POKÉ: A Compact and Efficient PKE from Higher-dimensional Isogenies

Andrea Basso, Luciano Maino

May 5th — EUROCRYPT 2025

A brief history of isogeny-based encryption

SIDH

First practical isogeny-based protocol

2011

A brief history of isogeny-based encryption

SIDH

First practical isogeny-based protocol

2011

2018

CSIDH

Based on commutative group action

The (C)SIDH protocol

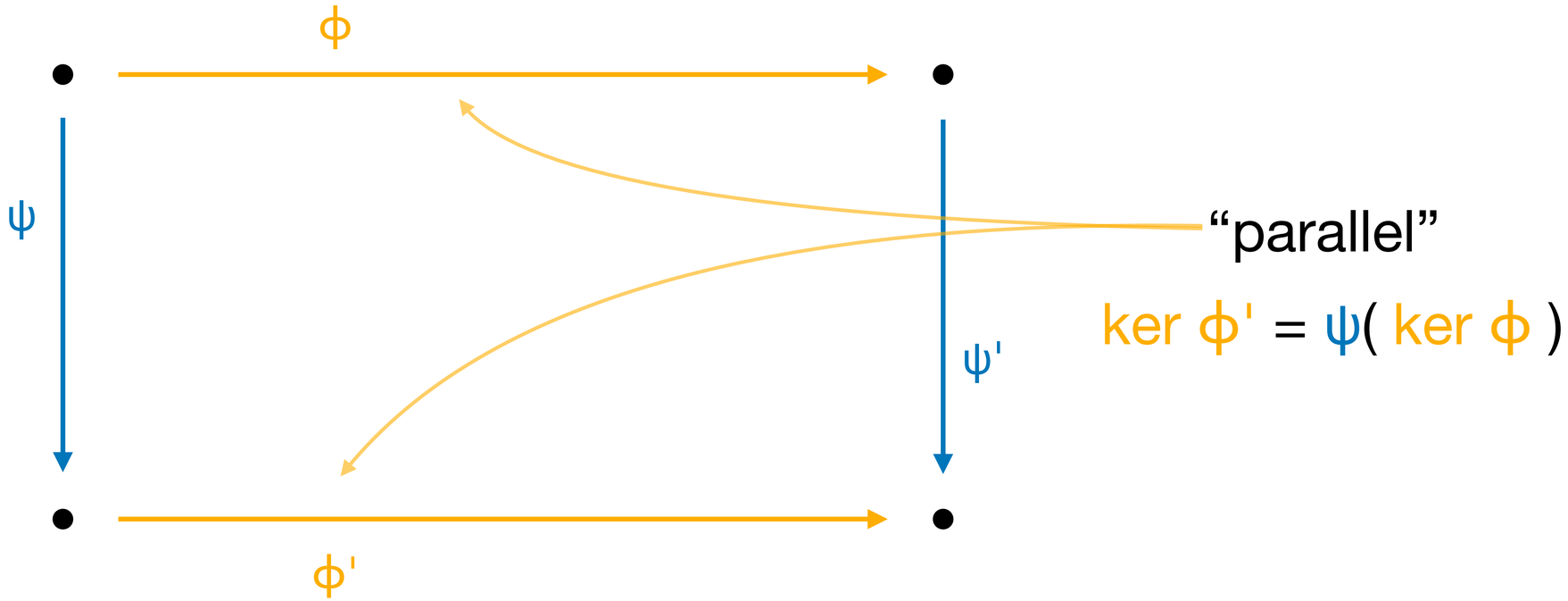
-

The (C)SIDH protocol

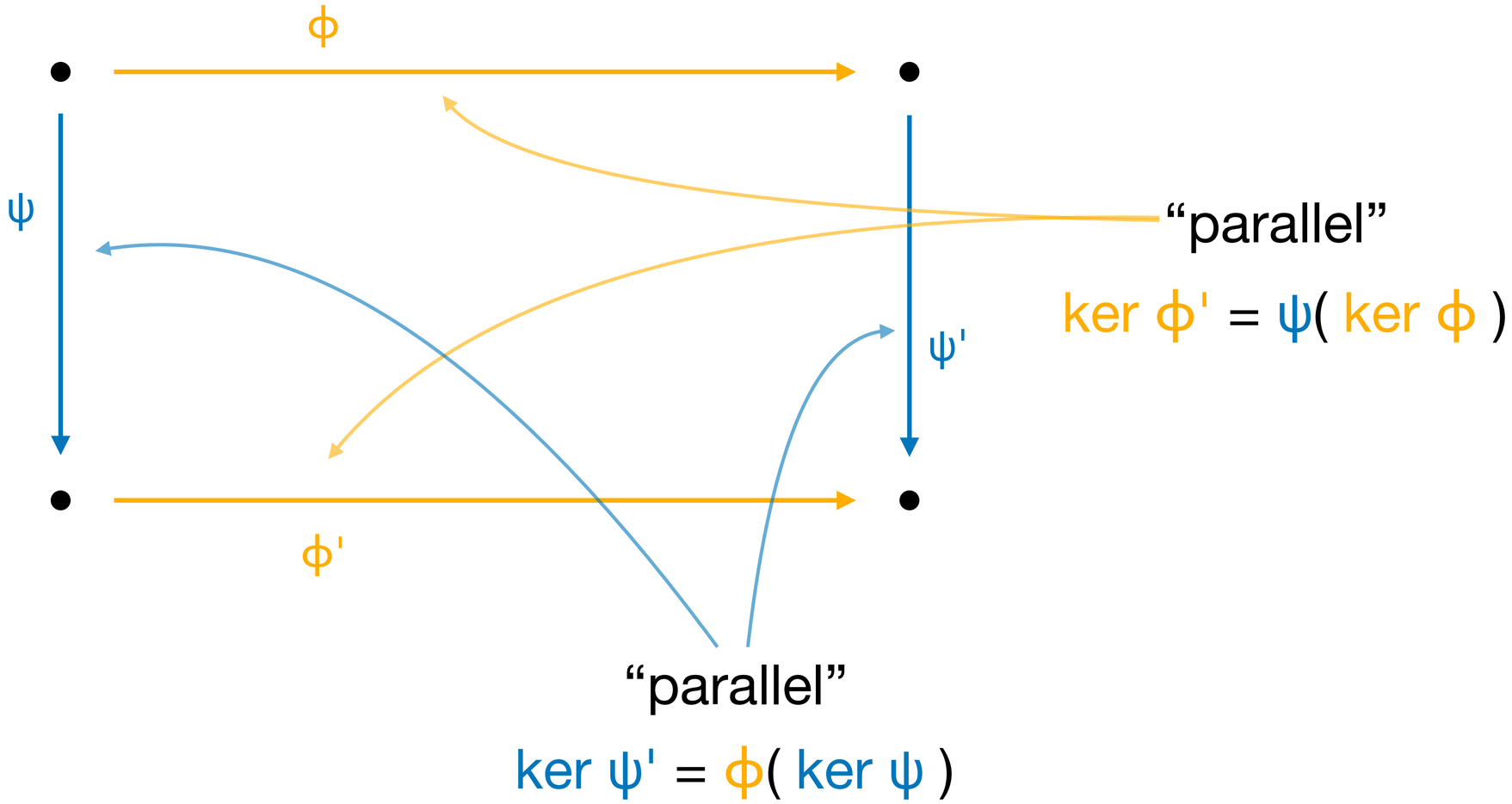
The (C)SIDH protocol

The (C)SIDH protocol

The (C)SIDH protocol



The (C)SIDH protocol



A brief history of isogeny-based encryption

SIDH

First practical isogeny-based protocol

2011

2018

CSIDH

Based on commutative group action

A brief history of isogeny-based encryption

SIDH

First practical isogeny-based protocol

2011

CSIDH

Based on commutative group action

2018

SIDH attacks

Efficient key-recovery attacks on SIDH

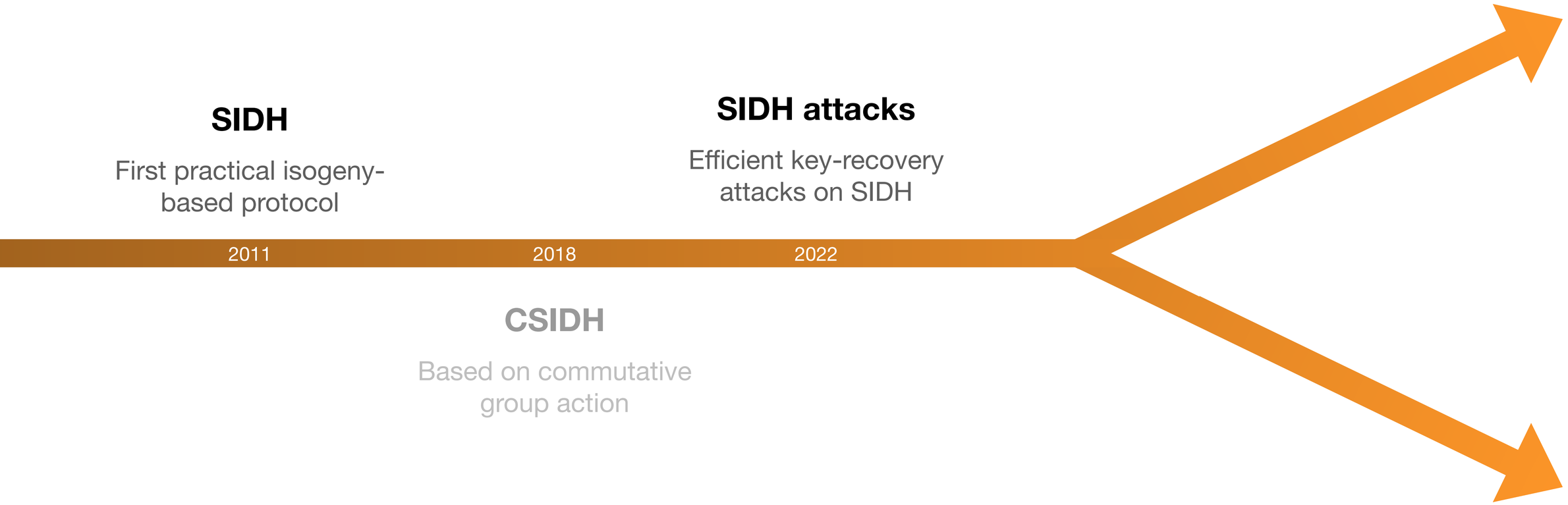
2022

Higher-dimensional representations

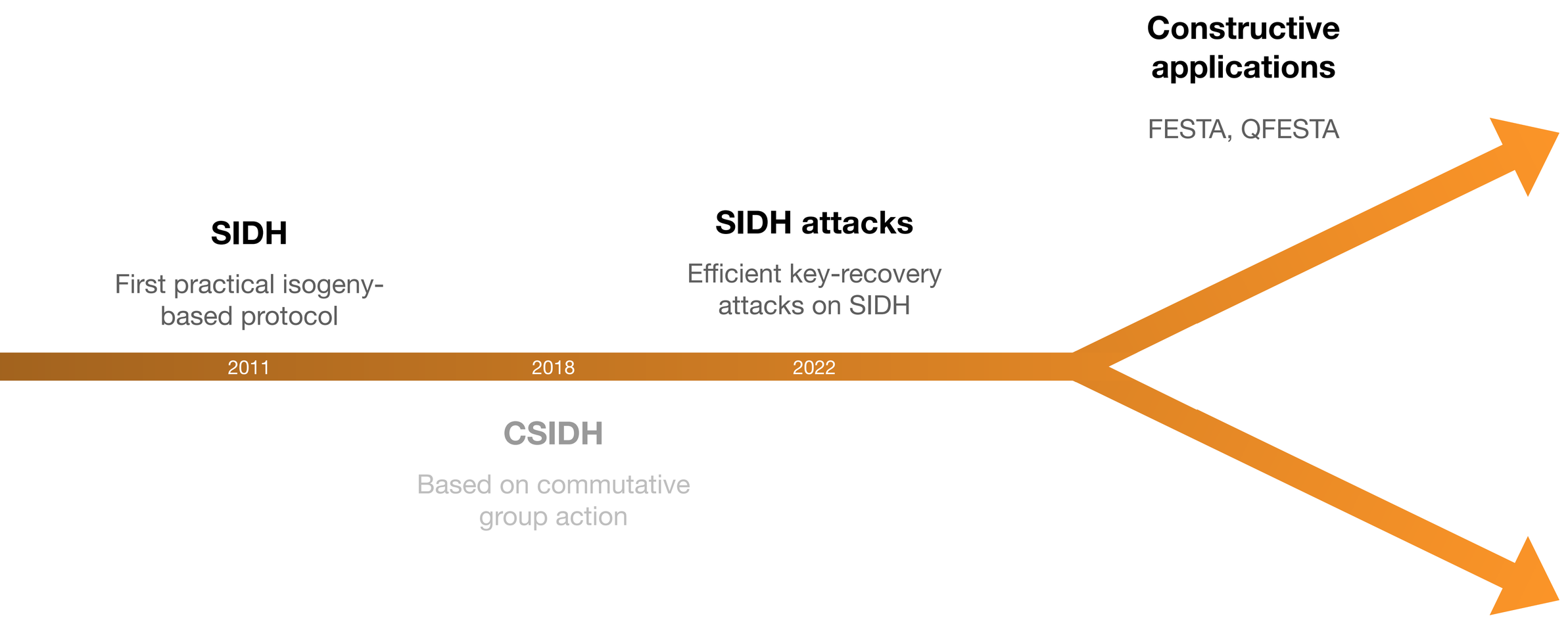
Higher-dimensional representation

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

A brief history of isogeny-based encryption

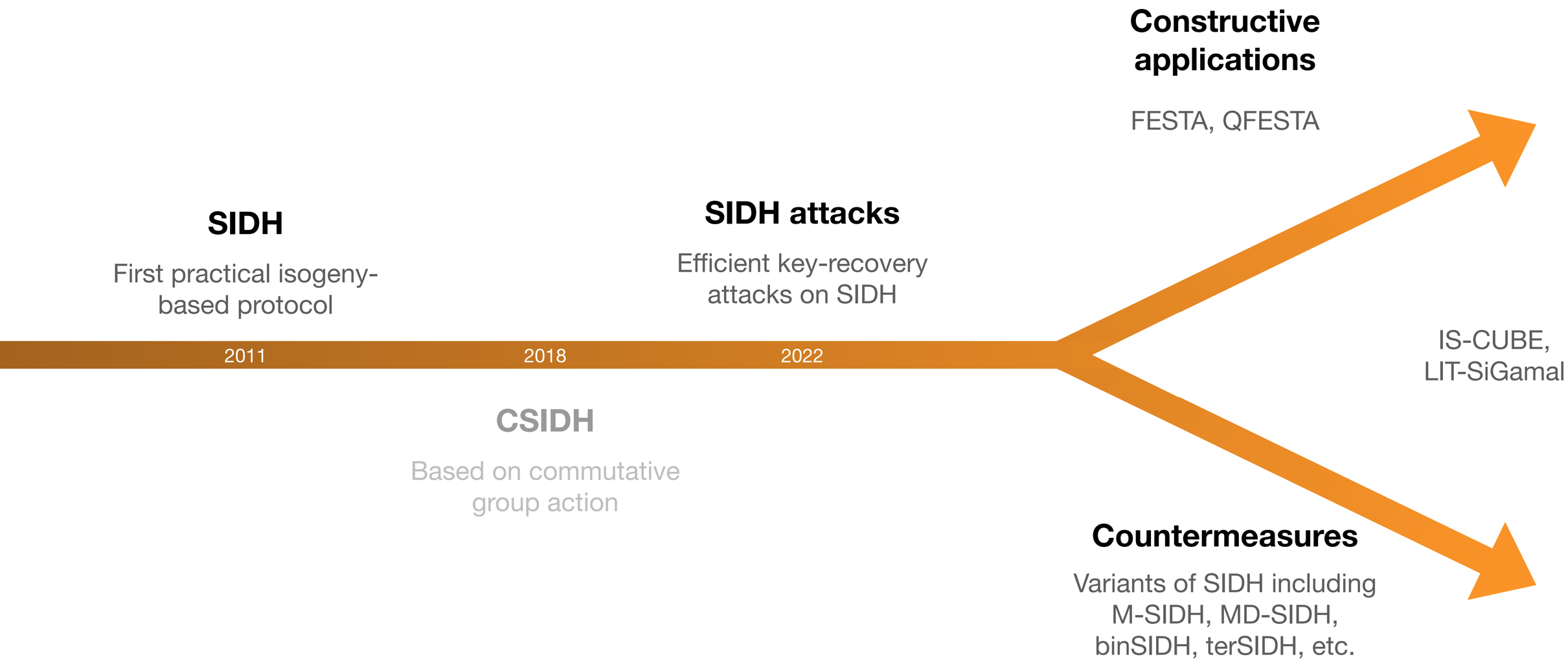


A brief history of isogeny-based encryption



A brief history of isogeny-based encryption

A brief history of isogeny-based encryption



Public/private HD representations

Higher-dimensional representation

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

Public/private HD representations

public/private

Higher-dimensional representation

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

Public/private HD representations

public/private

Higher-dimensional representation

- E_0, E_1
- P, Q and [a]ϕ(P), [a]ϕ(Q)
- deg ϕ

Public/private HD representations

public/private

Higher-dimensional representation

- E_0, E_1
- P, Q and $[a]\phi(P)$, $[a]\phi(Q)$
- deg ϕ
- a

Public/private HD representations

public/private

Higher-dimensional representation

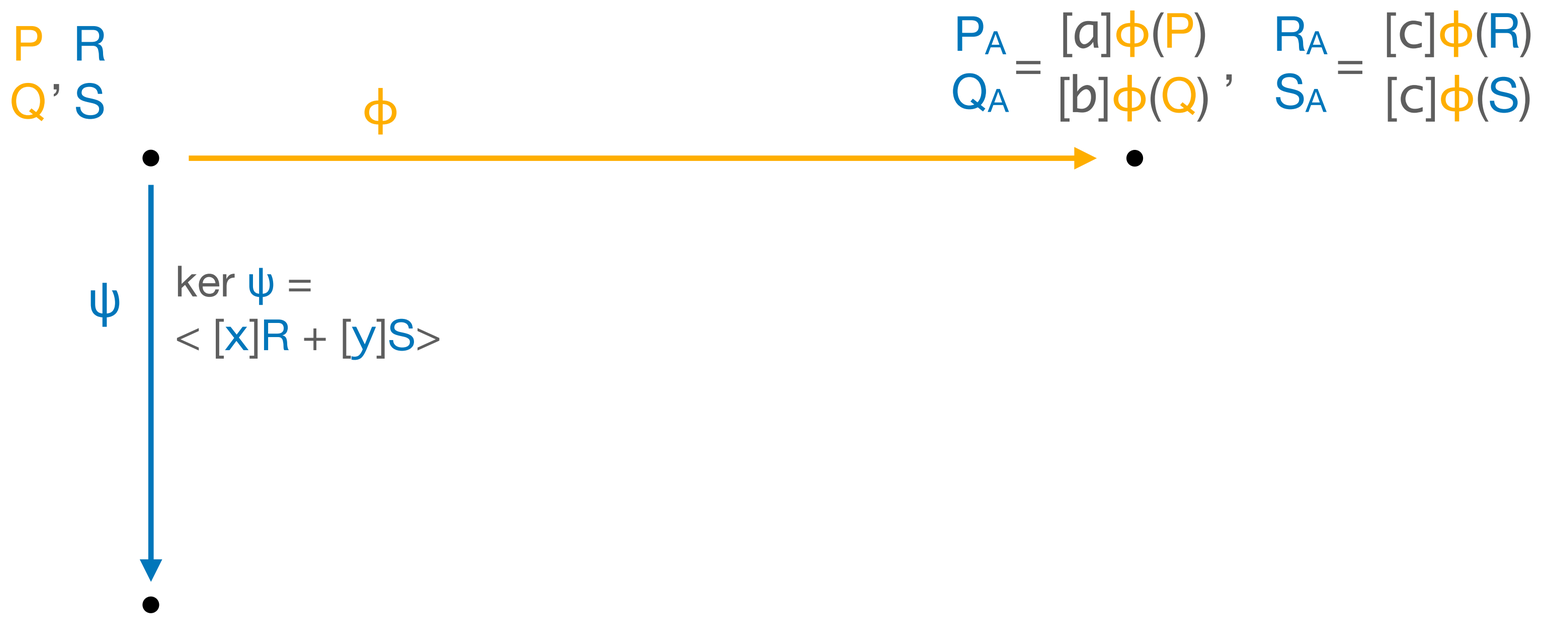
- E_0, E_1
- P, Q and $[a]\phi(P)$, $[a]\phi(Q)$
- deg ϕ
- a

} public

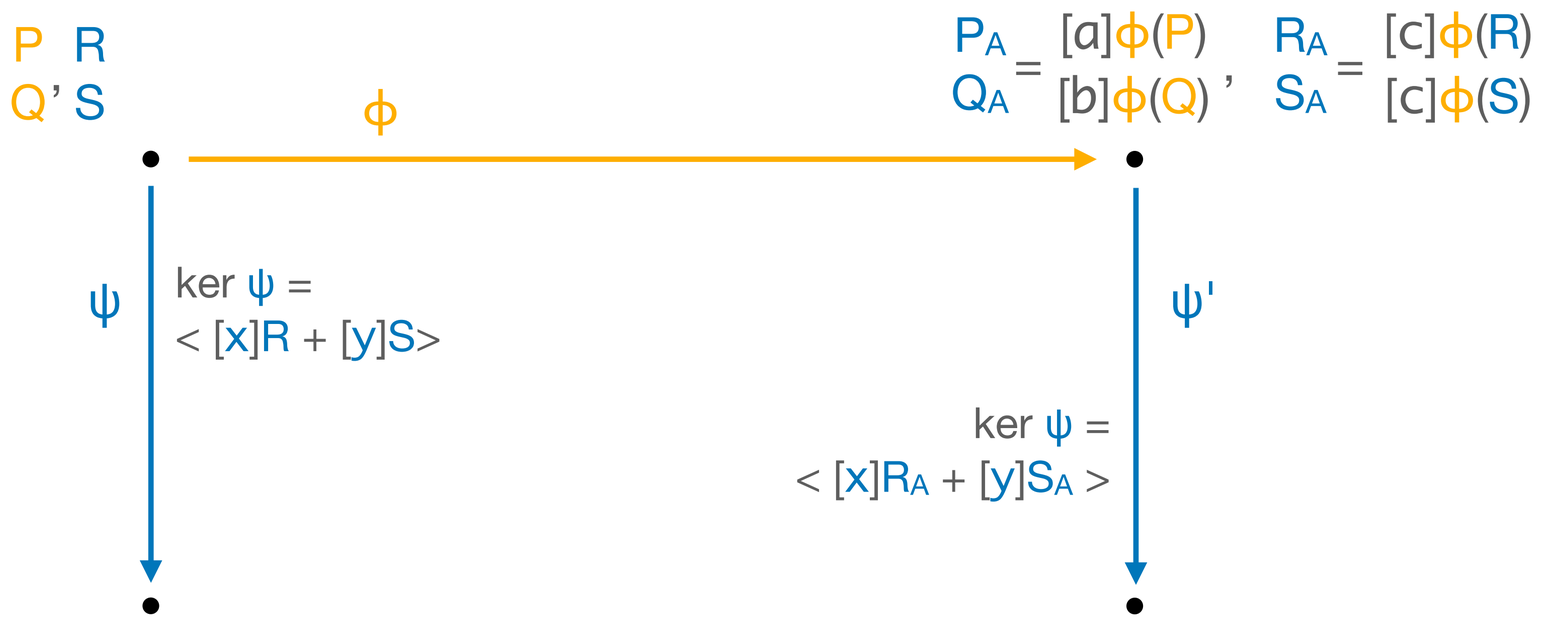
secret

Computing parallel isogenies from HD representations

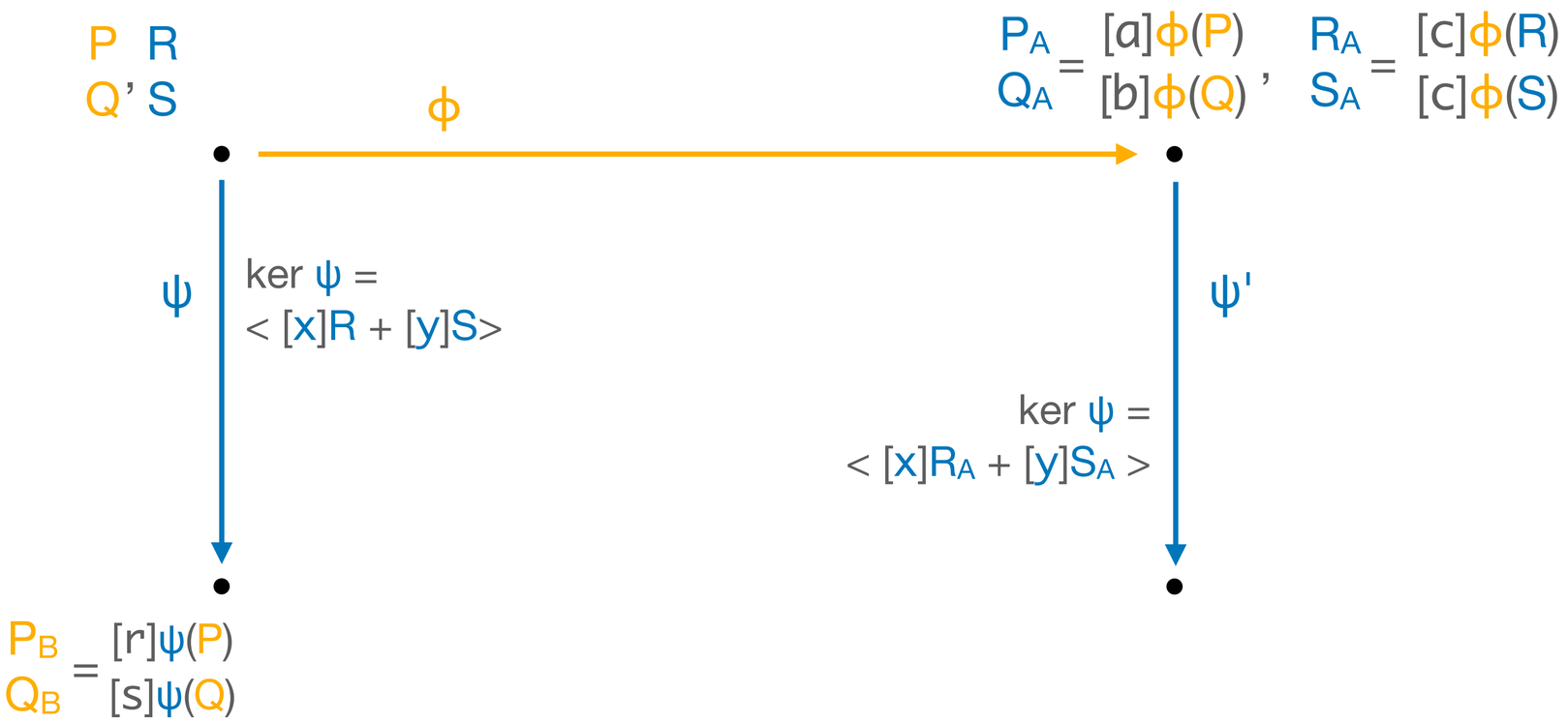
Computing parallel isogenies from HD representations



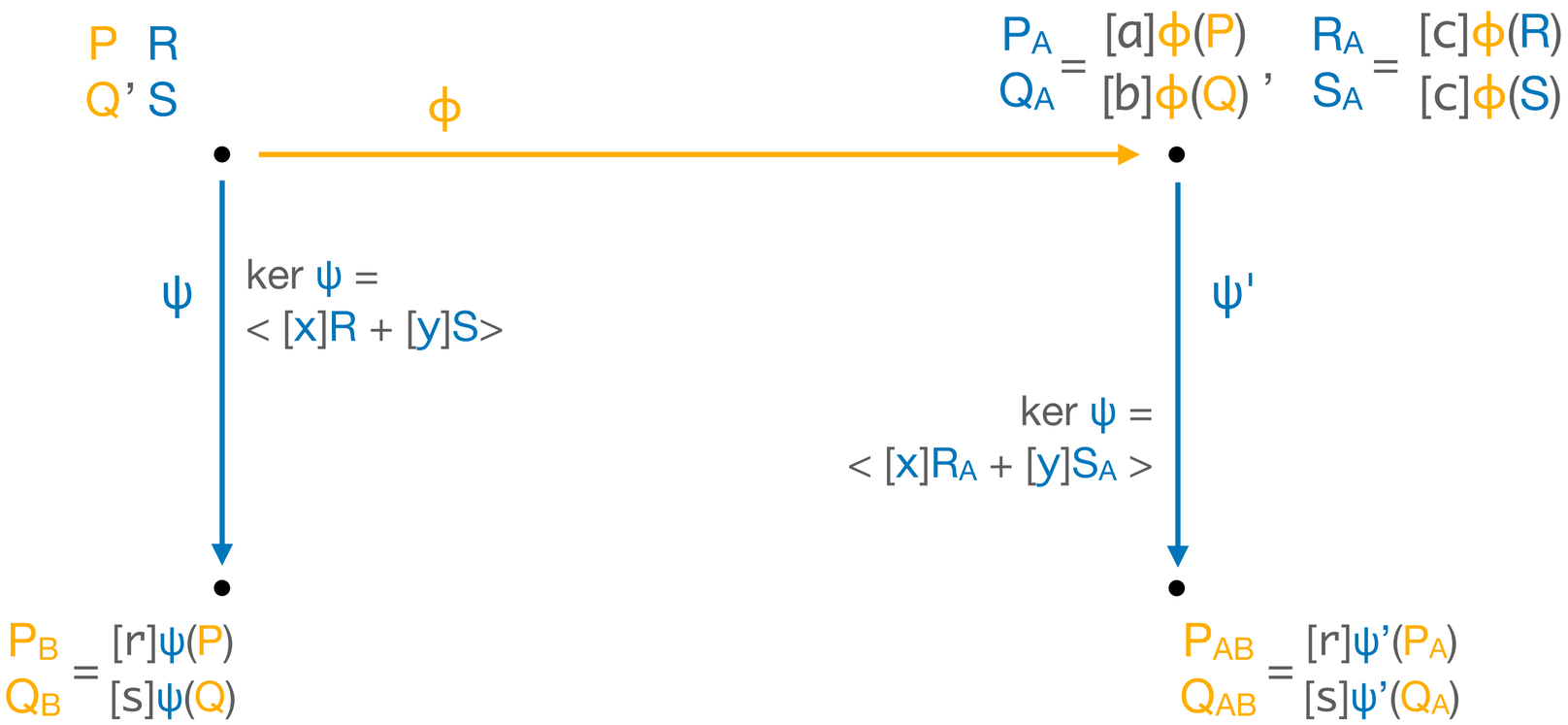
Computing parallel isogenies from HD representations



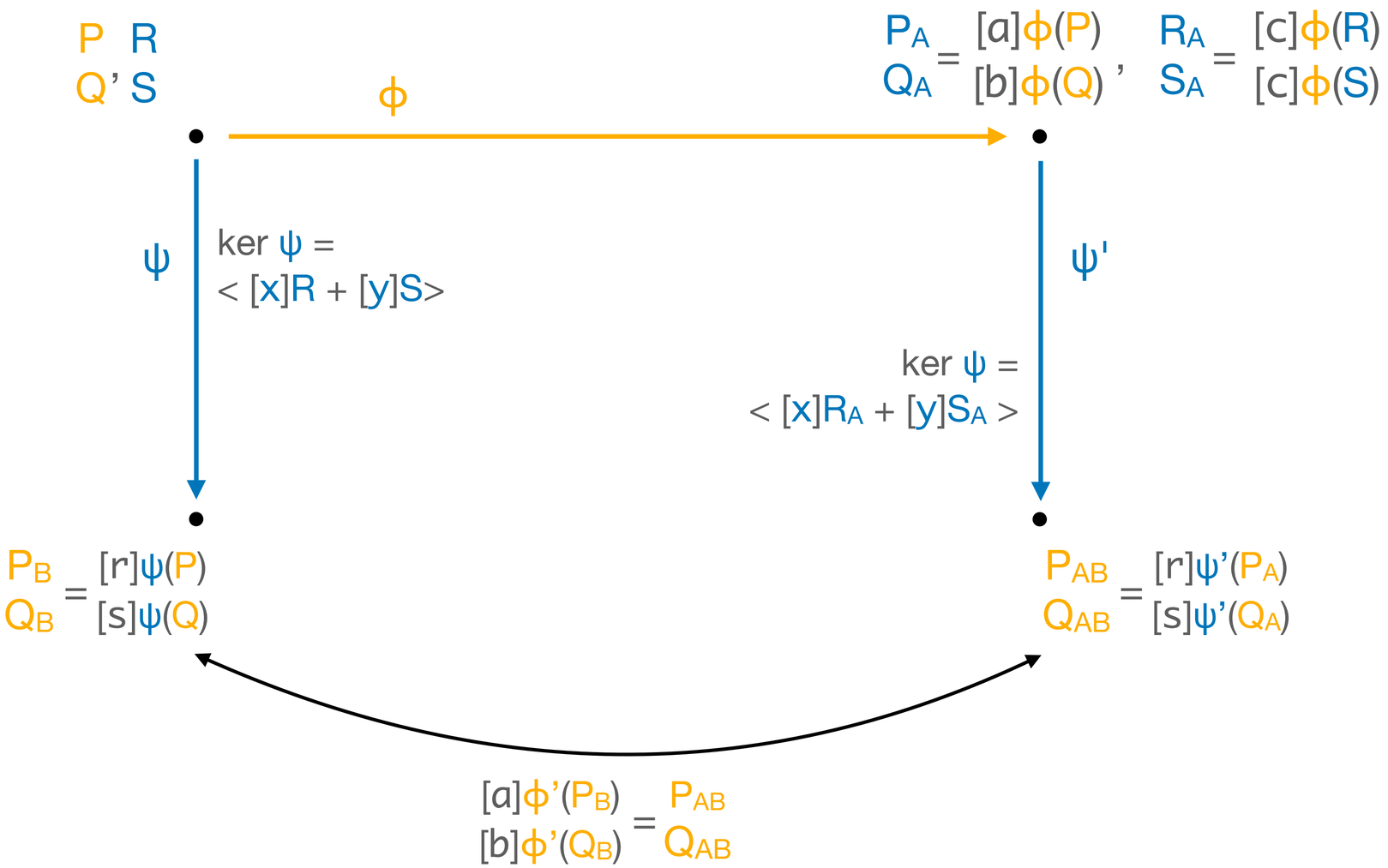
Computing parallel isogenies from HD representations



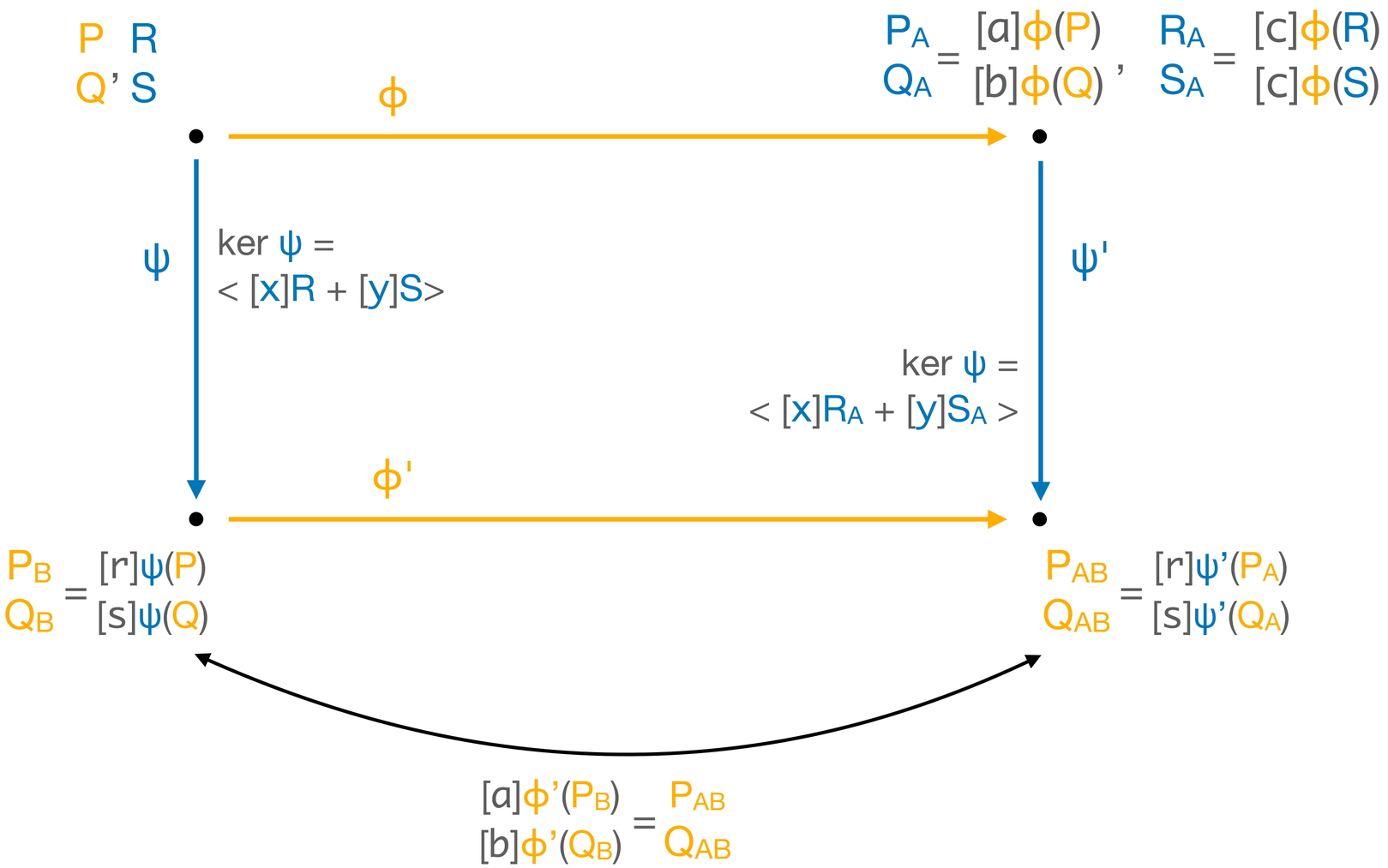
Computing parallel isogenies from HD representations



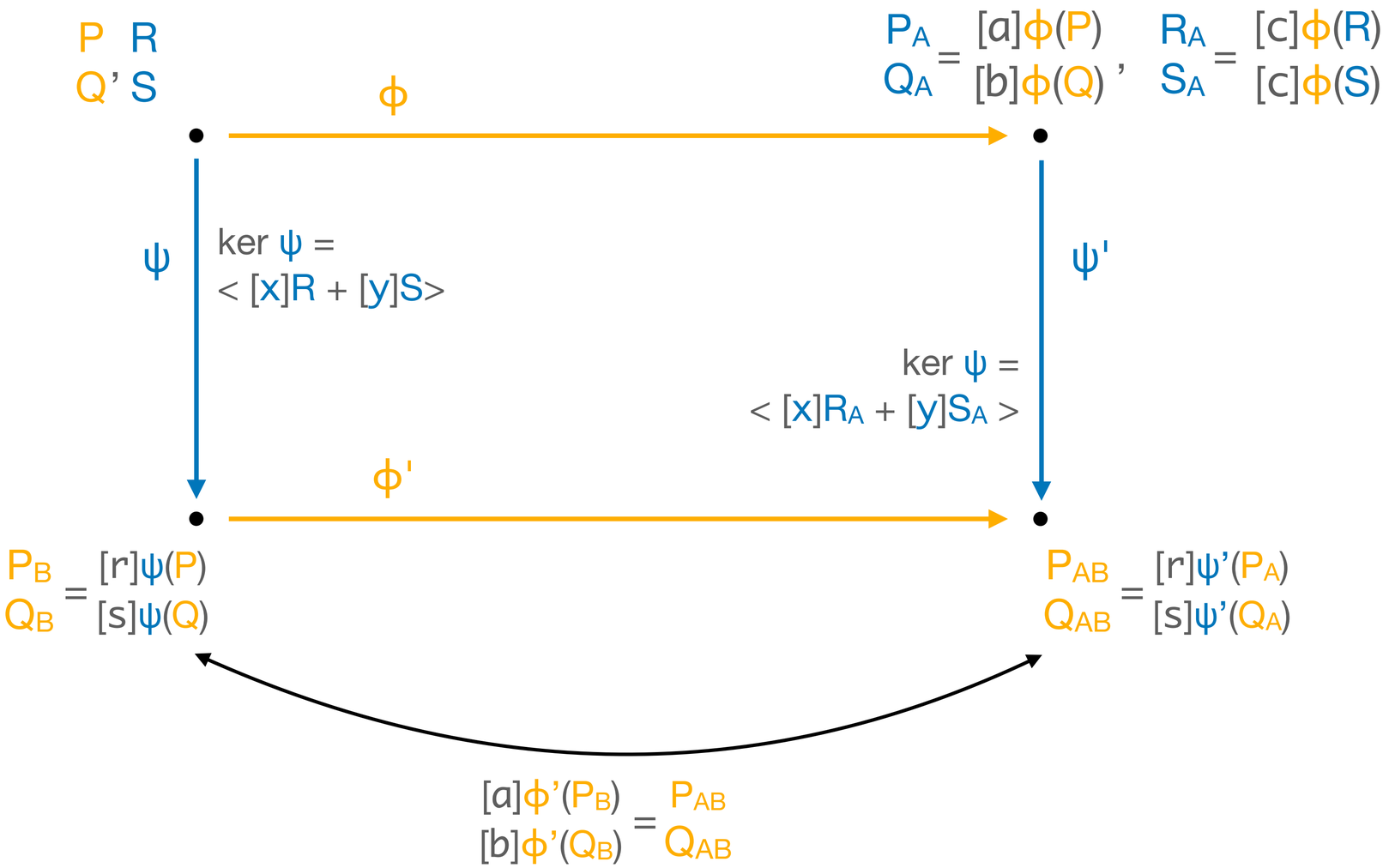
Computing parallel isogenies from HD representations



Computing parallel isogenies from HD representations

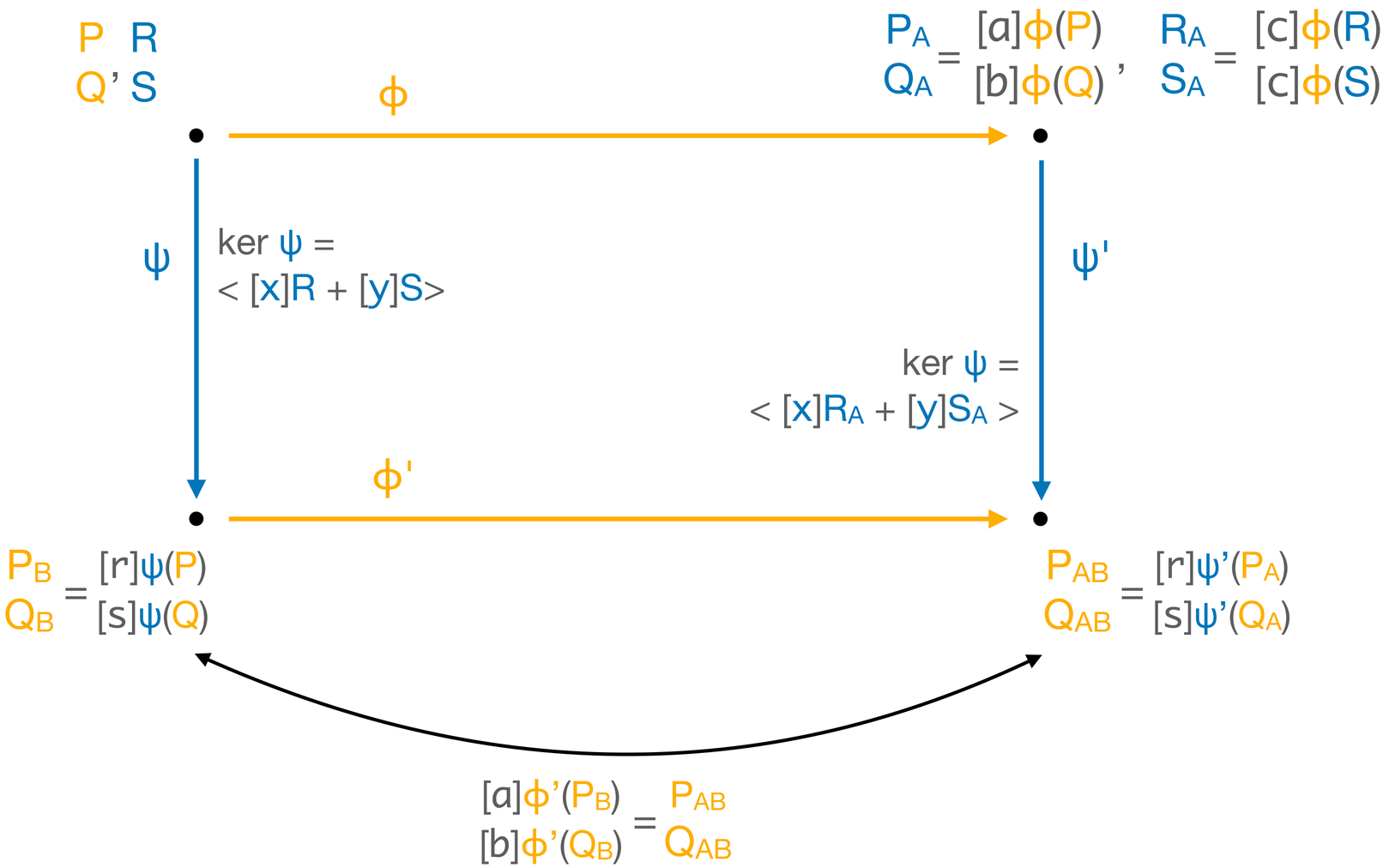


Computing parallel isogenies from HD representations



public/private HD representations

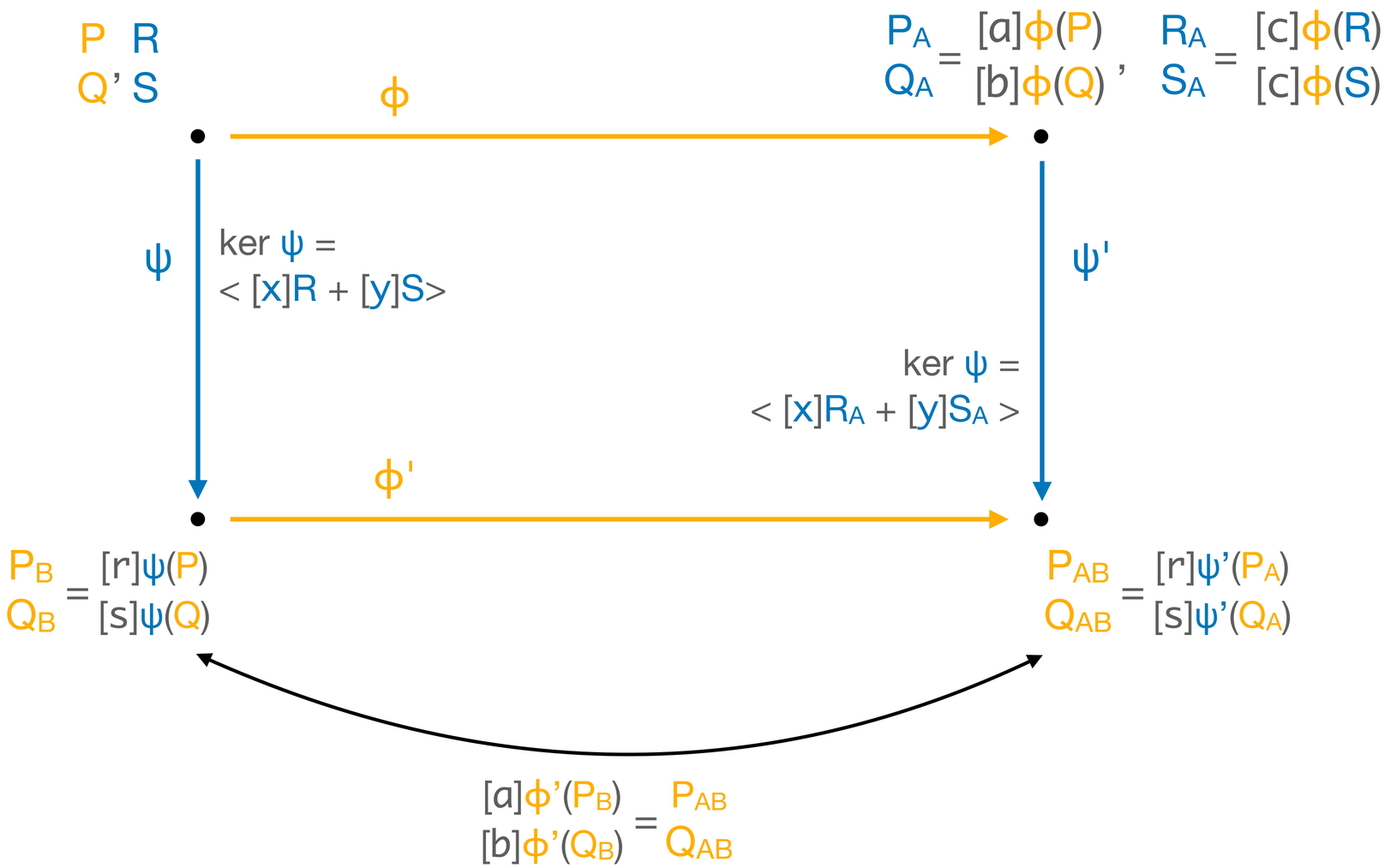
Computing parallel isogenies from HD representations



public/private HD representations

⇓

Computing parallel isogenies from HD representations

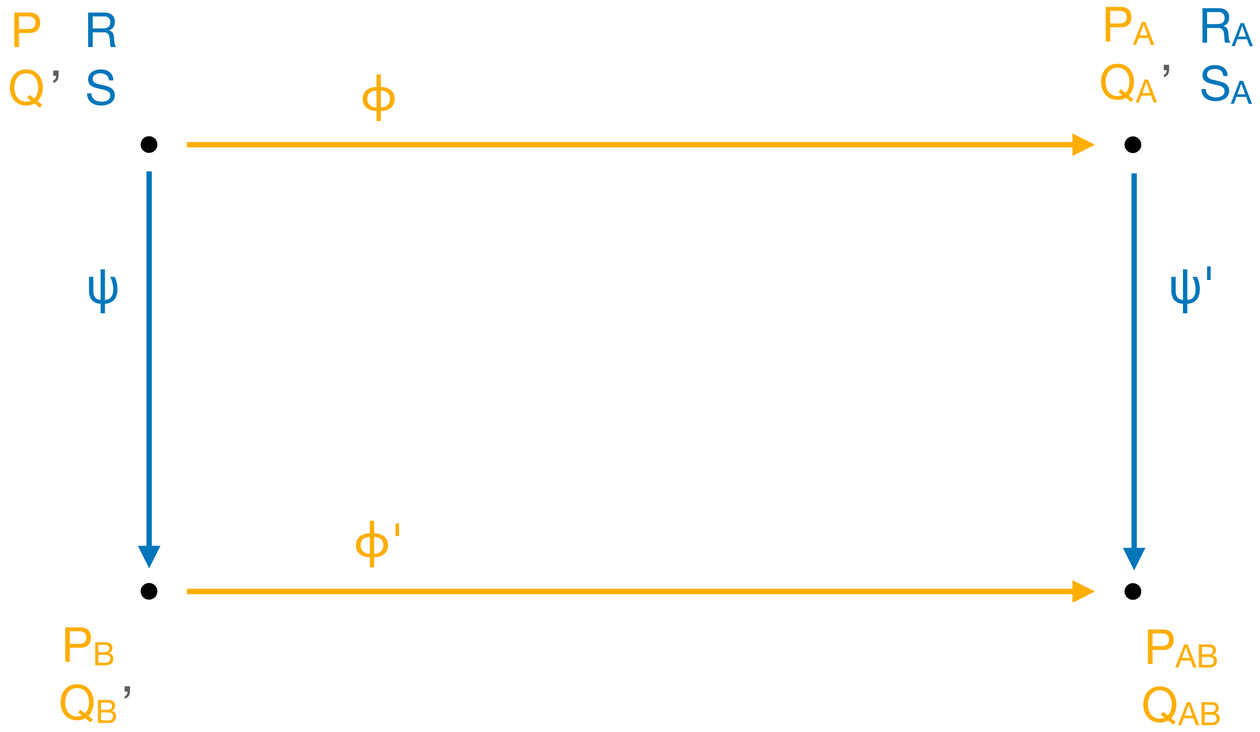


public/private HD representations

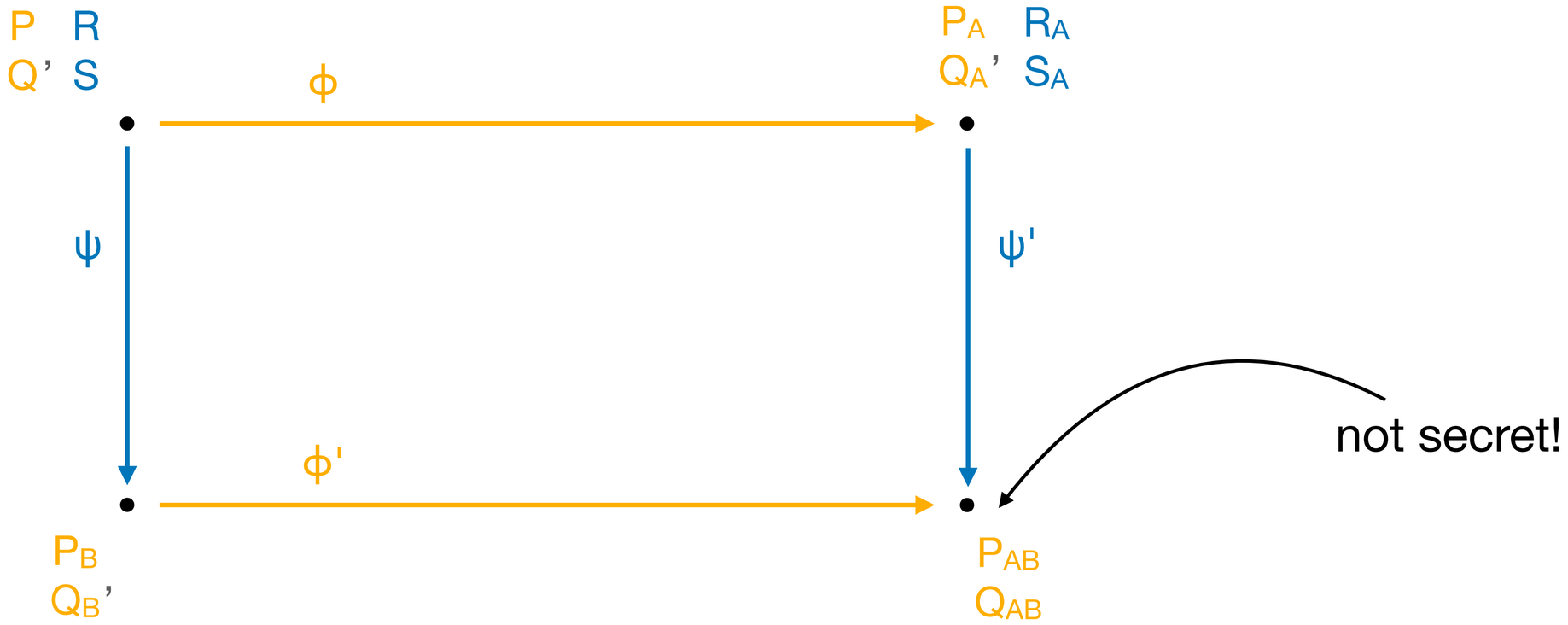
⇓

parallel isogenies like in (C)SIDH

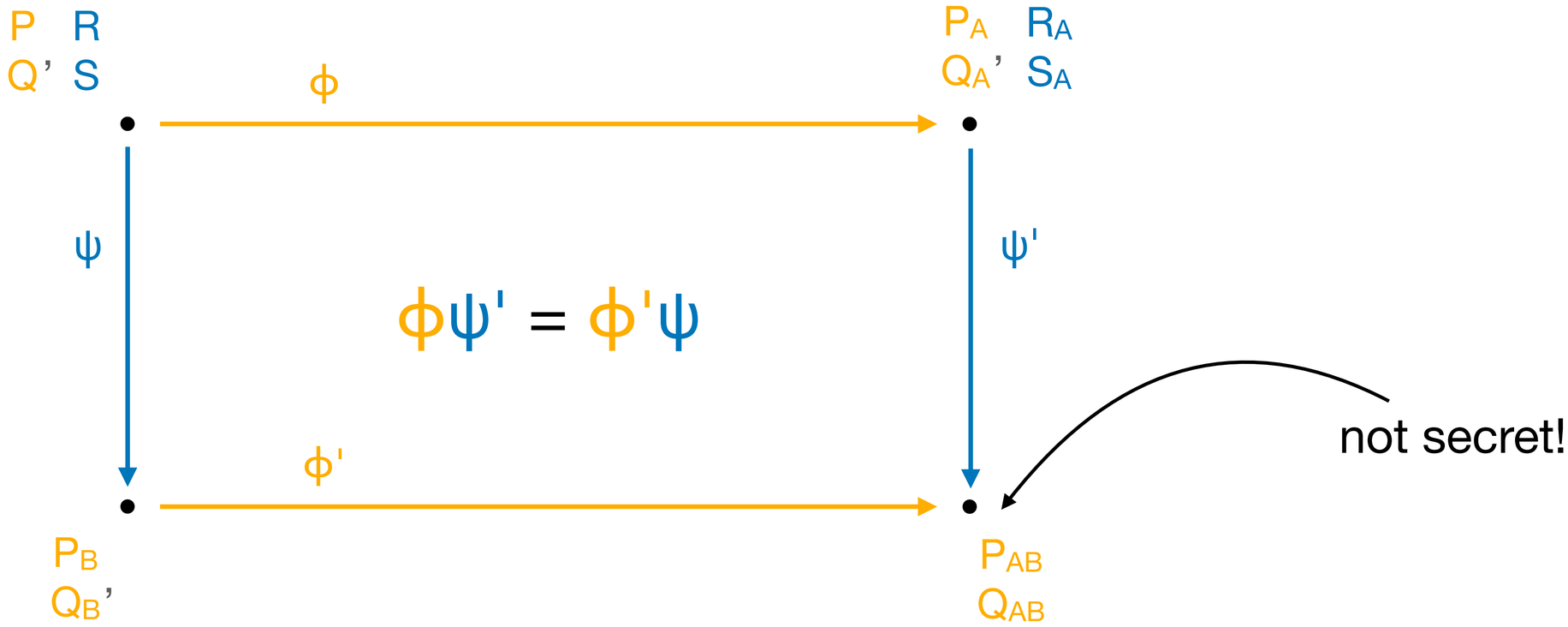
A shared secret?



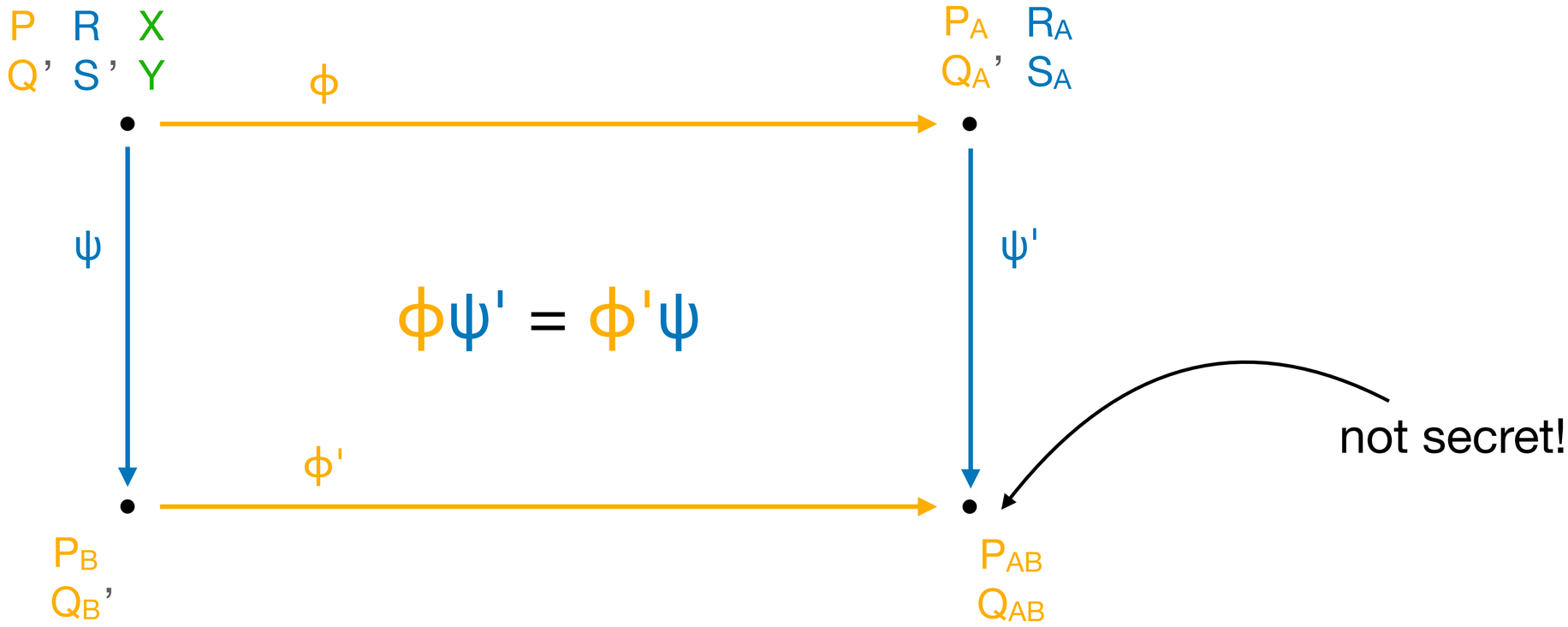
A shared secret?



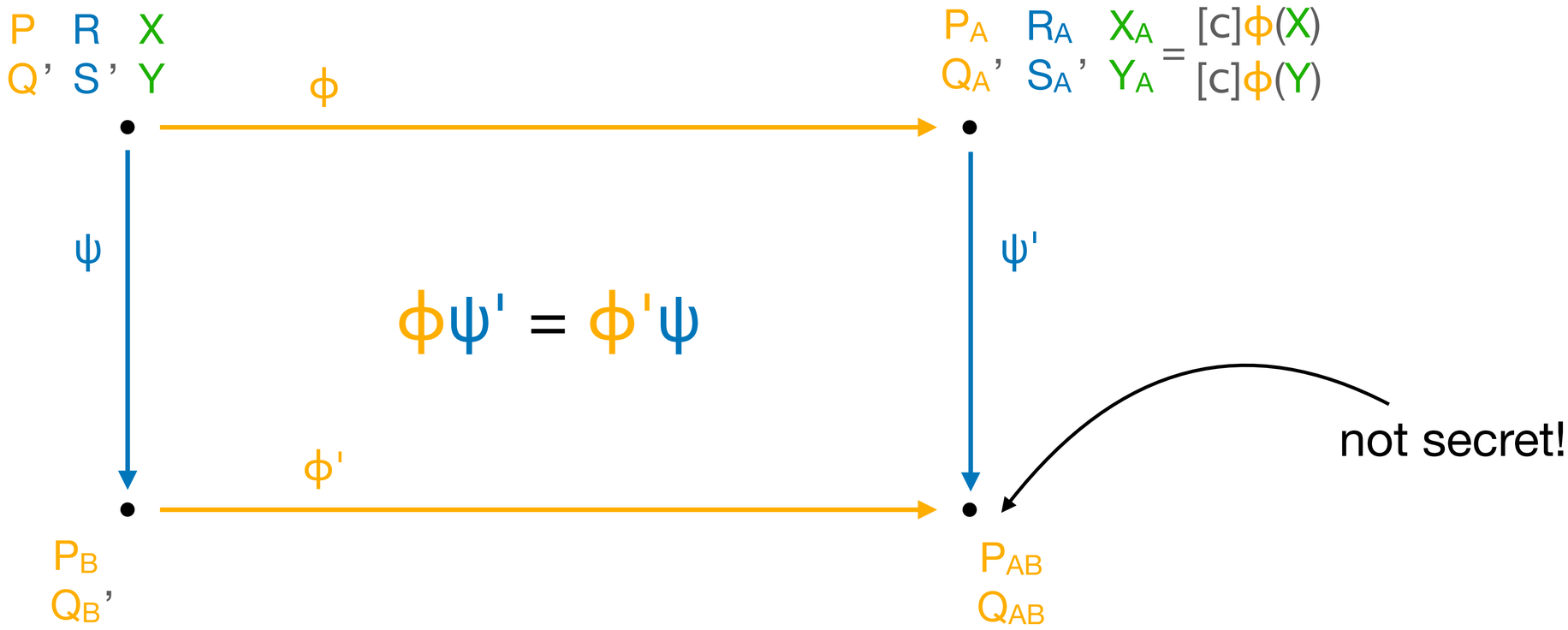
A shared secret?



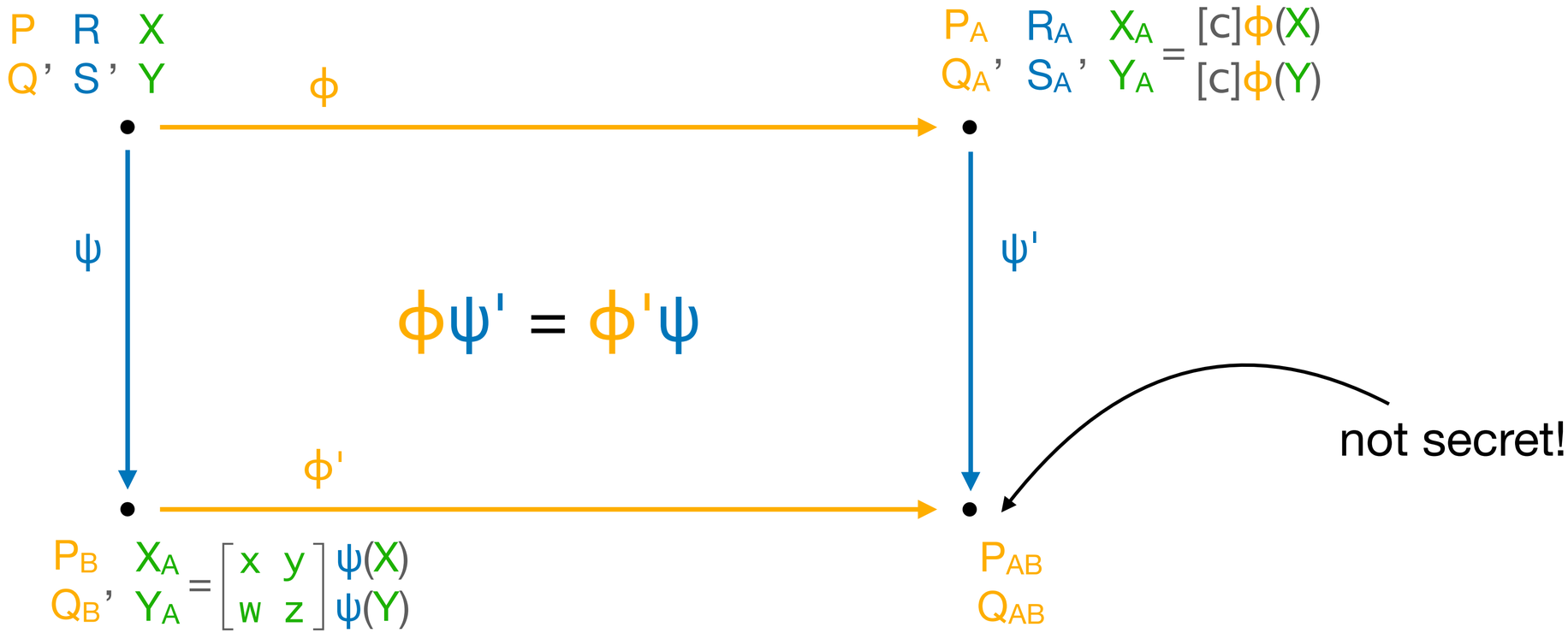
A shared secret?



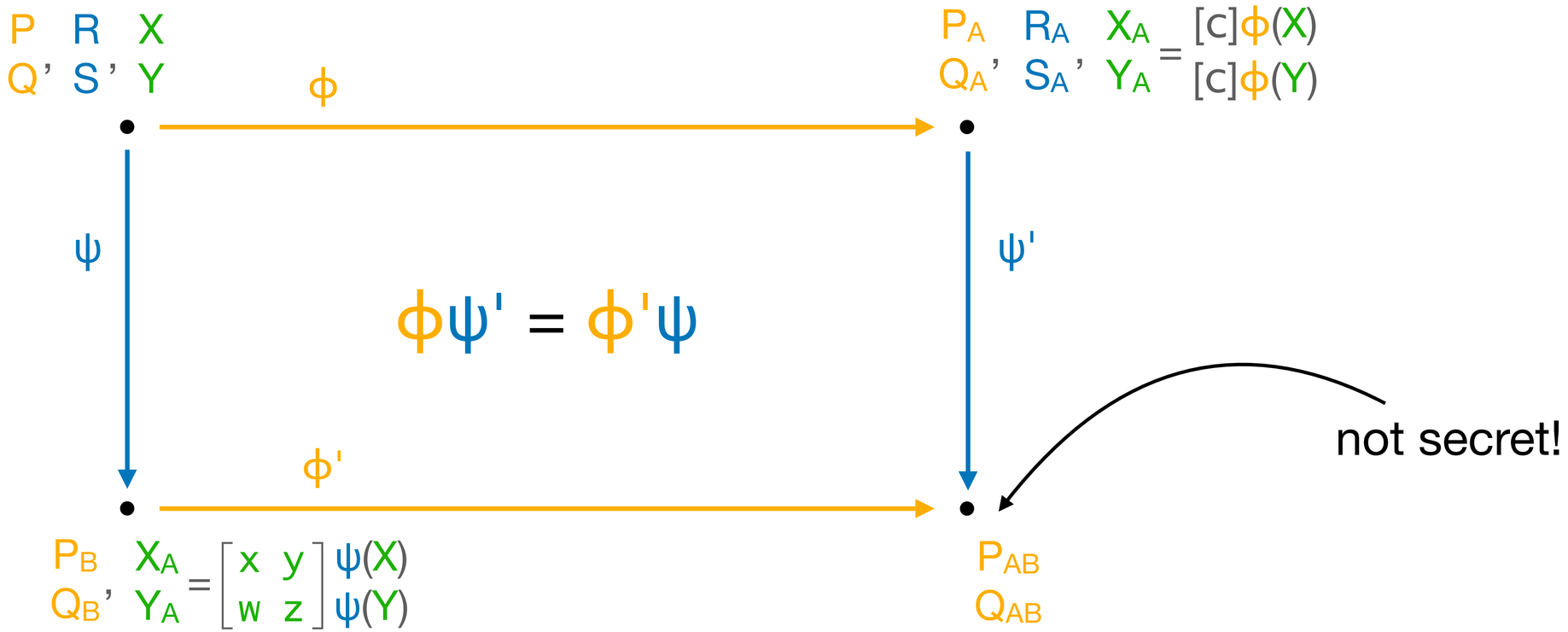
A shared secret?



A shared secret?



A shared secret?

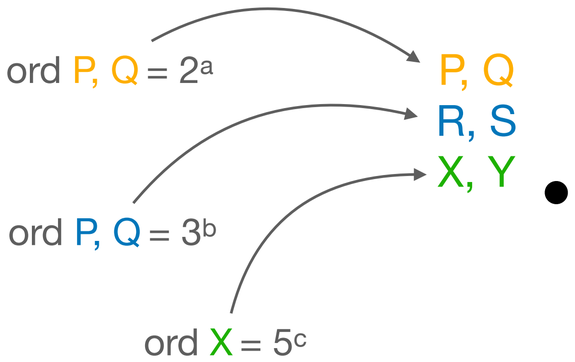


$$X_{AB} = \begin{bmatrix} x & y \\ w & z \end{bmatrix} \psi'(X_A) = [c]\phi'(X_B)$$
$$Y_{AB} = \begin{bmatrix} x & y \\ w & z \end{bmatrix} \psi'(Y_A) = [c]\phi'(Y_B)$$

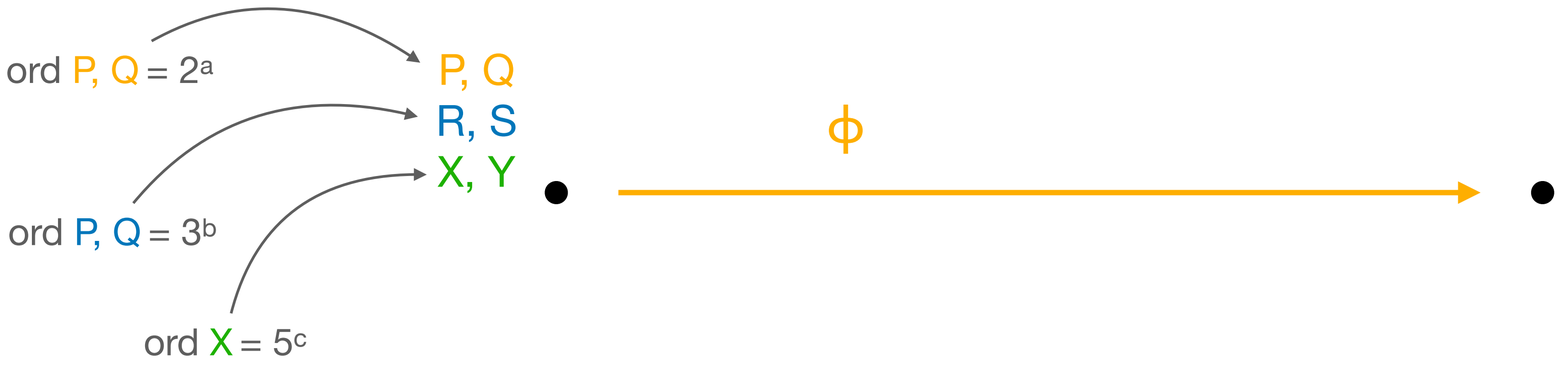
The POKE PKE

P, Q
R, S
X, Y .

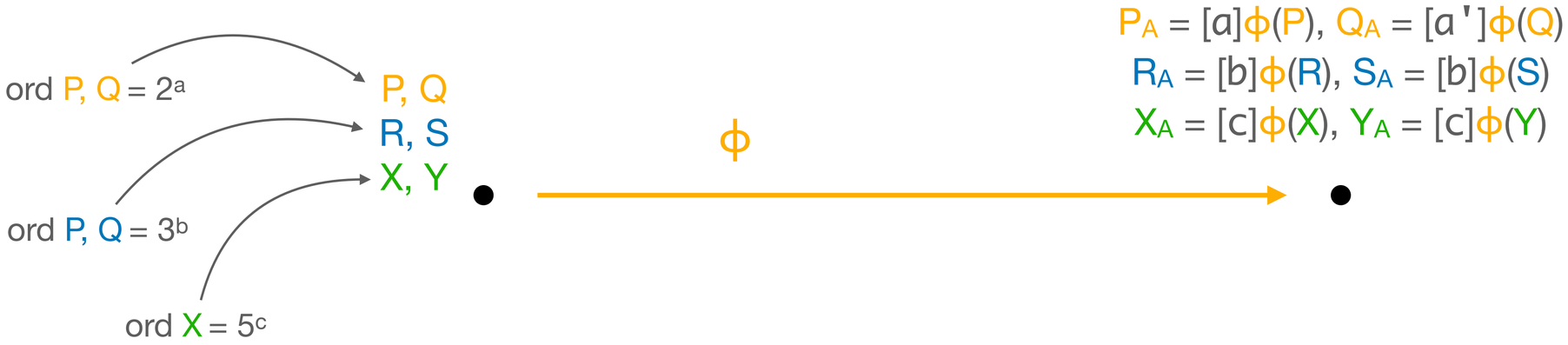
The POKE PKE



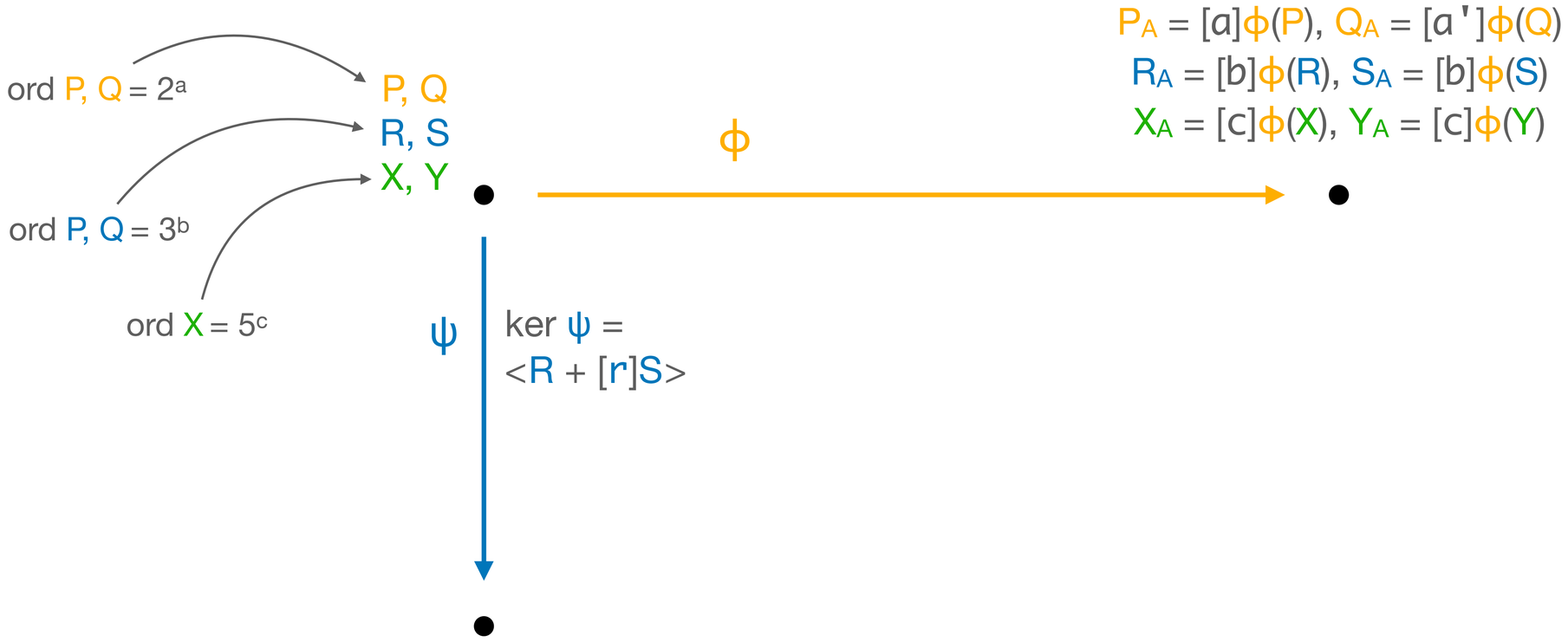
The POKE PKE



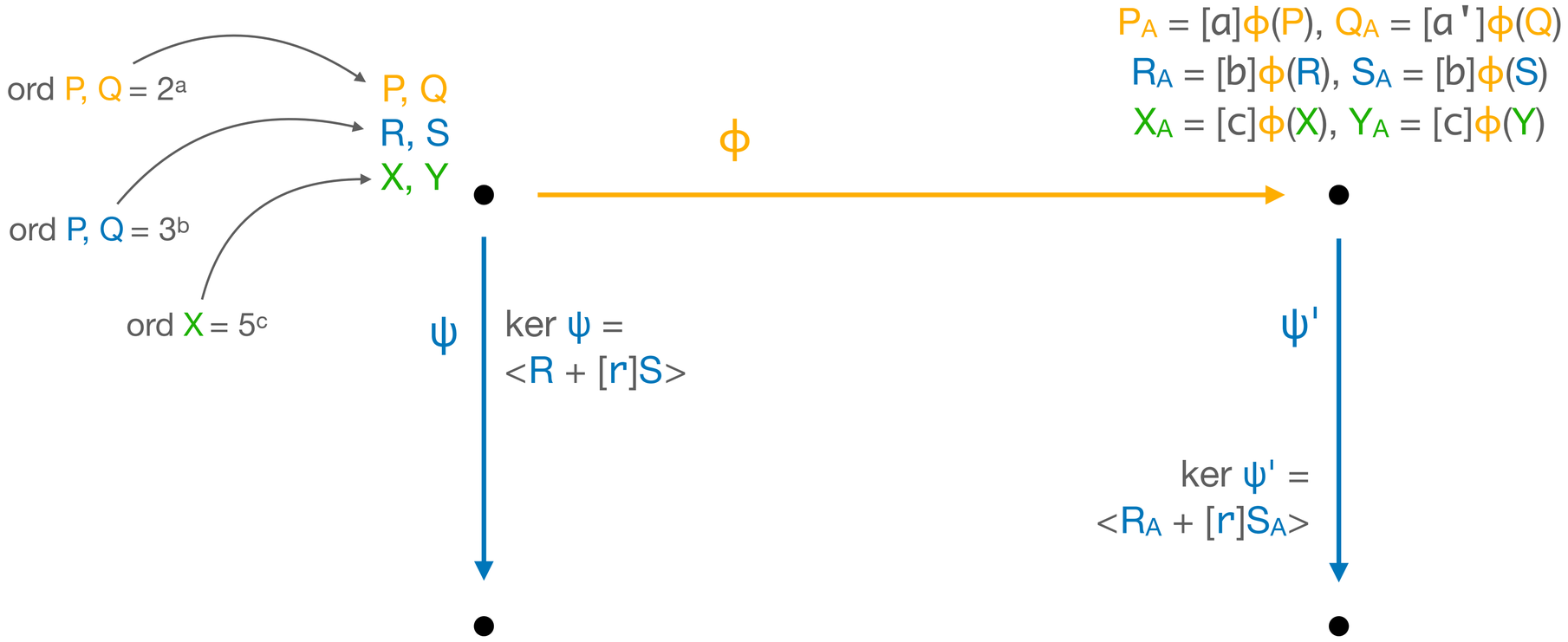
The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)

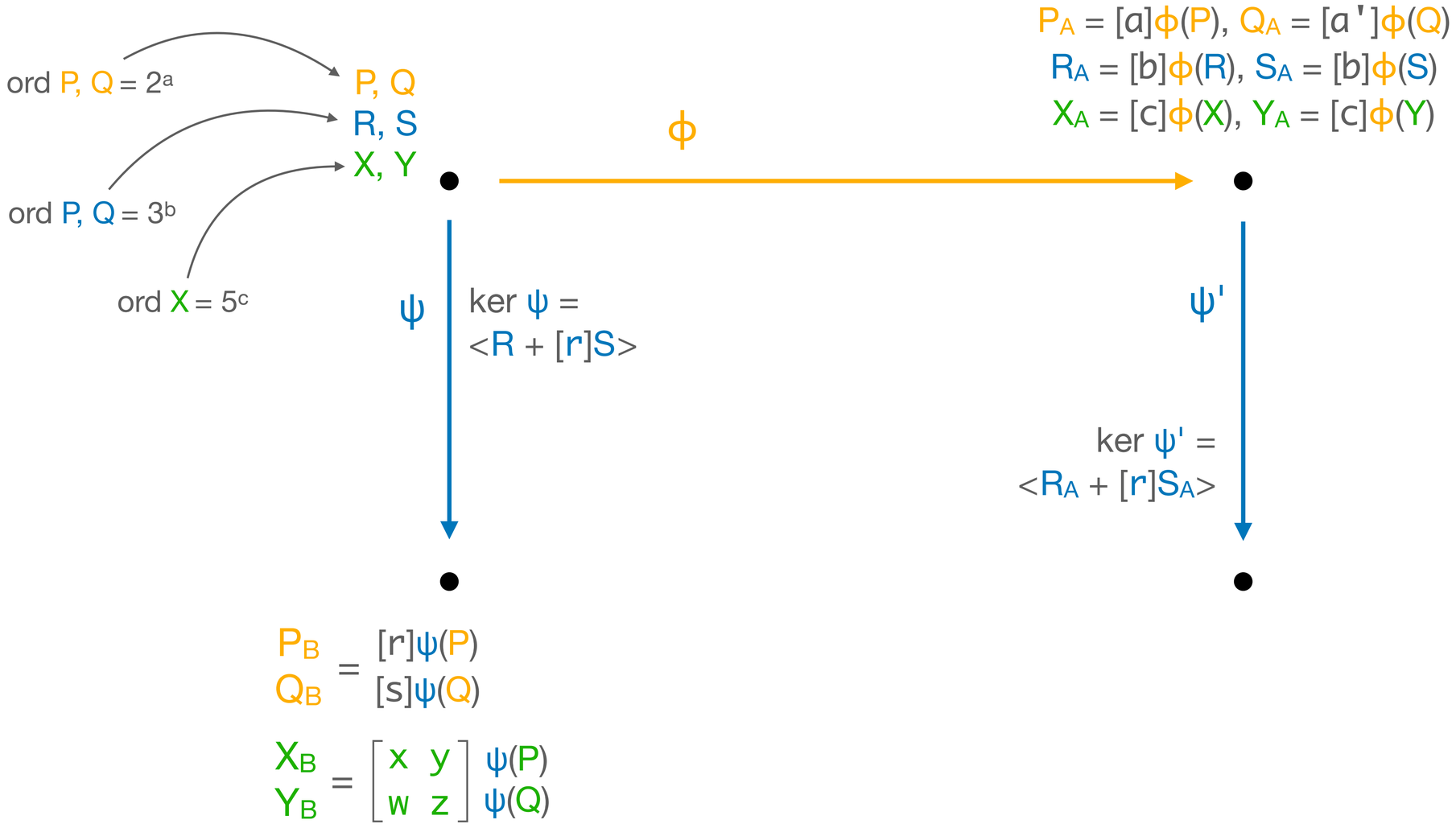
The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
ψ
ker ψ =
<R + [r]S>
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)

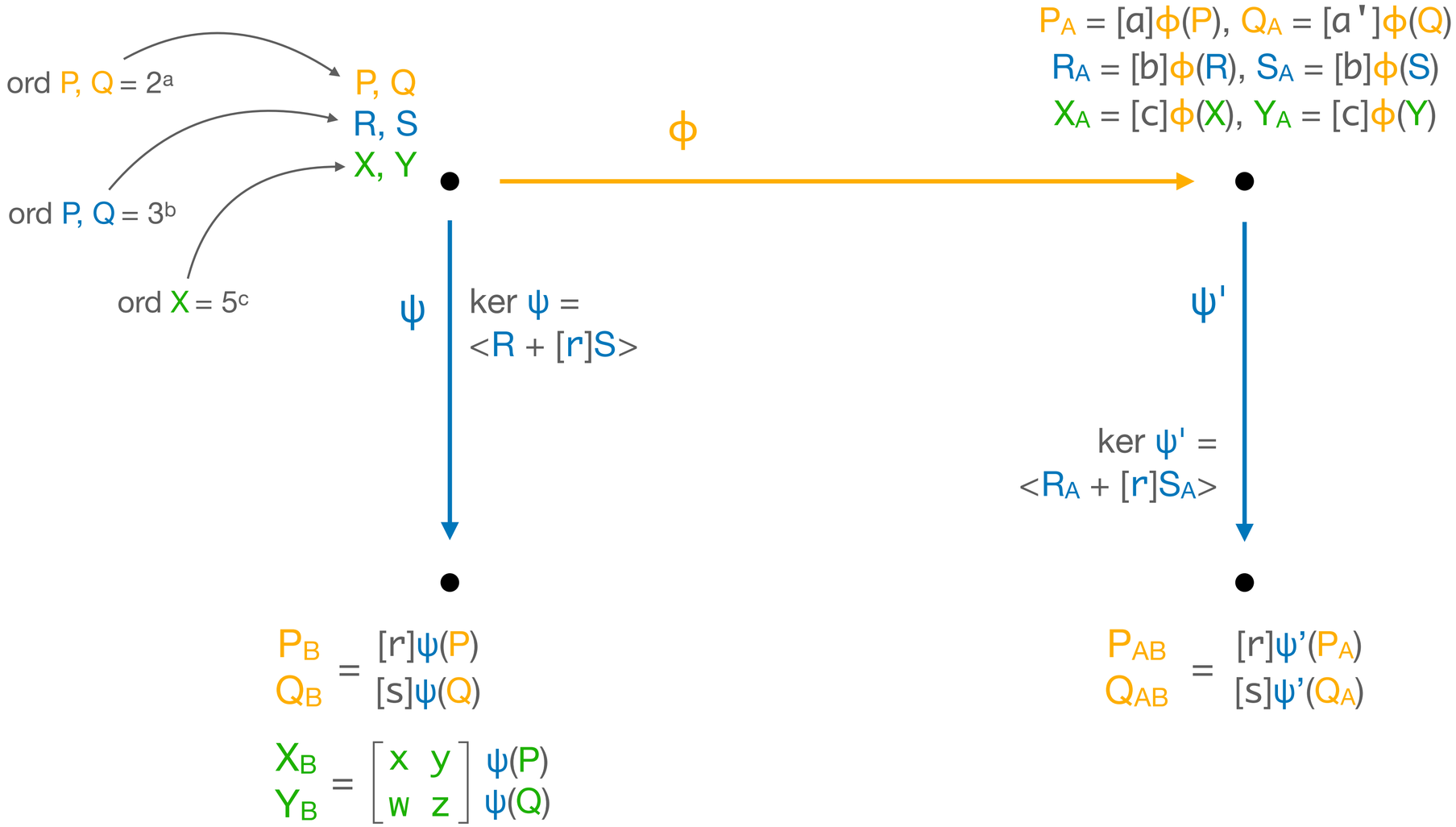
The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)
ψ
ker ψ =
<R + [r]S>
ψ'
ker ψ' =
<R_A + [r]S_A>

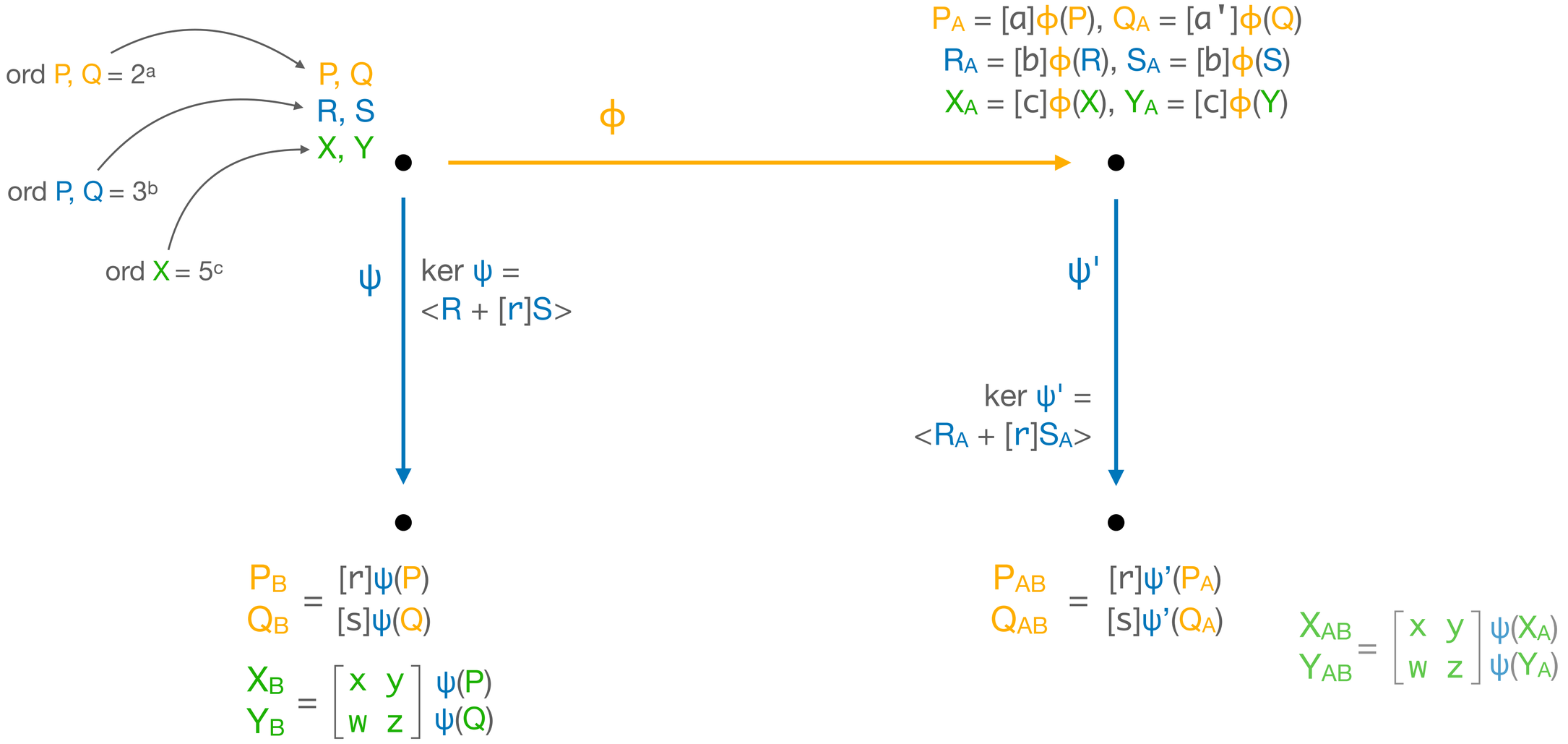
The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)
ψ
ker ψ = <R + [r]S>
ψ'
ker ψ' = <R_A + [r]S_A>
P_B = [r]ψ(P)
Q_B = [s]ψ(Q)
X_B / Y_B = [x y; w z] ψ(P), ψ(Q)

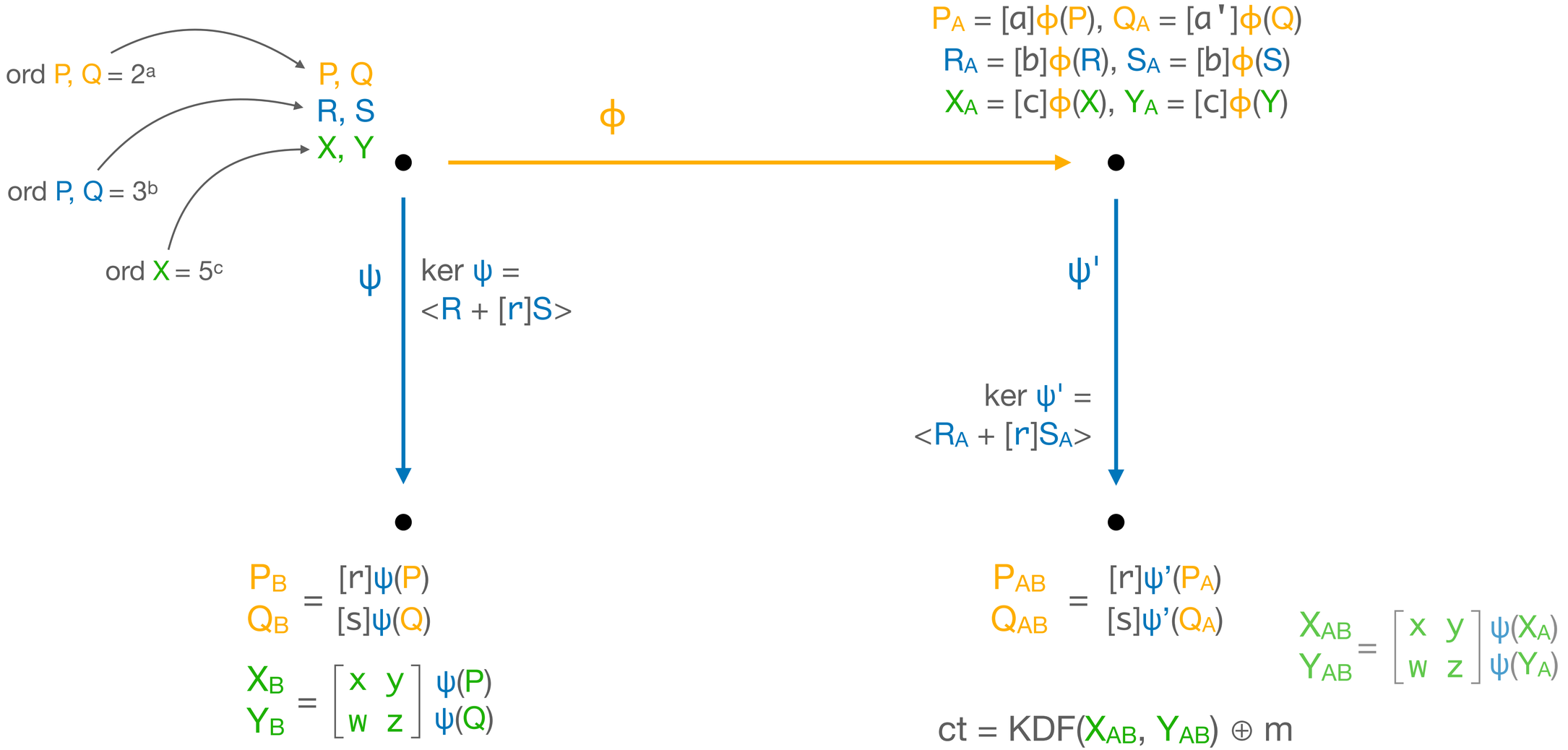
The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
ψ
ker ψ =
<R + [r]S>
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)
ψ'
ker ψ' =
<R_A + [r]S_A>
P_B = [r]ψ(P)
Q_B = [s]ψ(Q)
X_B = [x y] ψ(P)
Y_B = [w z] ψ(Q)
P_AB = [r]ψ'(P_A)
Q_AB = [s]ψ'(Q_A)

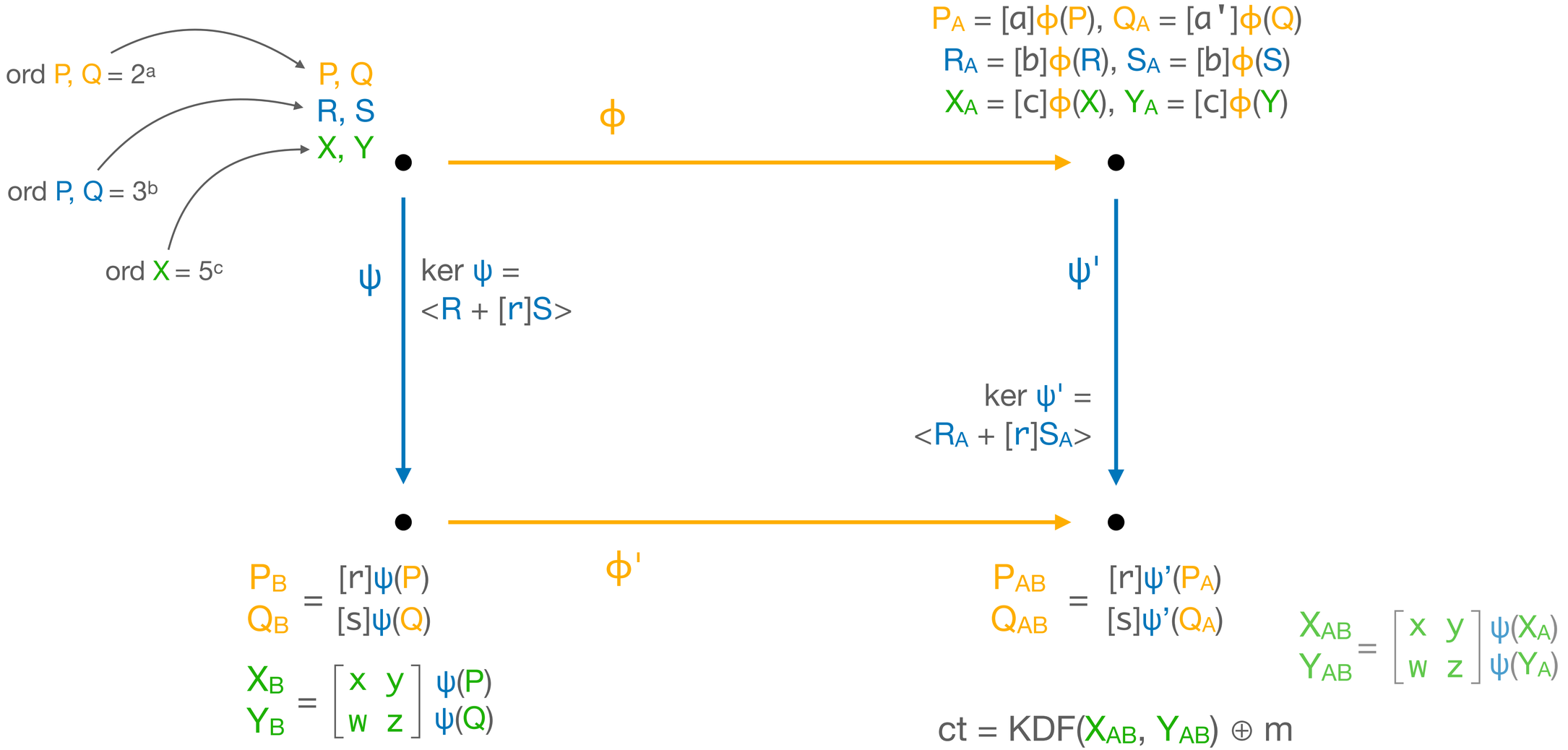
The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)
ψ
ker ψ = <R + [r]S>
ψ'
ker ψ' = <R_A + [r]S_A>
P_B = [r]ψ(P)
Q_B = [s]ψ(Q)
X_B = [x y; w z] ψ(P)
Y_B = [x y; w z] ψ(Q)
P_AB = [r]ψ'(P_A)
Q_AB = [s]ψ'(Q_A)
X_AB = [x y; w z] ψ(X_A)
Y_AB = [x y; w z] ψ(Y_A)

The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
ψ
ker ψ = <R + [r]S>
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)
ψ'
ker ψ' = <R_A + [r]S_A>
P_B = [r]ψ(P)
Q_B = [s]ψ(Q)
X_B, Y_B = [x y; w z] ψ(P), ψ(Q)
P_AB = [r]ψ'(P_A)
Q_AB = [s]ψ'(Q_A)
X_AB, Y_AB = [x y; w z] ψ(X_A), ψ(Y_A)
ct = KDF(X_AB, Y_AB) ⊕ m

The POKE PKE


ord P, Q = 2^a
ord P, Q = 3^b
ord X = 5^c
P, Q
R, S
X, Y
ϕ
P_A = [a]ϕ(P), Q_A = [a']ϕ(Q)
R_A = [b]ϕ(R), S_A = [b]ϕ(S)
X_A = [c]ϕ(X), Y_A = [c]ϕ(Y)
ψ
ker ψ = <R + [r]S>
ψ'
ker ψ' = <R_A + [r]S_A>
ϕ'
P_B = [r]ψ(P)
Q_B = [s]ψ(Q)
X_B, Y_B = [x y; w z] ψ(P), ψ(Q)
P_AB = [r]ψ'(P_A)
Q_AB = [s]ψ'(Q_A)
X_AB, Y_AB = [x y; w z] ψ(X_A), ψ(Y_A)
ct = KDF(X_AB, Y_AB) ⊕ m

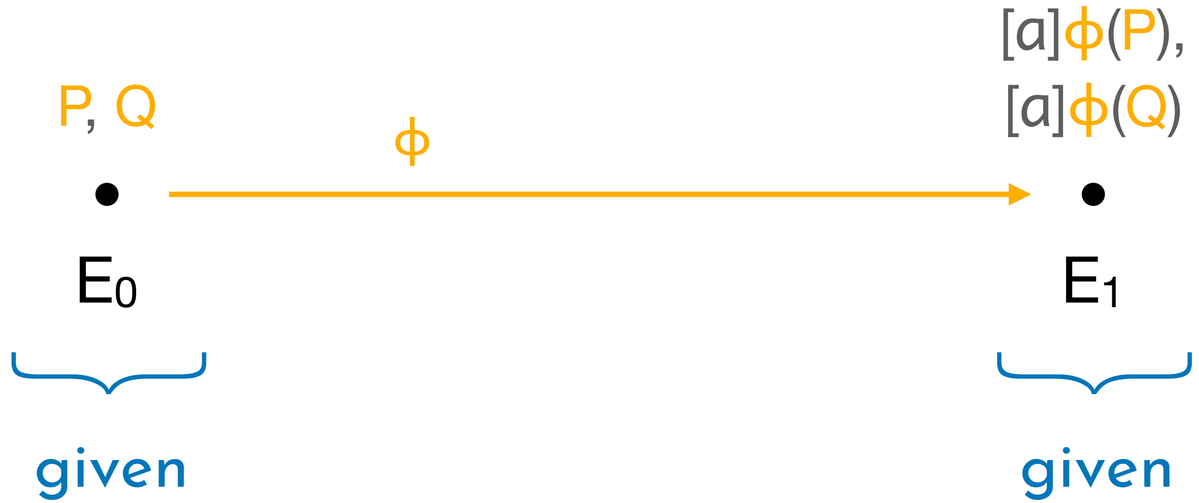
Security

Formally: security depends on CDH-type assumption

Security

Formally: security depends on CDH-type assumption

Unknown Degree Isogeny Problem:



Results

Parameters

- 2^{λ} : order of torsion points for HD repr (P, Q)
- $3^{b} \approx 2^{2\lambda}$: degree of smooth isogenies (R, S)
- $5^{c} \approx 2^{\lambda/3}$: order of validation points (X, Y)

Results

Parameters

- 2^{λ} : order of torsion points for HD repr (P, Q)
- $3^{b} \approx 2^{2\lambda}$: degree of smooth isogenies (R, S)
- $5^{c} \approx 2^{\lambda/3}$: order of validation points (X, Y)

$$p = 2^{a}\, 3^{b}\, 5^{c}\, f - 1 \quad \approx 2^{3.3\lambda}$$

Results

Parameters

- 2^λ : order of torsion points for HD repr (P, Q)
- $3^b \approx 2^{2\lambda}$: degree of smooth isogenies (R, S)
- $5^c \approx 2^{\lambda/3}$: order of validation points (X, Y)

$$p = 2^a\, 3^b\, 5^c\, f - 1 \quad \approx 2^{3.3\lambda}$$

Sizes

- Public key: 6 log p (≈324 bytes)
- Ciphertext: 12 log p (≈648 bytes)

- Both (comp.): 5 log p (≈270 bytes)

Results

Parameters

- 2^λ : order of torsion points for HD repr (P, Q)
- $3^b \approx 2^{2\lambda}$: degree of smooth isogenies (R, S)
- $5^c \approx 2^{\lambda/3}$: order of validation points (X, Y)

$$p = 2^a\, 3^b\, 5^c\, f - 1 \quad \approx 2^{3.3\lambda}$$

Sizes

- Public key: 6 log p (≈324 bytes)
- Ciphertext: 12 log p (≈648 bytes)

- Both (comp.): 5 log p (≈270 bytes)

Performance

Results

Parameters

- 2^λ : order of torsion points for HD repr (P, Q)
- $3^b \approx 2^{2\lambda}$: degree of smooth isogenies (R, S)
- $5^c \approx 2^{\lambda/3}$: order of validation points (X, Y)

$$p = 2^a\, 3^b\, 5^c\, f - 1 \quad \approx 2^{3.3\lambda}$$

Sizes

- Public key: 6 log p (≈324 bytes)
- Ciphertext: 12 log p (≈648 bytes)

- Both (comp.): 5 log p (≈270 bytes)

Performance

POKÉ is the fastest isogeny-based PKE

Conclusion

1 New PKE based on the **public/ private HD representations**

Conclusion

1 New PKE based on the **public/ private HD representations**

2 Compact and very efficient: POKE is the **fastest isogeny-based encryption** protocol

Conclusion

1 New PKE based on the **public/ private HD representations**

2 Compact and very efficient: POKE is the **fastest isogeny-based encryption** protocol

3 POKE has an **SIDH-like structure**: can we use it to build advanced primitives?

Conclusion

1 New PKE based on the **public/ private HD representations**

2 Compact and very efficient: POKE is the **fastest isogeny-based encryption** protocol

3 POKE has an **SIDH-like structure**: can we use it to build advanced primitives?

Paper

https://ia.cr/2024/624

POC source code

https://github.com/andreavico/POKE-PKE