§1.4 Technical Overview

Attempts based on Wiesner States.

story: We start by recalling the unclonable encryption scheme (original) due to Broadbent & Lord [BL20].

- Idea: Encrypt(m) := Sample a secret key x,
  Encode x into an unclonable state ρ_x.
  Encrypt m using x $Enc_x(m)$

: Intuitively, for any splitting adversary (A, B, C)

there's no way for A to split ρ_x into two quantum states s.t. non-communicating B & C can both recover info about x to decrypt $Enc_x(m)$.

- Choice of no-cloning states:
  (i) Wiesner conjugate coding: $\int$ The conjugate encoding of $x \in \{0,1\}^\lambda$ under $\theta \in \{0,1\}^\lambda$
  is given by $H^\theta |x\rangle$ &
  is denoted by $|x^\theta\rangle$.

(ii) the no-cloning property of Wiesner states is captured by by "monogamy of entanglement games" (MOE games) in [TFKW13, BL20].
(A, B, C)

[BL20] show that no strategy $\mathcal{A}$ wins the following MOE game w/ prob. more than 0.85^{λ}:

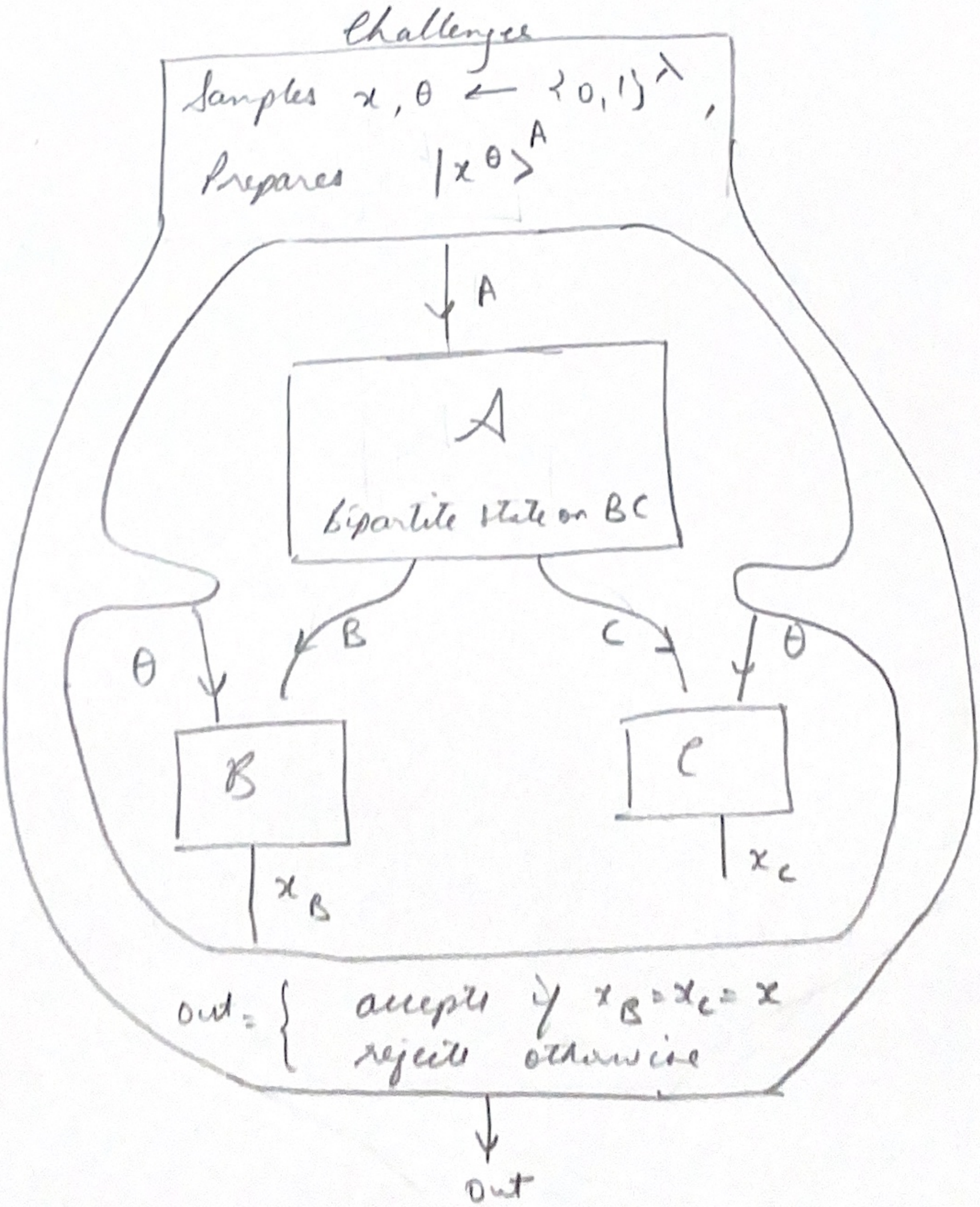

Fig1: MOE Game for Wiesner states.

(ii) the no-cloning property of Wisner states is captured by by "monogomy of entanglement games" (MOE games) in [TFKW13, BL20].
(A, B, C)

[BL20] show that no strategy wins the following MOE game w/ prob. more than 0.85^{λ}.

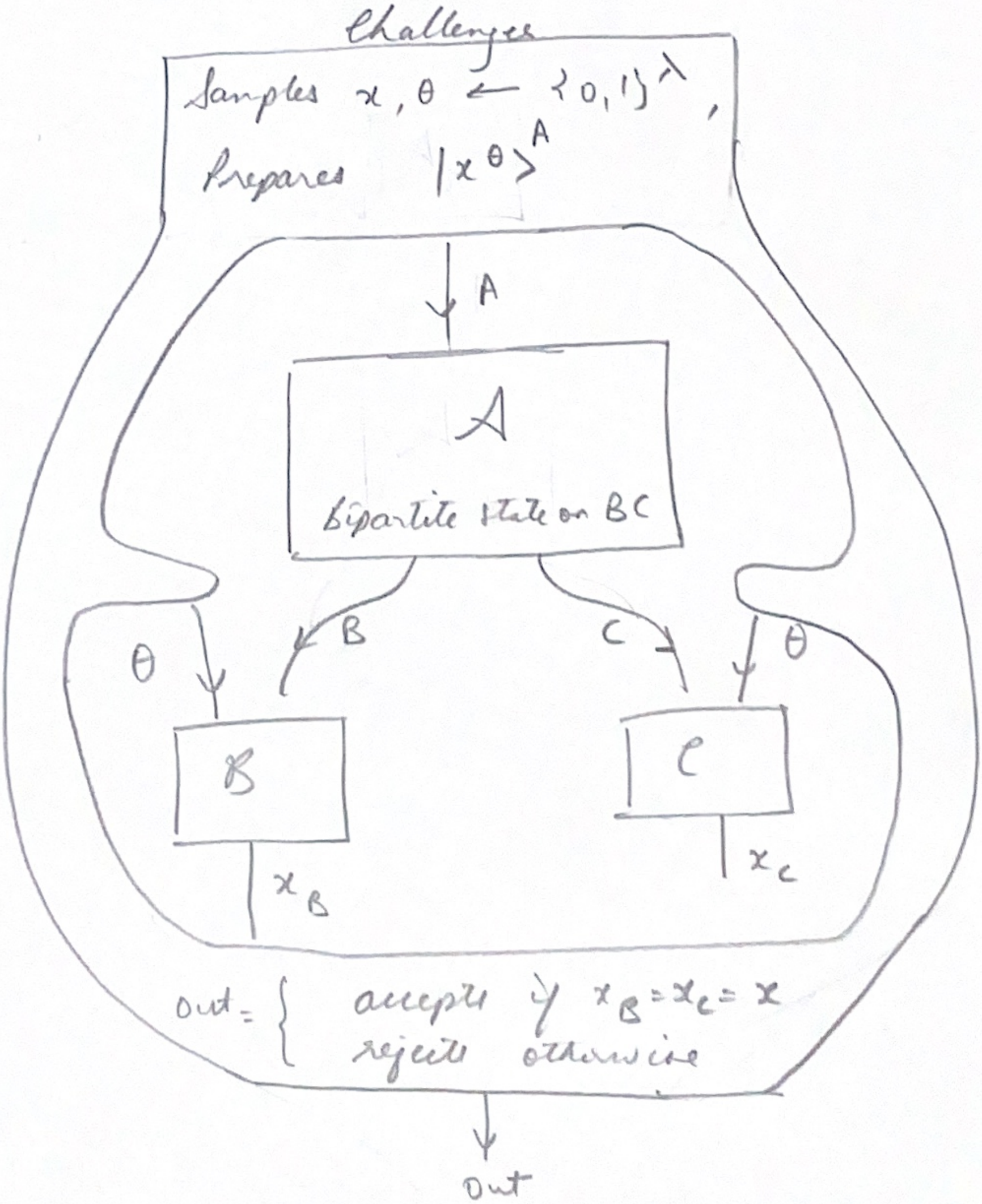

Fig1: MOE Game for Wiesner states.

- Constructions using Wiesner states:

(i) Compose a one-time pad with Wiesner states.

Construction: Gen: returns a random $\theta \leftarrow \{0,1\}^n$

$\text{Encrypt}_\theta(m) :=$ samples $x \leftarrow \{0,1\}^n$

outputs $m \oplus x$, $H^\theta |x\rangle$

Intuition: At a high level, no split adversary can have both

B & C recover m (fully).

$\therefore$ no adversary can have B & C completely recover x.

NB: However, such a scheme can never satisfy (the strongest notion)

uniformable indistinguishability.

Why? $\because$ recall that B, C cannot both distinguish encryptions of m_0 from m_1.

Now, as BL (Broadbent & Lord) observed, while B & C cannot learn all of m, they can still recover half of it —

w.p. $\frac{1}{2}$, a θ_i is guessed correctly

$\therefore$ w.p. ≈ 1, half the θ are guessed correctly

— & therefore distinguish w.p. essentially 1.

If $m_0 = 00\ldots0$

$m_1 = 11\ldots1$

then after decryption,

the "correct key" would be, say 1s

& the rest be random.

So the guess is wrong bit,

after decrypting by guessing 0 randomly,

appears w.p. 1.

(This is just one testing of this is so big! Are you going to work?)

(ii) Broadbent Lord:

- Introduce a uncloneable indistinguishability. the following scheme to satisfy

- Use a random oracle $H: \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^n$

- If an adversary can distinguish b/w

$m_0 \oplus H(\alpha, x)$ &

$m_1 \oplus H(\alpha, x)$

it must query $H(\alpha, x)$ at some point &
∴ one should be able to extract x from this adversary

Here's the scheme: by measuring one query at random.
(i.e. measure the query register at the i^{th} query where i is sampled uniformly)

$Gen(1^\lambda)$: ~~on input λ,~~ returns $(\alpha, \theta) \leftarrow \{0,1\}^{2\lambda}$

$Enc^H((\alpha,\theta), m)$: { samples $x \in \{0,1\}^\lambda$
outputs (returns) $|x^\theta\rangle, m \oplus H(\alpha, x)$

$Dec^H((\alpha,\theta), (|x^\theta\rangle, c))$: { Recovers x from $|x^\theta\rangle$
Returns $c \oplus H(\alpha, x)$

- This idea turns out to be hard to instantiate.

- One has to extract from x from both B & C. ⎫ ∵ one of them can extract x that easy – just have A send the entire state

~~Public~~ uncloneable indistinguishability requires that both B & C shouldn't be able distinguish, i.e. at least one must fail.

- ∵ B & C can be highly entangled, extraction success on (one) B may

(ii) Broadbent Zord:

- Introduce a uncloneable indistinguishability. the following scheme to satisfy

- Use a random oracle $H: \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^n$

- If an adversary can distinguish b/w

$m_0 \oplus H(\alpha, x)$ &

$m_1 \oplus H(\alpha, x)$

it must query $H(\alpha, x)$ at some point &
∴ one should be able to extract x from this adversary

Here's the scheme: by measuring one query at random.
(i.e. measure the query register at the i^{th} query where i is sampled uniformly)

$Gen(1^\lambda)$: ~~on input λ,~~ returns $(\alpha, \theta) \leftarrow \{0,1\}^{2\lambda}$

$Enc^H((\alpha,\theta), m)$: { samples $x \in \{0,1\}^\lambda$
outputs (returns) $|x^\theta\rangle, m \oplus H(\alpha, x)$

$Dec^H((\alpha,\theta), (|x^\theta\rangle, c))$: { Records x from $|x^\theta\rangle$
Returns $c \oplus H(\alpha, x)$

- This idea turns out to be hard to instantiate,
  - One has to extract from x from both

B & C. ⎫ ∵ one of them can extract x
⎪ that's easy — just have A send the
⎪ entire state
⎪ ~~Hence~~ uncloneable indistinguishability
⎪ requires that both B & C
⎪ shouldn't be able distinguish,
⎪ i.e. at least one must
⎭ fail.

∴ ∵ B & C can be highly entangled, extraction success on (one) B may

result in failure of extraction on (the other) C.

- Broadbent & Lord use a "simultaneous" version of the ~~[O2H]~~ O2H lemma (due to Unruh) to show that their scheme satisfies unclonable indistinguishability,

~~in the~~ when (a) the adversaries are un-entangled & (B & C) (OR?)

(b) the message has const length.

- The case for general adversaries & message spaces remains quite mysterious.

Majenz, Schaffner, Tahmasbi [MST'21]

show that there's an inherent limitation to this sim. simultaneous variant of O2H.

By an explicit example, they show such an approach cannot work to prove the security of unclon [BL]'s scheme.