

On the feasibility of Unloneable Encryption & more

Araujo, Kalvogu, Li, Liu, Zhandry.

Abstract :

Unloneable encryption:

"one-time" encryption scheme s.t.

Any non-local adversary (A, B, c)

cannot simultaneously distinguish

encryptions of two equal length messages.

Prior works: focused on

simultaneous recovery of

the entire message

State of the art: No scheme is known to satisfy
unloneable indistinguishability
(even for 1-bit messages)

In this paper: (1) Schemes satisfying unloneable indistinguishability
exist unconditionally in the R.O.M.

(2) Show that a large class of schemes cannot
satisfy unloneable encryption —

(3) Also suggest the need of oracles.
Also show copy protection for single output point f.s.

§ 1. Introduction

No cloning allows one to realize many primitives that are classically impossible:

- (a) quantum money - & variants
 - (b) Tamper detection
 - (c) Quantum copy protection
 - (d) Secure Software Leasing
 - (e) Copy Protection
- & more.

Story: Uncloneable Encryption.

- It is a one-time secure encryption w/ quantum ciphertexts

has the following guarantee:

Informal

{

 [
 no adversary,
 given a ciphertext (modelled as a quantum state)
 can produce two (possibly entangled) states
 that both encode "some information"
 about the original message
]

This is formalized using a "splitting game" as follows:

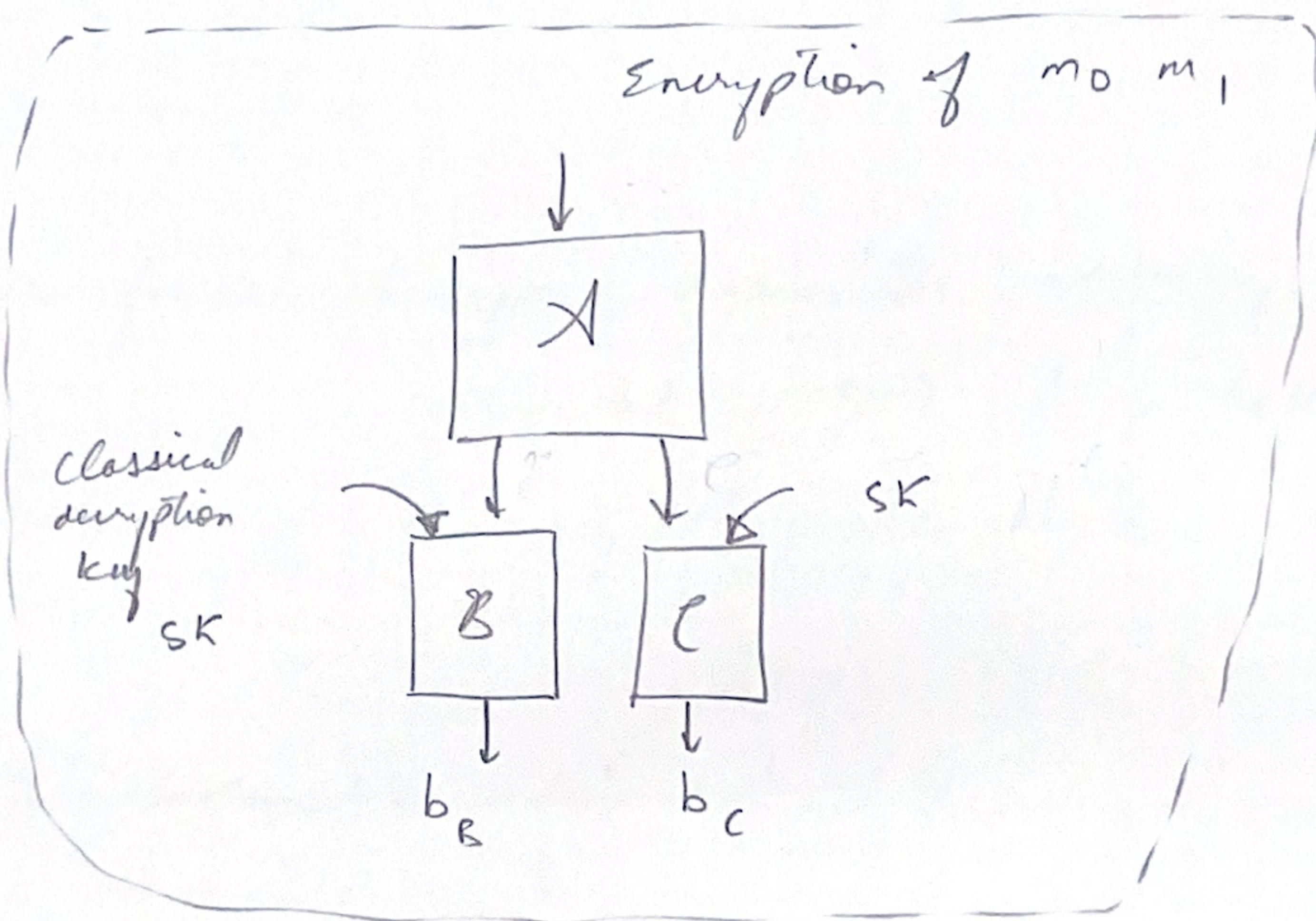
Consider:

A splitting adversary (A, B, C)

- first has A receive an encryption of m_0

for two messages $\{m_0, m_1\}$.

- A then outputs a bipartite state to $B \& C$,



who also get the classical decryption key as an input &

who output b_B & b_C resp.

- They win if $b = b_B = b_C$.

NB: A could give the ciphertext to B in which case,
 B can output $b_B = b$ w.p. 1.

adversary

$\frac{1}{2} \rightarrow \text{reg}$

weakly indistinguishability

adversaries

adversary could be
b in both cases,
well.

allows A to compute b_A ,
 b_A to tell B b_A

but $b_B = b_A$
 $b_C = b_A$

weakly indistinguishability game
at least that of the
benign adv. winning the semantic
security game. -4-

Which means $\exists (\lambda, B, \epsilon)$ s.t.

it wins the splitly game w.p. $\frac{1}{2} + \epsilon$.

Require:

- (thus) security requires that no splitly adversary should win w.p. greater than $\frac{1}{2} + \text{negl}$.

Defⁿ: An encryption scheme satisfies unclonable indistinguishability
if holds for all splitly adversaries.

[Question for me: I suppose, again, the adversary could be unbounded or QPT & in both cases, this would make sense.]

NB: Unclonable indistinguishability
||

Semantic Security

\therefore a Semantic Adversary allows \mathcal{A} to compute b_A , it can send b_A to both $B \& C$

$$\text{who can output } b_B := b_A$$

$$b_C := b_A$$

\mathcal{B} wins the unclonable indistinguishability game w.p. at least that of the Semantic Adv. winning the semantic security game.

Applications of Unclonable Encryption:

Me: So why does
that help?

- \Rightarrow private key quantum money.
- Prevents storage attacks — where malicious entities can steal ciphertexts & hope to decrypt them when if the secret key is compromised.
- \Rightarrow copy protection for a restricted class of functions,
w/ computation al guarantees.

I thought we
already had
constructions in
that setting.

Prior works: Previous works — showed a weaker property,

"unclonability":

Same as unclonable indistinguishability
except, (b) the message m being encrypted
is sampled uniformly at random

§

(b) B & C are expected to
guess the message m in

: NR: this is obviously far less useful; doesn't even imply semantic security, its entirety

Main Question: Do encryption schemes satisfying uncloneable indistinguishability exist?

Story:

Copy protection for Point Functions

- Another primitive closely related to uncloneable encryp".
- Informally: it is a compiler that converts any program into a quantum state s.t. (a) original functionality is maintained & (b) the following property holds:
 - a splitting adversary (A, B, C)
 - (i) first has A receive as input a copy-protected state that can be used to compute a function f
 - (ii) A then outputs a bipartite state to $B \& C$.

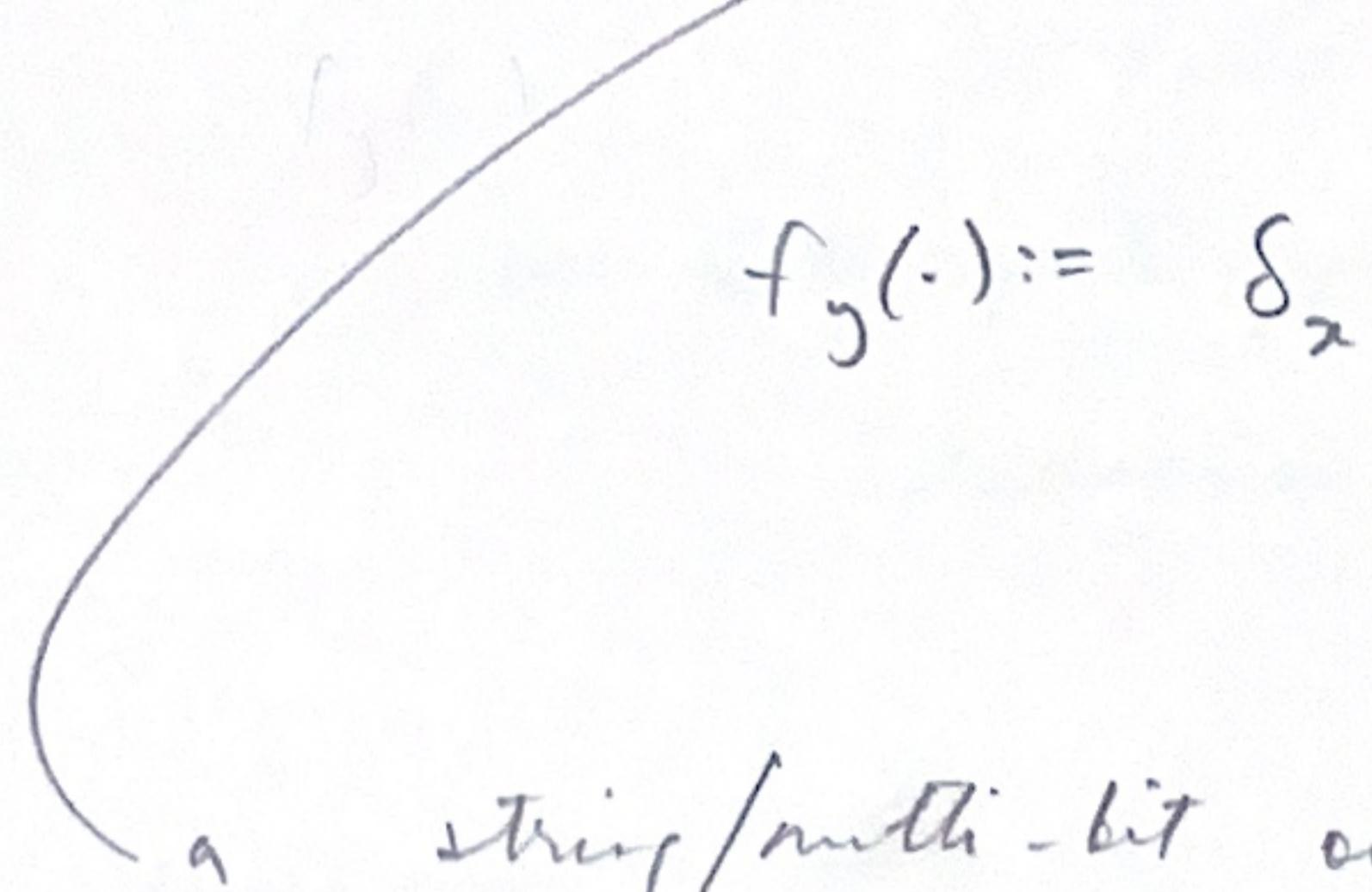
The security requirement is that both $B \& C$ should not be able to simultaneously compute f .

Re: I guess for "learnable functions" this is already impossible — I can learn the function & pass on its description to B&C, breaking copy-protection trivially.

Prior work

[AL21] • copy protection is known to be impossible for general unlearnable functions.

Here • What about simpler classes of functions?

e.g. point functions

 a (single-bit output)
 point f^* is just a delta function:

$$f_y(\cdot) := \delta_{xy} = \begin{cases} 1 & y = x \\ 0 & \text{else} \end{cases}$$

a string/multi-bit output point f^* is the same except it outputs a large string instead of a bit.

Prior works: construct copy protection for either

[CMP20] (i) Multi-bit point functions or

[AK21] (ii) Single-bit point f^* 's but w/
 "const security"

Me: I guess for "learnable functions" this is already impossible - I can learn the function & pass on its description to B&C, breaking copy-protection trivially.

Prior work

[AL21] • copy protection is known to be impossible for general unlearnable functions.

[Zhe] • What about simpler classes of functions?

e.g. point functions λ
 a single-bit output
 point f^* is just a delta function:

$$f_y(\cdot) := \delta_{x,y} = \begin{cases} 1 & y = y \\ 0 & \text{else} \end{cases}$$

a string/multi-bit output point f^* is the same except it outputs a large string instead of a bit.

Prior works: constant copy protection for either

[CMP20] (i) Multi-bit point functions or

[AK21] (ii) Single-bit point f^* 's but w/ "const security"

Question: Does copy protection for single-bit output functions, w/ optimal security, exist?

§ 1.1 Achieving Uncloneable Indistinguishability: Challenges

Story: How hard can it be! — we want one-time security

: One may think: going from the "weaker unclonability property" to achieving uncloneable indistinguishability might be easy.

: ∵ the former is a search problem & the latter is a decision problem one could hope to apply known search -to- decision reduction (i.e. if search is hard, then decision is hard).

[doesn't mean the other way]
which is trivial), that
a search solver solves
decision

Reducing Prob A To Prob B

means it suffices to solve B
to solve A.

i.e. can reduce the search problem to a decision problem & then if there's a decision solver, it also solves the search problem & if we already have a proof showing search is hard, then so is decision).

: But this intuition is false - ∵ quantum effects &
∴ unbreakable encryption involves
multiple parties.

Some of the obvious approaches that fail
(also give us some intuition about why
unbreakable encryption is so non-trivial).

(A) Why it is tricky to use usual cryptographic tools -
The secret key is revealed in the end.

- Consider this construction:

$\text{Gen}(1^x)$: $k \leftarrow \{0,1\}^X$, return k .

$\text{Enc}_k(m)$: $a \leftarrow \{0,1\}^X$,
return $(a, \text{PRF}(k,a) \oplus m)$

Me: Recall this is the CPA secure encryption
we reviewed from Koblitz & Lindell

But this intuition is false - ∵ of quantum effects &
∴ unclonable encryption involves
multiple parties.

Some of the obvious approaches that fail:

(also give us some intuition about why
unclonable encryption is so non-trivial).

(A) Why it is trivial to use usual cryptographic tools -
the secret key is revealed in the end.

- Consider this construction:

$\text{Gen}(1^\lambda)$: $k \leftarrow \{0,1\}^\lambda$, return k .

$\text{Enc}_k(m)$: $s \leftarrow \{0,1\}^\lambda$,
return $(s, \text{PRF}(k,s) \oplus m)$

Me: Recall this is the CPA secure encryption
we reviewed from Koblitz & Lindell.

- NB: In the security game, the secret key k
will be revealed, to both B & C.

∴ clearly, both can learn m , breaking
any notion of unclonability.

(B) How does one perform security reduction?

- Which adversary among B & C should be used to break the underlying game?
 - e.g. (i) If B is used to break the game,
A could simply have handed over
the ciphertext to C.
So B indeed cannot be used to
break the underlying game.
 - (ii) What if A sends a superposition of
"entire ciphertext to B" &
"entire ciphertext to C".
- (c) Extending unclenable indistinguishability from
1-bit messages to
multi-bit messages.
 - In classical crypto, 1-bit to multi-bit is
a hybrid argument.
 - This approach, (at least directly) fails here:
e.g. suppose a 2-bit message $m = m_1 \parallel m_2$
is encrypted as P_1, P_2 , where
 P_i is encryption of m_i .
This scheme is insecure.

\therefore it allows a splitting adversary (A, B, C) to distinguish encryptions of 00 from those of 11: (w.p. 1)

A sends p_1 to B & p_2 to C.

B & C : decrypt (using the secret key they receive)

to obtain b from p_1 & p_2 resp.)

C output b.

(D) [MST '21]: Majenz, Schaffner & Tahmasti give necessary conditions ciphertexts (satisfying the indistinguishability property) must satisfy.

Specifically: these ciphertexts, when represented as density matrices,

must have "large eigenvalues".

NB: the original scheme due to [BL'20]

doesn't satisfy this property.

(I'm skipping this for now)

An example that more concretely shows (A)(B)(C)(D) : Extractors.

Consider the scheme: m is encrypted as extractor w/ seed s.

$(p_x, \text{e.g. } \overbrace{\text{Ext}(s, x) \oplus m})$

satisfies the weak comlocoreability property classical encryption of a random seed.

[<I'm skipping this example for now>

§ 1.2 Our Results

Unclonable Encryption

Story: First, feasibility of unclonable encryption.

Thm (informal) 1.1. There exists an unconditionally secure one-time encryption scheme satisfying unclonable indistinguishability in the R.O.M.

Story: The construction is simple: makes novel use of "coset states" considered in recent work [CLLZ 21].

The analysis is involved: uses, notably, a "threshold projective implementation" introduced by Zhandry [Zha21].

[AK21]: Shows how to generically transform from one-time unclonable encryption to public key unclonable encryption.

(Corollary (inf) 1.2.) Assuming the existence of post-quantum public key encryption,
 ⇒ a post-quantum public-key

encryption scheme satisfying the uncloneable indistinguishability property, in the quantum random oracle model.

Story: Can one achieve uncloneable encryption in the plain model?

: They show a class of uncloneable encryption, they call "deterministic" are impossible to achieve.

encrypt & decrypt (are both unitary)
is U is U^\dagger

: The result continues to hold even if $U \notin U^\dagger$
take exponential time.

(informal)

Thm 1.3. There are no unconditionally secure deterministic one-time encryption schemes satisfying the uncloneable indistinguishability property.

Story:

- Any classical scheme can be made deterministic
(randomness absorbed in the secret key)
- Alternative proof that [BL20] cannot satisfy uncloneable indistinguishability.
(originally due to [MST21])

- Can be overcome by either
 - (1) computational assumptions
 - (2) non-unitary operations
(i.e. trace out at least a part of the system)

Copy-Protection for Point functions

Thm 1.4 (inv). \exists a copy-protection scheme for a single-bit output point function in the quantum random oracle model.

Story: Prior works show how to generically transform copy protection for point f's

uncloakable encryption to

BUT

these assume multi-bit output point functions.