Collusion-Resistant Copy-Protection for Watermarkable Functionalities

Jiahui Liu, Qipeng Liu, Luowen Qian and Mark Zhandry

TEXAS The University of Texas at Austin

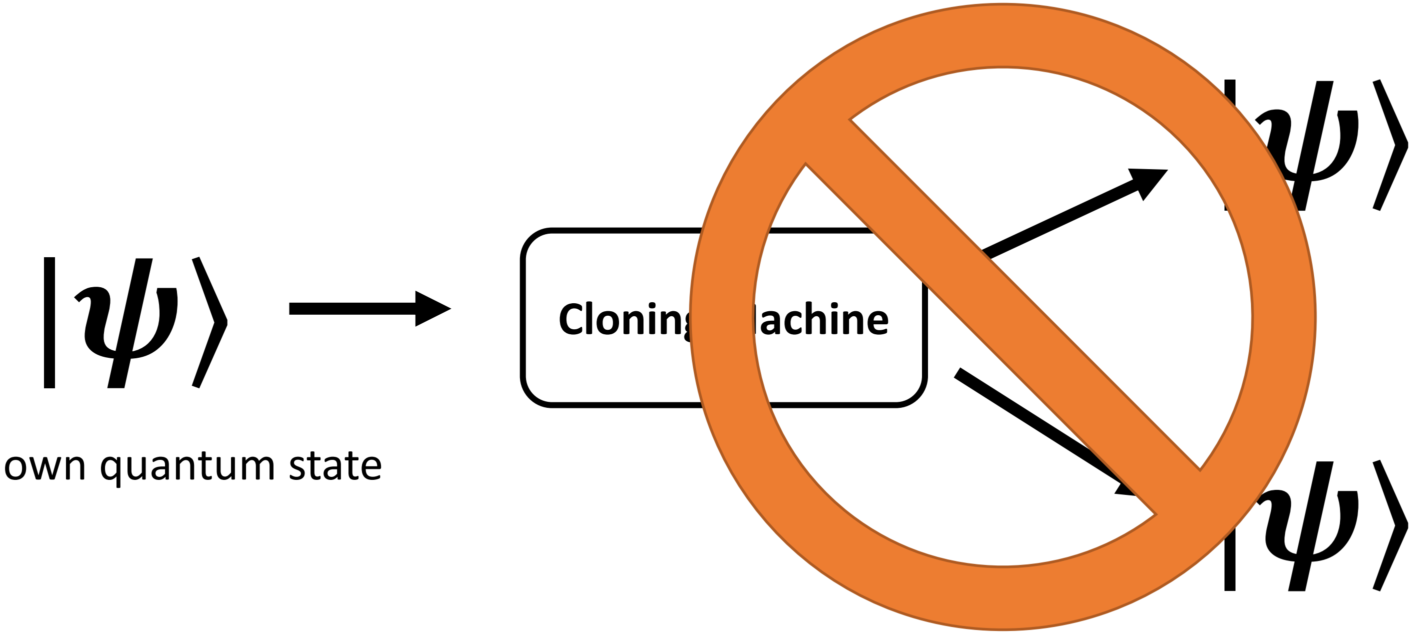
SIMONS INSTITUTE for the Theory of Computing

BOSTON UNIVERSITY

PRINCETON UNIVERSITY

NTT Research

No-Cloning Theorem



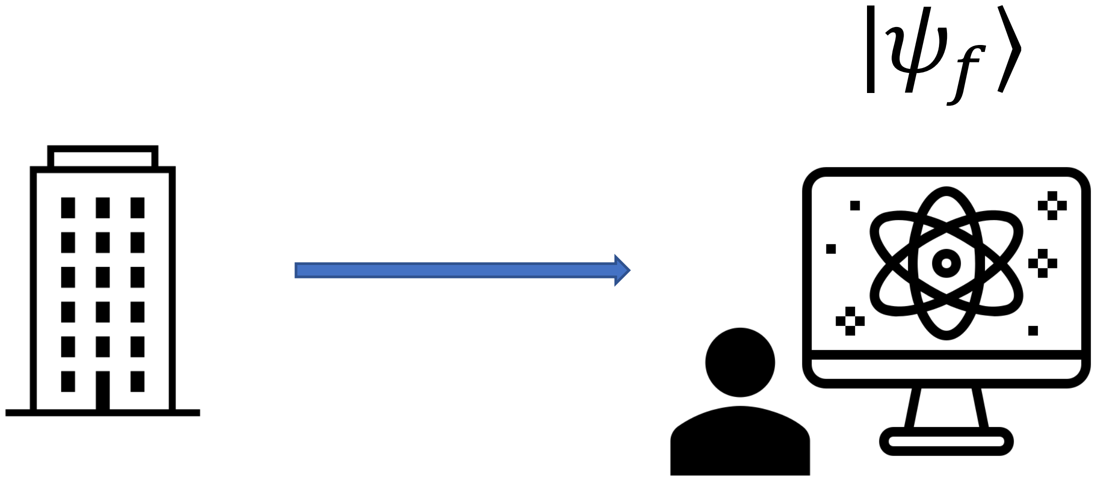
Classically Impossible Primitives

- QKD [BB’84]
- Quantum Money [Wiesner’69, AC’12, Zhandry’19…]
- Quantum Copy-Protection [Aaronson’09, CLLZ’21 …]
- Signature Token [BS’16, AGKZ’20, CLLZ’21]
- Unclonable Encryption, Decryption [Gottesman’02, BL’19, GZ’20, CLLZ’21]
- …

Quantum Copy Protection

Can we obtain unclonable states with ”functionalities”?

[Aaronson09]: Quantum Copy Protection for softwares

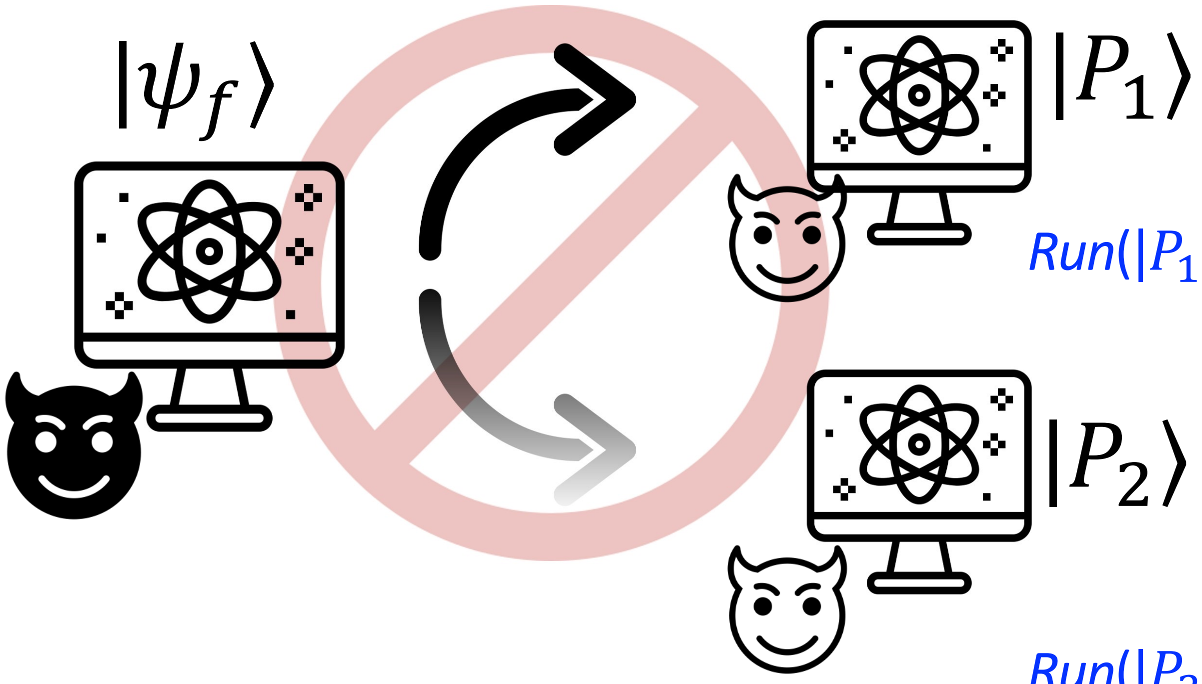


Classical: $f \xrightarrow{\text{copy−protect}} |\psi_f\rangle$

$\not\forall x,\ Run(|\psi_f\rangle\ ,x)\ =\ f(x)$

Quantum Copy Protection

[Aaronson09]: Quantum Copy Protection for softwares



Run$(|P_1\rangle, x) = f(x)$?

Run$(|P_2\rangle, x) = f(x)$?

Detour: Watermarking

- Watermarking:
  - cannot remove watermark without destroying functionality
- Copy-protection:
  - cannot clone without destroying functionality

- Intuitively, goal of adversary is to create illegal copies
  - Watermarking is the classical analogy of copy-protection

- Known watermarkable functionalities: decryption, PRF, signatures
  - [CHN+15, KW17, YAL+19, GKM+19, …]

Some Previous Results

	Unclonable Decryption	Copy-Protection PRF	Unclonable Signing Key
VBB/Oracle	VBB [GZ20, ALL+21]	VBB [ALL+21]	VBB [ALL+21]
Plain Model	iO + OWF [CLLZ21]	iO + OWF [CLLZ21]	Not known

[ALL+21]: Can all watermarkable functions be copy-protected?

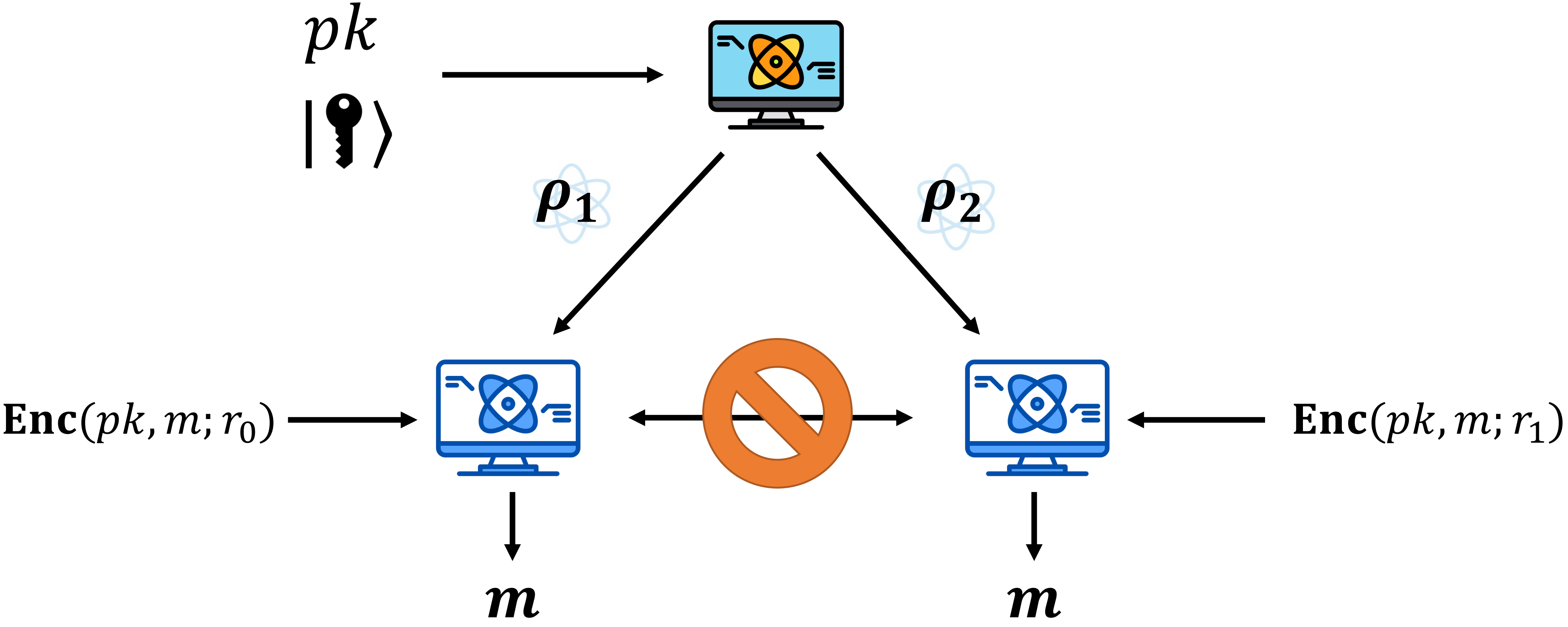
Unclonable Decryption (1->2) [CLLZ’21]

- **KeyGen**(λ): outputs pk, |🔑⟩

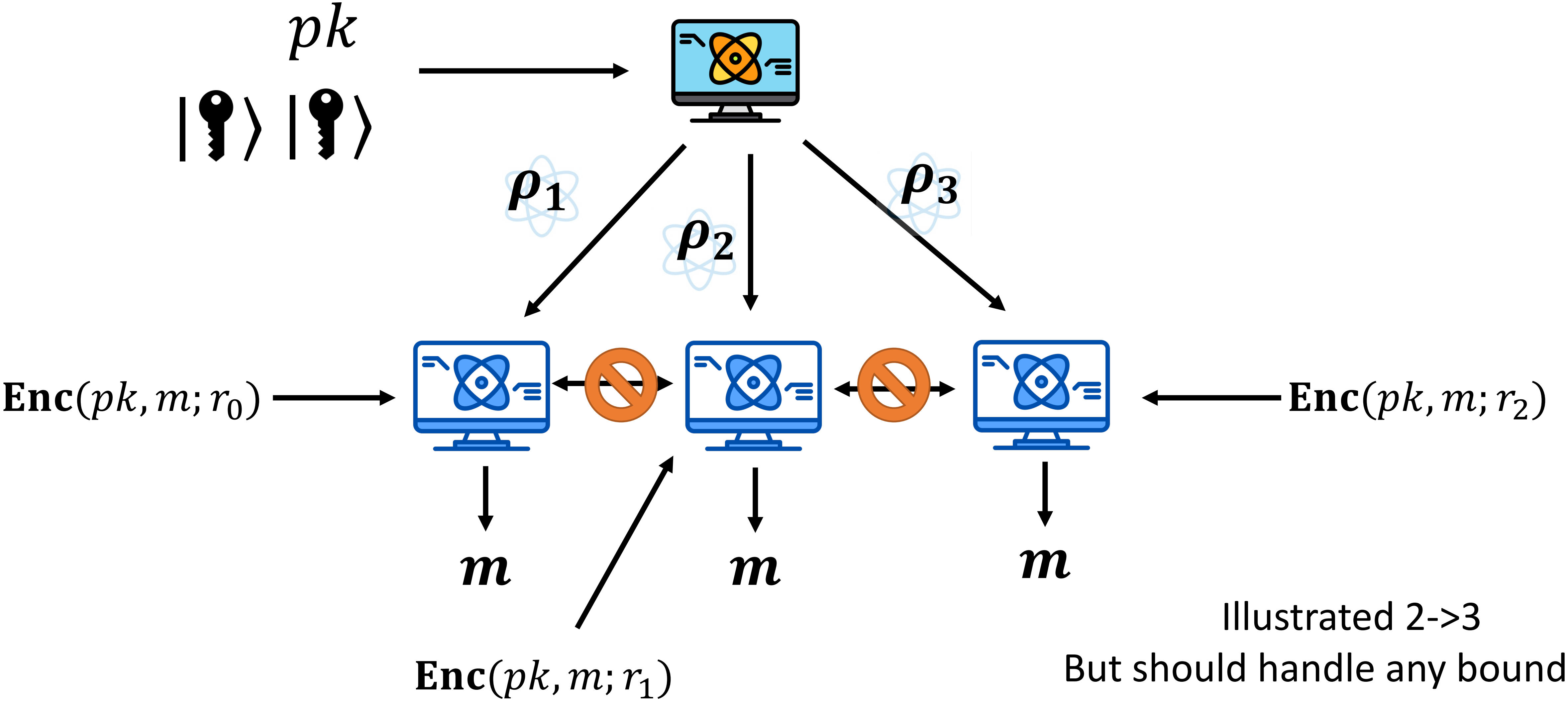
- **Enc**(pk, m): outputs c

- **Dec**(|🔑⟩, c): outputs m

Unclonable Decryption Key[GZ20,CLLZ21]



Collusion-Resistance (k->k+1)



pk

$|🔑\rangle\,|🔑\rangle$

$\boldsymbol{\rho_1}$

$\boldsymbol{\rho_2}$

$\boldsymbol{\rho_3}$

$\mathbf{Enc}(pk, m; r_0)$

$\mathbf{Enc}(pk, m; r_2)$

$\boldsymbol{m}$

$\boldsymbol{m}$

$\boldsymbol{m}$

$\mathbf{Enc}(pk, m; r_1)$

Illustrated 2->3

But should handle any bounded k

Previous Results

	Unclonable Decryption	Copy-Protection PRF	Unclonable Signing Key
VBB/Oracles	VBB [GZ20]	VBB [ALL+21]	VBB [ALL+21]
Plain Model	iO + OWF [CLLZ21]	iO + OWF [CLLZ21]	Not known

Not Collusion-Resistant!

Our Results: Collusion-Resistant CP

	Unclonable Decryption	**Copy-Protection PRF**	**Unclonable Signing Key**
Plain Model	[This Work] iO + OWF	[This Work] iO + OWF	[This Work] iO + OWF

All Made Collusion Resistant!

Unclonable Decryption (2->3) [This Work]

- **KeyGen**(λ): outputs pk pk $\lvert$🔑$\rangle$ $\lvert$🔑$\rangle$

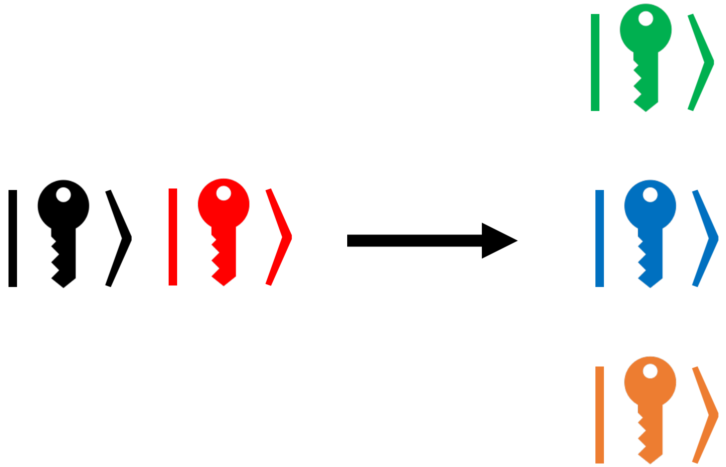
- **Enc**(pk, pk, m): outputs c=

  Enc(pk, m) **Enc**(pk, m)

- **Dec**($\lvert$🔑$\rangle$,$\lvert$🔑$\rangle$, c):
  - Use either key to decrypt any of the cipher $c = c_1\ c_2$

$c_1 \xrightarrow[\lvert 🔑 \rangle]{} m_1$ $c_2 \xrightarrow[\lvert 🔑 \rangle]{} m_2$

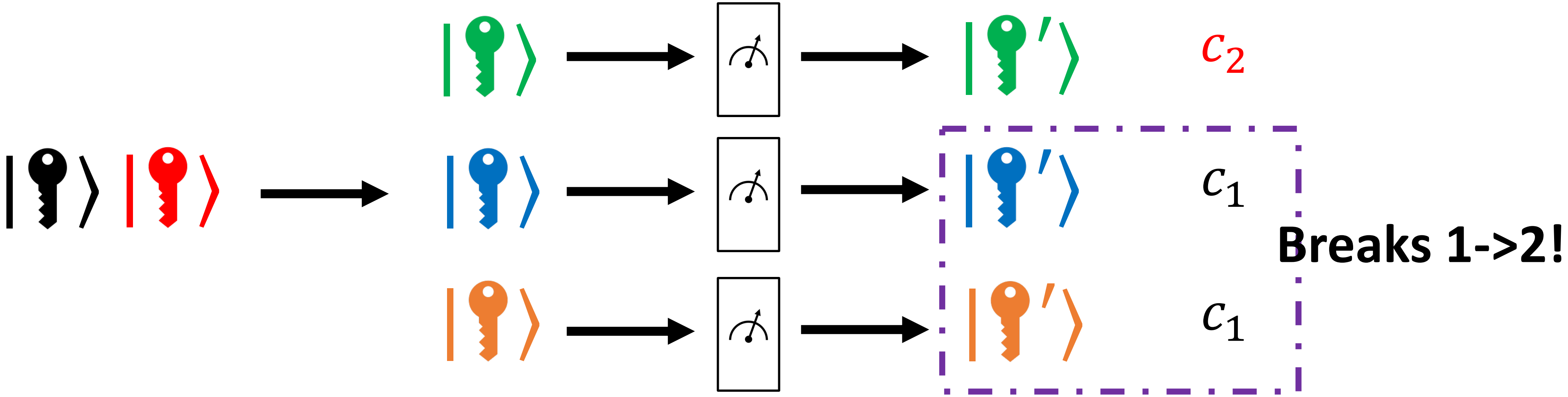
Reduction idea: reduce to 1-2 security



$c = c_1 \, {\color{red} c_2}$

- Produce three keys
- Each decrypts one of c_1 and ${\color{red} c_2}$
- (Classical) Pigeonhole principle?
  - **Not working!**

Reduction idea [This work]

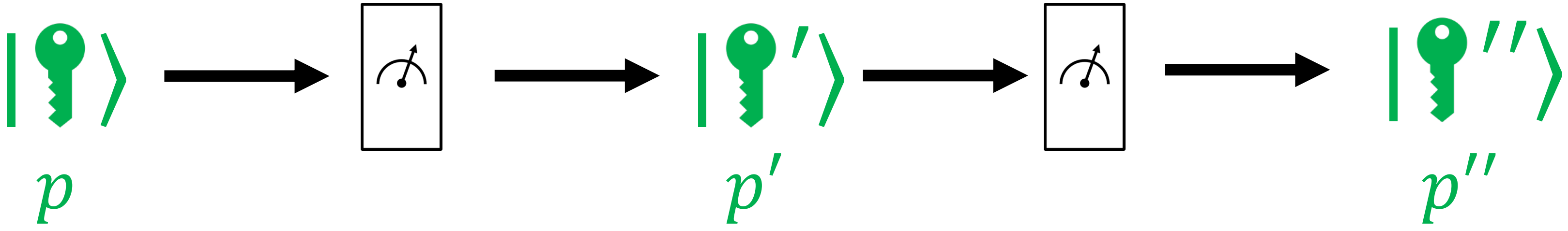


$c = c_1\ c_2$

Technique: Measure which ciphertext to decrypt

Technical Details: High-level

Pirate Decryotion keys:



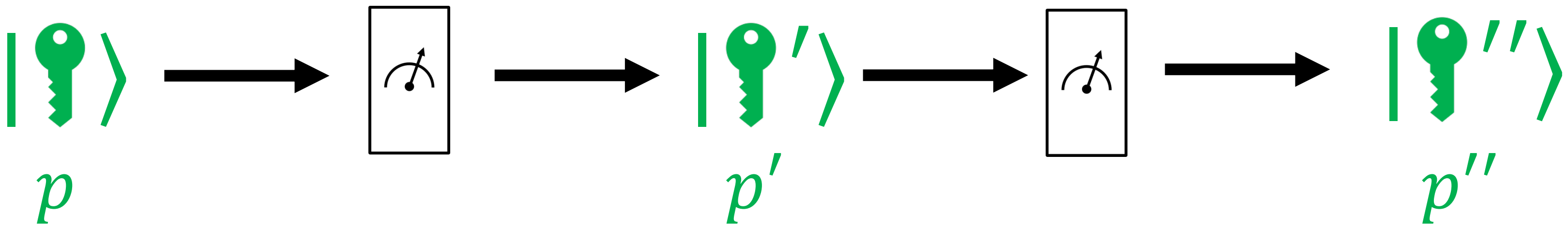
p p' p''

p: decryption probability over uniform $c = c_1\ c_2$

p': decryption probability over uniform $c = \perp\ c_2$

p'': decryption probability over uniform $c = \perp\ \perp$

Technical Details: High-level



p: decryption probability over uniform $c = c_1\ c_2$

p': decryption probability over uniform $c = \perp\ c_2$

If $p - p' \geq 1/\mathrm{poly}$, |🔑⟩ must decrypt c_1

More subtlety to handle!

Open Problems

- Unbounded Collusion-Resistant? i.e. KeyGen does not depend on number of keys issued
- Collusion-resistant copy protection for all unlearnable functions?

Thank you!