On the feasibility of Unclonable Encryption & more

Ananth, Kaleoglu, Li, Liu, Zhandry.

Abstract:

Unclonable encryption:

"one-time" encryption scheme s.t.

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

cannot <u>simultaneously distinguish</u>

encryptions of two equal length messages.

Prior works: focussed on

<u>simultaneous recovery</u> of

the entire message

State of the art: No scheme is known to satisfy

unclonable indistinguishability

(even for 1-bit messages)

In this paper: (1) Schemes satisfying unclonable indistinguishability

exist unconditionally in the R.O.M.

(2) Show that a large class of schemes cannot

satisfy unclonable encryption —

suggesting the need of oracles.

(3) Also show copy protection for simple output pseudo

§ 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 <u>one-time</u> secure encryption w/ quantum ciphertexts

Informal

Satisfies the following guarantee:

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:

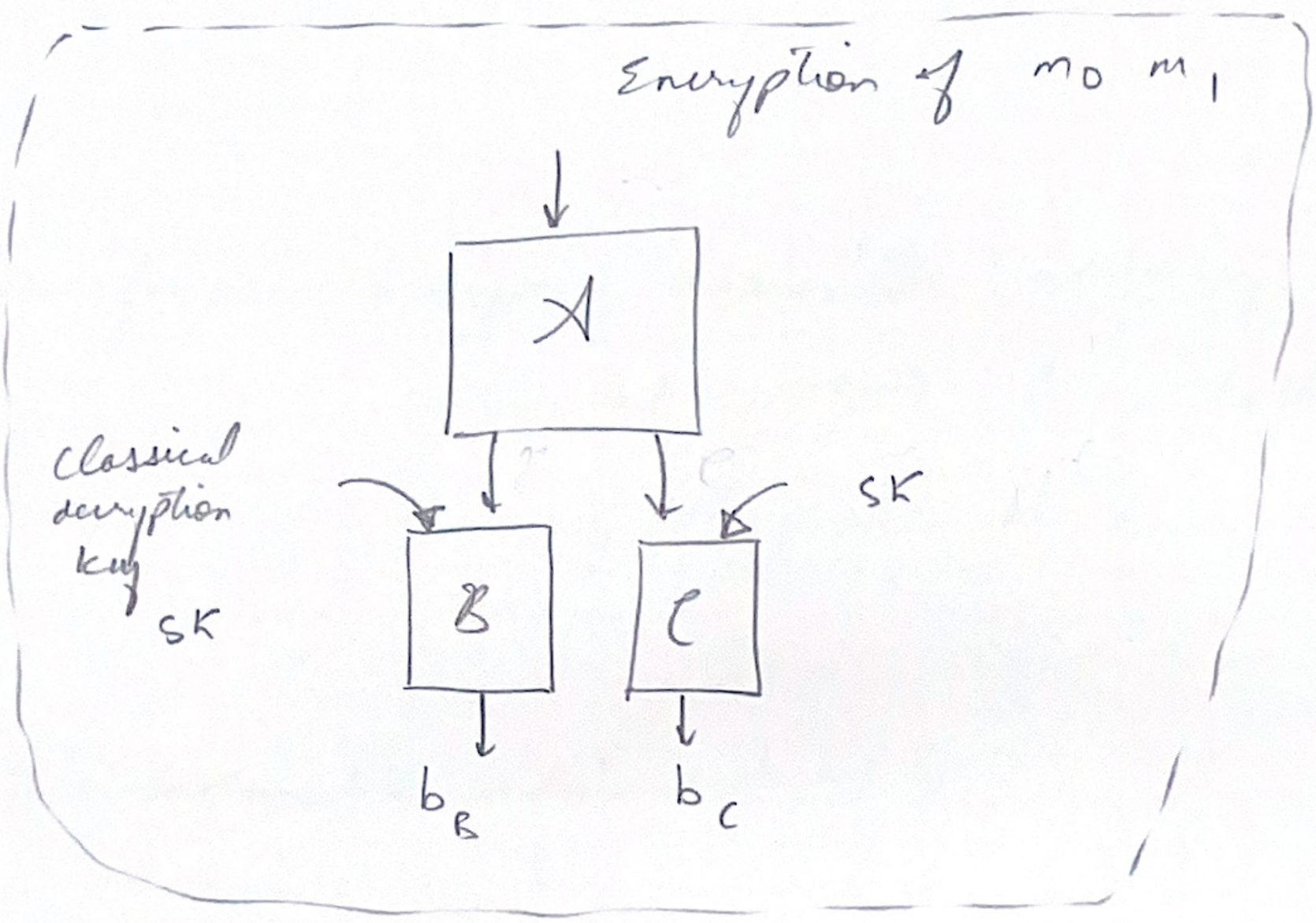
Consider:

A splitting Adversary (A, B, C)

- first has A receive an encryption of m_b

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 entire ciphertext to B in which case, B can output $b_B = b$ w.p. 1.

Which means $\exists (A, B, C)$ s.t.

it wins the splitting game w.p. $\frac{1}{2}$.

Require:

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

Def^: An encryption scheme satisfies **uncloneable indistinguishability** if holds for all splitting adversaries.

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

NB: Uncloneable indistinguishability

$\Downarrow$

Semantic Security

$\therefore$ a Semantic Adversary allows A to compute b_A,

it can send b_A to both B & C

who can output $b_B := b_A$

$b_C := b_A$

& win the uncloneable indistinguishability game w.p. at least that of the Semantic Adv. winning the semantic security game.

Applications of Uncloneable Encryption:

- ⇒ private key quantum money.

Me: So why does that help? I thought we already had constructions in that setting.

- Secret storage attacks —
  where malicious entities can steal ciphertexts & hope to decrypt them when/if the secret key is compromised.

- ⇒ copy protection for a restricted class of functions, w/ computational guarantees.

Prior works: Previous works — showed a weaker property, "uncloneability":

same as uncloneable indistinguishability except, (a) the <u>message m</u> being encrypted is sampled <u>uniformly</u> at random

&

(b) $\mathcal{B}$ & $\mathcal{C}$ are expected to guess the message m in its entirety

:NB: This is obviously far less useful; doesn't even imply semantic security,

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 — ∵ A 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^n is just a delta function:

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

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

Prior works: Construct copy protection for either

[CMP'20] (i) Multi bit point functions or

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

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

§1.1 Achieving Uncloneable Indistinguishability: Challenges

Me: not fully sure what this means; I guess one doesn't repeatedly split.

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

: One may think: going from the "weaker uncloneability 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.

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).

[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.

But this intuition is false — ∵ ∃ quantum effects &

∵ uncloneable encryption involves multiple parties.

Some of the obvious approaches that fail.
(also give us some intuition about why uncloneable 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:

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

$Enc_k(\tilde{m} \in \{0,1\})$: $s \leftarrow \{0,1\}^\lambda$,
return $(s, PRF(k,s) \oplus m)$

Re: Recall this is the CPA secure encryption we reviewed from Katz & 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 uncloneability.

(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 uncloneable indistinguishability from 1-bit messages to multi-bit messages.

. In classical crypto, 1-bit to multi-bit via a hybrid argument.

. This approach, (at least directly) fails here:

e.g. suppose a 2-bit message $m = m_1 \| m_2$ is encrypted as $\rho_1 \cdot \rho_2$ where ρ_i is encryption of m_i

This scheme is insecure.

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

$\mathcal{A}$ sends ρ_1 to $\mathcal{B}$ & ρ_2 to $\mathcal{C}$.

$\mathcal{B}$ & $\mathcal{C}$: decrypt (using the secret key they recieve) to obtain b from ρ_1 & ρ_2 resp.) & output b.

(D) [MST '21]: Majenz, Schaffner & Tahmasbi 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 $\overbrace{(\rho_x, C_s, \overline{Ext(s,x) \oplus m})}$ — extractor w/ seed s.

satisfies the weak uncloneability property — classical encryption of a random seed.

└ <I'm skipping this example for now>

§ 1.2 Our Results

Uncloneable Encryption

Story: First, feasibility of uncloneable encryption.

Thm (informal) 1.1. There exists an unconditionally secure one-time encryption scheme satisfying uncloneable 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 uncloneable encryption to public key uncloneable encryption.

Corollary (inf) (stated as a theorem) 1.2. Assuming the existence of post-quantum public key encryption, $\exists$ 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 encryptions, they call "deterministic" are impossible to achieve.

encryption & decryption (are both unitary)
is U is $U^\dagger$

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

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

"one-time encryption"
Story: • Any classical scheme can be made deterministic (randomness absorbed in the secret key)

• Alternate proof that [BL20] cannot satisfy uncloneable indistinguishability. (originally due to [MST21])

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

Copy-Protection for Point functions

Thm 1.4 (inf) ∃ a copy-protection scheme for single-bit output point functions in the quantum random oracle model.

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

BUT

these assume multi-bit output point functions.