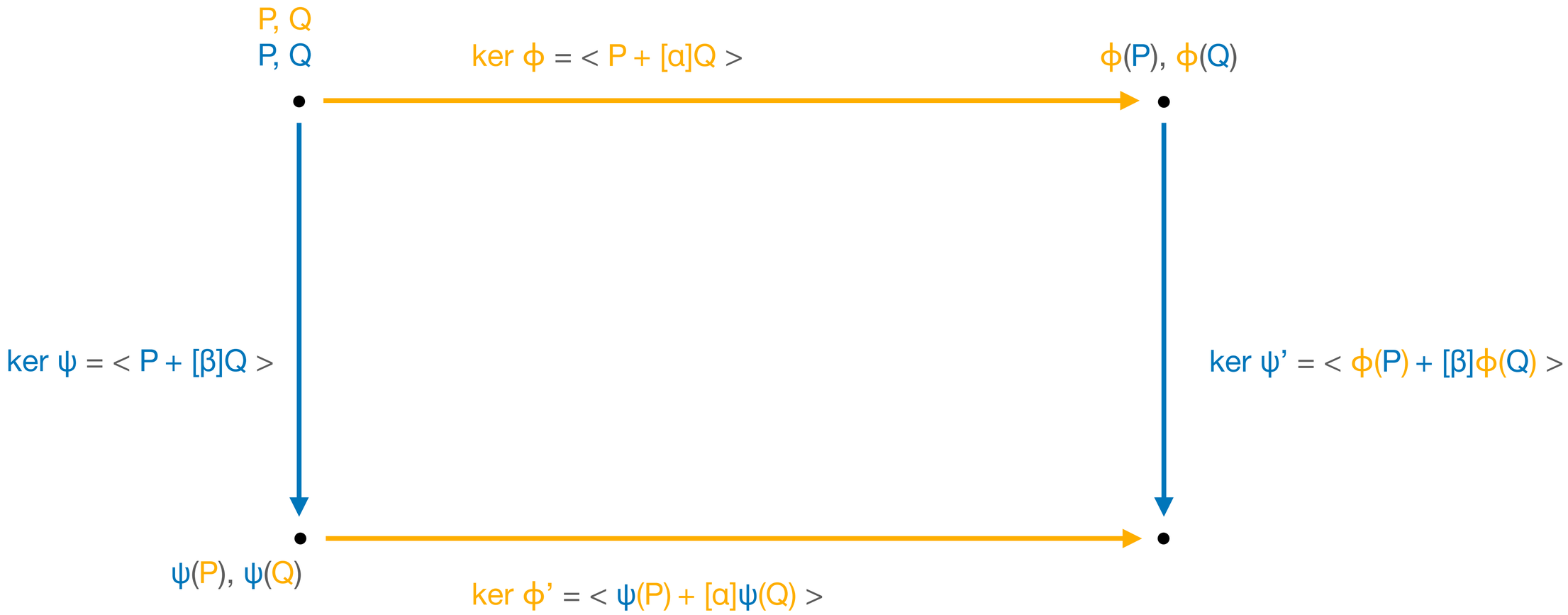
New SIDH Countermeasures for a More Efficient Key Exchange

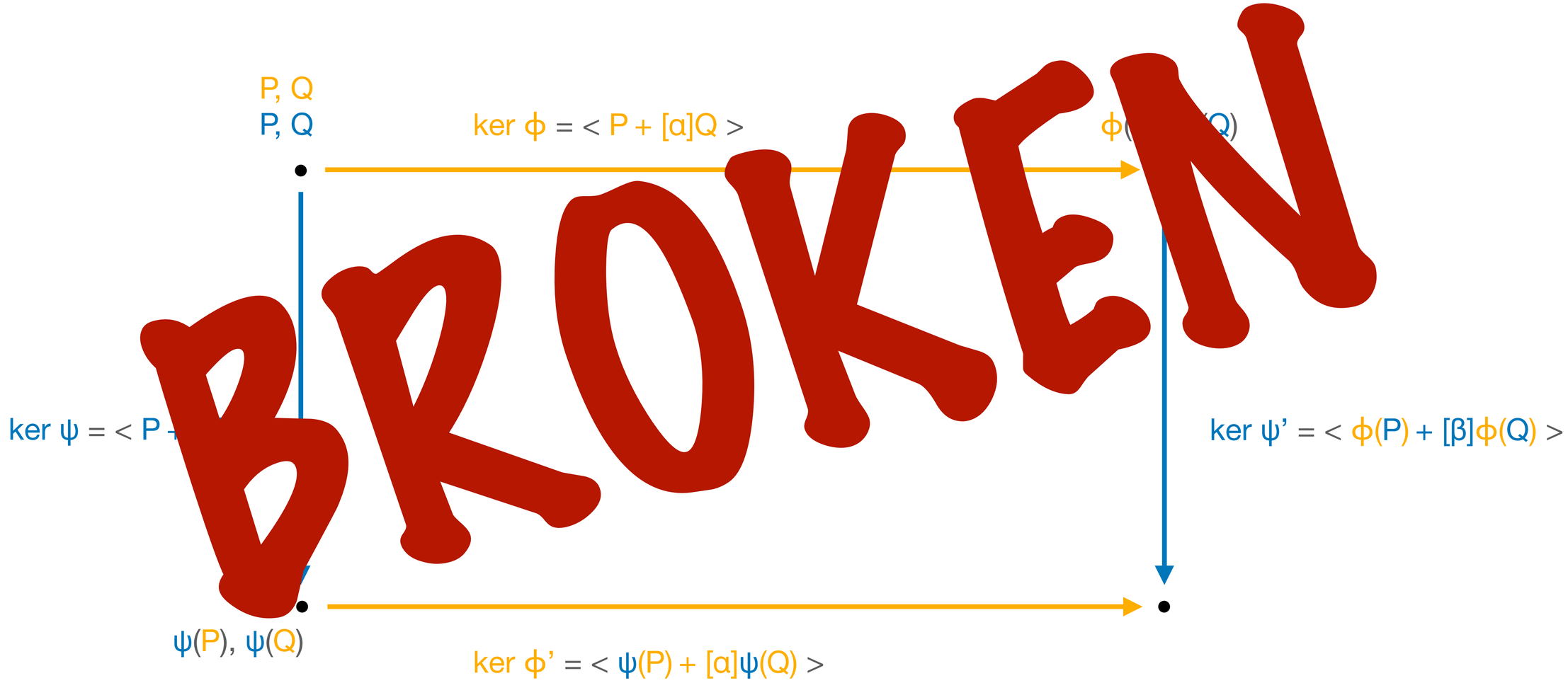
Andrea Basso, Tako Boris Fouotsa

ASIACRYPT 2023 — December 5th, 2023

Previously, in isogeny land...

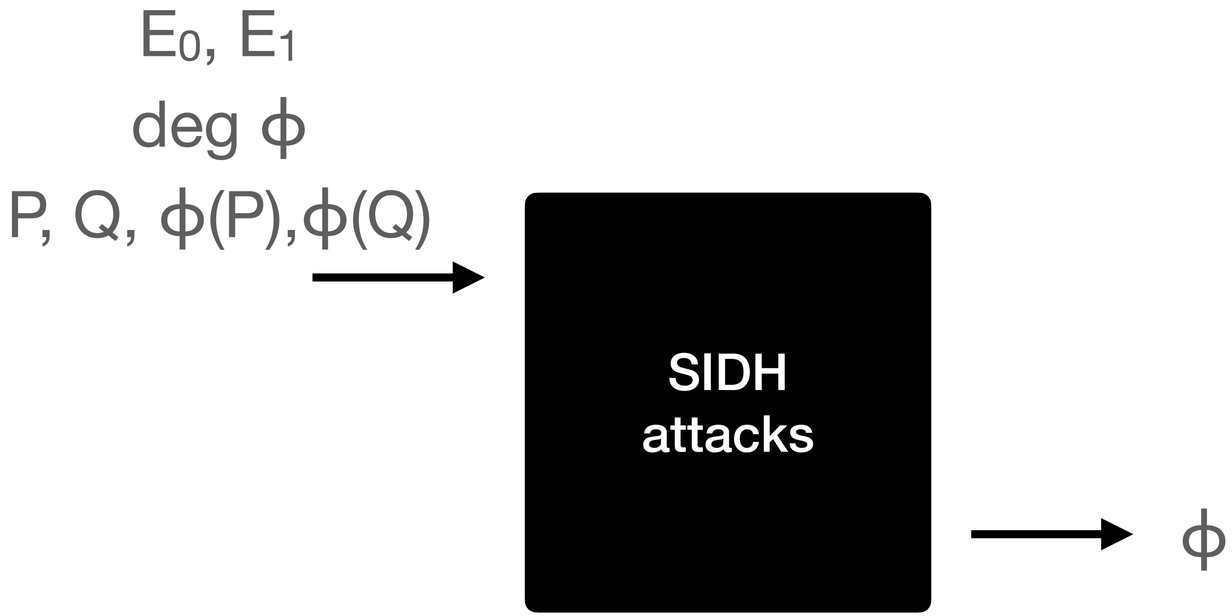


Previously, in isogeny land...

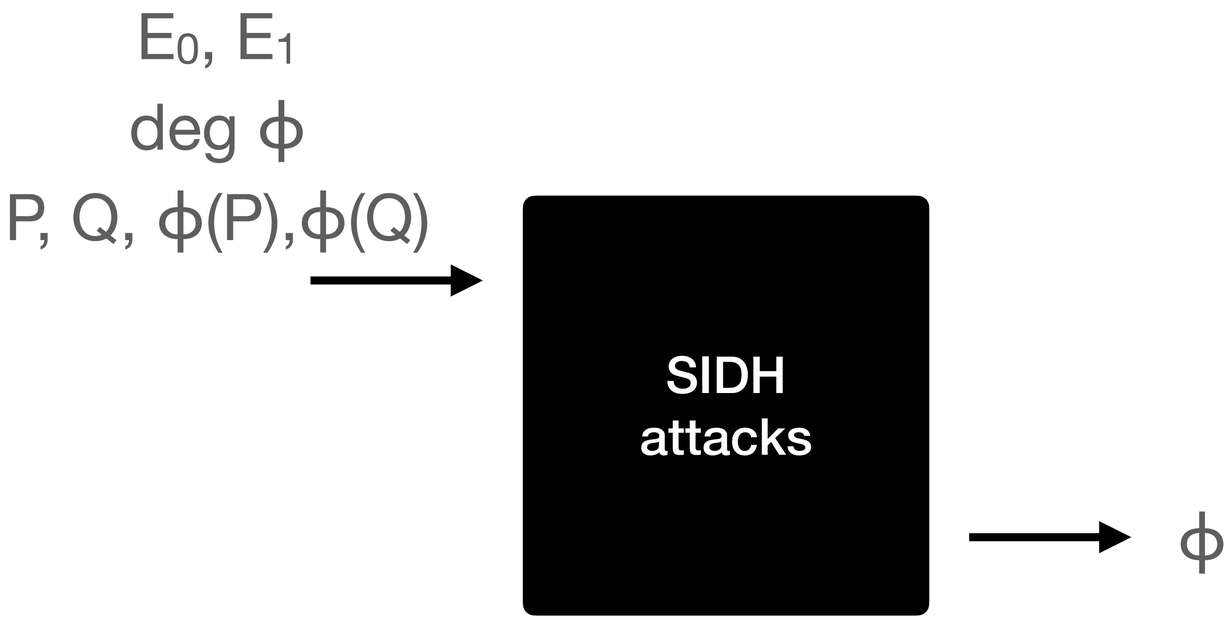


The attacks on SIDH

The attacks on SIDH



The attacks on SIDH



Countermeasures

- Masked degree
- Masked torsion

The attacks on SIDH

E_0, E_1
deg ϕ
P, Q, $\phi(P)$,$\phi(Q)$

Countermeasures

- Masked degree
- Masked torsion

$\phi(P),\phi(Q) \longrightarrow [\alpha]\phi(P), [\alpha]\phi(Q)$

The attacks on SIDH

E_0, E_1
deg ϕ
P, Q, $\phi(P)$,$\phi(Q)$

Countermeasures

- Masked degree
- Masked torsion

$\phi(P),\phi(Q) \longrightarrow [\alpha]\phi(P), [\alpha]\phi(Q)$

$\Downarrow$

leaks α^2

The attacks on SIDH

E_0, E_1
deg ϕ
P, Q, $\phi(P)$,$\phi(Q)$

Countermeasures

- Masked degree
- Masked torsion

$\phi(P),\phi(Q) \longrightarrow [\alpha]\phi(P), [\alpha]\phi(Q)$

$\Downarrow$

leaks α^2

$\Downarrow$

very large params ($p \approx 2^{6000} - 2^{14,000}$)

A new approach

A new approach

A new approach

A new approach

A new approach

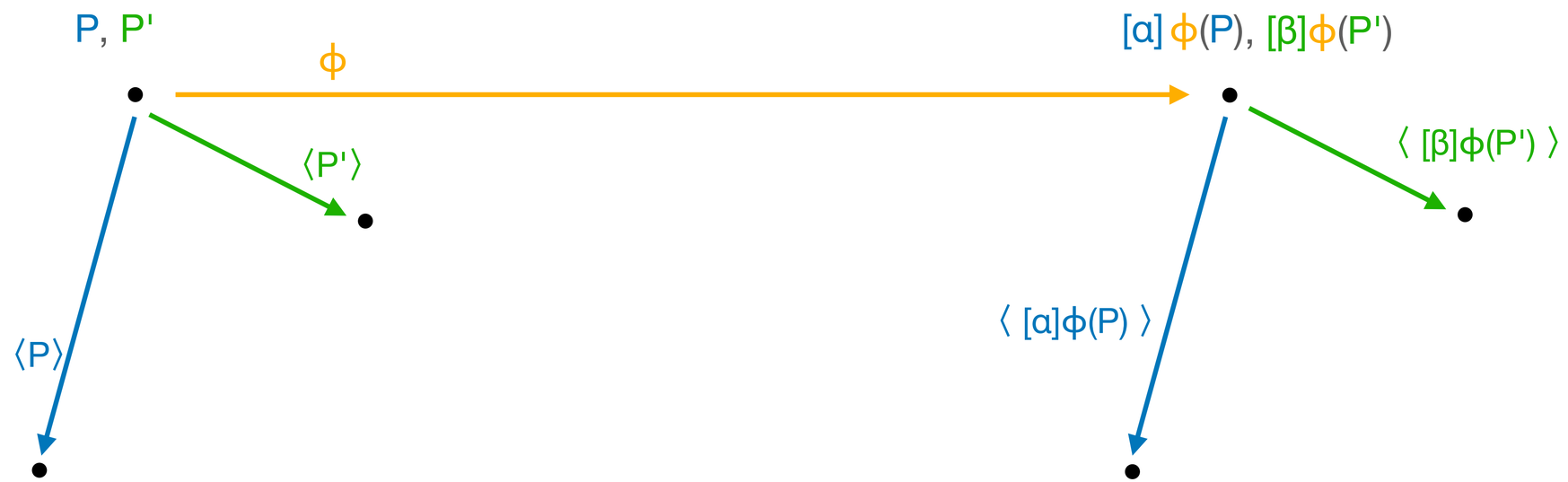
A new approach

A new approach

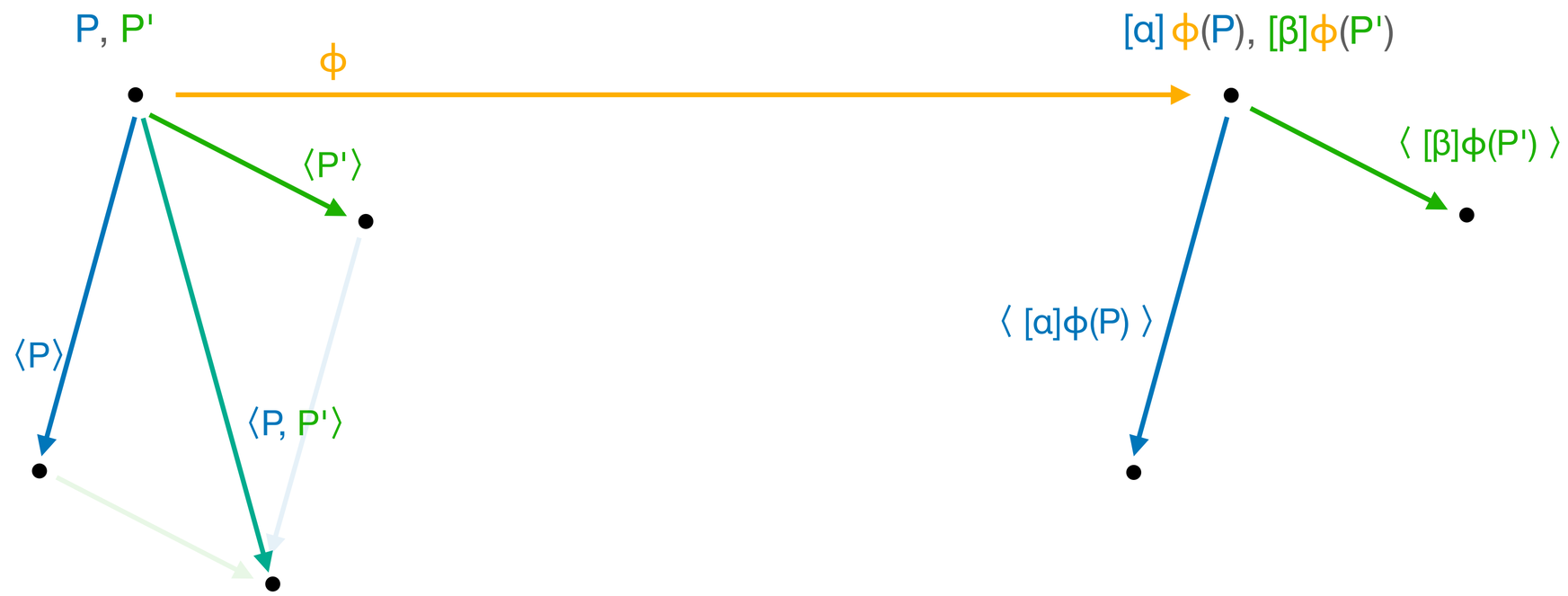
A new approach

A new approach

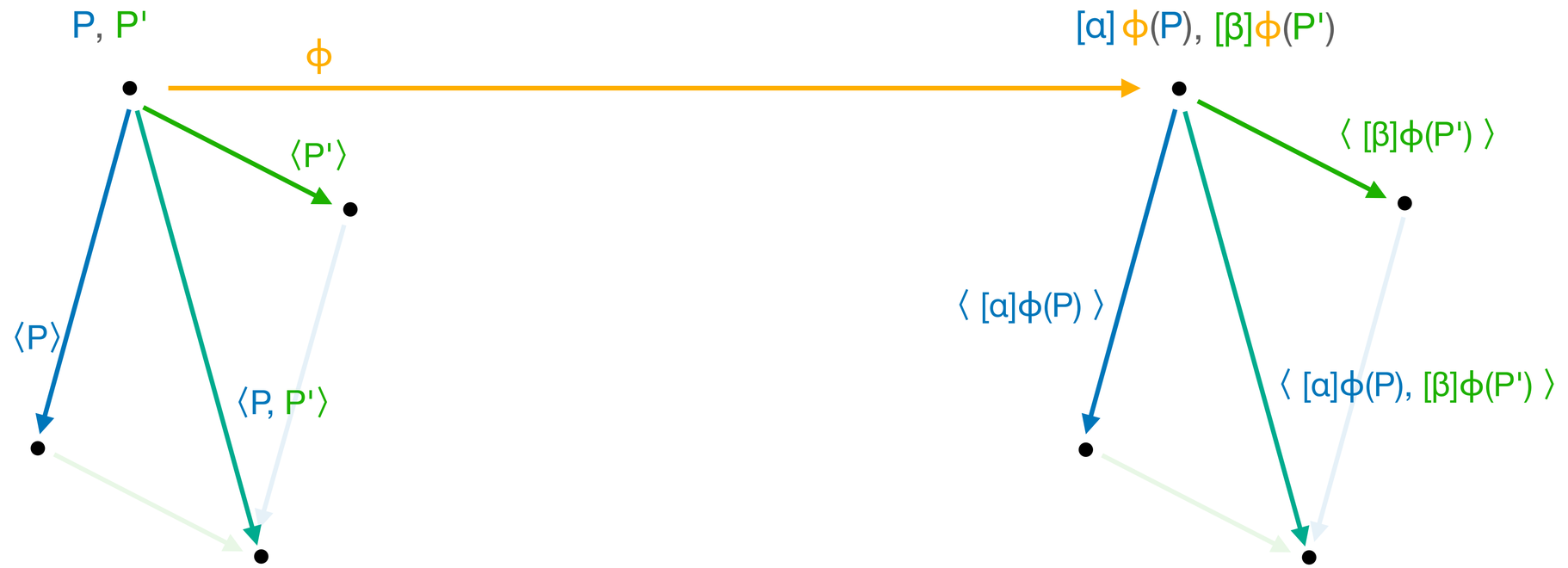
A new approach



A new approach



A new approach

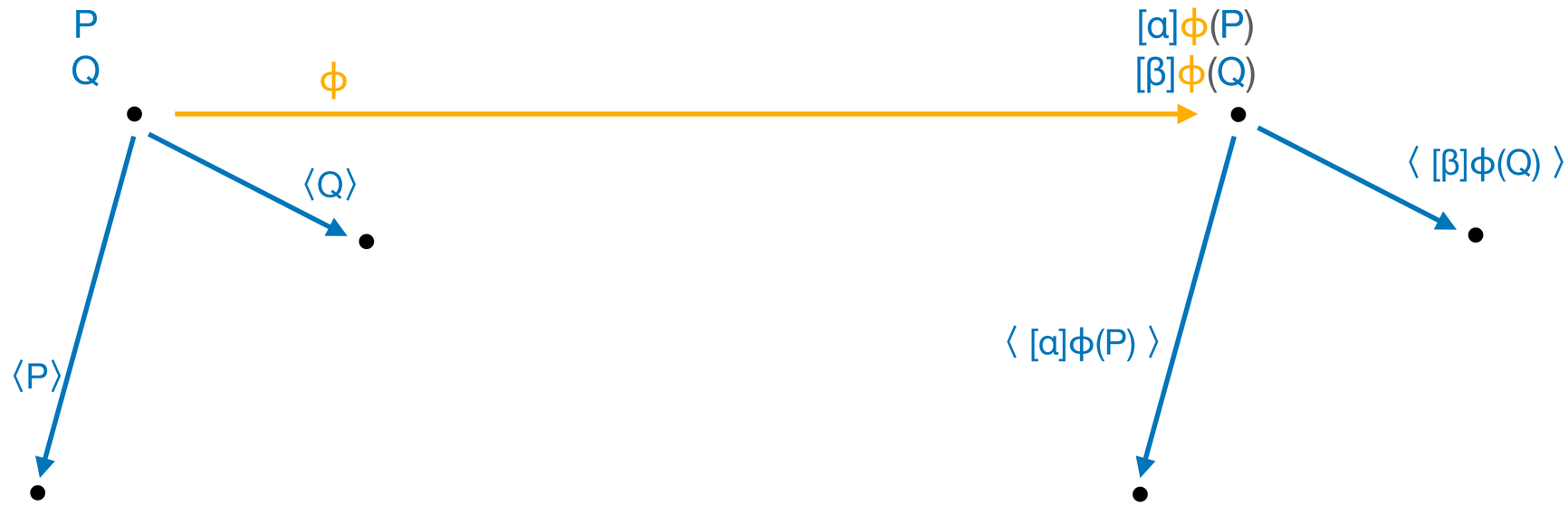


But, we can do better!

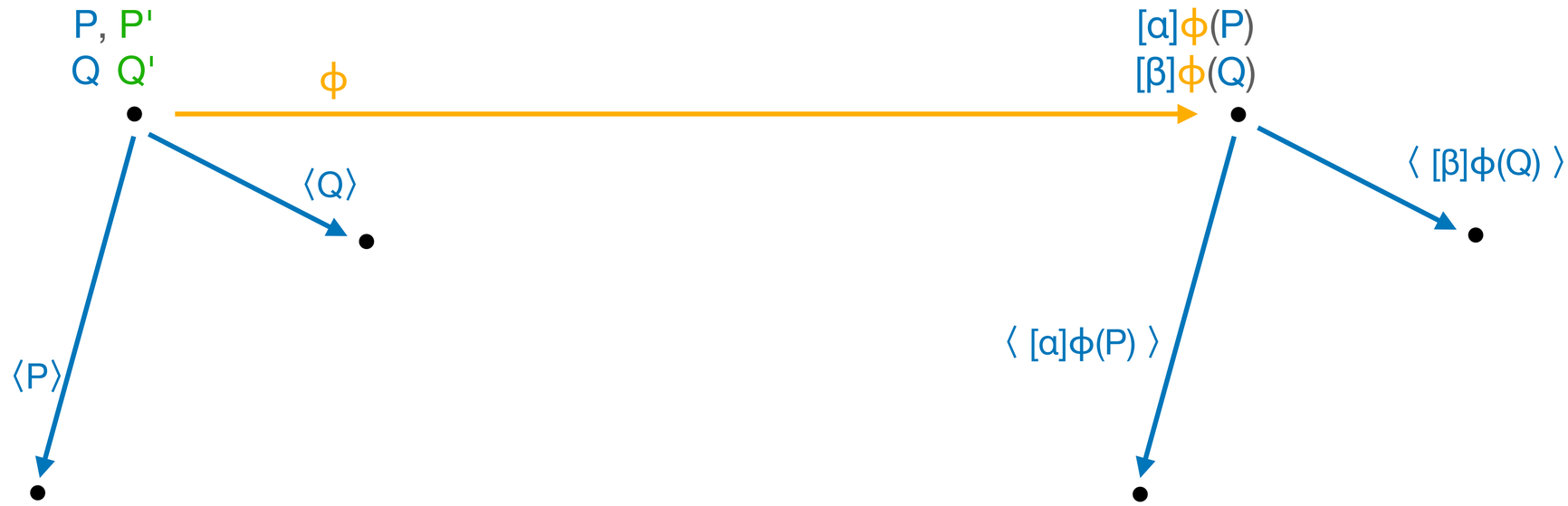
But, we can do better!

But, we can do better!

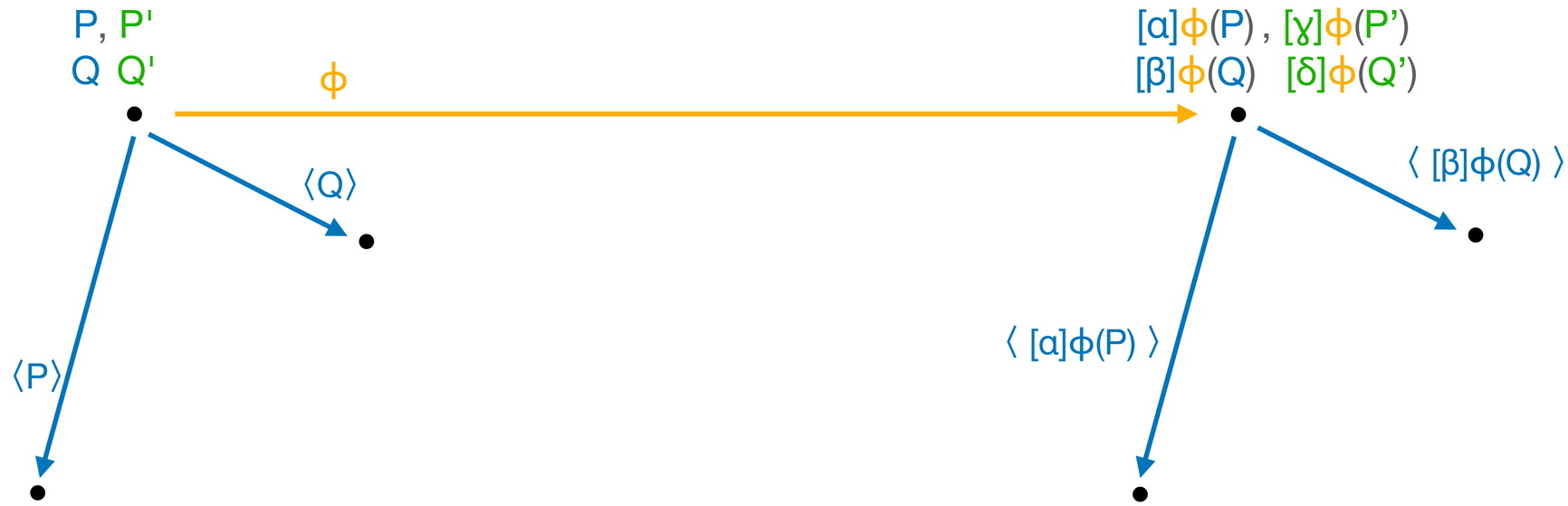
But, we can do better!



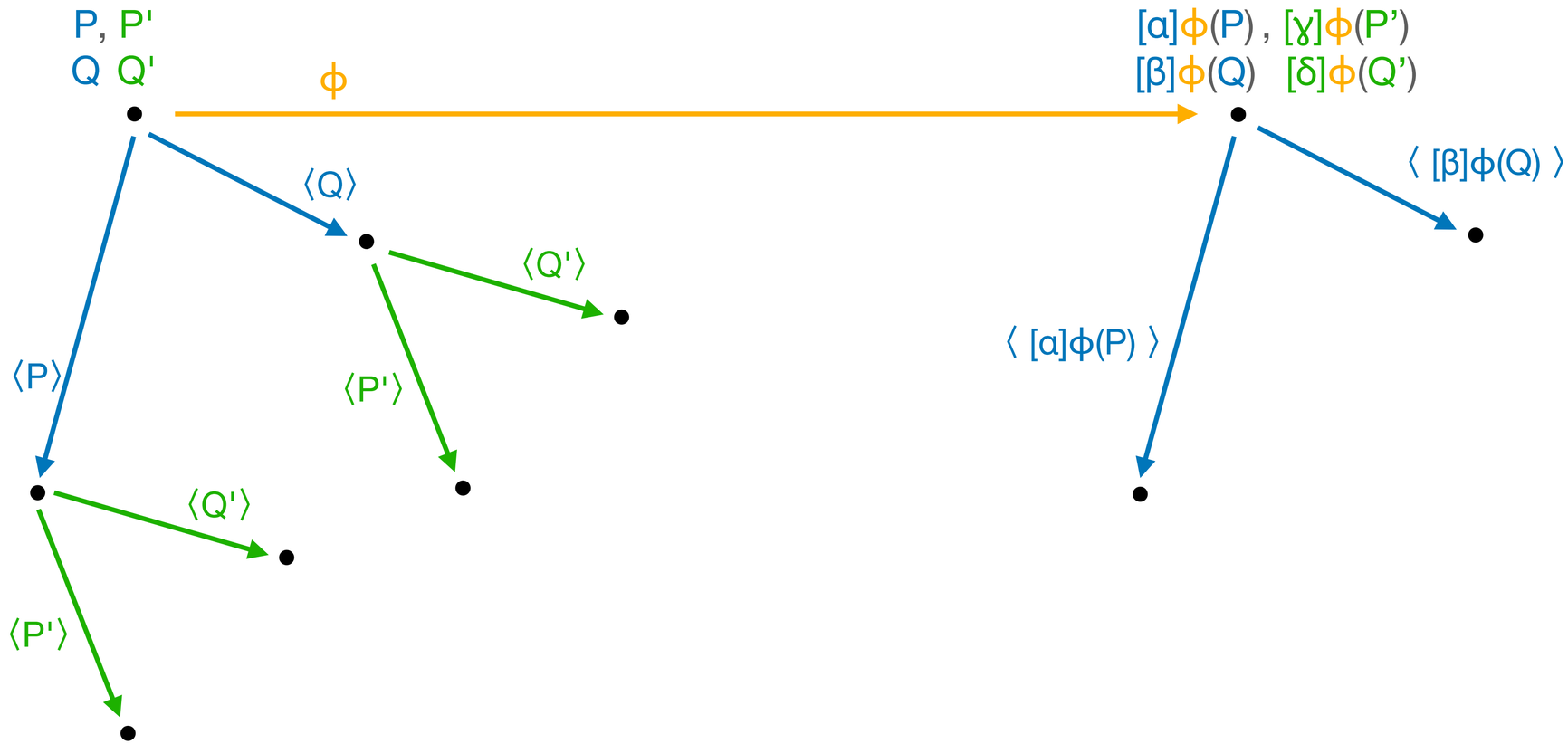
But, we can do better!



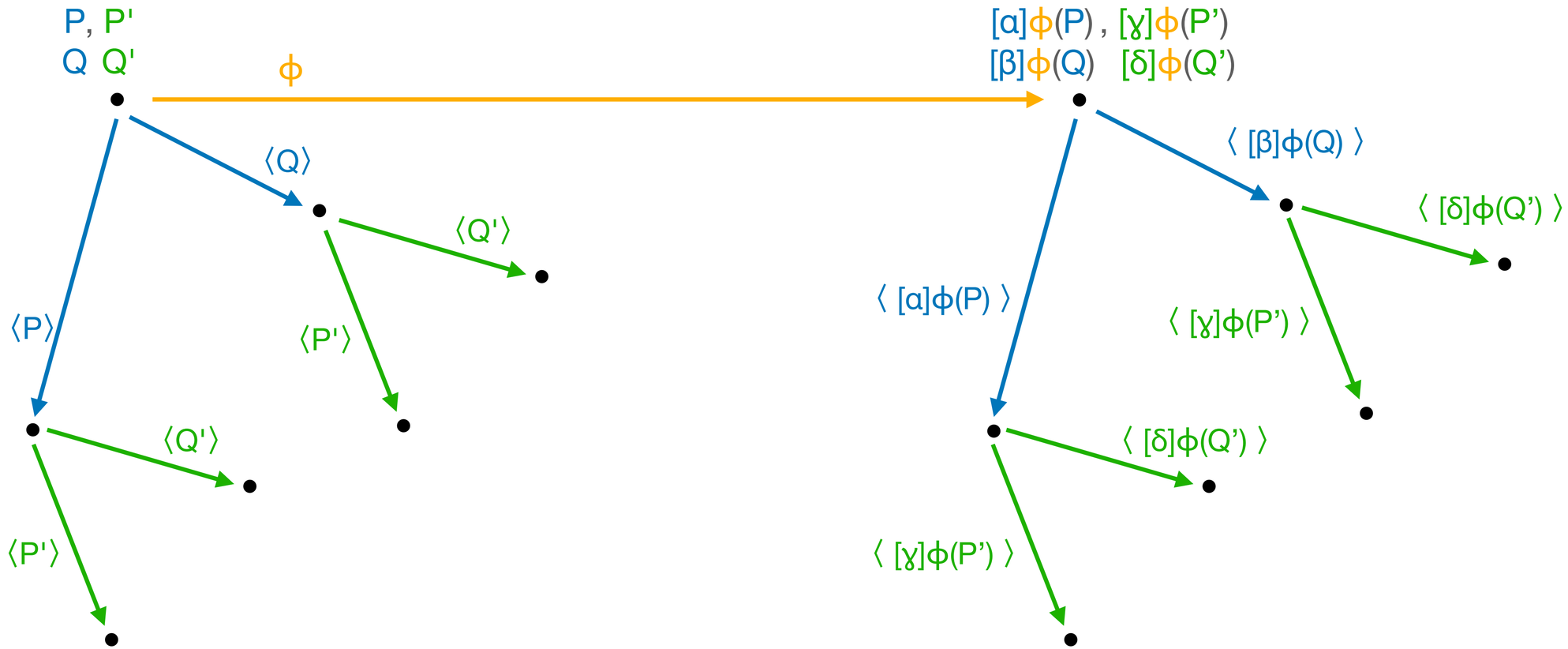
But, we can do better!



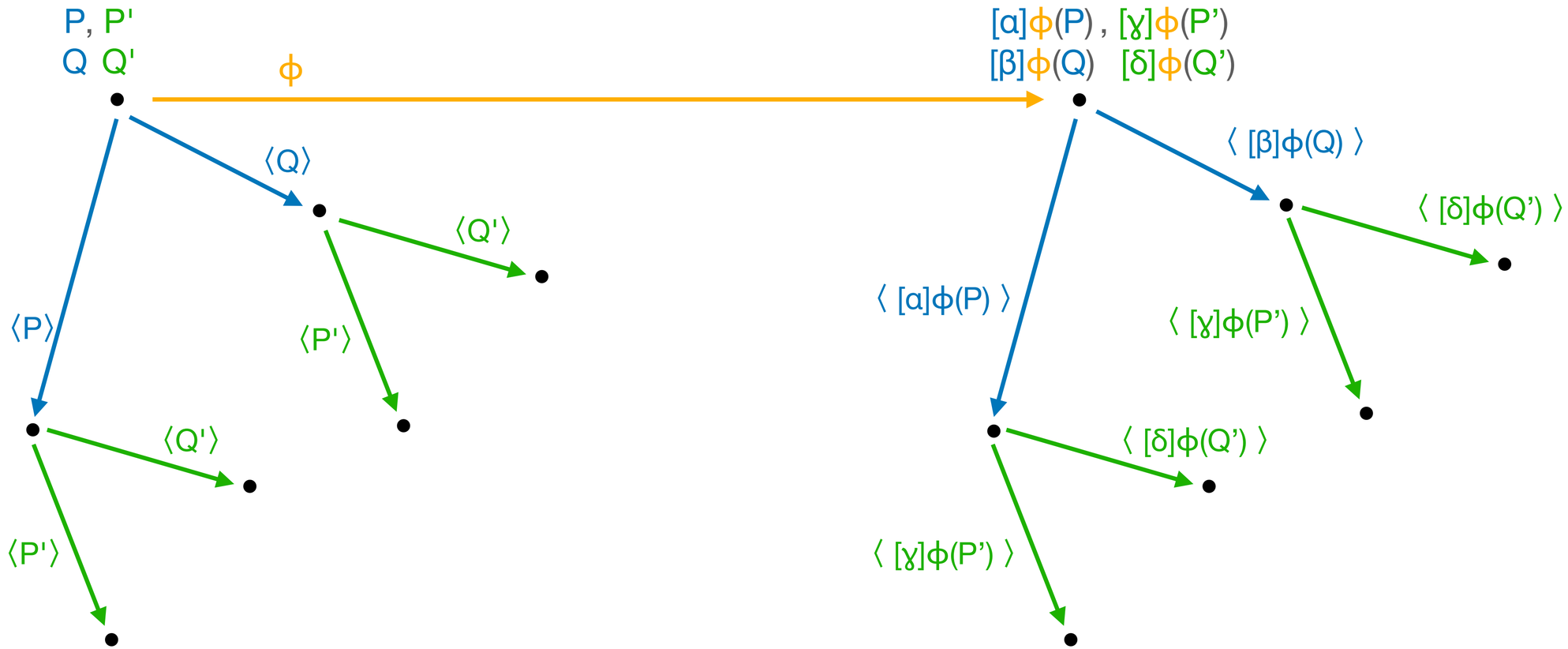
But, we can do better!



But, we can do better!

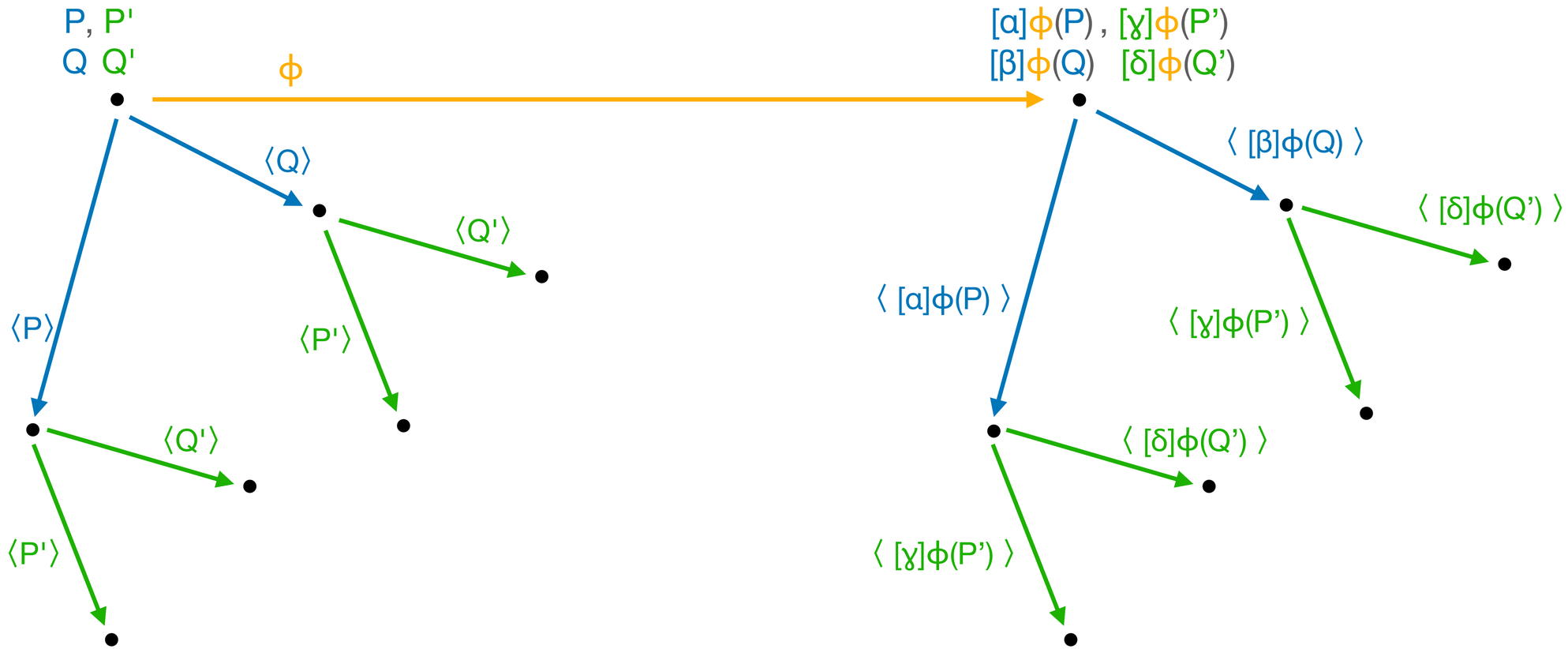


But, we can do better!



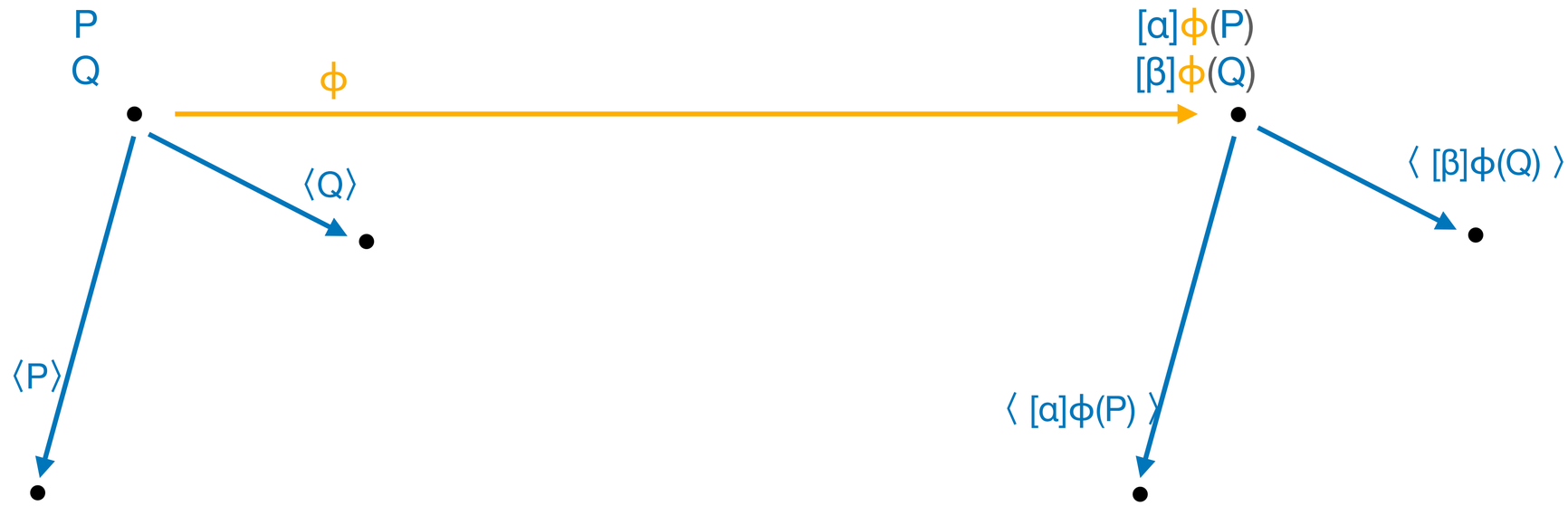
$e([\alpha]P, [\beta]Q) = e(P, Q)^{\alpha\beta}$

But, we can do better!

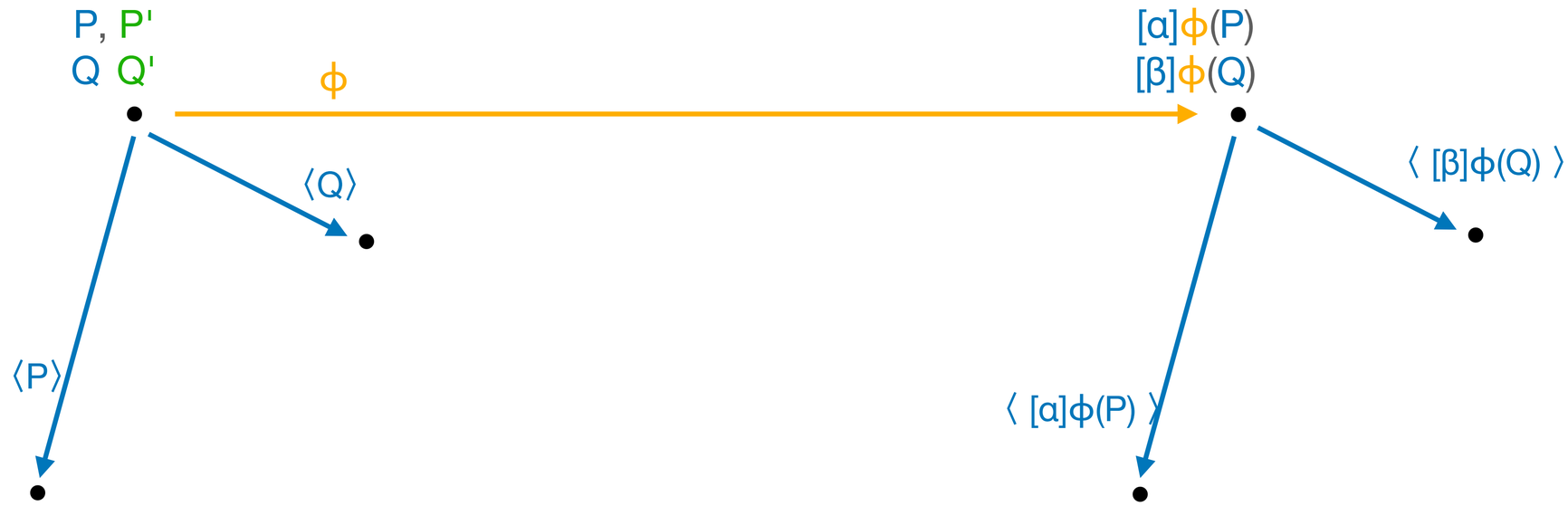


$e([\alpha]P, [\beta]Q) = e(P, Q)^{\alpha\beta}$ ⇒ $p \approx 2^{2400}$

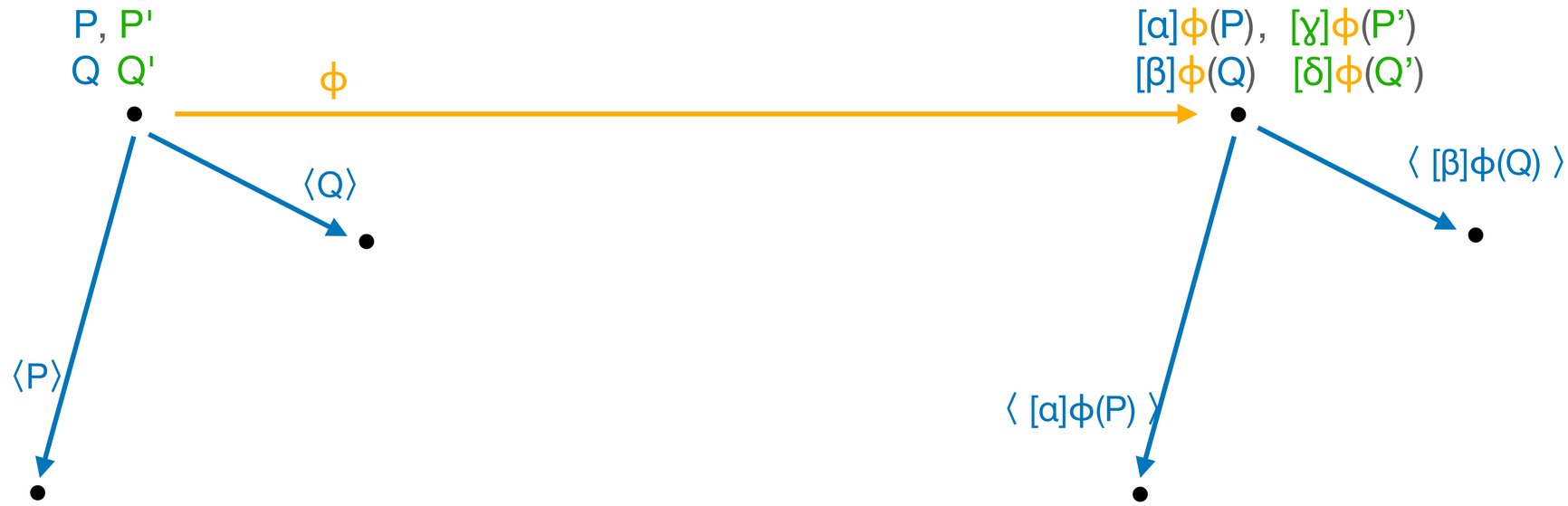
Even better?



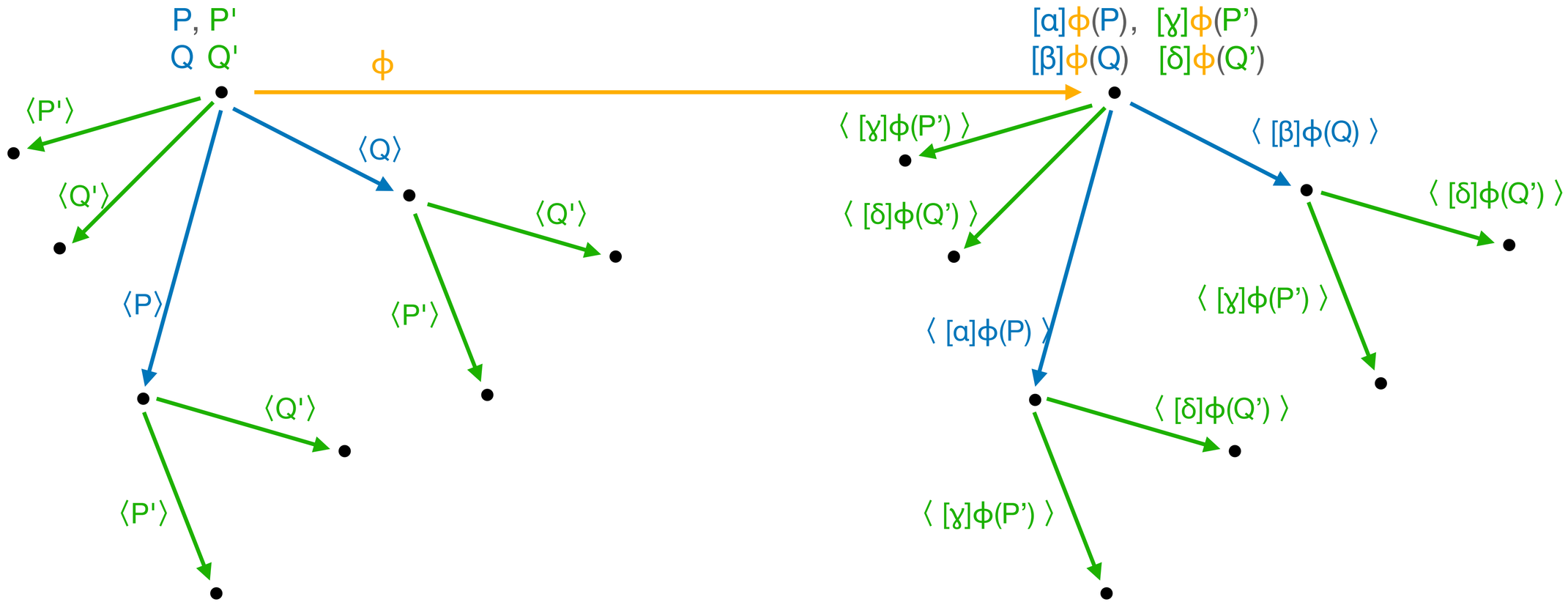
Even better?



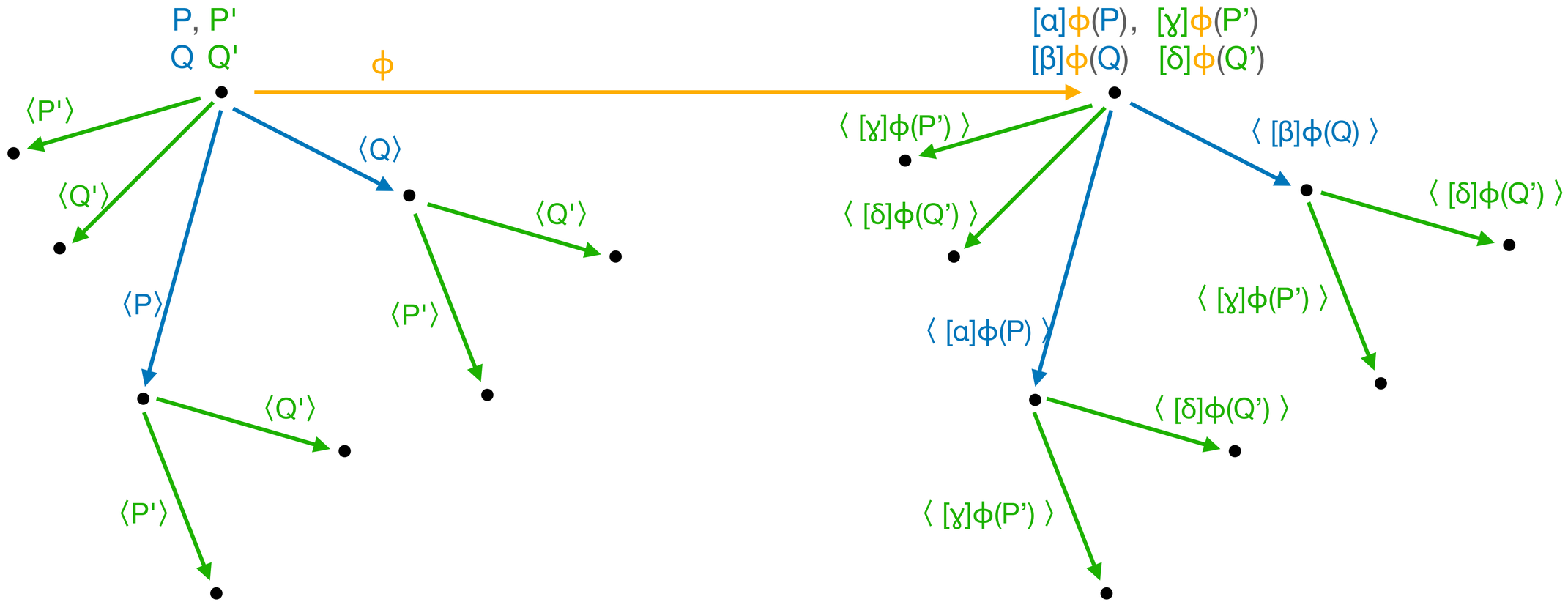
Even better?



Even better?



Even better?



$\Rightarrow \quad p \approx 2^{1500}$

New key exchanges: binSIDH and terSIDH

New key exchanges: binSIDH and terSIDH

-

New key exchanges: binSIDH and terSIDH

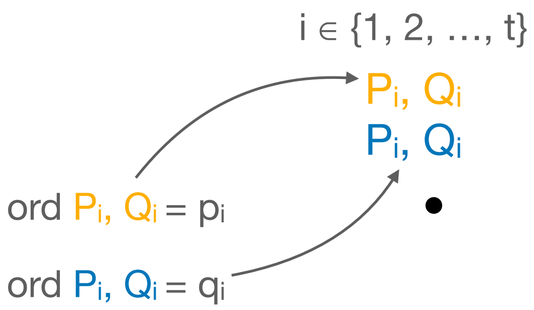
$i \in \{1, 2, \ldots, t\}$

P_i, Q_i

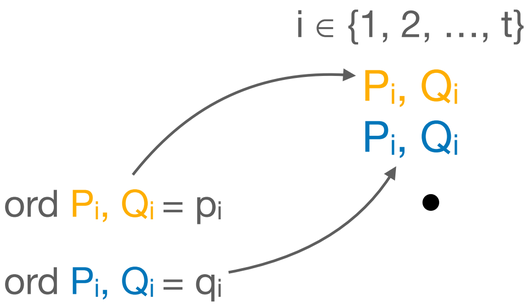
P_i, Q_i

•

New key exchanges: binSIDH and terSIDH

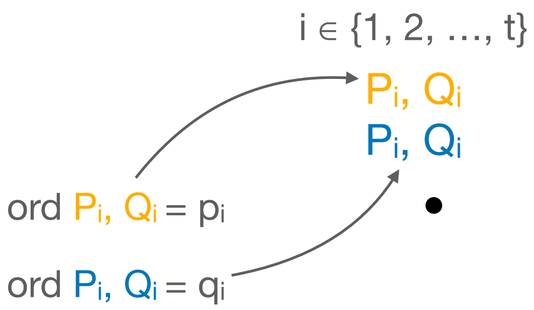


New key exchanges: binSIDH and terSIDH



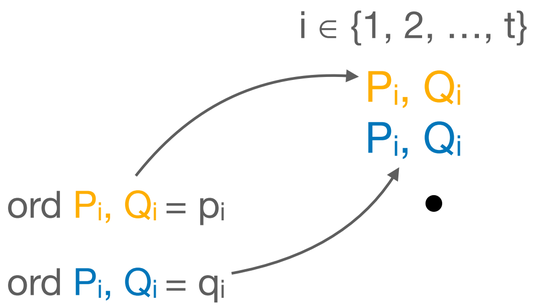
$$\ker \phi = \left\langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \dots, \frac{P_t}{Q_t} \right\rangle$$

New key exchanges: binSIDH and terSIDH



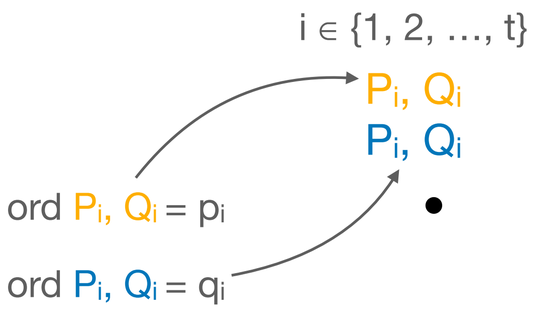
$$\ker \phi = \left\langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \dots, \frac{P_t}{Q_t} \right\rangle$$

New key exchanges: binSIDH and terSIDH



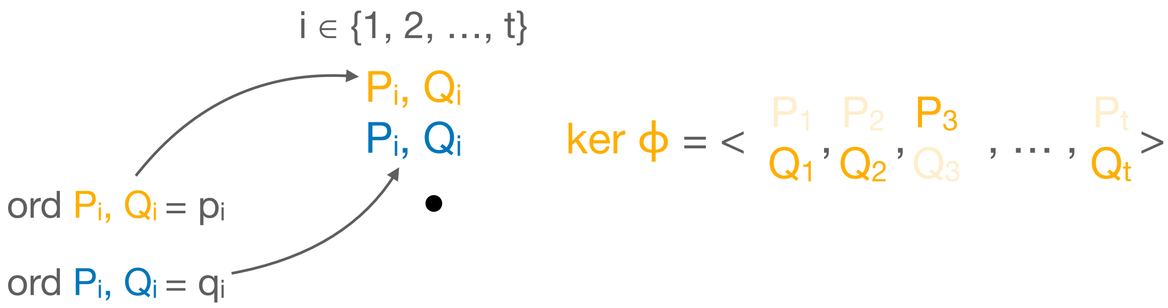
$$\ker \phi = \left\langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \dots, \frac{P_t}{Q_t} \right\rangle$$

New key exchanges: binSIDH and terSIDH



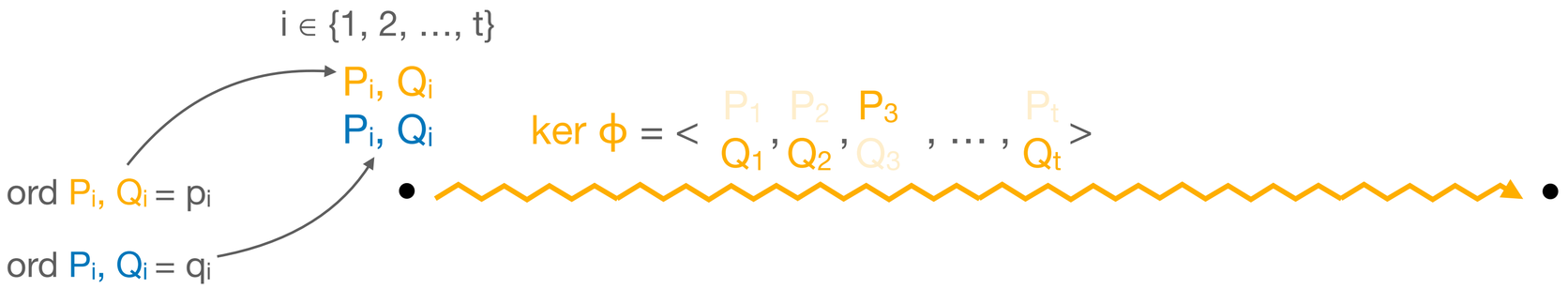
$$\ker \phi = \left\langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \dots, \frac{P_t}{Q_t} \right\rangle$$

New key exchanges: binSIDH and terSIDH

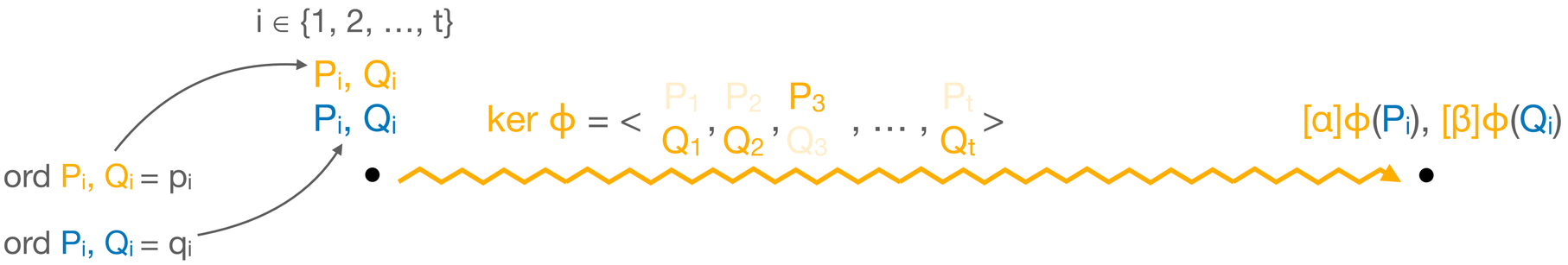


$$\ker \phi = \left\langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots, \frac{P_t}{Q_t} \right\rangle$$

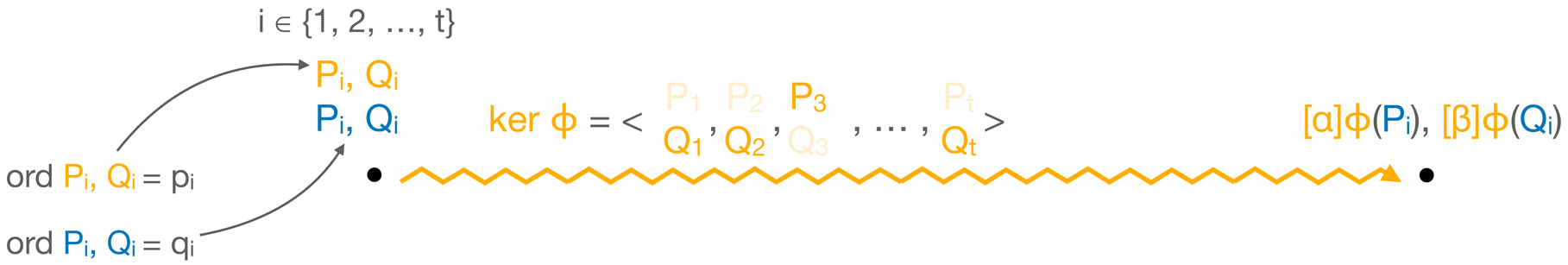
New key exchanges: binSIDH and terSIDH



New key exchanges: binSIDH and terSIDH

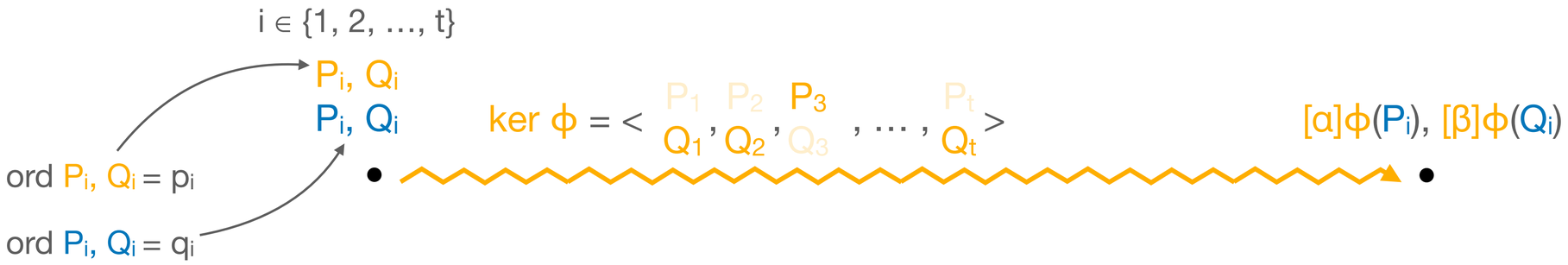


New key exchanges: binSIDH and terSIDH



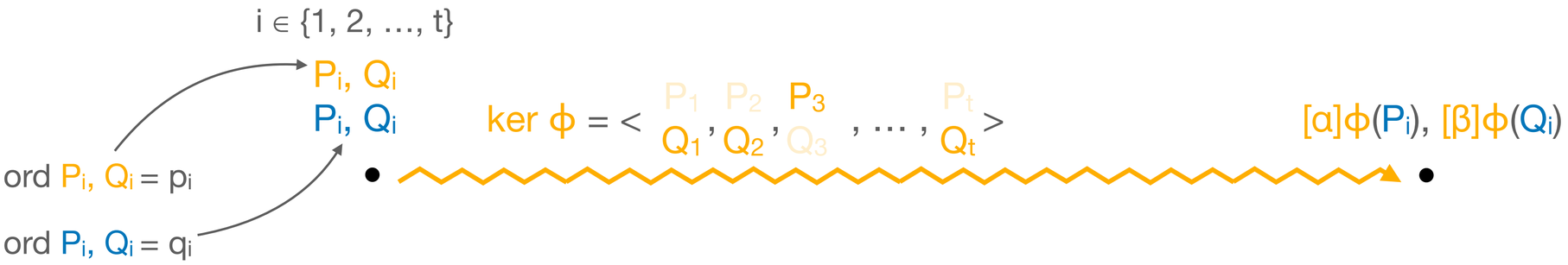
$$\ker \psi = \langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots, \frac{P_t}{Q_t} \rangle$$

New key exchanges: binSIDH and terSIDH



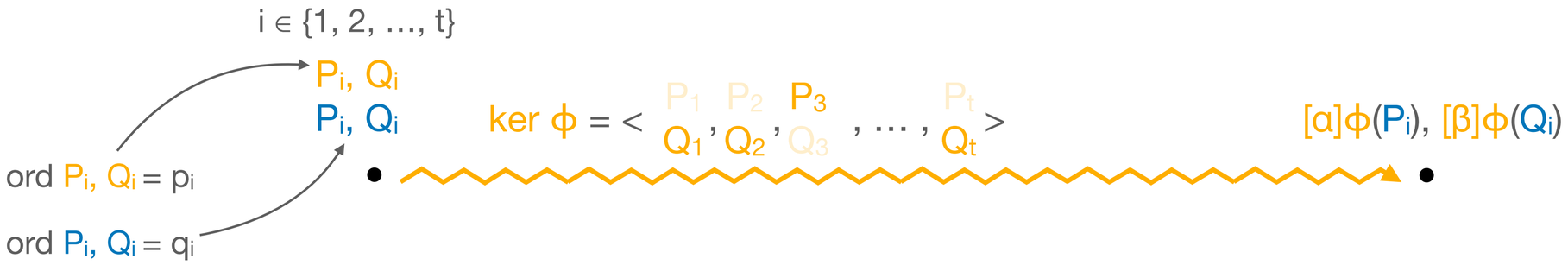
$$\ker \psi = \left\langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \dots, \frac{P_t}{Q_t} \right\rangle$$

New key exchanges: binSIDH and terSIDH



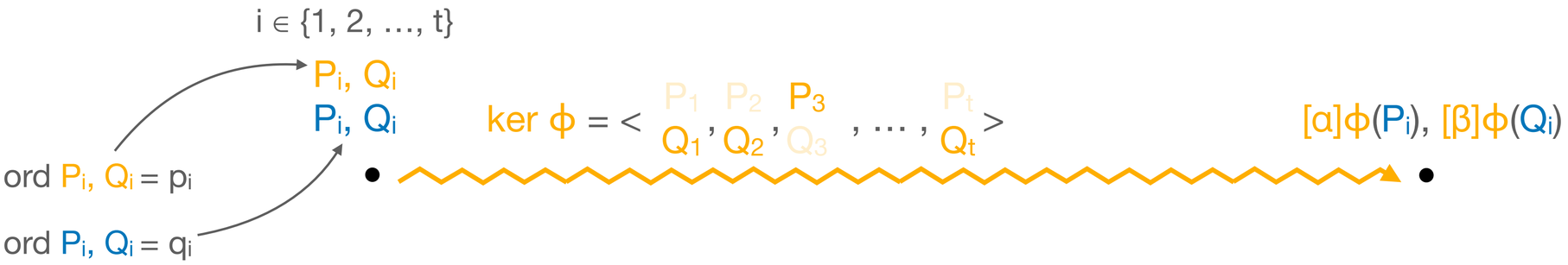
$$\ker \psi = \langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots, \frac{P_t}{Q_t} \rangle$$

New key exchanges: binSIDH and terSIDH



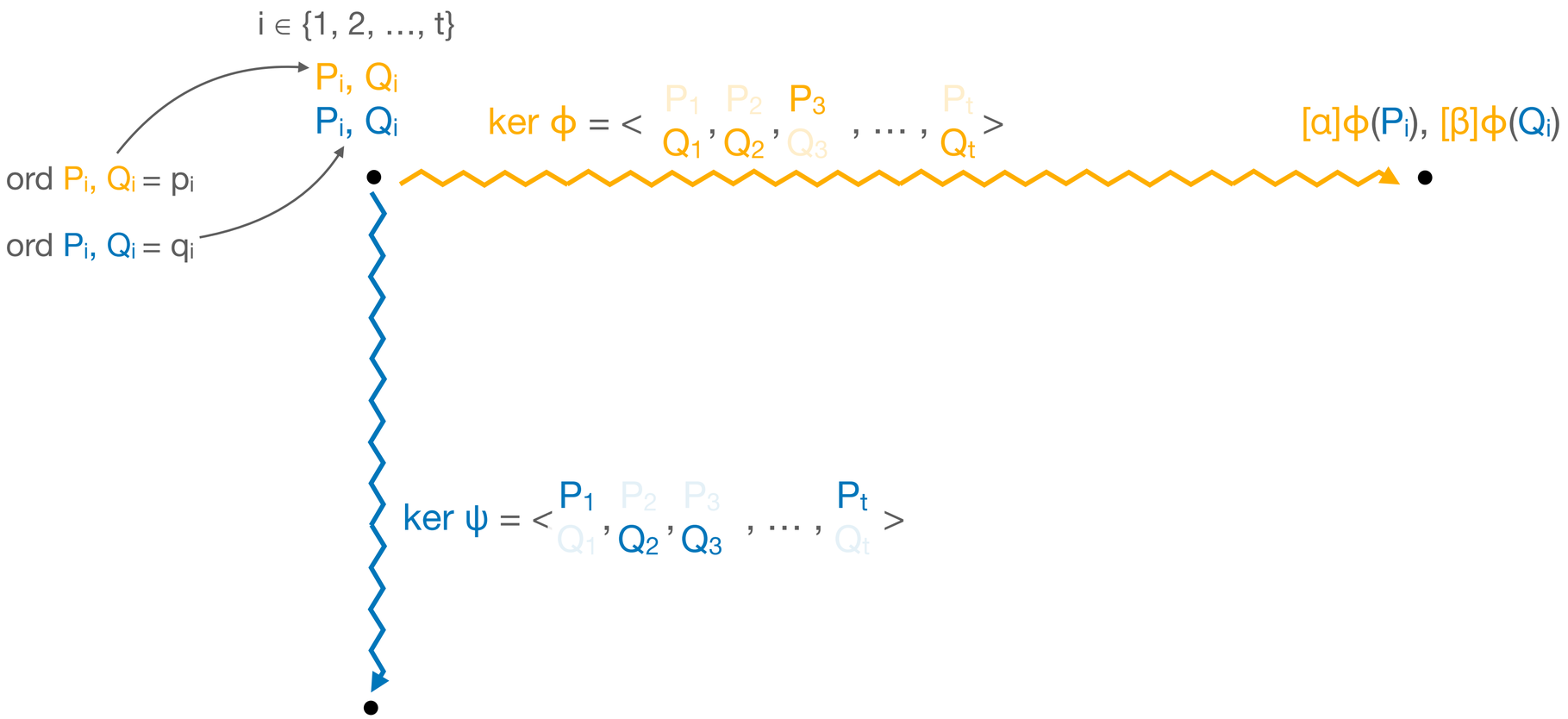
$$\ker \psi = \langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots, \frac{P_t}{Q_t} \rangle$$

New key exchanges: binSIDH and terSIDH

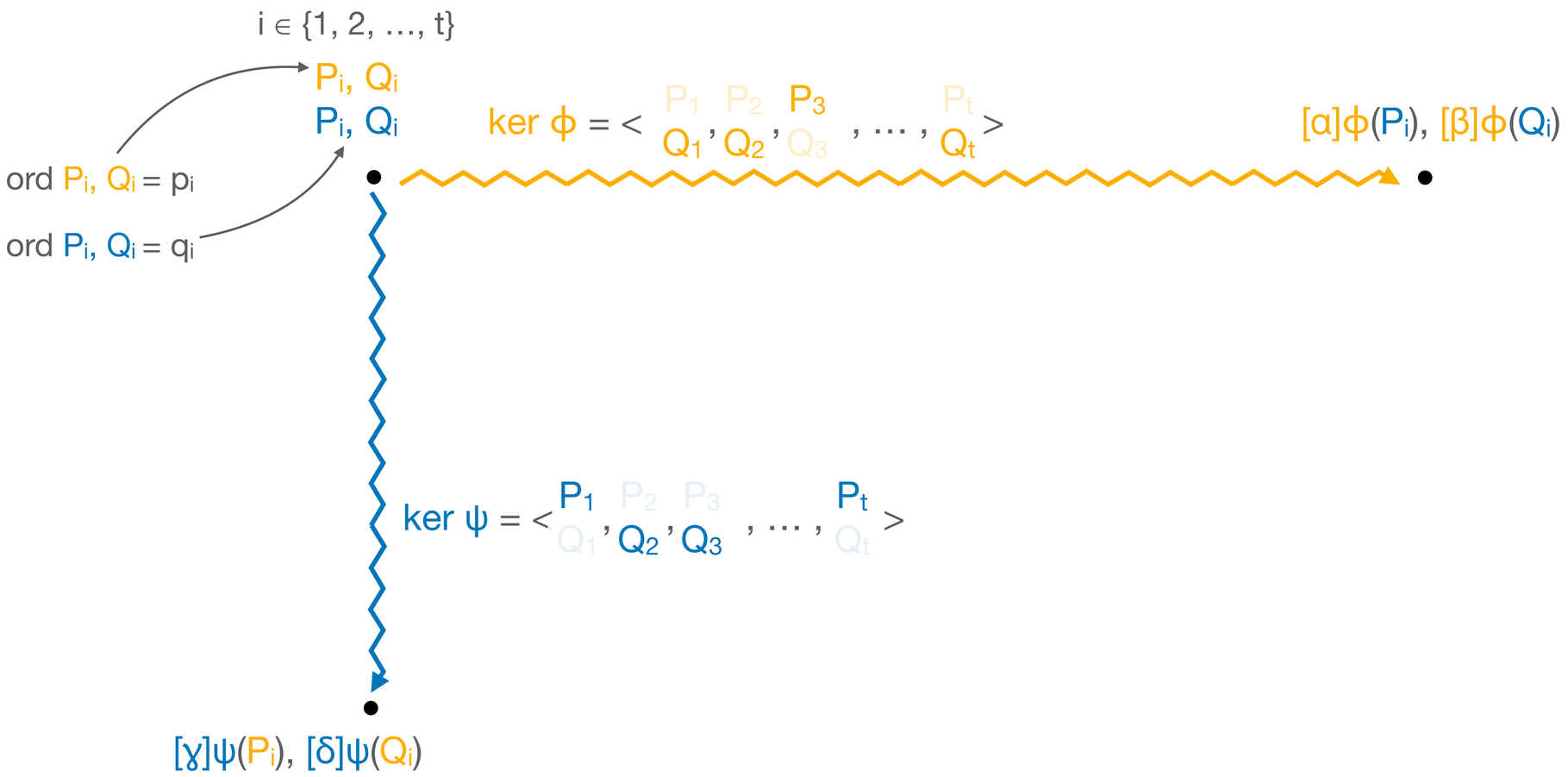


$$\ker \psi = \langle \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots, \frac{P_t}{Q_t} \rangle$$

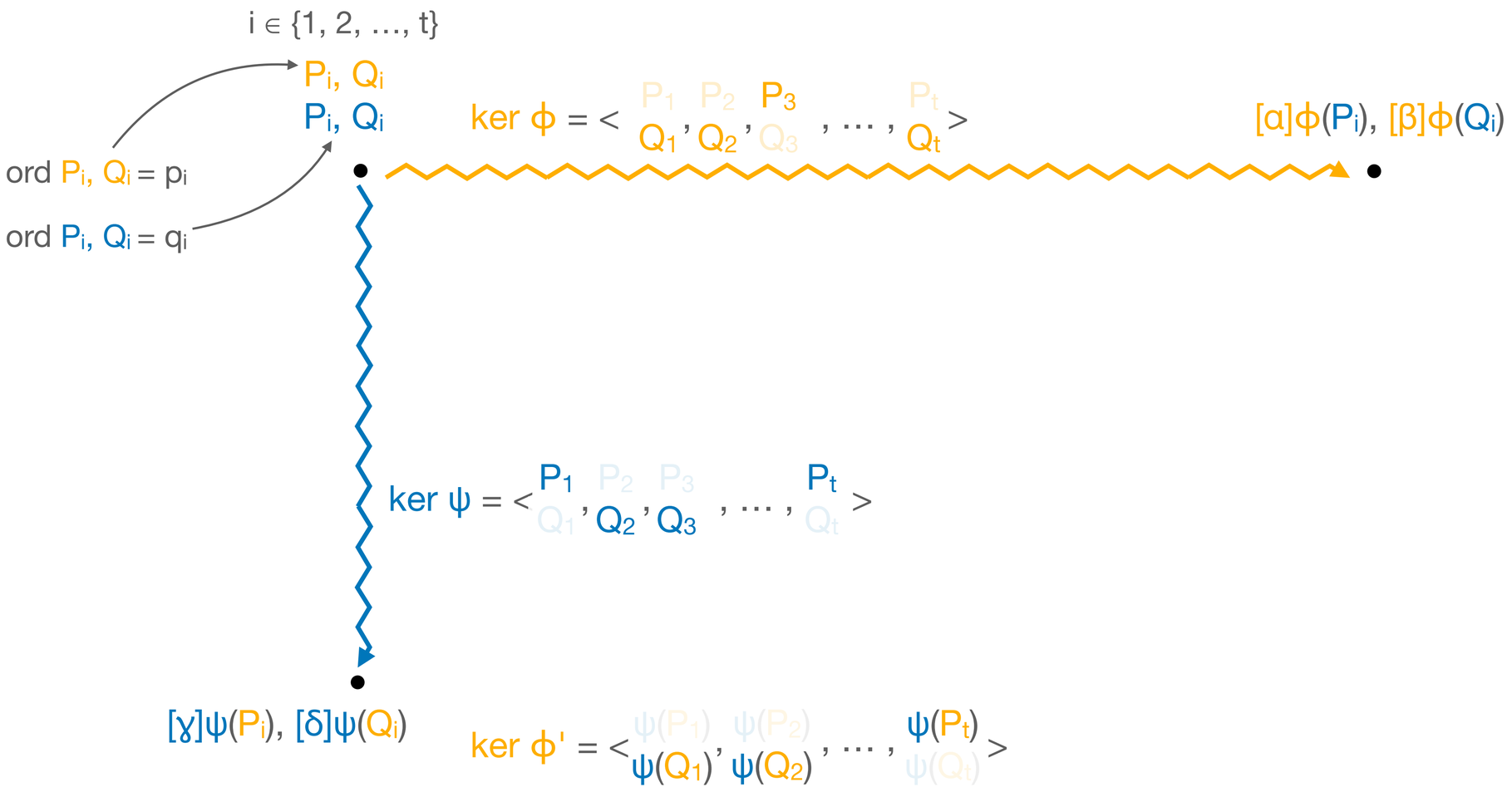
New key exchanges: binSIDH and terSIDH



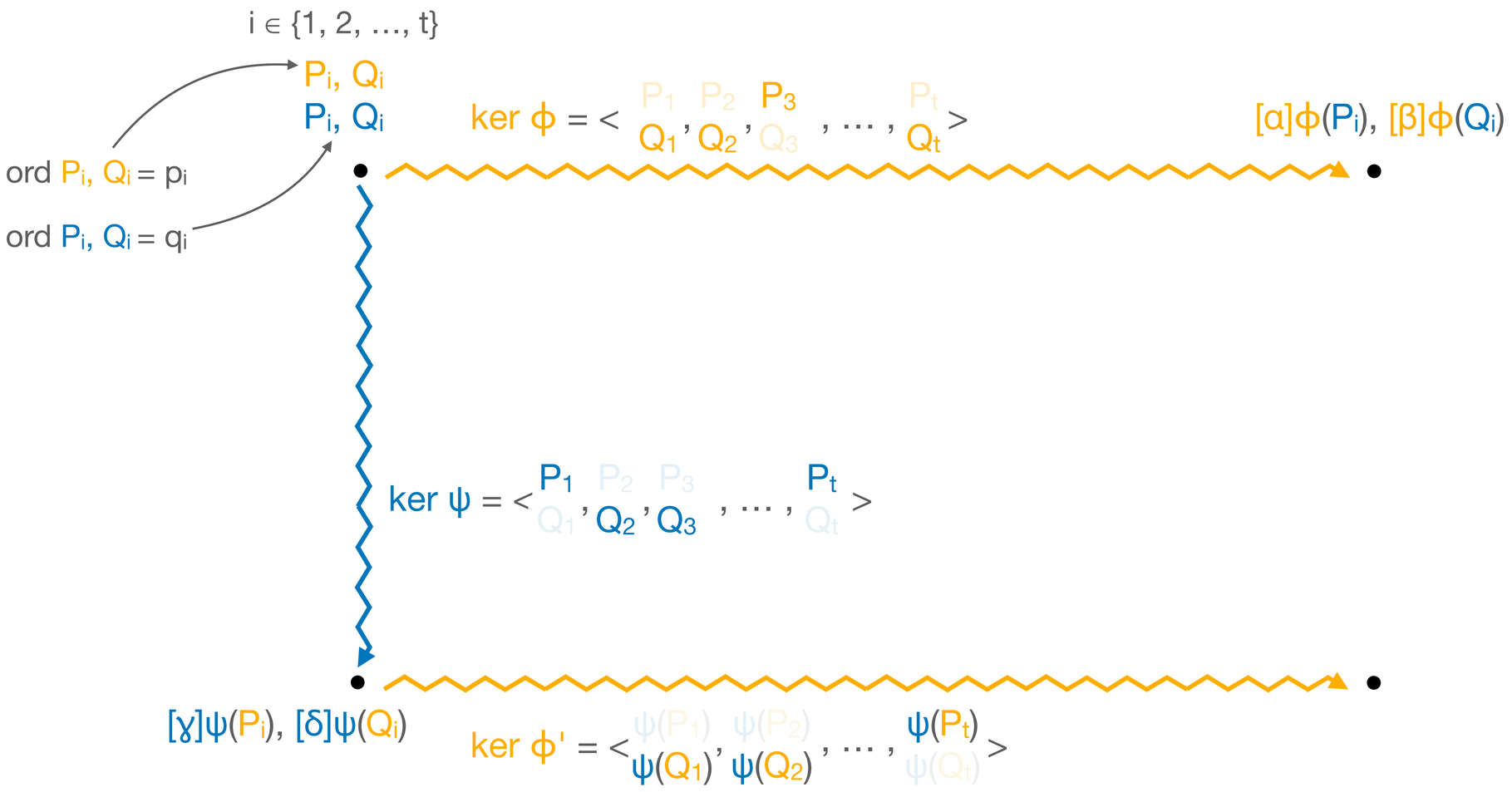
New key exchanges: binSIDH and terSIDH



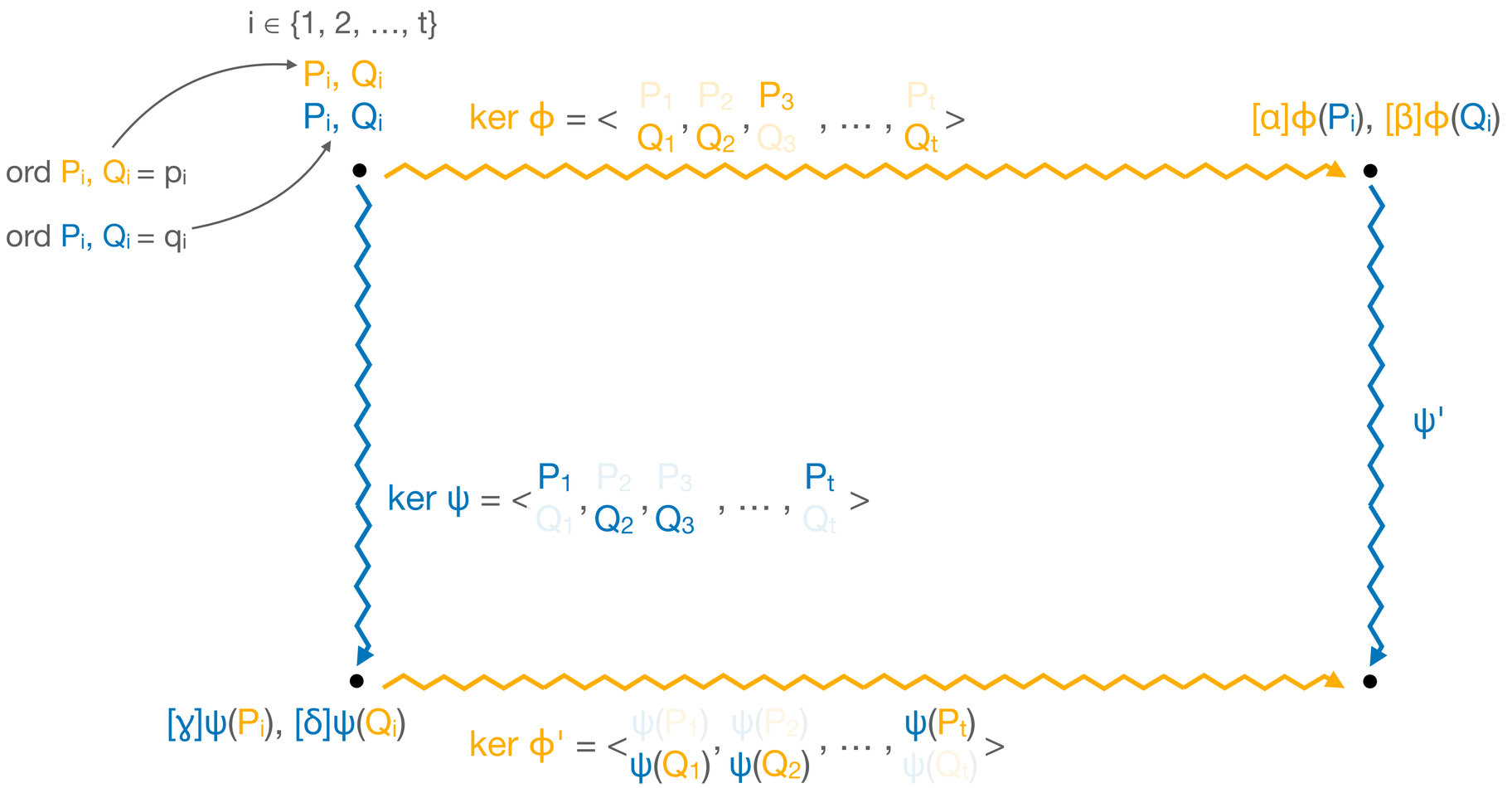
New key exchanges: binSIDH and terSIDH



New key exchanges: binSIDH and terSIDH



New key exchanges: binSIDH and terSIDH



Is it secure?

Compute ϕ, given:

- **E_0, E_1,**
- **P, Q,**
- **[α]ϕ(P), [β]ϕ(Q),**
- **deg ϕ**

Is it secure?

Compute ϕ, given:

- **E_0, E_1,**
- **P, Q,**
- **[α]ϕ(P), [β]ϕ(Q),**
- **deg ϕ**

only 2 subgroups!

A hybrid construction

What if Alice computes bin/ter-SIDH isogenies and Bob computes SIDH-like isogenies?

1. bin/terSIDH isogenies are quite long
2. We can safely reveal the exact torsion images of some small points (with current params, up to $2^{2\lambda}$ is safe)
3. Other party can compute SIDH-like isogenies

Results

			Timings (s)			
	λ	$\log p$	KeyGen_A	KeyGen_B	$\mathsf{SharedKey}_A$	$\mathsf{SharedKey}_B$
$\mathsf{binSIDH}^{\mathsf{hyb}}$	128	2004	0.23	14.33	0.22	10.66
	192	3126	0.62	56.77	0.61	42.85
	256	4267	1.41	157.58	1.34	117.07
$\mathsf{terSIDH}^{\mathsf{hyb}}$	**128**	**1532**	**0.16**	**3.21**	**0.16**	**1.96**
	192	2373	0.47	13.44	0.44	10.01
	256	3216	0.94	34.66	0.90	23.57

Conclusion

1. New techniques for computing parallel isogenies while revealing much less information

Conclusion

1. New techniques for computing parallel isogenies while revealing much less information

2. Four new protocols, depending on the application and use cases

Conclusion

1. New techniques for computing parallel isogenies while revealing much less information

2. Four new protocols, depending on the application and use cases

3. Faster and more compact than previous constructions, with encouraging results for terSIDH-hyb