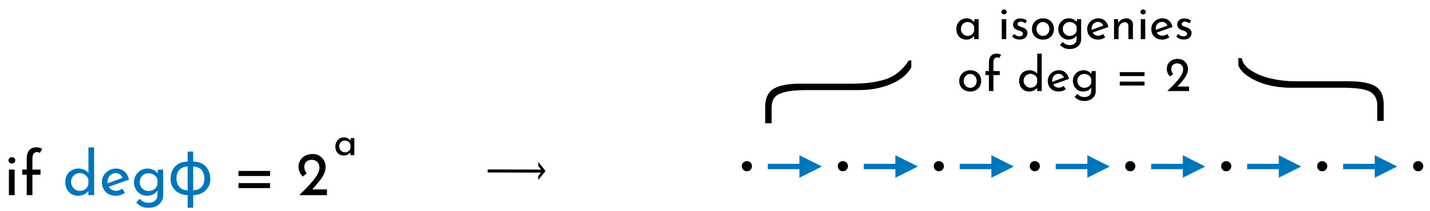


if degϕ = prime — Higher-dimensional representation

- E_0, E_1
- P, Q and ϕ(P), ϕ(Q)
- deg ϕ

How do we represent isogenies?





if degϕ = prime

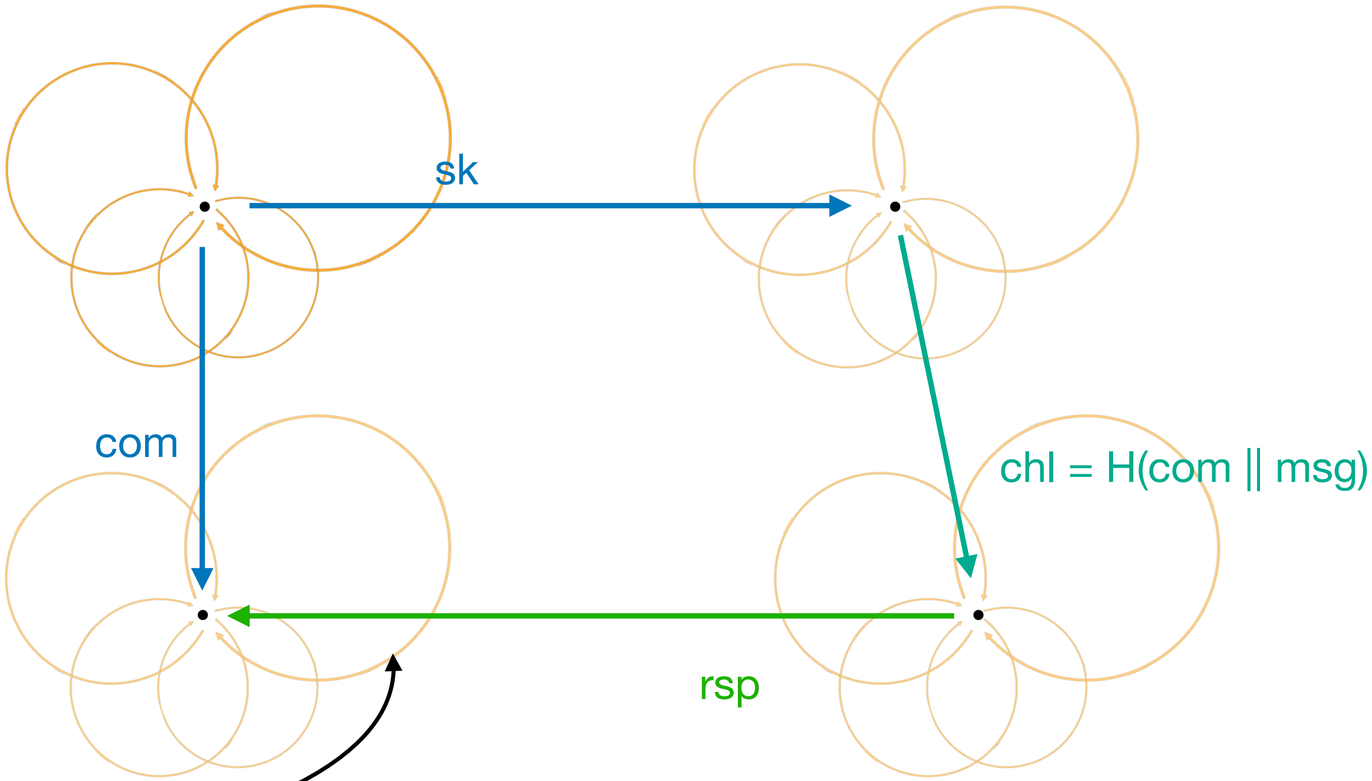
Higher-dimensional representation

- E_0, E_1
- P, Q and ϕ(P), ϕ(Q)
- deg ϕ

cost =

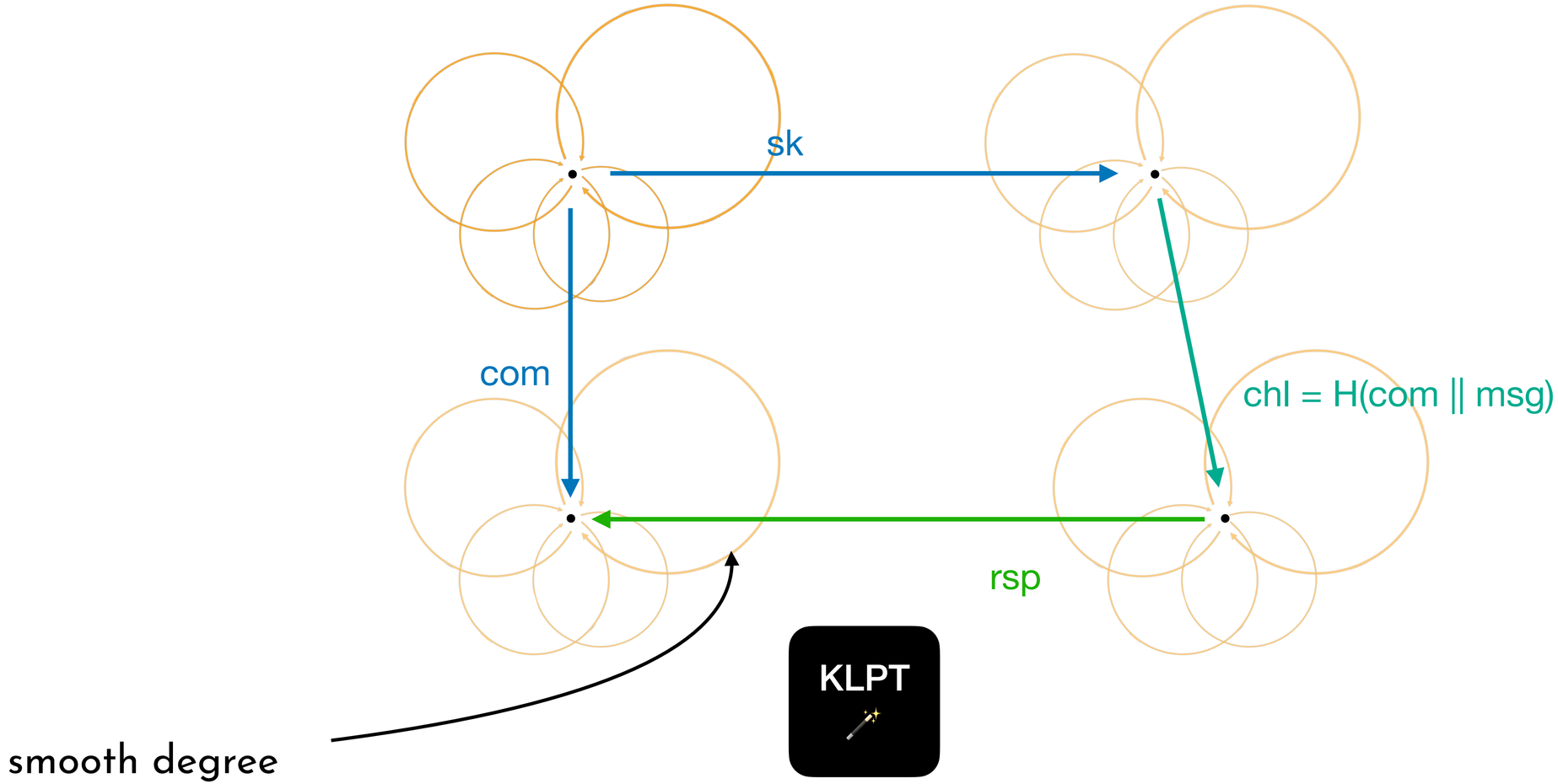
- 😄 if degϕ = q(2^a - q)
- 😐 otherwise

SQIsign1D – smooth responses

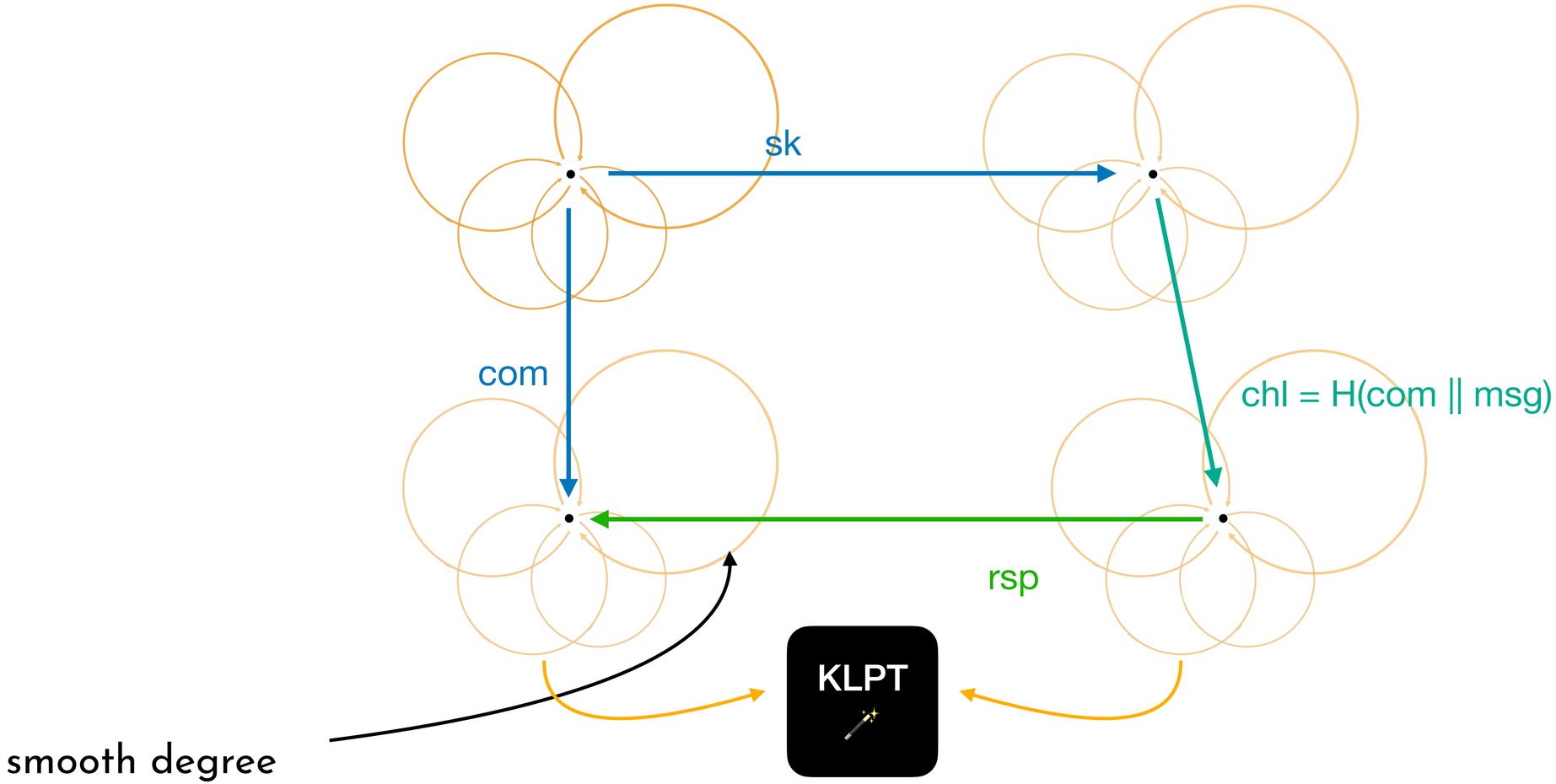


smooth degree

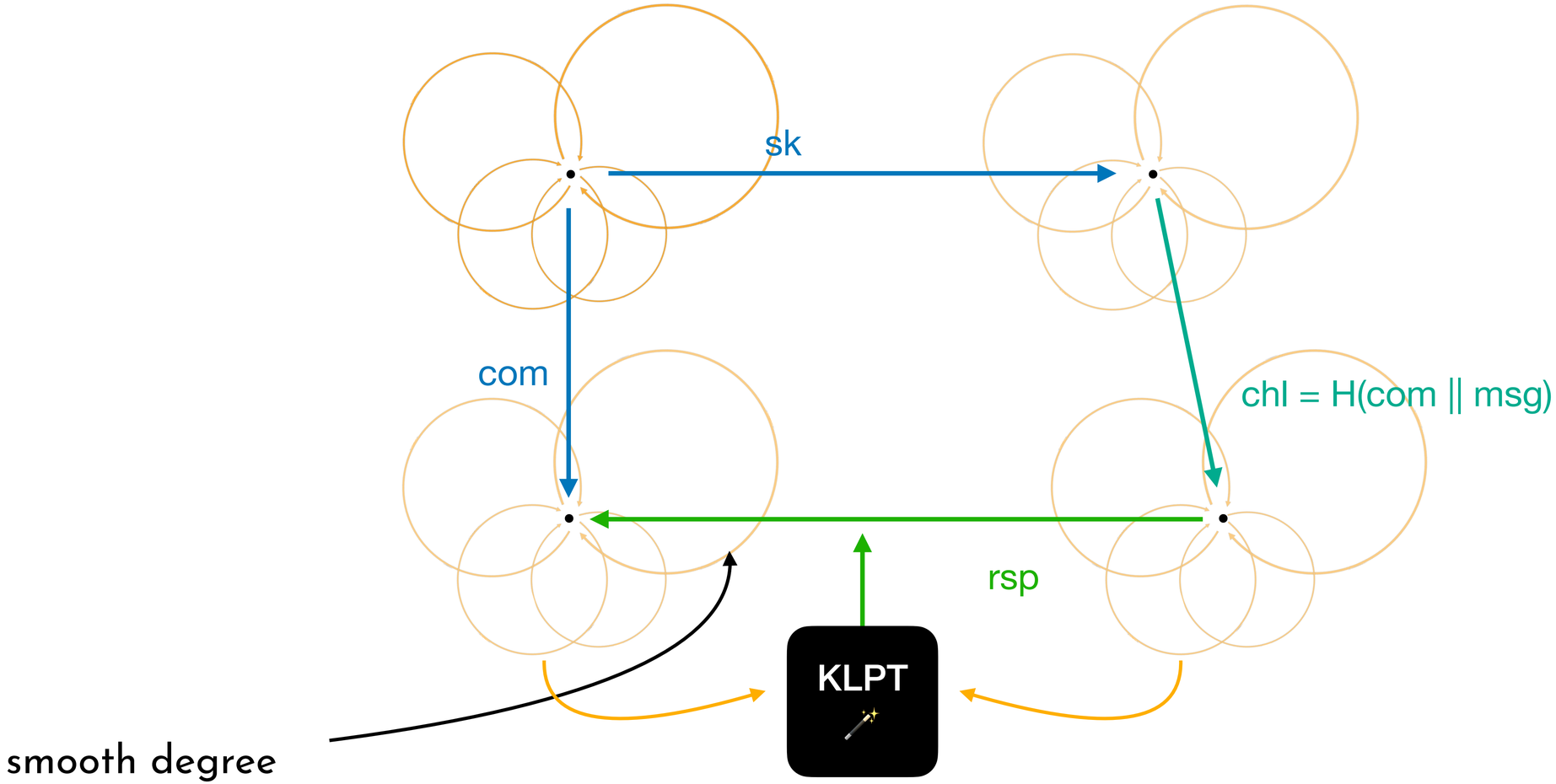
SQIsign1D – smooth responses



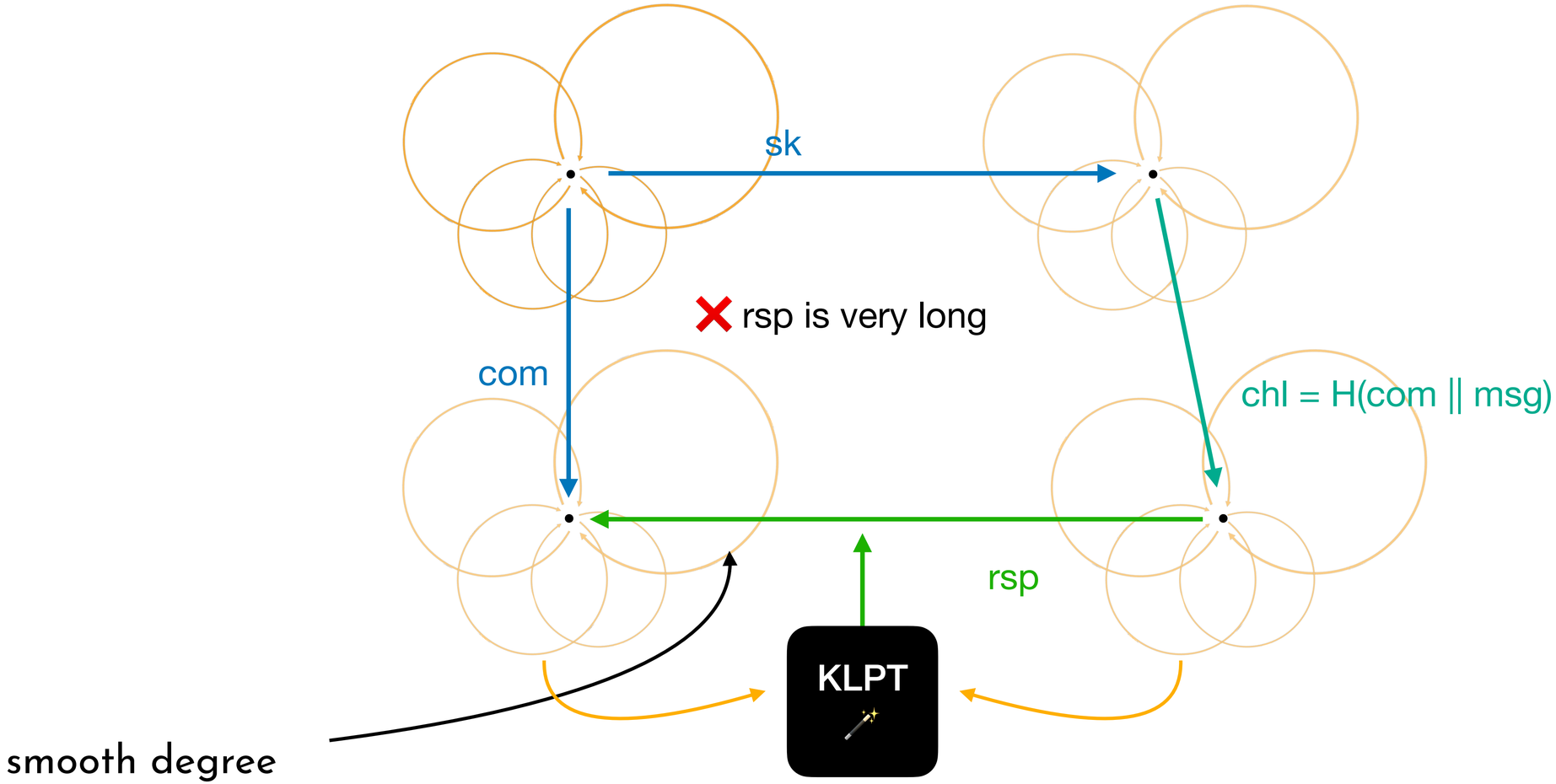
SQIsign1D – smooth responses



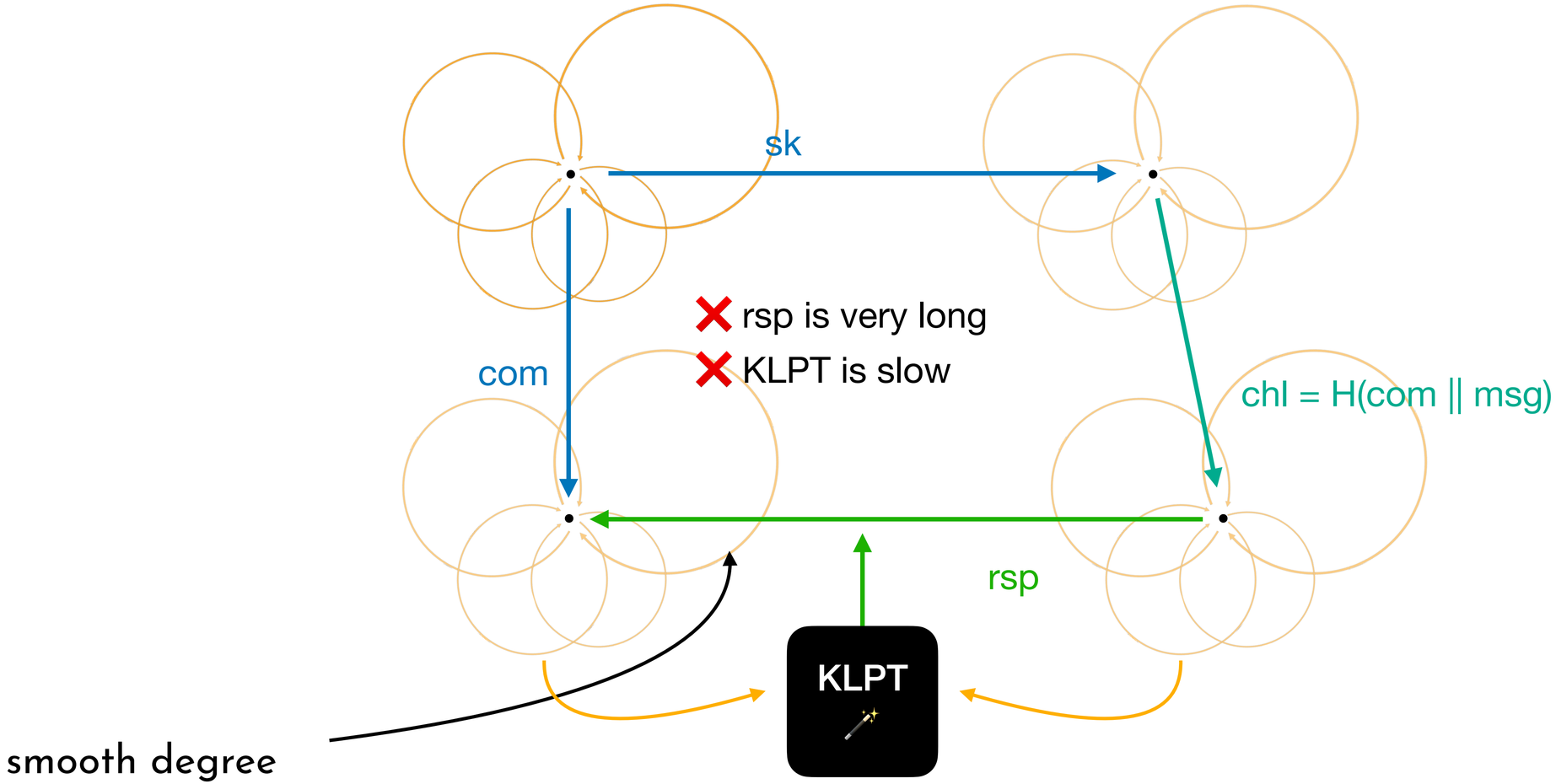
SQIsign1D – smooth responses



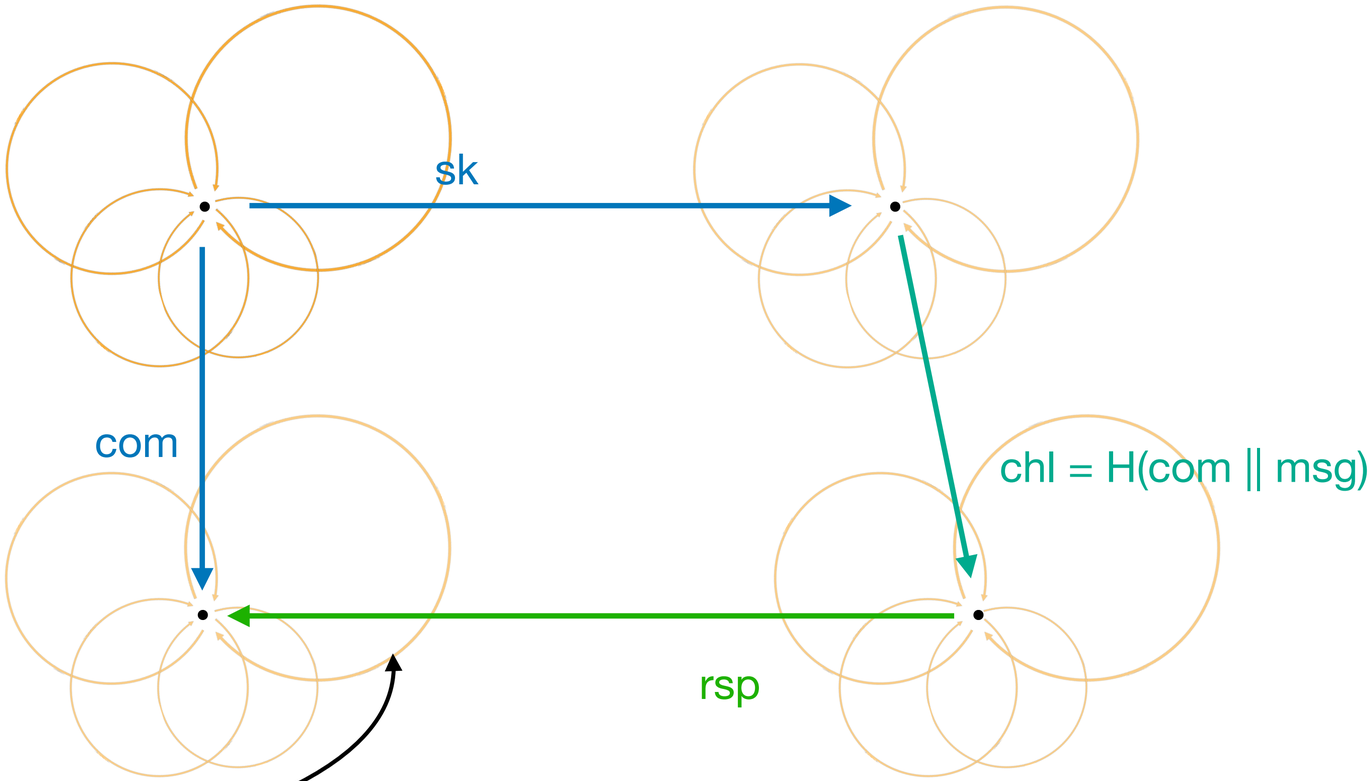
SQIsign1D – smooth responses



SQIsign1D – smooth responses

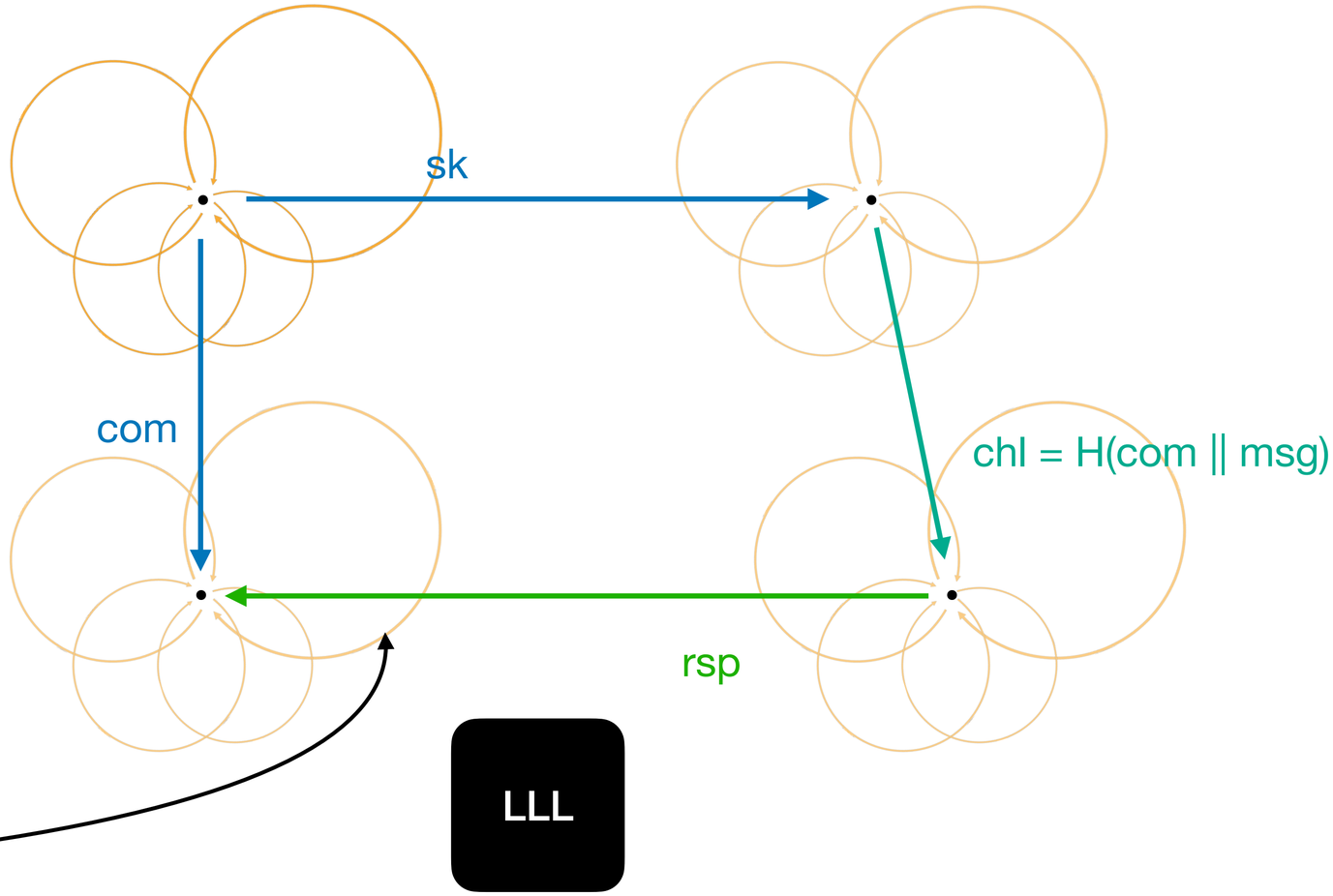


SQIsignHD

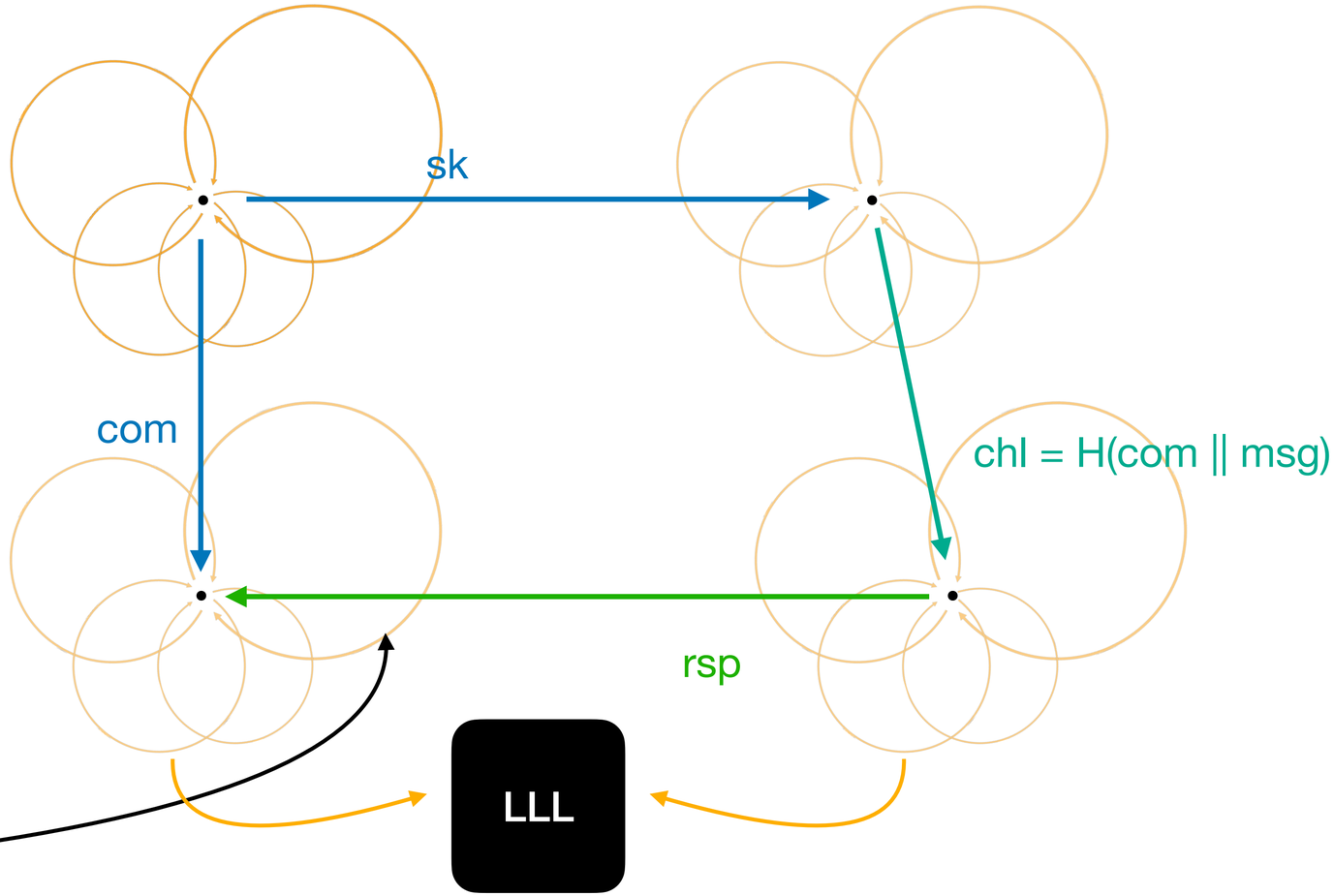


UNsmooth degree,
4-dimensional
representation

SQIsignHD

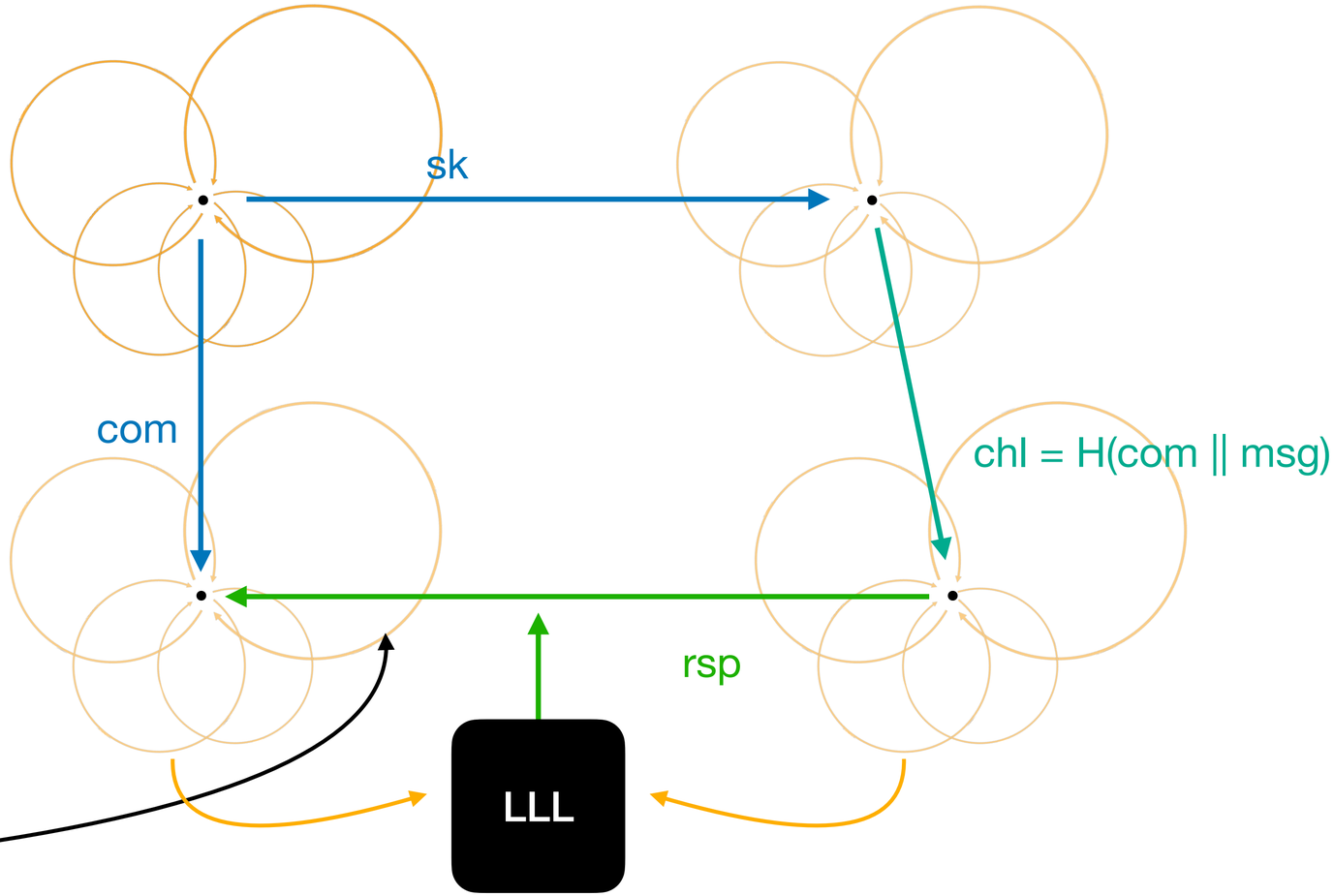

sk
com
chl = H(com || msg)
rsp
LLL
UNsmooth degree,
4-dimensional
representation

SQIsignHD



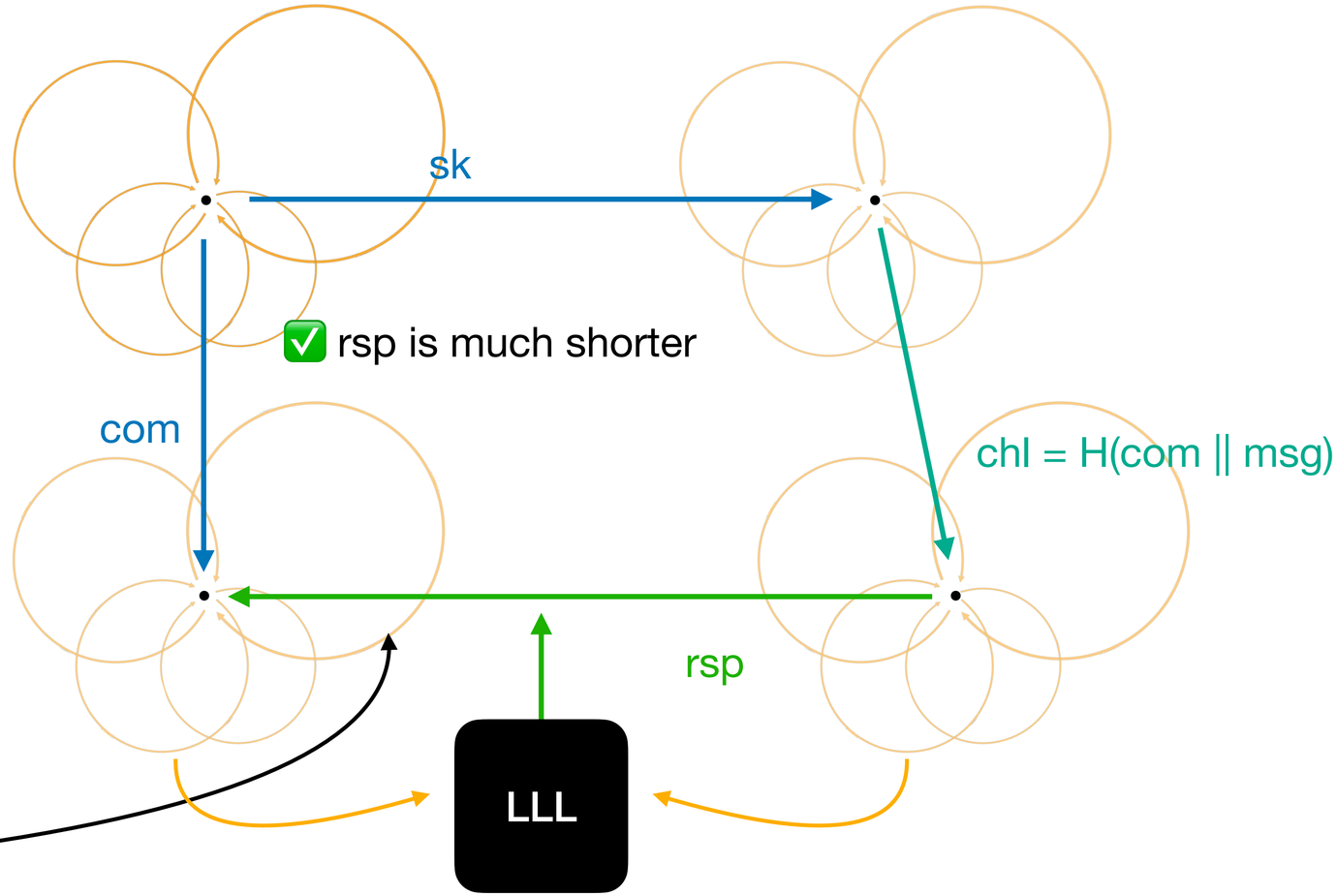
UNsmooth degree,
4-dimensional
representation

SQIsignHD

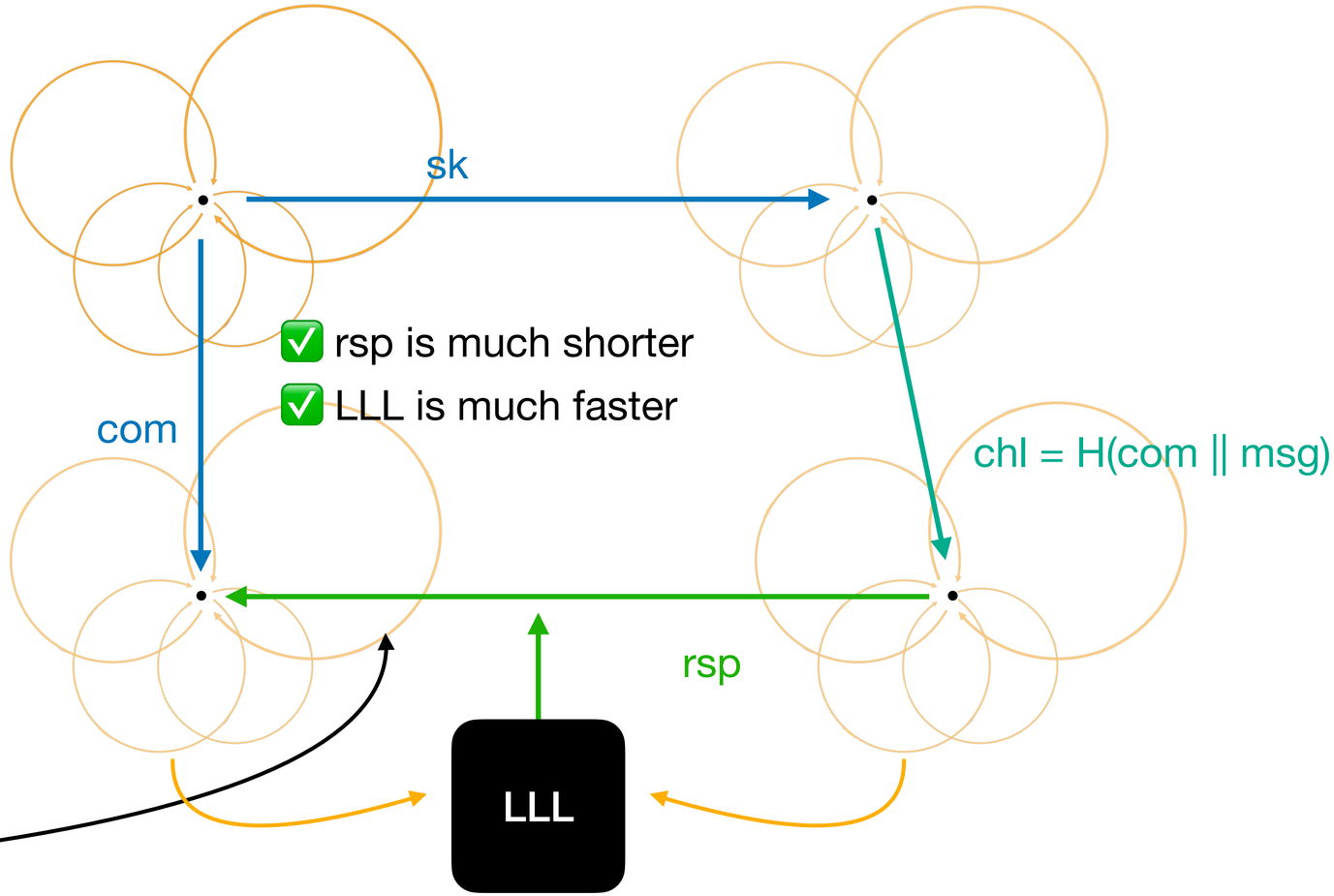


UNsmooth degree,
4-dimensional
representation

SQIsignHD

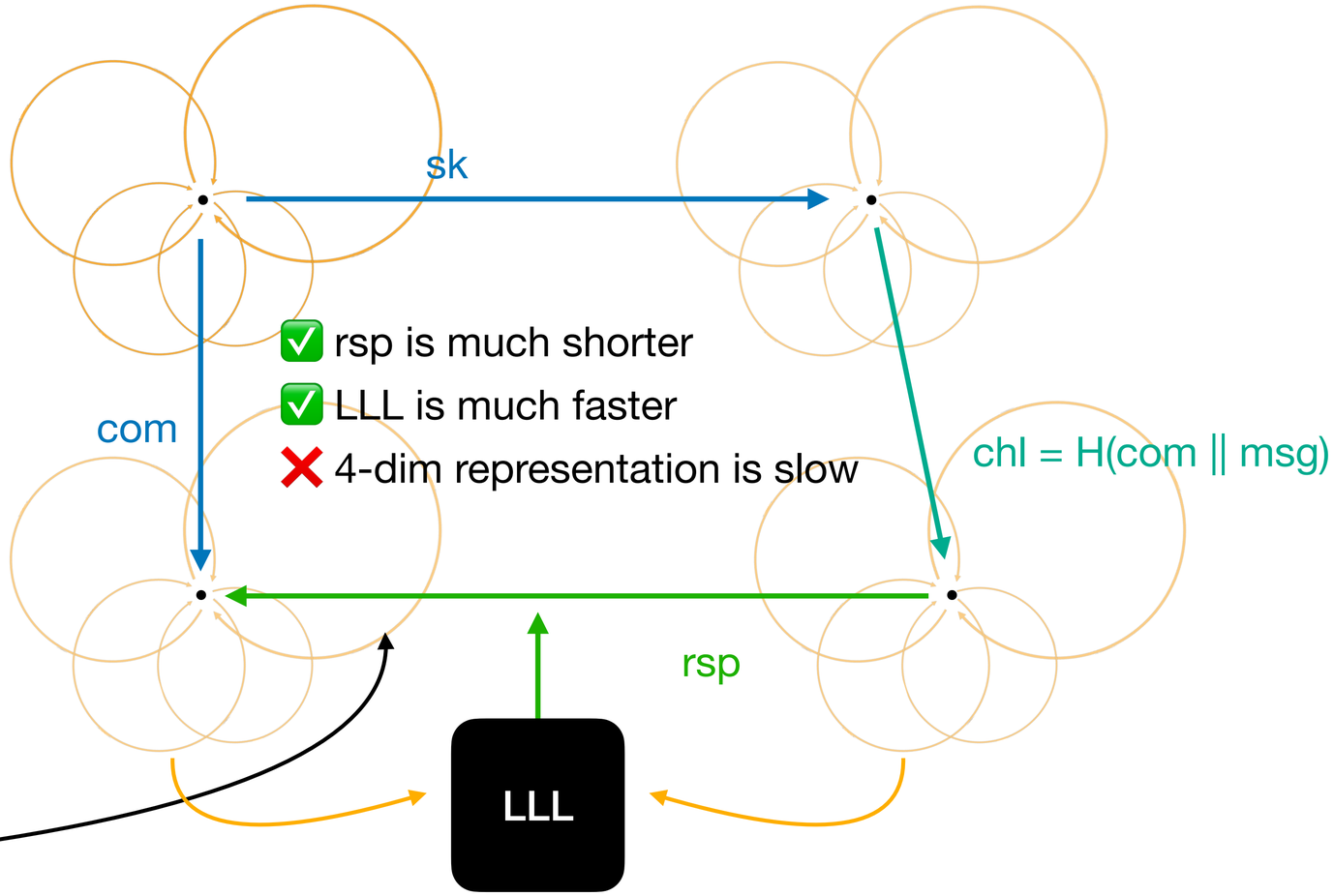

sk
✅ rsp is much shorter
com
chl = H(com || msg)
rsp
LLL
UNsmooth degree,
4-dimensional
representation

SQIsignHD



UNsmooth degree,
4-dimensional
representation

SQIsignHD

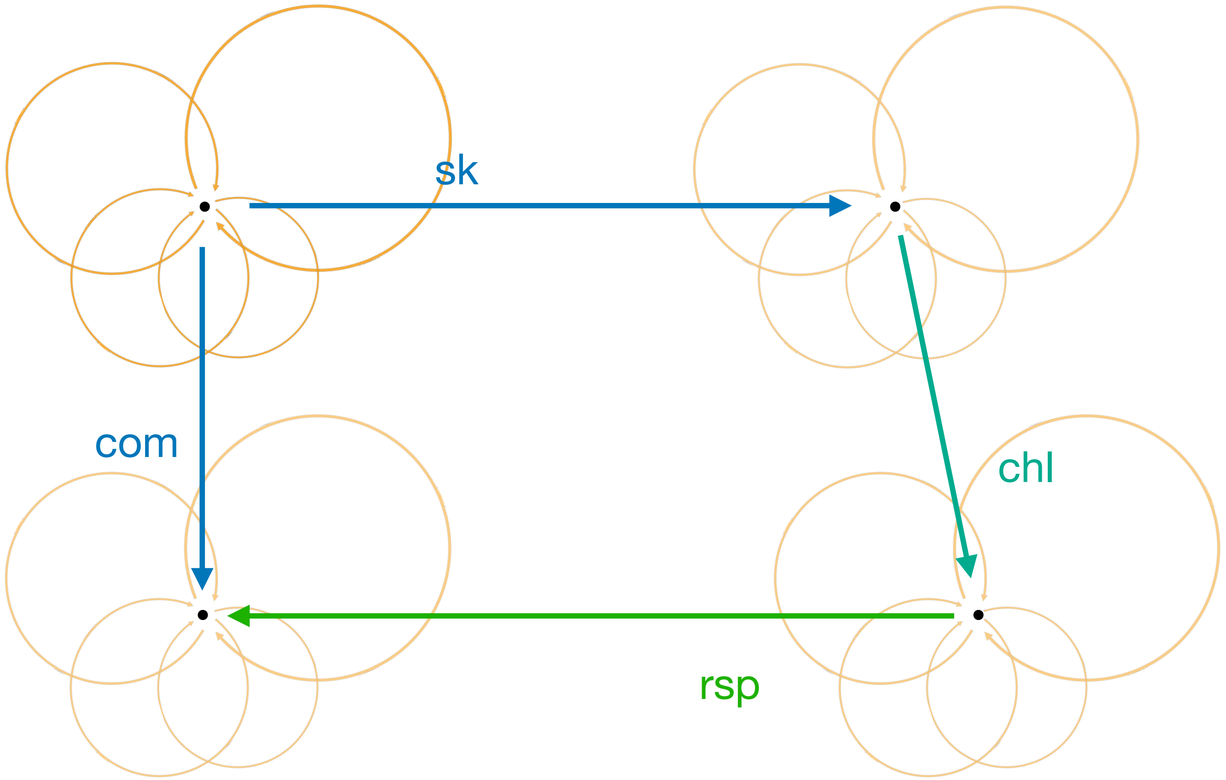


UNsmooth degree,
4-dimensional
representation

SQIsign2D

2-dimensional representation requires

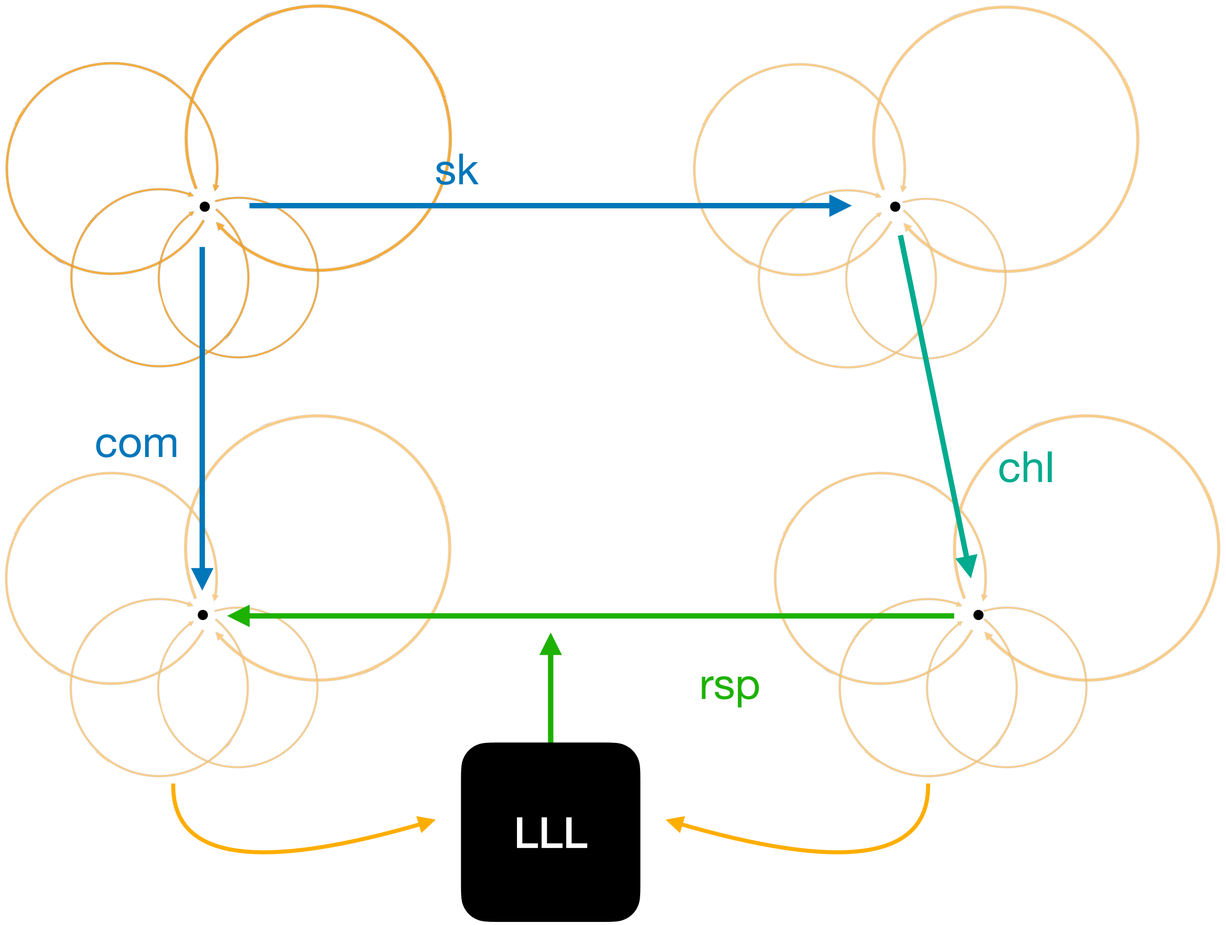
deg rsp = $q(2^a - q)$



SQIsign2D

2-dimensional representation requires

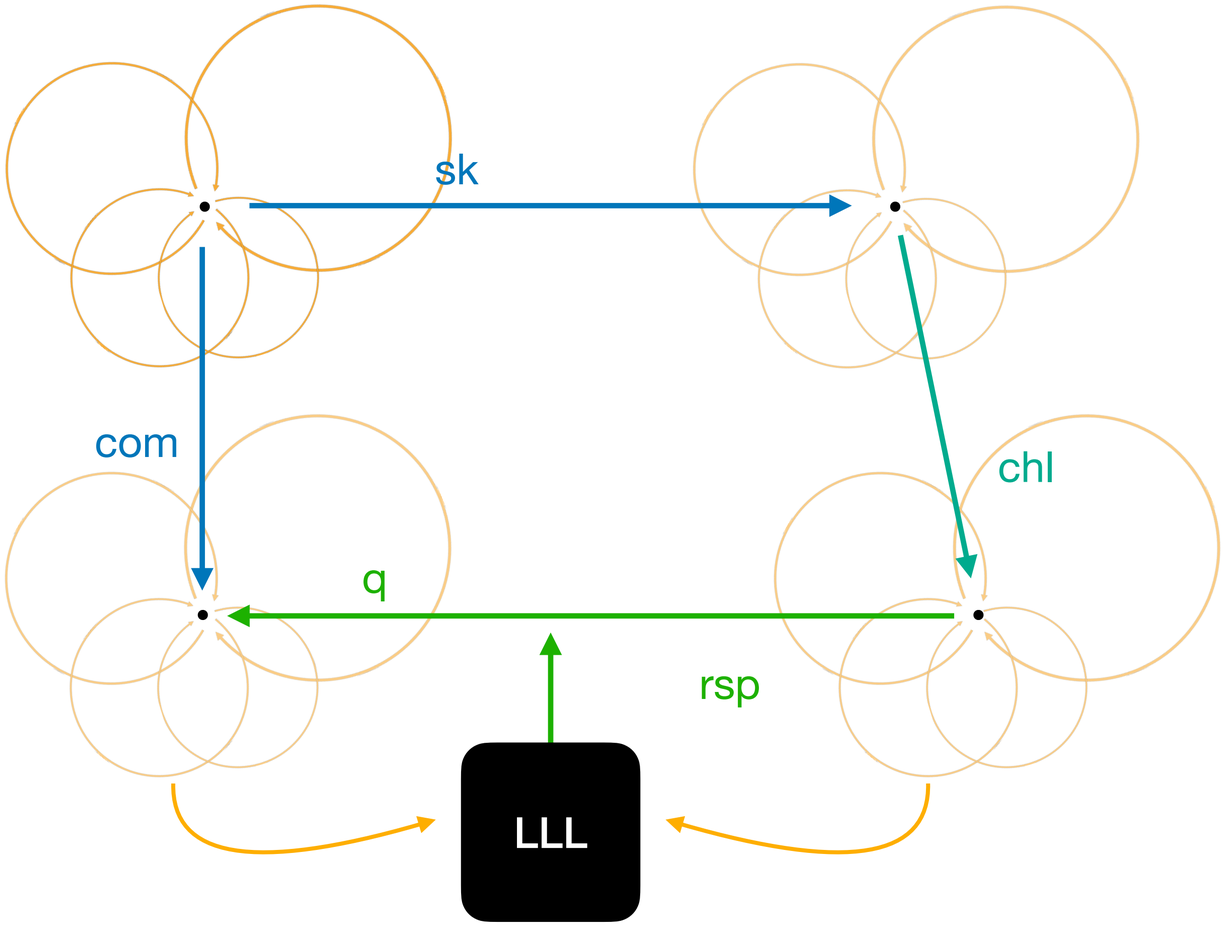
deg rsp = $q(2^a - q)$



SQIsign2D

2-dimensional representation requires

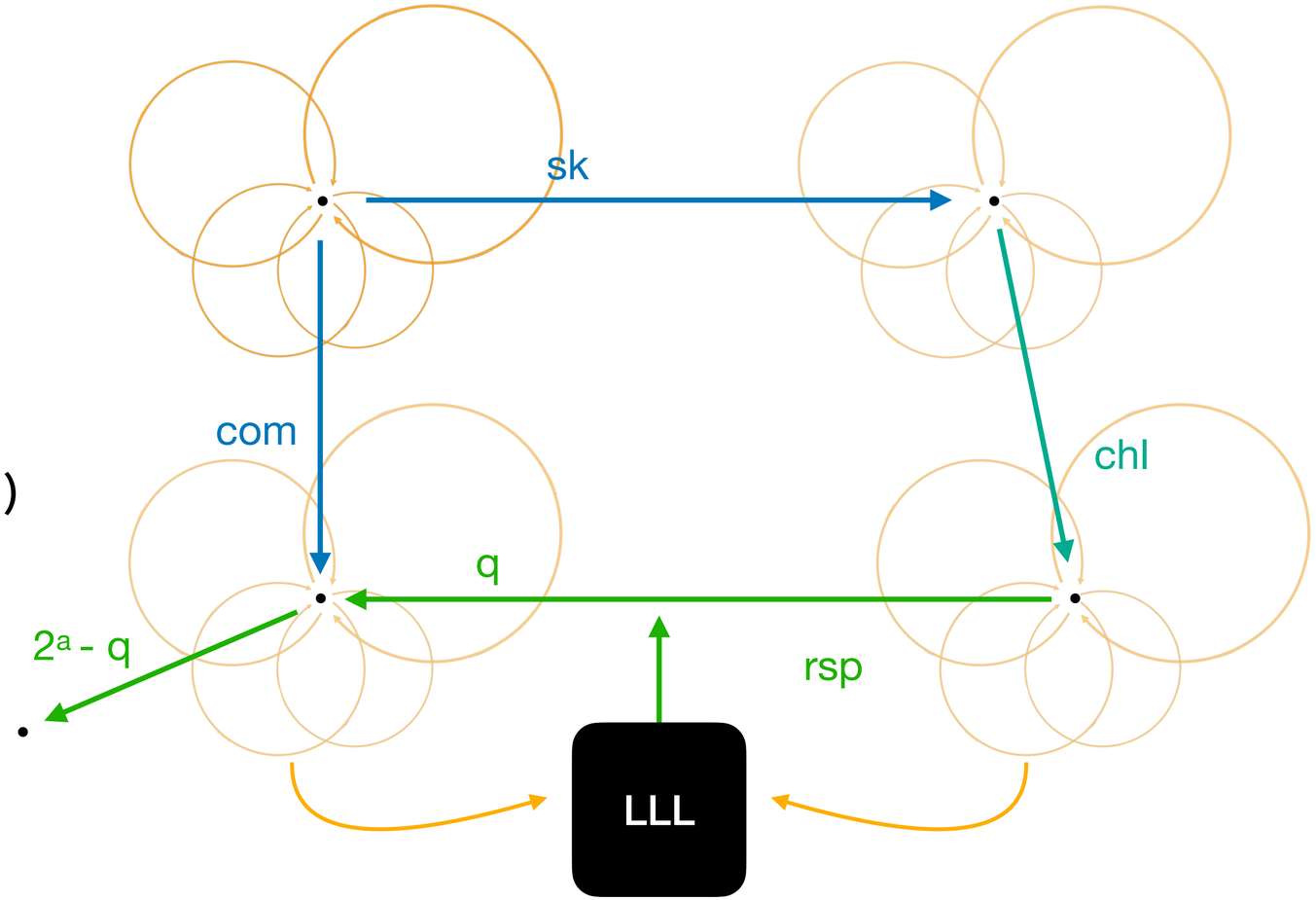
deg rsp = $q(2^a - q)$



SQIsign2D

2-dimensional representation requires

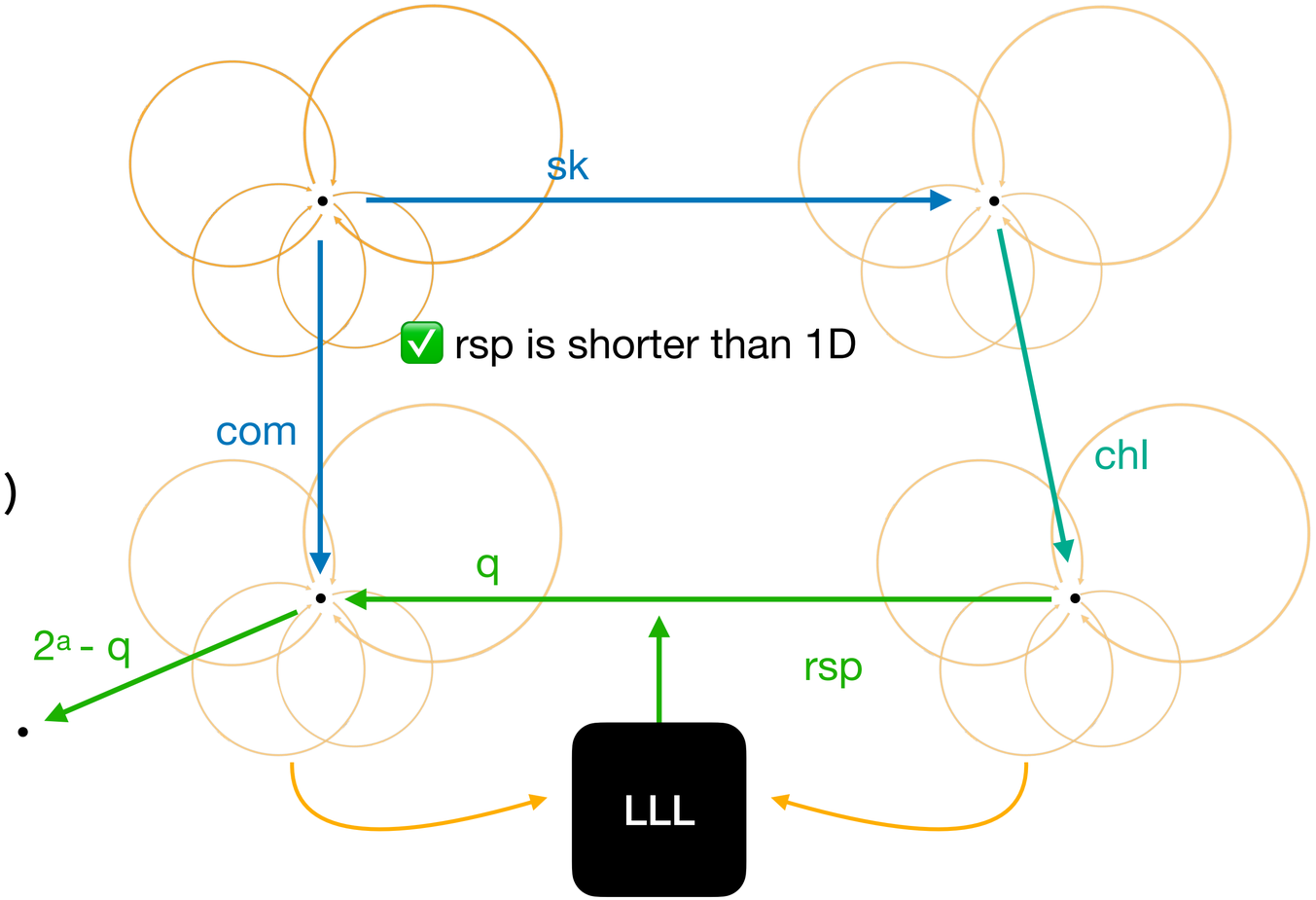
deg rsp = $q(2^a - q)$



SQIsign2D

2-dimensional representation requires

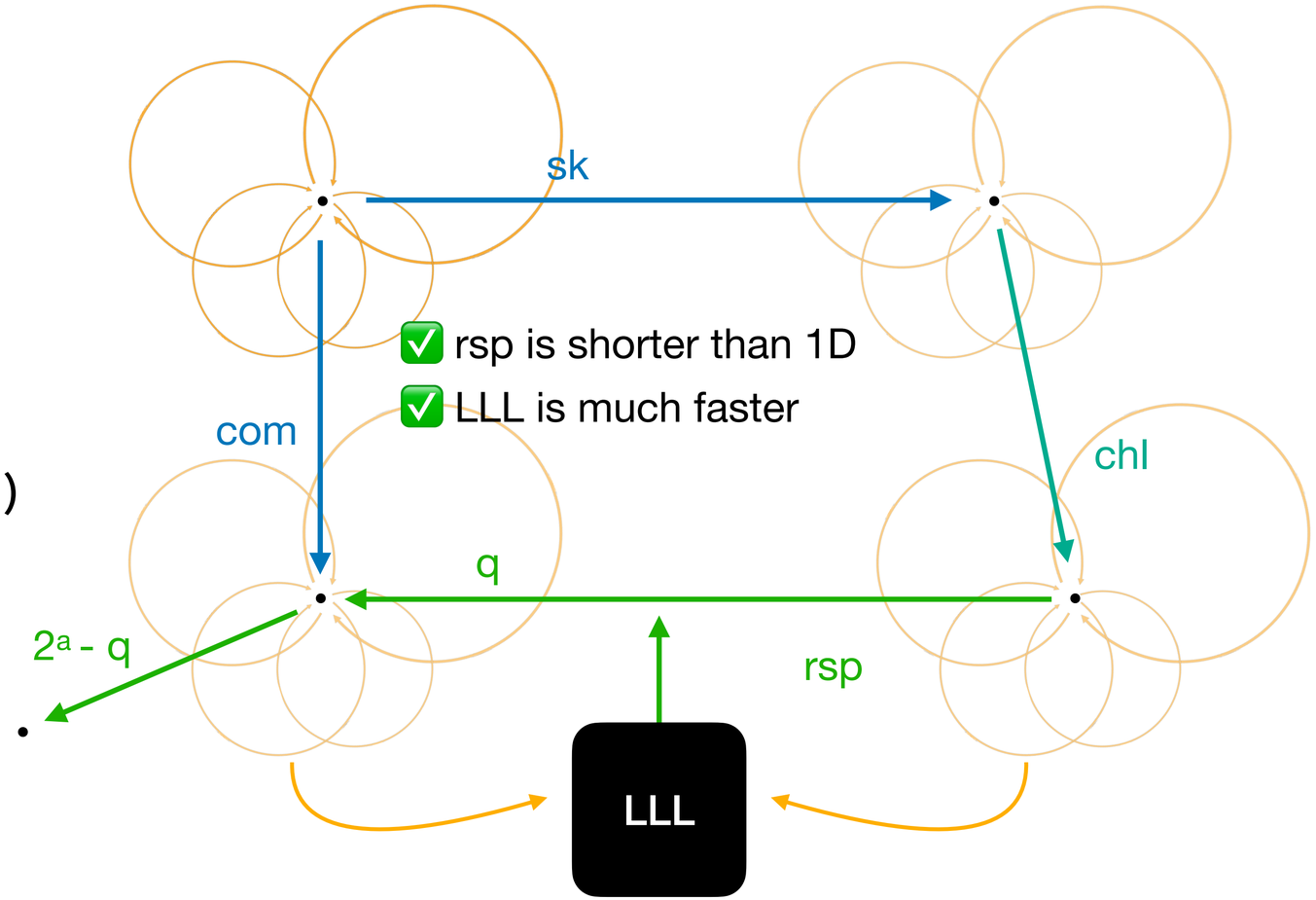
deg rsp = $q(2^a - q)$



SQIsign2D

2-dimensional representation requires

deg rsp = $q(2^a - q)$



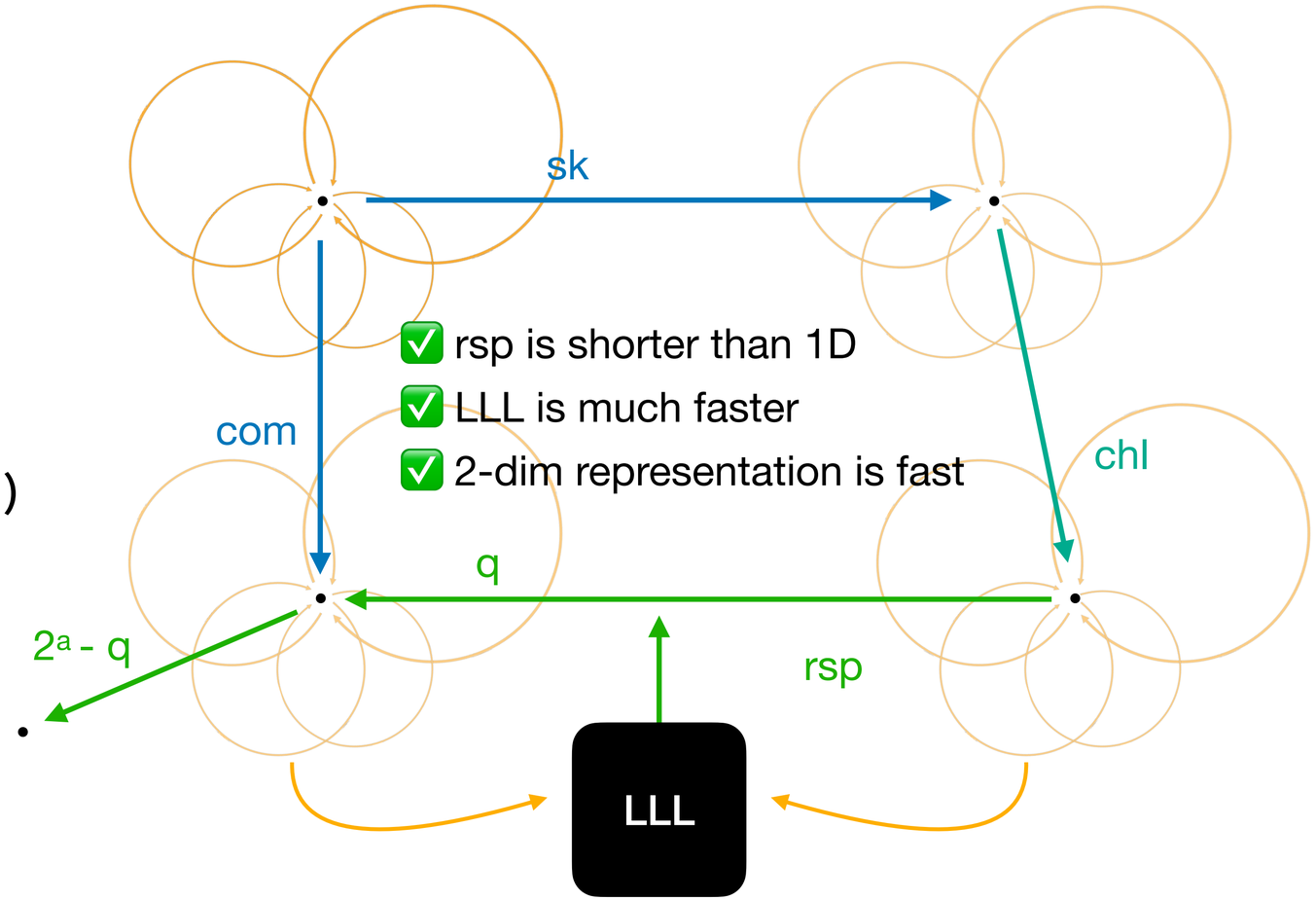
✅ rsp is shorter than 1D

✅ LLL is much faster

SQIsign2D

2-dimensional representation requires

deg rsp = $q(2^a - q)$



✅ rsp is shorter than 1D

✅ LLL is much faster

✅ 2-dim representation is fast

SQIsign SQIsignHD SQIsign2D

		SQIsign	SQIsignHD	SQIsign2D
Signature size		🎉	🎉🎉	🎉

	SQIsign	SQIsignHD	SQIsign2D
Signature size	🎉	🎉🎉	🎉
Signing efficiency	😔	👍👍	👍

	SQIsign	SQIsignHD	SQIsign2D
Signature size	🎉	🎉🎉	🎉
Signing efficiency	😔	👍👍	👍
Verification efficiency	👍	😶	👍👍

	SQIsign	SQIsignHD	SQIsign2D
Signature size	🎉	🎉🎉	🎉
Signing efficiency	😔	👍👍	👍
Verification efficiency	👍	😶	👍👍
Security	😶	👍	👍

	SQIsign	SQIsignHD	SQIsign2D
Signature size	🎉	🎉🎉	🎉
Signing efficiency	😔	👍👍	👍
Verification efficiency	👍	😶	👍👍
Security	😶	👍	👍
Scalability	👎	🎉	🎉

SQIsign2D brings the efficiency of 2D representations while keeping HD improvements

1

SQIsign2D brings the efficiency of 2D representations while keeping HD improvements

2

Better security due to weaker assumptions than SQIsign1D

1 **SQIsign2D** brings the efficiency of 2D representations while keeping HD improvements

2 Better security due to weaker assumptions than SQIsign1D

3 Big improvements in short time (thanks to *HD representations*): what comes next?

SQIsign2D-West: The Fast, the Small, and the Safer

Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert and Benjamin Wesolowski

10^{th} December, 2024

What does it mean?

- **The Fast:** together with SQIsign2D-East, it is the fastest variant.

What does it mean?

- **The Fast:** together with SQIsign2D-East, it is the fastest variant.
- **The Small:** incredibly compact!

	NIST I	NIST III	NIST V
Pub. key (B)	66	98	130
Signature (B)	148	222	294

What does it mean?

- **The Fast:** together with SQIsign2D-East, it is the fastest variant.
- **The Small:** incredibly compact!
- **The Safer:** provable security.

	NIST I	NIST III	NIST V
Pub. key (B)	66	98	130
Signature (B)	148	222	294

Fixed-Degree Isogeny [NO24]

Setup

Let $E_0/\mathbb{F}_p$ be the curve with j-invariant 1728, where $p = c \cdot 2^e - 1$. Define $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$.

Fixed-Degree Isogeny [NO24]

Setup

Let $E_0/\mathbb{F}_p$ be the curve with j-invariant 1728, where $p = c \cdot 2^e - 1$. Define $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$.

`FixedDegreeIsogeny`(u)

I An odd $0 < u < 2^e$.

O An isogeny $\varphi_u : E_0 \to E$ of degree u.

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

1. Find two ideals $I \sim I_1, I_2$ such that there exist $u, v > 0$ verifying $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^n$, for some $n \leq e$ and $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$.

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

1. Find two ideals $I \sim I_1, I_2$ such that there exist $u, v > 0$ verifying $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^n$, for some $n \leq e$ and $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$.
2. Let $I_1 = I\overline{\beta}_1 / \operatorname{nrd}(I)$ and $I_2 = I\overline{\beta}_2 / \operatorname{nrd}(I)$.

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

1. Find two ideals $I \sim I_1, I_2$ such that there exist $u, v > 0$ verifying $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^n$, for some $n \leq e$ and $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$.
2. Let $I_1 = I\overline{\beta}_1 / \operatorname{nrd}(I)$ and $I_2 = I\overline{\beta}_2 / \operatorname{nrd}(I)$.
3. Evaluate $\theta = \widehat{\varphi}_{I_2} \circ \varphi_{I_1} = \beta_2 \cdot \overline{\beta}_1 / \operatorname{nrd}(I)$ on $E_0[2^e]$.

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

1. Find two ideals $I \sim I_1, I_2$ such that there exist $u, v > 0$ verifying $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^n$, for some $n \leq e$ and $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$.
2. Let $I_1 = I\overline{\beta}_1 / \operatorname{nrd}(I)$ and $I_2 = I\overline{\beta}_2 / \operatorname{nrd}(I)$.
3. Evaluate $\theta = \widehat{\varphi}_{I_2} \circ \varphi_{I_1} = \beta_2 \cdot \overline{\beta}_1 / \operatorname{nrd}(I)$ on $E_0[2^e]$.
4. Compute $(\varphi_u : E_0 \to E_u) =$ `FixedDegreeIsogeny`(u), $(\varphi_v : E_0 \to E_v) =$ `FixedDegreeIsogeny`(v).

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

1. Find two ideals $I \sim I_1, I_2$ such that there exist $u, v > 0$ verifying $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^n$, for some $n \leq e$ and $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$.
2. Let $I_1 = I\overline{\beta}_1 / \operatorname{nrd}(I)$ and $I_2 = I\overline{\beta}_2 / \operatorname{nrd}(I)$.
3. Evaluate $\theta = \widehat{\varphi}_{I_2} \circ \varphi_{I_1} = \beta_2 \cdot \overline{\beta}_1 / \operatorname{nrd}(I)$ on $E_0[2^e]$.
4. Compute $(\varphi_u : E_0 \to E_u) =$ `FixedDegreeIsogeny`(u), $(\varphi_v : E_0 \to E_v) =$ `FixedDegreeIsogeny`(v).
5. Evaluate $\varphi_v \circ \theta \circ \widehat{\varphi}_u : E_u \to E_v$ on $E_u[2^e]$.

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

1. Find two ideals $I \sim I_1, I_2$ such that there exist $u, v > 0$ verifying $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^n$, for some $n \leq e$ and $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$.
2. Let $I_1 = I\overline{\beta}_1 / \operatorname{nrd}(I)$ and $I_2 = I\overline{\beta}_2 / \operatorname{nrd}(I)$.
3. Evaluate $\theta = \widehat{\varphi}_{I_2} \circ \varphi_{I_1} = \beta_2 \cdot \overline{\beta}_1 / \operatorname{nrd}(I)$ on $E_0[2^e]$.
4. Compute $(\varphi_u : E_0 \to E_u) =$ `FixedDegreeIsogeny`(u), $(\varphi_v : E_0 \to E_v) =$ `FixedDegreeIsogeny`(v).
5. Evaluate $\varphi_v \circ \theta \circ \widehat{\varphi}_u : E_u \to E_v$ on $E_u[2^e]$.
6. Extract the component $\varphi_{I_1} \circ \widehat{\varphi}_u$.

New Ideal to Isogeny (Inspired by [PR23])

`IdealToIsogeny`(I)

I A left $\mathcal{O}_0$-ideal I.

O The isogeny $\varphi_I : E_0 \to E$ corresponding to the ideal I.

1. Find two ideals $I \sim I_1, I_2$ such that there exist $u, v > 0$ verifying $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^n$, for some $n \leq e$ and $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$.
2. Let $I_1 = I\overline{\beta}_1 / \operatorname{nrd}(I)$ and $I_2 = I\overline{\beta}_2 / \operatorname{nrd}(I)$.
3. Evaluate $\theta = \widehat{\varphi}_{I_2} \circ \varphi_{I_1} = \beta_2 \cdot \overline{\beta}_1 / \operatorname{nrd}(I)$ on $E_0[2^e]$.
4. Compute $(\varphi_u : E_0 \to E_u) =$ `FixedDegreeIsogeny`(u), $(\varphi_v : E_0 \to E_v) =$ `FixedDegreeIsogeny`(v).
5. Evaluate $\varphi_v \circ \theta \circ \widehat{\varphi}_u : E_u \to E_v$ on $E_u[2^e]$.
6. Extract the component $\varphi_{I_1} \circ \widehat{\varphi}_u$.
7. From φ_{I_1}, recover φ_I.

Key Generation

E_0

Setup:

- $p = c \cdot 2^e - 1 \approx 2^{2\lambda}$;
- E_0 is the curve with j-invariant 1728, $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$.

Key Generation

$$E_0 \xrightarrow{\varphi_{\mathsf{sk}}} E_{\mathsf{pk}}$$

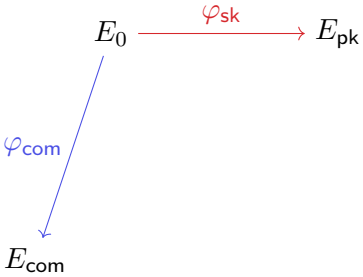
Setup:

- $p = c \cdot 2^e - 1 \approx 2^{2\lambda}$;
- E_0 is the curve with j-invariant 1728, $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$.

KeyGen:

- Sample a random left $\mathcal{O}_0$-ideal I_{sk} of large norm;
- $\varphi_{\mathsf{sk}} \leftarrow \texttt{IdealToIsogeny}(I_{\mathsf{sk}})$;
- $\mathsf{pk} \leftarrow E_{\mathsf{pk}}$;
- $\mathsf{sk} \leftarrow I_{\mathsf{sk}}$.

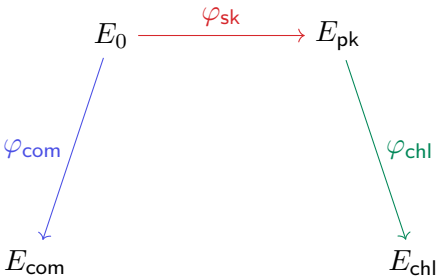
Commitment



Commitment:

- Sample a random left $\mathcal{O}_0$-ideal I_{com} of large norm;
- $\varphi_{\mathsf{com}} \leftarrow \texttt{IdealToIsogeny}(I_{\mathsf{com}})$;
- $\mathsf{com} \leftarrow E_{\mathsf{com}}$.

Challenge



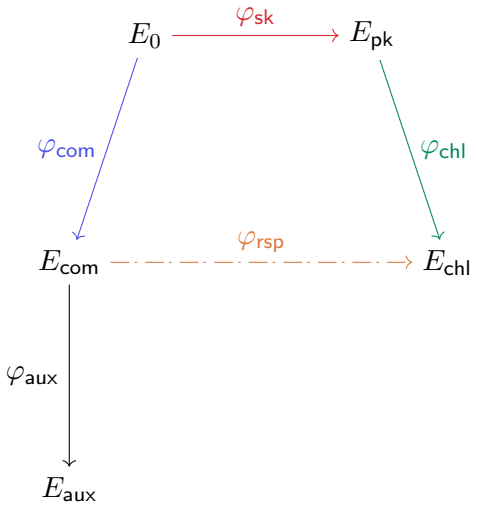
Constants:

$e \approx 2\lambda$, $e_{\mathsf{chl}} \approx \lambda$.

Challenge:

- Compute a deterministic basis $\langle P_{\mathsf{pk}}, Q_{\mathsf{pk}} \rangle = E_{\mathsf{pk}}[2^e]$;
- $\mathsf{chl} \leftarrow_{\$} \{0, 2^{e_{\mathsf{chl}}}\}$;
- $\varphi_{\mathsf{chl}} \colon E_{\mathsf{pk}} \to E_{\mathsf{chl}}$, where $\ker(\varphi_{\mathsf{chl}}) = \langle P_{\mathsf{pk}} + [\mathsf{chl}]Q_{\mathsf{pk}} \rangle$.

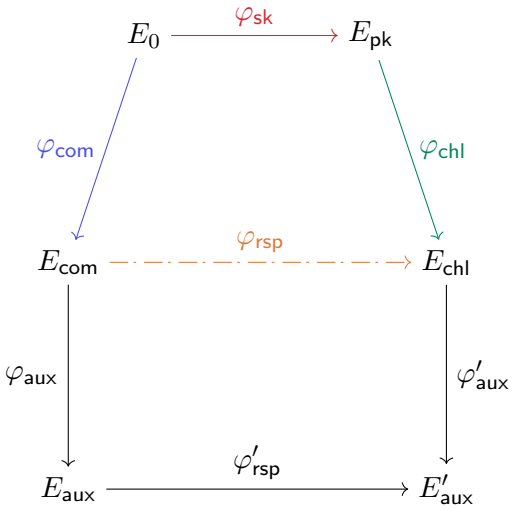
Response



Constants:
$2^{e_{\mathsf{rsp}}} \geq 2\sqrt{2p}/\pi$.
Response:

- Compute I_{chl} associated with φ_{chl};
- $J \leftarrow \overline{I}_{\mathsf{com}} \cdot I_{\mathsf{sk}} \cdot I_{\mathsf{chl}}$;
- Compute a random $I_{\mathsf{rsp}} \sim J$ of norm $q < 2^{e_{\mathsf{rsp}}}$;
- Technical condition: q can be even, but suppose q is odd.
- Using `IdealToIsogeny`, compute $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \to E_{\mathsf{chl}}$ and an isogeny $\varphi_{\mathsf{aux}} : E_{\mathsf{com}} \to E_{\mathsf{aux}}$ of degree $2^{e_{\mathsf{rsp}}} - q$.
- $\mathsf{rsp} \leftarrow (\varphi_{\mathsf{rsp}}|_{E_{\mathsf{com}}[2^{e_{\mathsf{rsp}}}]}, \varphi_{\mathsf{aux}}|_{E_{\mathsf{com}}[2^{e_{\mathsf{rsp}}}]})$

Verification



Verification:

- Compute the challenge isogeny $\varphi_{\mathsf{chl}} \colon E_{\mathsf{pk}} \to E_{\mathsf{chl}}$;
- Using $\varphi_{\mathsf{rsp}}|_{E_{\mathsf{com}}[2^{e_{\mathsf{rsp}}}]}$, $\varphi_{\mathsf{aux}}|_{E_{\mathsf{com}}[2^{e_{\mathsf{rsp}}}]}$, attempt to compute

$$\begin{pmatrix} \widehat{\varphi}_{\mathsf{aux}} & -\widehat{\varphi}_{\mathsf{rsp}} \\ \varphi'_{\mathsf{rsp}} & \varphi'_{\mathsf{aux}} \end{pmatrix} : E_{\mathsf{aux}} \times E_{\mathsf{chl}} \to E_{\mathsf{com}} \times E'_{\mathsf{aux}}.$$

Performance

Table 1: Performance on Intel Xeon Gold 6338 (Ice Lake, 2GHz), with finite field arithmetic optimised using intrinsics for the Ice Lake architecture, GMP 6.2.1. Turbo-boost disabled. Timings in 10^6 cycles.

	Level	**SQIsign** (NIST)	**SQIsign** (EC 2023)	**SQIsign2D**
Keygen	I	1,700	400	60
	III	—	—	170
	V	—	—	360
Sign	I	2,400	1880	160
	III	—	—	460
	V	—	—	940
Verify	I	39	29	9
	III	—	—	29
	V	—	—	62

Thanks for your attention!

Questions?