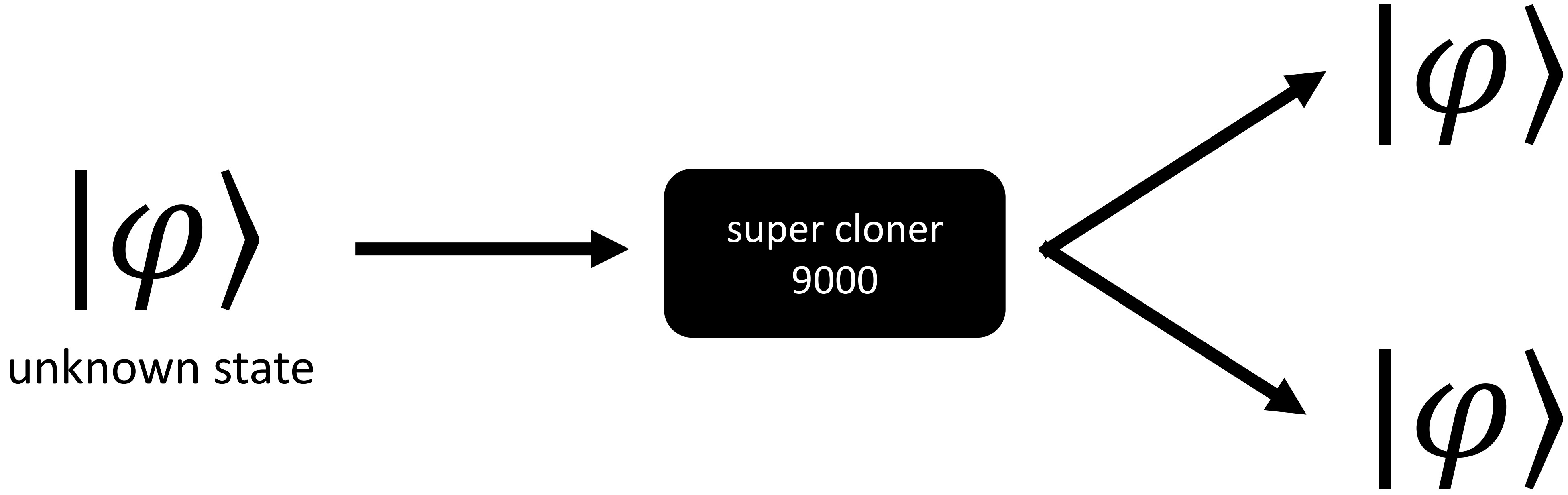
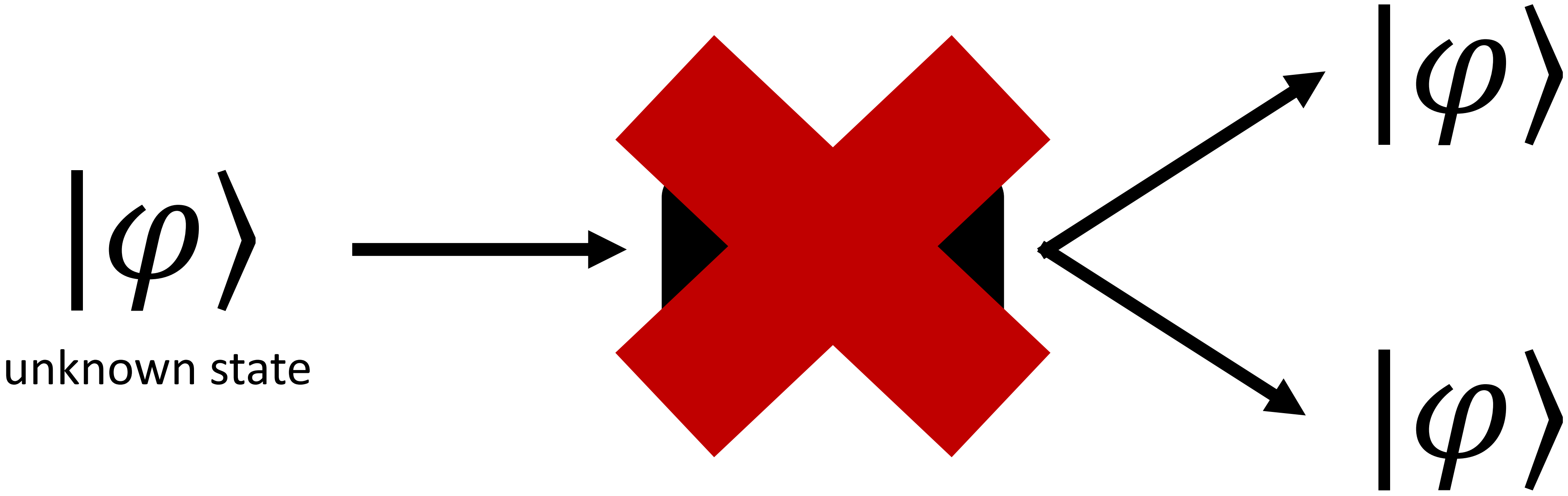
Untelegraphable Encryption and its Applications

Jeffrey Champion, Fuyuki Kitagawa,
Ryo Nishimaki, Takashi Yamakawa

No-Cloning Theorem

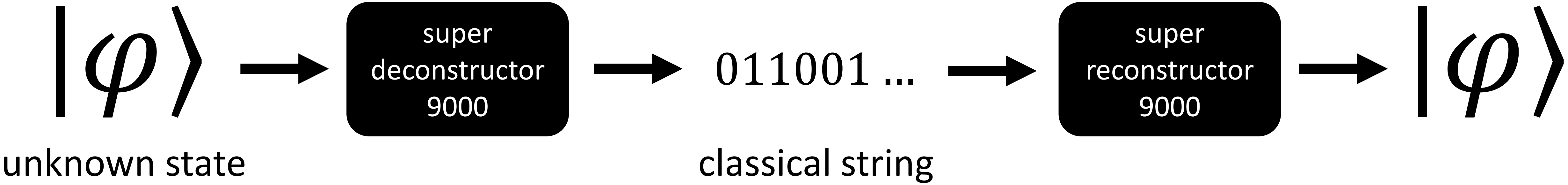


No-Cloning Theorem



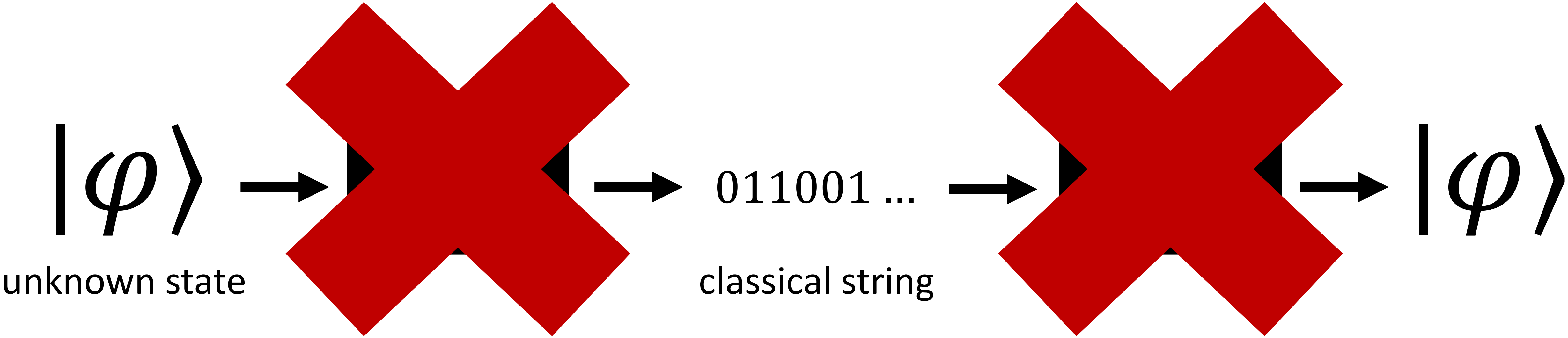
No-Telegraphing Theorem

(previously called no-teleportation)



No-Telegraphing Theorem

(previously called no-teleportation)



No-Cloning vs No-Telegraphing

- Equivalent: a set of quantum states is clonable iff it is telegraphable

No-Cloning vs No-Telegraphing

- Equivalent: a set of quantum states is clonable iff it is telegraphable

- Nehoran and Zhandry [NZ24]: there are sets of states that can be efficiently cloned but *cannot* be efficiently telegraphed

No-Cloning vs No-Telegraphing

- Equivalent: a set of quantum states is clonable iff it is telegraphable

- Nehoran and Zhandry [NZ24]: there are sets of states that can be efficiently cloned but *cannot* be efficiently telegraphed

Can we further leverage the computational hardness of telegraphing compared to cloning?

Unclonable Cryptography

- Quantum money [Wie83]
- Quantum copy-protection [Aar09]
- Unclonable encryption [Got03, BL20]

…

Unclonable Cryptography

- Quantum money [Wie83]
- Quantum copy-protection [Aar09]
- Unclonable encryption [Got03, BL20]

…

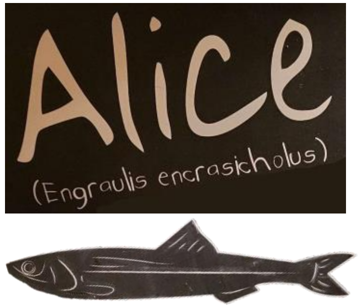
Current constructions of these primitives use very strong or non-standard assumptions!

Unclonable Encryption (UE)

[BL20]

Unclonable Encryption (UE)

[BL20]



classical key

encrypts m

$|\mathrm{ct}\rangle$

classical key

One-Way Secure UE

[BL20]

Adversary

Challenger

One-Way Secure UE

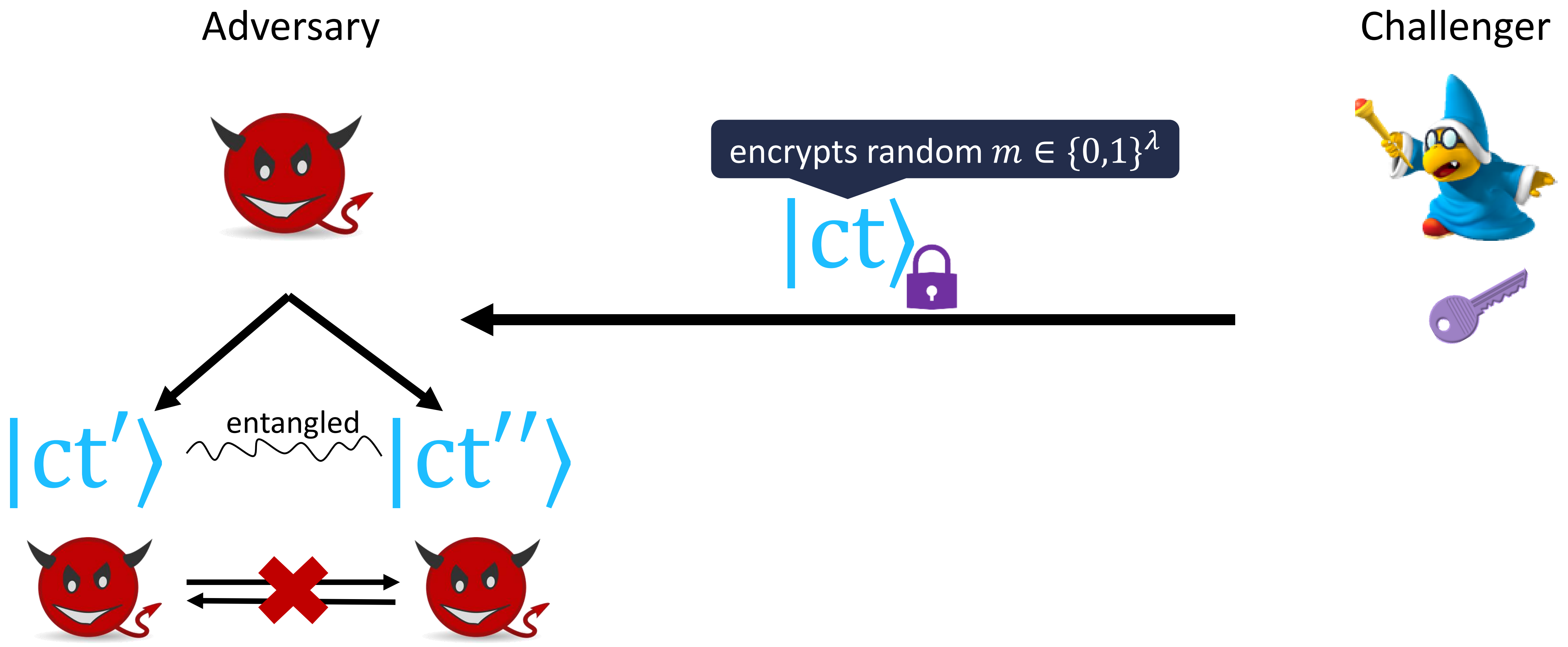
[BL20]

Adversary

Challenger

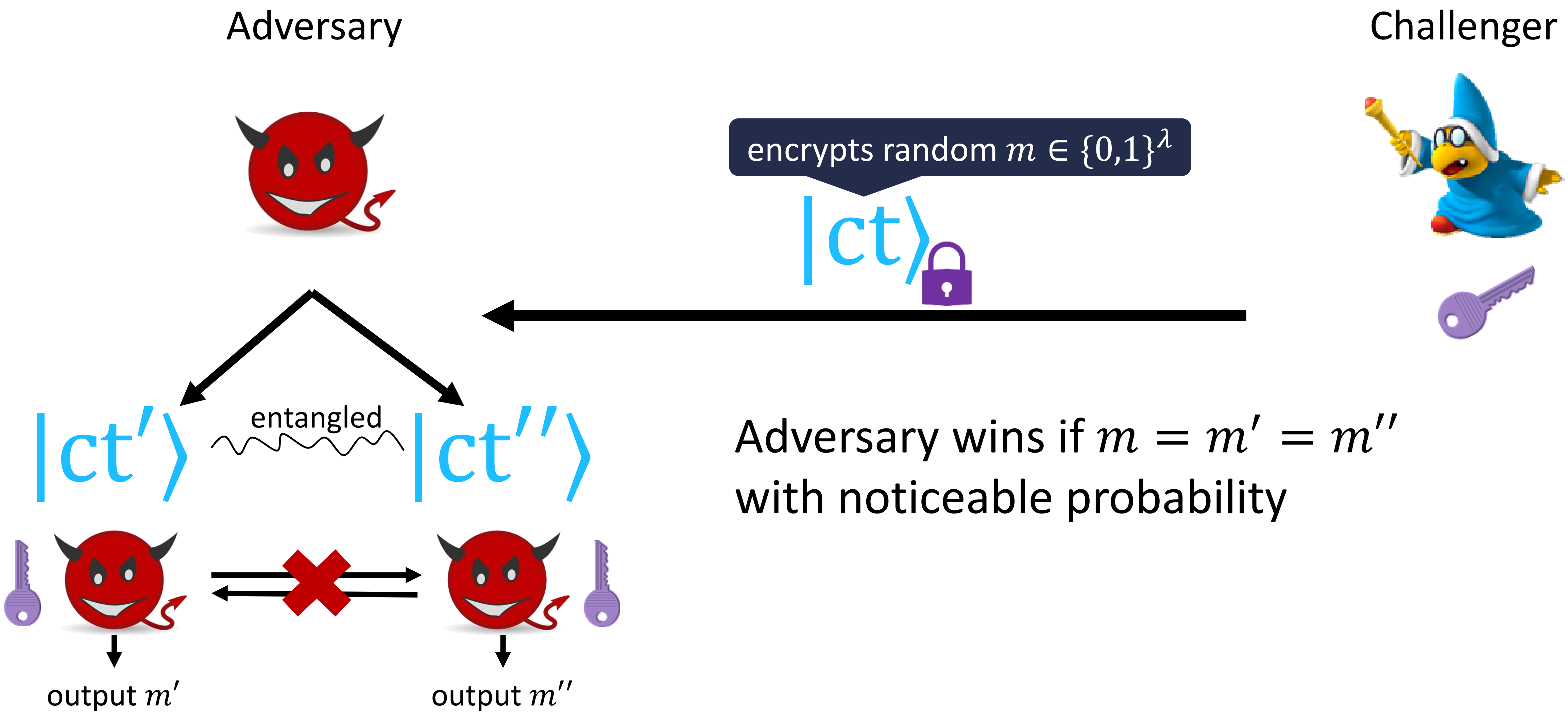
One-Way Secure UE

[BL20]



One-Way Secure UE

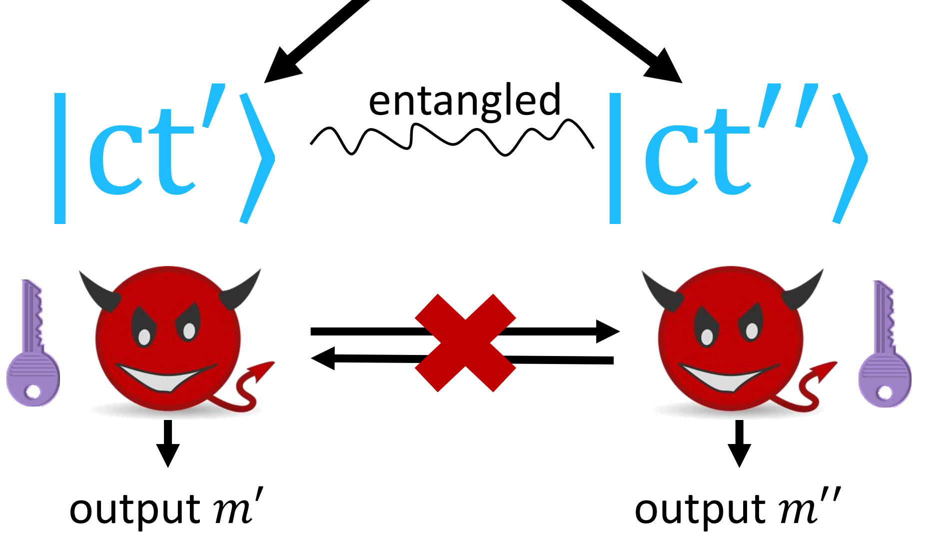
[BL20]



Adversary wins if $m = m' = m''$ with noticeable probability

One-Way Secure UE

[BL20]

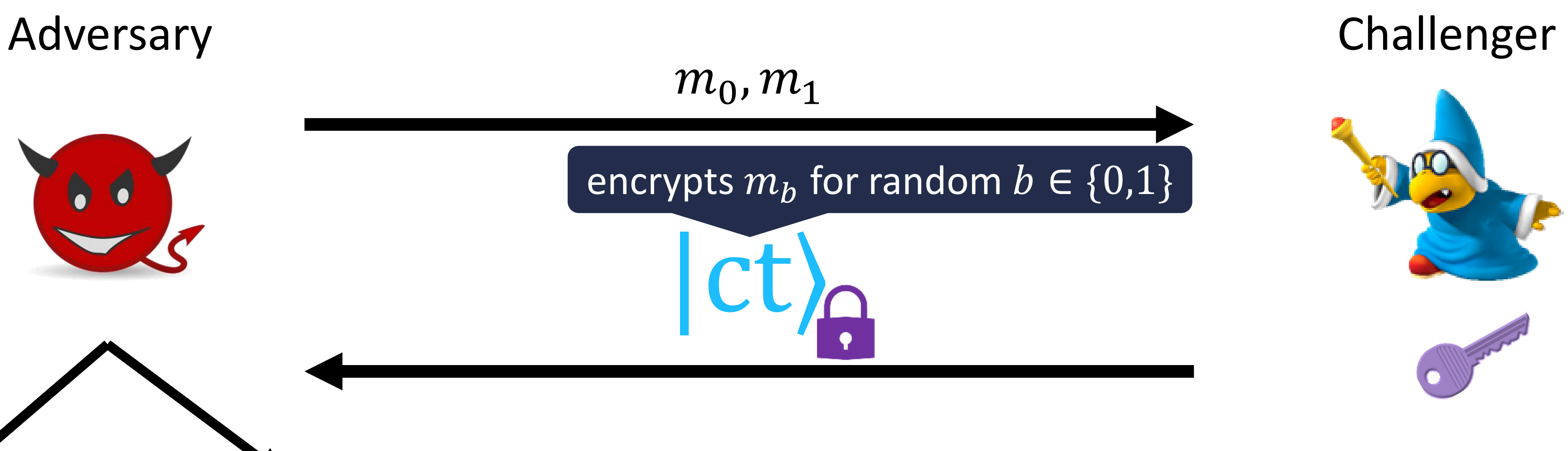


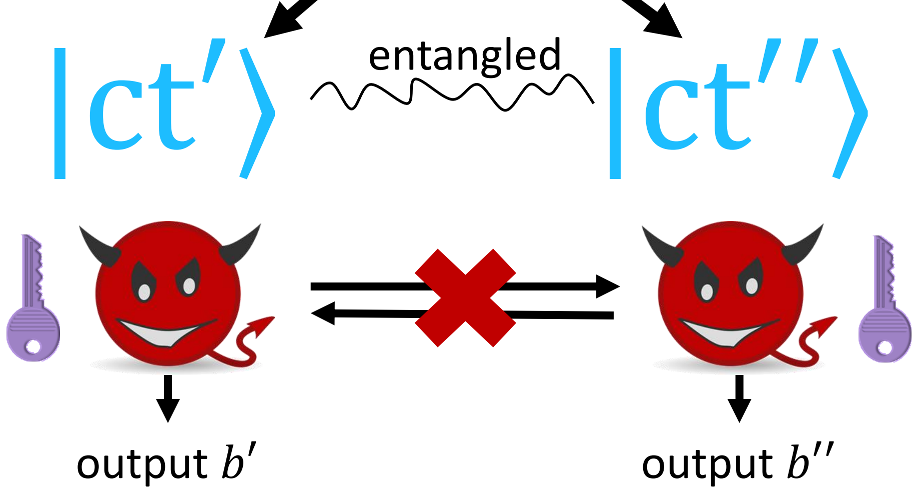
Adversary wins if $m = m' = m''$
with noticeable probability

Can be constructed information theoretically!

Semantically Secure UE

[BL20]

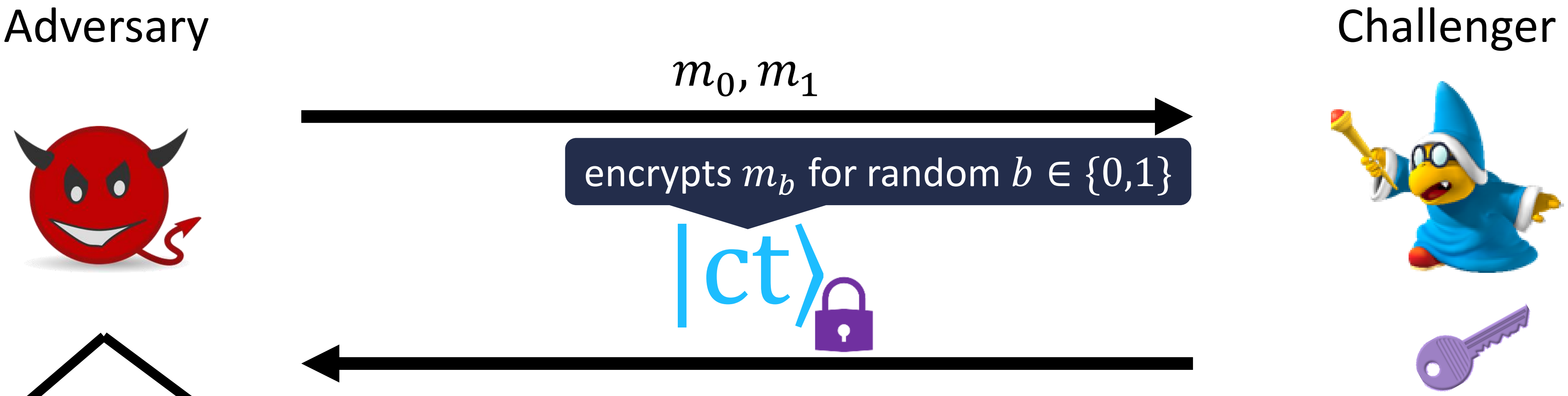


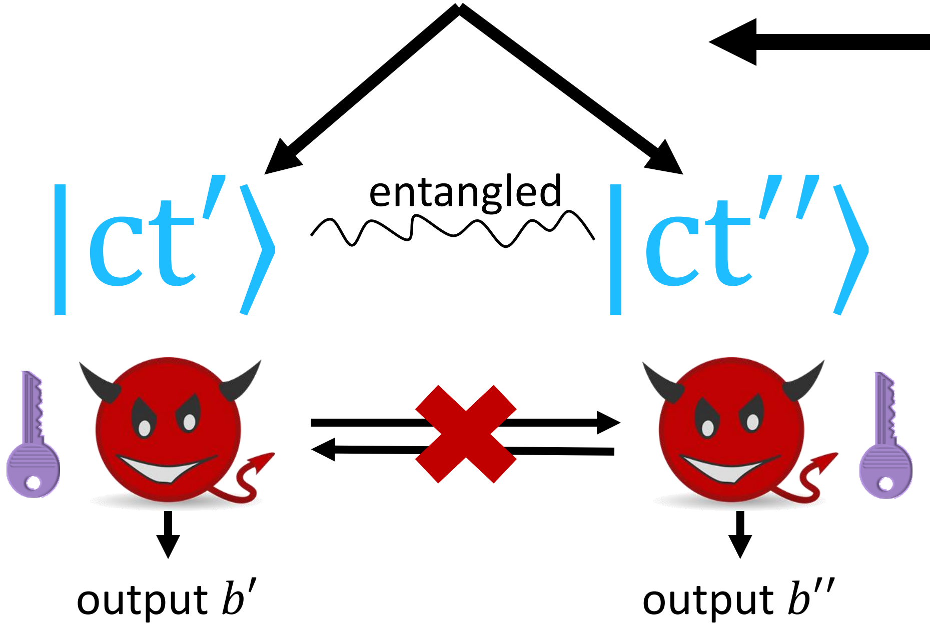


Adversary wins if $b = b' = b''$ with noticeable probability over 1/2

Semantically Secure UE

[BL20]





Adversary wins if $b = b' = b''$ with noticeable probability over 1/2

No constructions in the plain model from standard assumptions!

Why Is Semantically Secure UE So Much Harder?

1. Entanglement makes the standard search to decision techniques challenging to implement

2. (Second stage) adversary learning the key along with a function of the ciphertext is at odds with most classical cryptographic techniques

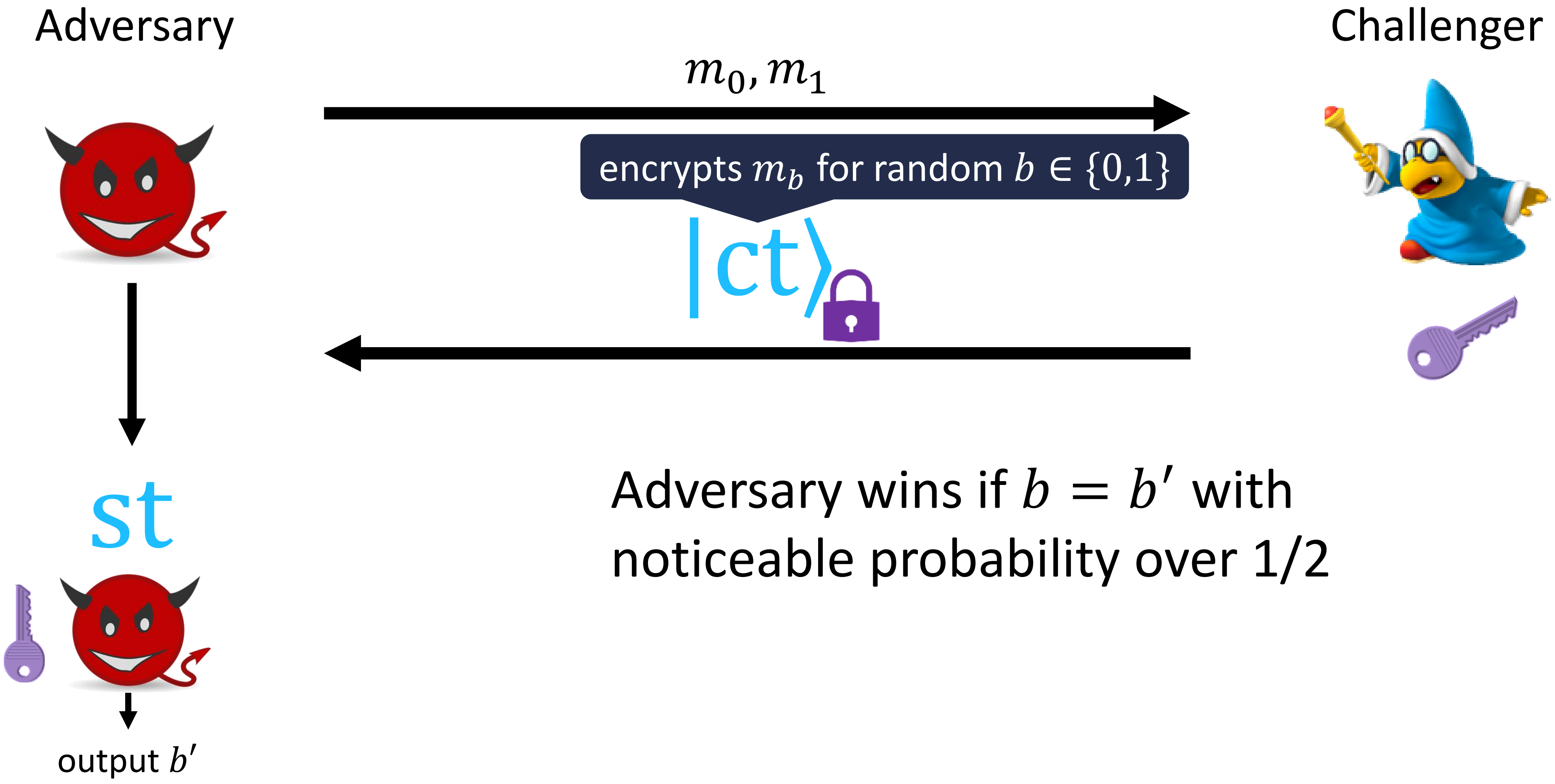
Why Is Semantically Secure UE So Much Harder?

1. Entanglement makes the standard search to decision techniques challenging to implement

2. (Second stage) adversary learning the key along with a function of the ciphertext is at odds with most classical cryptographic techniques

Does untelegraphability still provide a meaningful notion here?

Semantically Secure Untelegraphable Encryption



Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model

Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model
- Collusion-resistant security from one-way functions (OWFs)

Adversary can make many encryption queries, separates UTE from UE

Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model
- Collusion-resistant security from one-way functions (OWFs)
- Everlasting (collusion-resistant) security in the quantum random oracle model (QROM)

Second stage adversary can be computationally unbounded

Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model
- Collusion-resistant security from one-way functions (OWFs)
- Everlasting (collusion-resistant) security in the quantum random oracle model (QROM)
- Secure UTE from one-shot MACs in the classical oracle model, such that UE security is broken for an *unbounded* polynomial number of decryptors

Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model
- Collusion-resistant security from one-way functions (OWFs)
- Everlasting (collusion-resistant) security in the quantum random oracle model (QROM)
- Secure UTE from one-shot MACs in the classical oracle model, such that UE security is broken for an *unbounded* polynomial number of decryptors
- Untelegraphable functional encryption

Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model
- Collusion-resistant security from one-way functions (OWFs)
- Everlasting (collusion-resistant) security in the quantum random oracle model (QROM)
- Secure UTE from one-shot MACs in the classical oracle model, such that UE security is broken for an *unbounded* polynomial number of decryptors
- Untelegraphable functional encryption

Previously required oracles [Aar19,Kre21] or indistinguishability obfuscation [ÇG24]!

Can relax collusion-resistance to get a lower-bound from PRSGs!

Applications:

- Hyper-efficient shadow tomography cannot exist if collusion-resistant UTE exists, and "weakly-efficient" shadow tomography cannot exist if everlasting collusion-resistant UTE exists

Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model
- Collusion-resistant security from one-way functions (OWFs)
- Everlasting (collusion-resistant) security in the quantum random oracle model (QROM)
- Secure UTE from one-shot MACs in the classical oracle model, such that UE security is broken for an *unbounded* polynomial number of decryptors
- Untelegraphable functional encryption

Applications:

- Hyper-efficient shadow tomography cannot exist if collusion-resistant UTE exists, and "weakly-efficient" shadow tomography cannot exist if everlasting collusion-resistant UTE exists
- Secret sharing for all poly-size policies that is resilient to *joint* and *unbounded* classical leakage

[ÇGLR24]: limited to local leakage on each share

Our Results

Untelegraphable Encryption (UTE):

- Information-theoretic semantic security in the plain model
- Collusion-resistant security from one-way functions (OWFs)
- Everlasting (collusion-resistant) security in the quantum random oracle model (QROM)
- Secure UTE from one-shot MACs in the classical oracle model, such that UE security is broken for an *unbounded* polynomial number of decryptors
- Untelegraphable functional encryption

This Talk

Applications:

- Hyper-efficient shadow tomography cannot exist if collusion-resistant UTE exists, and "weakly-efficient" shadow tomography cannot exist if everlasting collusion-resistant UTE exists
- Secret sharing for all poly-size policies that is resilient to *joint* and *unbounded* classical leakage

Primary Tool: Non-Committing SKE (NCE)

[JL00,CHK05]

Primary Tool: Non-Committing SKE (NCE)

[JL00,CHK05]

Functions like a regular SKE scheme:

$$\mathrm{KeyGen}(1^\lambda) \to (\mathrm{ek}, \mathrm{dk})$$

$$\mathrm{Encrypt}(\mathrm{ek}, m) \to \mathrm{ct}$$

$$\mathrm{Decrypt}(\mathrm{dk}, \mathrm{ct}) \to m$$

Primary Tool: Non-Committing SKE (NCE)

[JL00,CHK05]

Functions like a regular SKE scheme:

$\mathrm{KeyGen}(1^{\lambda}) \rightarrow (\mathrm{ek}, \mathrm{dk})$

$\mathrm{Encrypt}(\mathrm{ek}, m) \rightarrow \mathrm{ct}$

$\mathrm{Decrypt}(\mathrm{dk}, \mathrm{ct}) \rightarrow m$

But can also **fake** ciphertexts:

$\mathrm{Fake}(\mathrm{ek}) \rightarrow (\mathrm{ct}, \mathrm{st})$

$\mathrm{Reveal}(\mathrm{st}, m') \rightarrow \mathrm{dk}'$

Primary Tool: Non-Committing SKE (NCE)

[JL00,CHK05]

Functions like a regular SKE scheme:

$\mathrm{KeyGen}(1^\lambda) \to (\mathrm{ek}, \mathrm{dk})$

$\mathrm{Encrypt}(\mathrm{ek}, m) \to \mathrm{ct}$

$\mathrm{Decrypt}(\mathrm{dk}, \mathrm{ct}) \to m$

But can also **fake** ciphertexts:

$\mathrm{Fake}(\mathrm{ek}) \to (\mathrm{ct}, \mathrm{st})$

$\mathrm{Reveal}(\mathrm{st}, m') \to \mathrm{dk}'$

Security:

Adversary

Challenger

Primary Tool: Non-Committing SKE (NCE)

[JL00,CHK05]

Functions like a regular SKE scheme:

$\mathrm{KeyGen}(1^\lambda) \rightarrow (\mathrm{ek}, \mathrm{dk})$

$\mathrm{Encrypt}(\mathrm{ek}, m) \rightarrow \mathrm{ct}$

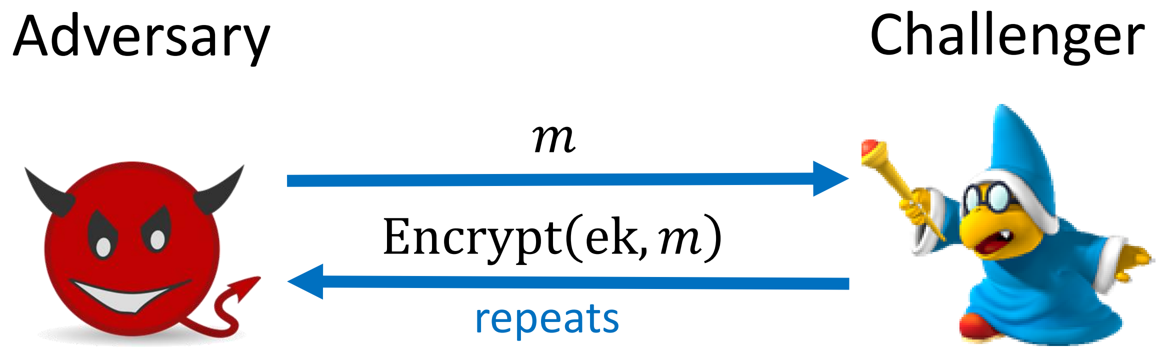
$\mathrm{Decrypt}(\mathrm{dk}, \mathrm{ct}) \rightarrow m$

But can also **fake** ciphertexts:

$\mathrm{Fake}(\mathrm{ek}) \rightarrow (\mathrm{ct}, \mathrm{st})$

$\mathrm{Reveal}(\mathrm{st}, m') \rightarrow \mathrm{dk}'$

Security:



Primary Tool: Non-Committing SKE (NCE)

[JL00,CHK05]

Functions like a regular SKE scheme:

$\mathrm{KeyGen}(1^\lambda) \to (\mathrm{ek}, \mathrm{dk})$

$\mathrm{Encrypt}(\mathrm{ek}, m) \to \mathrm{ct}$

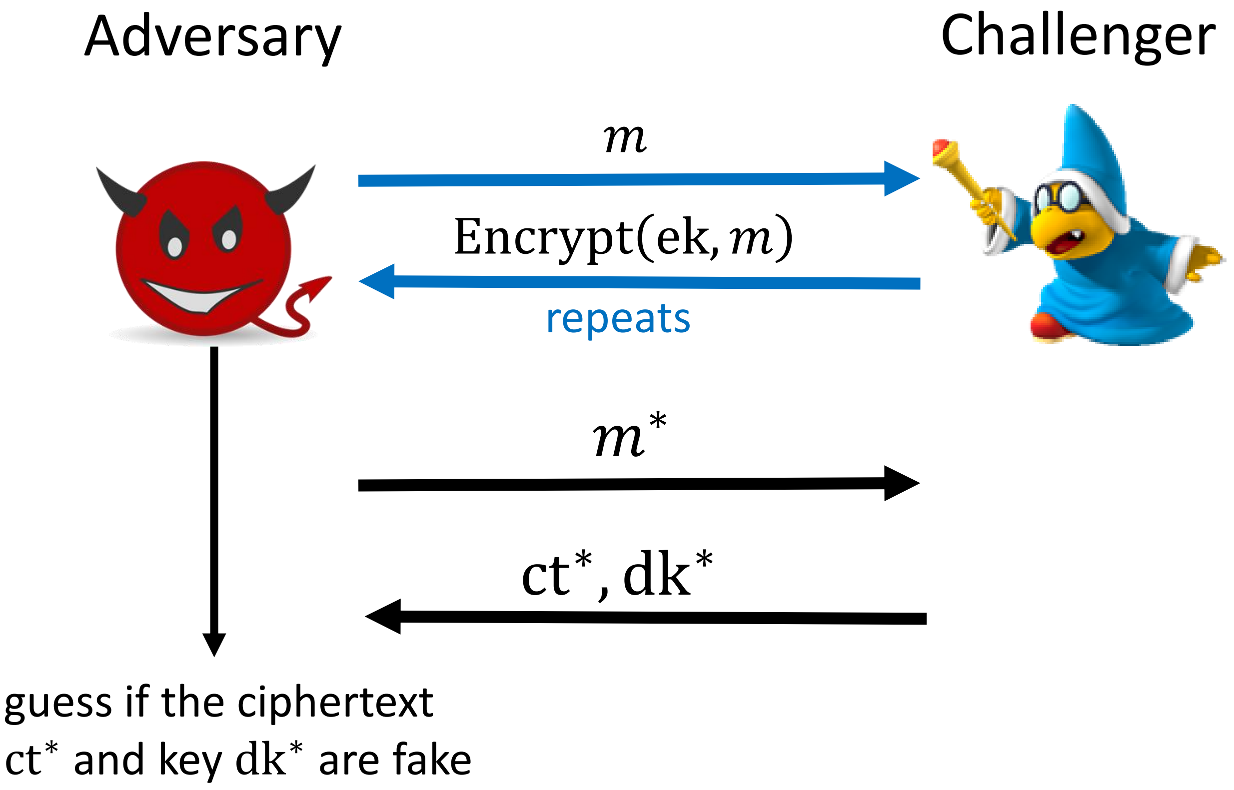
$\mathrm{Decrypt}(\mathrm{dk}, \mathrm{ct}) \to m$

But can also **fake** ciphertexts:

$\mathrm{Fake}(\mathrm{ek}) \to (\mathrm{ct}, \mathrm{st})$

$\mathrm{Reveal}(\mathrm{st}, m') \to \mathrm{dk}'$

Security:



Primary Tool: Non-Committing SKE (NCE)

[JL00,CHK05]

Functions like a regular SKE scheme:

$\mathrm{KeyGen}(1^\lambda) \to (\mathrm{ek}, \mathrm{dk})$

$\mathrm{Encrypt}(\mathrm{ek}, m) \to \mathrm{ct}$

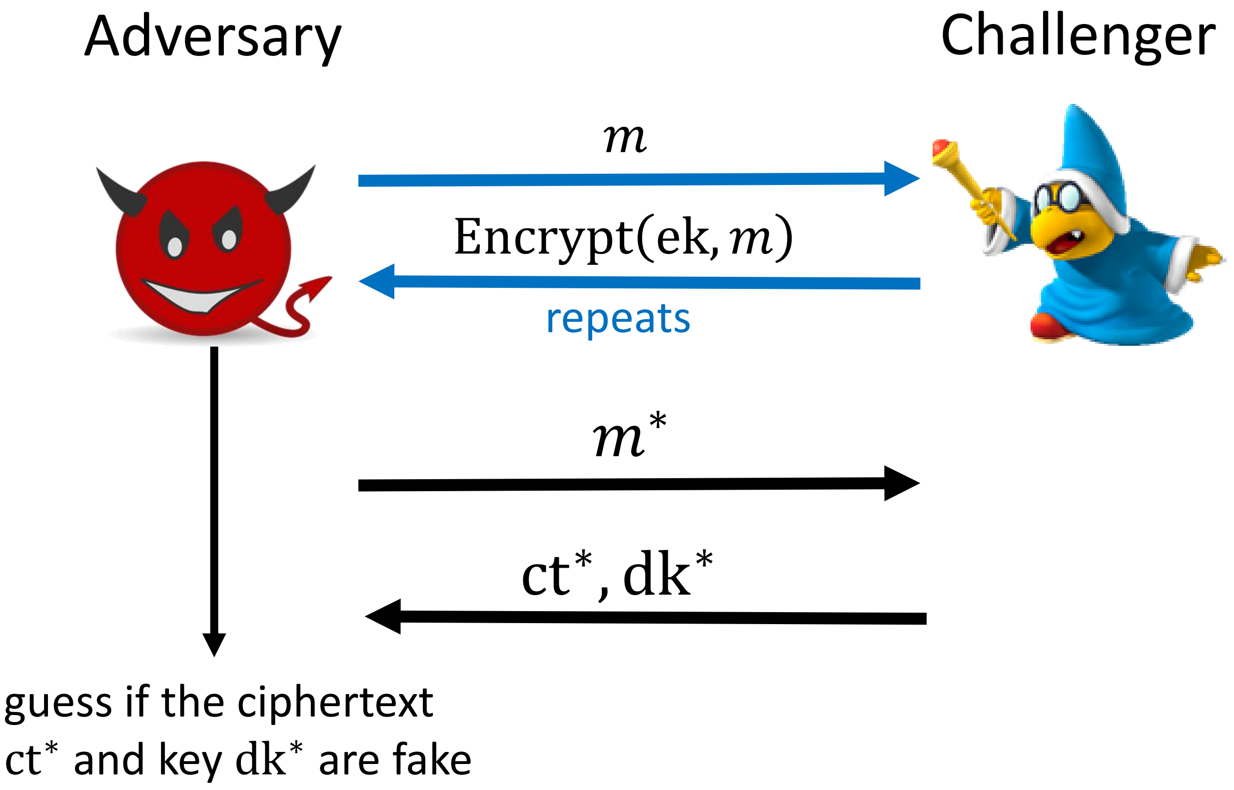
$\mathrm{Decrypt}(\mathrm{dk}, \mathrm{ct}) \to m$

But can also **fake** ciphertexts:

$\mathrm{Fake}(\mathrm{ek}) \to (\mathrm{ct}, \mathrm{st})$

$\mathrm{Reveal}(\mathrm{st}, m') \to \mathrm{dk}'$

Security:



Can be constructed from OWFs!

Warm-Up: Constructing Semantically Secure UTE

- Ingredients:
  - One-way secure UTE (follows from one-way secure UE)
  - Universal hash family with domain $\{0,1\}^n$ and range $\{0,1\}^\lambda$

Warm-Up: Constructing Semantically Secure UTE

- Ingredients:
  - One-way secure UTE (follows from one-way secure UE)
  - Universal hash family with domain $\{0,1\}^n$ and range $\{0,1\}^\lambda$

- Construction:
  - **Secret key:** the OW secure UTE key $\mathrm{sk}_{\mathrm{OW}}$, a random function h from the hash family, and a random string $r \in \{0,1\}^\lambda$

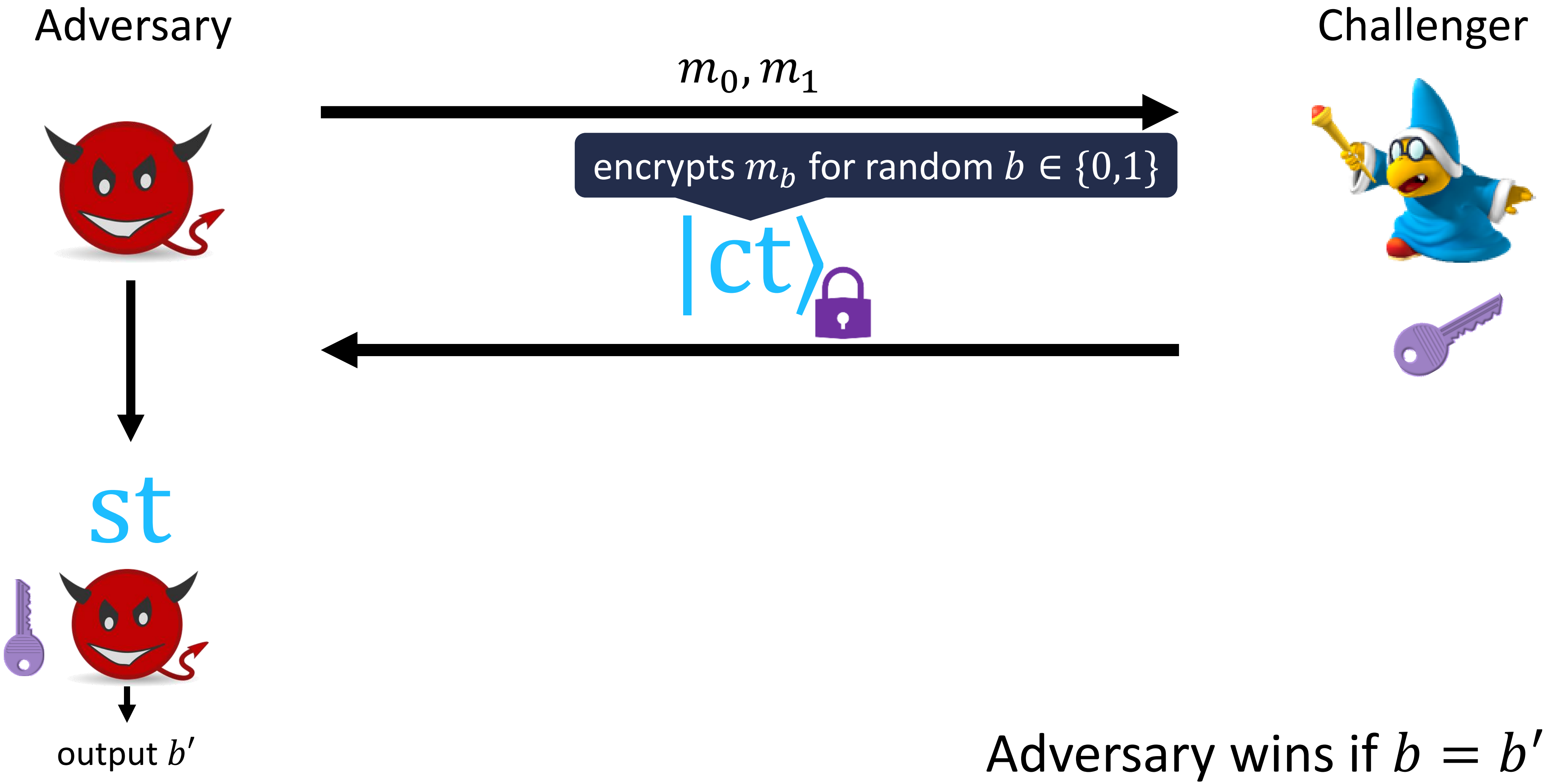
Warm-Up: Constructing Semantically Secure UTE

- Ingredients:
  - One-way secure UTE (follows from one-way secure UE)
  - Universal hash family with domain $\{0,1\}^n$ and range $\{0,1\}^\lambda$

- Construction:
  - **Secret key:** the OW secure UTE key $\mathrm{sk}_{\mathrm{OW}}$, a random function h from the hash family, and a random string $r \in \{0,1\}^\lambda$
  - **Ciphertext for message $m \in \{0,1\}^\lambda$:** an encryption $|\mathrm{ct}_{\mathrm{OW}}\rangle$ of a random message $x \in \{0,1\}^n$ and a string $r' = r \oplus h(x) \oplus m$

Functions like a "one-time NCE"

Proving Security



Adversary wins if $b = b'$ with noticeable probability over 1/2

Proving Security

Adversary

Challenger

m_0, m_1

$r \oplus h(x) \oplus m_b$

$(|\mathrm{ct_{OW}}\rangle, r')$

$(\mathrm{sk_{OW}}, h, r)$

st

$(\mathrm{sk_{OW}}, h, r)$

output b'

Adversary wins if $b = b'$ with noticeable probability over 1/2

Proving Security

Adversary

m_0, m_1

Challenger

uniform

$(|\mathrm{ct}_{\mathrm{OW}}\rangle, r')$

$(\mathrm{sk}_{\mathrm{OW}}, h)$

st

$r' \oplus h(x) \oplus m_b$

$(\mathrm{sk}_{\mathrm{OW}}, h, r)$

output b'

Adversary wins if $b = b'$ with noticeable probability over 1/2

Proving Security

Adversary

Challenger

m_0, m_1

uniform

$(|\mathrm{ct_{OW}}\rangle, r')$

$(\mathrm{sk_{OW}}, h)$

st

$r' \oplus h(x) \oplus m_b$

$(\mathrm{sk_{OW}}, h, r)$

output b'

By OW security, x has high entropy from the view of the second stage adversary even given $\mathrm{sk_{OW}}$!

Adversary wins if $b = b'$ with noticeable probability over 1/2

Proving Security

Adversary

Challenger

m_0, m_1

uniform

$(|\text{ct}_{\text{OW}}\rangle, r')$

$(\text{sk}_{\text{OW}}, h)$

st

$r' \oplus h(x) \oplus m_b$

$(\text{sk}_{\text{OW}}, h, r)$

output b'

By OW security, x has high entropy from the view of the second stage adversary even given sk_{OW}!

Thus, $h(x)$ is uniform and hides m_b by the leftover hash lemma

Adversary wins if $b = b'$ with noticeable probability over 1/2

Collusion-Resistant UTE

- Ingredients:
  - One-time semantically secure UTE (just shown)
  - Non-Committing SKE

Collusion-Resistant UTE

- Ingredients:
  - One-time semantically secure UTE (just shown)
  - Non-Committing SKE

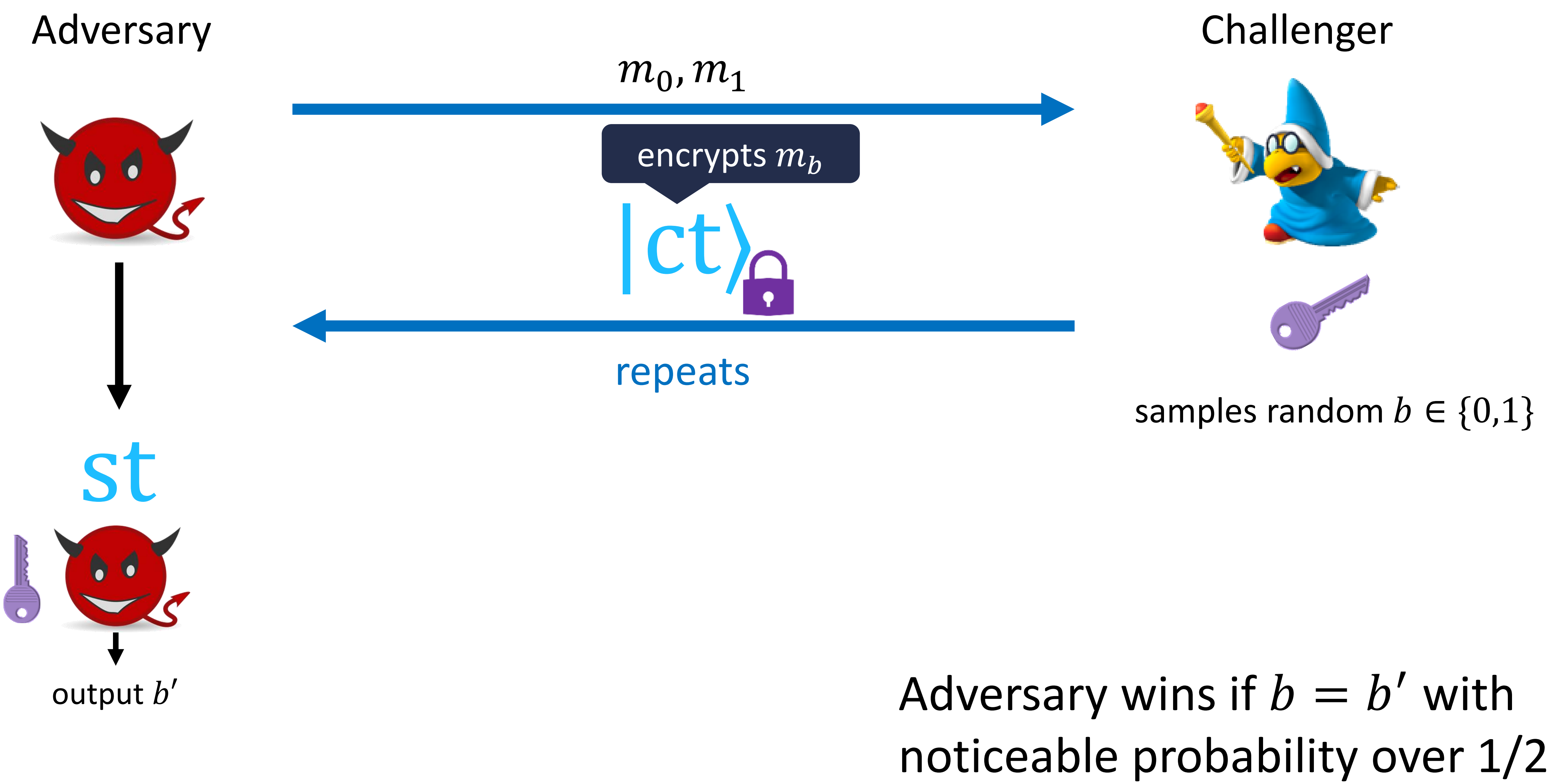
- Construction:
  - **Encryption and decryption key:** the NCE encryption and decryption keys

Collusion-Resistant UTE

- Ingredients:
  - One-time semantically secure UTE (just shown)
  - Non-Committing SKE

- Construction:
  - **Encryption and decryption key:** the NCE encryption and decryption keys
  - **Ciphertext for message m:** sample a secret key $\mathrm{sk}_{1\mathrm{UTE}}$ for the one-time UTE scheme, output an encryption $|\mathrm{ct}_{1\mathrm{UTE}}\rangle$ of m along with an NCE encryption $\mathrm{ct}_{\mathrm{NCE}}$ of $\mathrm{sk}_{1\mathrm{UTE}}$

Proving Security



Proving Security

Adversary

Challenger

m_0, m_1

encrypts m_b

encrypts fresh $\mathsf{sk}_{1\mathrm{UTE}}$

$(|\mathsf{ct}_{1\mathrm{UTE}}\rangle, \mathsf{ct}_{\mathrm{NCE}})$

repeats

$(\mathsf{ek}, \mathsf{dk})$

samples random $b \in \{0,1\}$

st

dk

output b'

Adversary wins if $b = b'$ with noticeable probability over 1/2

Proving Security

Adversary

Challenger

$(\mathrm{ek}, \mathrm{dk})$

samples random $b \in \{0,1\}$

m_0, m_1

encrypts m_b

fake encryption

$(|\mathrm{ct}_{1\mathrm{UTE}}\rangle, \mathrm{ct}_{\mathrm{NCE}})$

repeats

st

reveals $\mathrm{sk}_{1\mathrm{UTE}}$

dk

output b'

Can fake NCE part of a given query and still answer others

Adversary wins if $b = b'$ with noticeable probability over 1/2

Proving Security

Adversary

Challenger

m_0, m_1

encrypts 0

fake encryption

$(|\mathrm{ct}_{1\mathrm{UTE}}\rangle, \mathrm{ct}_{\mathrm{NCE}})$

repeats

$(\mathrm{ek}, \mathrm{dk})$

samples random $b \in \{0,1\}$

st

reveals $\mathrm{sk}_{1\mathrm{UTE}}$

dk

output b'

Can fake NCE part of a given query and still answer others

Can switch UTE ciphertext of the same query to an encryption of 0

Adversary wins if $b = b'$ with noticeable probability over 1/2

Shadow Tomography

[Aar19]

Shadow Tomography

[Aar19]

$$E: [M] \times \mathcal{H} \rightarrow \{0,1\}$$

Set of M binary outcome measurements that act on n qubit states (represented by a circuit E)

$$|\varphi\rangle^{\otimes k}$$

k copies of an unknown state

shadow tomographer 9000

$$C$$

Quantum circuit that estimates $\Pr[E(i, |\varphi\rangle) = 1]$ up to error ϵ

Shadow Tomography

[Aar19]

$$E: [M] \times \mathcal{H} \to \{0,1\}$$

Set of M binary outcome measurements that act on n qubit states (represented by a circuit E)

$$|\varphi\rangle^{\otimes k} \rightarrow \text{shadow tomographer 9000} \rightarrow C$$

k copies of an unknown state

shadow tomographer 9000

Quantum circuit that estimates $\Pr[E(i, |\varphi\rangle) = 1]$ up to error ϵ

Can be done with $\text{poly}(\log(M), n, 1/\epsilon)$ copies!

Hyper-Efficient Shadow Tomography (HEST)

[Aar19]

$$E: [M] \times \mathcal{H} \rightarrow \{0,1\}$$

Set of M binary outcome measurements that act on n qubit states (represented by a circuit E)

$$|\varphi\rangle^{\otimes k}$$

k copies of an unknown state

shadow tomographer 9000

$$C$$

Quantum circuit that estimates $\Pr[E(i, |\varphi\rangle) = 1]$ up to error ϵ

A shadow tomography procedure is *hyper-efficient* if both the runtime and number of copies is $\mathrm{poly}(\log(M), n, 1/\epsilon)$

HEST vs Collusion-Resistant UTE

HEST vs Collusion-Resistant UTE

$$|\varphi\rangle^{\otimes k}$$

k copies of an unknown state

$$|\mathrm{ct}\rangle^{\otimes k}$$

k encryptions of a bit $b \in \{0,1\}$

HEST vs Collusion-Resistant UTE

$$|\varphi\rangle^{\otimes k}$$

k copies of an unknown state

$$[M]$$

indices for E

$$|\mathrm{ct}\rangle^{\otimes k}$$

k encryptions of a bit $b \in \{0,1\}$

$$\mathcal{DK}$$

set of decryption keys

HEST vs Collusion-Resistant UTE

$$|\varphi\rangle^{\otimes k}$$

k copies of an unknown state

$$[M]$$

indices for E

$$E$$

circuit of interest

$$|\mathrm{ct}\rangle^{\otimes k}$$

k encryptions of a bit $b \in \{0,1\}$

$$\mathcal{DK}$$

set of decryption keys

$$\mathrm{Decrypt}$$

decryption circuit

Attacking UTE with HEST

Adversary

query k times

$0,1$

Challenger

shadow tomographer 9000

encrypts b

$|\mathrm{ct}\rangle$

repeats

$(\mathrm{ek}, \mathrm{dk})$

samples random $b \in \{0,1\}$

$\mathrm{st} = C$

dk

compare $C(\mathrm{dk})$ to ½ and output b' accordingly

Adversary wins if $b = b'$ with noticeable probability over 1/2

Attacking UTE with HEST

Adversary

shadow tomographer 9000

$\mathrm{st} = C$

dk

compare $C(\mathrm{dk})$ to ½ and output b' accordingly

query k times

0,1

encrypts b

$|\mathrm{ct}\rangle$

repeats

Wins game with optimal advantage as long as $\epsilon < \frac{1}{2}$

Challenger

$(\mathrm{ek}, \mathrm{dk})$

samples random $b \in \{0,1\}$

Adversary wins if $b = b'$ with noticeable probability over 1/2

Open Problems

- Ruling out HEST for pure states: collusion-resistant UTE with pure ciphertexts and non-trivial security is sufficient
- Everlasting UTE in the plain model
- More applications of UTE and untelegraphability

Thanks for listening!

https://arxiv.org/abs/2410.24189