

Cloning Games: A General Framework for Unclonable Primitives

QCrypt 2023

Prabhanjan Ananth

UCSB

Fatih Kaleoglu

UCSB

Qipeng Liu

Simons
Institute

Unclonable Primitives

Unclonable Functionality ----- Primitive

- Ciphertext ----- Unclonable Encryption (UE)
- Decryption Key ----- Single-Decryptor Encryption (SDE)
- Function Evaluation ----- Copy-Protection (CP)
- Passing Public Verification ----- Public-Key Quantum Money
- ...

(Focus of this work)

Prior Work – Unclonable Encryption

- IT construction with weak security (BL '20)
- QROM construction from coset states (AKLLZ, '22)
- Variants
 - Public-Key (AK '21)
 - Independent Keys (KT '22)

Prior Work – Single-Decryptor Encryption

- GZ '20:
 - Equivalence to UE
 - Public-key construction from heavy assumptions
- Public-key construction from post-quantum IO (CLLZ '21)
- Relationship to Copy-Protection (SW '22)

Prior Work – Copy Protection

- Feasibility:
 - Compute & Compare functions in QROM (CMP '20)
 - Point functions in QROM (AKLLZ '22)
- Impossibility:
 - Plain model (AL '20)
 - Classical-Accessible Random Oracle Model (AK '22)

How to Improve Prior Work?

- Most works focus on feasibility.
- Limited work on understanding the relationship between different primitives (CMP '20, AK '21, SW '22)
- Need to understand better the applicability of different techniques in the literature

Why Study the Relationship between Unclonable Primitives?

- What computational assumptions are necessary for each primitive?
 - Classical Cryptography: Impagliazzo's 5 worlds and BB separations
 - Unclonable Cryptography: Implications/separations mostly unknown
- Types of States
 - Wiesner (BB84) states; prepare & measure
 - Coset states; entangled

Why Study the Relationship between Unclonable Primitives? (continued)

- Challenge distributions: independent vs. identical
 - SDE results are for different challenge distributions (GZ '20, CLLZ '21)
 - Lack a good understanding of how they relate
- Using existing classical techniques
 - Hybrid method
 - Goldreich-Levin

Contributions (Results)

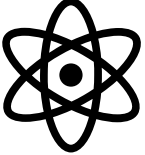
1. First IT-secure construction of SDE in the plain model
2. UE in QROM [from Wiesner \(BB84\) states](#) (*)
3. CP for single-bit point functions in QROM [from Wiesner \(BB84\) states](#) (*)
4. Show relationship between identical/independent-challenge security for SDE/CP
5. New construction of Encryption with Certified Deletion. (*)

(*) Simplified security proof

Contributions (Conceptual)

- New framework for unclonable primitives: Cloning Games
- General theorem statements for cloning games which imply the results for unclonable primitives.

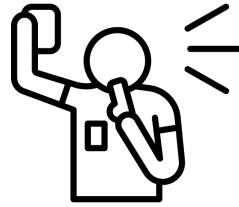
Cloning Games (Idea)

Quantum token  that can be verified.

Passing verification functionality is unclonable.

Cloning Games

- Security game between



Referee

and



Alice



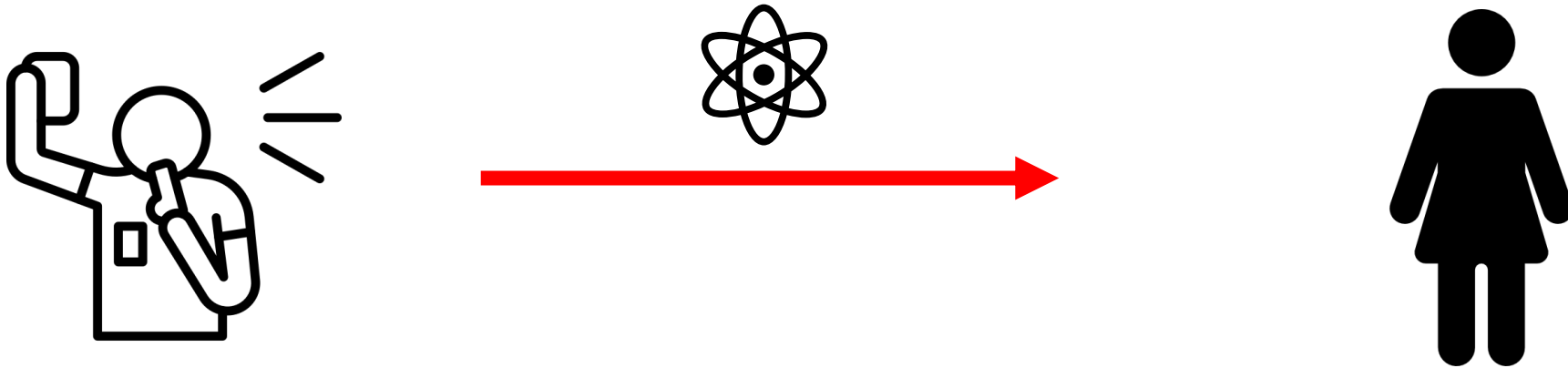
Bob

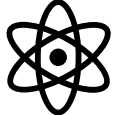


Charlie

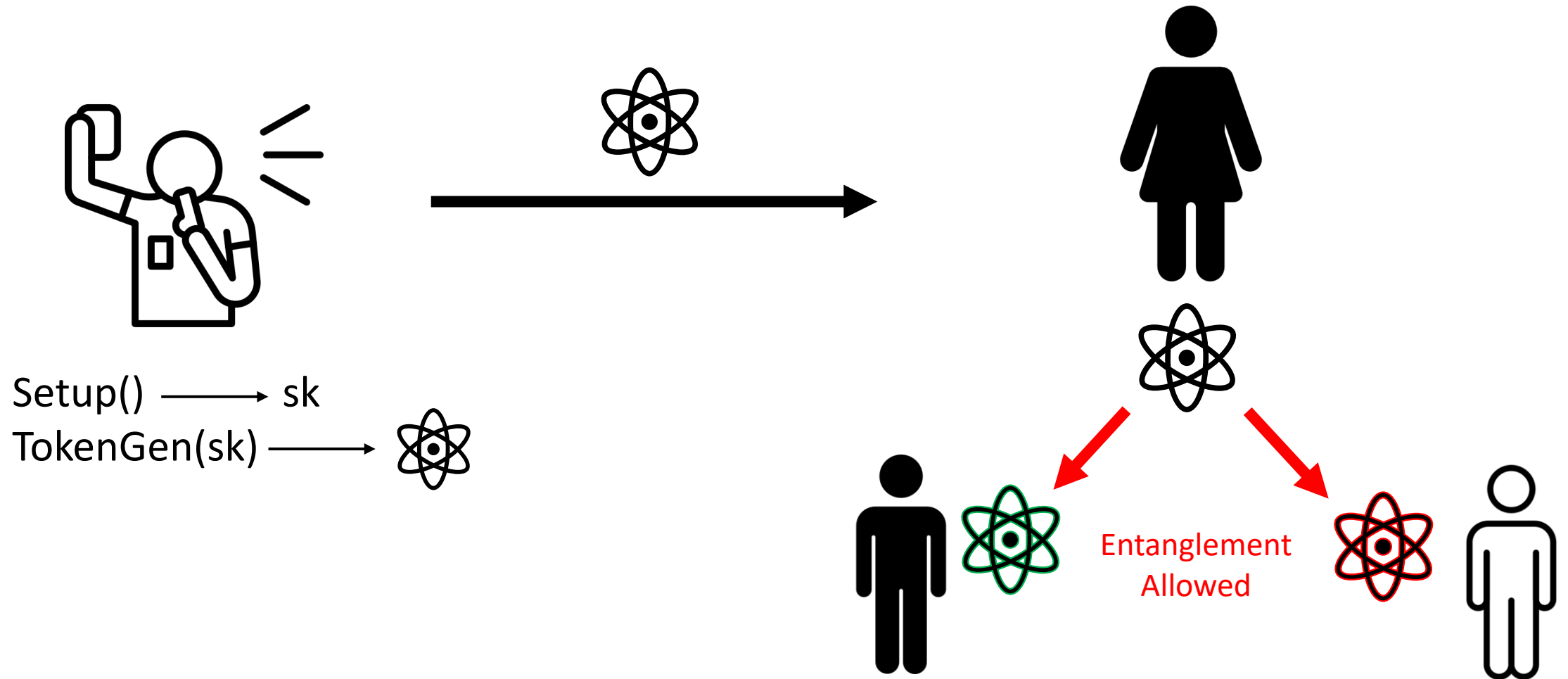
- Three phases:
 1. the Setup Phase
 2. the Splitting Phase
 3. the Verification Phase

Cloning Games (Setup Phase)

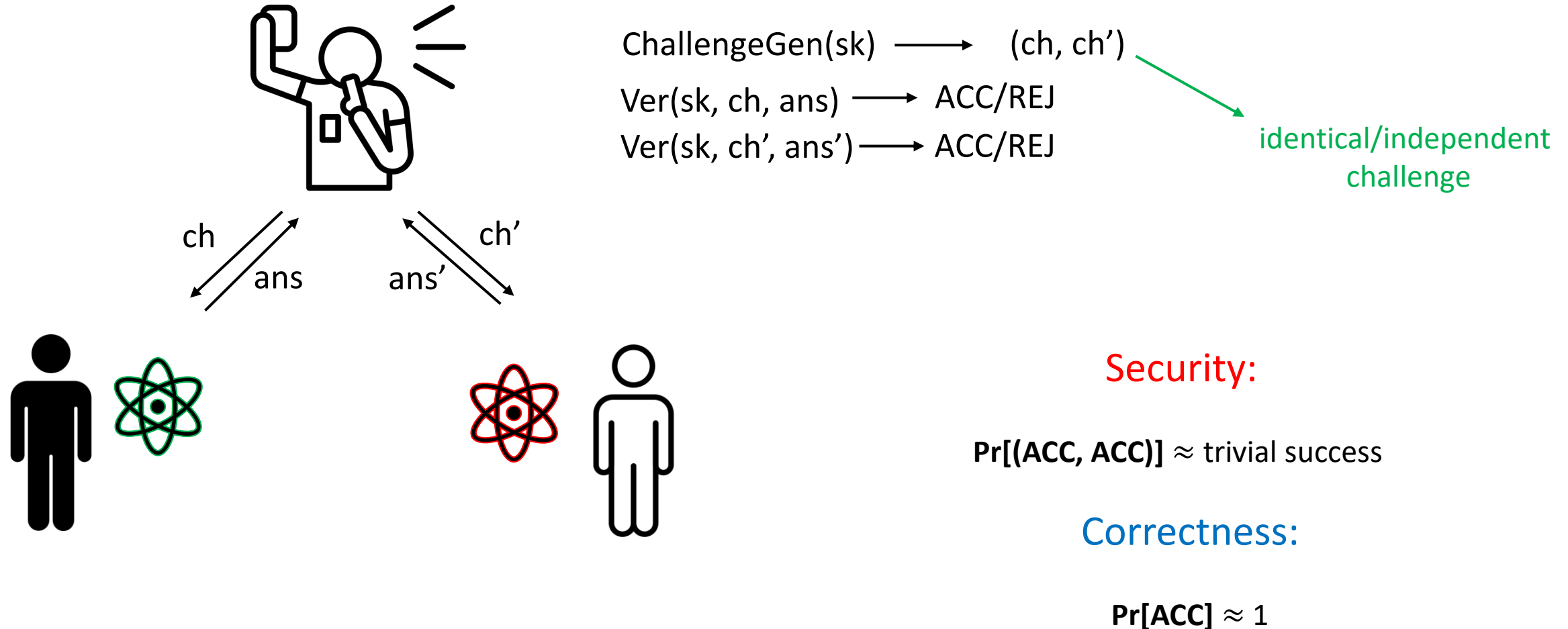


Setup() \longrightarrow sk
TokenGen(sk) \longrightarrow 

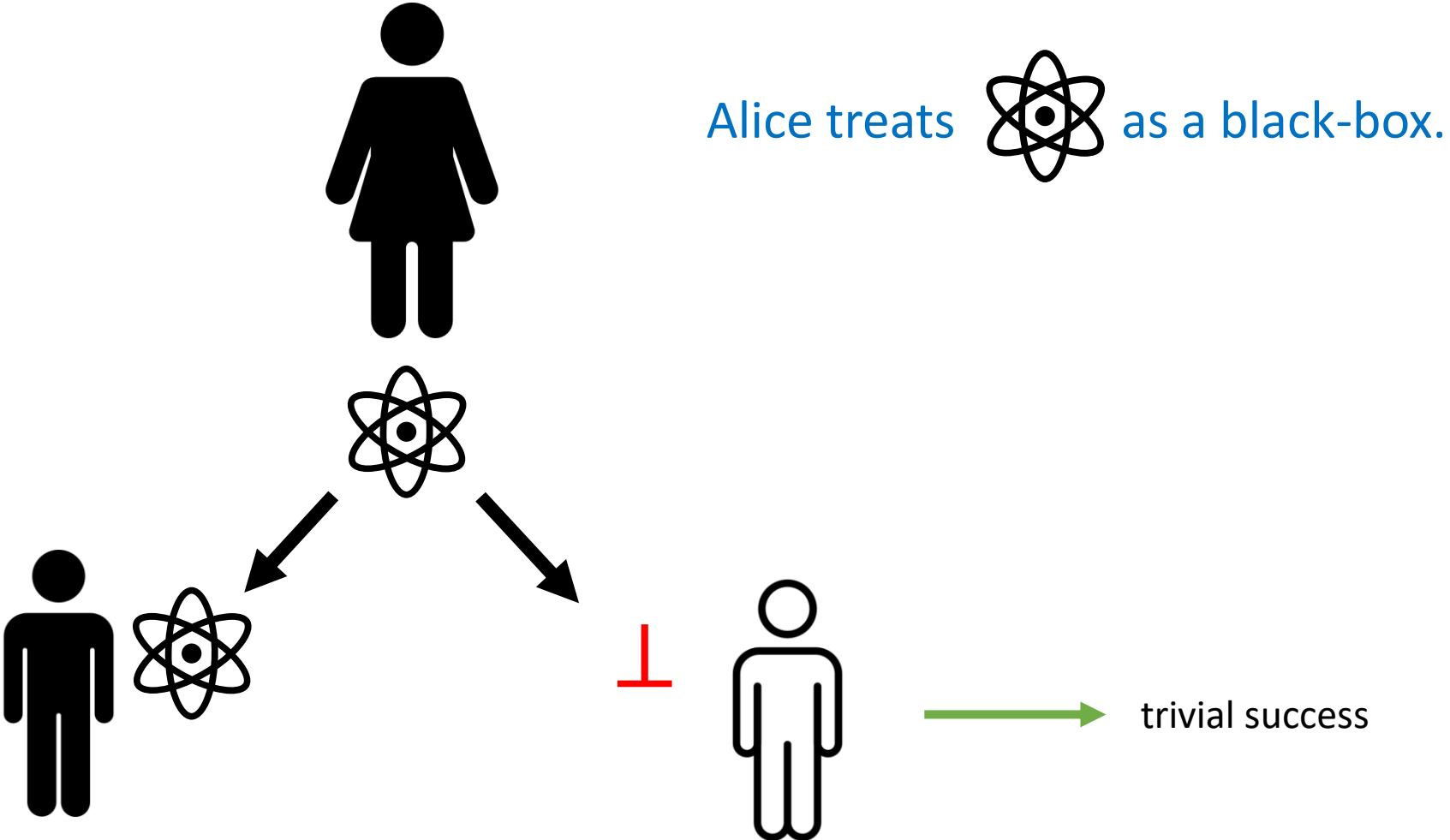
Cloning Games (Splitting Phase)



Cloning Games (Verification Phase)

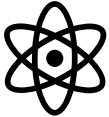


Trivial Cloning Attack



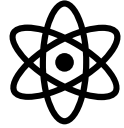
Unclonable Primitives as Cloning Games

Unclonable Encryption

- $\text{Setup}() \rightarrow (\text{sk}, m); \quad \text{sk} \leftarrow \text{Gen}(), \quad m \leftarrow \{m_0, m_1\}$
- $\text{Enc}(\text{sk}, m) \rightarrow$ 
- $\text{ch} = \text{ch}' = \text{sk}$
- $\text{Ver}(\text{sk}, m, \text{ans}) \rightarrow \text{ACC} \iff \text{ans} = m$

Unclonable Primitives as Cloning Games

Copy-Protection

- $\text{Setup}() \rightarrow f; \quad f \leftarrow F$ (unlearnable function family)
- $\text{CopyProtect}(f) \rightarrow$ 
- $\text{ChallengeGen}(f) \rightarrow (x, x')$ (pair of inputs)
- $\text{Ver}(f, x, \text{ans}) \rightarrow \text{ACC} \iff f(x) = \text{ans}$

Captures almost all* primitives:

- Single-Decryptor Encryption
- Quantum Money
- Tokenized Signatures
- Certified Deletion
- ...

*One-time primitives tricky to integrate

Relationship Between Challenge Distributions

Definition: An *evasive* cloning game has negligible trivial success probability. (E.g. CP with multi-bit output, SDE with multi-bit message)

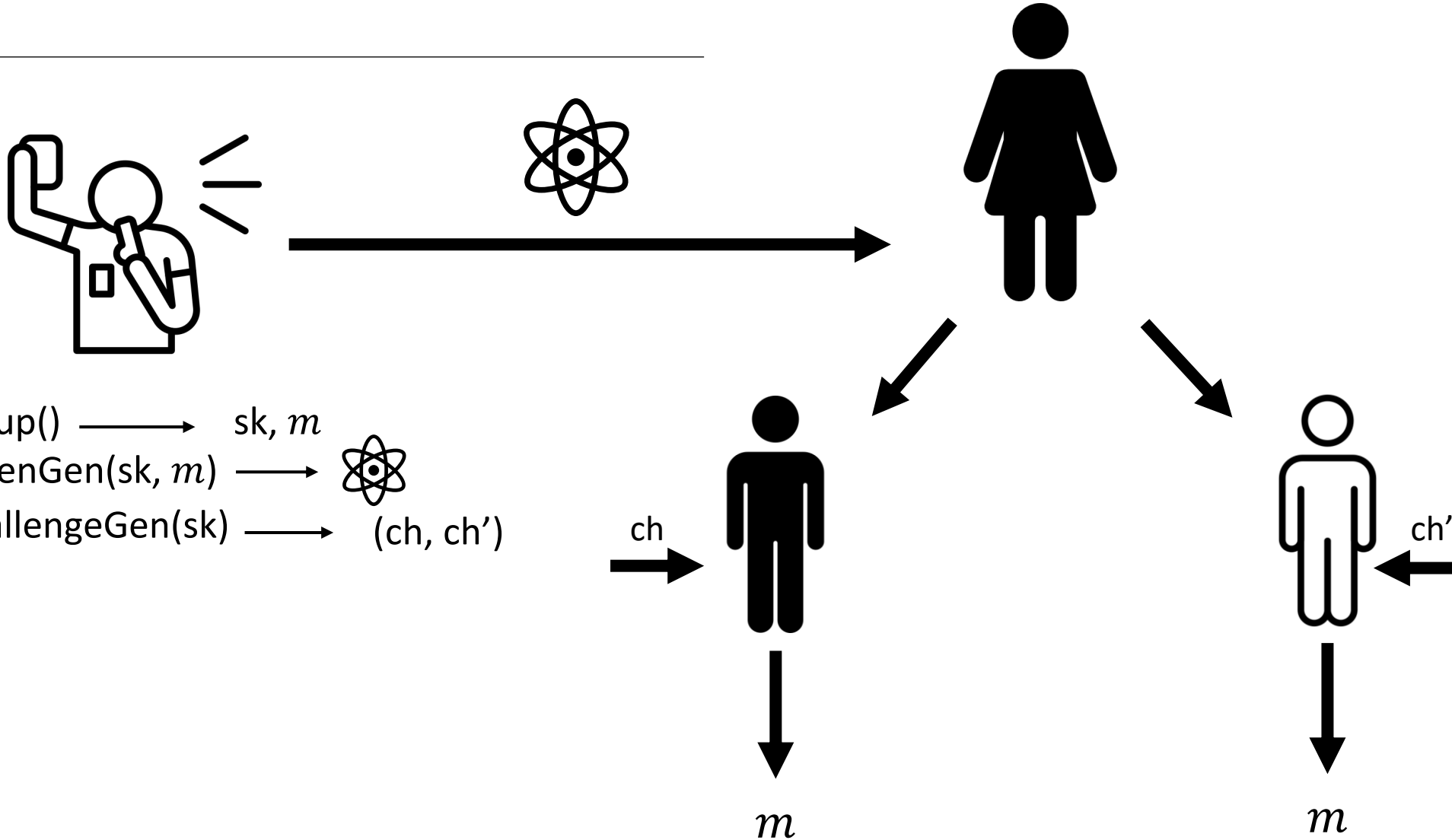
Theorem: An evasive cloning game secure against independent-challenges is also secure against identical-challenges.

MAJOR TECHNIQUES

- Achieving UE and CP for point functions in QROM from Wiesner states:
 - AKLLZ (CRYPTO '22) – Program testing
 - [This work](#): Augmented security for search games
- Lifting Classical BB Reductions to Quantum
 - BBK (CRYPTO '22) – State repair
 - [This work](#): Generalize to the non-local setting

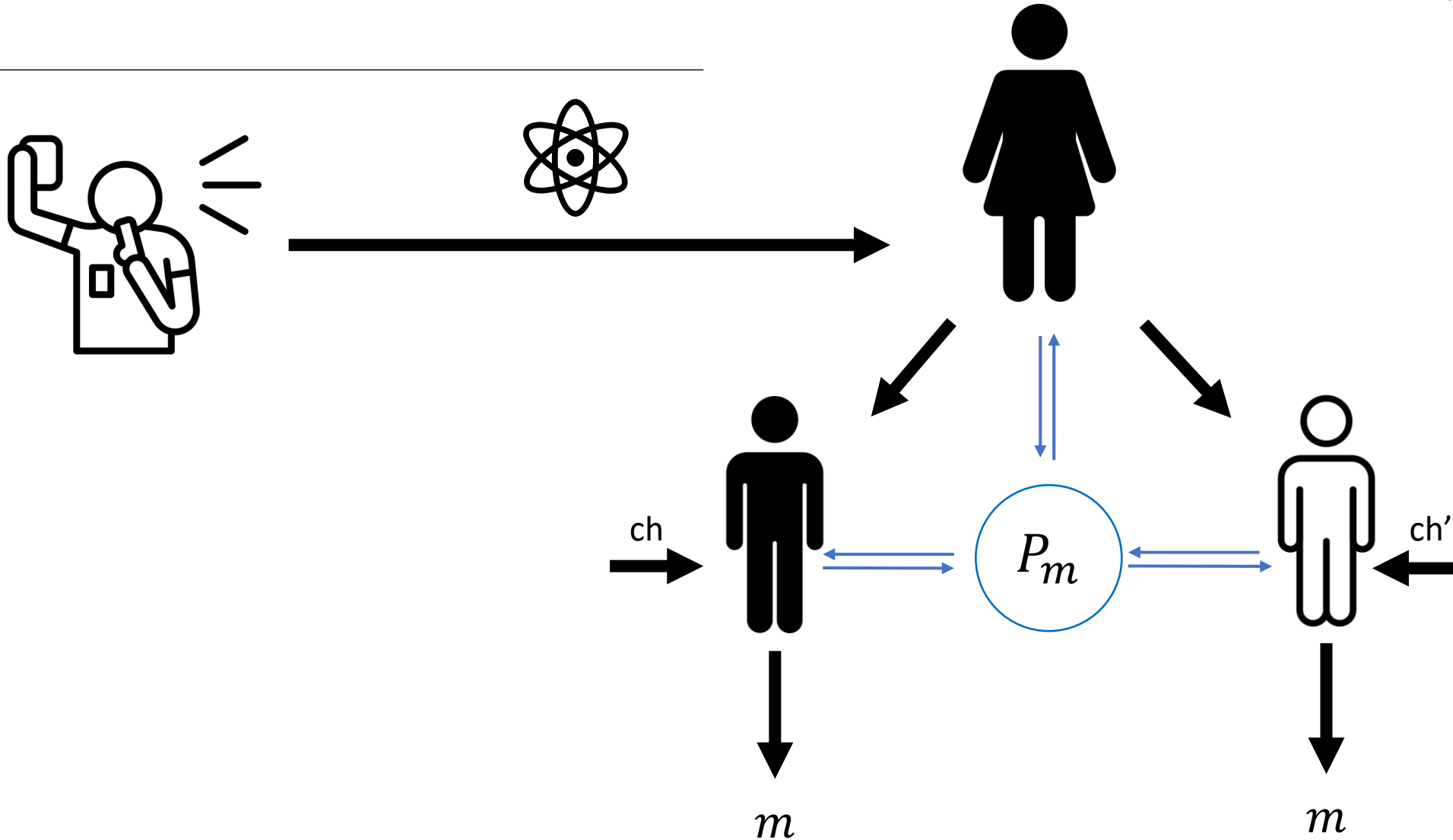
Search Game

Bob and Charlie need to output a high min-entropy answer m



Augmented Security

$$P_m(m) = 1$$
$$P_m(m') = 0, \forall m \neq m'$$



Why do we need augmented security?

- AKLLZ '22:

- Strong monogamy game for cosets (CLLZ '21)
- Identical challenge to independent challenge reduction via program testing (Zhandry '20)

- This work:

- Weak unclonable security of Wiesner states (BL '20)
- Augmented security of Wiesner states
- Identical challenge to independent challenge reduction via program testing (Zhandry '20)



Reduction requires access to
the verification oracle $P_m(\cdot)$

Lifting Classical Black-Box Reductions

Prior Work (BBK '22):

Classical Black-Box
Non-Adaptive
Reduction



Quantum Black-Box
Non-Adaptive
Reduction

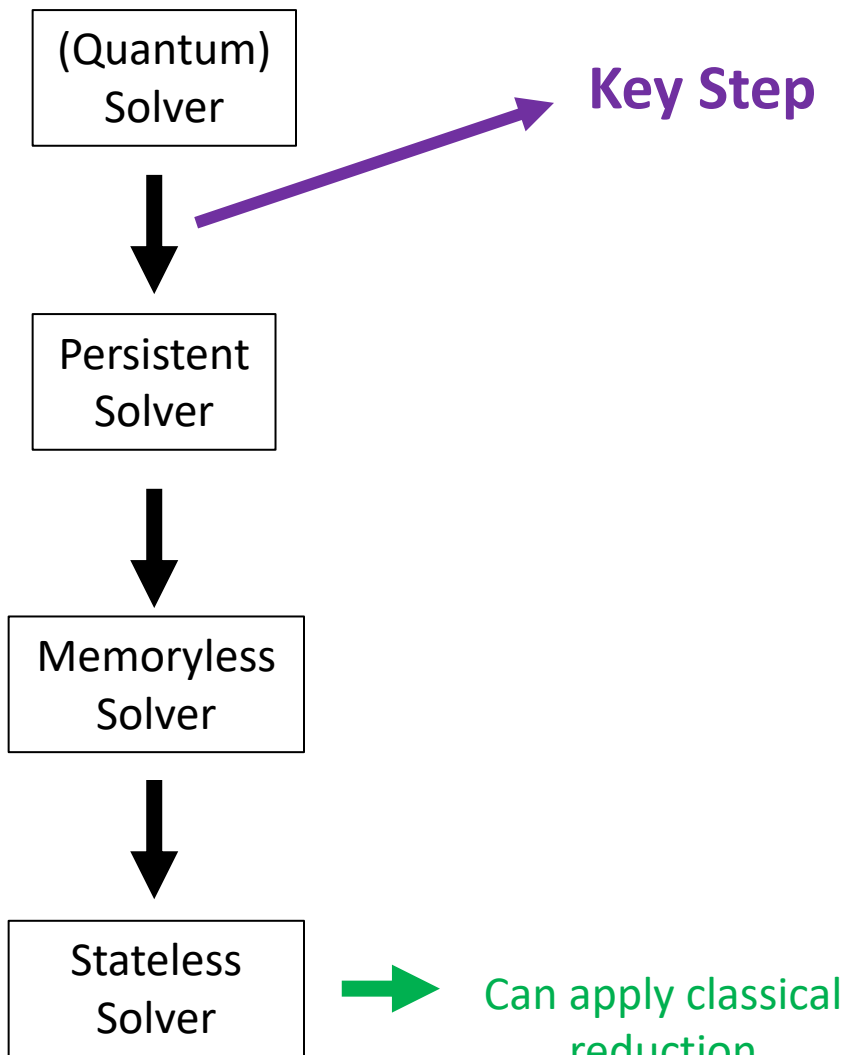
This Work:

Classical Non-Local
Black-Box Non-Adaptive
Reduction

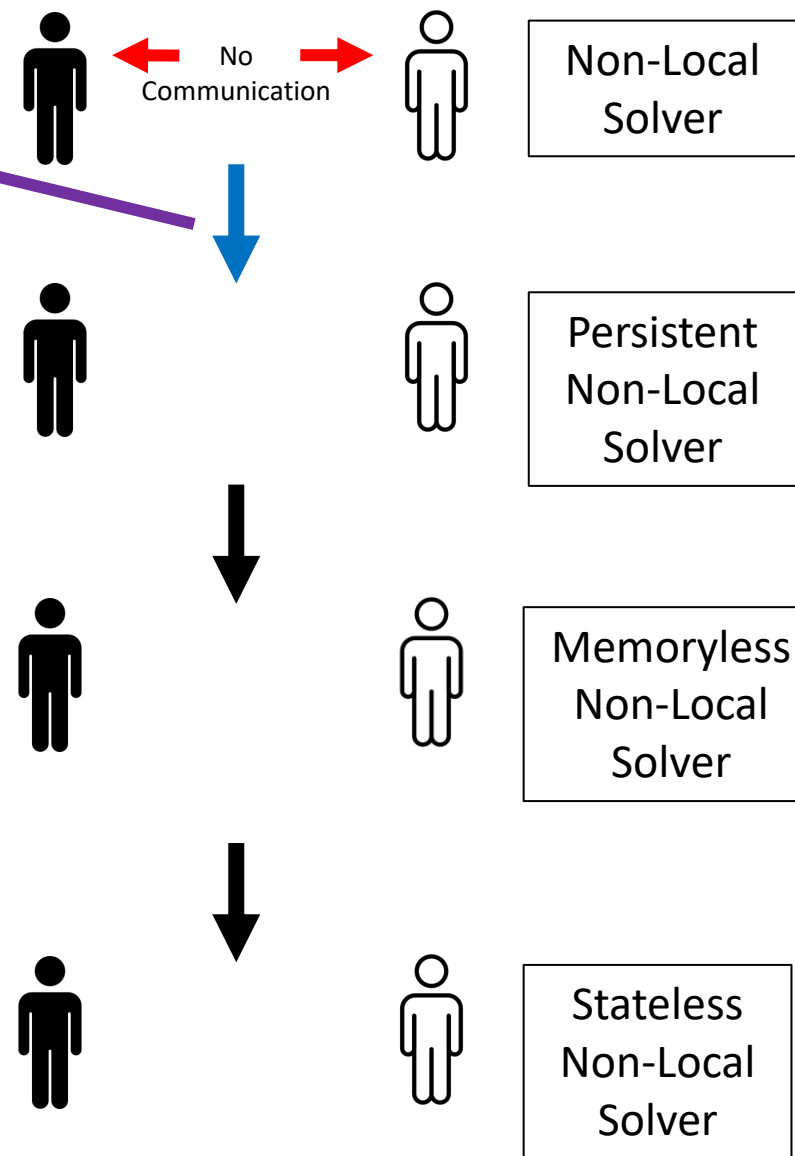


Quantum Non-Local
Black-Box Non-Adaptive
Reduction

Prior Work (BBK '22):

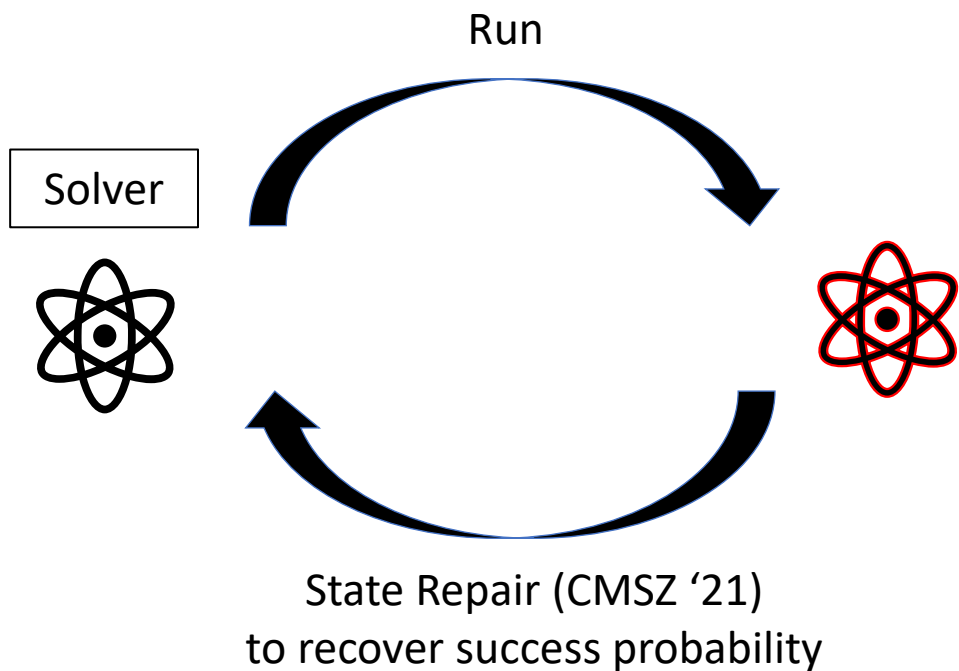


This Work:



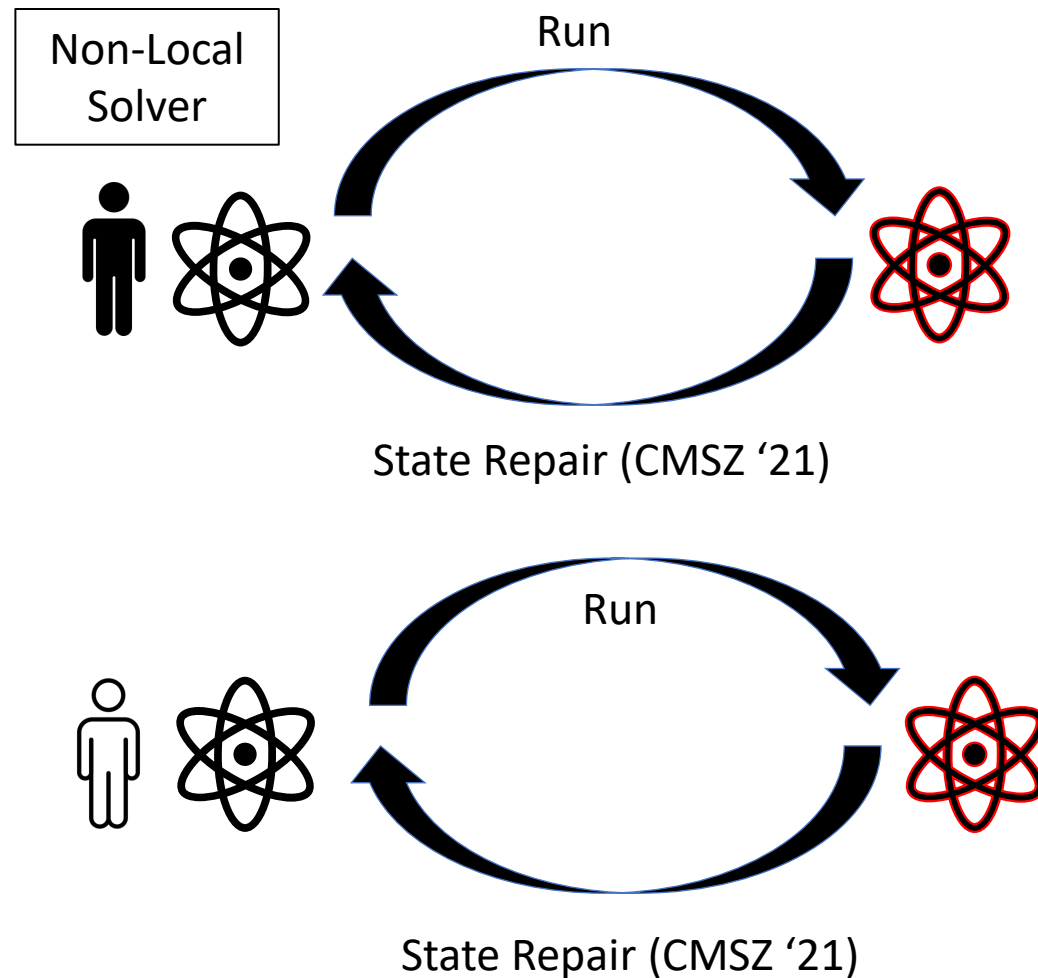
Prior Work (BBK '22):

Persistence Theorem:



This Work:

Persistence Theorem:



Ideas

- Locally repair both Bob's and Charlie's states.
- Works in the independent challenge setting.
- Proof by looking at the Jordan decompositions.

Applications

- Independent vs. identical challenge security of cloning games
- One-time SDE in the plain model

Open Problems

1. Relating challenge distributions for non-evasive cloning games
2. Achieving UE and CP for point functions in the plain model
3. Removing Black-Box/Non-Adaptive restrictions from the Non-Local Lifting Theorem

Q & A