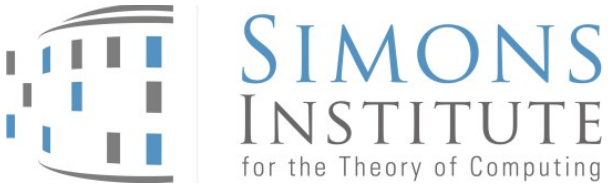
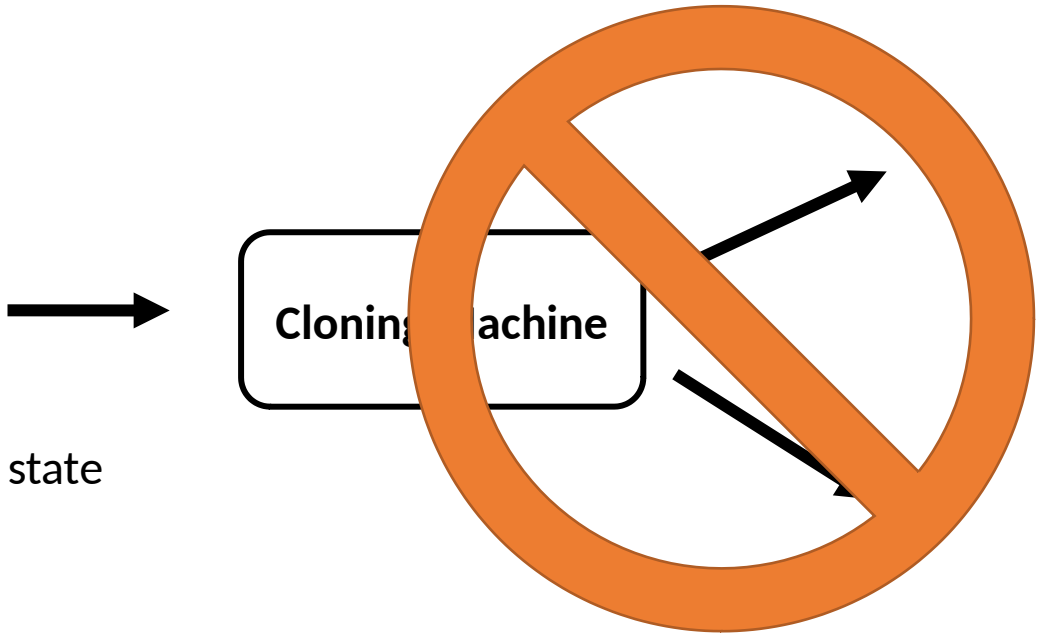
Hidden Cosets and Applications to Unclonable Cryptography

Andrea Coladangelo, Jiahui Liu, **Qipeng Liu**, and Mark Zhandry



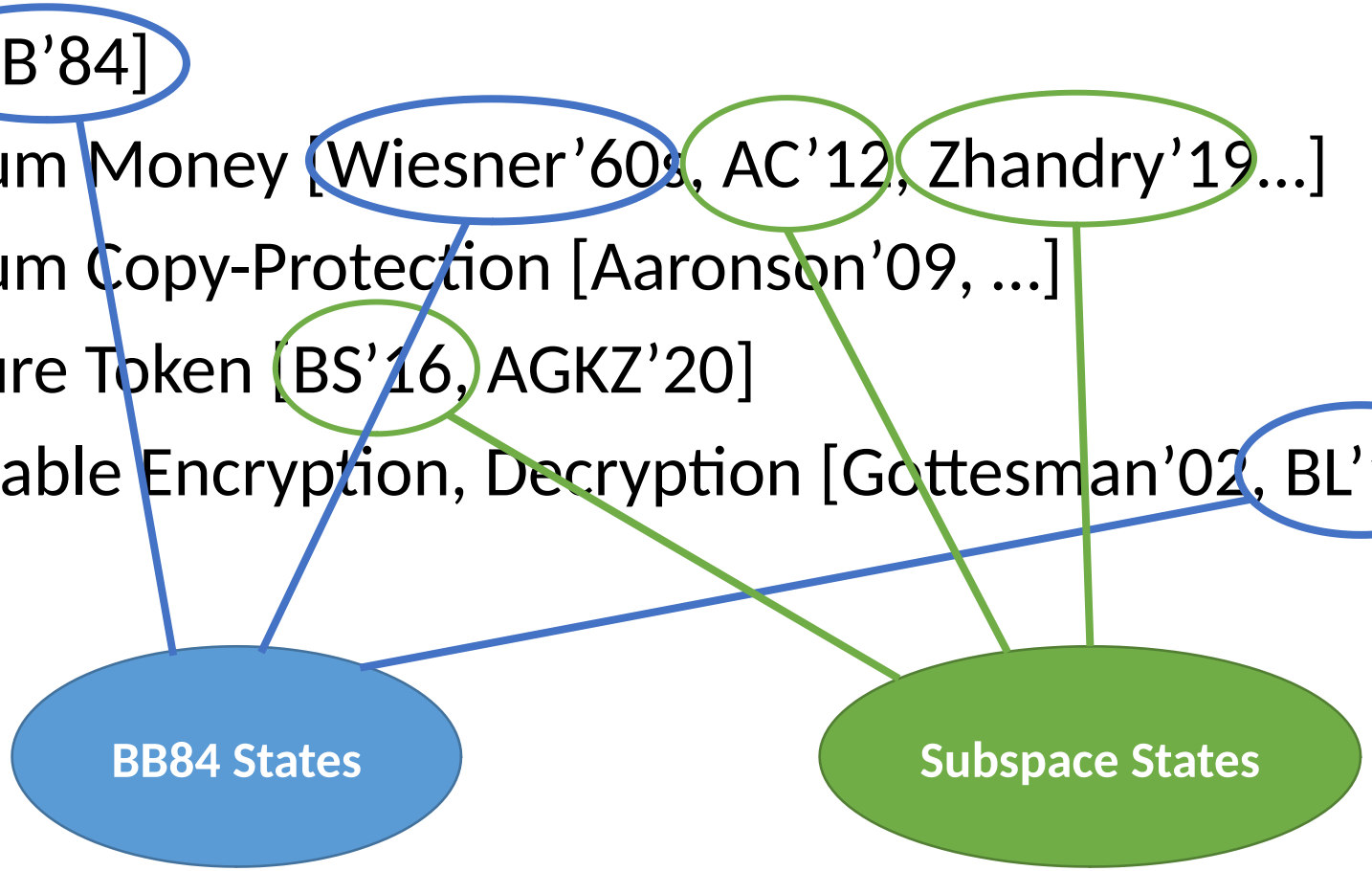
No-Cloning Theorem



unknown quantum state

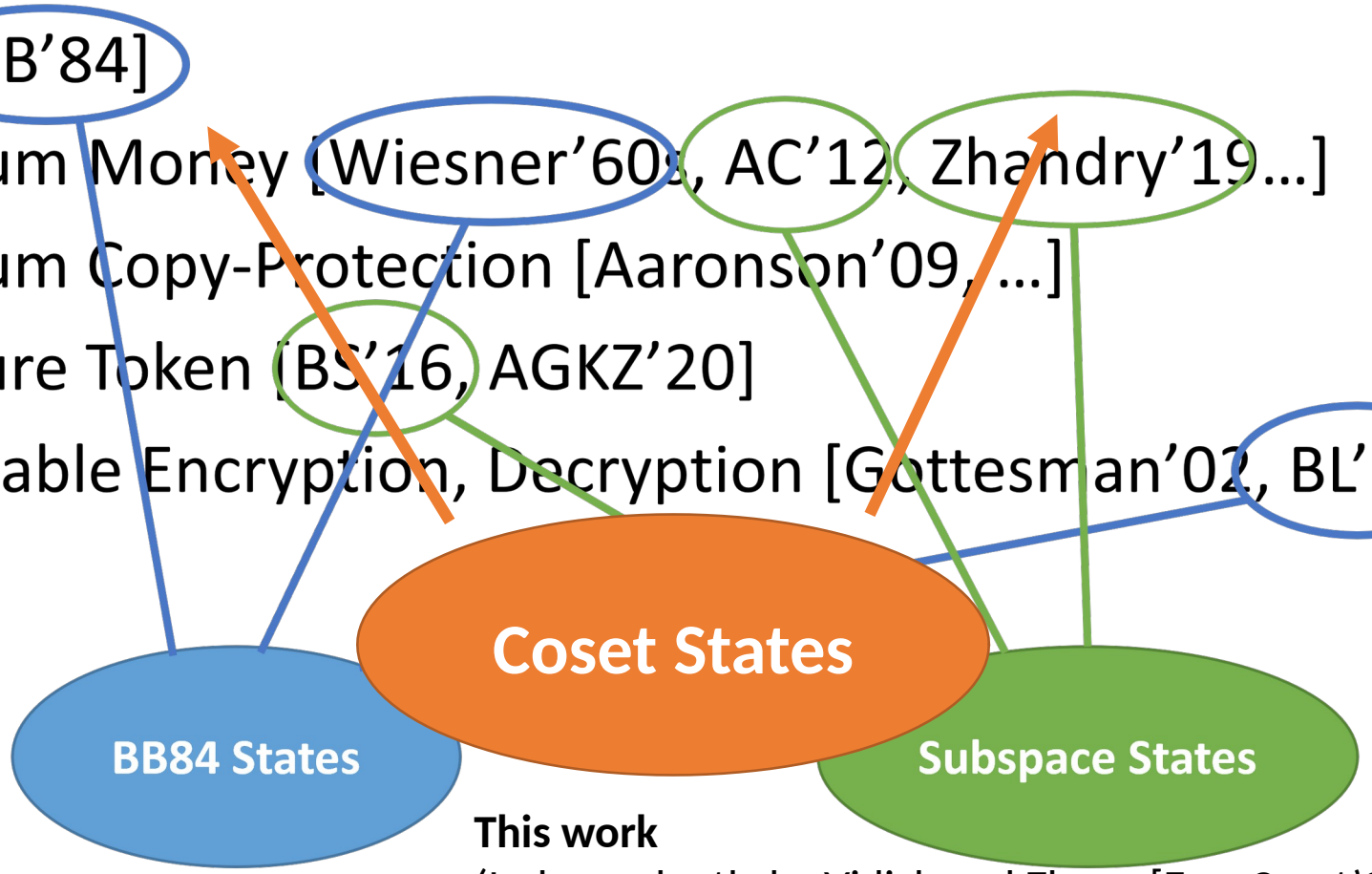
Classically Impossible Primitives

- QKD [BB’84]
- Quantum Money [Wiesner’60s, AC’12, Zhandry’19…]
- Quantum Copy-Protection [Aaronson’09, …]
- Signature Token [BS’16, AGKZ’20]
- Unclonable Encryption, Decryption [Gottesman’02, BL’19, GZ’20]
- …



Classically Impossible Primitives

- QKD [BB'84]
- Quantum Money [Wiesner'60s, AC'12, Zhandry'19…]
- Quantum Copy-Protection [Aaronson'09, …]
- Signature Token [BS'16, AGKZ'20]
- Unclonable Encryption, Decryption [Gottesman'02, BL'19, GZ'20]
- …



This work
(Independently by Vidick and Zhang [EuroCrypt'21])

Previous Results

	Signature Token	Unclonable Decryption
Subspace States	VBB [BS'16]	VBB [GZ'20]

- These results are proved relative to oracles/VBB.

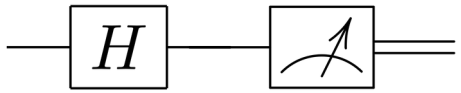
Our Results

	Signature Token	Unclonable Decryption	Copy-Protection PRF
Subspace States	VBB [BS'16]	VBB [GZ'20]	Not known
Coset States	iO + OWF [This Work]	iO + OWF* [This Work]	iO + OWF* [This Work]

* We need additionally conjecture coset states have a strong `monogamy-of-entanglement' property. The property is proved in a follow-up work by Culf and Vidick: https://arxiv.org/abs/2107.13324

Subspace States [Aaronson-Christiano'12]

- Hidden subspace state for some unknown space



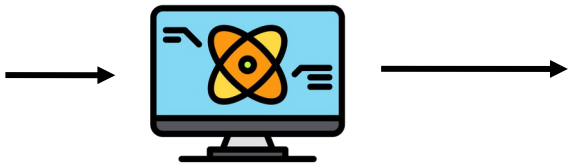
Definition:

- Let , be the membership checking programs for and

Subspace Stat

Definition:

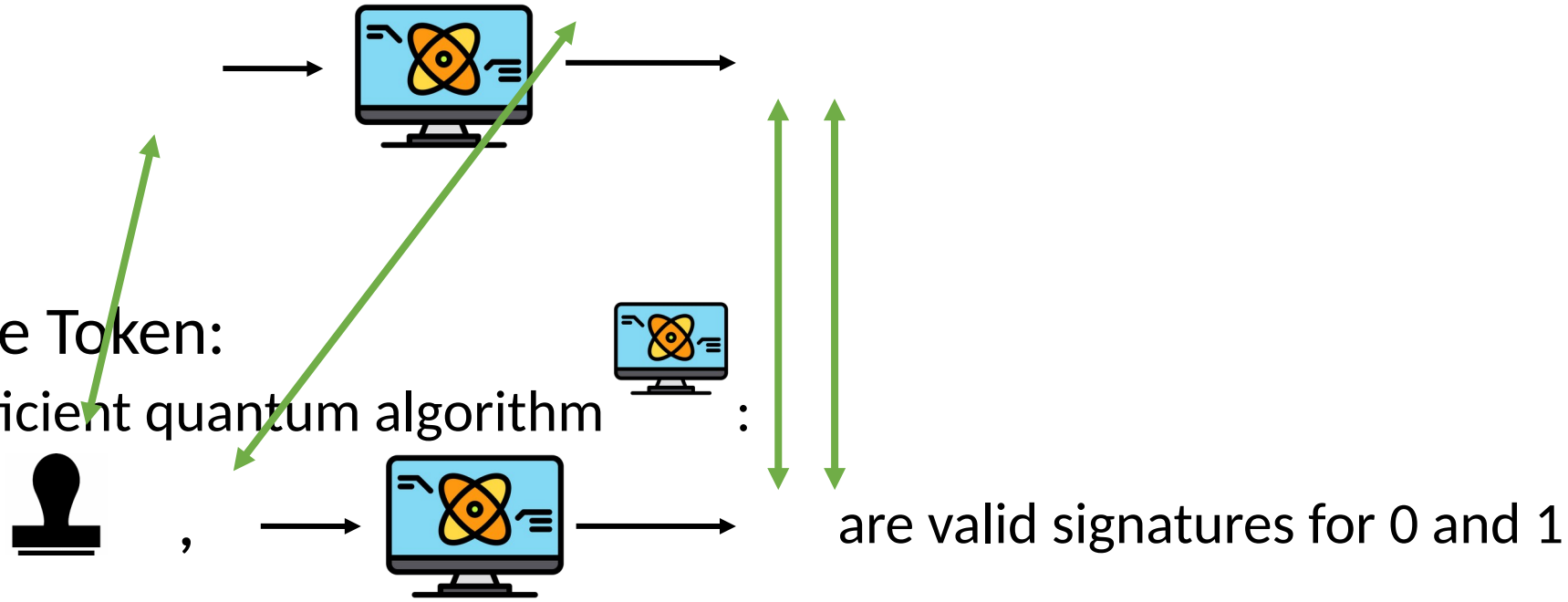
- Direct-Product Hardness [Ben-David and Sattath'16]:
  - No (query-bounded) quantum algorithm  :



Subspace Stat

Definition:

- Direct-Product Hardness [Ben-David and Sattath'16]:
  - No (query-bounded) quantum algorithm  :



- Signature Token:
  - No efficient quantum algorithm :

 , are valid signatures for 0 and 1

Signature Token in the Plain Model?

- ? 

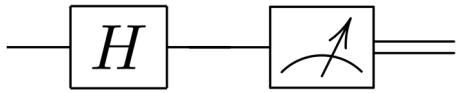
- Similar ideas were deployed to achieve quantum money in the plain model:
  - Rely on **a weaker property** of subspace states.
  - [AC'12]: quantum money relative to classical oracles
  - [Zha'19]: same construction, but iO + OWF

- Apply to direct product hardness? **No!** The same reduction fails.

Coset States [This Work]

- Hidden coset state
  - for unknown space and unknown vector

+s

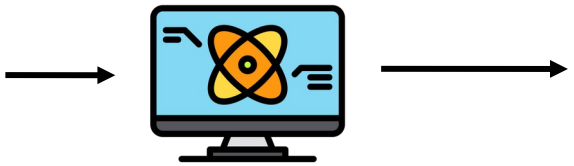


Definition:

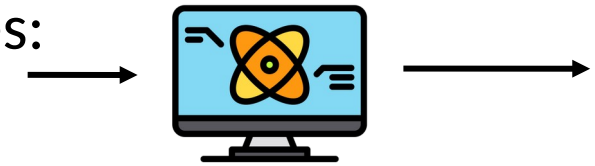
- Let , be the membership checking programs.

Coset States

- Direct-Product Hardness [This Work]:
  - No (query-bounded) quantum algorithm  :



  - Subspace states:



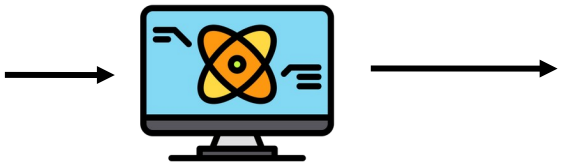
Removing Oracles/VBB

- 

- Achieve the followings in the plain model:
  - direct-product hardness
  - signature token

- No QPT algorithm  :

Computational Direct-Product Hardness



Ideas

- **Hyb 0**:

- **Hyb 1**:

  where and , , random

- **Hyb 2**:

  where and ,

  ,

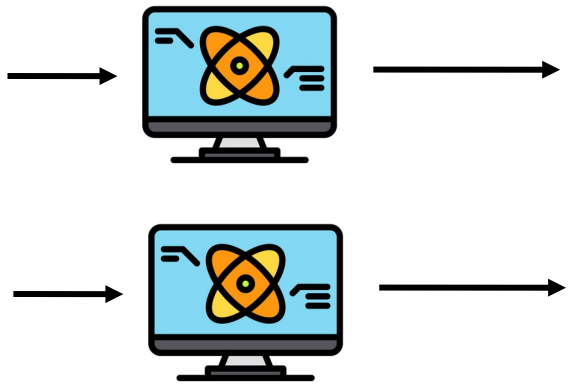
Ideas (cont’d)

- **Hyb 2**:

  where and ,

  ,

- No QPT algorithm :



Conclusion(Part 1)

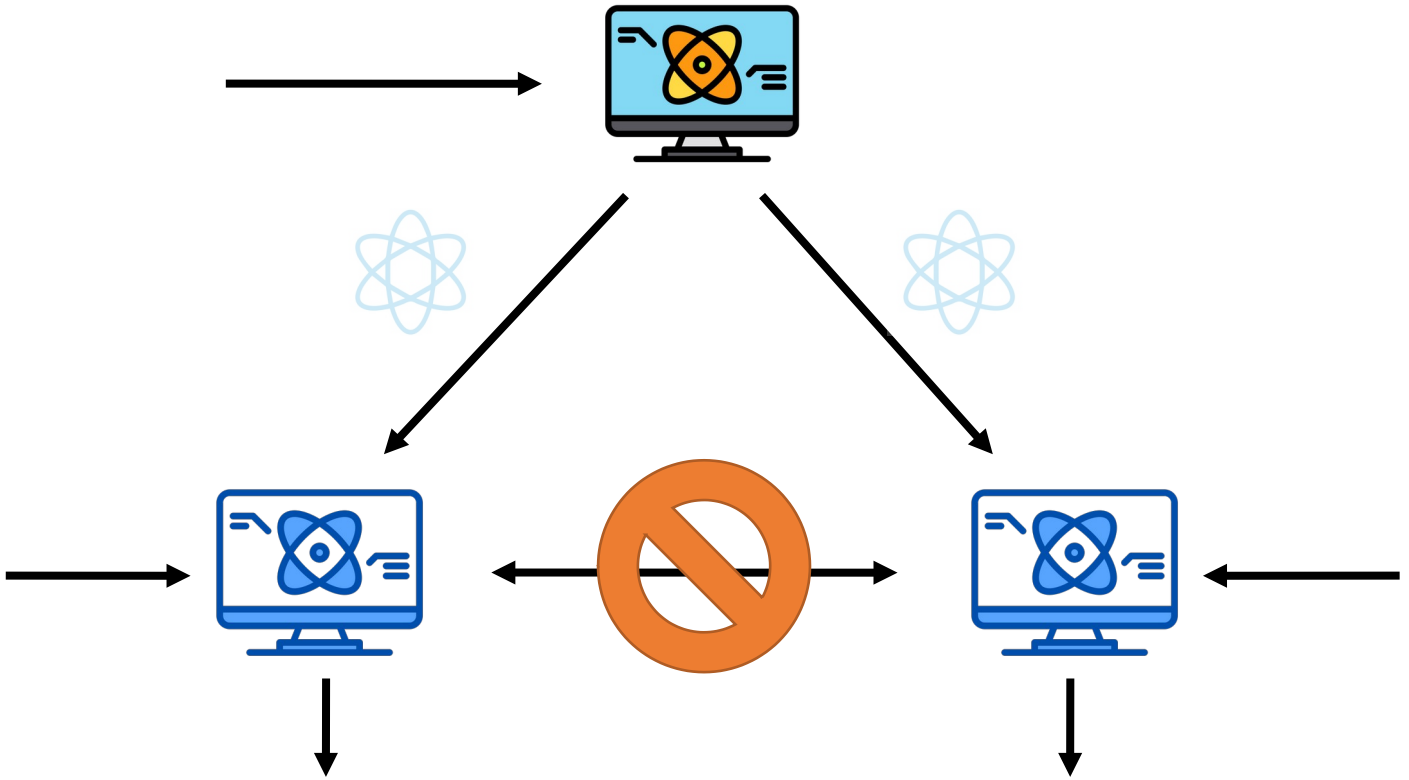
Theorem: Coset states satisfy *computational direct-product hardness*, assuming iO and OWF.

Corollary: There exists *signature token schemes* in the plain model.

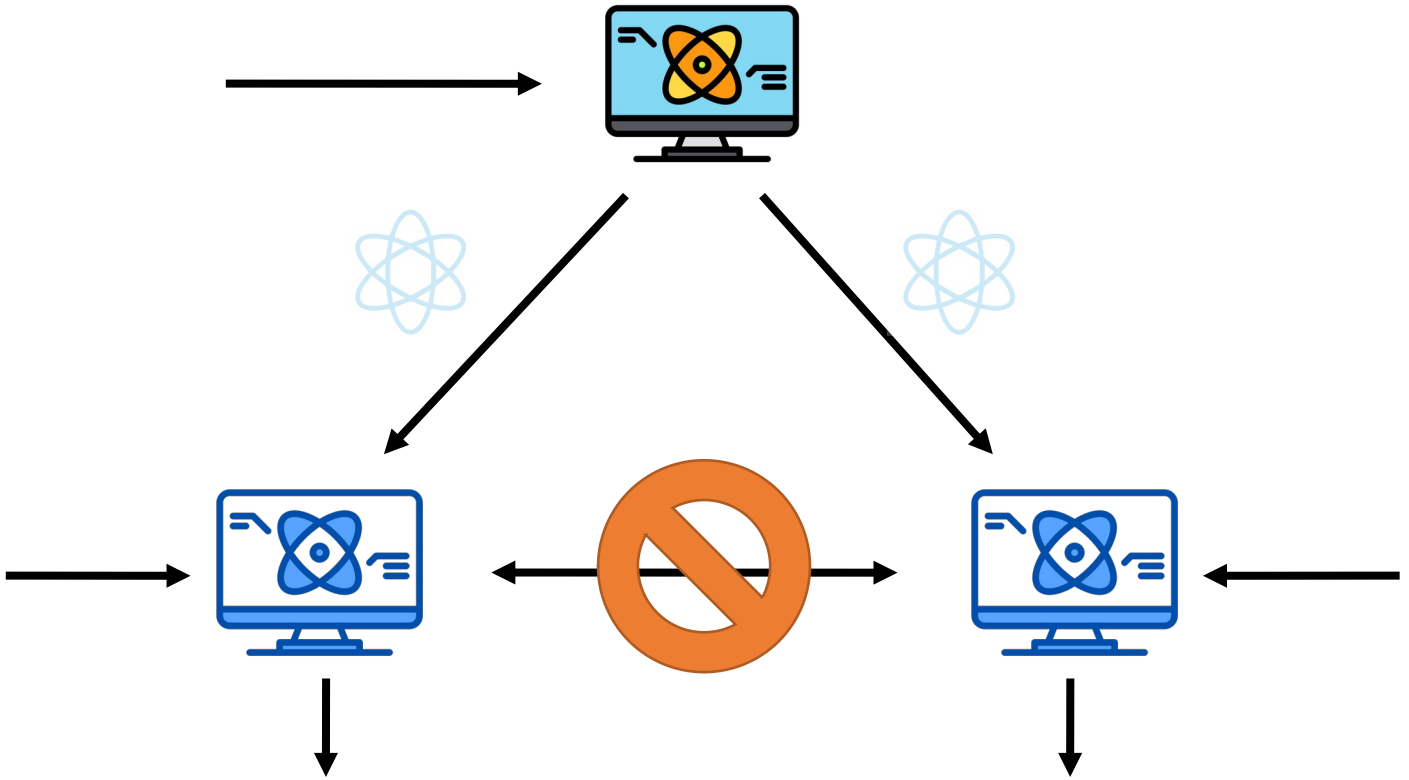
Monogamy of Entanglement (MOE)

- Studied in [Tomamichel, Fehr, Kaniewski, Wehner’ 13] for BB84 states

MOE game



(Conjectured) Strong MOE game [Culf, Vidick 21]



Unclonable Decryption

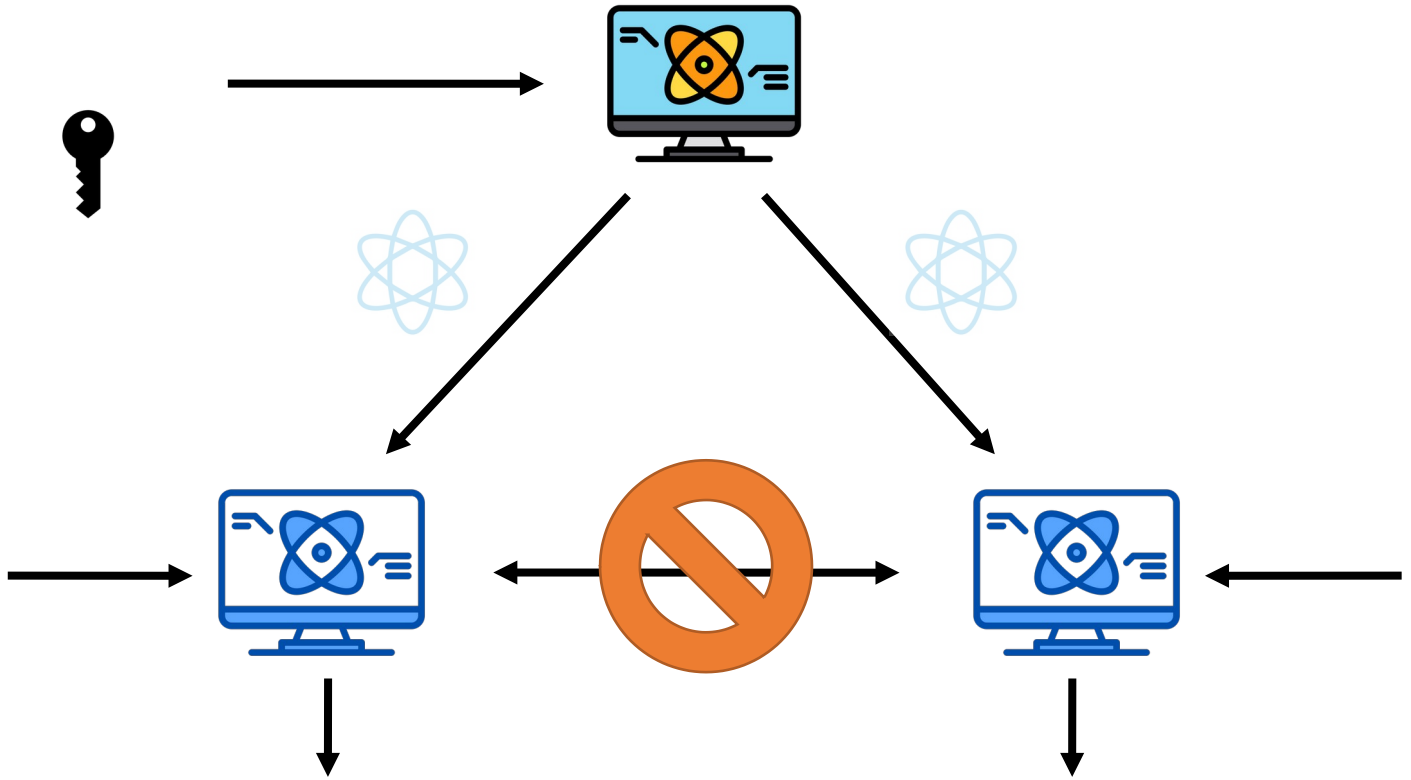
- **KeyGen**(): outputs 
- **Enc**(): outputs
- **Dec**( ,): outputs

Enc():
flip a coin
output ()

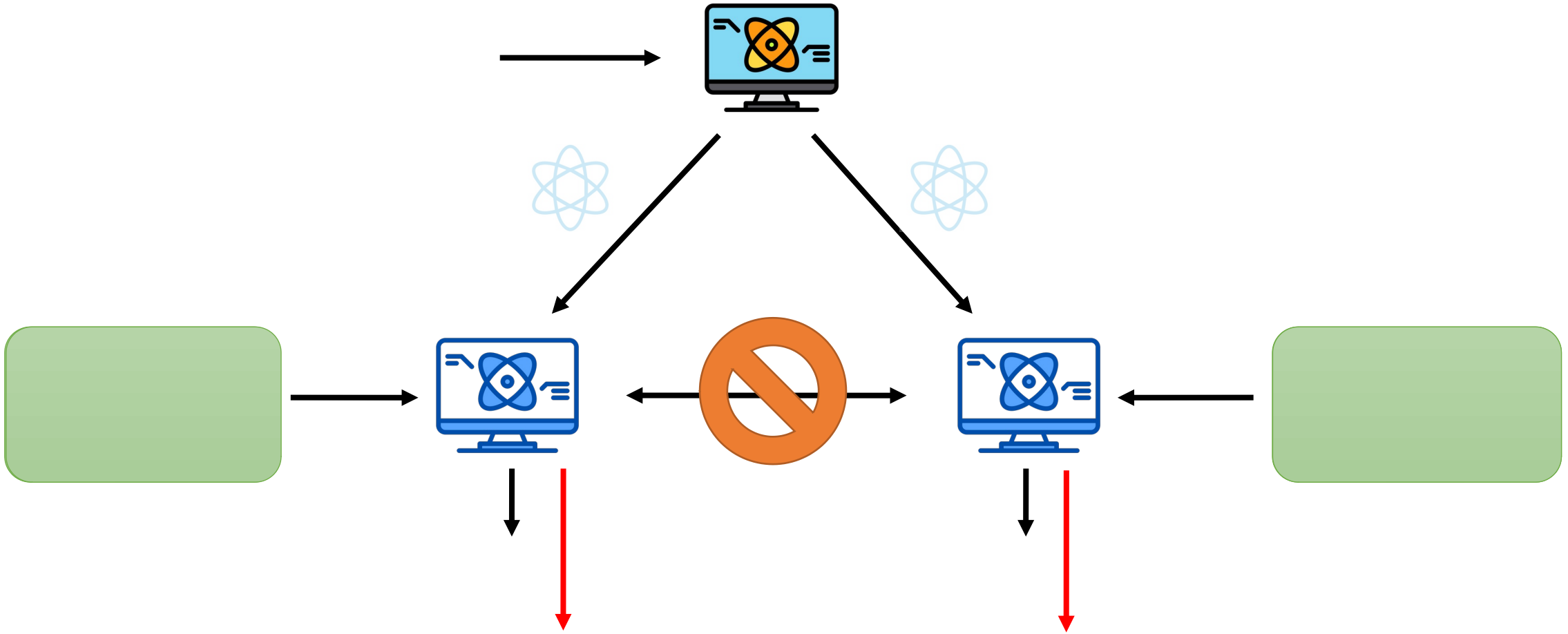
output
iff

output
iff

Unclonability of Decryption Key



Unclonability of Decryption Key



Conclusion(Part 2)

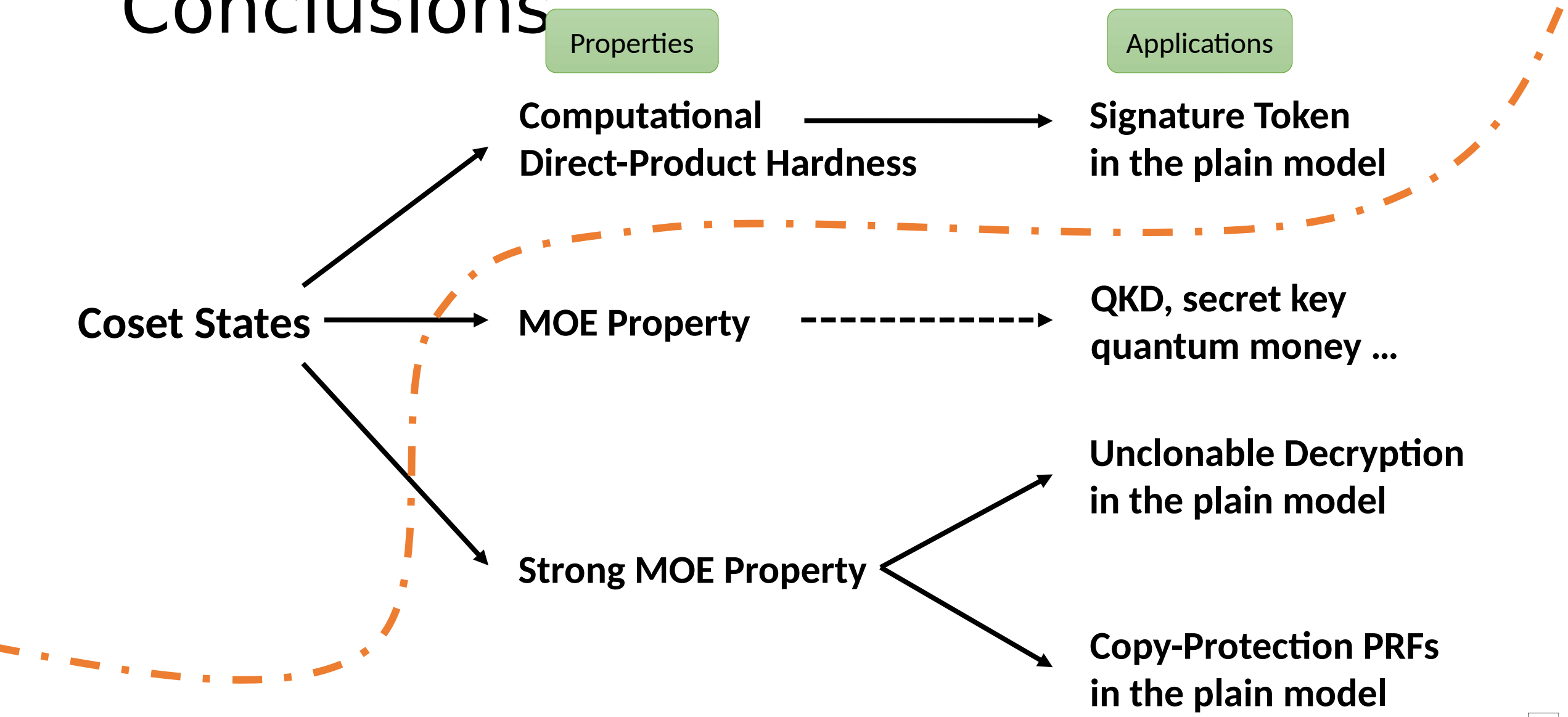
Theorem: Coset states satisfy *computational MOE/strong MOE*, assuming iO and OWF.

Theorem: There exists *unclonable decryption* in the plain model.

`Hidden Trigger' in [Sahai, Waters'14, ...]

Theorem: There exist *copy-protection PRFs* in the plain model.

Conclusions



Thank you!