Unclonable Non-Interactive Zero-Knowledge

Ruta Jawale and Dakshita Khurana

Motivation: No-Cloning Theorem

No-cloning Theorem:

- Cannot create independent, identical "clone" of arbitrary, unknown quantum state

Led to many unclonable primitives [AC13, CLLZ21, Got03, AKL+22, GZ20, KN23, MS24, AGLL24...]

Open problems posed by Aaronson [Aar09]:

- Can we construct unclonable quantum proofs?
- How do these proofs relate to quantum money?

Applications: Signatures & Credentials

- Unclonable Signatures of Knowledge
- Revocable Anonymous Credentials
- Unclonable Anonymous Credentials
- Certified Deletion of NIZK

Application: Signatures

Non-Interactive Prevention of Replay Attacks

Replay Attack

Sender

sk, m

$Sign_{sk}(m)$

Receiver

Adversary

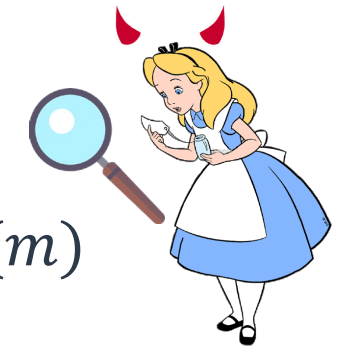
Application: Signatures

Non-Interactive Prevention of Replay Attacks

Replay Attack

Receiver

Adversary

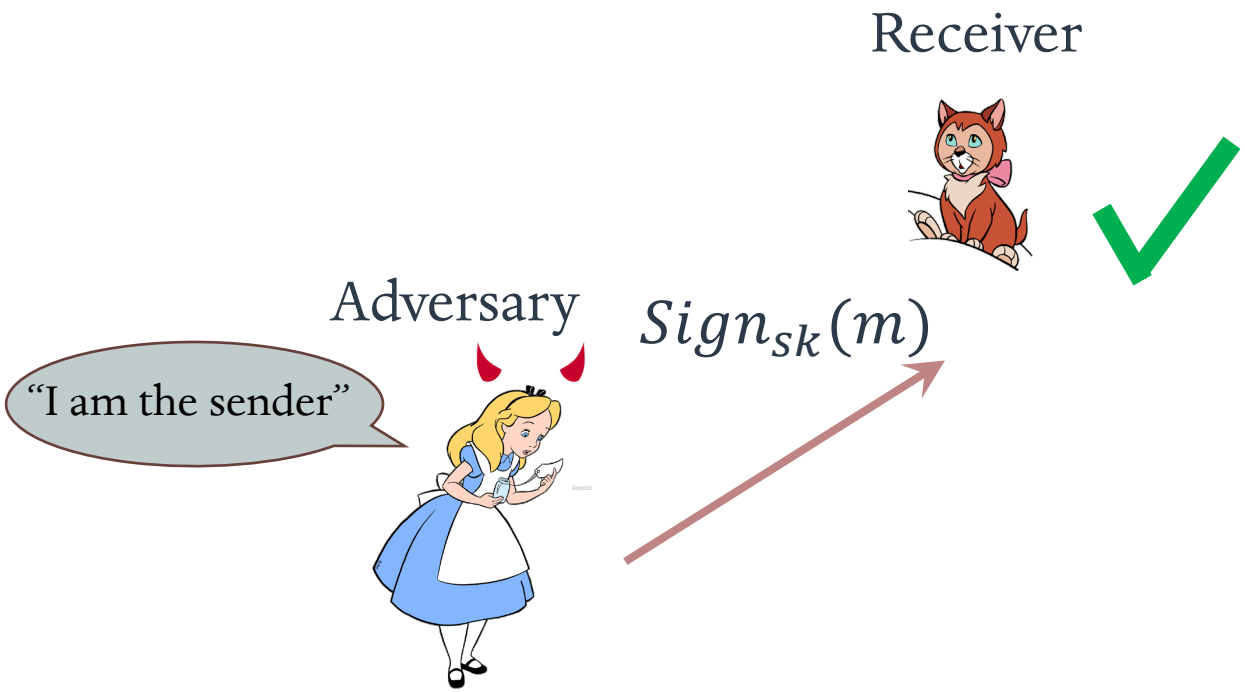


$Sign_{sk}(m)$

Application: Signatures

Non-Interactive Prevention of Replay Attacks

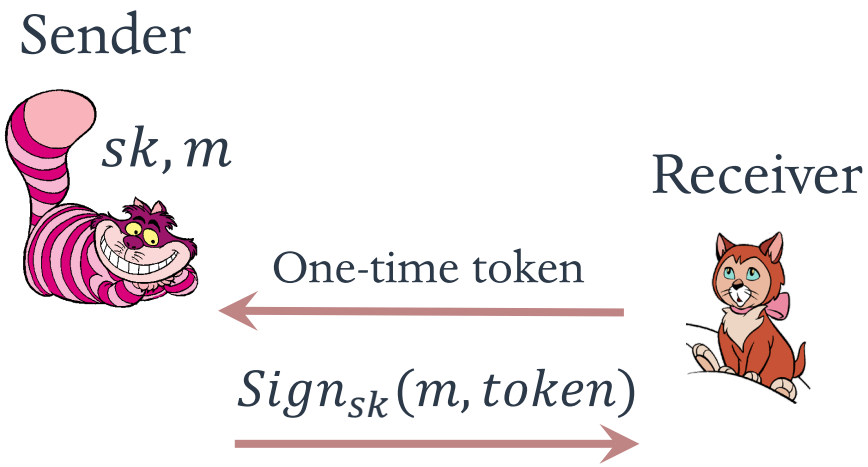
Replay Attack



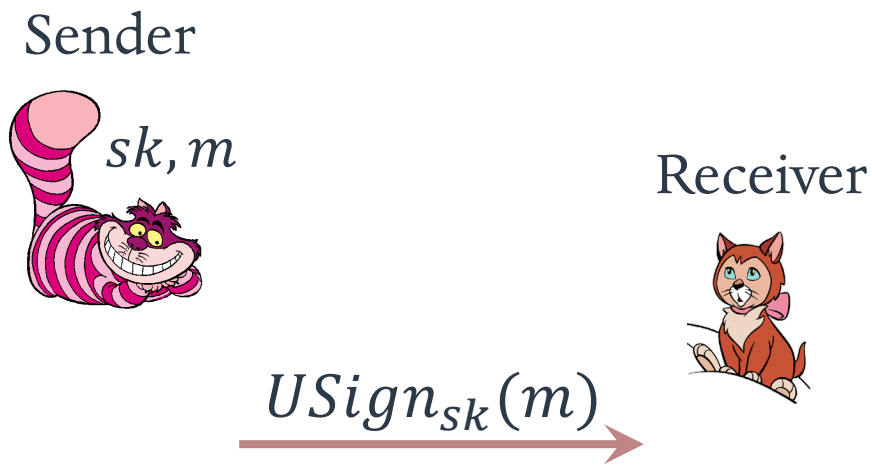
Application: Signatures

Non-Interactive Prevention of Replay Attacks

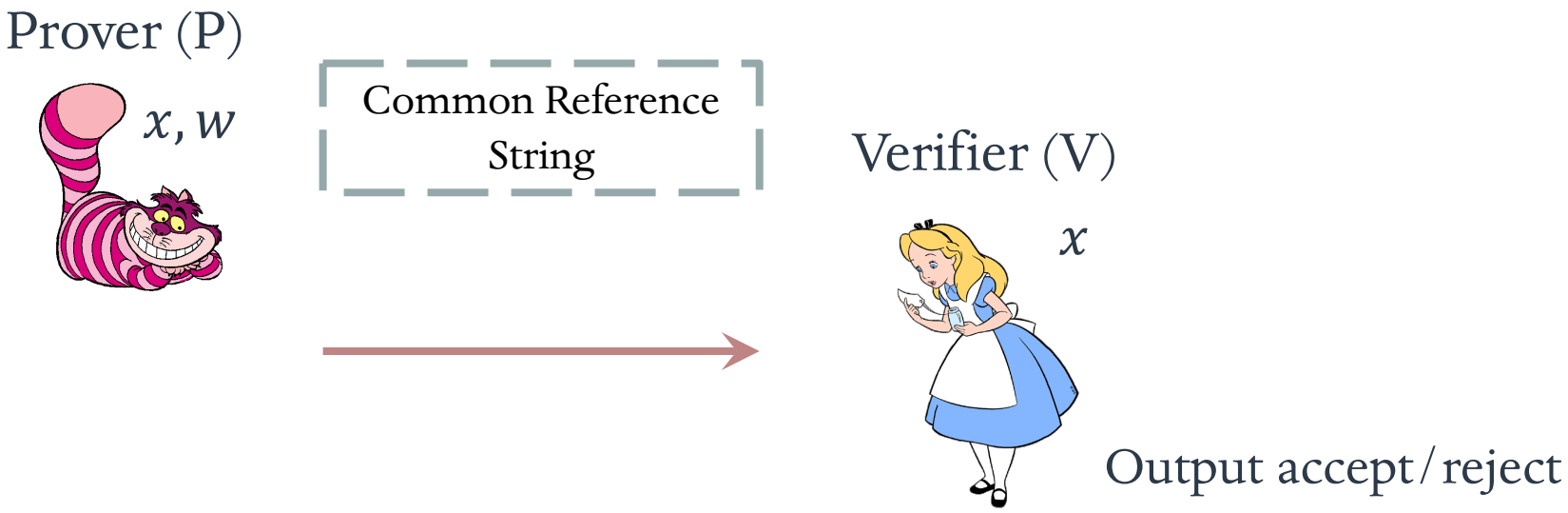
- Current: Session ID Approach



- Proposed: Unclonability Approach



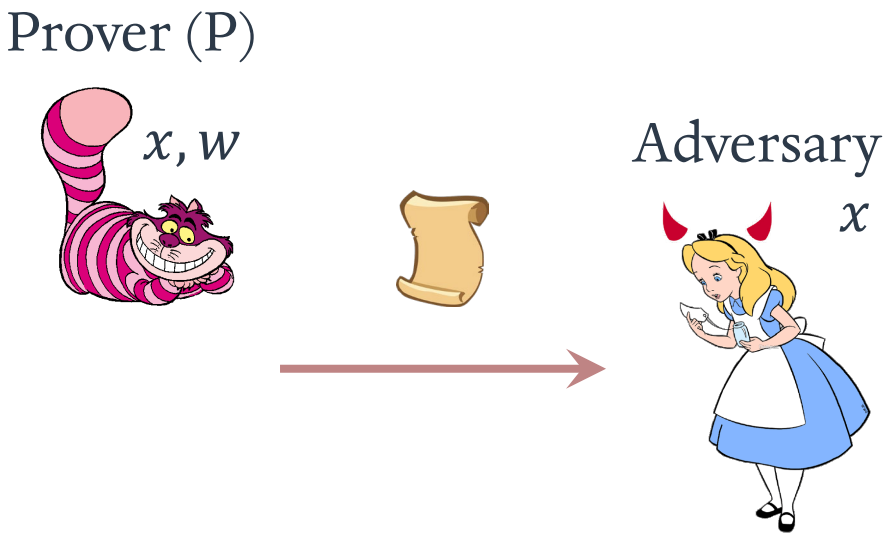
Recall: Non-Interactive Proof System for NP



- Completeness
  - $\forall x \in L,\ \Pr[V\ accepts] = 1$
- Soundness
  - $\forall P^*, x \notin L,\ \Pr[V\ accepts] = negl(\lambda)$

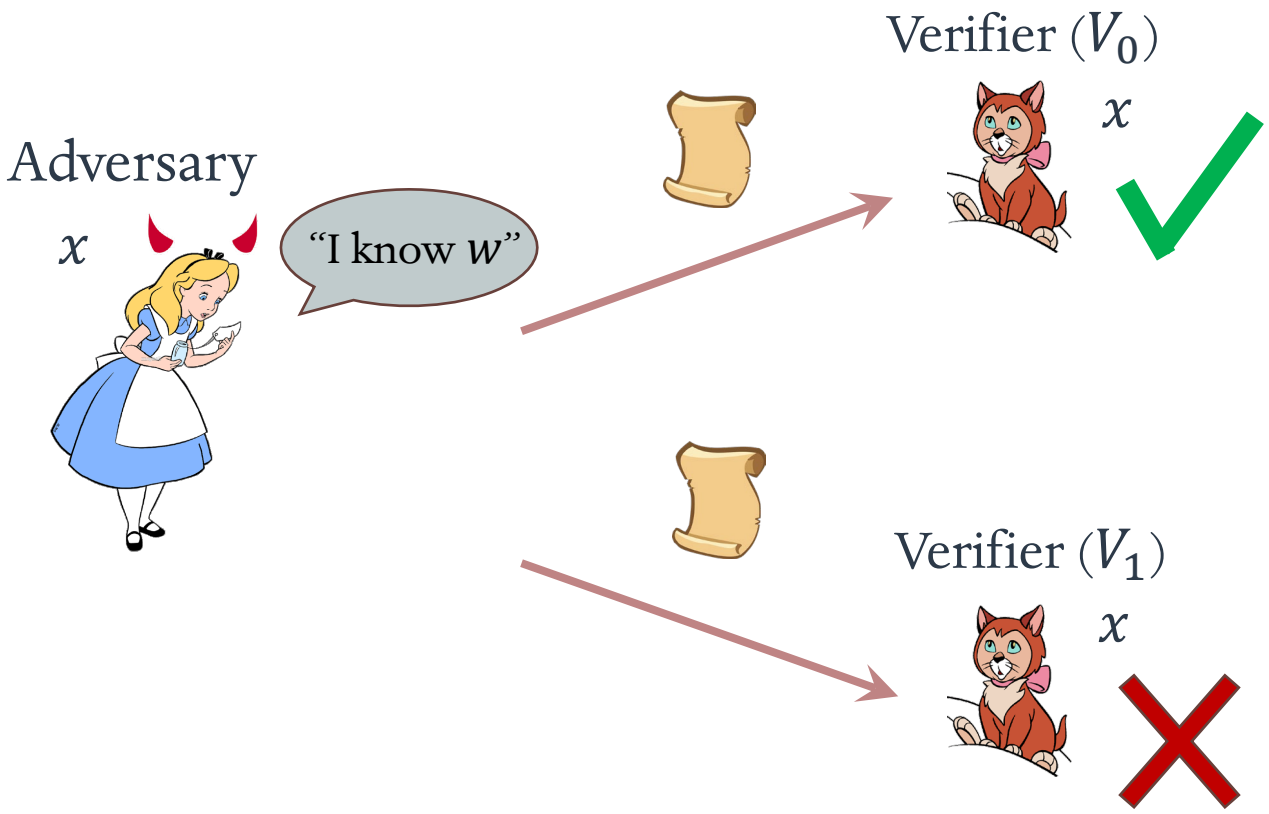
- Zero-Knowledge
  - V^* learns nothing beyond $x \in L$

Problem #1: Define Unclonable Proofs



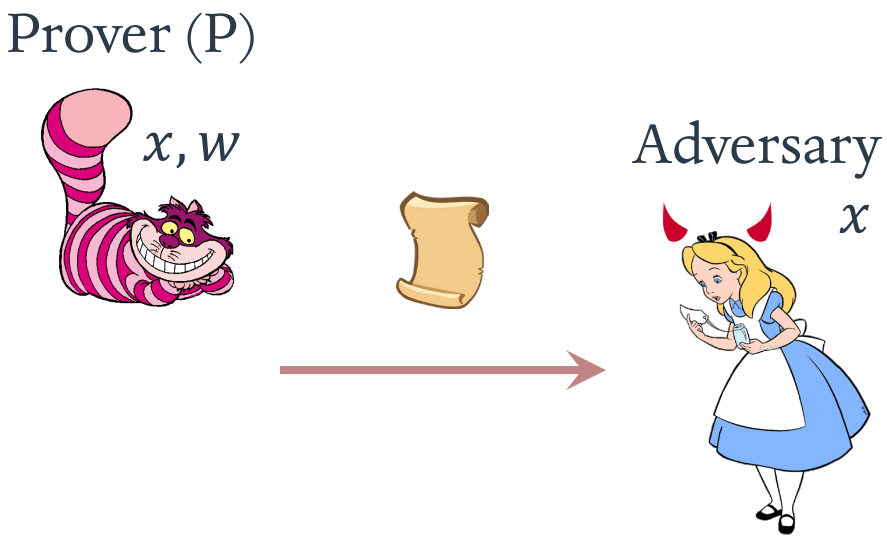
Problem #1: Define Unclonable Proofs

Problem #1: Define Unclonable Proofs



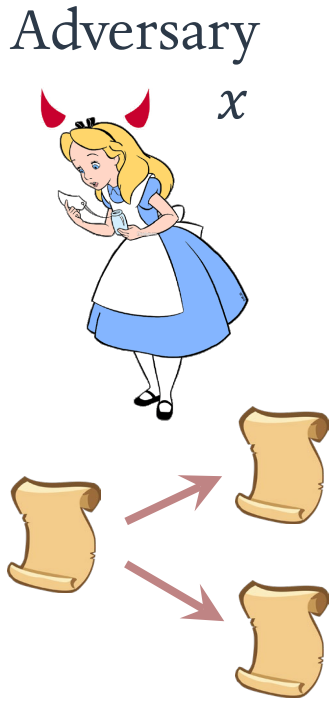
Challenges: Define Unclonable Proofs

- Must be quantum, otherwise…



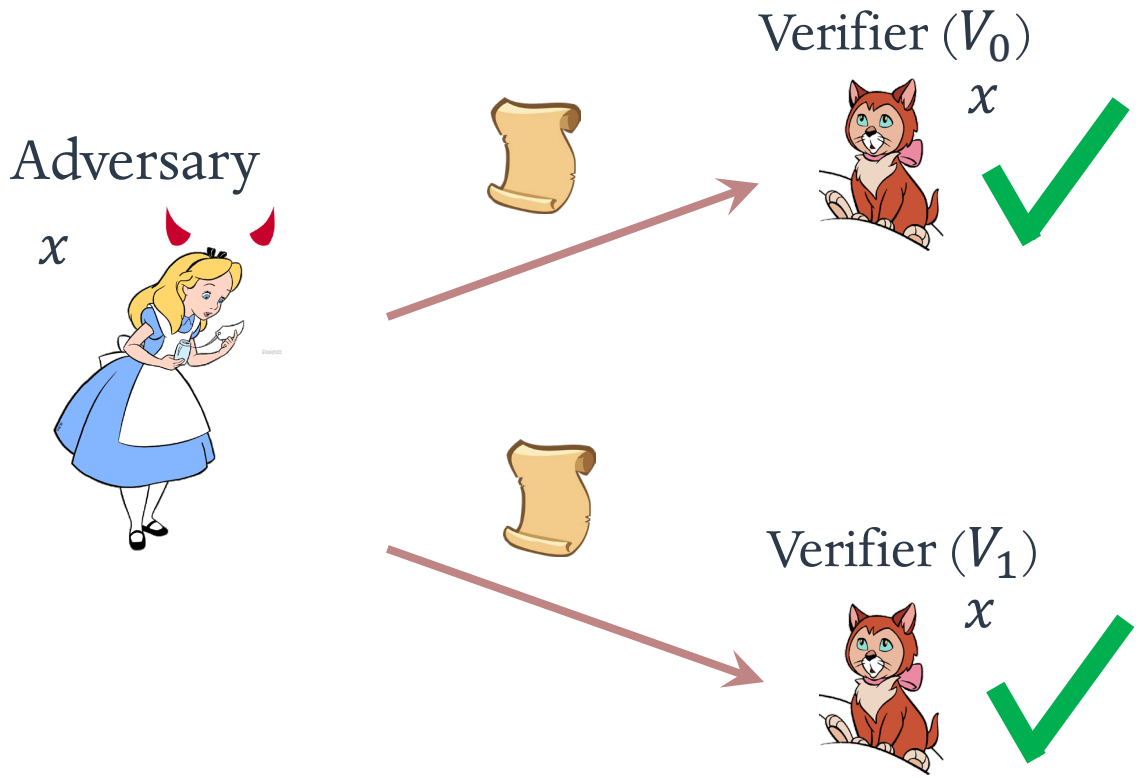
Challenges: Define Unclonable Proofs

- Must be quantum, otherwise…



Challenges: Define Unclonable Proofs

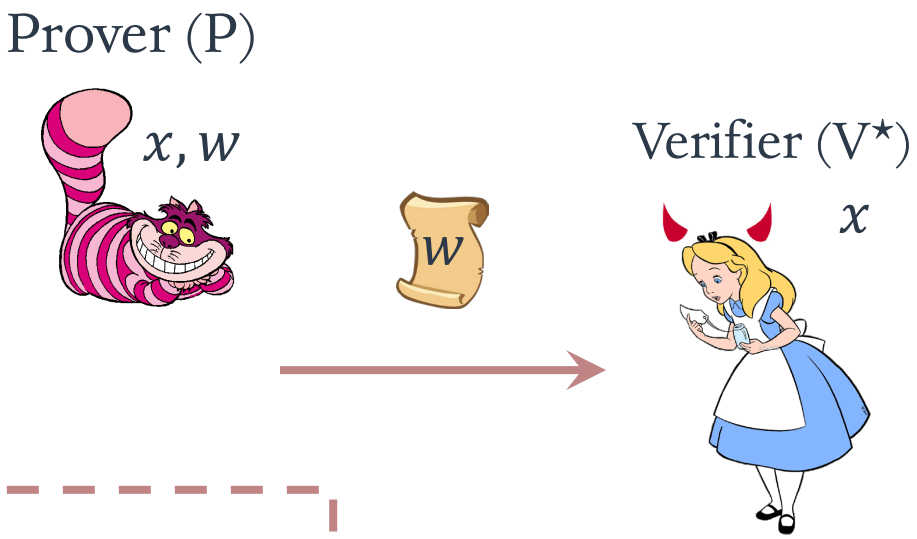
- Must be quantum, otherwise…



- Quantum

Challenges: Define Unclonable Proofs

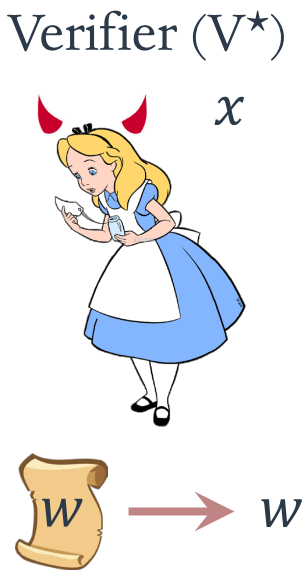
- Must be Zero-Knowledge, otherwise…



- Quantum

Challenges: Define Unclonable Proofs

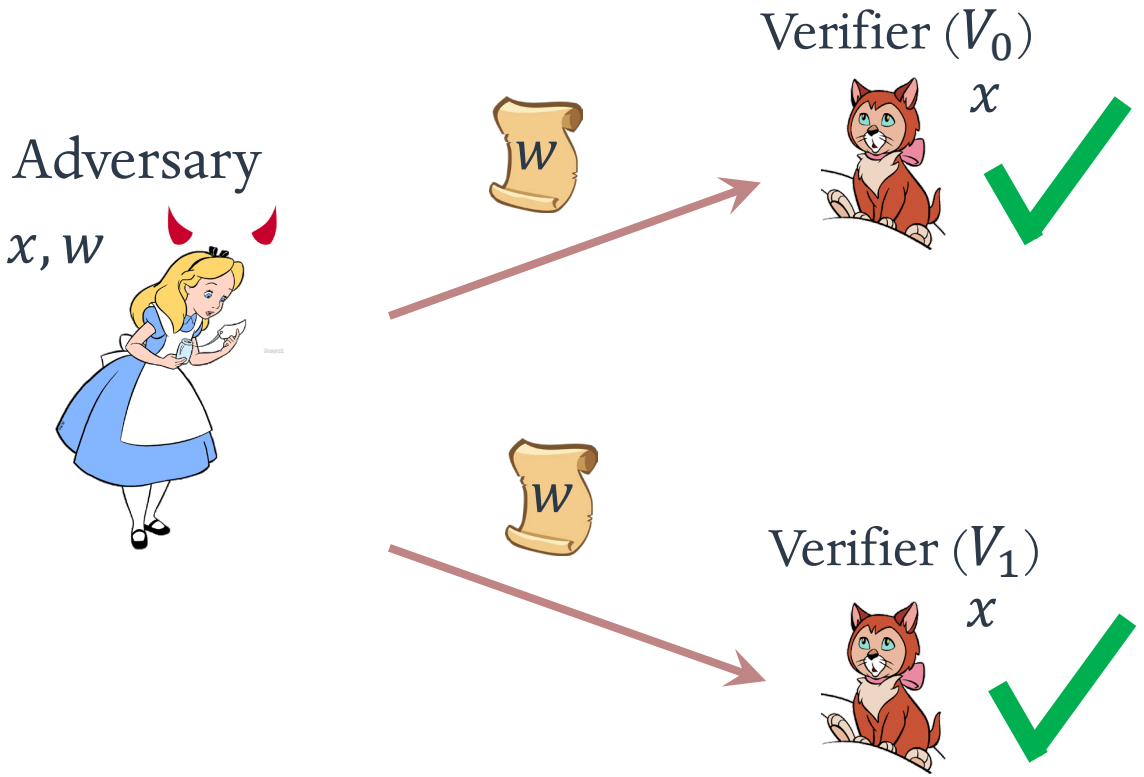
- Must be Zero-Knowledge, otherwise…



- Quantum

Challenges: Define Unclonable Proofs

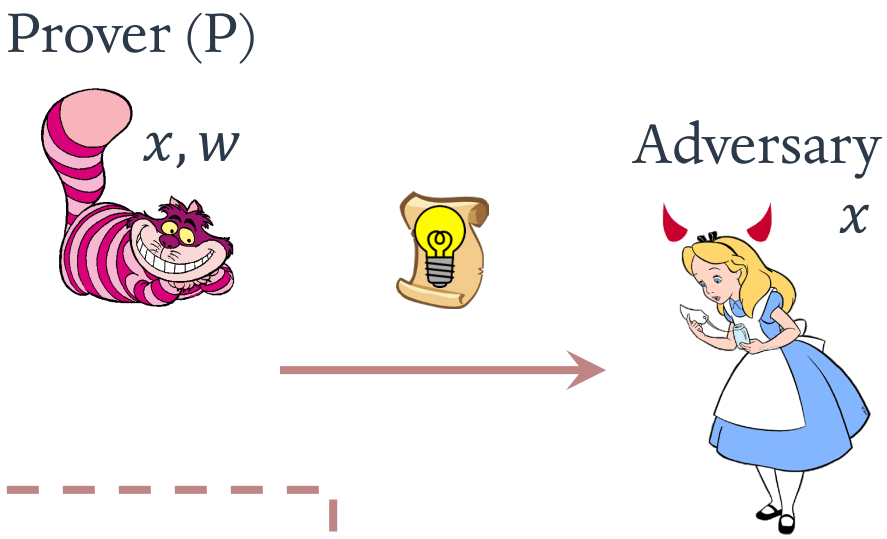
- Must be Zero-Knowledge, otherwise…



- Quantum
- Zero-Knowledge

Challenges: Define Unclonable Proofs

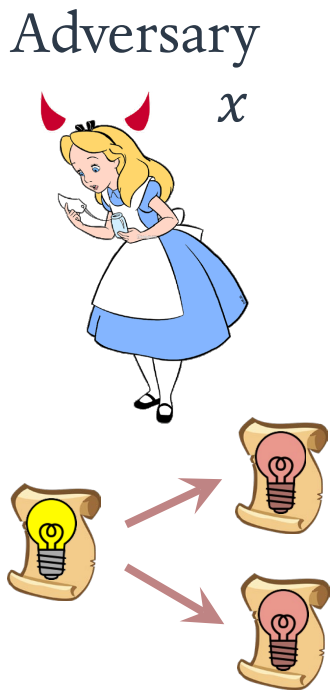
- Must be "Non-Malleable" (must be defined carefully), otherwise…



- Quantum
- Zero-Knowledge

Challenges: Define Unclonable Proofs

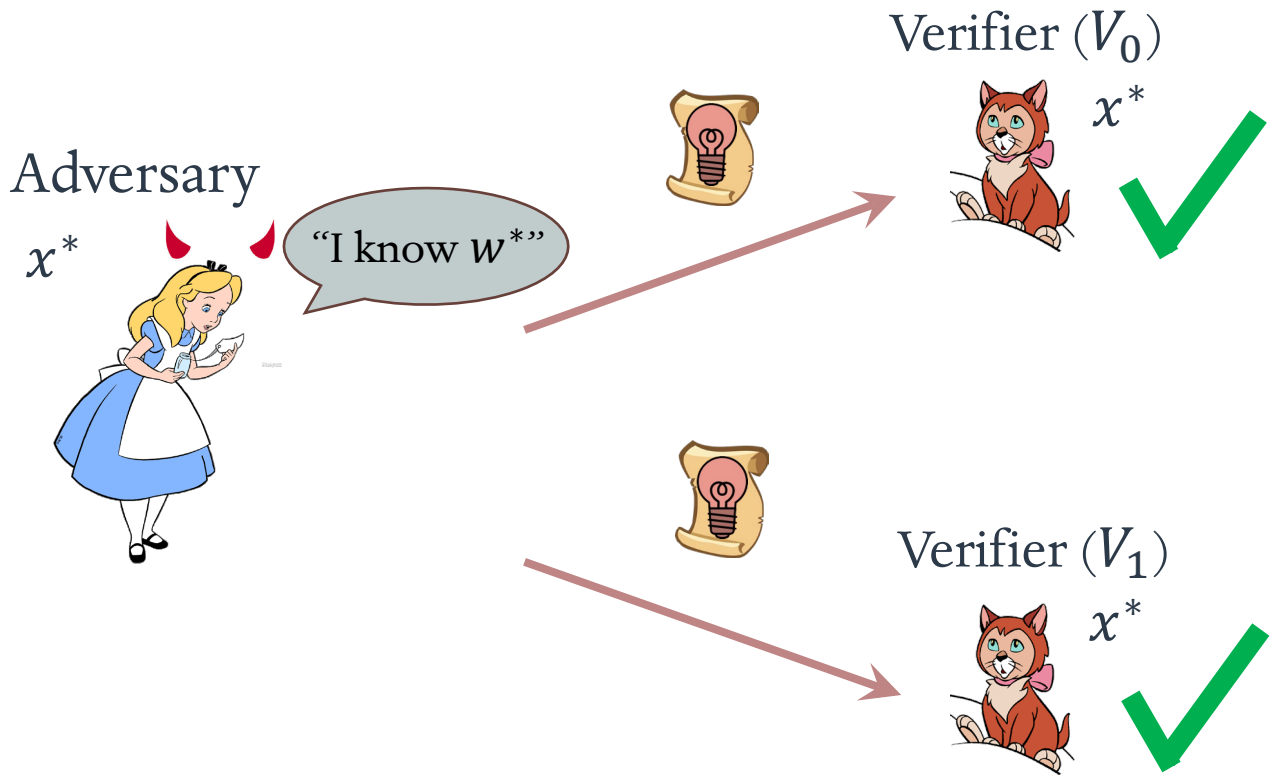
- Must be "Non-Malleable" (must be defined carefully), otherwise…



- Quantum
- Zero-Knowledge

Challenges: Define Unclonable Proofs

- Must be "Non-Malleable" (must be defined carefully), otherwise…



- Quantum
- Zero-Knowledge
- "Non-Malleable"

Problem #2: Construct Unclonable NIZK

Theorem Statements (Informal)

- Assuming
  - Public-key quantum money
  - Public-key encryption
  - Commitments
  - Simulation-sound NIZK for NP
- Then we have Unclonable NIZK
  - In common reference string model

- Assuming
  - Public-key quantum money
  - Sigma protocols for NP
- Then we have Unclonable NIZK
  - In quantum random oracle model

Recall: Public-Key Quantum Money

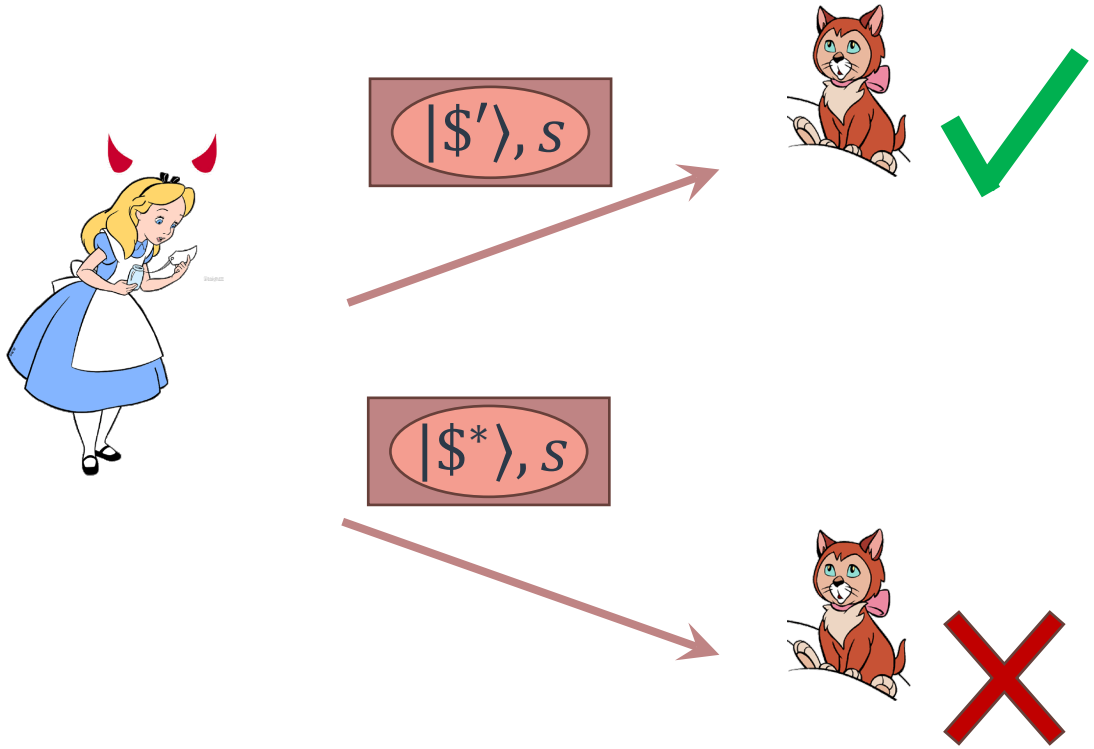
Unforgeability

Recall: Public-Key Quantum Money

Unforgeability

Recall: Public-Key Quantum Money

Unforgeability



Construction: Unclonable NIZK in CRS

Prover (P)

x, w

$pk, c = Com(0)$

$|\$\rangle, s$

$ct = Enc_{pk}(w)$

NIZK Proof:

"ct is an encryption of w"
OR
"c is a commitment of serial number s"

Verifier (V)

x

1. Verify banknote
2. Verify NIZK proof

Proof: Unclonable

Key Insight:
Adversary must have w unless they forge a quantum money banknote

Assume…

Prover (P)

x, w

$pk, c = Com(0)$

$|\$\rangle, s$

Adversary

x

$ct = Enc_{pk}(w)$

NIZK Proof:

"ct is an encryption of w"
OR
"c is a commitment of serial number s"

Proof: Unclonable

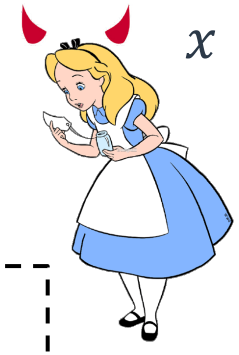
Key Insight:
Adversary must have w unless they forge a quantum money banknote

Assume…

$pk, c = Com(0)$

Adversary

x



$|\$\rangle, s$

$ct = Enc_{pk}(w)$

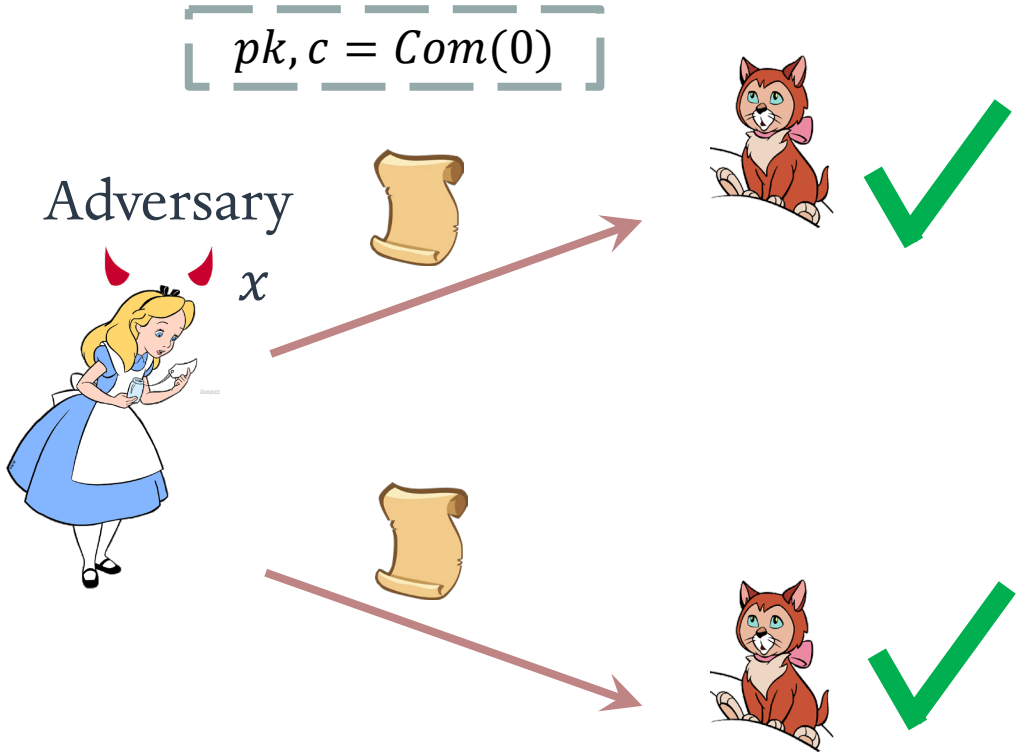
NIZK Proof:

"ct is an encryption of w"
OR
"c is a commitment of serial number s"

Proof: Unclonable

Key Insight:
Adversary must have w unless they forge a quantum money banknote

Assume…



Proof: Unclonable

Key Insight:
Adversary must have w unless they forge a quantum money banknote

Indistinguishably switch to second branch…

Prover (P)

x, w

$pk, c = Com(0)$

$|\$\rangle, s$

Adversary

x

$ct = Enc_{pk}(w)$

NIZK Proof:

"ct is an encryption of w"
OR
"c is a commitment of serial number s"

Proof: Unclonable

Key Insight:
Adversary must have w unless they forge a quantum money banknote

Indistinguishably switch to second branch…

Simulator (Sim)

x

$pk, c = Com(s)$

$|\$\rangle, s$

$ct = Enc_{pk}(0)$

NIZK Proof:

"ct is an encryption of w"
OR
"c is a commitment of serial *number* s"

Adversary

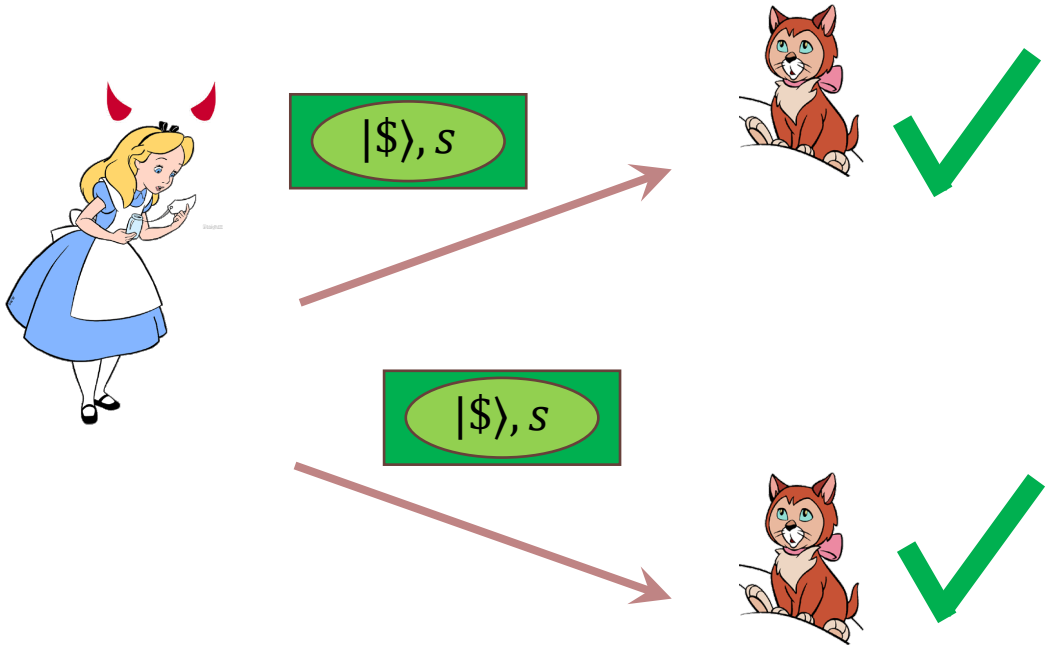
x

Proof: Unclonable

Key Insight:
Adversary must have w unless they forge a quantum money banknote

Either…

$pk, c = Com(s)$



⊥ breaks unforgeability of quantum money

Or…

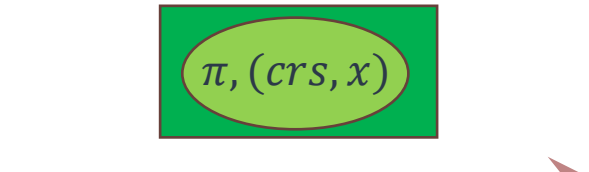
$pk, c = Com(s)$

One of  s:

contains $ct = Enc_{pk}(w)$

Adversary knows w!

Unclonable NIZK ⇒ Quantum Money



$(x, w) \leftarrow (X, W)$

$crs \leftarrow \text{UNIZK.Setup}(1^{\lambda})$

$\pi \leftarrow \text{UNIZK.Prove}(crs, x, w)$

$\text{UNIZK.Verify}(crs, x, \pi)$

Summary of Results

- Define Unclonable (Extractable) NIZKs
- Quantum Money (and other standard assumptions) ⇒ Unclonable NIZK
  - In CRS and QRO model
- Unclonable NIZK ⇒ Quantum money
  - In CRS and QRO model