

the Algebraic Isogeny Model

marius aardal, andrea basso, doreen riepel

EUROCRYPT 2026

may 12, 2026

many isogeny-based
protocols
rely on **new assumptions**

many isogeny-based
protocols
rely on **new assumptions**

these assumptions
lack structure
for meaningful reductions
(especially in unoriented setting)

many isogeny-based
protocols
rely on **new assumptions**

these assumptions
lack structure
for meaningful reductions
(especially in unoriented setting)

this means new protocols
often rely on
ad-hoc assumptions

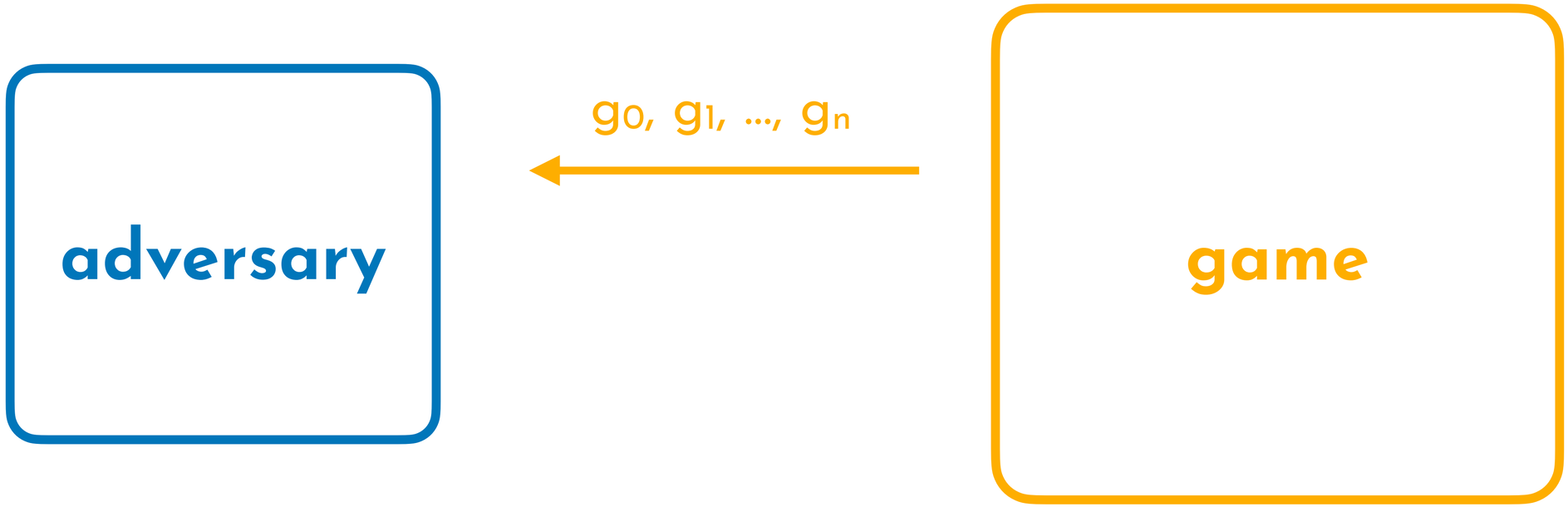
the Algebraic Group Model (AGM)





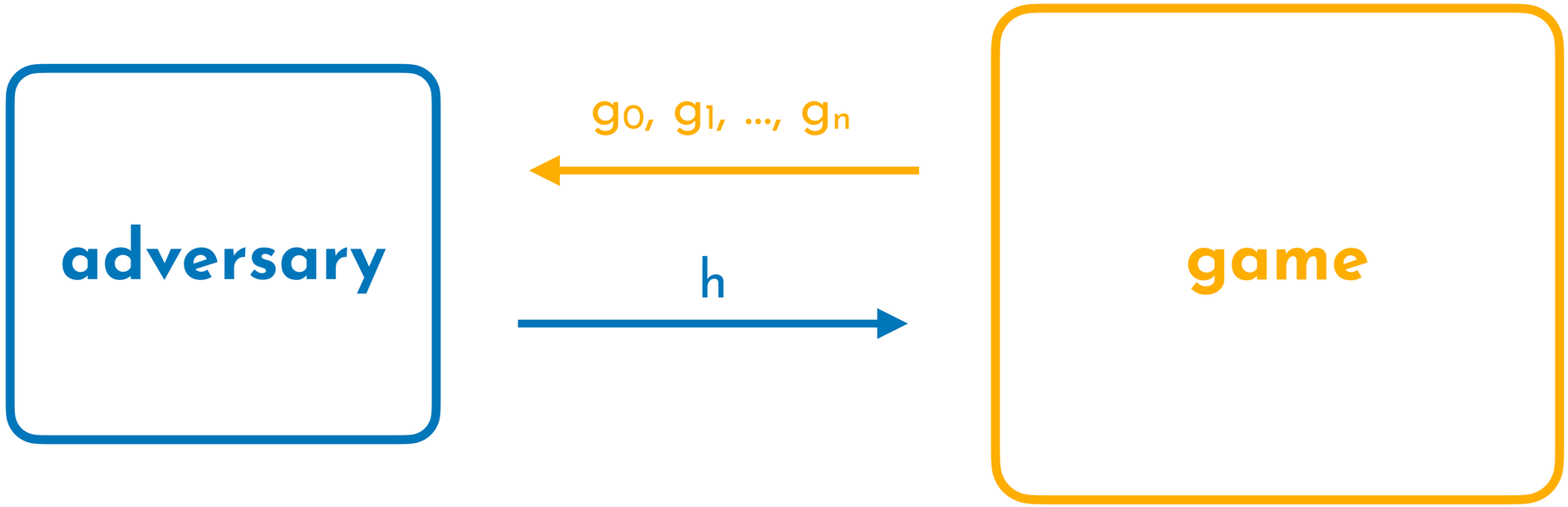
Georg Fuchsbauer, Eike Kiltz, and Julian Loss, The Algebraic Group Model and its Applications, https://ia.cr/2017/620

the Algebraic Group Model (AGM)



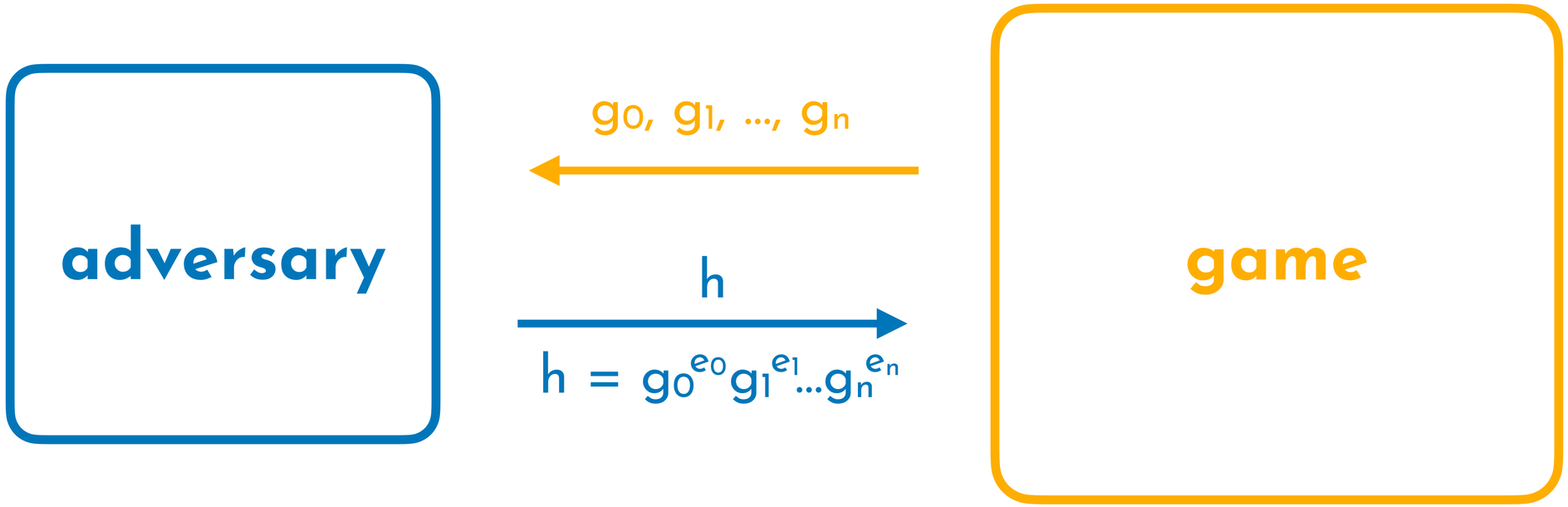
Georg Fuchsbauer, Eike Kiltz, and Julian Loss, The Algebraic Group Model and its Applications, https://ia.cr/2017/620

the Algebraic Group Model (AGM)



Georg Fuchsbauer, Eike Kiltz, and Julian Loss, The Algebraic Group Model and its Applications, https://ia.cr/2017/620

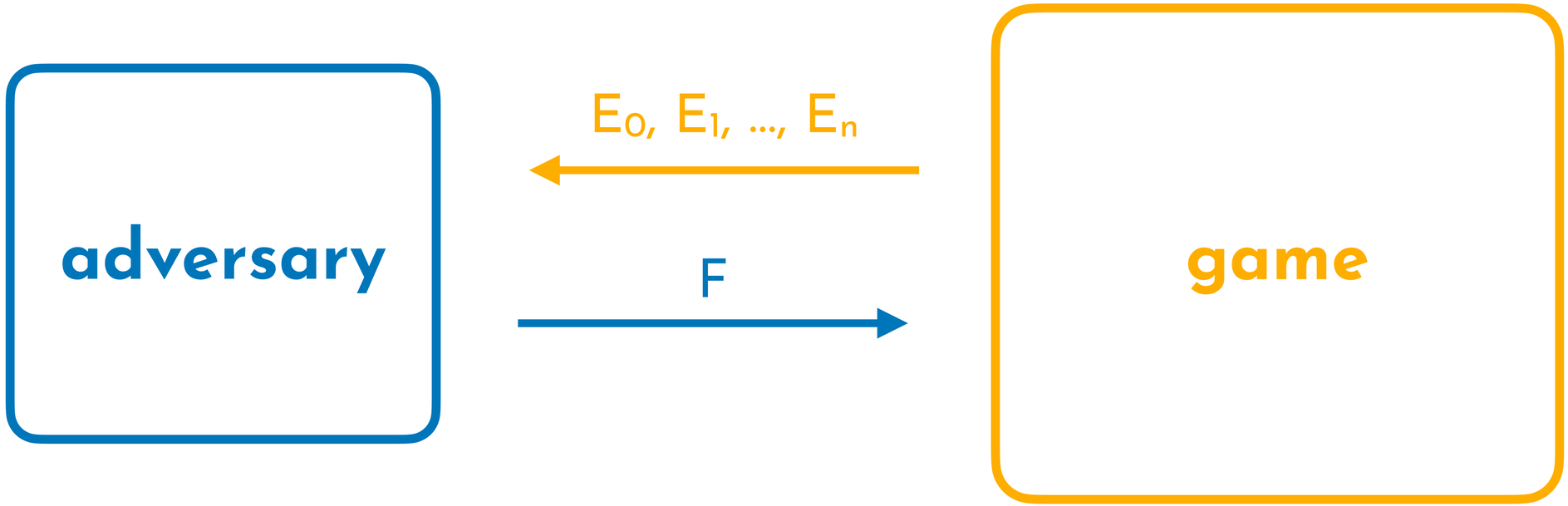
the Algebraic Group Model (AGM)



Georg Fuchsbauer, Eike Kiltz, and Julian Loss, The Algebraic Group Model and its Applications, https://ia.cr/2017/620

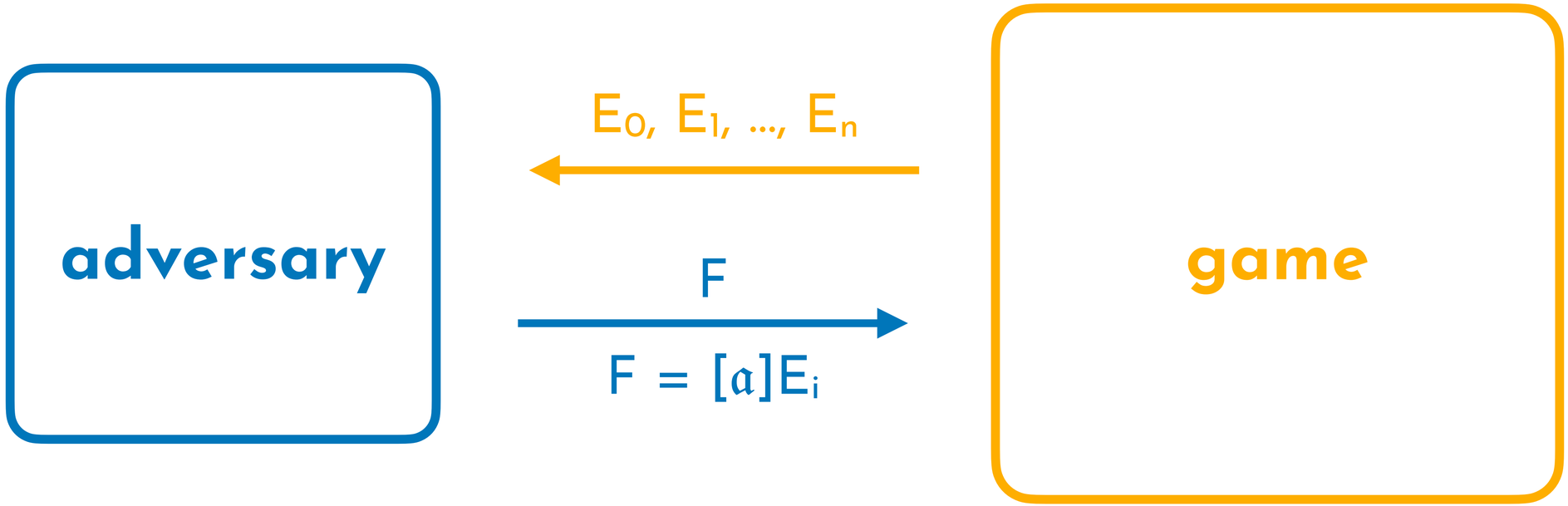
can we do the same with isogenies?

the Algebraic Group Action Model (AGAM)



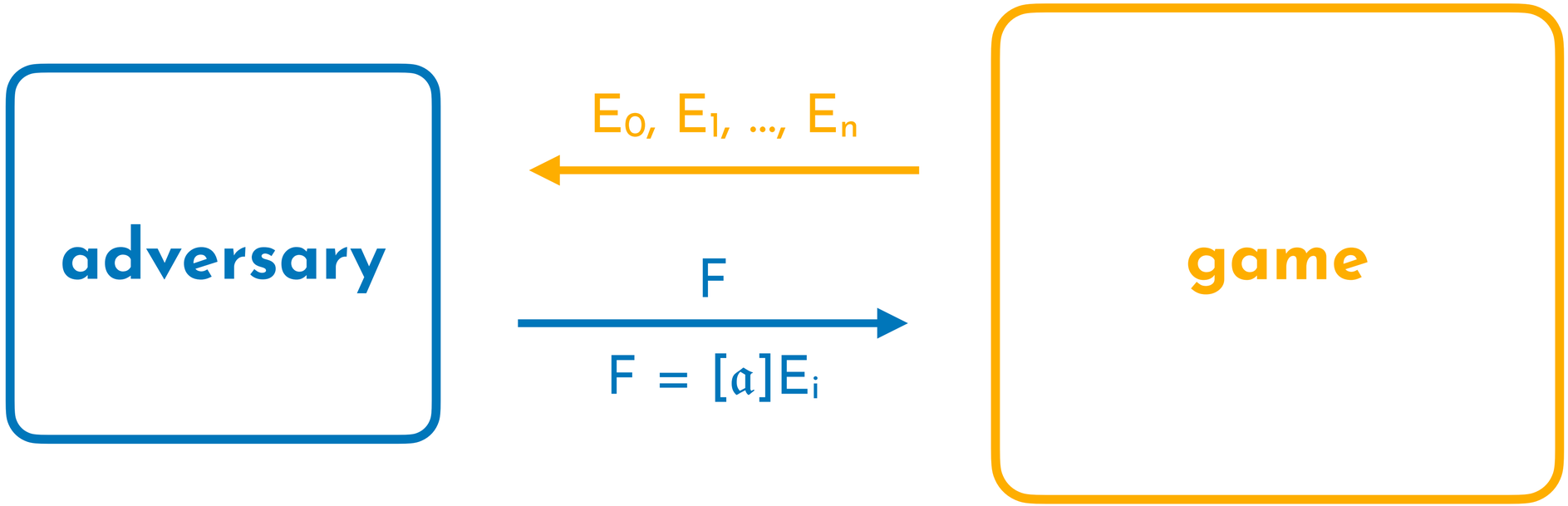
J. Duman, D. Hartmann, E. Kiltz, S. Kunzweiler, J. Lehmann, D. Riepel, Generic Models for Group Actions, https://ia.cr/2023/186
E. Orsini, R. Zanotto, Simple Two-Round OT in the Explicit Isogeny Model, https://eprint.iacr.org/2023/269

the Algebraic Group Action Model (AGAM)



J. Duman, D. Hartmann, E. Kiltz, S. Kunzweiler, J. Lehmann, D. Riepel, Generic Models for Group Actions, https://ia.cr/2023/186
E. Orsini, R. Zanotto, Simple Two-Round OT in the Explicit Isogeny Model, https://eprint.iacr.org/2023/269

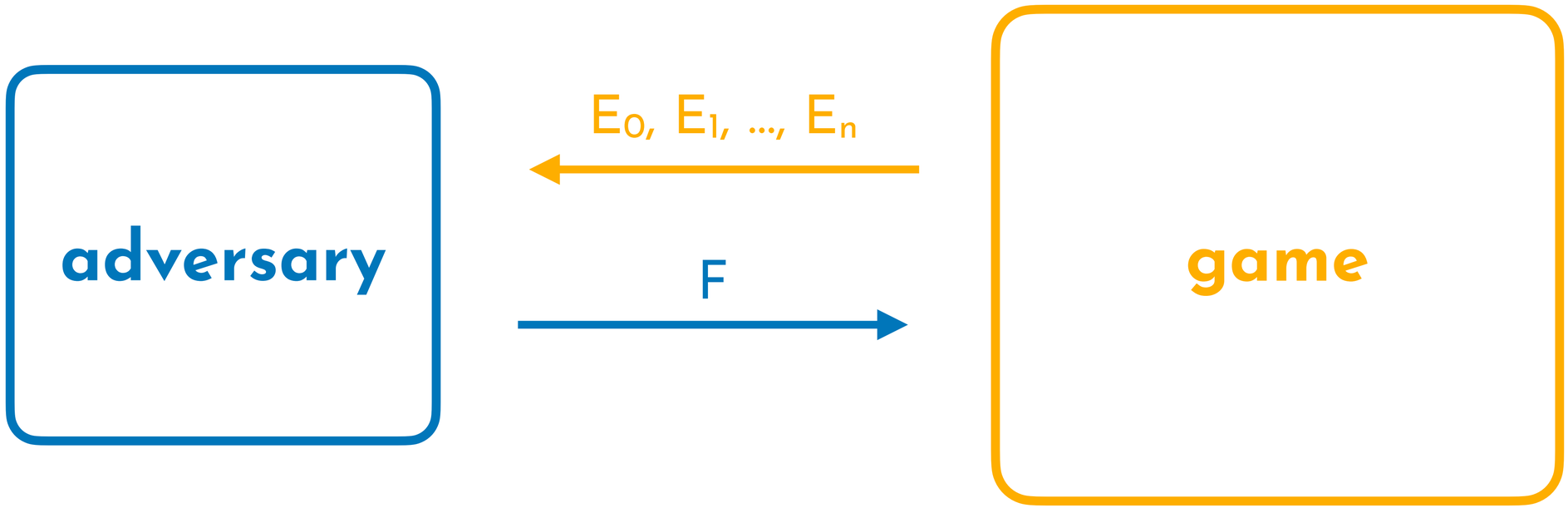
the Algebraic Group Action Model (AGAM)



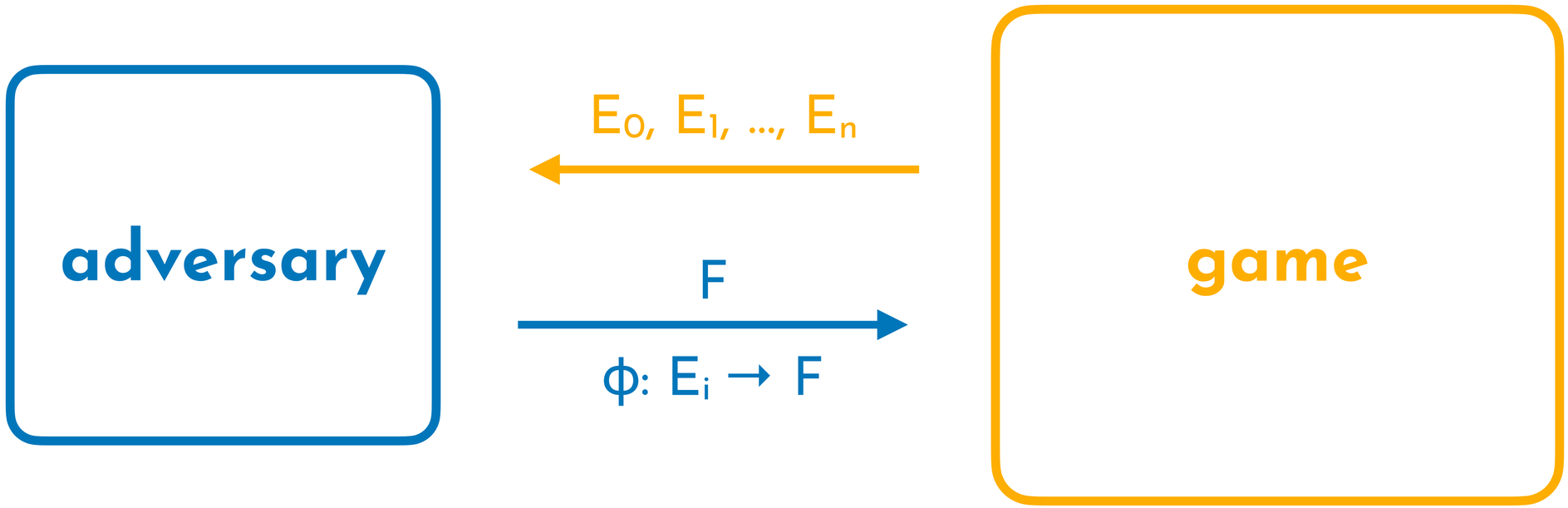
only works with protocols based on (black-box) group actions

J. Duman, D. Hartmann, E. Kiltz, S. Kunzweiler, J. Lehmann, D. Riepel, Generic Models for Group Actions, https://ia.cr/2023/186
E. Orsini, R. Zanotto, Simple Two-Round OT in the Explicit Isogeny Model, https://eprint.iacr.org/2023/269

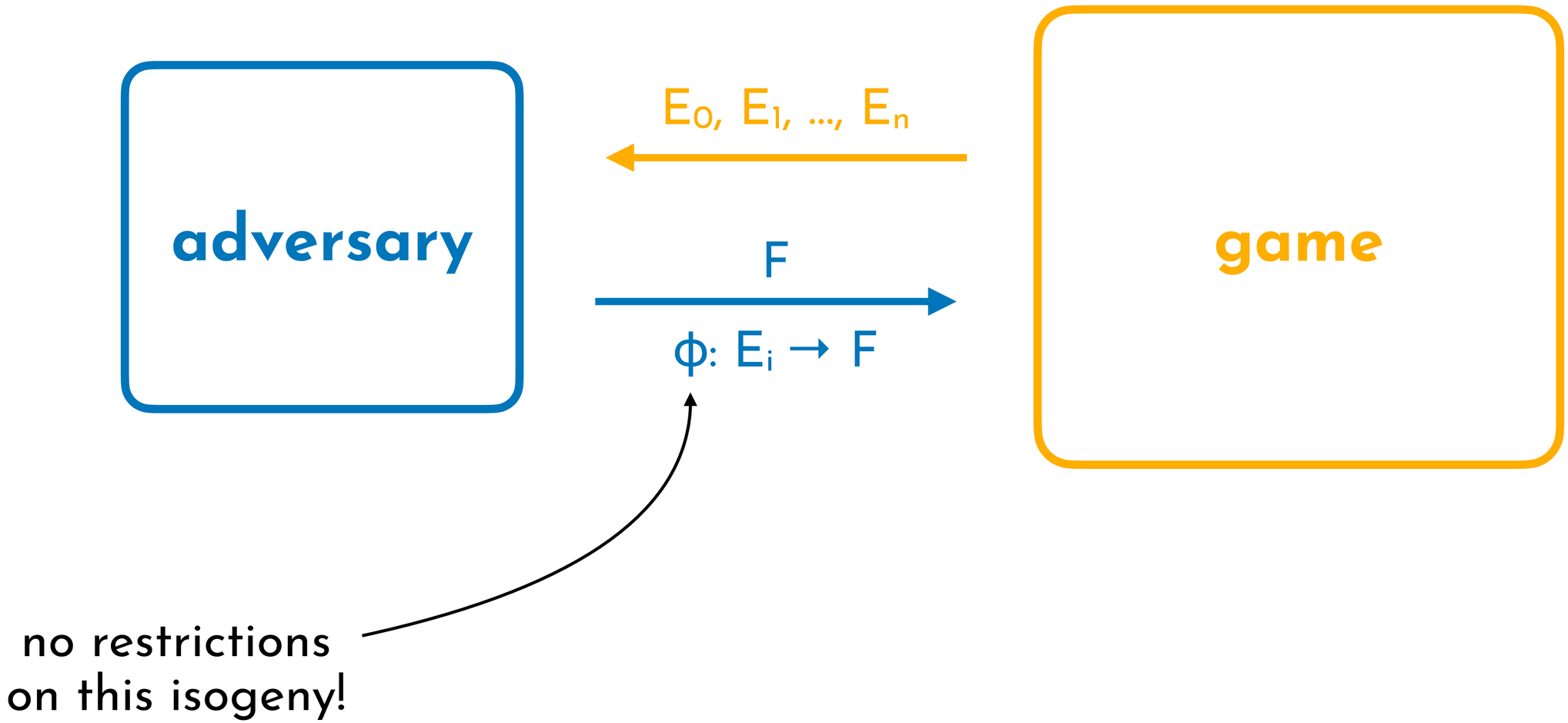
the Algebraic Isogeny Model (AIM)



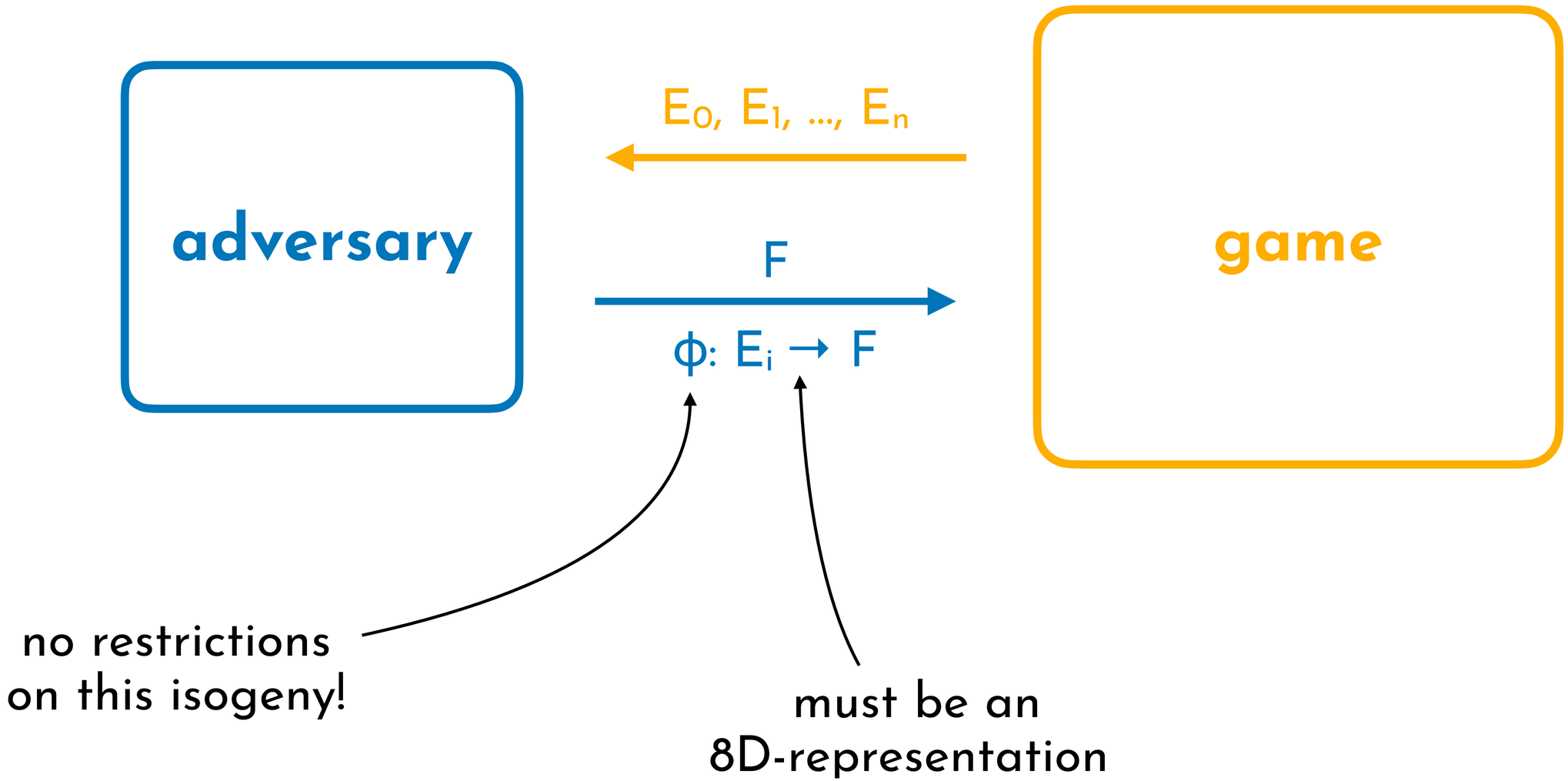
the Algebraic Isogeny Model (AIM)



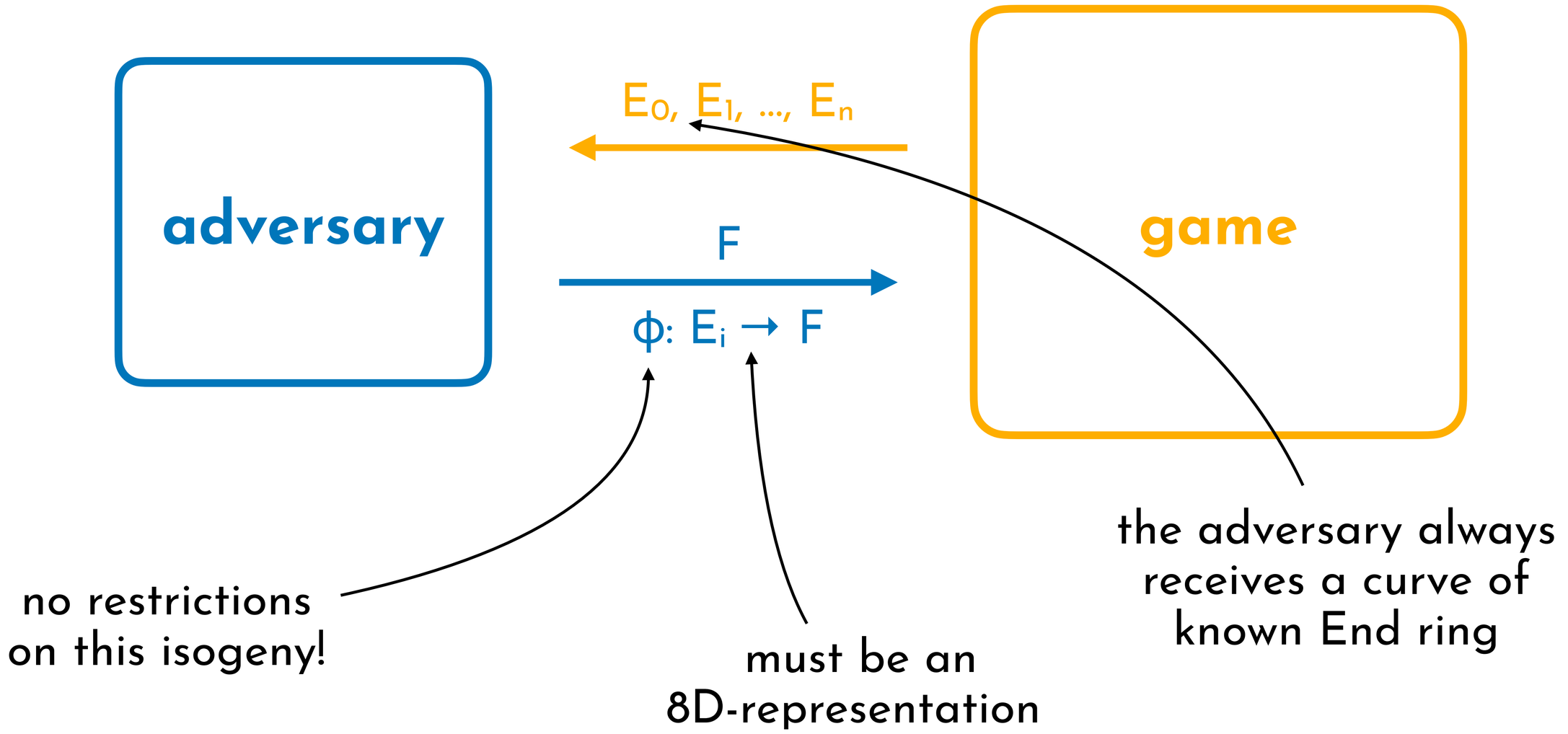
the Algebraic Isogeny Model (AIM)



the Algebraic Isogeny Model (AIM)



the Algebraic Isogeny Model (AIM)



results (in the AIM)

results (in the AIM)

all results in the AGAM (with twist) also hold in the AIM

results (in the AIM)

1 all results in the AGAM (with twist) also hold in the AIM

2 SQIsign is EUF-CMA secure in the QROM

results (in the AIM)

1 all results in the AGAM (with twist) also hold in the AIM

2 SQIsign is EUF–CMA secure in the QROM

3 CDH is equivalent to DLOG, for all isogeny formulations (CSIDH, M-SIDH, MD-SIDH, binSIDH, terSIDH, etc.)

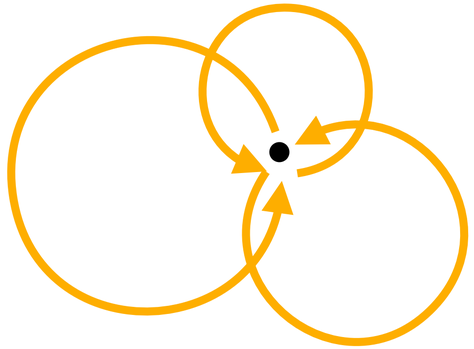
results (in the AIM)

1 all results in the AGAM (with twist) also hold in the AIM

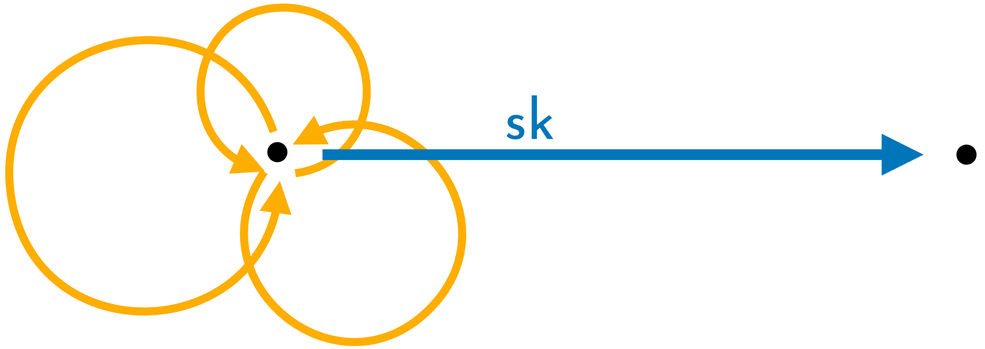
2 SQIsign is EUF–CMA secure in the QROM

3 CDH is equivalent to DLOG, for all isogeny formulations (CSIDH, M-SIDH, MD-SIDH, binSIDH, terSIDH, etc.)

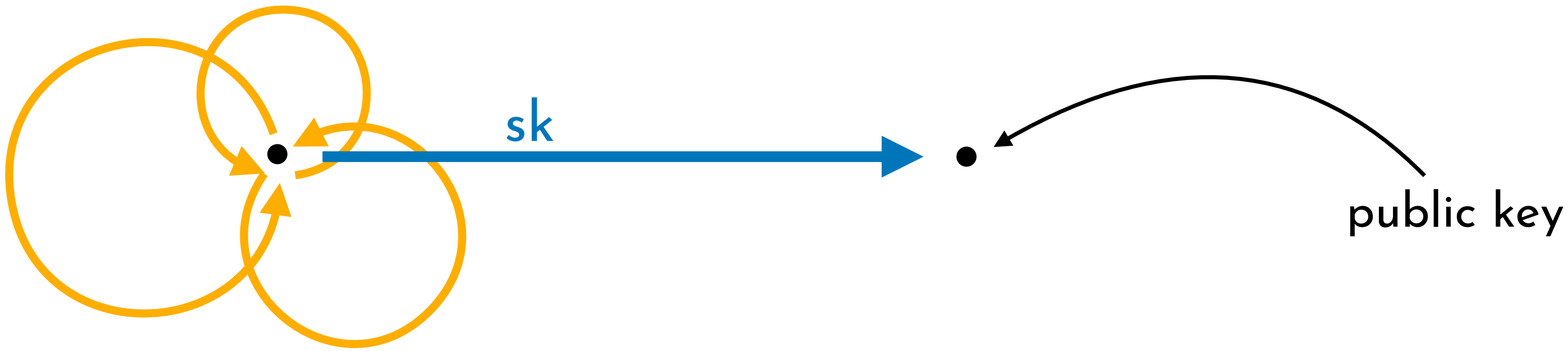
SQIsign



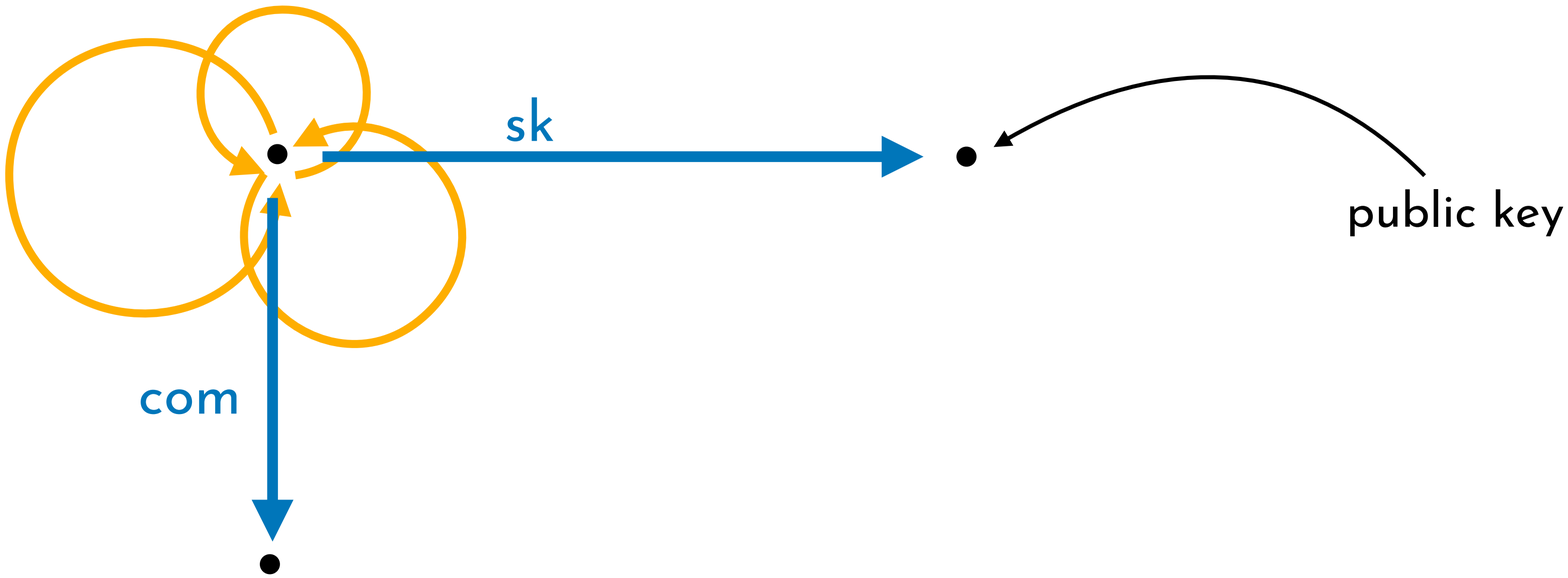
SQIsign



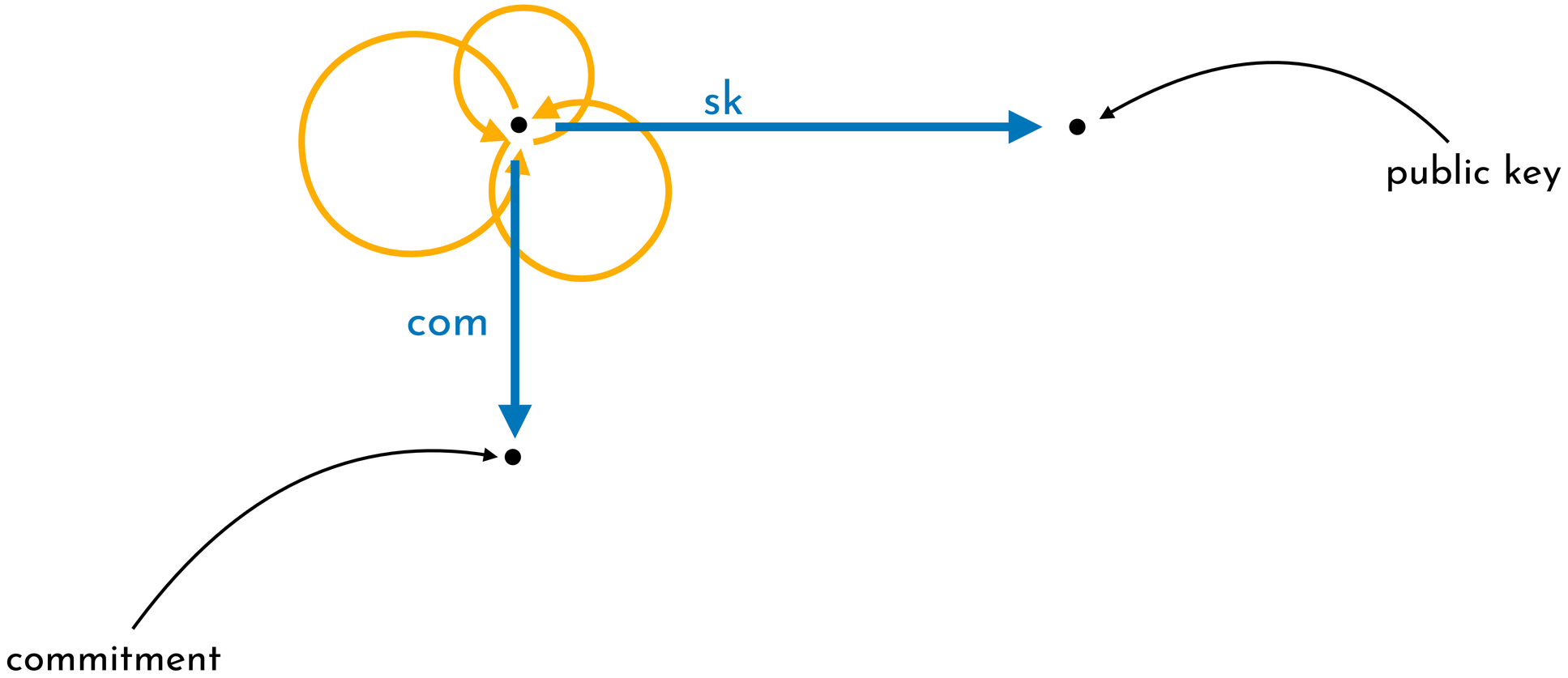
SQIsign



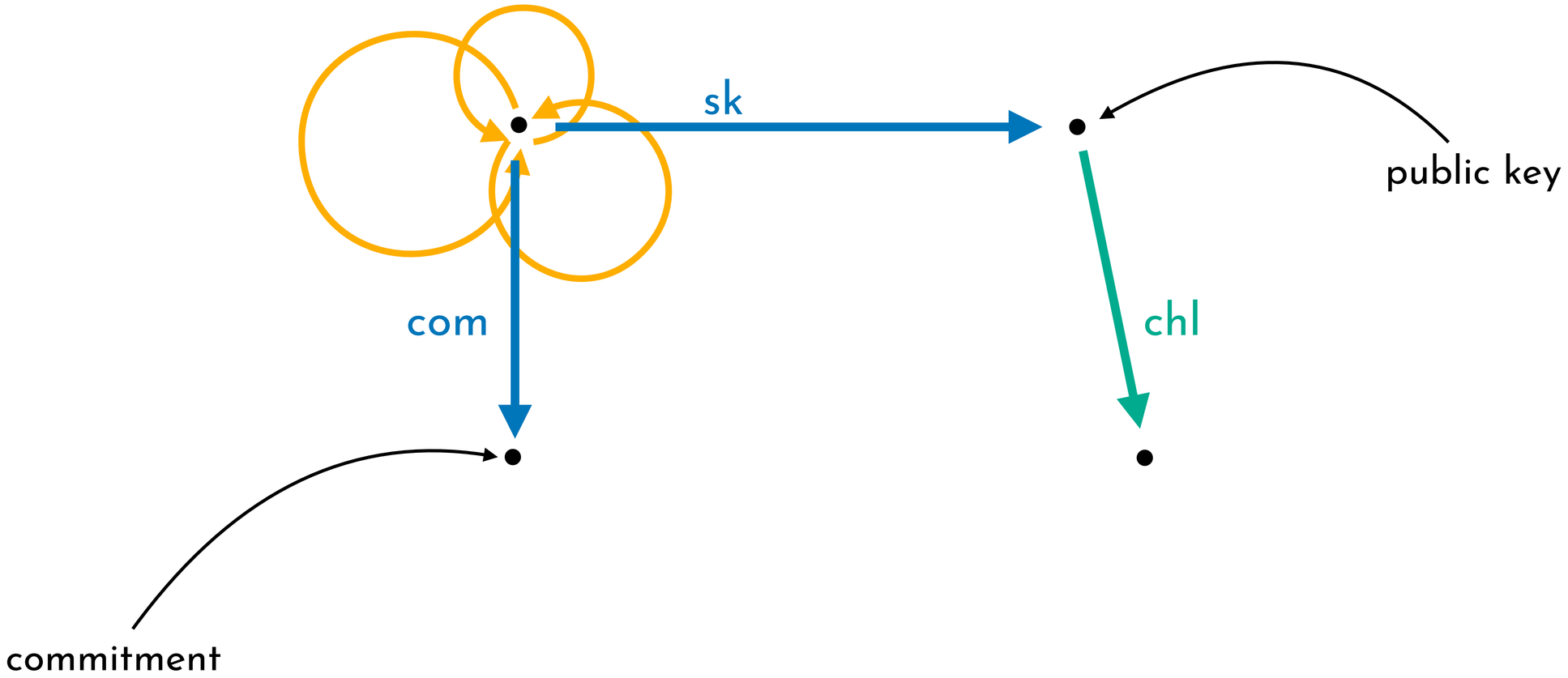
SQIsign



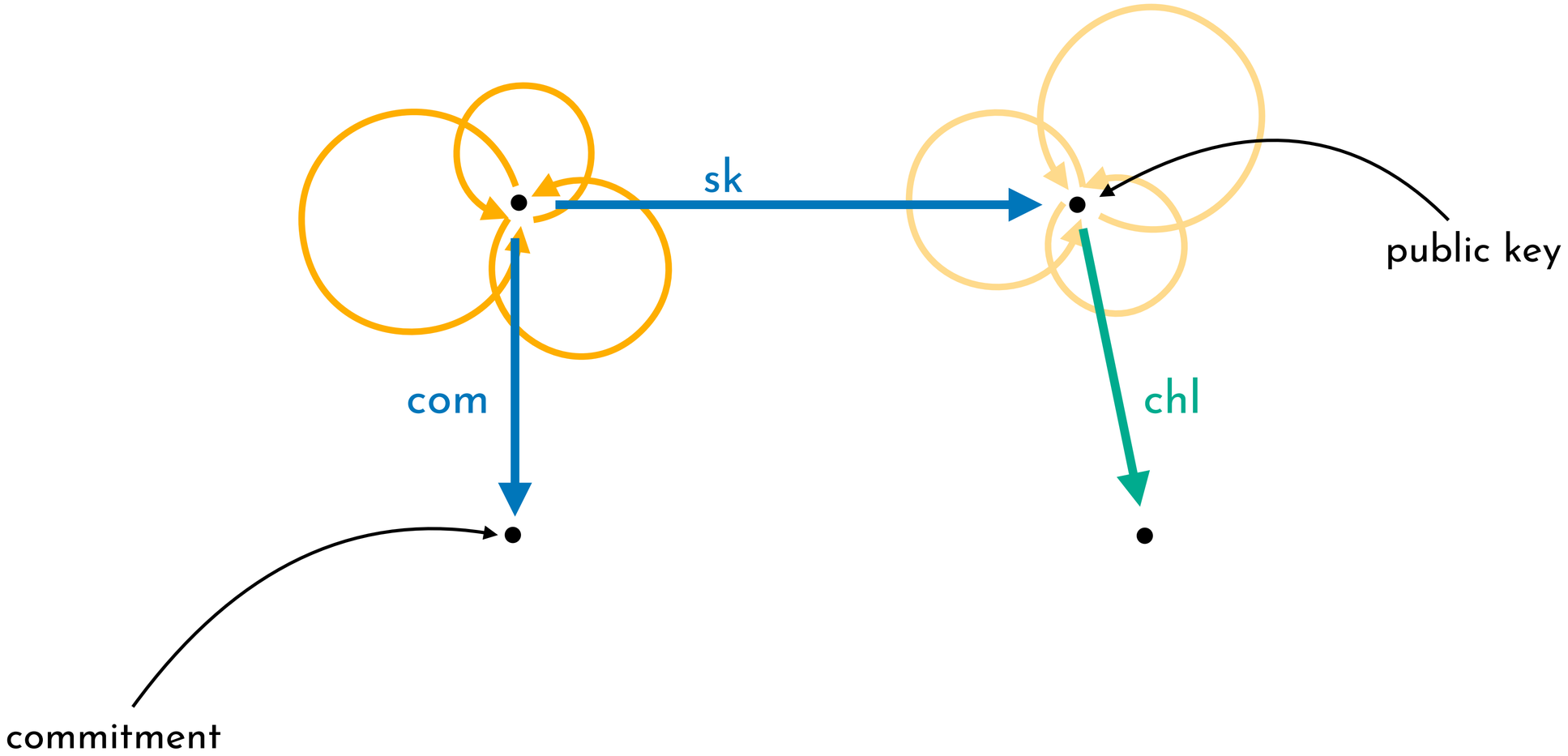
SQIsign



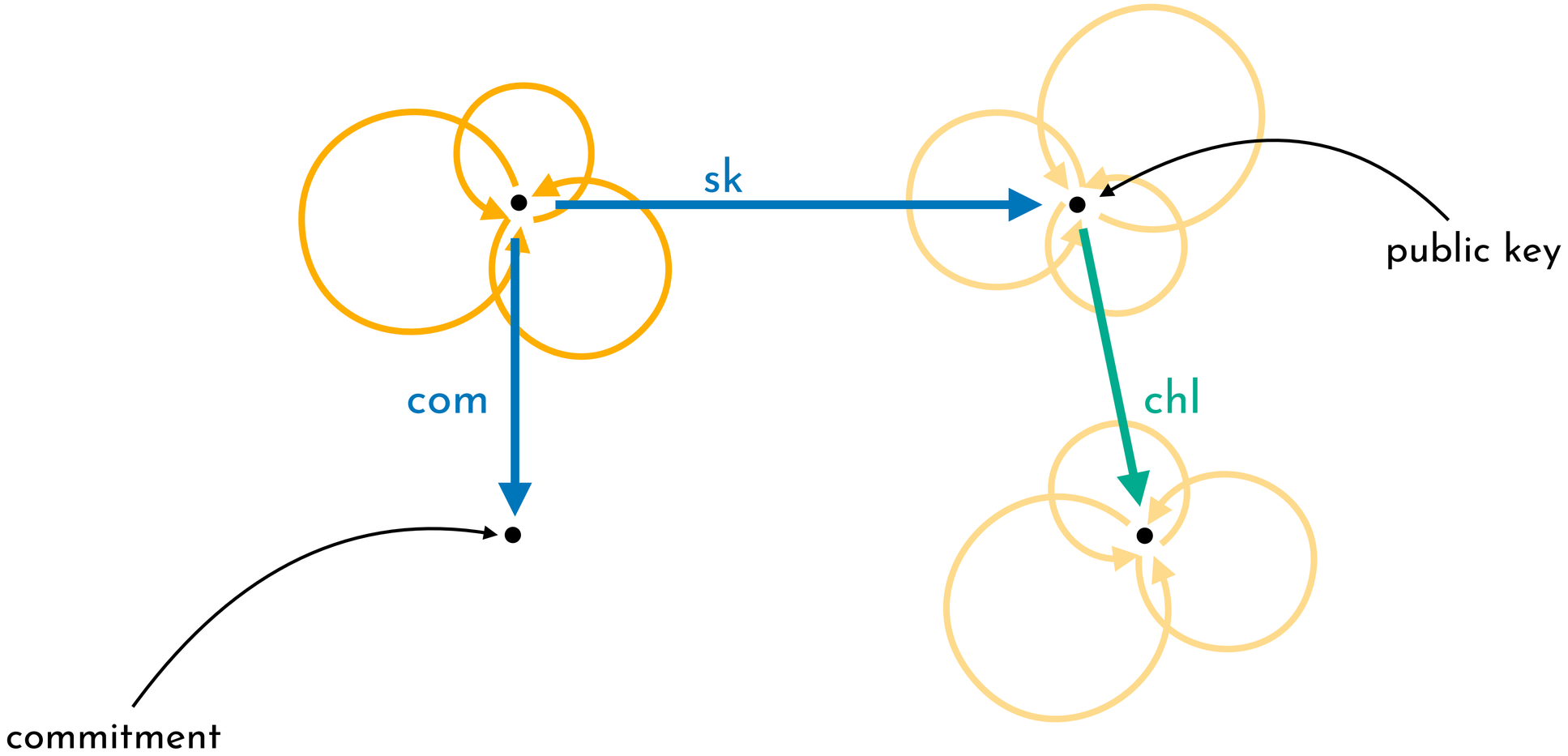
SQIsign



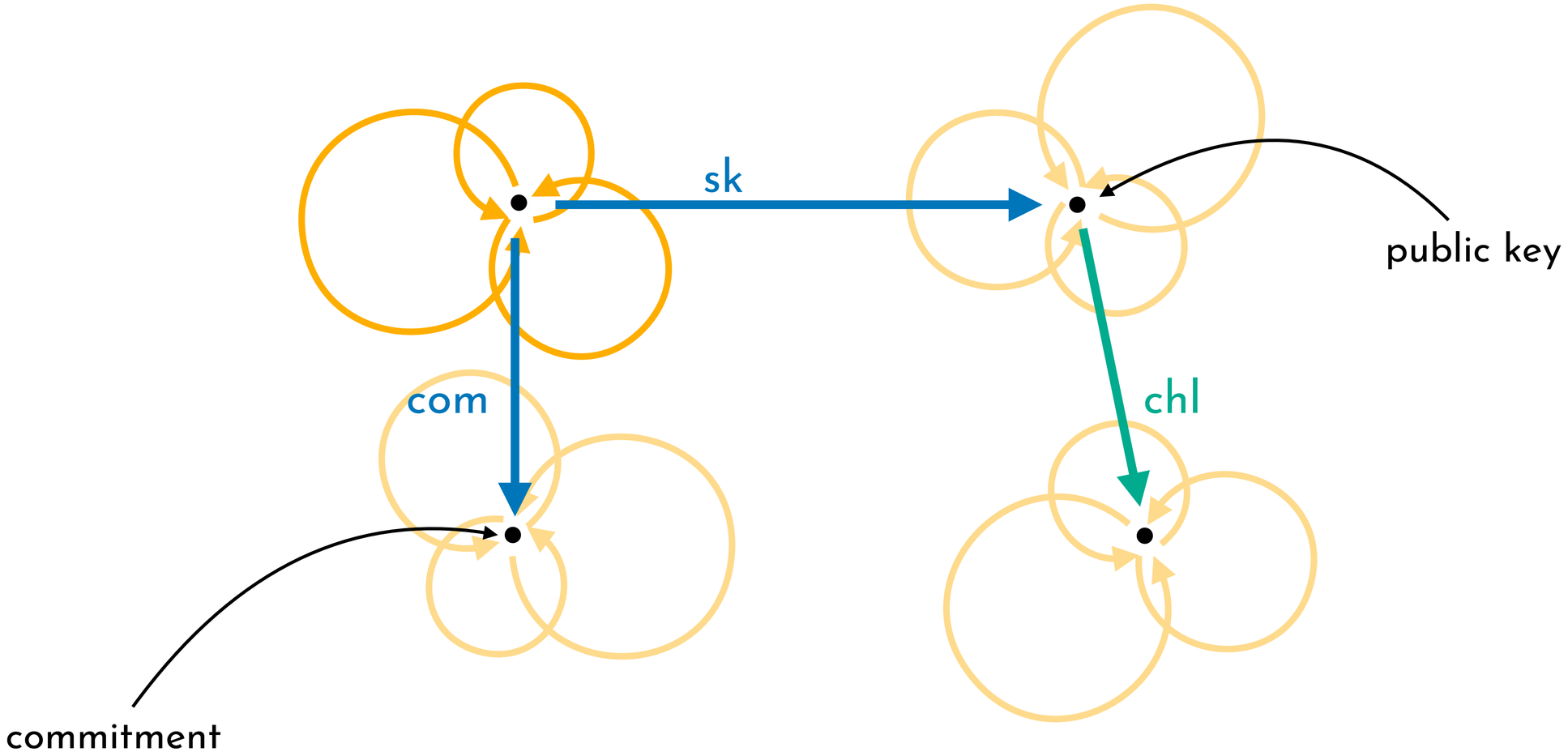
SQIsign



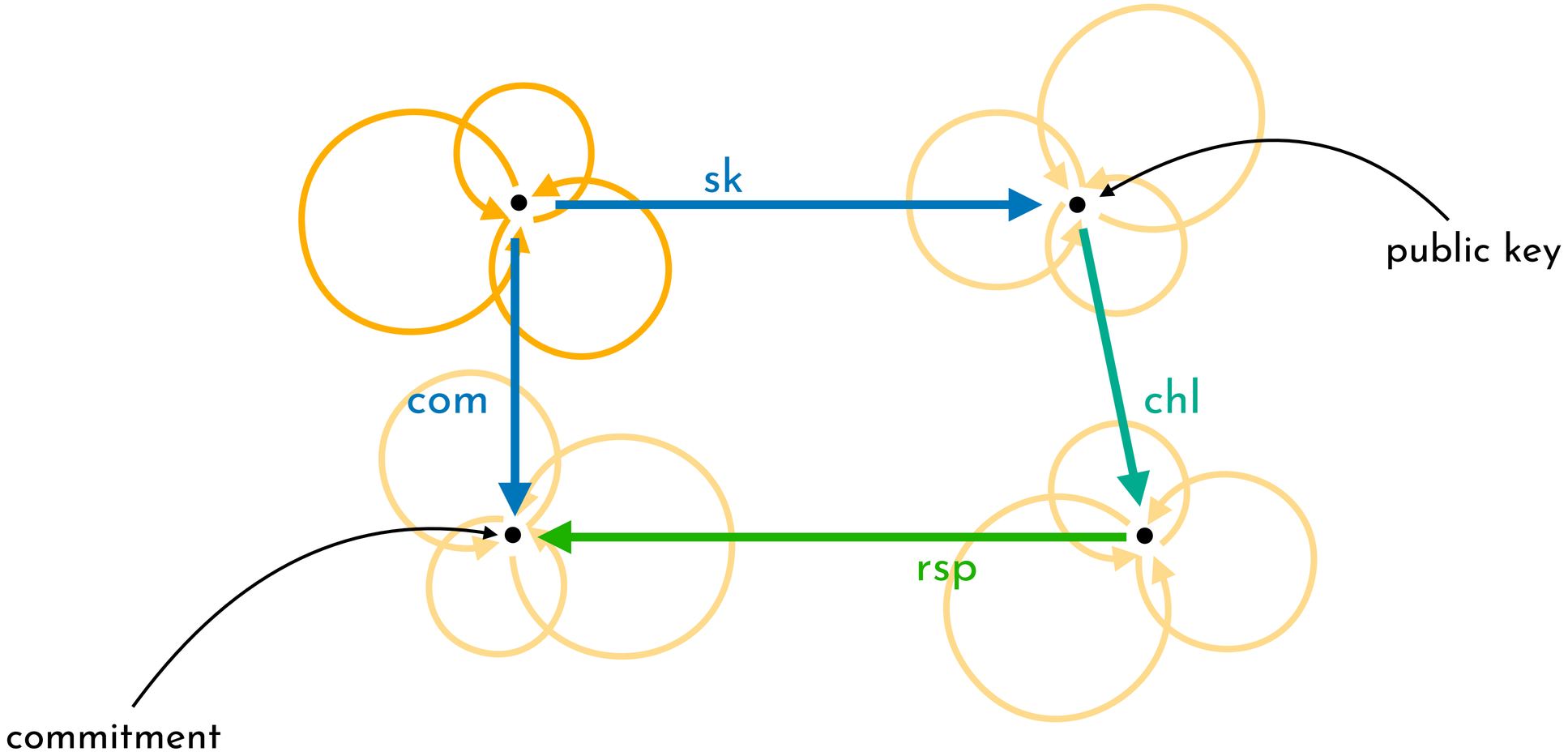
SQIsign



SQIsign

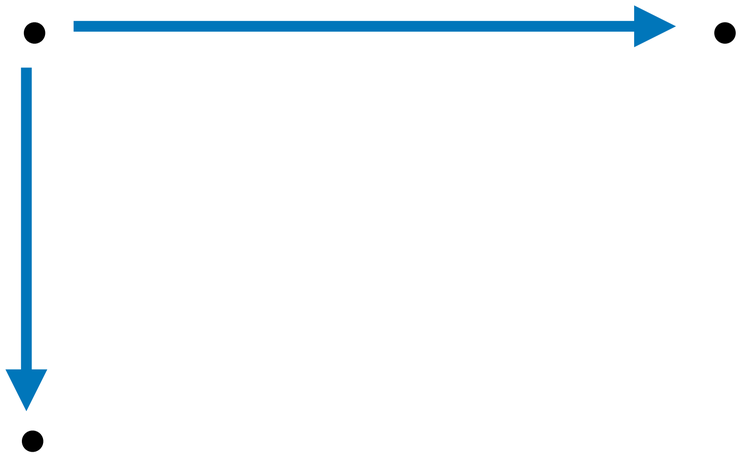


SQIsign

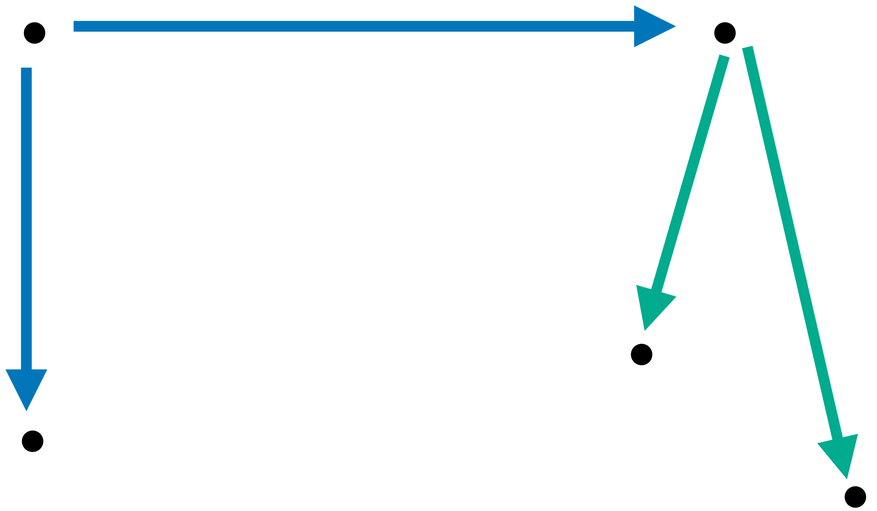


two-special soundness

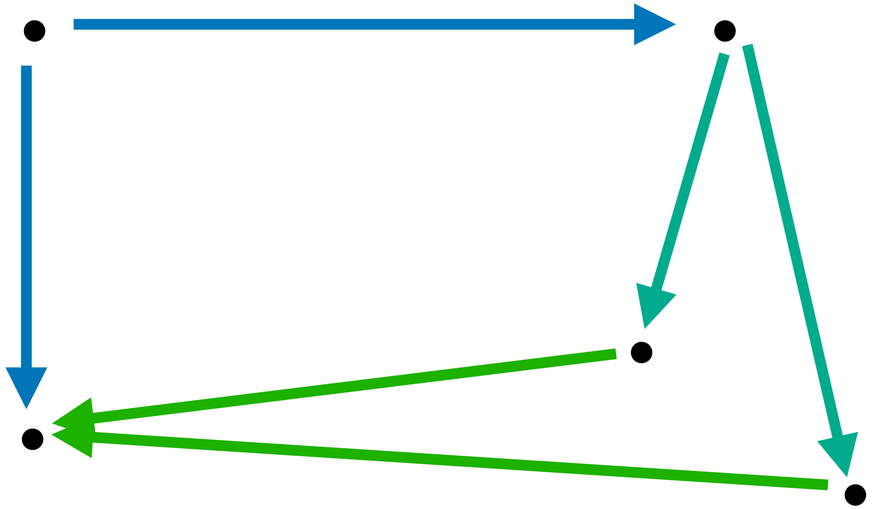
two-special soundness



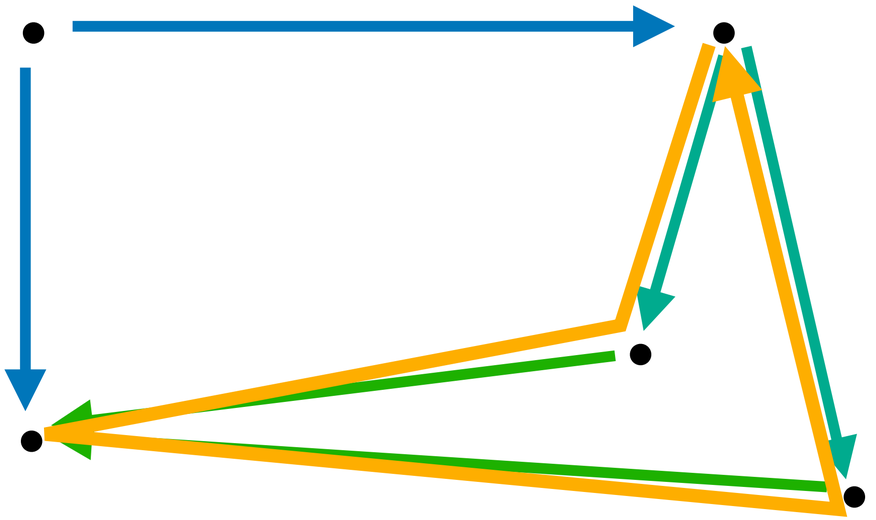
two-special soundness



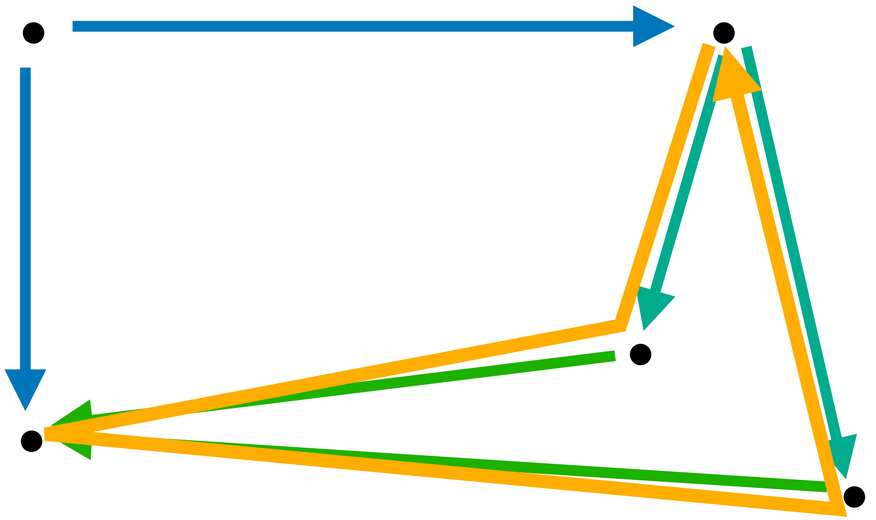
two-special soundness



two-special soundness



two-special soundness

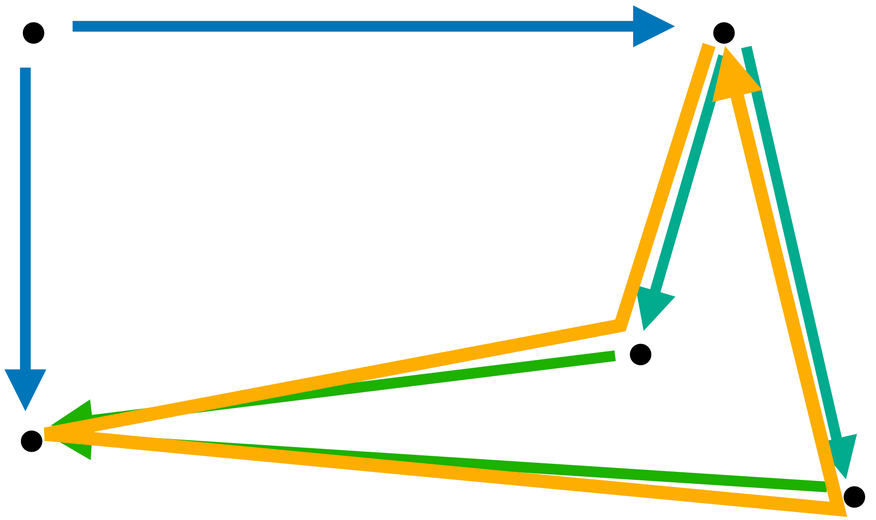


two transcripts,
one commitment

$\Longrightarrow$

one endomorphism
of pk

two-special soundness



two transcripts,
one commitment

$\Longrightarrow$

one endomorphism
of pk

$\Longrightarrow$

endomorphism
ring of pk

soundness notions

1 two-special soundness

(com, chl, rsp)
(com, chl', rsp')

chl ≠ chl'

⇓

witness

soundness notions

1 two-special soundness

special soundness
is not enough
to get
QROM security

witness

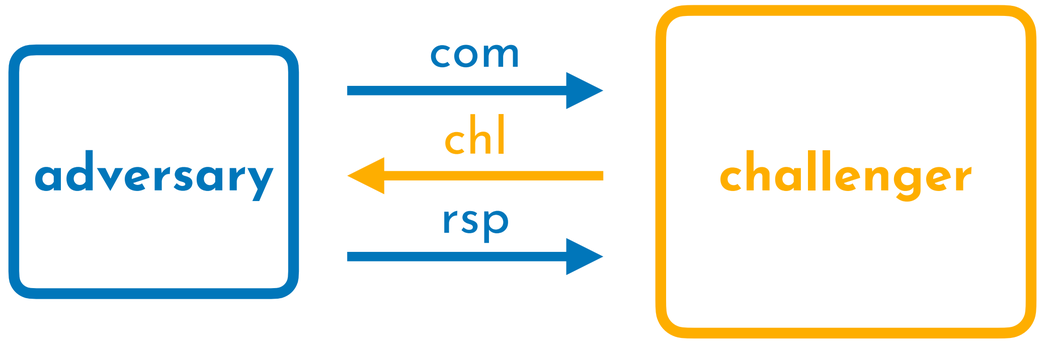
soundness notions

1 two-special soundness

special soundness
is not enough
to get
QROM security

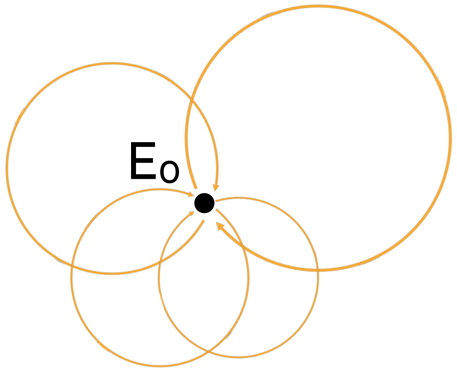
witness

2 ID soundness



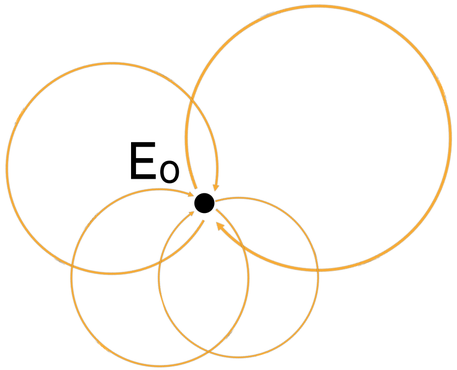
witness

SQIsign





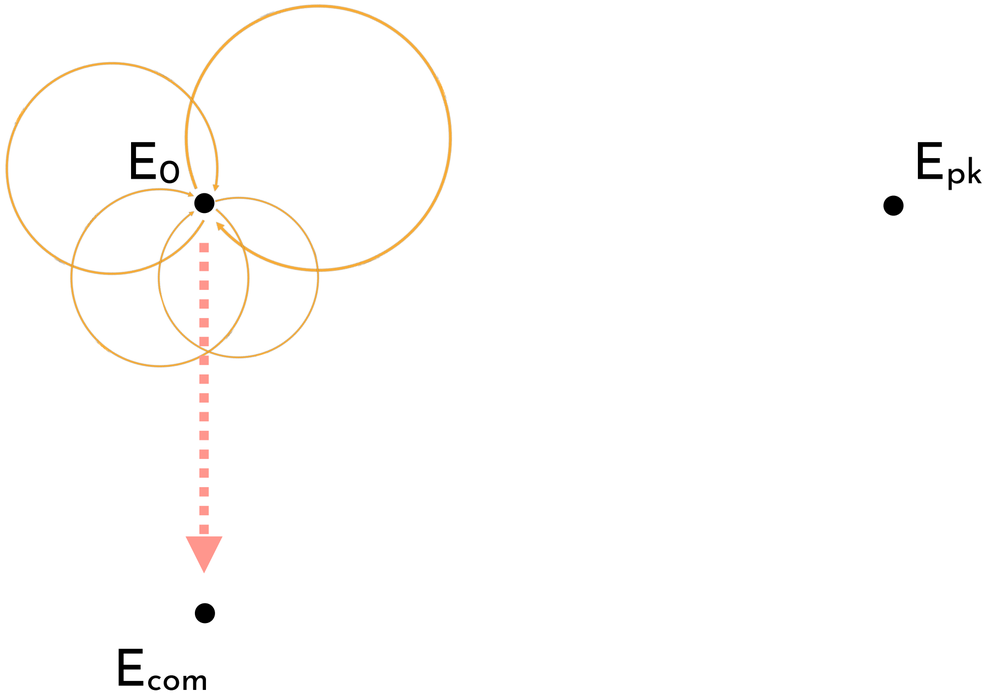
SQIsign



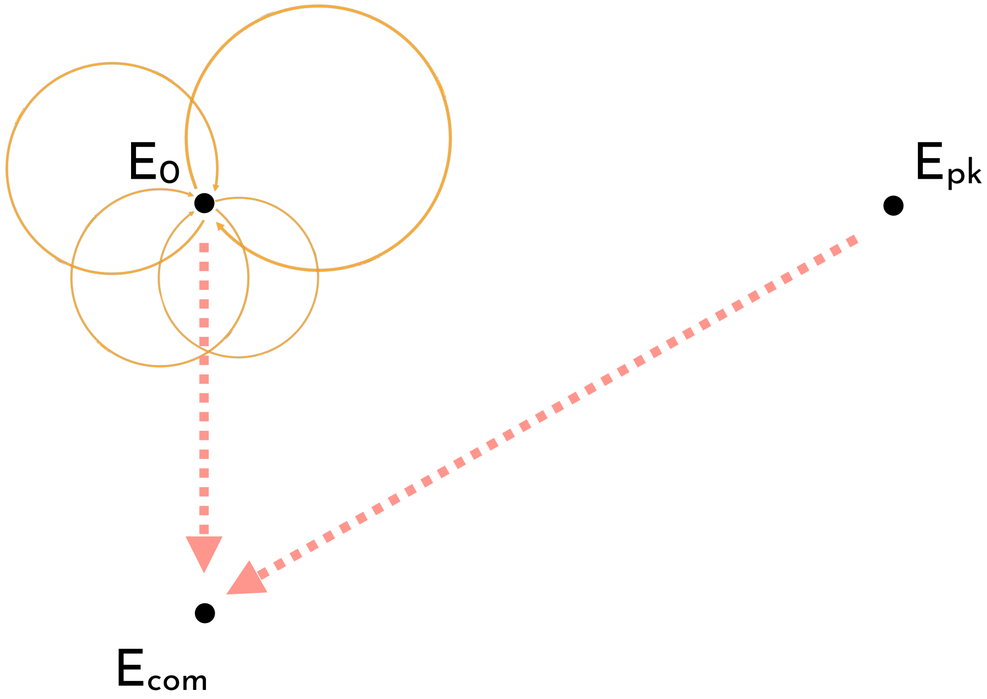




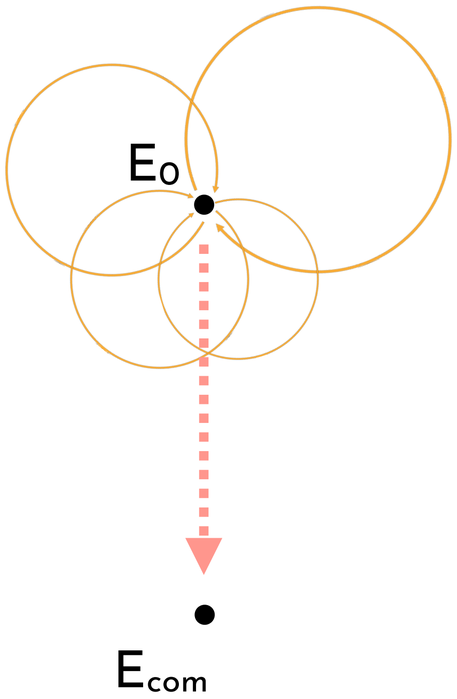
SQIsign



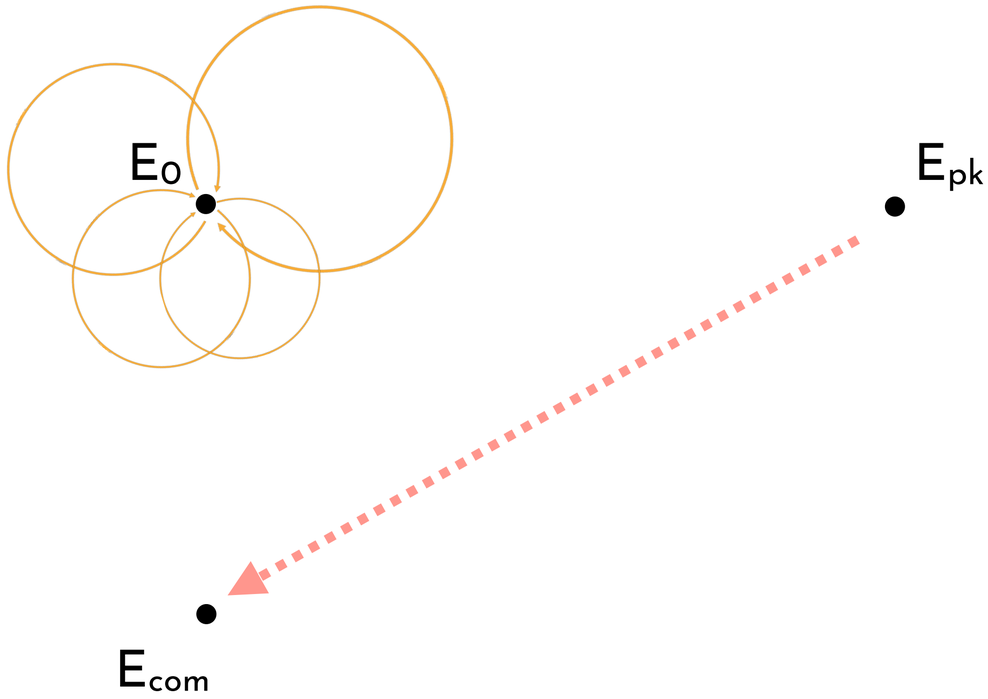
SQIsign



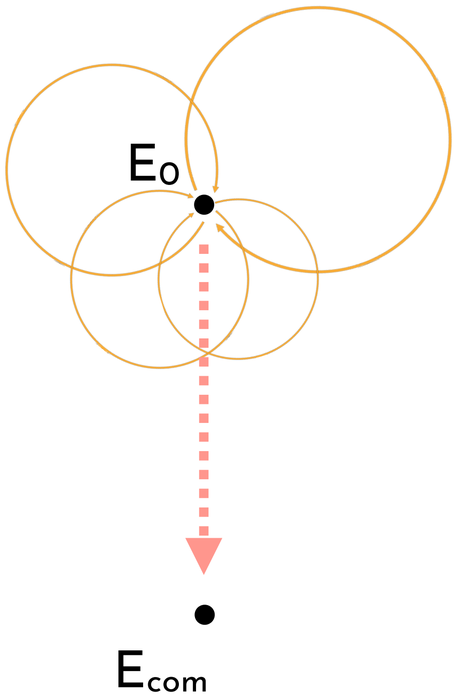
SQIsign is sound



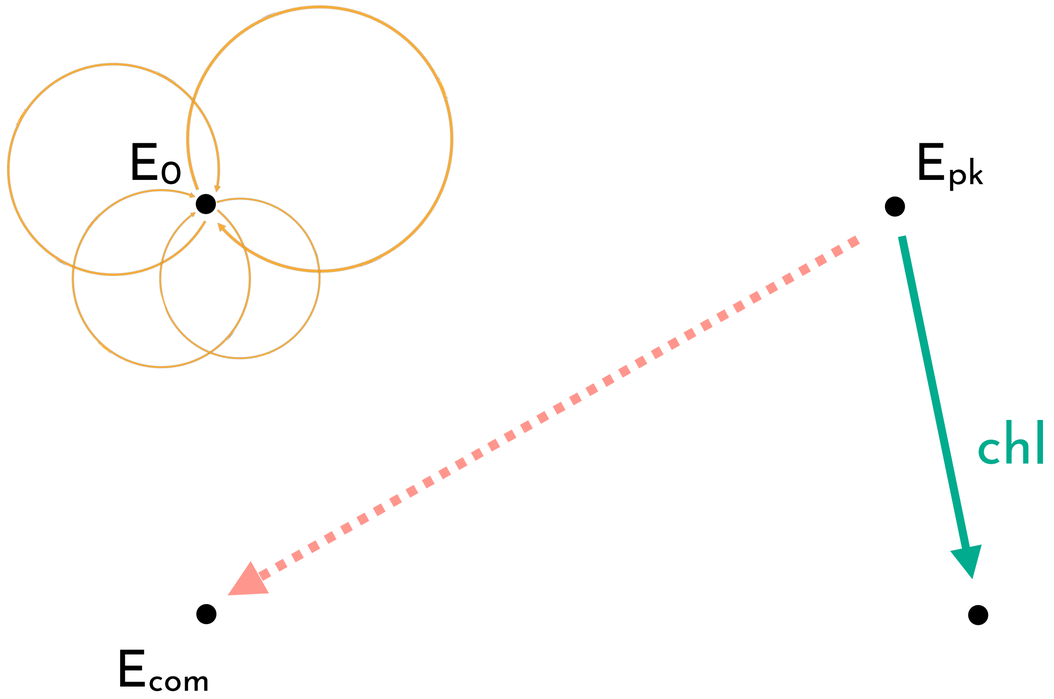




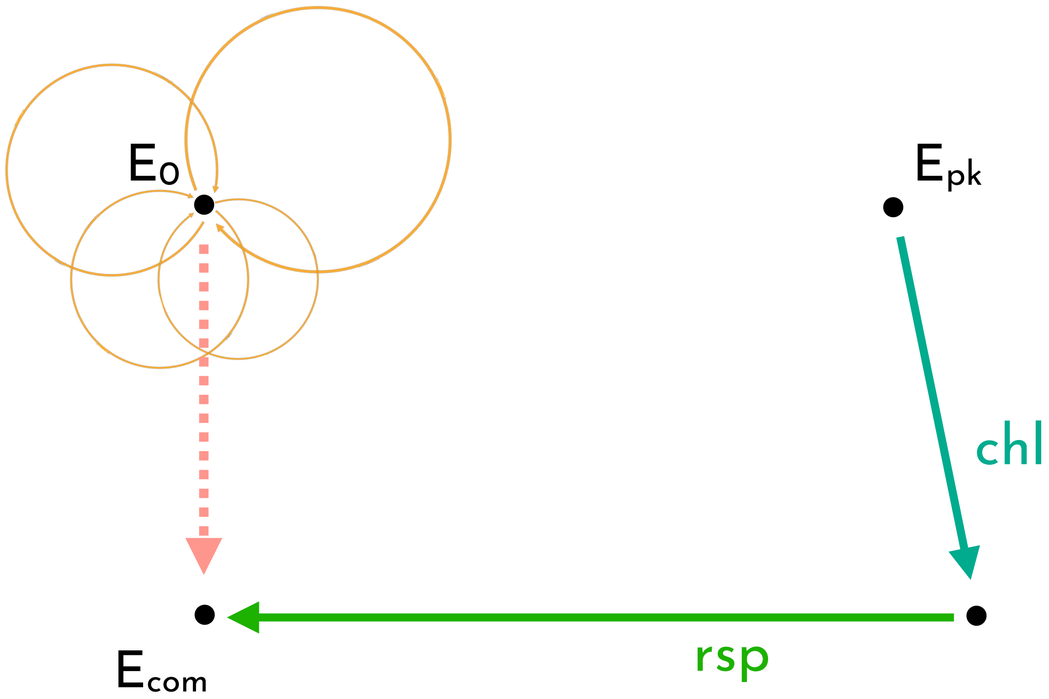
SQIsign is sound

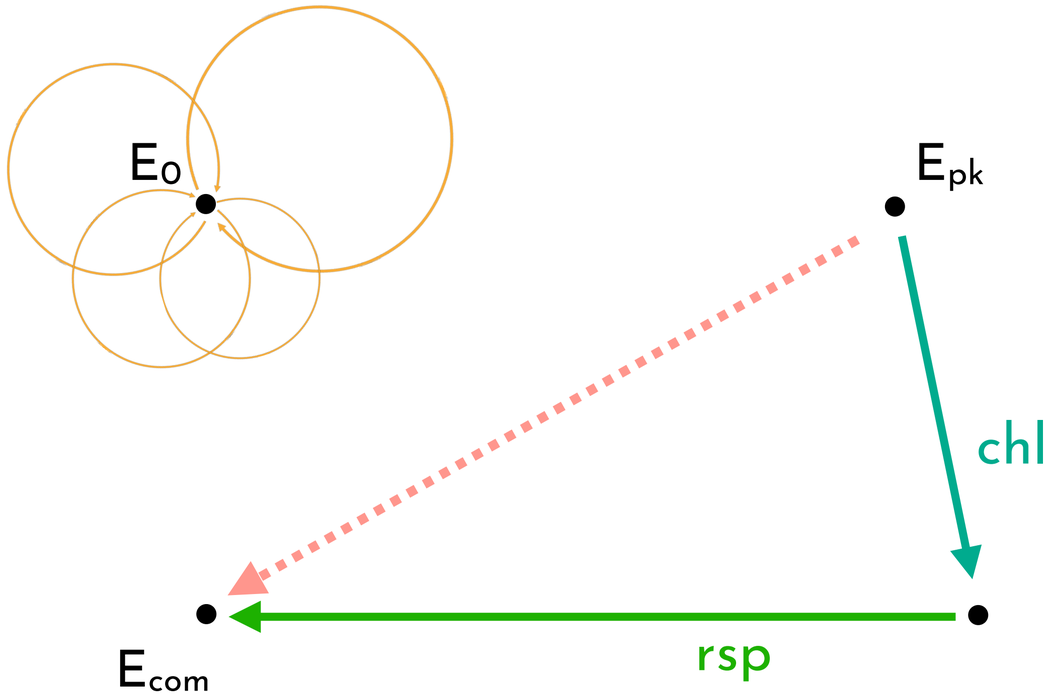




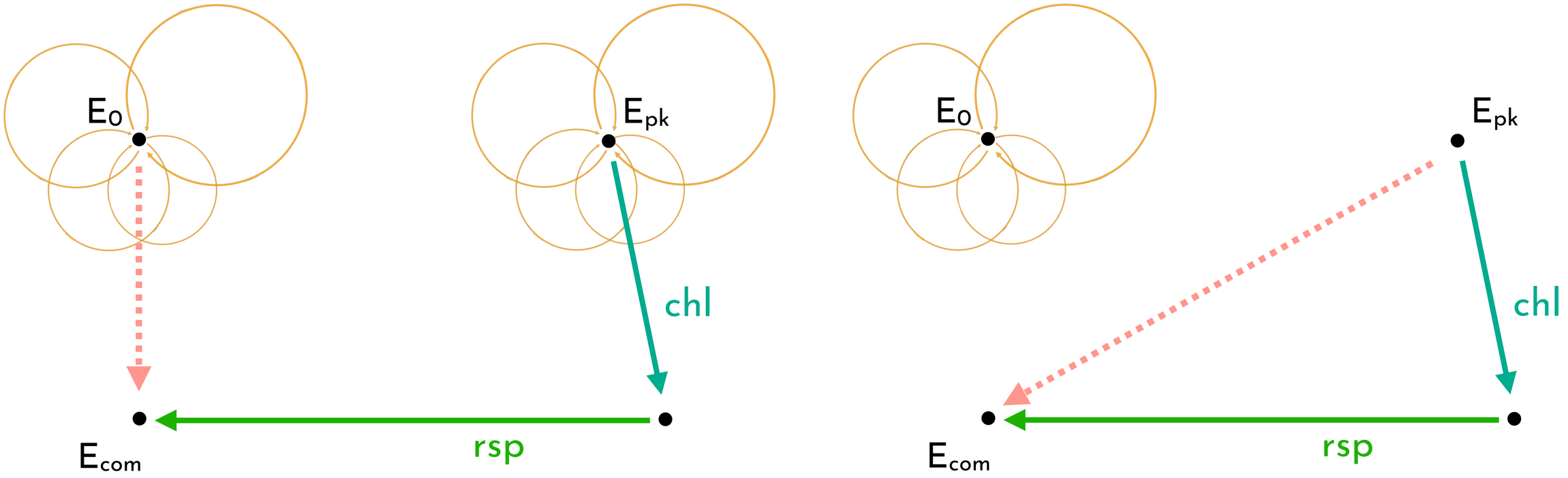


SQIsign is sound

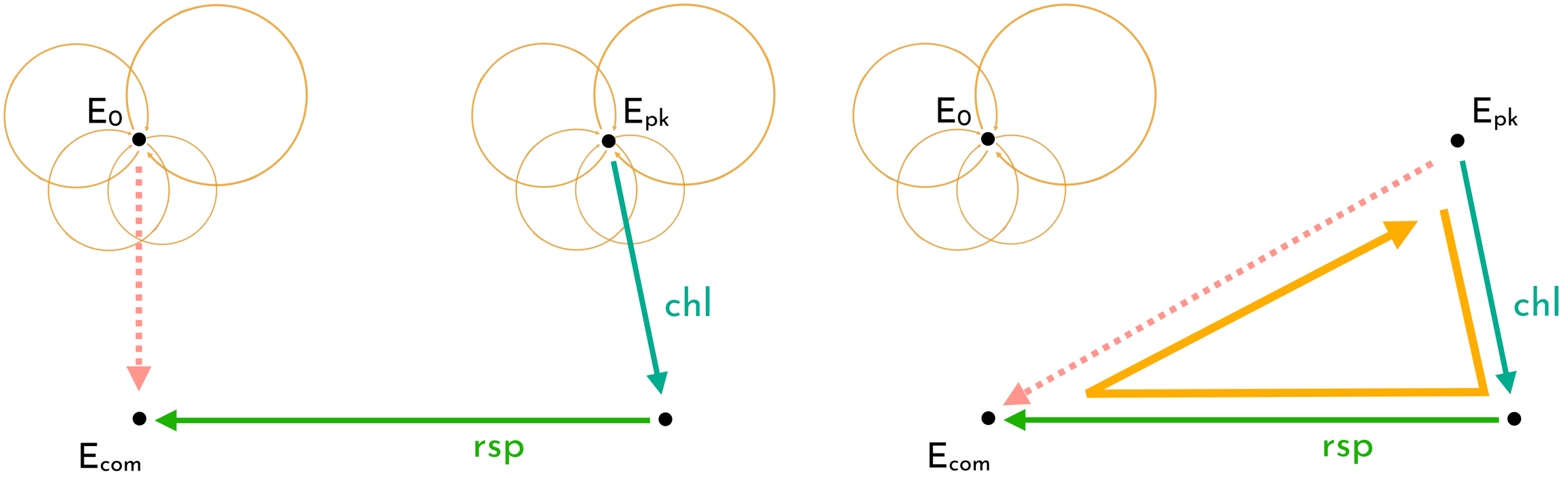




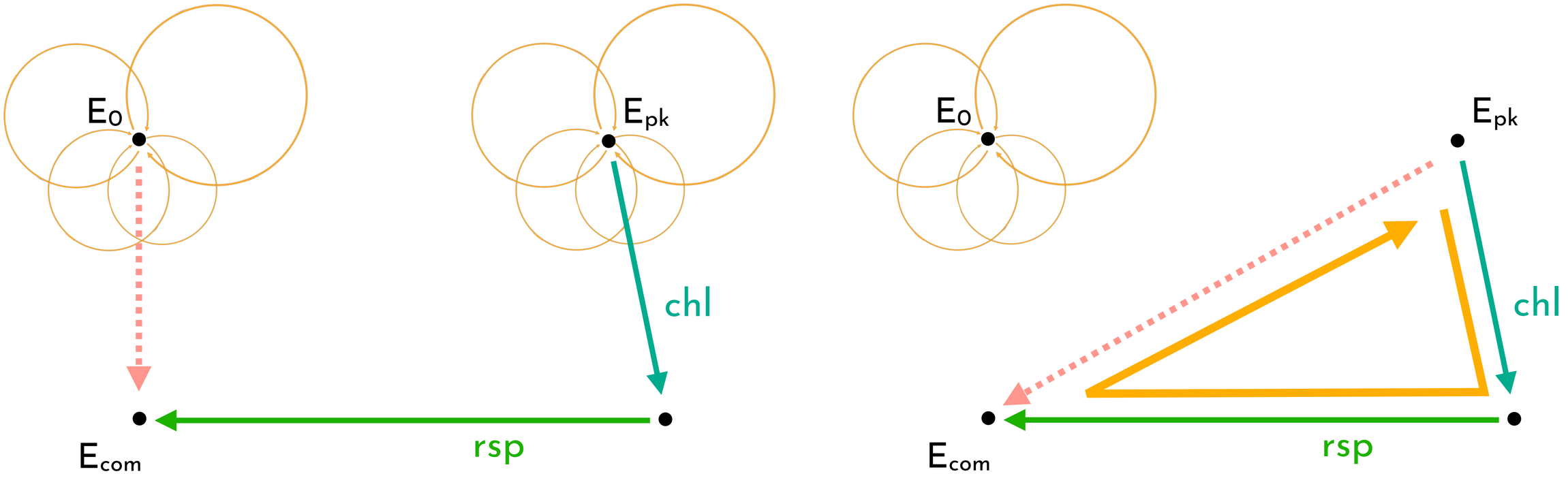
SQIsign is sound



SQIsign is sound



SQIsign is sound



we obtain (at least) one non-trivial endomorphism

SQIsign is EUF-CMA secure in the QROM

(in the AIM)

results (in the AIM)

1 all results in the AGAM (with twist) also hold in the AIM

2 SQIsign is EUF–CMA secure in the QROM

3 CDH is equivalent to DLOG, for all isogeny formulations (CSIDH, M-SIDH, MD-SIDH, binSIDH, terSIDH, etc.)

in this work

we introduce the
Algebraic Isogeny Model

in this work

we introduce the
Algebraic Isogeny Model

- SQIsign is secure in the QROM
- DLOG ≡ CDH (for all isogeny variants)
- all AGAM results hold

in this work

we introduce the
Algebraic Isogeny Model

- SQIsign is secure in the QROM
- DLOG ≡ CDH (for all isogeny variants)
- all AGAM results hold

- the INKE PKE
- OPRF
- …

in this work

new isogeny assumption?

give the AIM a try!

we introduce the
Algebraic Isogeny Model

- SQIsign is secure in the QROM
- DLOG ≡ CDH (for all isogeny variants)
- all AGAM results hold

- the INKE PKE
- OPRF
- …

backup slides

DLOG and CDH are equivalent for all SIDH variants

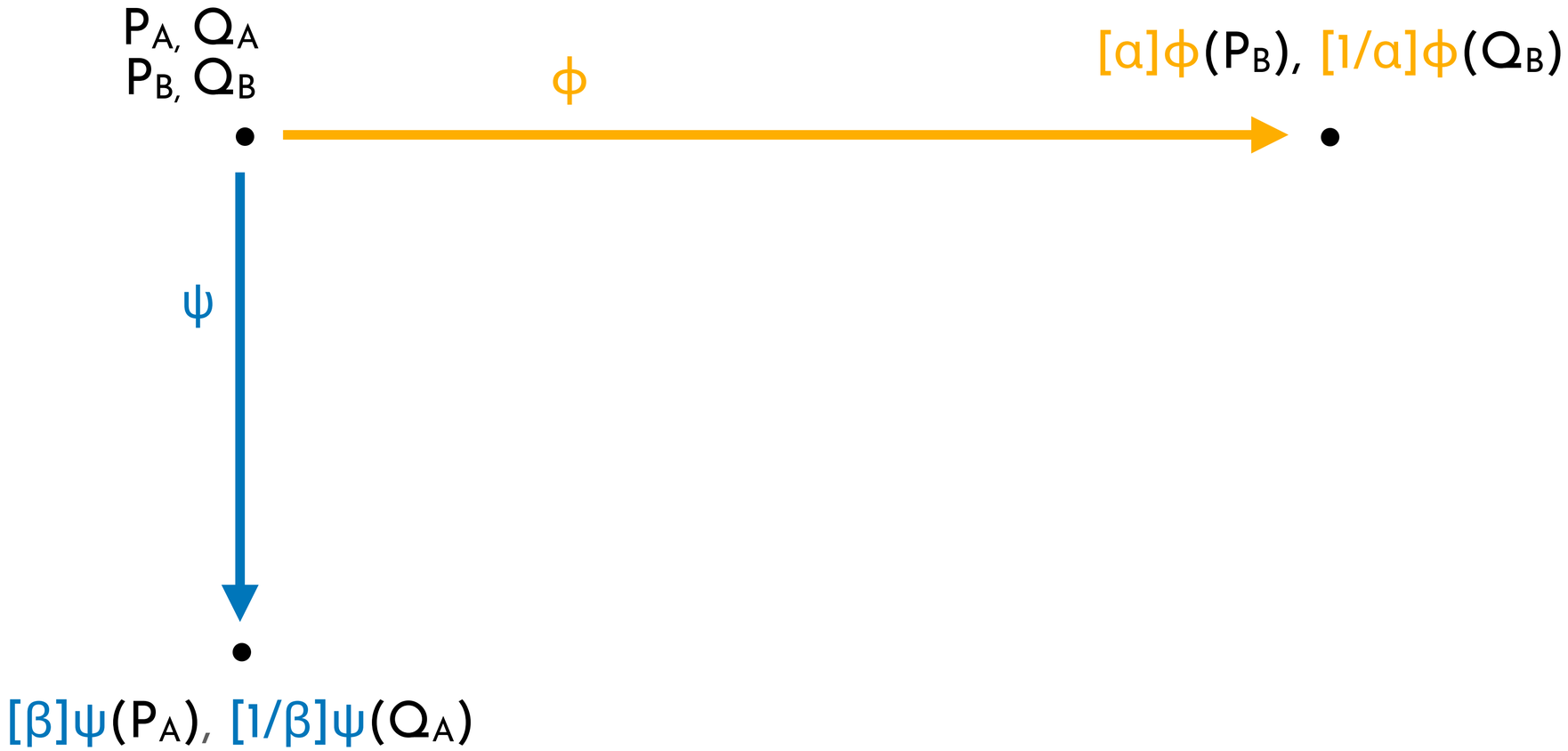
binSIDH

P_A, Q_A
P_B, Q_B

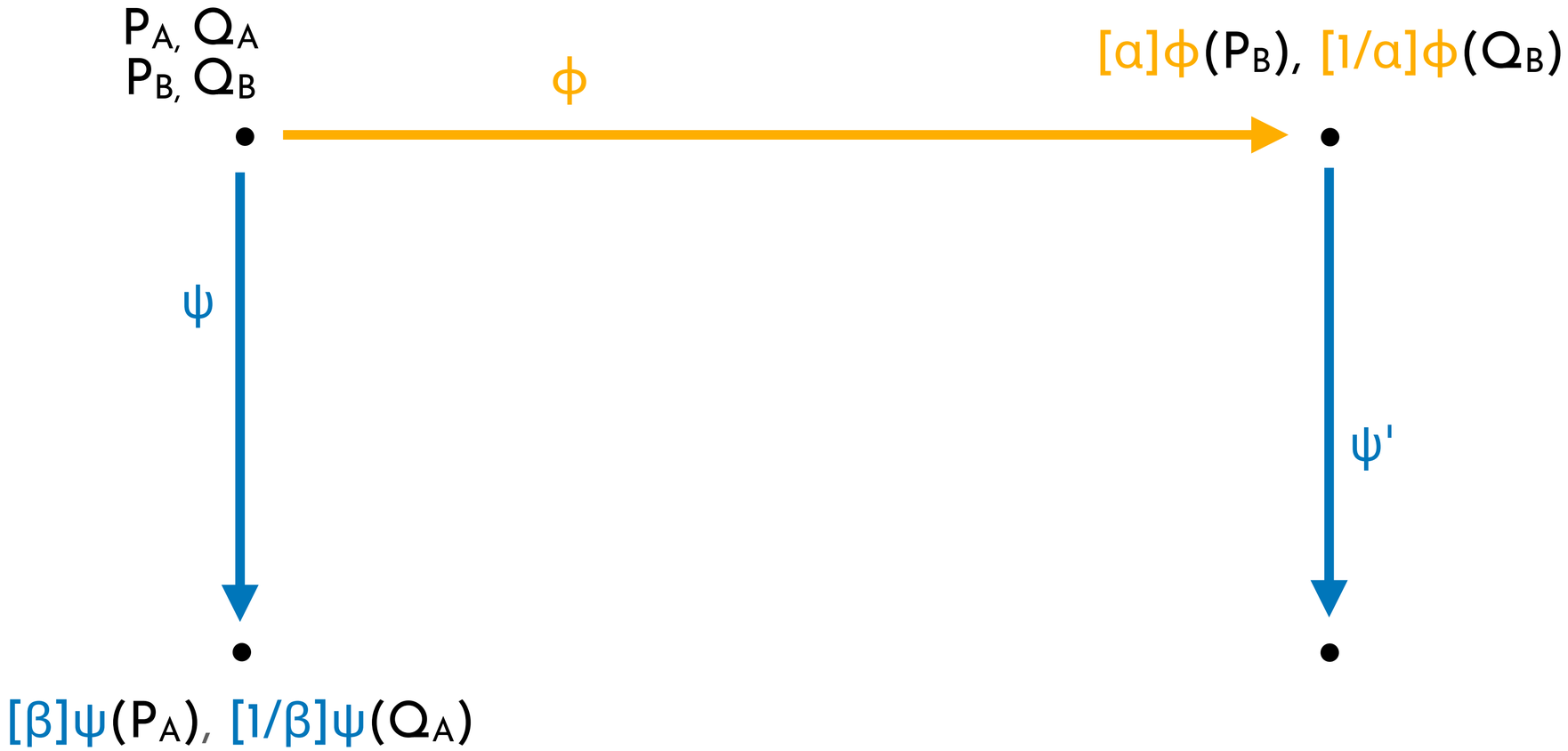
binSIDH



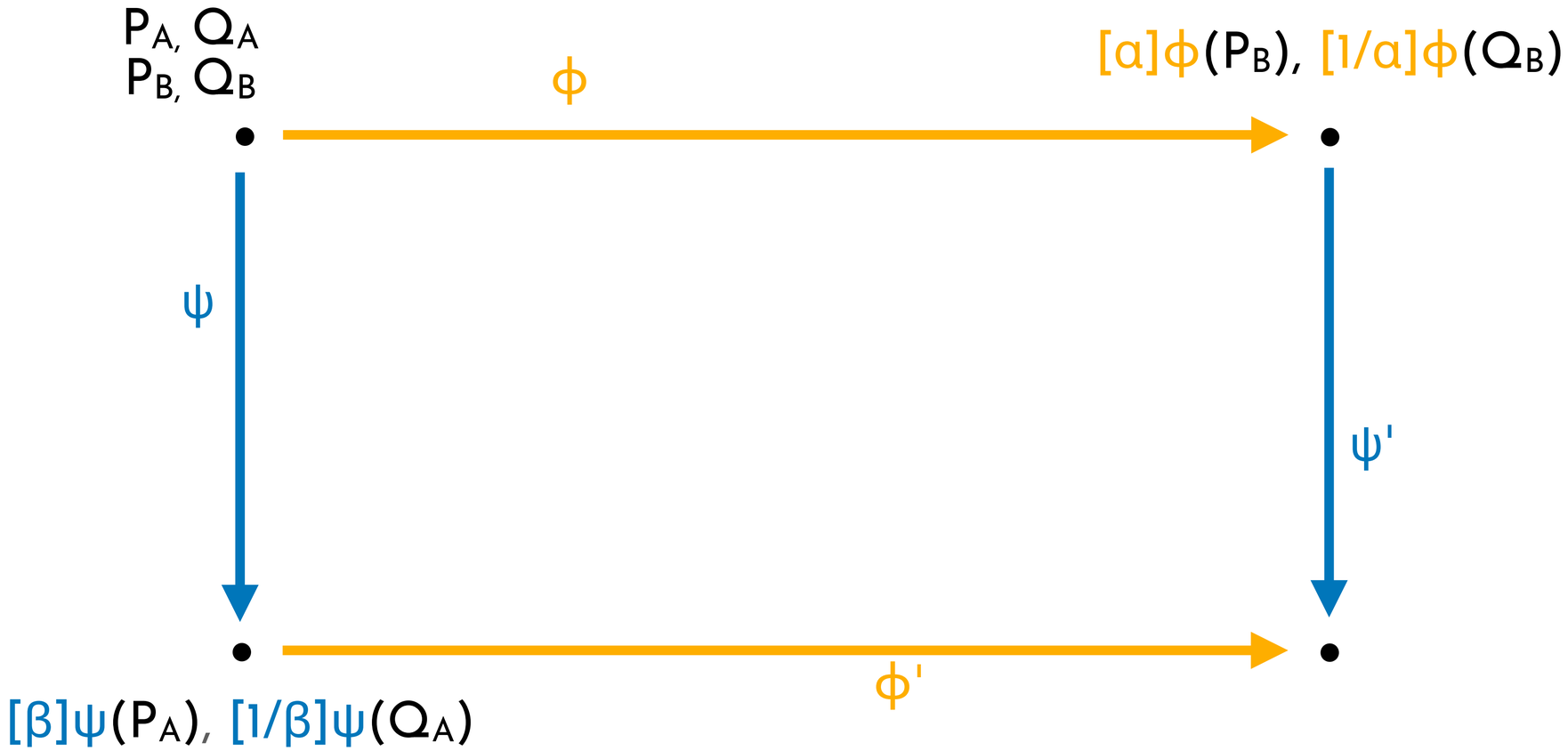
binSIDH


P_A, Q_A
P_B, Q_B
ϕ
$[\alpha]\phi(P_B), [1/\alpha]\phi(Q_B)$
ψ
$[\beta]\psi(P_A), [1/\beta]\psi(Q_A)$

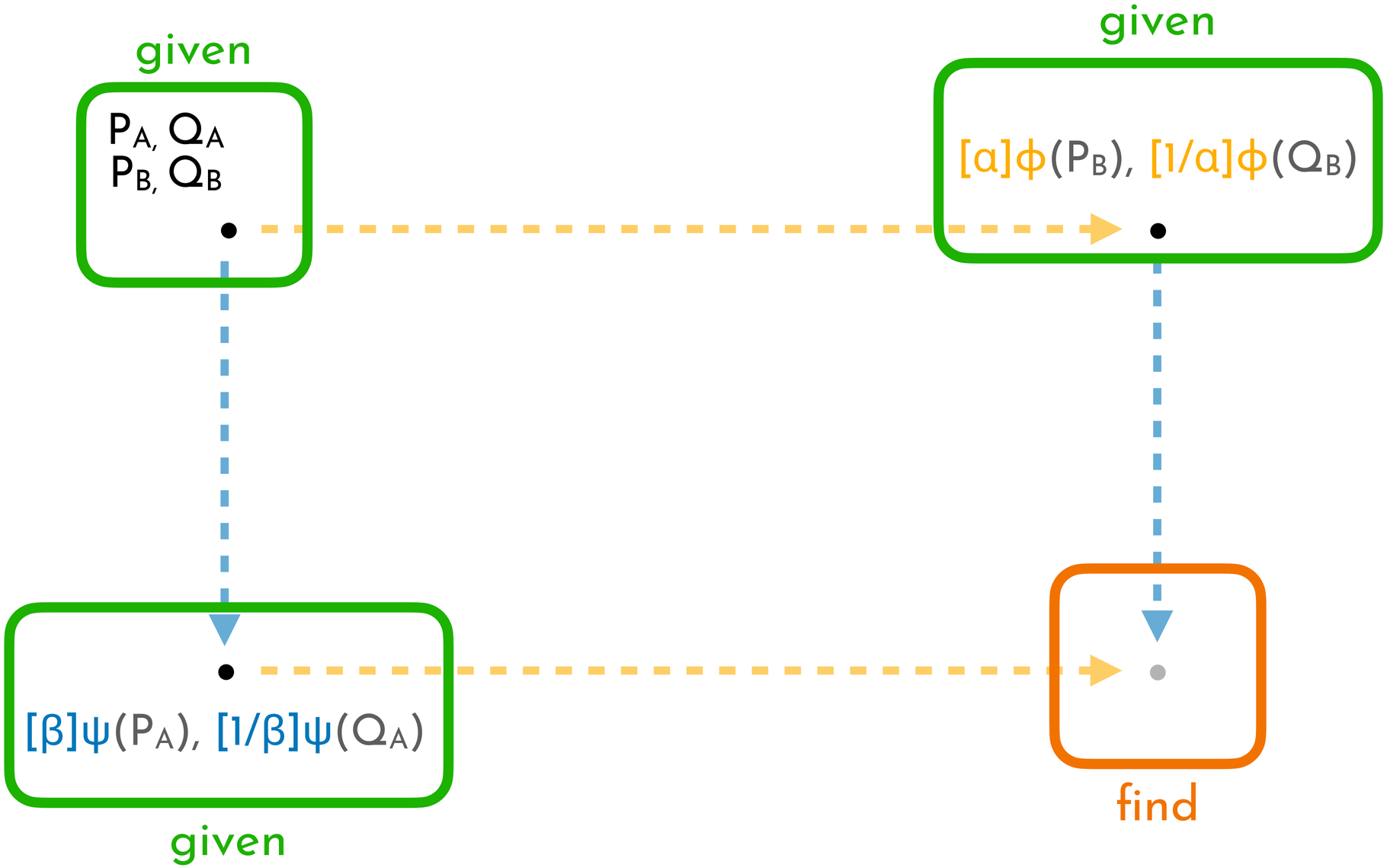
binSIDH


P_A, Q_A
P_B, Q_B
ϕ
$[\alpha]\phi(P_B), [1/\alpha]\phi(Q_B)$
ψ
ψ'
$[\beta]\psi(P_A), [1/\beta]\psi(Q_A)$

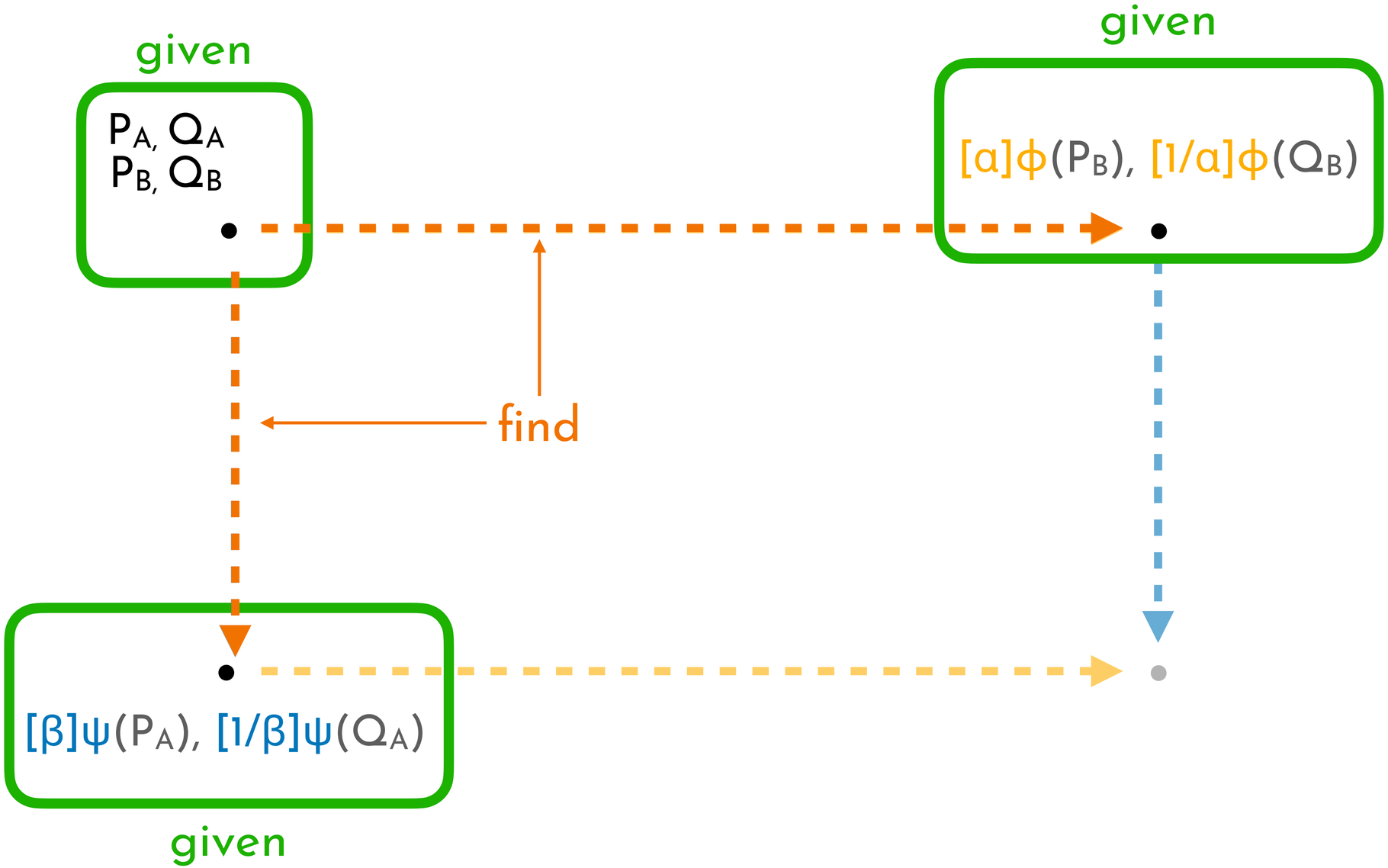
binSIDH


P_A, Q_A
P_B, Q_B
ϕ
$[\alpha]\phi(P_B), [1/\alpha]\phi(Q_B)$
ψ
ψ'
ϕ'
$[\beta]\psi(P_A), [1/\beta]\psi(Q_A)$

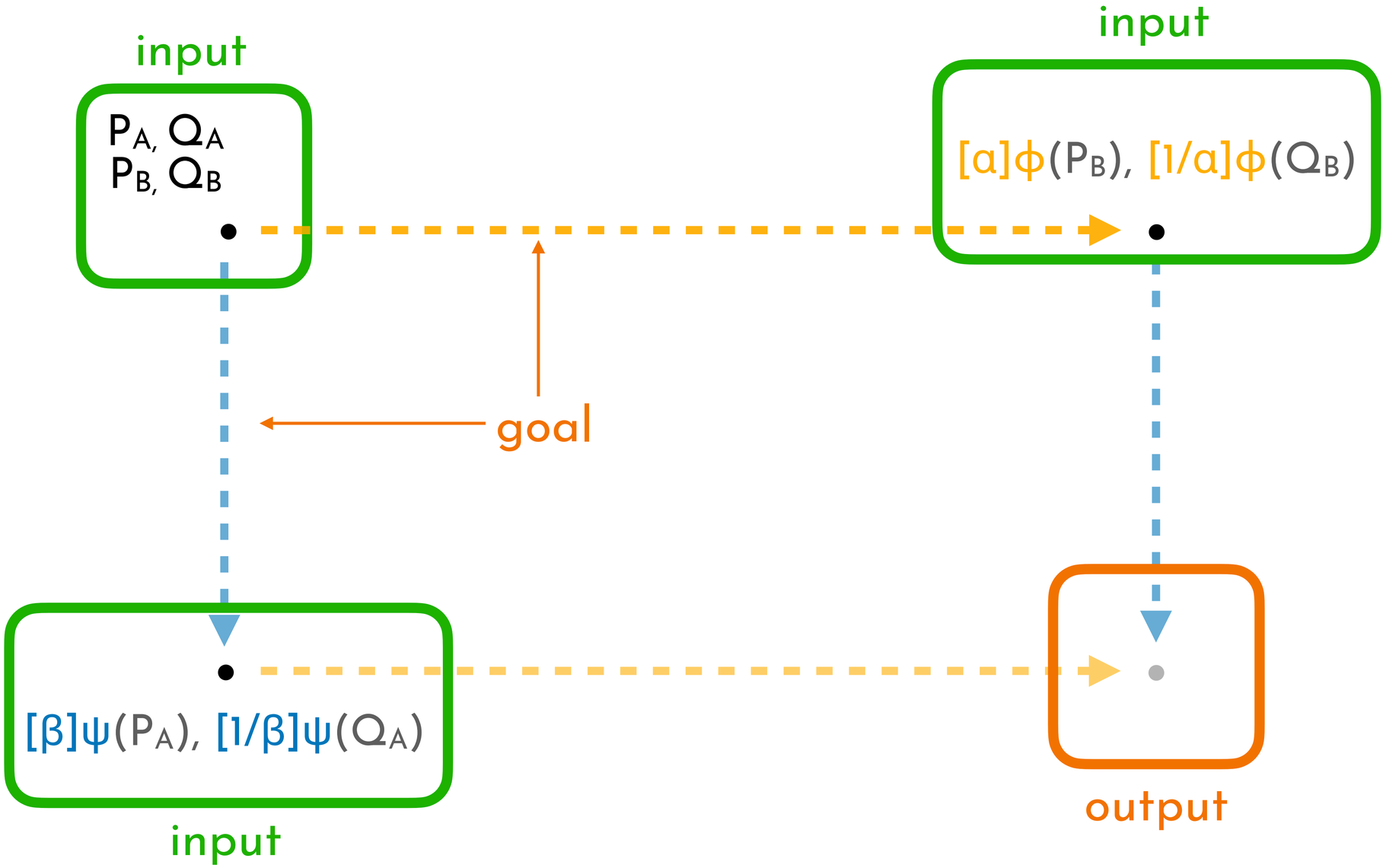
the binSIDH CDH problem



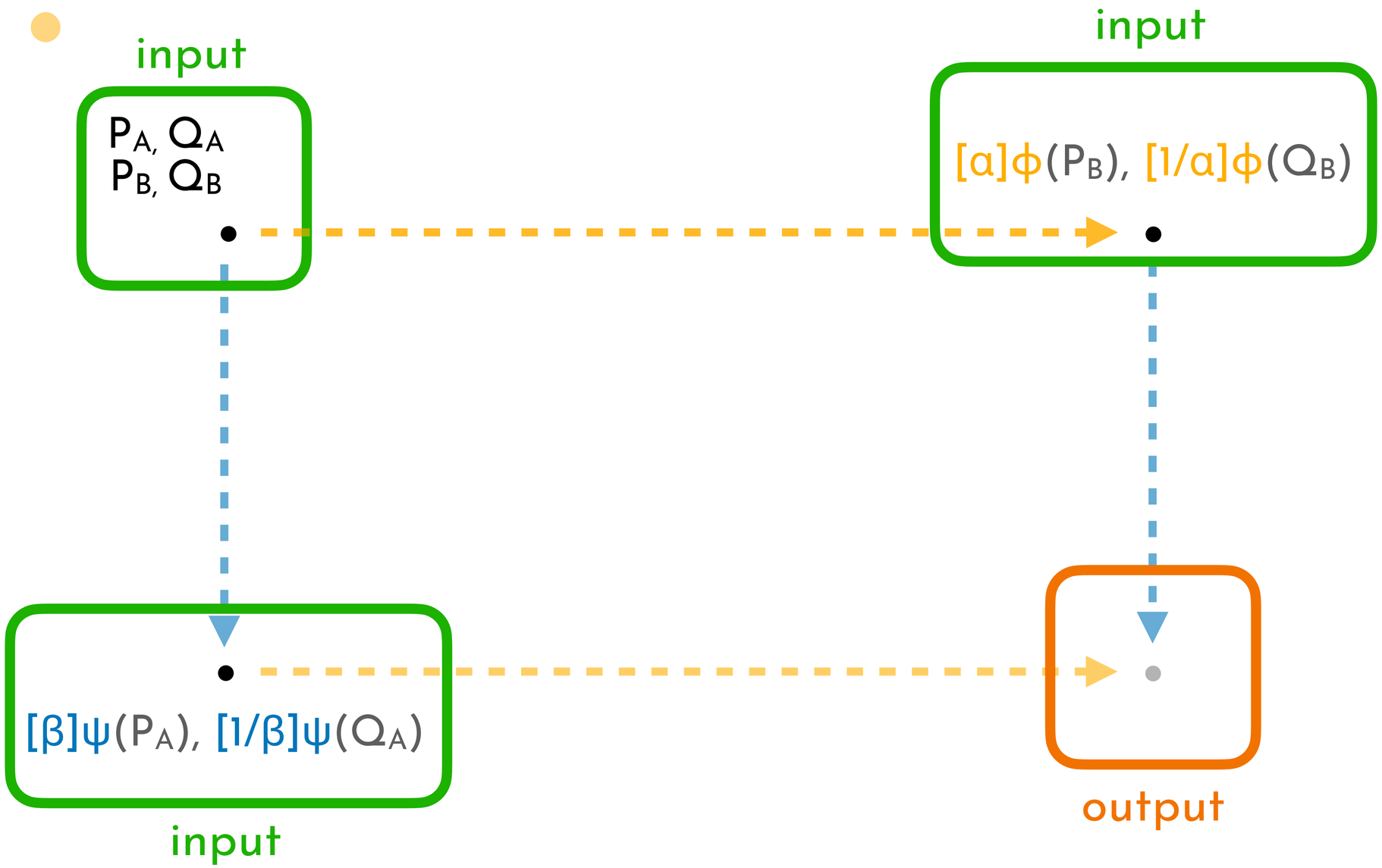
the binSIDH DLOG problem



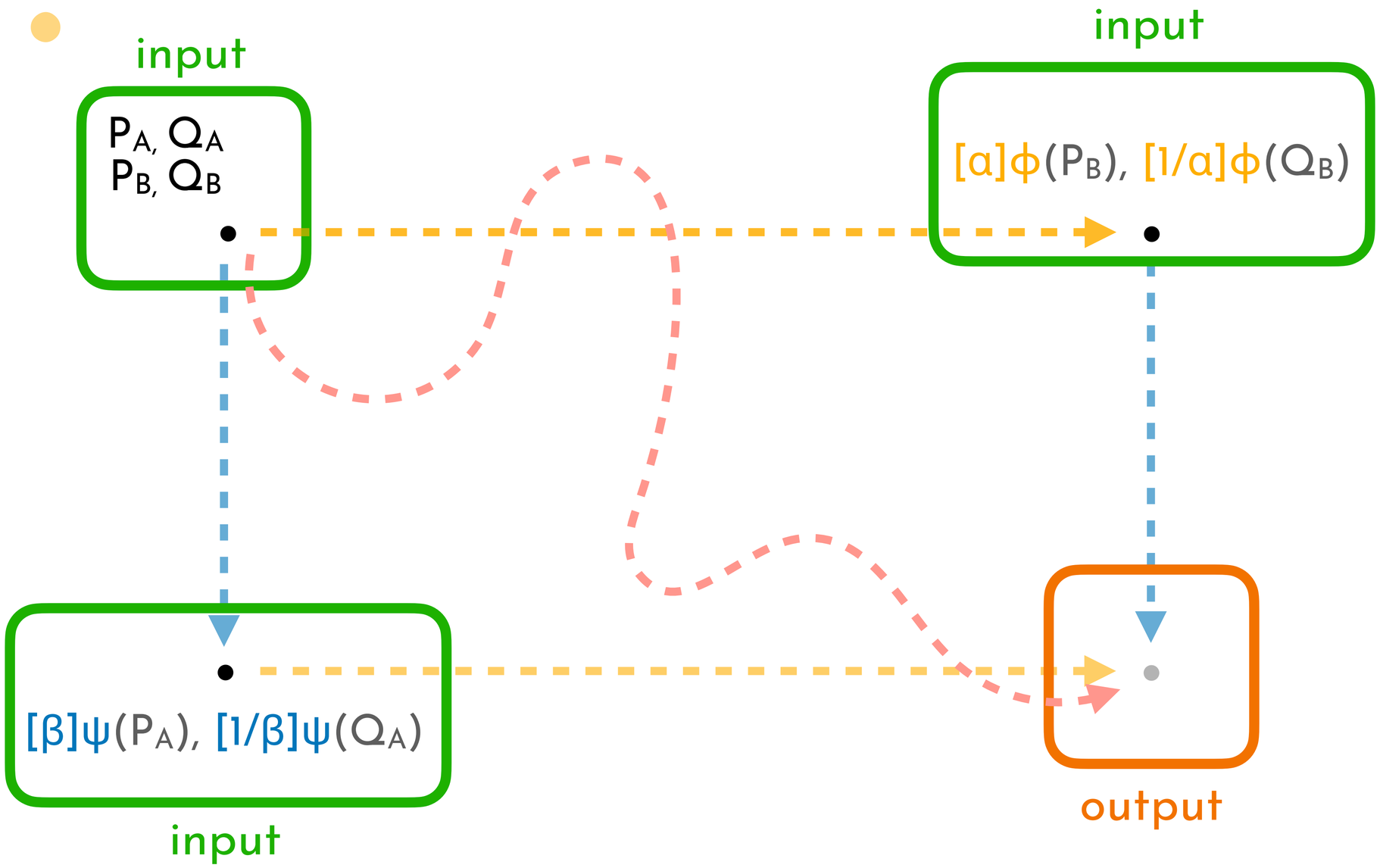
DLOG to CDH reduction



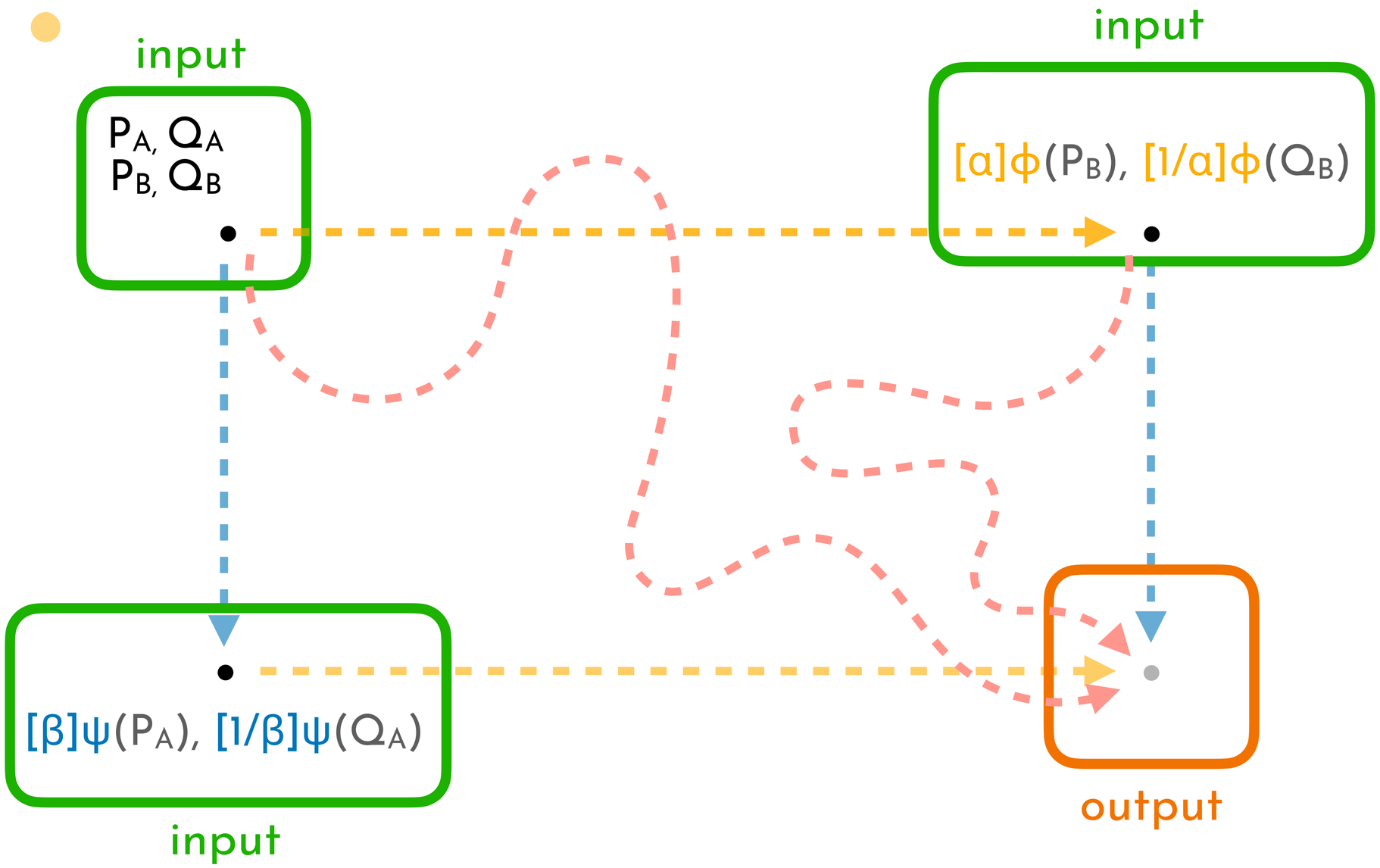
1 guess which explanation we get



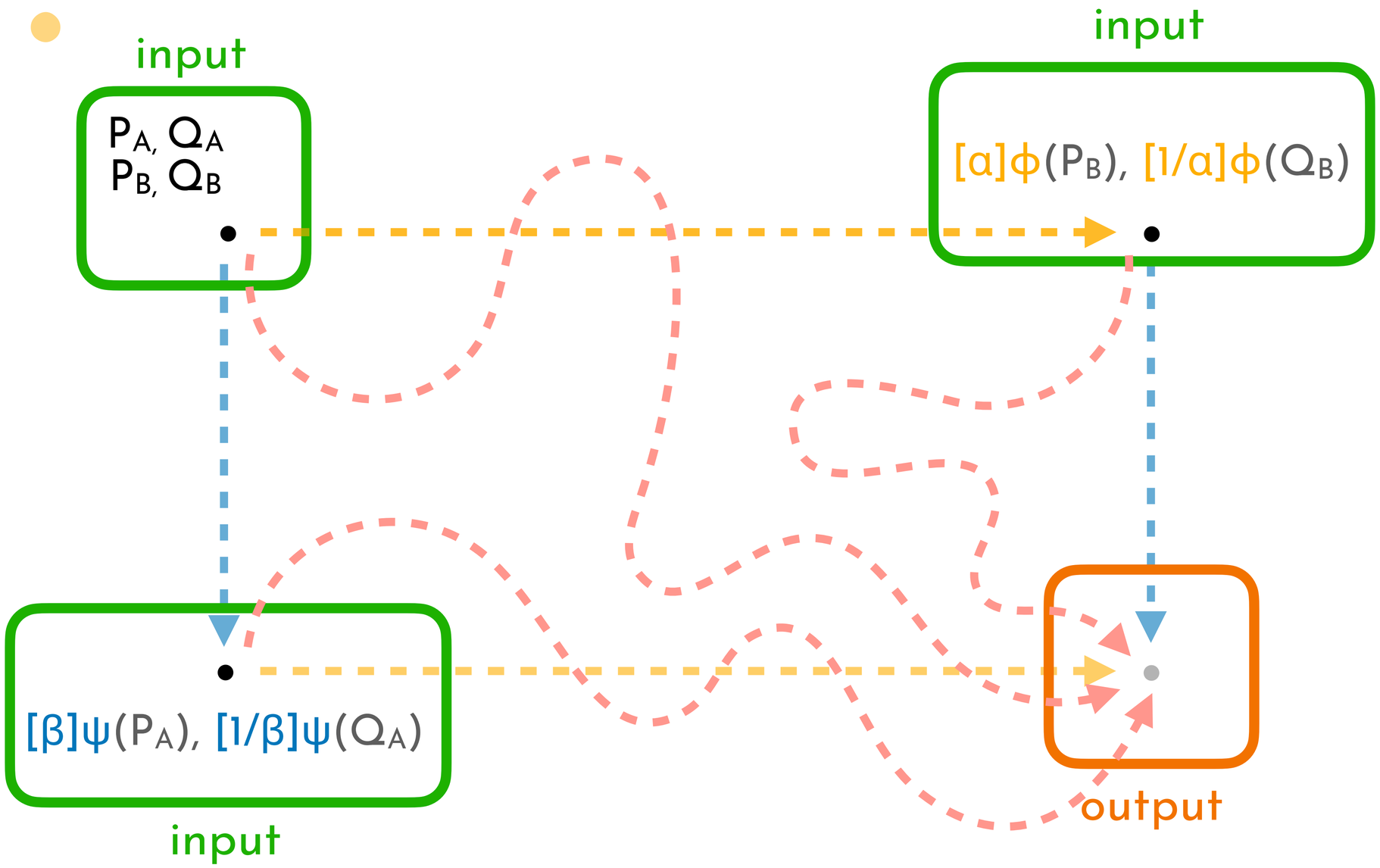
1 guess which explanation we get



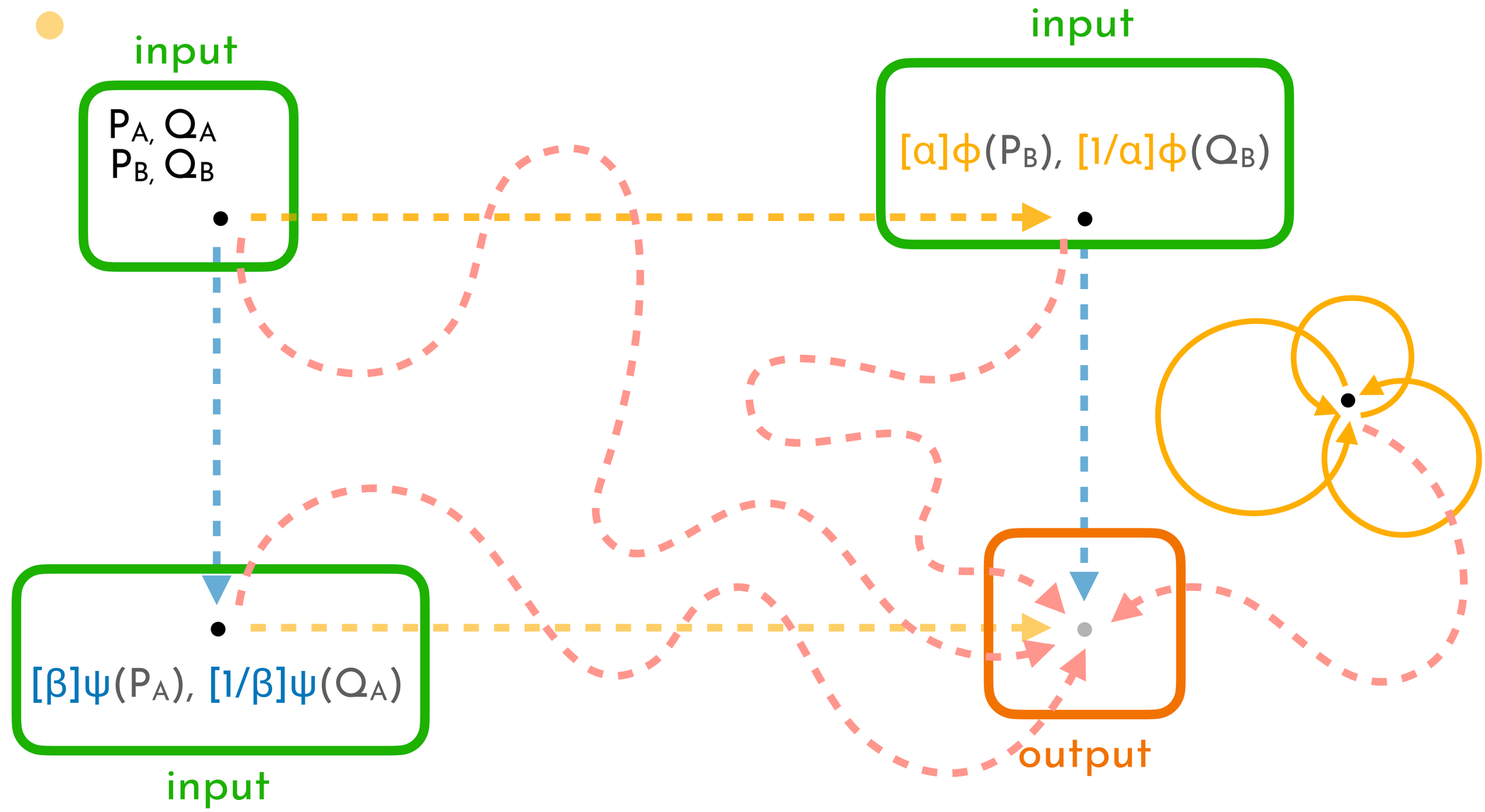
1 guess which explanation we get



1 guess which explanation we get



1 guess which explanation we get

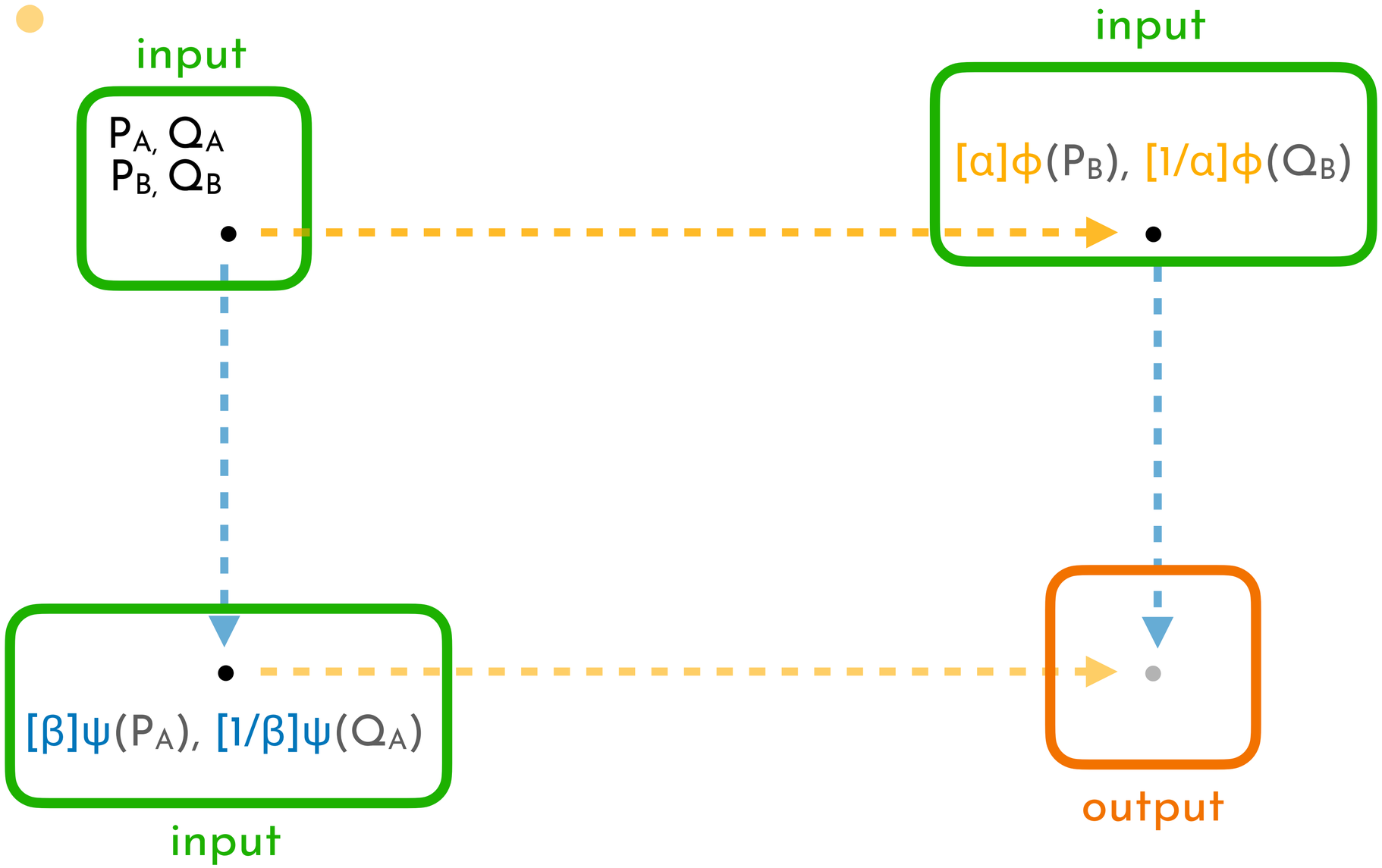


2. if guess is incorrect, stop

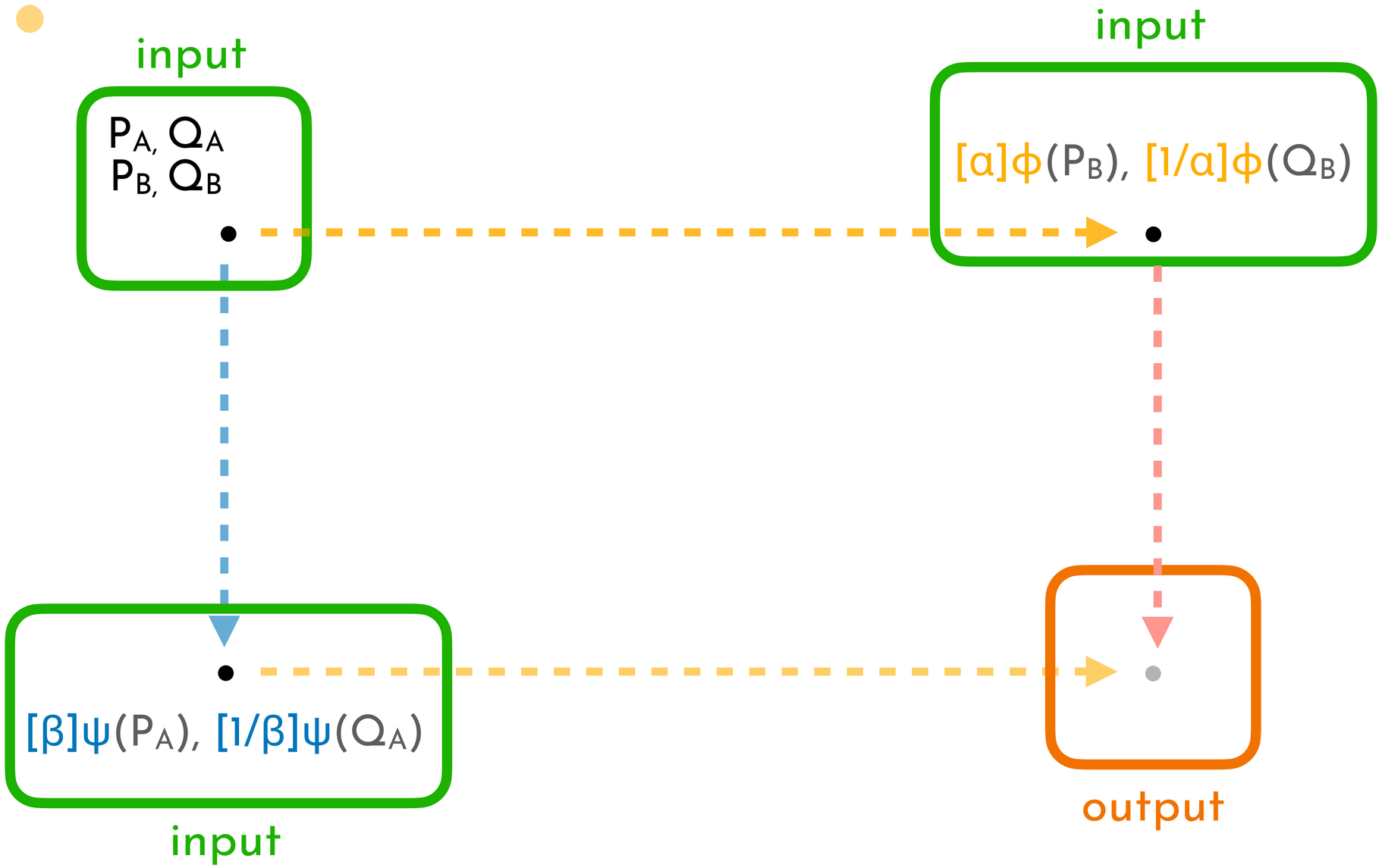
2. if guess is incorrect, stop

3. handle each case separately

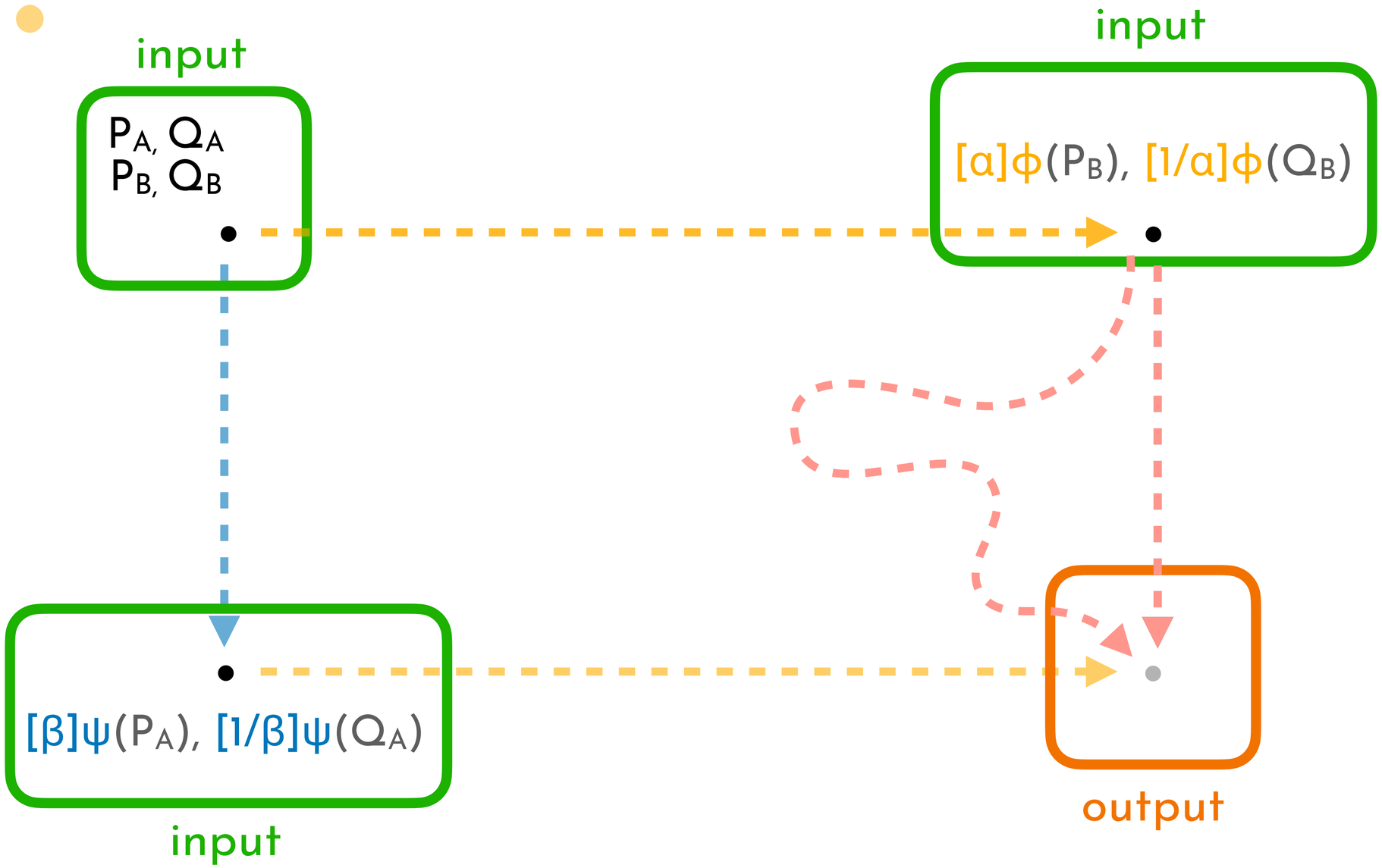
4. guess if the explanation is good



4. guess if the explanation is good



4. guess if the explanation is good

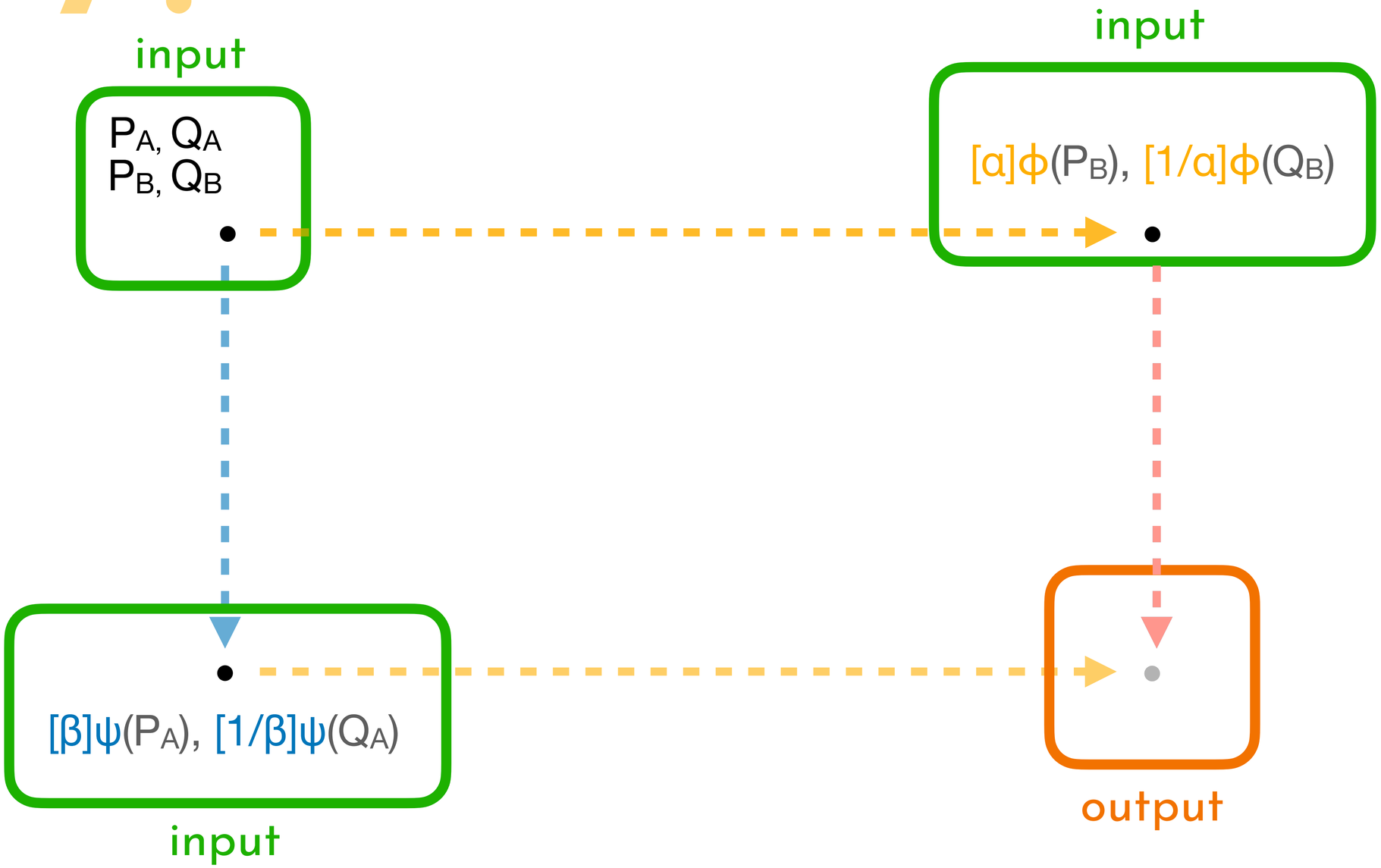


5. if guess is incorrect, stop

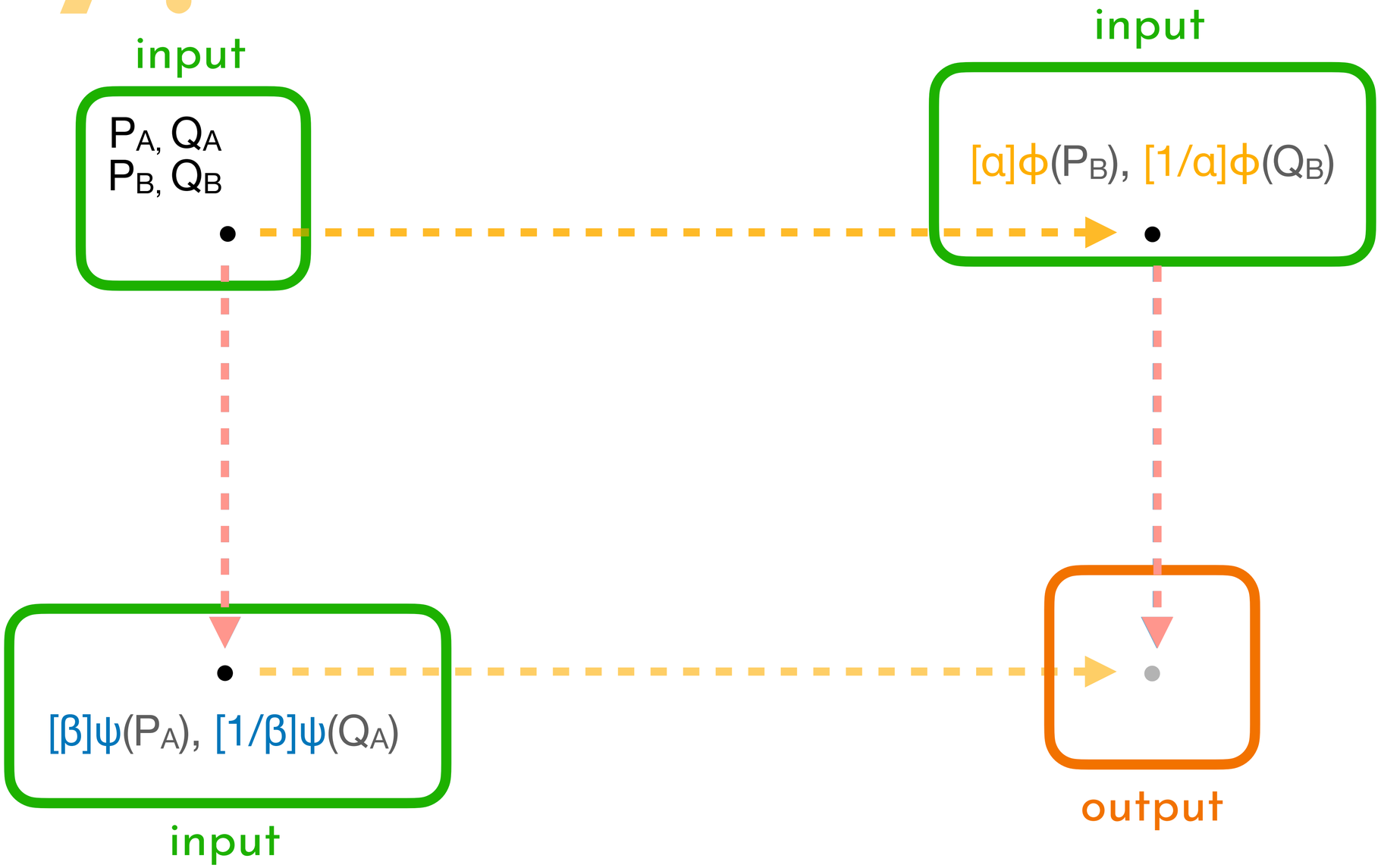
5. if guess is incorrect, stop

6. handle the two cases separately

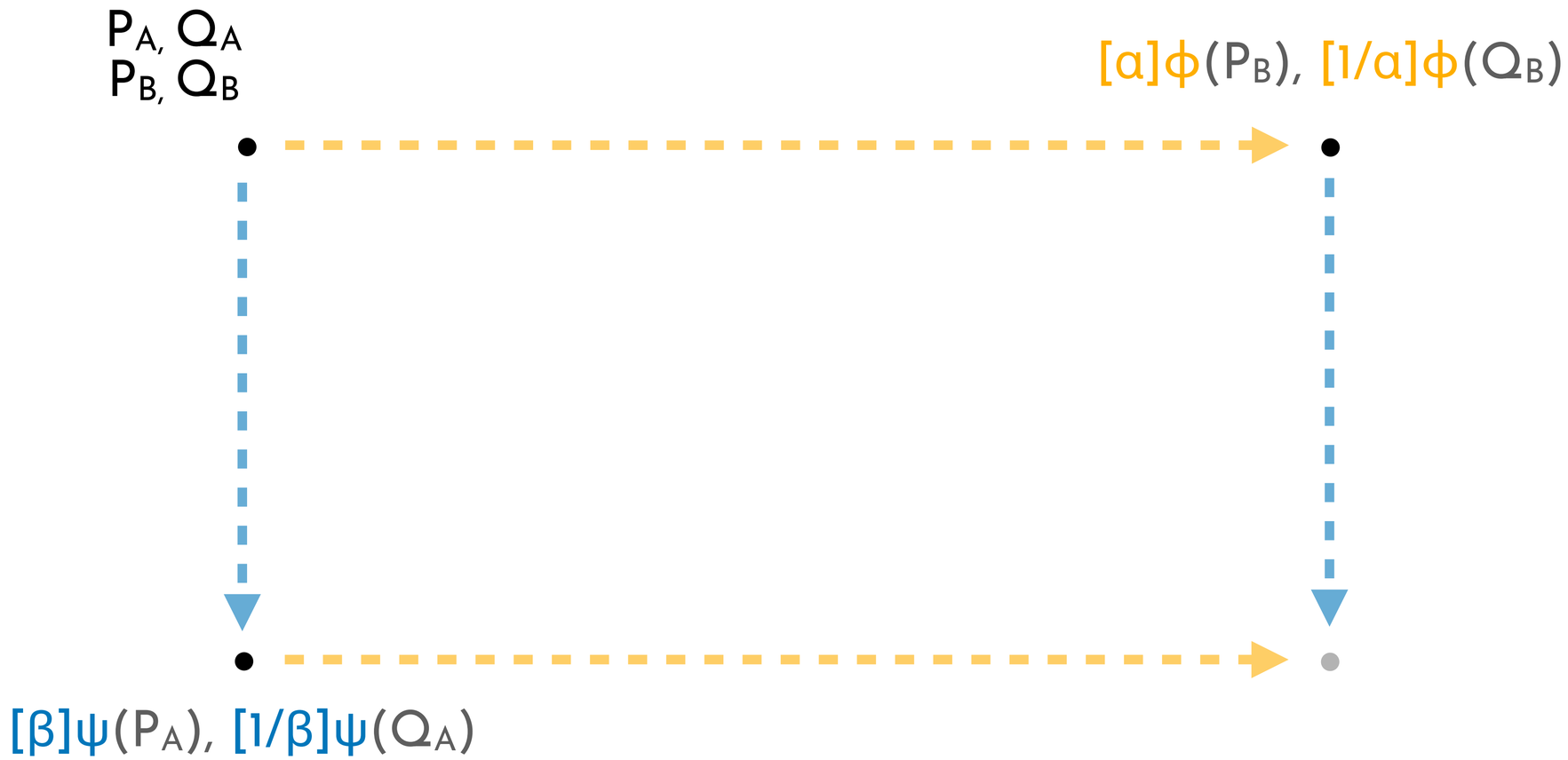
7. if good, extract the secret



7. if good, extract the secret



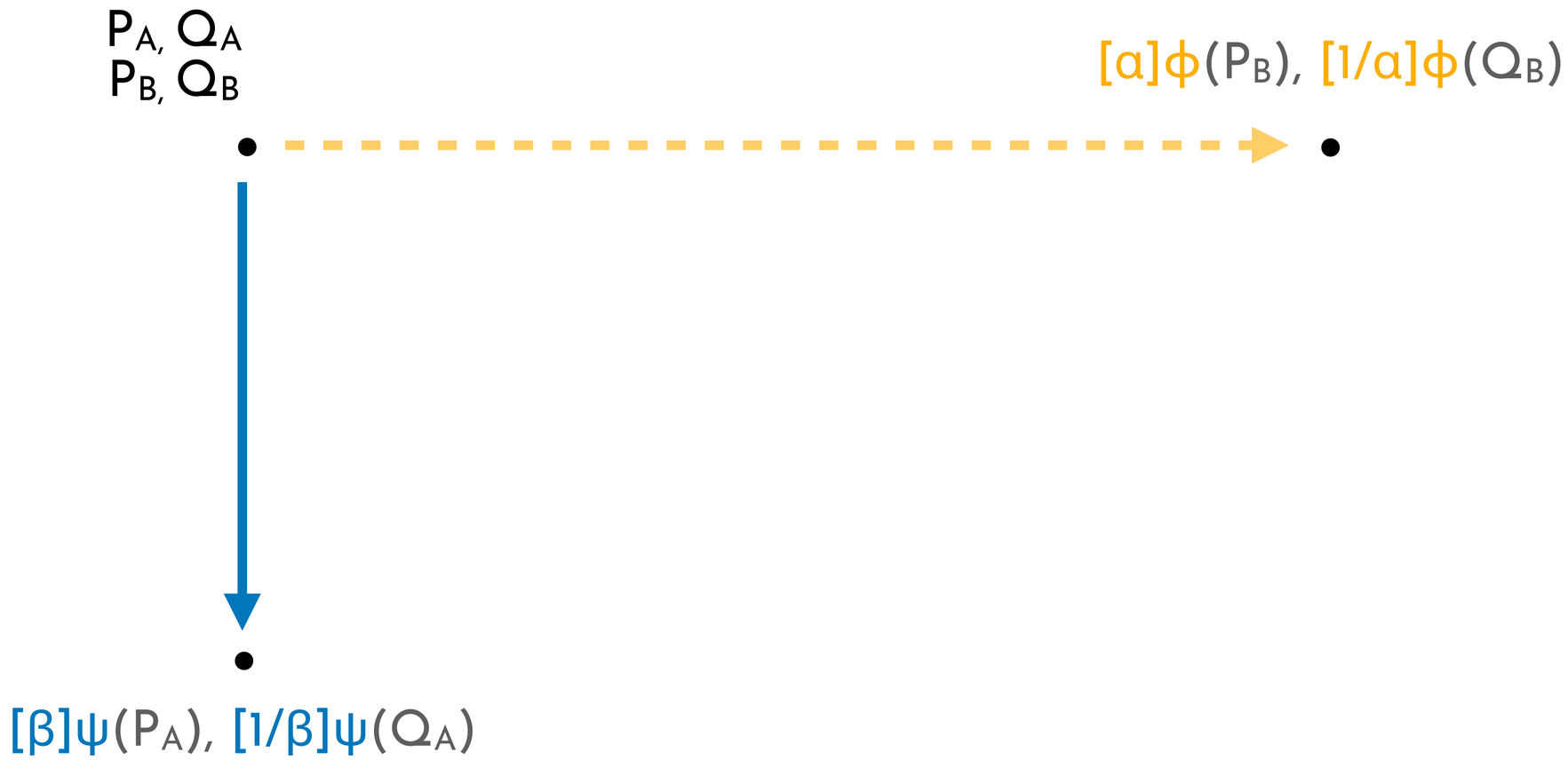
8. if bad, extract an endomorphism



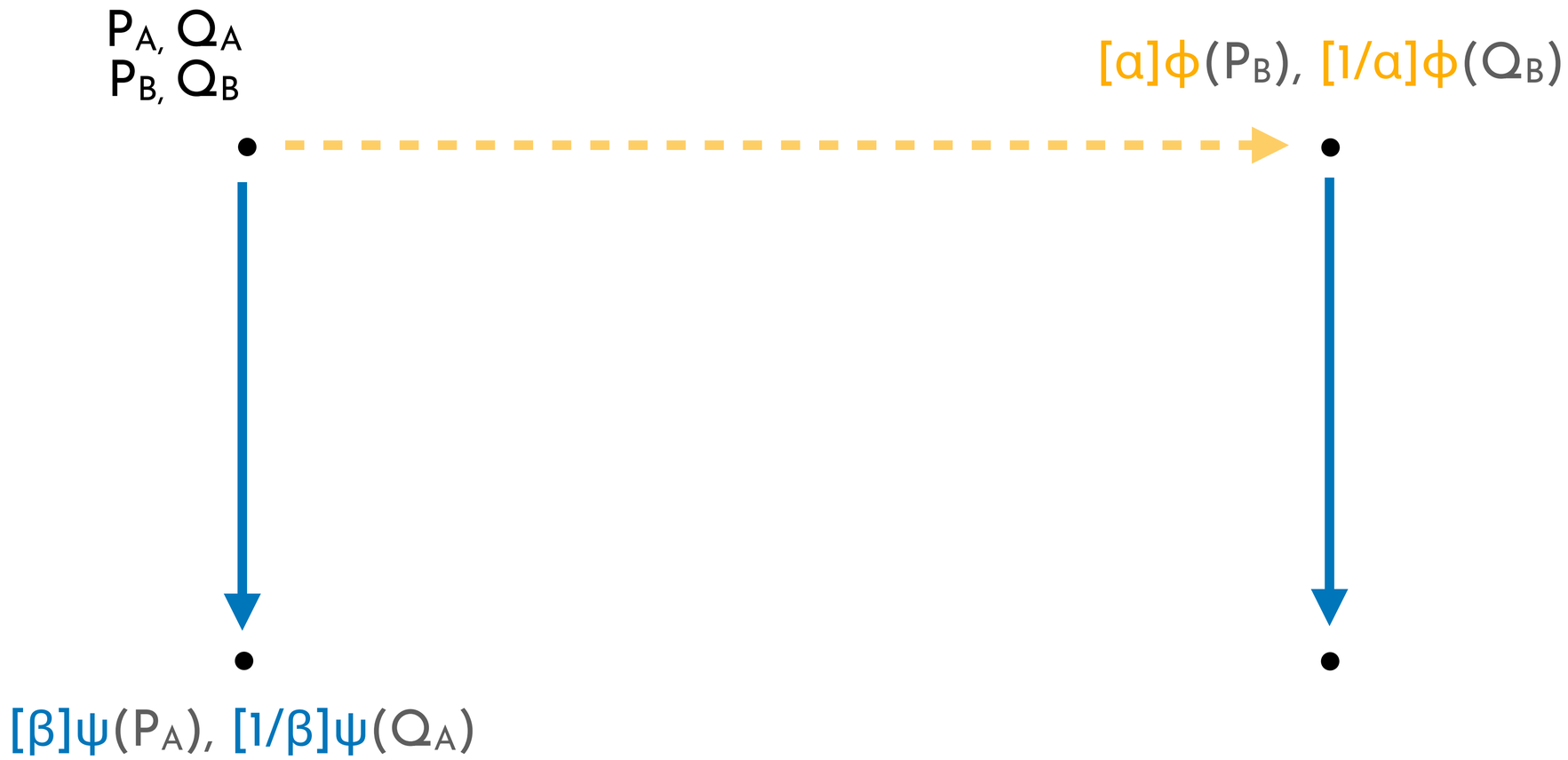
8. if bad, extract an endomorphism



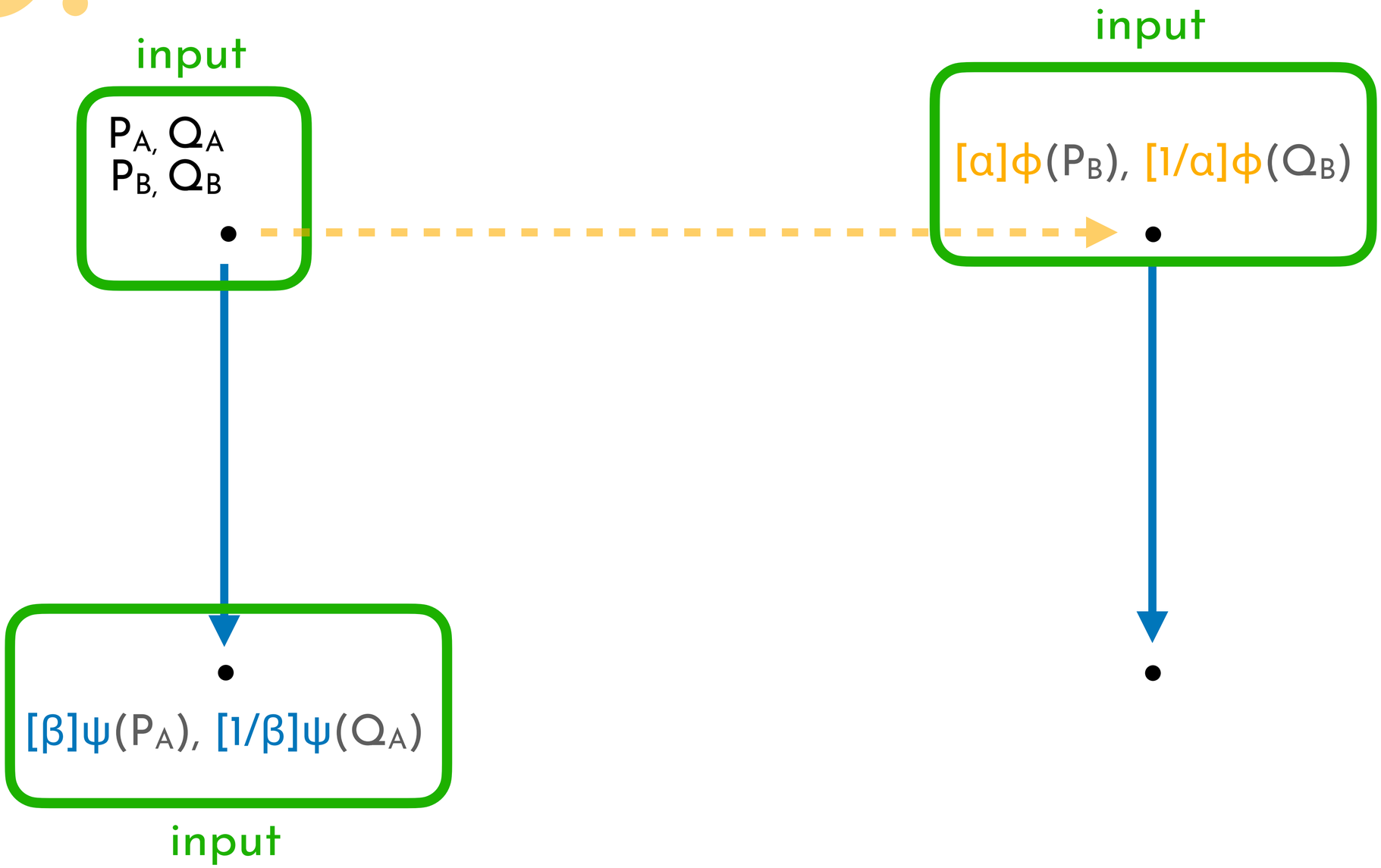
8. if bad, extract an endomorphism



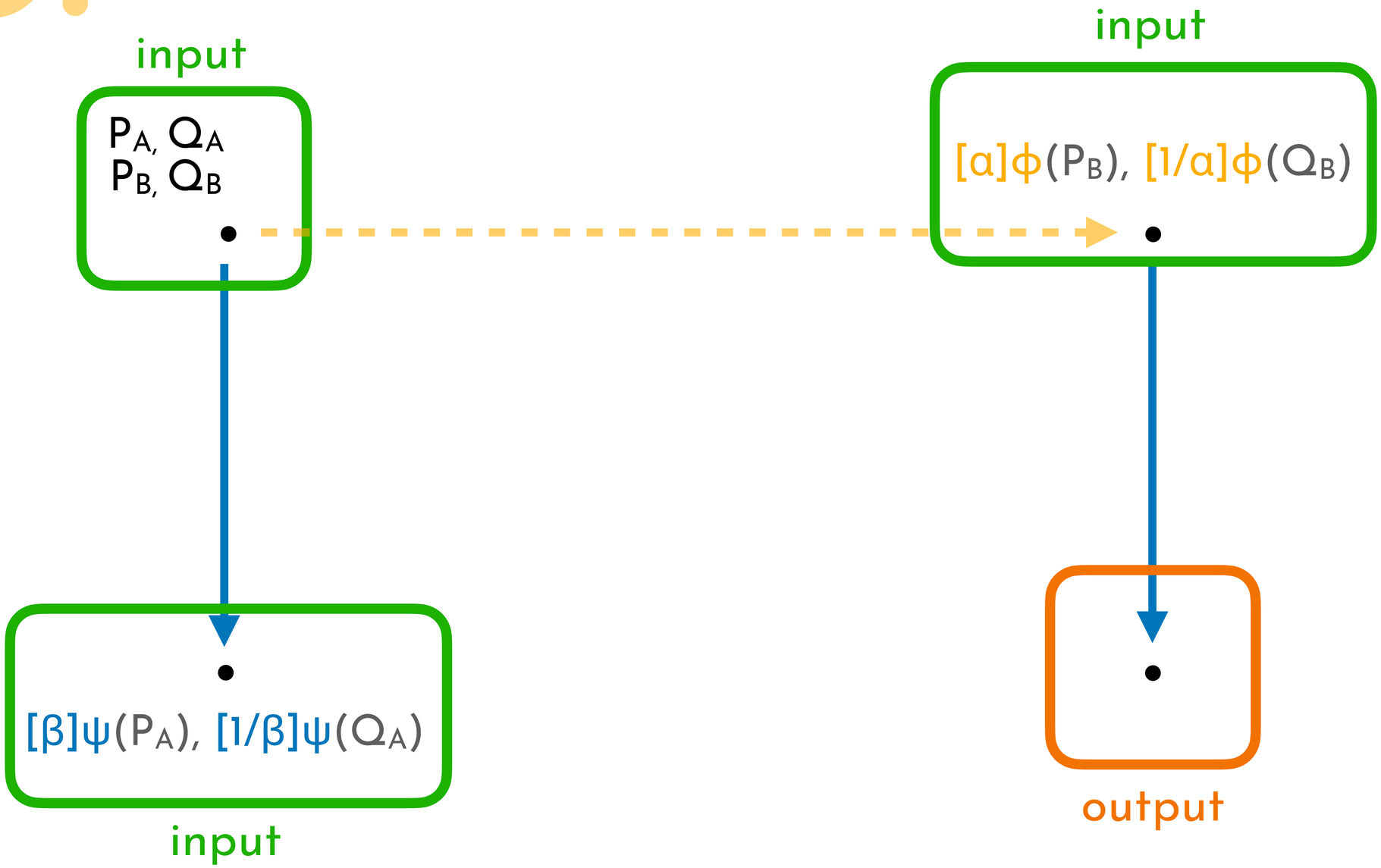
8. if bad, extract an endomorphism



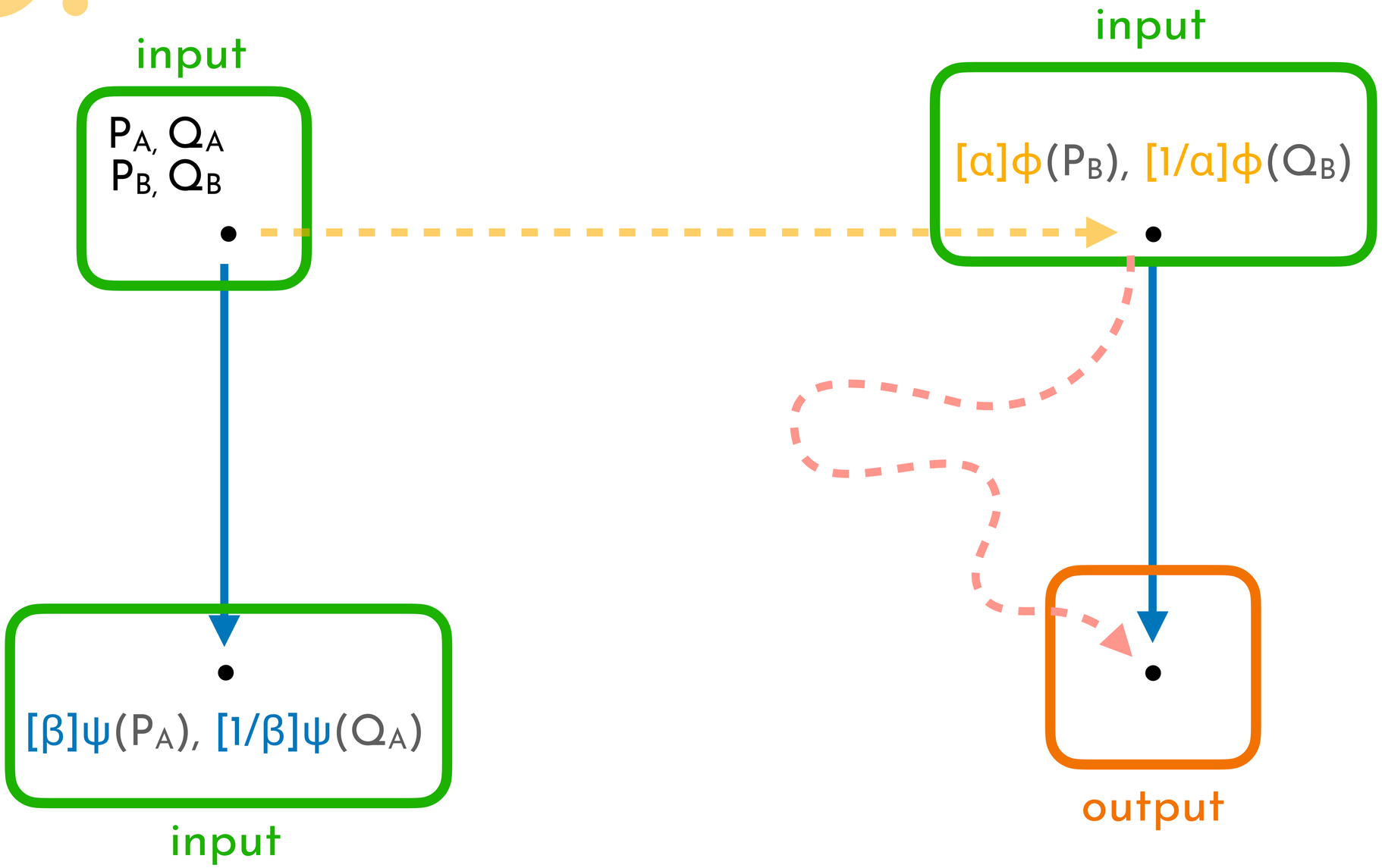
8. if bad, extract an endomorphism



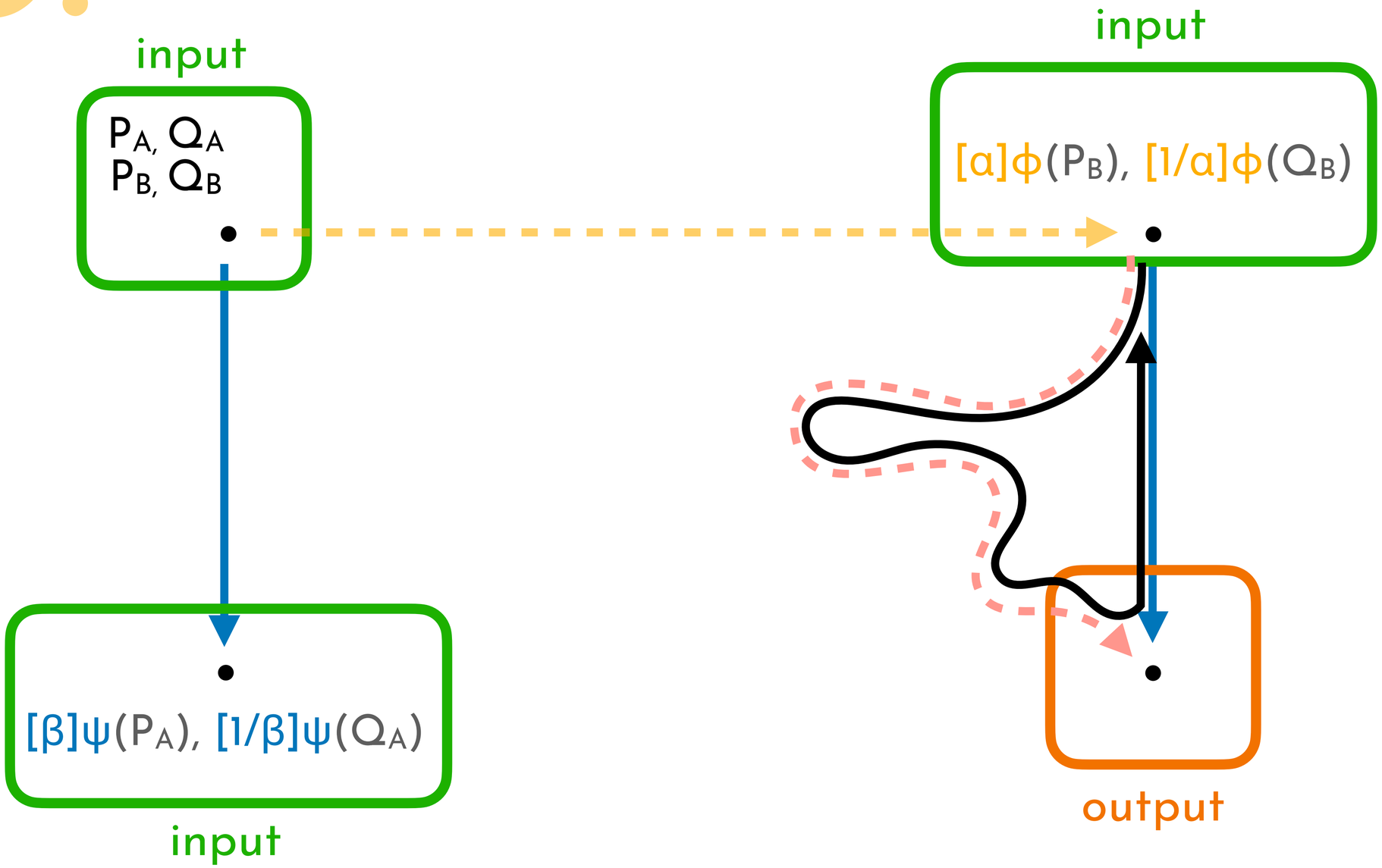
8. if bad, extract an endomorphism



8. if bad, extract an endomorphism



8. if bad, extract an endomorphism



9. repeat, until entire End ring is recovered

9. repeat, until entire End ring is recovered

10. from End ring, extract the secret*

DLOG to CDH reduction

DLOG to CDH reduction

1. guess which explanation the adversary produces

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**
    5. if the guess is incorrect, stop (and restart)

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**
    5. if the guess is incorrect, stop (and restart)
    6. handle each case separately:

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**
    5. if the guess is incorrect, stop (and restart)
    6. handle each case separately:
        7. **if the explanation is good, extract a secret**

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**
    5. if the guess is incorrect, stop (and restart)
    6. handle each case separately:
        7. **if the explanation is good, extract a secret**
        8. if the explanation is bad

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**
    5. if the guess is incorrect, stop (and restart)
    6. handle each case separately:
        7. **if the explanation is good, extract a secret**
        8. if the explanation is bad
            9. **extract an endomorphism**

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**
    5. if the guess is incorrect, stop (and restart)
    6. handle each case separately:
        7. **if the explanation is good, extract a secret**
        8. if the explanation is bad
            9. **extract an endomorphism**
            10. repeat until extracting the full End ring

DLOG to CDH reduction

1. **guess which explanation the adversary produces**
2. if the guess is incorrect, stop (and restart)
3. handle each case separately:
    4. **guess if the explanation is good**
    5. if the guess is incorrect, stop (and restart)
    6. handle each case separately:
        7. **if the explanation is good, extract a secret**
        8. if the explanation is bad
            9. **extract an endomorphism**
            10. repeat until extracting the full End ring
            11. extract the secret