## §1.4 Technical Overview

Attempts based on Wiesner States.

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

- Idea: $\mathrm{Encrypt}(m) :=$ sample a secret key $x$,
  Encode $x$ into an unclonable state $\rho_x$
  Encrypt $m$ using $x$ $\mathrm{Enc}_x(m)$

: Intuitively, for any splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$

there's no way for $\mathcal{A}$ to split $\rho_x$ into two quantum states s.t. non-communicating $\mathcal{B}$ & $\mathcal{C}$ can both recover info$^n$ about $x$ to decrypt $\mathrm{Enc}_x(m)$.

- Choice of no-cloning state:

(i) Wiesner conjugate coding: 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 "monogomy of entanglement games" (MOE games) in [TFKW13, BL20].

[BL20] show that no strategy $(\mathcal{A},\mathcal{B},\mathcal{C})$ wins the following MOE game w/ prob. more than $0.85^{\lambda}$.

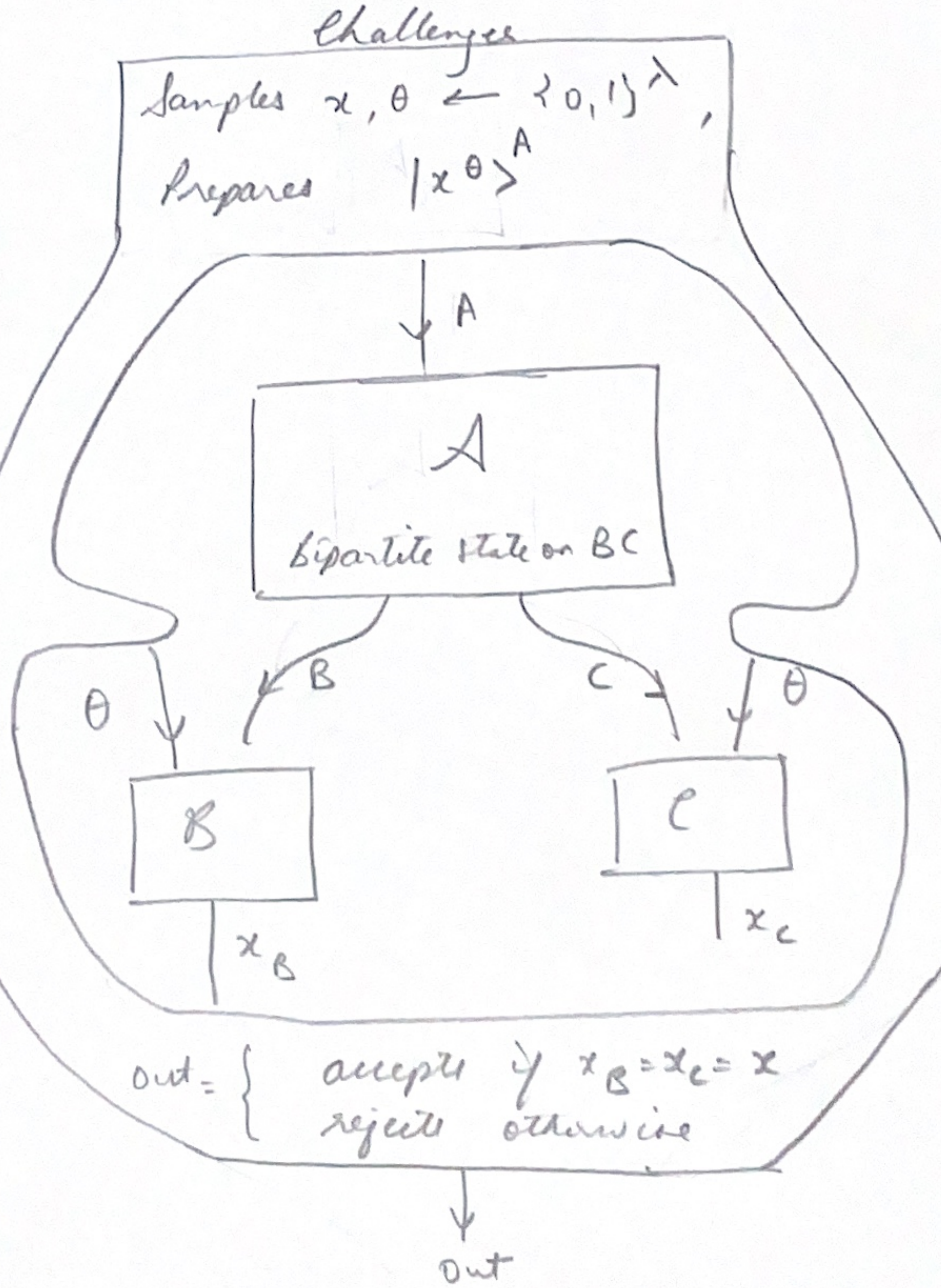

Fig1: MOE Game for Wiesner states.

- 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)
$\because$ no adversary can have $B$ & $C$ completely recover $x$.

NB: However, such a scheme can never satisfy (the stronger notion) uncloneable 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 — & therefore distinguish w.p. essentially 1.

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

so w.p. $\approx 1$, half the $\theta$ are guessed correctly

If ~~$\theta$~~ $m_0 = 00 \ldots 0$
$m_1 = 11 \ldots 1$

then after decryption,
the "correct half" would be, say 1s
& the rest be random.

So the guess is whichever bit, after decrypting by guessing $\theta$ randomly, appears w.p. 1.

(This is just me testing if this is so light! Are you going to work?)

(ii) Broadbent Lord:

- Introduces uncloneable indistinguishability.
  the following scheme to satisfy

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

- 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
  by measuring one query at random.
  (i.e. measure the query register at the $i^{th}$ query where $i$ is sampled uniformly)

Here's the scheme:

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

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

$\mathrm{Dec}^H((\alpha, \theta), (|x^\theta\rangle, c))$: $\begin{cases} \text{Recovers } x \text{ from } |x^\theta\rangle \\ \text{Returns } c \oplus H(\alpha, x) \end{cases}$

- This idea turns out to be hard to instantiate, ∵
  - One has to extract ~~from~~ $x$ from both $\mathcal{B}$ & $\mathcal{C}$.
    ∵ one of them can extract $x$ that's easy – just have $\mathcal{A}$ send the entire state
    ~~[illegible]~~ uncloneable indistinguishability requires that both $\mathcal{B}$ & $\mathcal{C}$ shouldn't be able distinguish, i.e. at least one must fail.
  - ∵ $\mathcal{B}$ & $\mathcal{C}$ can be highly entangled, extraction success on (one) $\mathcal{B}$ may

result is 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 (B & C) are un-entangled & (OR?) (b) the message has const length.

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

Majenz, Schaffner, Tahmasbi [MST'21] show that there's an inherent limitation to this same simultaneous variant of O2H. By an explicit example, they show such an approach cannot work to prove the security of unclon [BL]'s scheme.