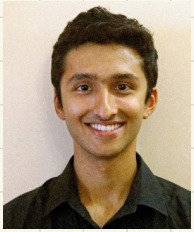
Commitment Over Unreliable Noisy Channels: When Awareness Meets Control

Manideep Mamindlapally
(TIFR, Mumbai)*

Amitalok Budkuley
(IIT Kharagpur)



Pranav Joshi
(Independent Researcher)

Anuj Kumar Yadav
(EPFL, Lausanne)

*work done while at IIT Kharagpur

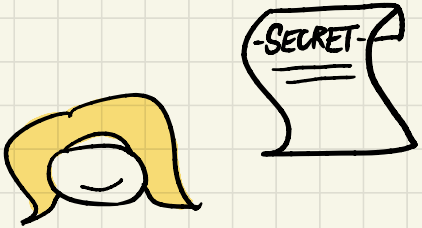
What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases

What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases

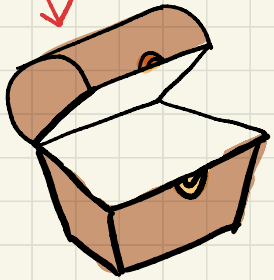
PHASE I



What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases

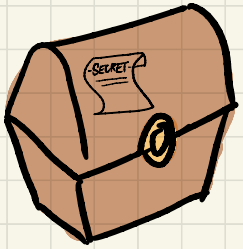
PHASE I



What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases

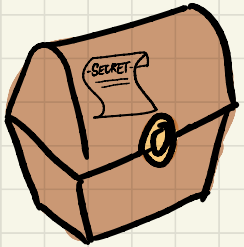
PHASE I



What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases

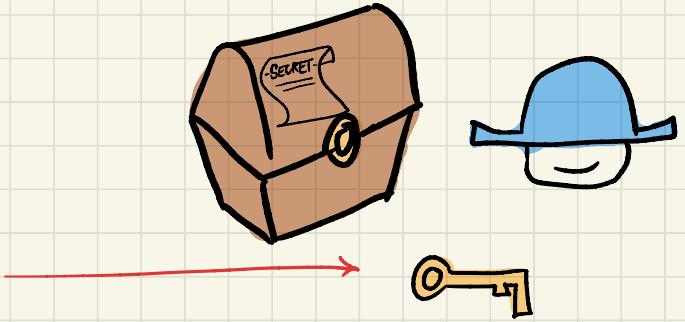
PHASE I



What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases

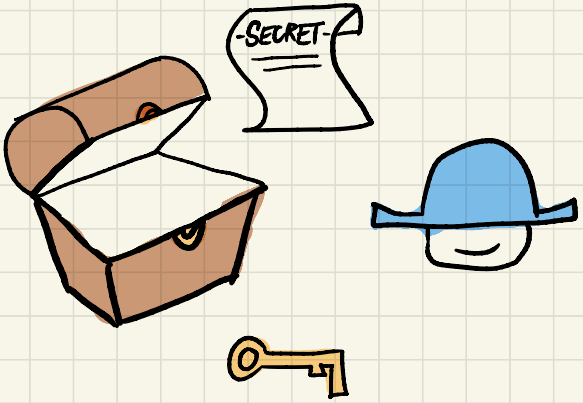
PHASE II



What Is Commitment?

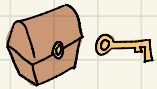
- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases

PHASE II



What Is Commitment?

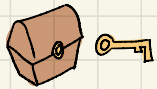
- Security Protocol.
- Two parties – COMMITTER  & VERIFIER 
- Two phases
  - COMMIT PHASE
  - REVEAL PHASE

Non trivial resource: 

- Security Guarantees
  - soundness, concealment, bindingness.

What Is Commitment?

- Security Protocol.
- Two parties — COMMITTER  & VERIFIER 
- Two phases
  - COMMIT PHASE
  - REVEAL PHASE

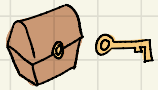
Non trivial resource: 

- Security Guarantees
  - soundness, concealment, bindingness.

— [Blum 1983] Commitment - Interactive Exchange of messages.

What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases
  - COMMIT PHASE
  - REVEAL PHASE

Non trivial resource: 

- Security Guarantees
  - soundness, concealment, bindingness.

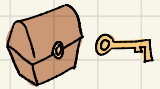
– [Blum 1983] Commitment - Interactive Exchange of messages.

↳ Conditionally secure [secure under computational assumptions]

– Unconditionally secure Commitment IMPOSSIBLE

What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases
  - COMMIT PHASE
  - REVEAL PHASE
- Security Guarantees
  - soundness, concealment, bindingness.

Non trivial resource: 

– [Blum 1983] Commitment - Interactive Exchange of messages.

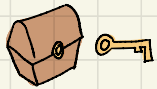
↳ Conditionally secure [secure under computational assumptions]

– Unconditionally secure Commitment IMPOSSIBLE

↳ unless you use some non-trivial resource

What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases
  - Commit Phase
  - Reveal Phase

Non trivial resource: 

- Security Guarantees
  - soundness, concealment, bindingness.

– [Blum 1983] Commitment - Interactive Exchange of messages.

↳ Conditionally secure [secure under computational assumptions]

– Unconditionally secure Commitment IMPOSSIBLE

↳ unless you use some non-trivial resource

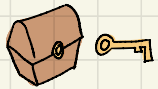
– Commitment using "noisy channels" resource. [Crepeau et al STOC 1988]

↳ Unconditionally Secure

(Information theoretically secure)

What Is Commitment?

- Security Protocol
- Two parties – COMMITTER  & VERIFIER 
- Two phases
  - COMMIT PHASE
  - REVEAL PHASE

Non trivial resource: 

- Security Guarantees
  - soundness, concealment, bindingness.

– [Blum 1983] Commitment - Interactive Exchange of messages.

↳ Conditionally secure [secure under computational assumptions]

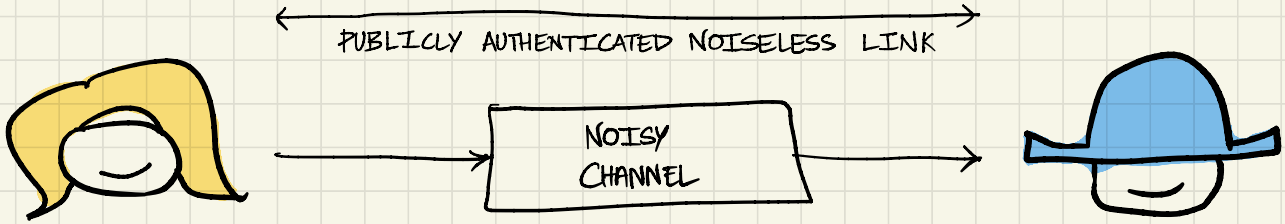
– Unconditionally secure Commitment IMPOSSIBLE

↳ unless you use some non-trivial resource

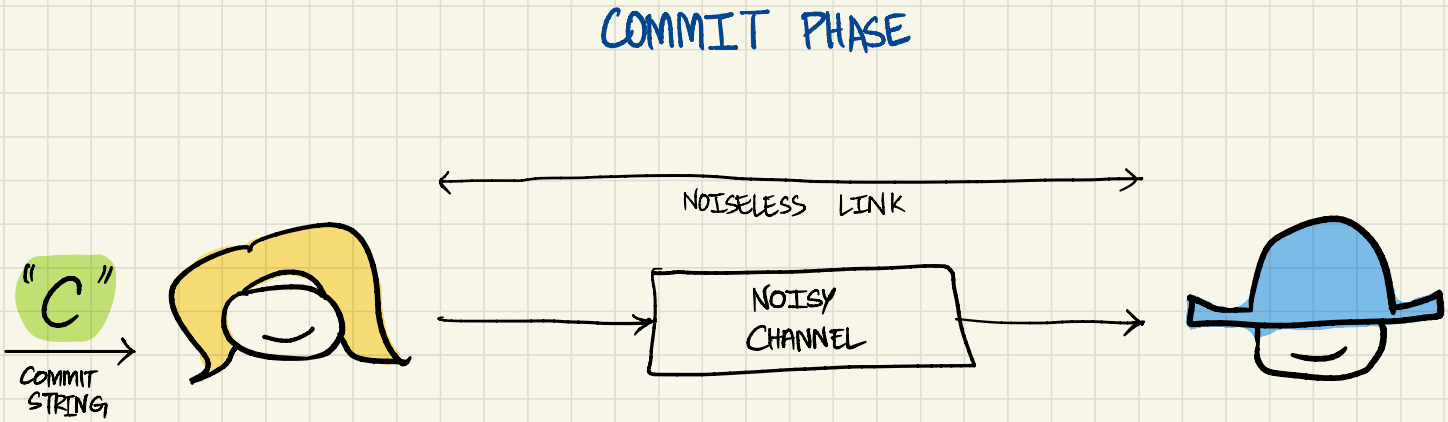
– Commitment using "noisy channels" resource. [Crepeau et al STOC 1988]

↳ Imperfectly characterised : "UNRELIABLE" NOISY CHANNELS

Problem Setup: Commitment Over Noisy Channels

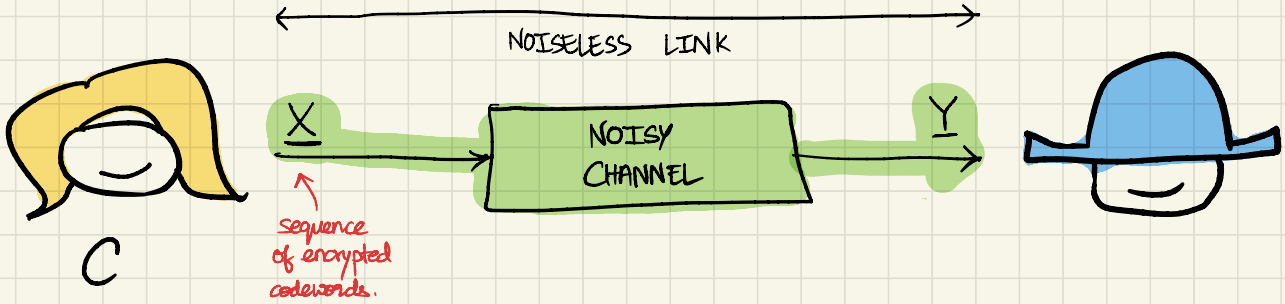


Problem Setup: Commitment Over Noisy Channels

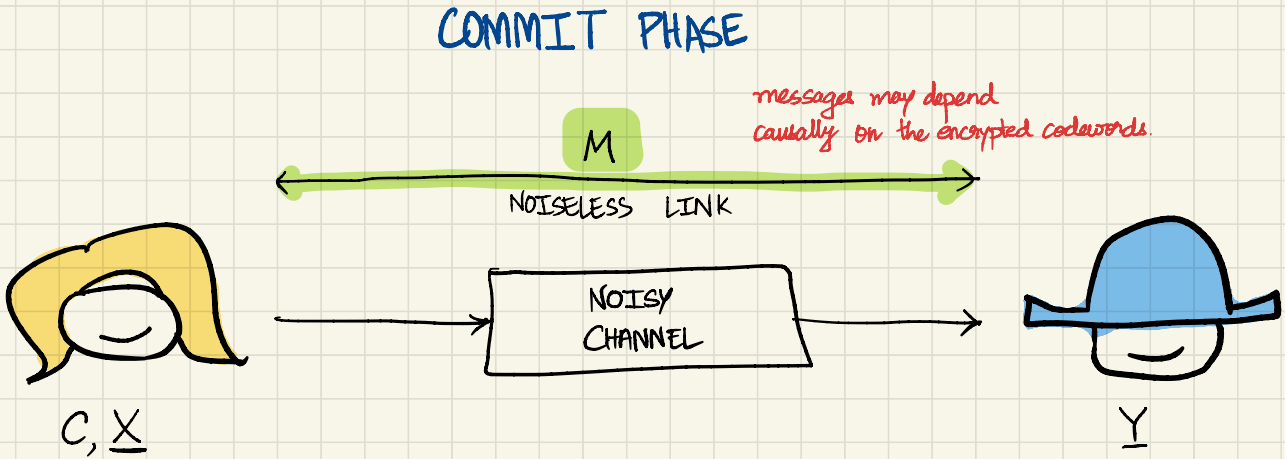


Problem Setup: Commitment Over Noisy Channels

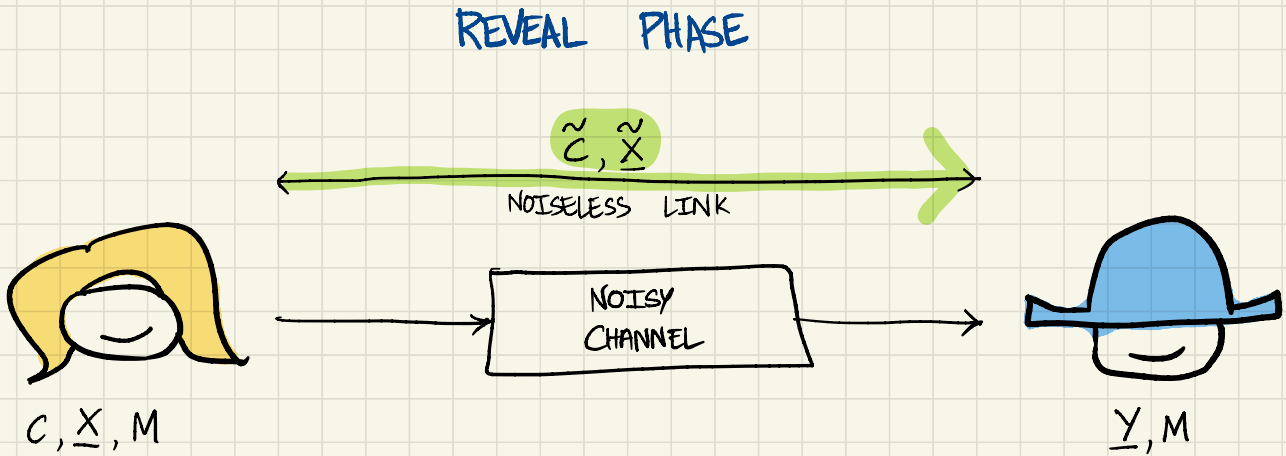
COMMIT PHASE



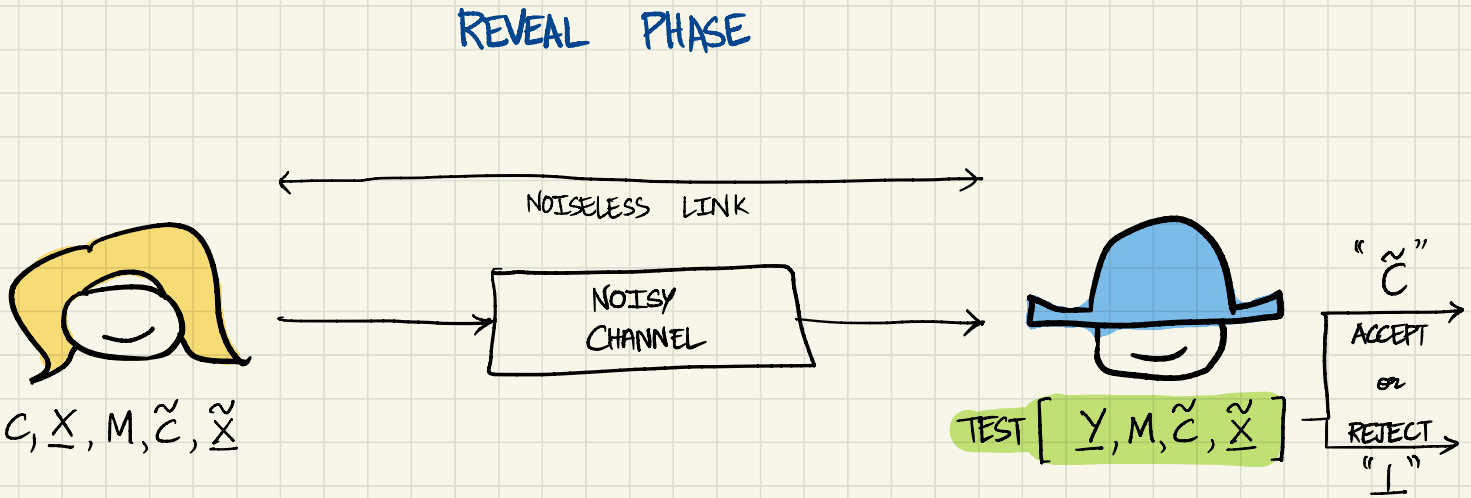
Problem Setup: Commitment Over Noisy Channels



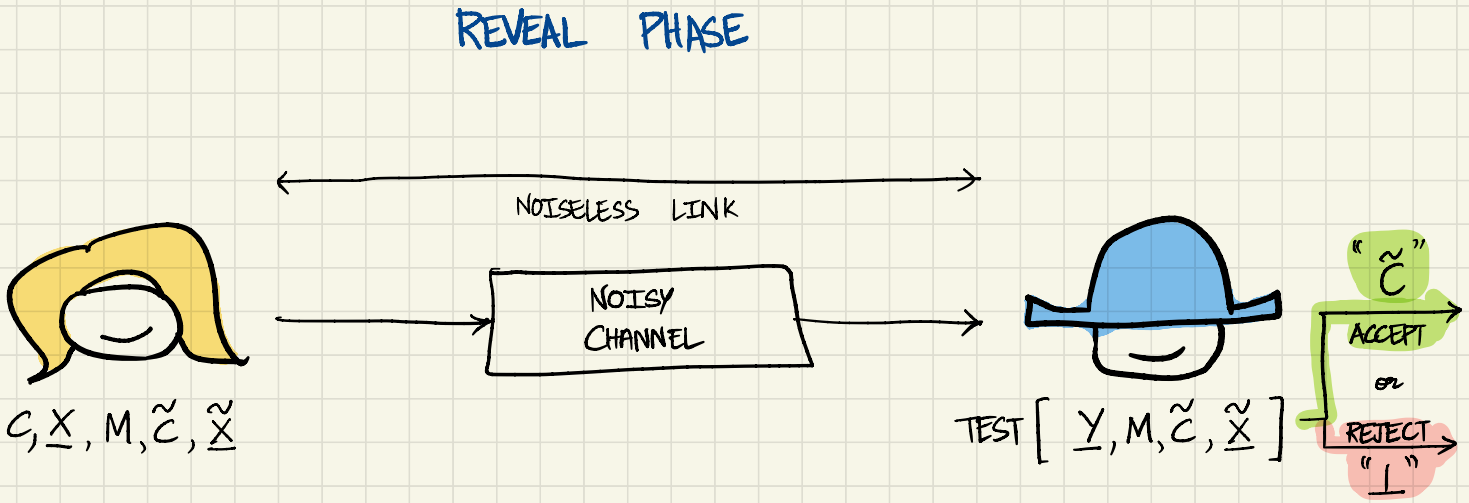
Problem Setup: Commitment Over Noisy Channels



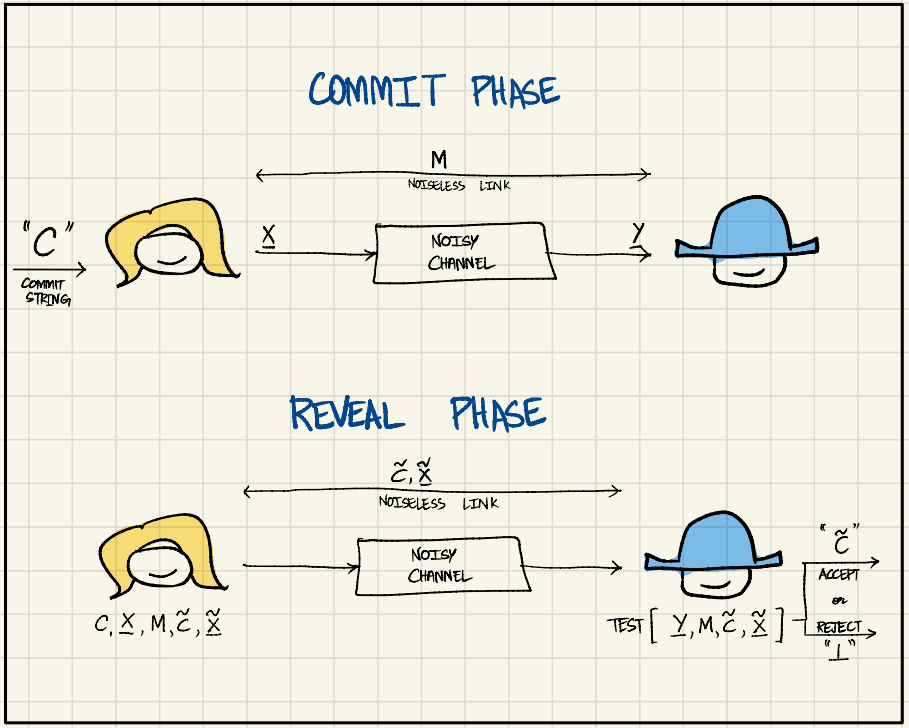
Problem Setup: Commitment Over Noisy Channels



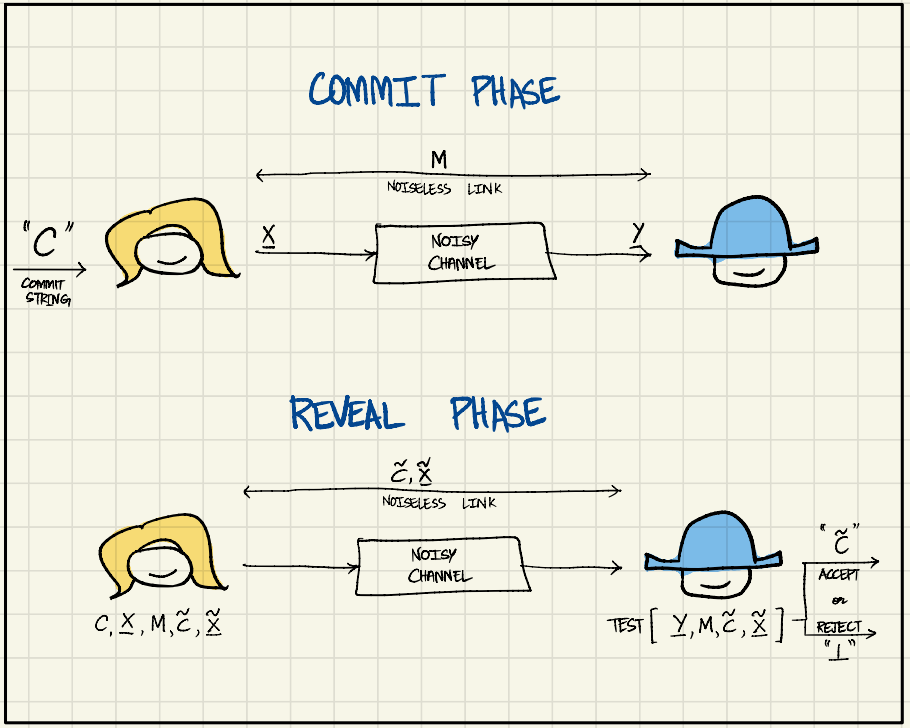
Problem Setup: Commitment Over Noisy Channels



Problem Setup: Commitment Over Noisy Channels



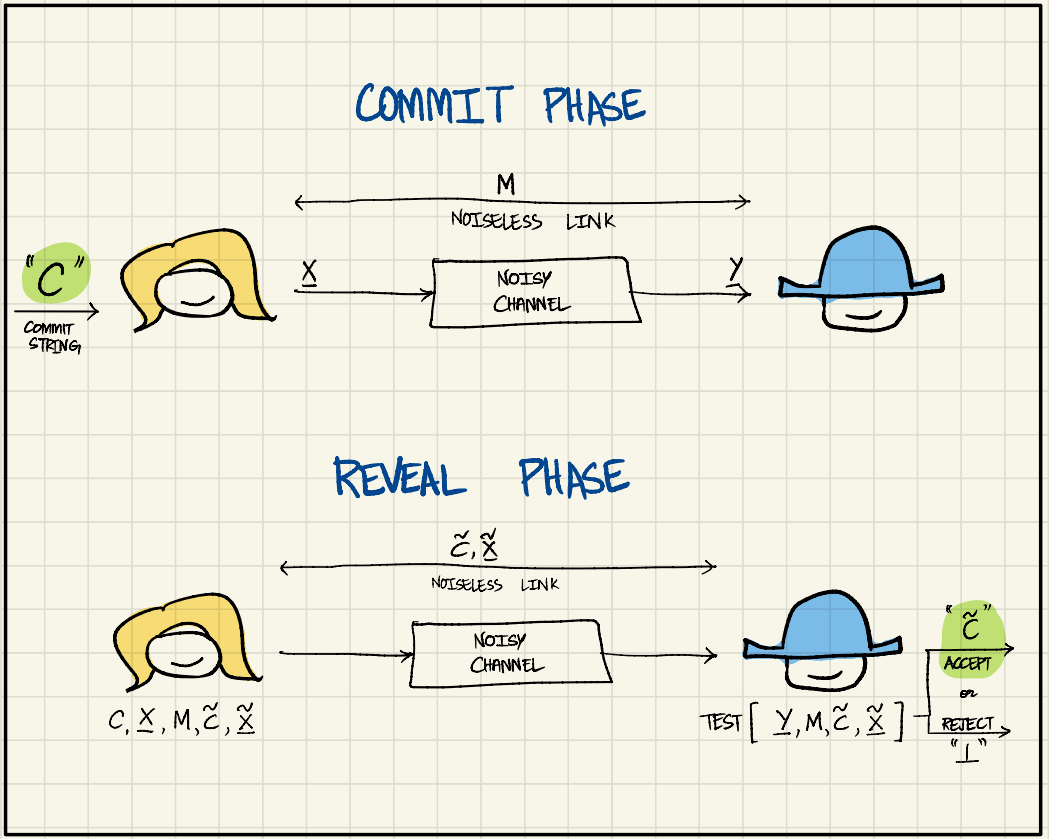
Problem Setup: Commitment Over Noisy Channels



Security Guarantees

1. Soundness
2. Concealment
3. Bindingness

Security Guarantee: Soundness

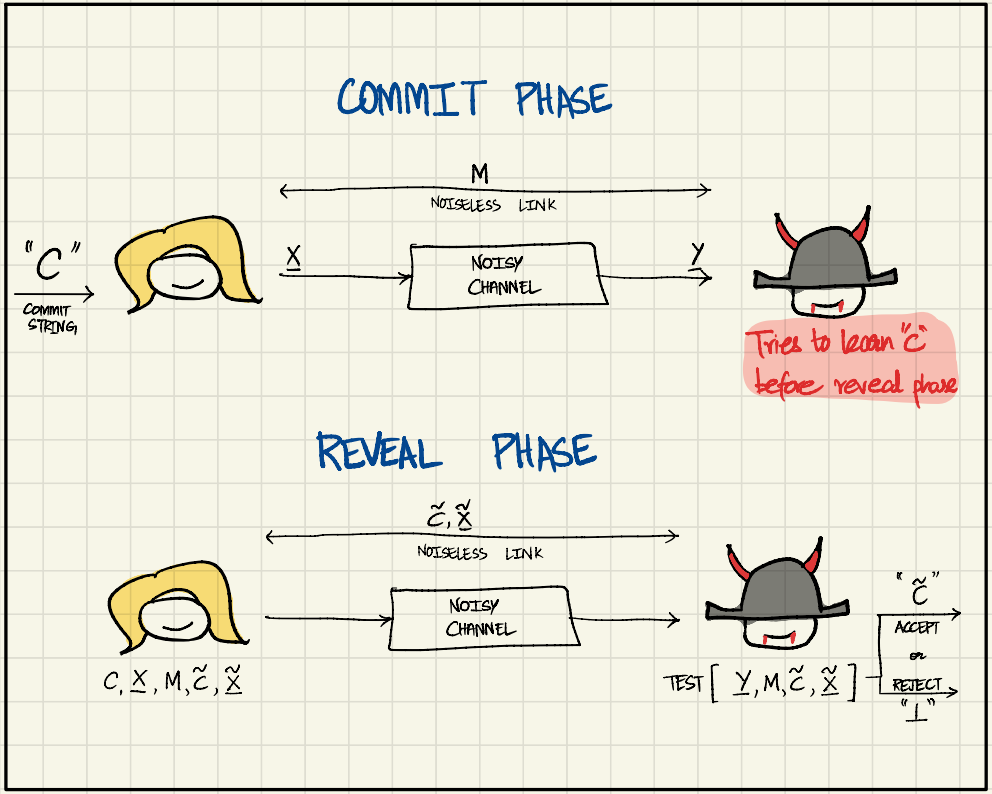


- When both Alice and Bob are honest, Bob's test T should PASS.

ϵ-Soundness

$$\mathbb{P}[T(Y, M, c, x) = \perp] \leq \epsilon \quad \forall\, c, x$$

Security Guarantee : Concealment



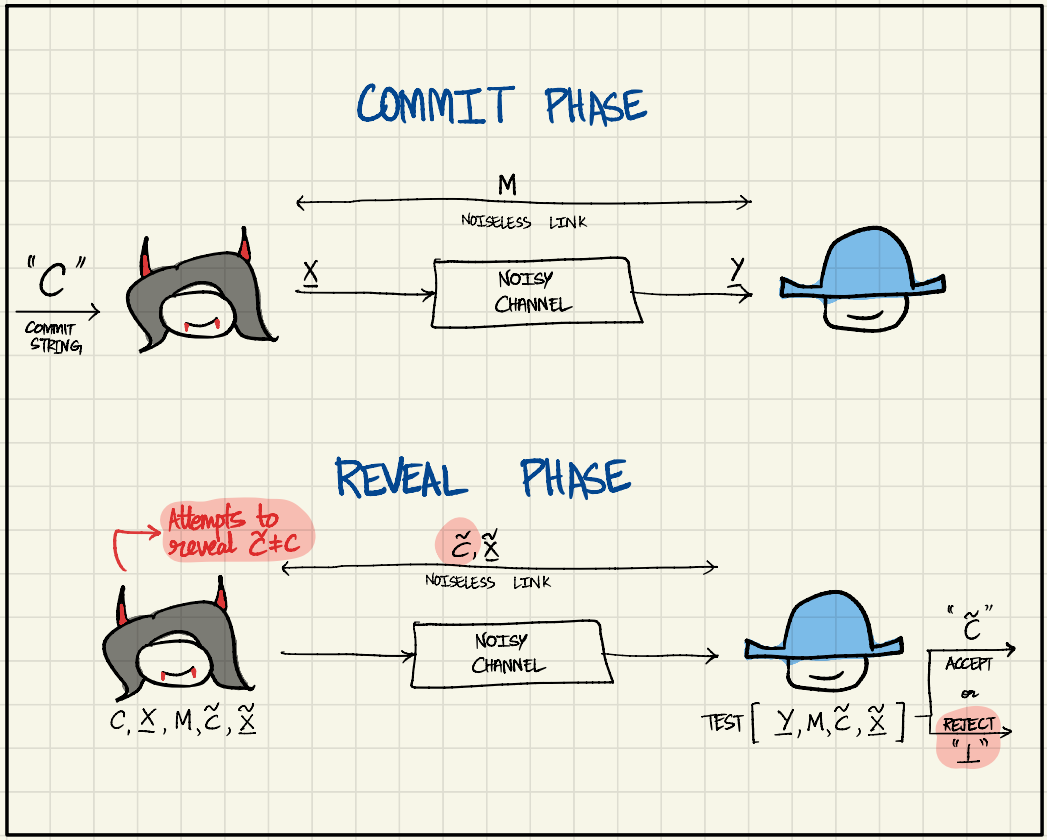
- Protection against Malicious Bob
- Ensures that Bob remains oblivious of "C" till the end of REVEAL PHASE.

ϵ-concealment

$$I(View_B : C) \leq \epsilon$$

where $View_B = (Y, M)$

Security Guarantee: Bindingness



- Protection against Malicious Alice.

- Ensures that Bob's test FAILS when Alice reveals $\tilde{C} \neq C$.

ϵ-bindingness

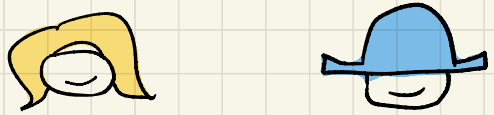
$$P\left[T(View_B, C_1, \underline{x}_1) = T(View_B, C_2, \underline{x}_2) = ACCEPT\right] \leq \epsilon$$

$$\forall\ C_1 \neq C_2, \underline{x}_1, \underline{x}_2$$

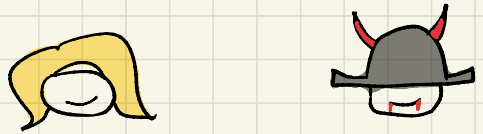
where $View_B = (\underline{Y}, M)$

Commitment Security Guarantees : Overview

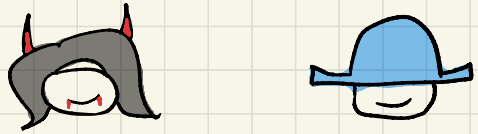
SOUNDNESS



CONCEALMENT



BINDINGNESS



Commitment Security Guarantees : Overview

SOUNDNESS

CONCEALMENT

BINDINGNESS

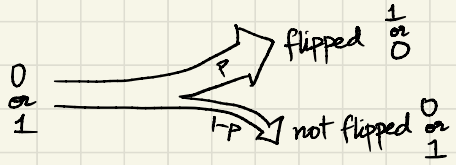
NO SECURITY GUARANTEES

Noisy Channels

"Reliable" Noisy Channels : Perfectly characterised by a Transition fxn.

Example: BSC(p)

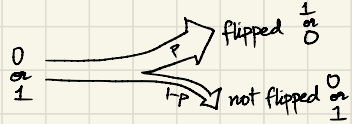
Characterised by $\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$



Noisy Channels

"Reliable" Noisy Channels : Perfectly characterised by a Transition fxn.

Example : BSC(p)



Characterised by $\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$

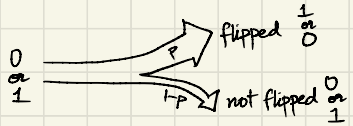
Throughput : # bits that can be committed per use of noisy channel

Commitment capacity : maximum throughput achievable (satisfying security guarantees)

Noisy Channels

"Reliable" Noisy Channels : Perfectly characterised by a Transition fxn.

Example : BSC(p)



Characterised by $\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$

$$C_{BSC(p)} = H(p)$$

[Winter et al ICCC 2003]

$$C_{DMC} = \max_{P_X} H(X|Y)$$

[Mamindlapally et al ISIT 2021]

$$C_{DMC,\varepsilon,\Gamma} = \max_{P_X : E_{\mathcal{R}}[\varepsilon(\mathcal{R})] \le \Gamma} H(X|Y)$$

$$= \min_{\gamma \ge 0} \max_{\mathcal{R}_y} \log\left[\sum_{x \in \mathcal{X}} \exp\{-D(W_{y|x} \| \mathcal{R}_y) + \gamma(\Gamma - \varepsilon(x))\}\right]$$

Throughput : # bits that can be committed per use of noisy channel.

Commitment capacity : maximum throughput achievable (satisfying security guarantees)

Unreliable Noisy Channels ("compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Unreliable Noisy Channels ("Compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC

~behaves like a BSC(p) with "p" not known to the parties

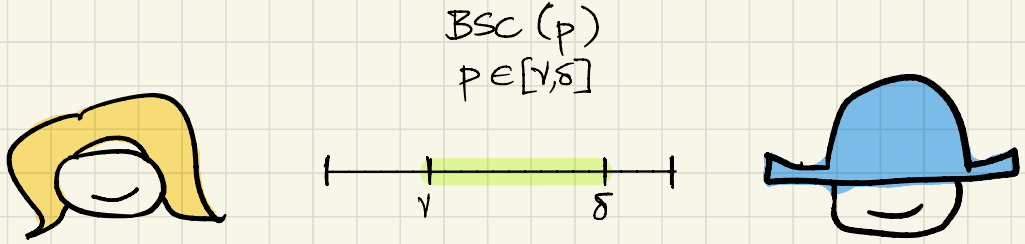
Unreliable Noisy Channels ("Compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound - BSC [γ,δ]

~behaves like a BSC(p) with "p" not known to the parties



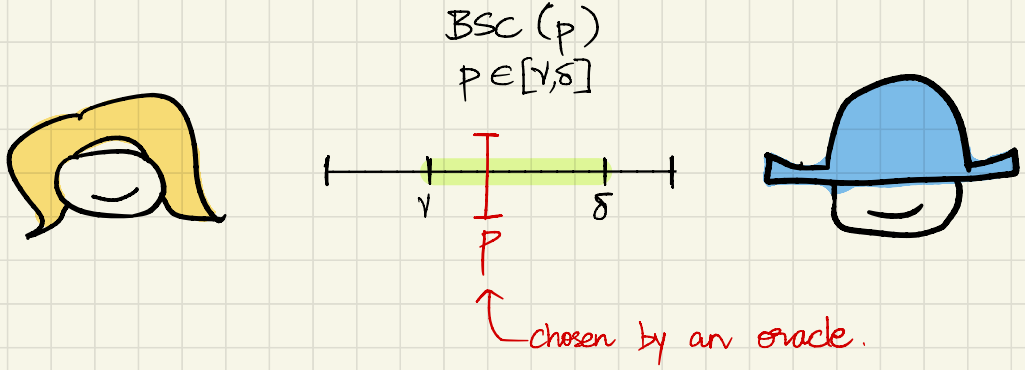
Unreliable Noisy Channels ("compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC[γ,δ]

~behaves like a BSC(p) with "p" not known to the parties



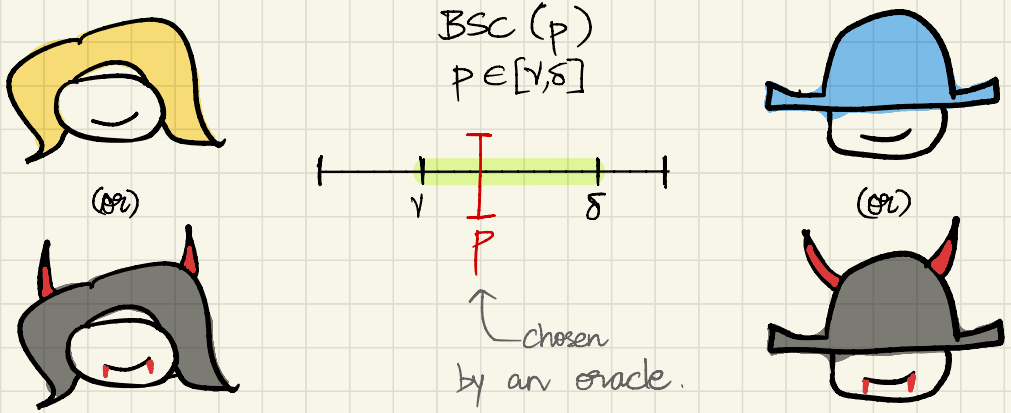
Unreliable Noisy Channels ("compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC$[\gamma,\delta]$

~behaves like a BSC(p) with "p" not known to the parties



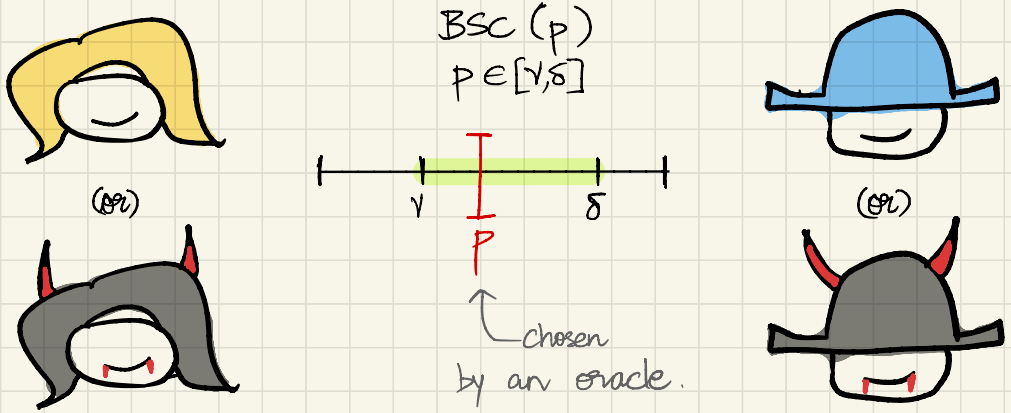
Unreliable Noisy Channels ("Compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC$[\gamma,\delta]$

~behaves like a BSC(p) with "p" not known to the parties.



[Yadav et al NCC 2022]

$C_{c\text{-}BSC} = H(\gamma)$

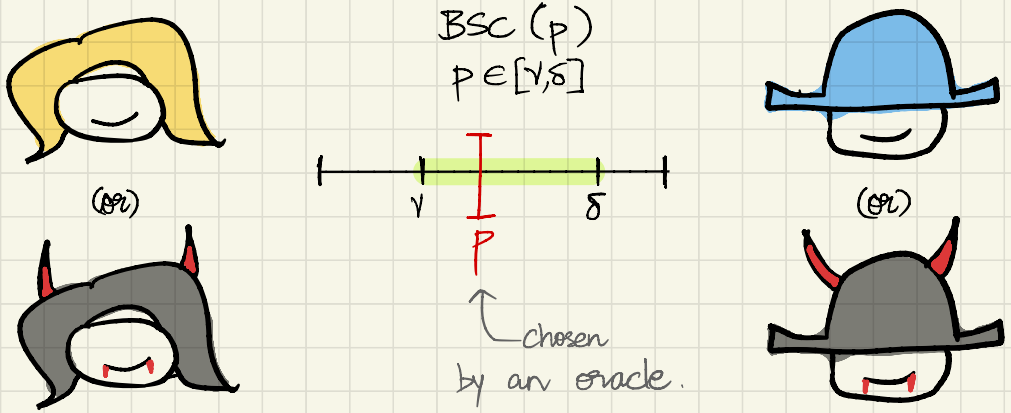
Unreliable Noisy Channels ("Compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC[γ,δ]

~behaves like a BSC(p) with "p" not known to the parties



[Yadav et al NCC 2022]

$C_{C\text{-}BSC} = H(\gamma)$

State Unaware Compound-BSC

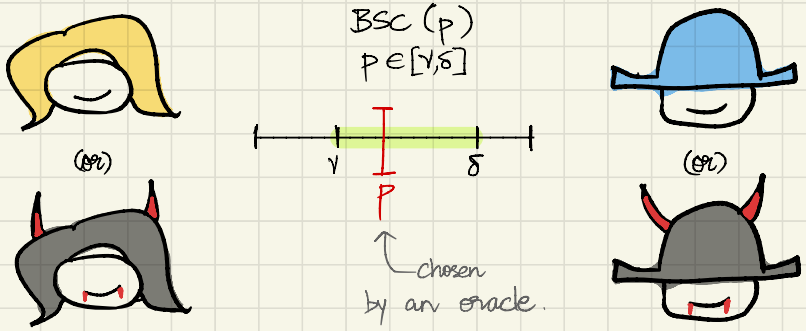
Unreliable Noisy Channels ("compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC[γ,δ]

~behaves like a BSC(p) with "p" not known to the parties



→ Further "unreliable variants"
Capabilities of Alice and Bob

① Awareness

② Control

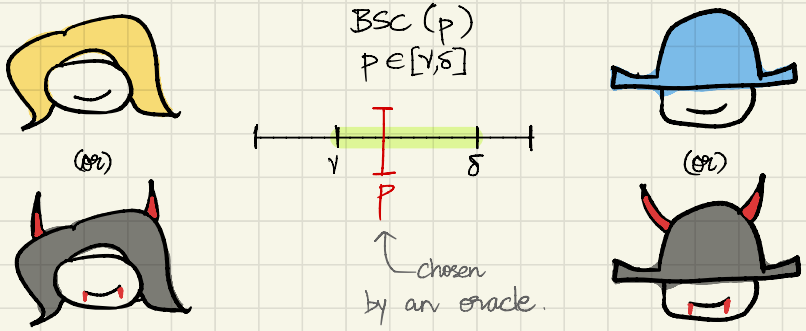
Unreliable Noisy Channels ("Compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC[γ,δ]

~behaves like a BSC(p) with "p" not known to the parties



→ Further "unreliable variants"
Capabilities of Alice and Bob

① Awareness]* Current Focus.

② Control

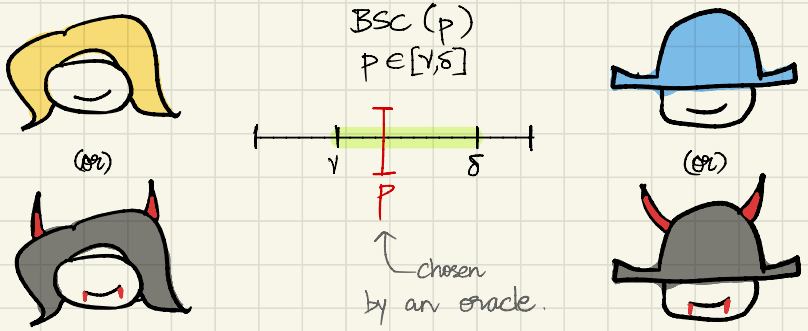
Unreliable Noisy Channels ("Compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC$[\nu,\delta]$

~behaves like a BSC(p) with "p" not known to the parties



→ Further "unreliable variants"
Capabilities of Alice and Bob

① Awareness]* Current Focus.

② Control

UNCs
[Dziembowski et al EUROCRYPT 1999]

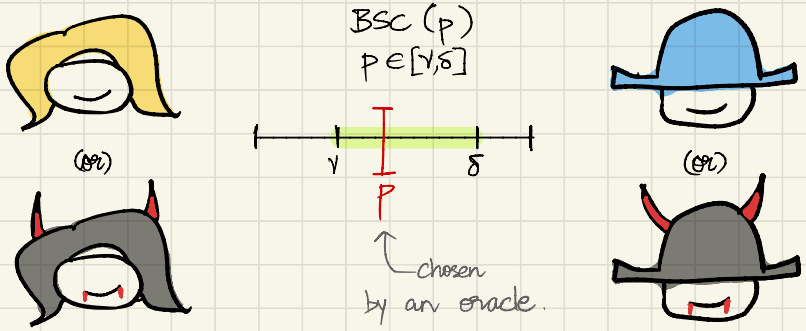
Unreliable Noisy Channels ("Compoundness")

Unreliable Noisy channels: Not perfectly characterized.

{Set of Transition fxns} ← From Alice and Bob's perspective

Example: Compound-BSC$[\nu,\delta]$

~behaves like a BSC(p) with "p" not known to the parties



→ Further "unreliable variants" Capabilities of Alice and Bob

① Awareness]* Current Focus.

② Control — UNCs [Ahlswede et al EUROCRYPT 1999]

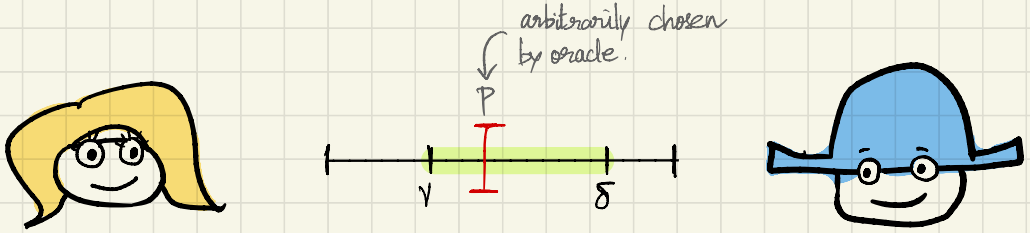
[Budkuley et al JSAC 2021] "Elasticity"

State Aware Variants of Compound BSCs

I:

State Aware Variants of Compound BSCs

I:

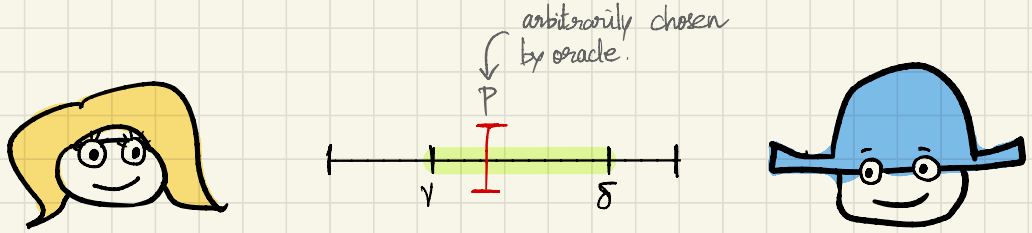


→ Channel behaves like a Compound-BSC except that Alice and Bob can now see the state 'p' that gets instantiated (because they have eyes)

→ The channel behaviour is same even for malicious Alice and Bob.

State Aware Variants of Compound BSCs

I: Alice-aware Bob-aware Variant $C\text{-}BSC_{AB}[\nu,\delta]$



→ Channel behaves like a Compound-BSC except that Alice and Bob can now see the state 'p' that gets instantiated (because they have eyes)

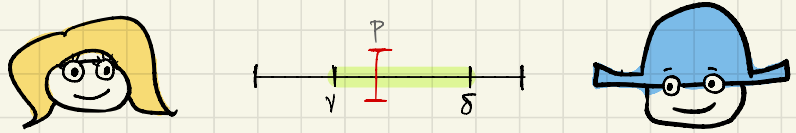
→ The channel behaviour is same even for malicious Alice and Bob.

→ We call this the Alice-aware Bob-aware variant.

State Aware Variants of Compound BSCs

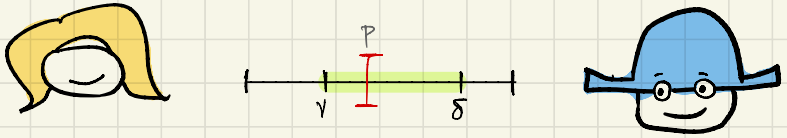
I: Alice-aware Bob-aware

$C\text{-}BSC_{A,B}[\gamma,\delta]$



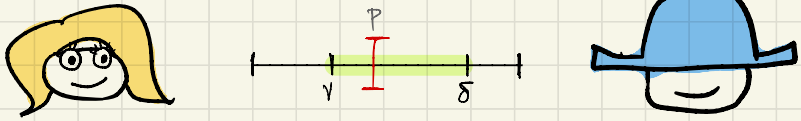
II: Alice-unaware Bob-aware

$C\text{-}BSC_{B}[\gamma,\delta]$



III: Alice-aware Bob-unaware

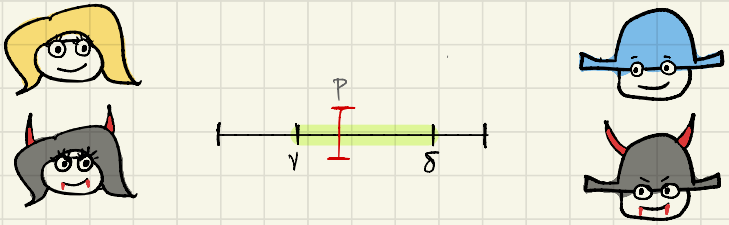
$C\text{-}BSC_{A}[\gamma,\delta]$



State Aware Variants of Compound BSCs

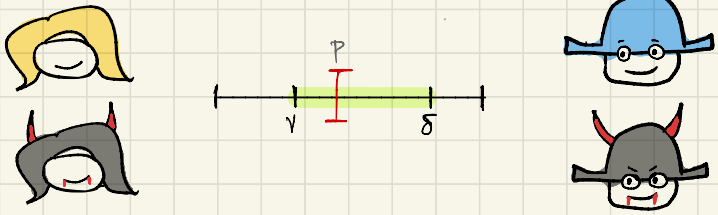
I: Alice-aware Bob-aware

$C\text{-}BSC_{A,B}[\gamma,\delta]$



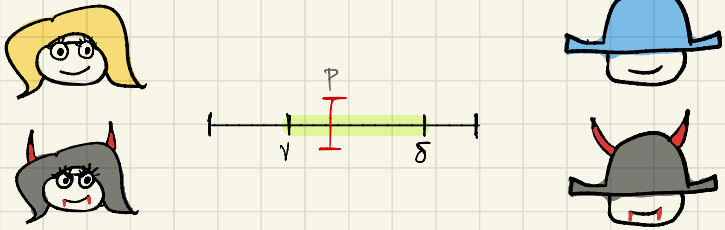
II: Alice-unaware Bob-aware

$C\text{-}BSC_{B}[\gamma,\delta]$



III: Alice-aware Bob-unaware

$C\text{-}BSC_{A}[\gamma,\delta]$

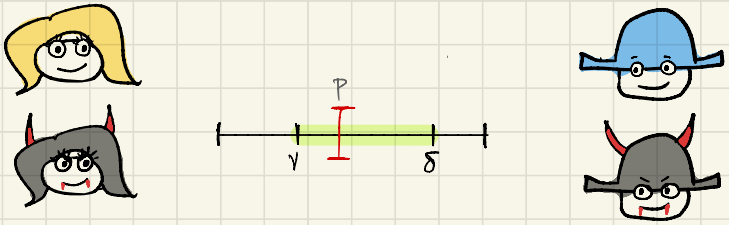


Note:
In all the variants, channel behaviour is the same for malicious and honest parties.

State Aware Variants of Compound BSCs

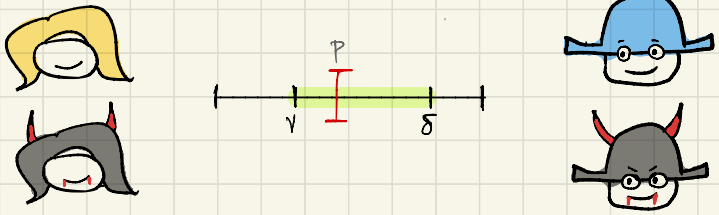
I: Alice-aware Bob-aware

$C\text{-}BSC_{A,B}[\gamma,\delta]$



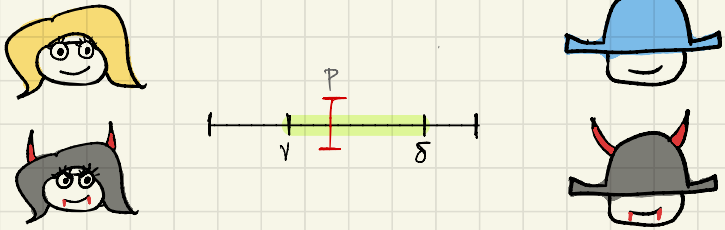
II: Alice-unaware Bob-aware

$C\text{-}BSC_{B}[\gamma,\delta]$



III: Alice-aware Bob-unaware

$C\text{-}BSC_{A}[\gamma,\delta]$



"unreliable variants"
Capabilities of Alice and Bob

① Awareness → OUR RESULT

② Control ↳ modelled in UNCs.

Unfair Noisy Channels : The UNCs

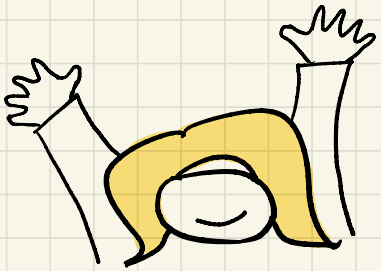
$UNC[\gamma, \delta]$

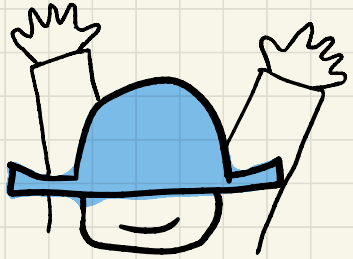
$0 \leq \gamma \leq \delta \leq \frac{1}{2}$.

[Damgard et al EUROCRYP 1988]

Unfair Noisy Channels : The UNCs

$UNC[\gamma, \delta]$ $\quad 0 \leq \gamma \leq \delta \leq \frac{1}{2}$.



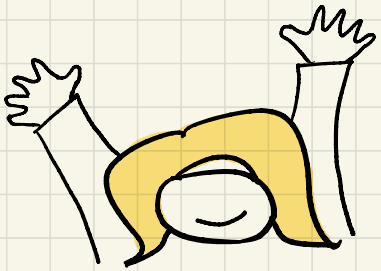


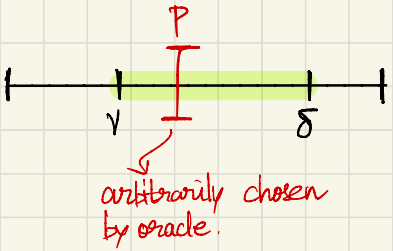
- Sender Alice and Receiver Bob
- Both have hands
- Are asked to hang them in the air.

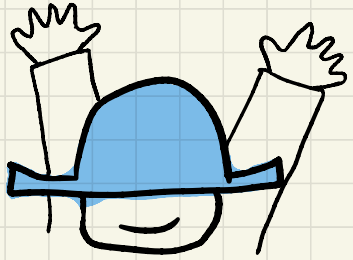
Unfair Noisy Channels : The UNCs

UNC$[\gamma, \delta]$

$0 \leq \gamma \leq \delta \leq \frac{1}{2}$

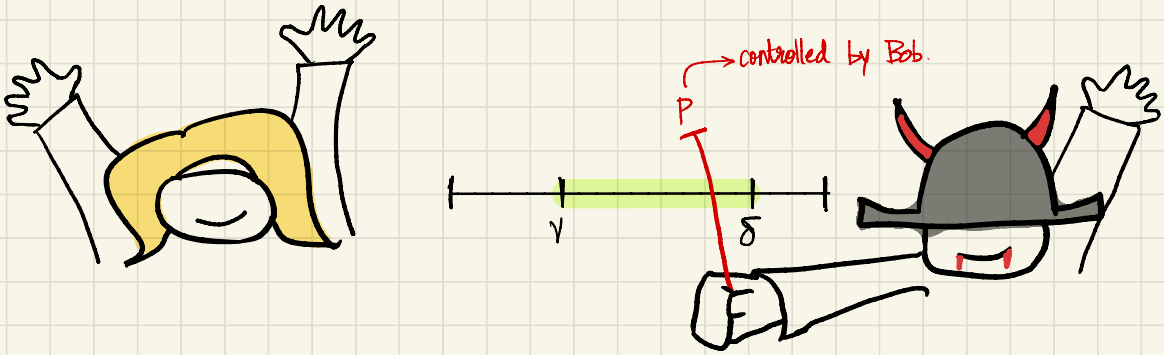






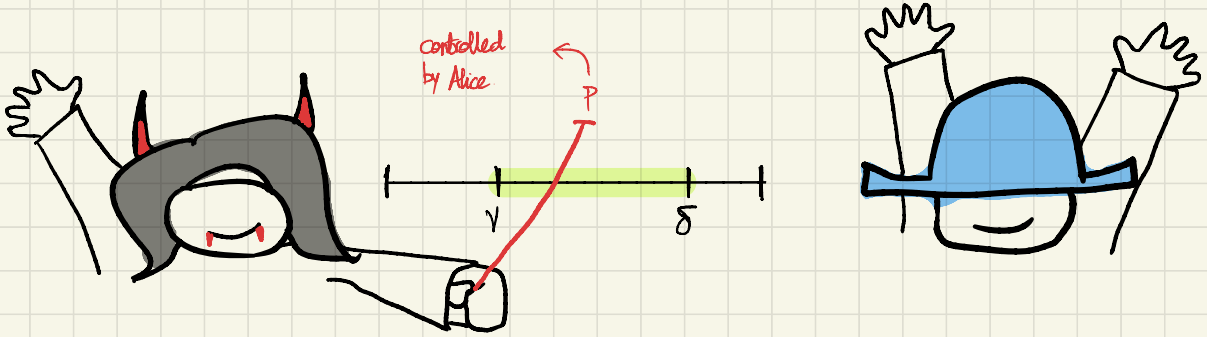
Unfair Noisy Channels : The UNCs

$UNC[\gamma, \delta]$ $\quad 0 \leq \gamma \leq \delta \leq \frac{1}{2}$



Unfair Noisy Channels : The UNCs

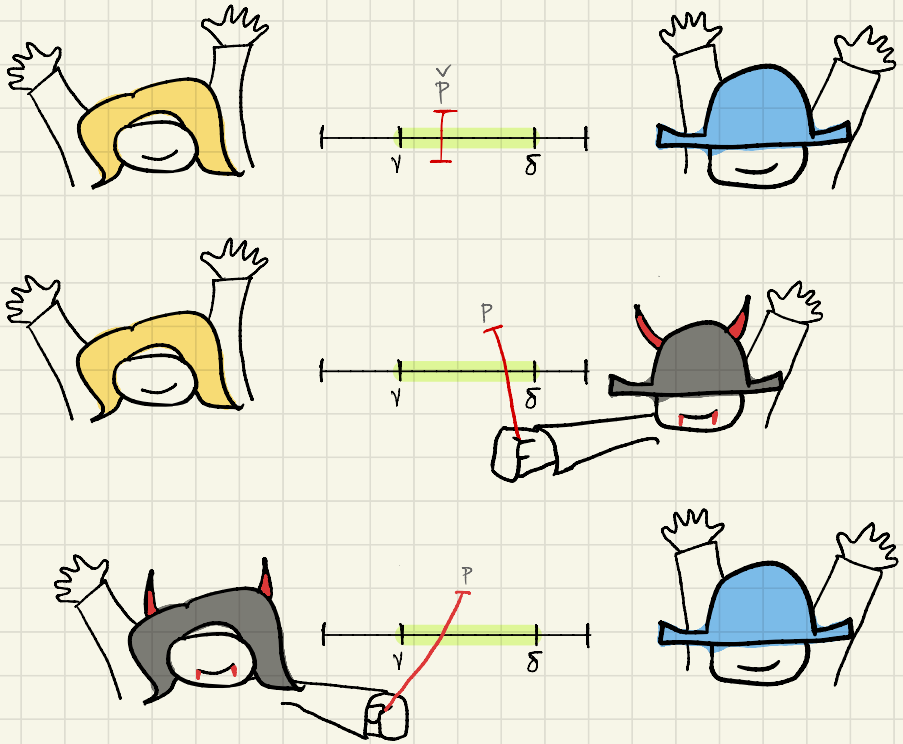
$UNC[\gamma, \delta]$ $\quad 0 \leq \gamma \leq \delta \leq \frac{1}{2}$



Unfair Noisy Channels : The UNCs

UNC[γ, δ]

$0 \le \gamma \le \delta \le \frac{1}{2}$



[Damgard et al. EUROCRYPT 1999]

$C_{UNC} > 0$ for $\delta < \gamma * \gamma$

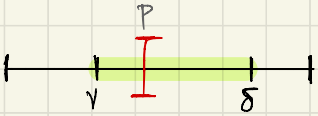
[Crepeau et al., TransIT 2020]

$C_{UNC[\gamma,\delta]} \ge H(\gamma) - H\left(\frac{\delta-\gamma}{1-2\gamma}\right)$

Main Results

I:

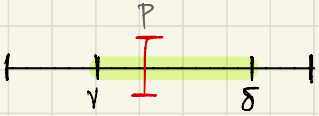
AWARE



AWARE

II:

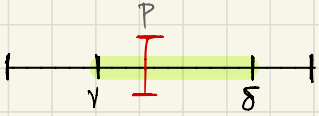
UNAWARE



AWARE

III:

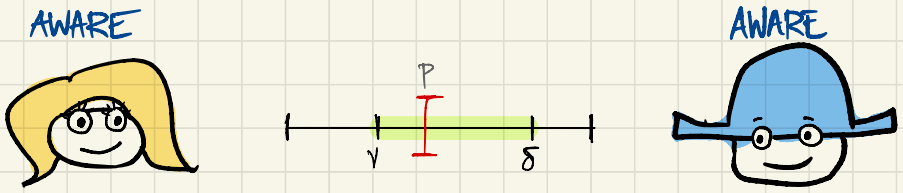
AWARE



UNAWARE

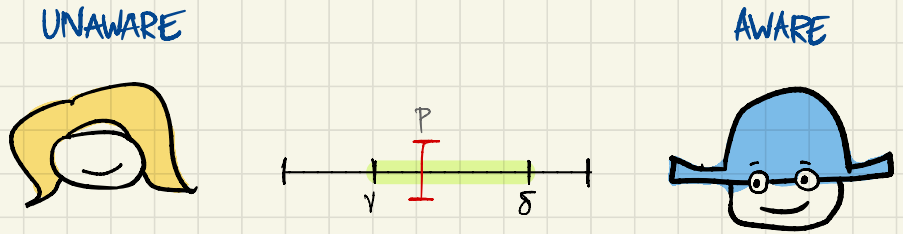
Main Results

I:



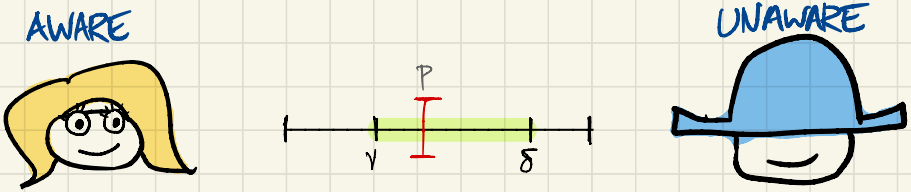
$$C_{C\text{-}BSC_{AB}} = H(\nu)$$

II:



$$C_{C\text{-}BSC_{B}} = H(\nu)$$

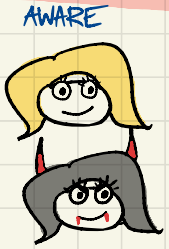
III:

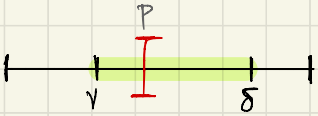


$$C_{C\text{-}BSC_{A}} \geq H(\nu) - H\left(\frac{\delta-\nu}{1-2\nu}\right)$$

Main Results

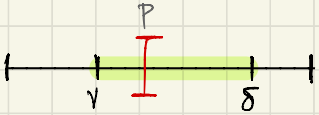
I:





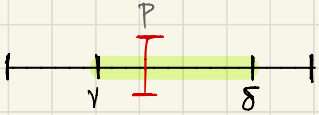
$$\mathbb{C}_{\text{C-BSC}_{1B}} = H(\gamma)$$

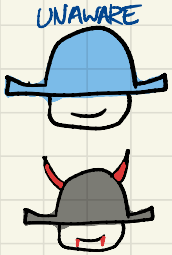
II:



$$\mathbb{C}_{\text{C-BSC}_{B}} = H(\gamma)$$

III:





$$\mathbb{C}_{\text{C-BSC}_{1}} \geq H(\gamma) - H\left(\frac{\delta-\gamma}{1-2\gamma}\right)$$

Main Results

Proofs for Commitment Capacity Expression.

for given conditions. "$\mathbb{C}_{\{conditions\}}$"

I: Achievability

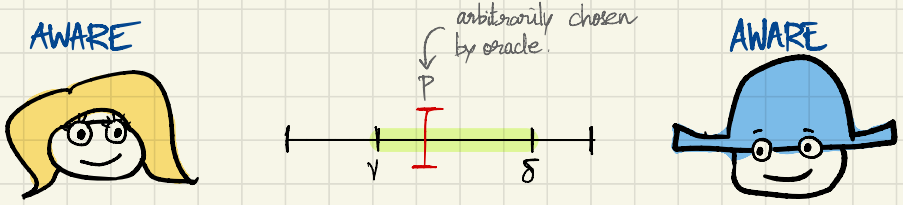
Design a protocol that is secure and has throughput $\geq \mathbb{C}_{\{conditions\}} - \epsilon$

II: Converse

Argue that any protocol with throughput $> \mathbb{C}_{\{conditions\}} + \epsilon$, is not secure.

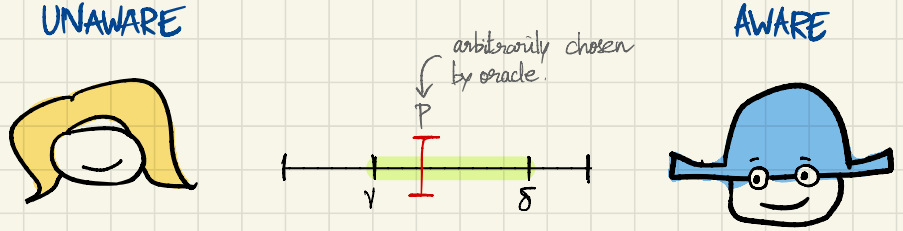
Main Results

I:



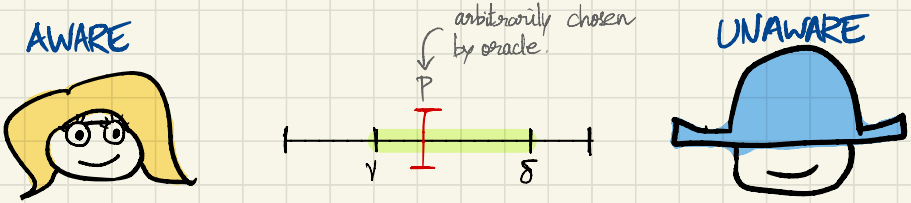
$$\mathbb{C}_{C\text{-}BSC_{1,B}} = H(\nu) = \min_{p} \mathbb{C}_{BSC(p)} = \min_{p} H(p)$$

II:



$$\mathbb{C}_{C\text{-}BSC_{B}} = H(\nu)$$

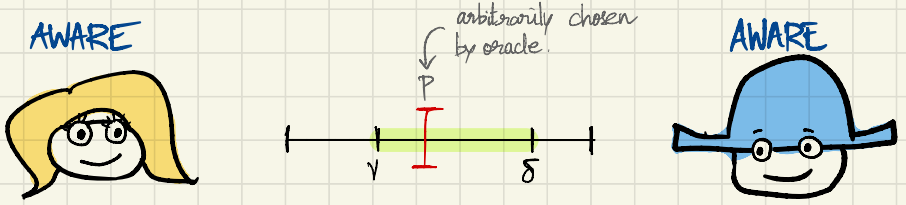
III:



$$\mathbb{C}_{C\text{-}BSC_{1}} \geq H(\nu) - H\left(\frac{\delta-\nu}{1-2\nu}\right)$$

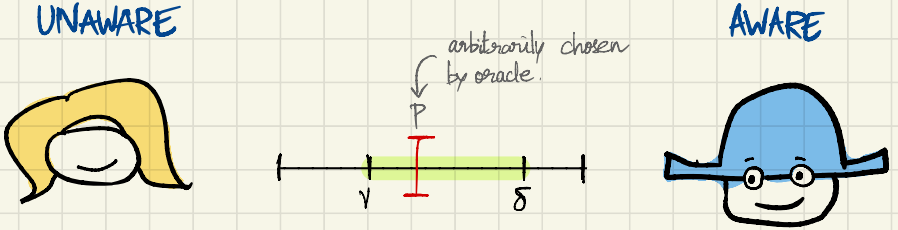
Main Results

I:



$$\mathbb{C}_{C\text{-}BSC_{1B}} = H(\nu)$$

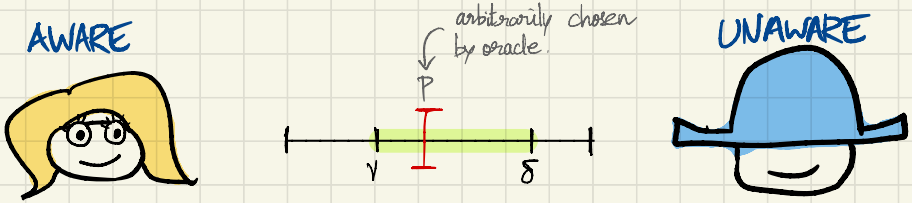
II:



$$\mathbb{C}_{C\text{-}BSC_{B}} = H(\nu)$$

→ Similar Achievability & Converse as in State-unaware case [Yadav et al NCC 2021]

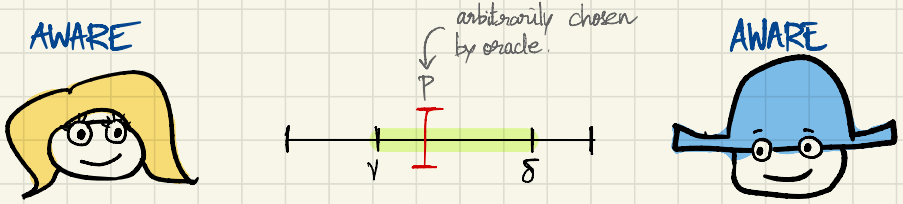
III:



$$\mathbb{C}_{C\text{-}BSC_{1}} \geqslant H(\nu) - H\left(\frac{\delta-\nu}{1-2\nu}\right)$$

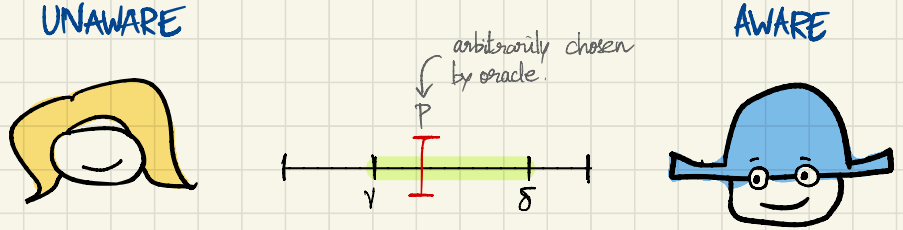
Main Results

I:



$$\mathbb{C}_{C\text{-}BSC_{1B}} = H(\nu)$$

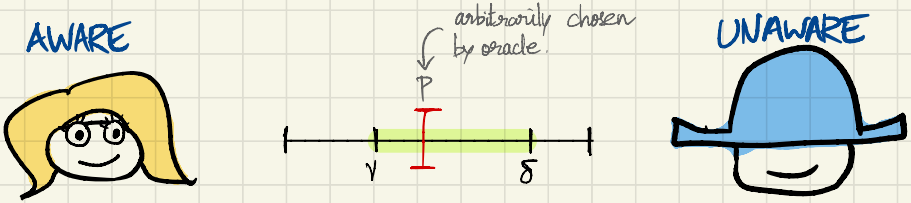
II:



$$\mathbb{C}_{C\text{-}BSC_{B}} = H(\nu)$$

AWARENESS MEETS CONTROL

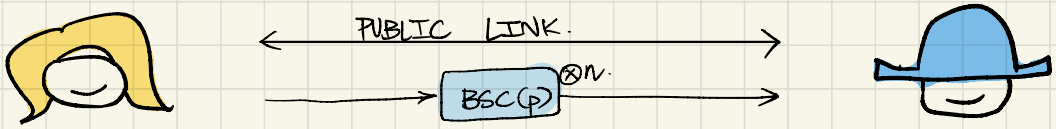
III:



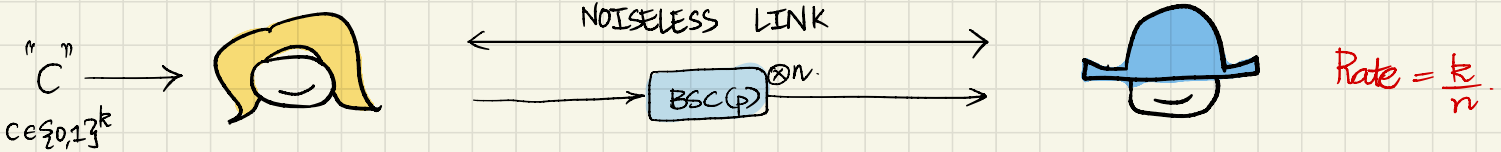
$$\mathbb{C}_{C\text{-}BSC_{1}} \geq H(\nu) - H\left(\frac{\delta-\nu}{1-2\nu}\right)$$

→ Achievability scheme [same as UNC≤]

Achievable Protocols over BSC(p)

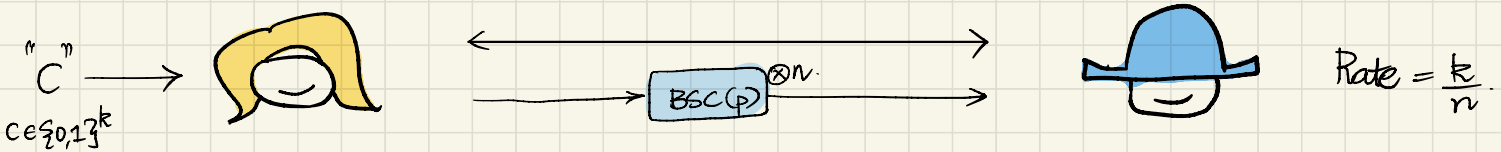


Achievable Protocols over BSC(p)



$\text{Rate} = \frac{k}{n}$.

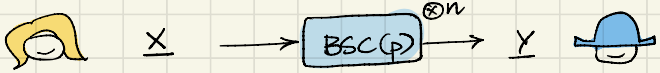
Achievable Protocols over BSC(p)



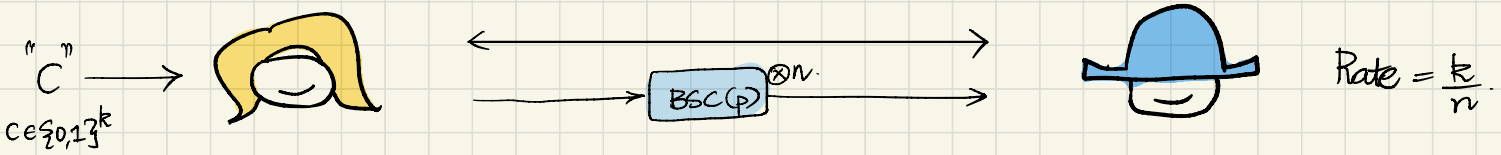
COMMIT PHASE

REVEAL PHASE

1. generates $\underline{x} \in \{0,1\}^n$ uniformly at random

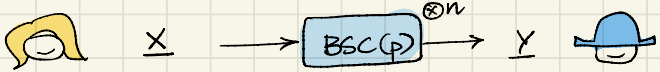


Achievable Protocols over BSC(p)



COMMIT PHASE

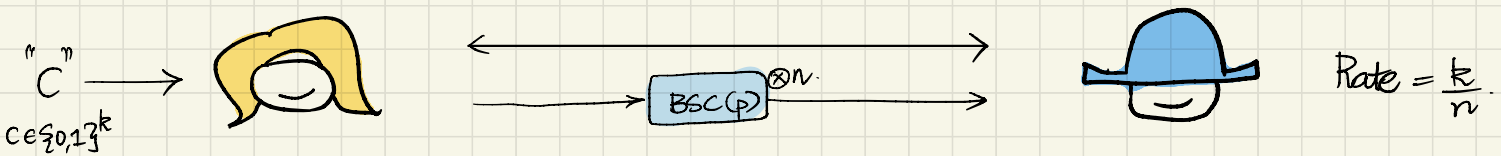
1. generates $\underline{x} \in \{0,1\}^n$ uniformly at random



2. picks Random Extractor "Ext"
$Ext : \{0,1\}^n \to \{0,1\}^k$

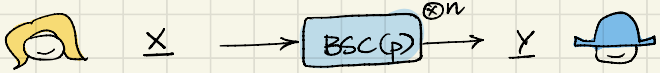
REVEAL PHASE

Achievable Protocols over BSC(p)



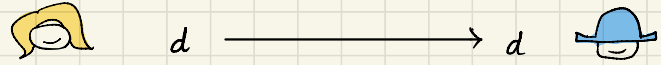
COMMIT PHASE

1. generates $\underline{x} \in \{0,1\}^n$ uniformly at random



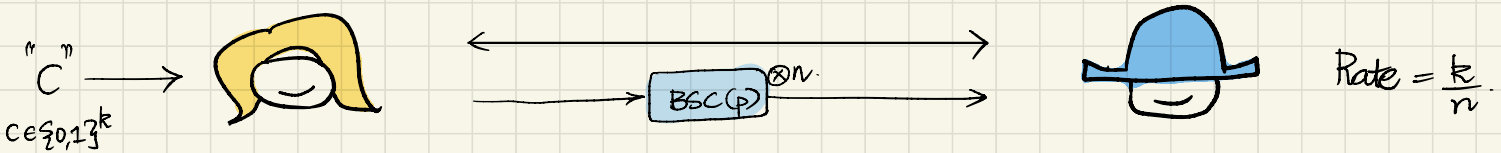
2. picks Random Extractor "Ext"
$Ext : \{0,1\}^n \to \{0,1\}^k$

3. $Ext(\underline{x}) = MASK$.
$c \oplus Ext(\underline{x}) =: d$



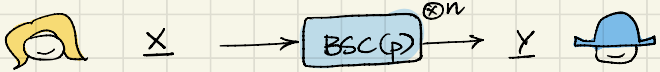
REVEAL PHASE

Achievable Protocols over BSC(p)



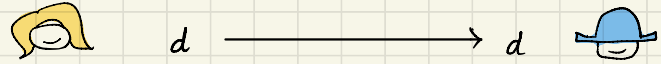
Commit Phase

1. generates $\underline{x} \in \{0,1\}^n$ uniformly at random



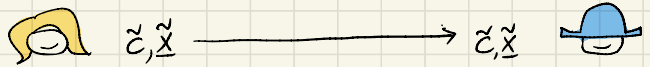
2. picks Random Extractor "Ext"
$\text{Ext} : \{0,1\}^n \to \{0,1\}^k$

3. $\text{Ext}(\underline{x}) = \text{MASK}$.
$c \oplus \text{Ext}(\underline{x}) =: d$

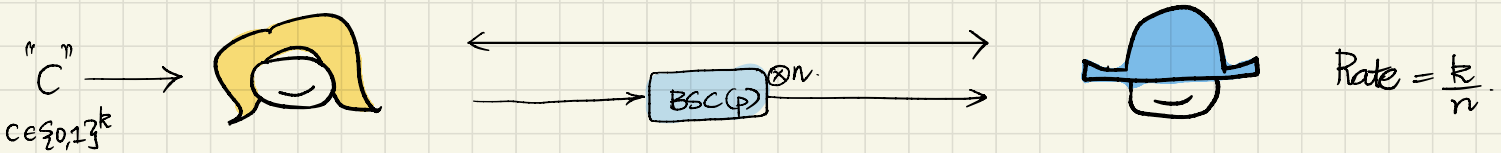


Reveal Phase

1. reveals $\tilde{c}, \underline{\tilde{x}}$

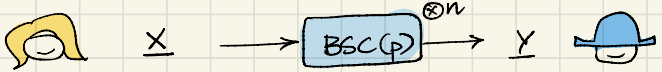


Achievable Protocols over BSC(p)



Commit Phase

1. generates $x \in \{0,1\}^n$ uniformly at random

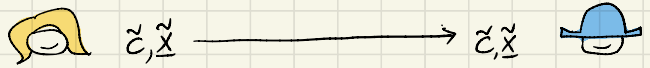


2. picks Random Extractor "Ext"
$Ext : \{0,1\}^n \to \{0,1\}^k$

3. $Ext(x) = MASK$.
$c \oplus Ext(x) =: d$

Reveal Phase

1. reveals $\tilde{c}, \tilde{x}$



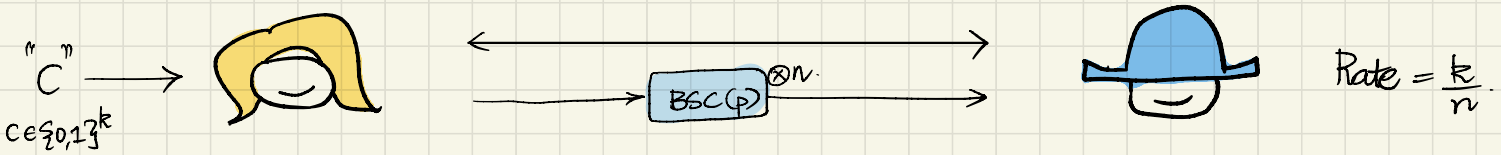
2. performs Tests. T.

(A) $\tilde{c} \oplus Ext(\tilde{x}) = d$
Are the mask and commit string consistent?

(B) $d_H(\tilde{x}, y) \in [np - n\nu, np + n\nu]$?

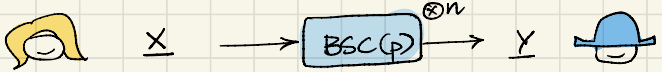
Theory of Typical sets, $\tilde{x}$ — BSC(p) — y ?

Achievable Protocols over BSC(p)



COMMIT PHASE

1. generates $x \in \{0,1\}^n$ uniformly at random



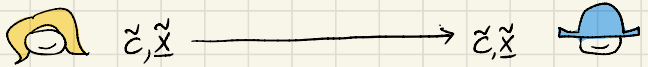
2. picks Random Extractor "Ext"
$Ext : \{0,1\}^n \to \{0,1\}^k$

3. $Ext(x) = MASK$.
$c \oplus Ext(x) =: d$

PRIVACY AMPLIFICATION (for concealment)

REVEAL PHASE

1. reveals $\tilde{c}, \tilde{x}$



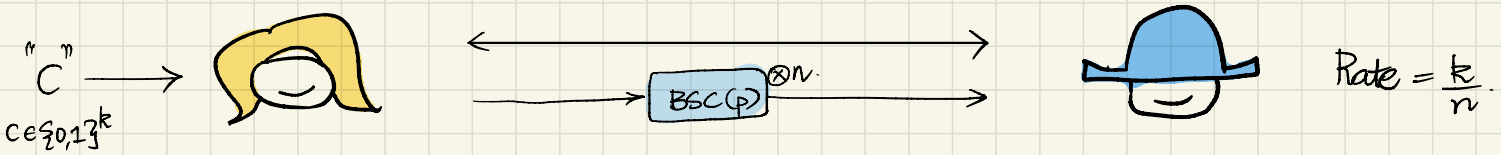
2. performs Tests. T.

→ (A) $\tilde{c} \oplus Ext(\tilde{x}) = d$
Are the mask and commit string consistent?

(B) $d_H(\tilde{x}, y) \in [np - n\nu, np + n\nu]$?

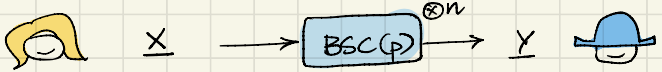
Theory of Typical sets, $\tilde{x}$ — BSC(p) — y ?

Achievable Protocols over BSC(p)



COMMIT PHASE

1. generates $\underline{x} \in \{0,1\}^n$ uniformly at random

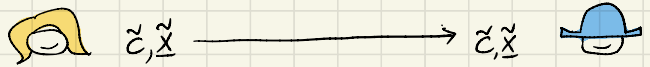


2. picks Random Extractor "Ext"
$\text{Ext} : \{0,1\}^n \to \{0,1\}^k$

3. $\text{Ext}(\underline{x}) = \text{MASK}$.
$c \oplus \text{Ext}(\underline{x}) =: d$

REVEAL PHASE

1. reveals $\tilde{c}, \underline{\tilde{x}}$



2. performs Tests. T.

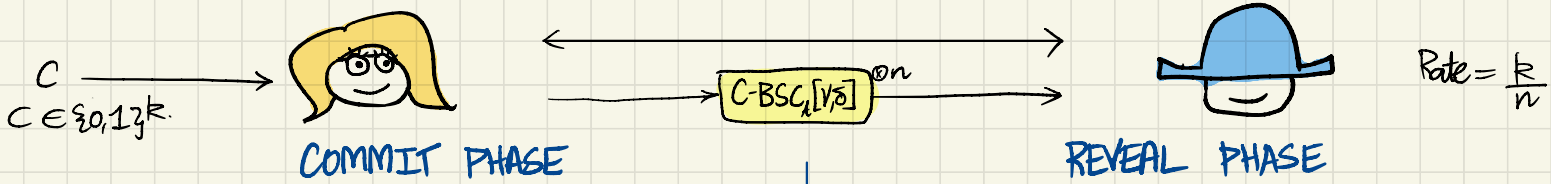
(A) $\tilde{c} \oplus \text{Ext}(\underline{\tilde{x}}) = d$
Are the mask and commit string consistent?

→ (B) $d_H(\underline{\tilde{x}}, \underline{y}) \in [np - n\nu, np + n\nu]$?

Theory of Typical sets, $\underline{\tilde{x}}$ — BSC(p) — $\underline{y}$?

↳ soundness, bindingness.

Achievable Protocol over C-BSC$_A$[γ,δ]



1. generates $\underline{X}$ → C-BSC$_A$[γ,δ] (⊗n) → $\underline{Y}$

4. picks Ext → Ext

5. $C \oplus Ext(X)$
   d → d

1. reveals $\tilde{C}, \underline{\tilde{X}}$

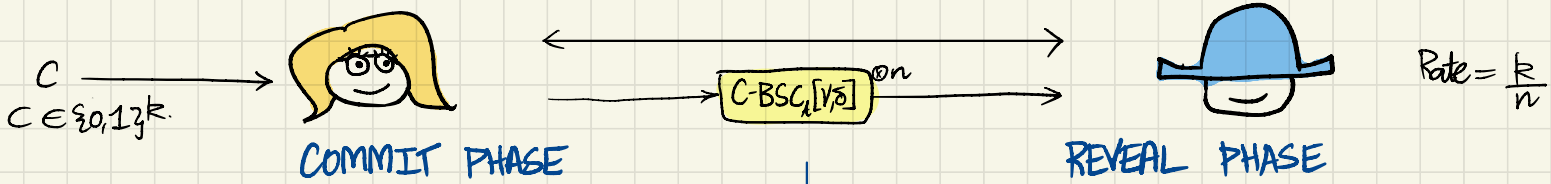
   $\tilde{C}, \underline{\tilde{X}}$ → $\tilde{C}, \underline{\tilde{X}}$

2. performs Tests. T.

(A) $\tilde{C} \oplus Ext(\underline{\tilde{X}}) = d$
Are the mask and commit string consistent?

(B) $d_H(\underline{\tilde{X}}, \underline{Y}) \in [n\gamma - n\epsilon, n\delta + n\epsilon]$

Achievable Protocol over C-BSC$_A$[γ,δ].



1. generates $\underline{X}$ → C-BSC$_A$[γ,δ] (⊗n) → $\underline{Y}$

4. picks Ext → Ext

5. $C \oplus Ext(X)$
   d → d

1. reveals $\tilde{C}, \underline{\tilde{X}}$

   $\tilde{C}, \underline{\tilde{X}}$ → $\tilde{C}, \underline{\tilde{X}}$

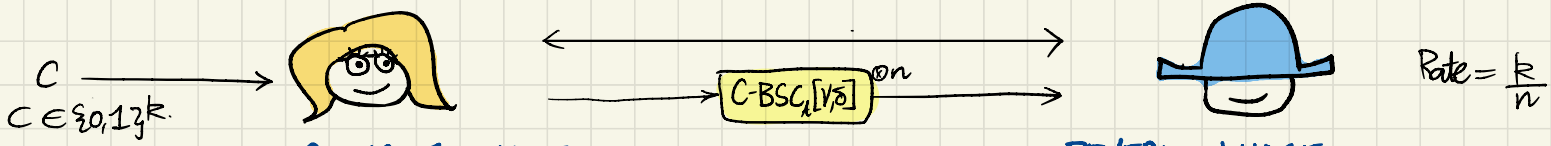
2. performs Tests. T.

(A) $\tilde{C} \oplus Ext(\underline{\tilde{X}}) = d$
Are the mask and commit string consistent?

(B) $d_H(\underline{\tilde{X}}, \underline{Y}) \in [n\gamma - n\epsilon, n\delta + n\epsilon]$

To account for $p \in [\gamma, \delta]$

Achievable Protocol over C-BSC$_A$[V,δ]



COMMIT PHASE

1. Alice generates $\underline{X}$ → C-BSC$_A$[V,δ] ⊗n → $\underline{Y}$
2. Bob picks $G_1 : \{0,1\}^n \to \{0,1\}^{\lceil nH(K) \rceil}$, sends G_1 to Alice
   Alice: $G_1(\underline{X})$ → $G_1(\underline{X})$
3. Alice picks $G_2 : \{0,1\}^n \to \{0,1\}^{nR_2}$, sends G_2 to Bob
   Alice: $G_2(\underline{X})$ → $G_2(\underline{X})$
4. Alice picks Ext → Ext
5. Alice: $C \oplus \text{Ext}(\underline{X}) = d$ → d

REVEAL PHASE

1. Alice reveals $\tilde{C}, \tilde{\underline{X}}$
   $\tilde{C}, \tilde{\underline{X}}$ → $\tilde{C}, \tilde{\underline{X}}$
2. Bob performs Tests. T.

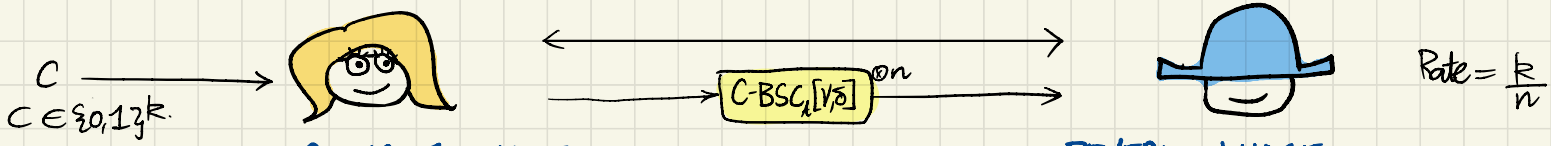
(A) $\tilde{C} \oplus \text{Ext}(\tilde{\underline{X}}) = d$
Are the mask and commit string consistent?

(B) $d_H(\tilde{\underline{X}}, \underline{Y}) \in [nV - n\epsilon, n\delta + n\epsilon]$

(C) $G_1(\tilde{\underline{X}}) = G_1(\underline{X})$, $G_2(\tilde{\underline{X}}) = G_2(\underline{X})$.

Extra-steps for bindingness ⇒ loss in throughput

Achievable Protocol over C-BSC$_A$[V,δ]



COMMIT PHASE

1. generates $\underline{X}$ → C-BSC$_A$[V,δ] ⊗n → $\underline{Y}$
2. picks $G_1 : \{0,1\}^n \to \{0,1\}^{n(H(K)-\frac{\alpha}{2})}$; G_1
   $G_1(\underline{X})$ → $G_1(\underline{X})$
3. picks $G_2 : \{0,1\}^n \to \{0,1\}^{n\alpha_2}$; G
   $G_2(\underline{X})$ → $G_2(\underline{X})$
4. picks Ext → Ext
5. $C \oplus Ext(\underline{X})$
   d → d

REVEAL PHASE

1. reveals $\tilde{C}, \tilde{\underline{X}}$
   $\tilde{C}, \tilde{\underline{X}}$ → $\tilde{C}, \tilde{\underline{X}}$
2. performs Tests. T.

(A) $\tilde{C} \oplus Ext(\tilde{\underline{X}}) = d$
Are the mask and commit string consistent?

(B) $d_H(\tilde{\underline{X}}, \underline{Y}) \in [nV - n\epsilon, n\delta + n\epsilon]$

(C) $G_1(\tilde{\underline{X}}) = G_1(\underline{X})$, $G_2(\tilde{\underline{X}}) = G_2(\underline{X})$.

OBSERVATIONS

Unreliable Noisy Channels – "Capabilities"

① AWARENESS
(publicly exercised)

② CONTROL
(privately exercised)

OBSERVATIONS

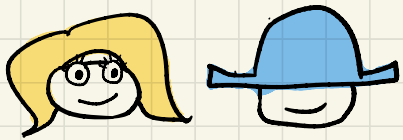
Unreliable Noisy Channels – "Capabilities"

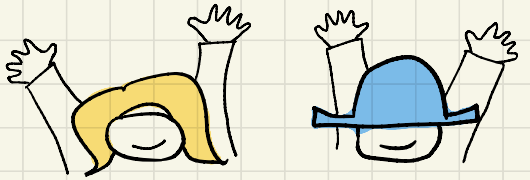
① AWARENESS (publicly exercised)

② CONTROL (privately exercised)

$C\text{-}BSC_{\lambda}[\gamma,\delta]$ $\equiv$ $UNC[\gamma,\delta]$

$\mathbb{C}_{C\text{-}BSC_{\lambda}}$ $\equiv$ $\mathbb{C}_{UNC}$





OBSERVATIONS

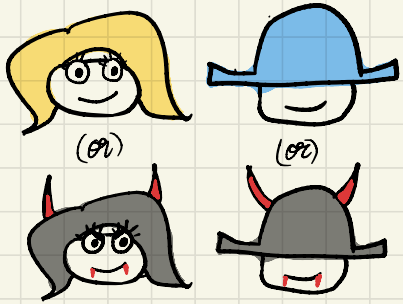
Unreliable Noisy Channels – "Capabilities"

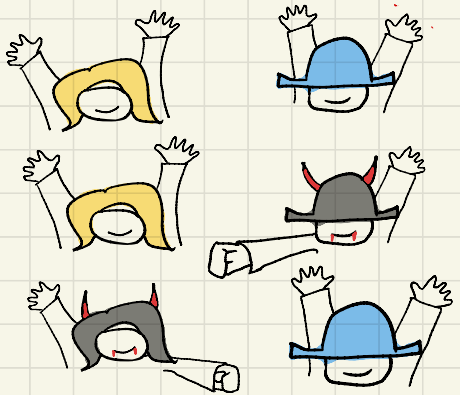
① AWARENESS
(publicly exercised)

② CONTROL
(privately exercised)

$C\text{-}BSC_\lambda[\gamma,\delta]$ $\quad=\quad$ $UNC[\gamma,\delta]$

$C_{C\text{-}BSC_\lambda}$ $\quad=\quad$ C_{UNC}





References

M. Blum, “Coin flipping by telephone a protocol for solving impossible problems,” ACM SIGACT News, vol. 15, no. 1, pp. 23–27, Jan. 198

C. Cre´peau and J. Kilian, “Achieving oblivious transfer using weakened security assumptions,” in [Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science. IEEE Computer Society, 1988, pp. 42–52.:

C. Cre´peau, “Efficient cryptographic protocols based on noisy chan- nels,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1997, pp. 306–317.

A. Winter, A. C. A. Nascimento, and H. Imai, “Commitment capacity of discrete memoryless channels,” in IMA International Conference on Cryptography and Coding. Springer, 2003, pp. 35–51.

M.Mamindlapally,A.K.Yadav,M.Mishra,andA.J.Budkuley,“Com- mitment capacity under cost constraints,” in 2021 IEEE International Symposium on Information Theory (ISIT). IEEE, 2021, pp. 3208–3213.

A. K. Yadav, M. Mamindlapally, A. J. Budkuley, and M. Mishra, “Commitment over compound binary symmetric channels,” in 2021 National Conference on Communications (NCC). IEEE, 2021, pp. 1–6.

I. Damga˚rd, J. Kilian, and L. Salvail, “On the (im) possibility of basing oblivious transfer and bit commitment on weakened security assump- tions,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 56–73.

C.Cre´peau,R.Dowsley,andA.C.A.Nascimento,“Onthecommitment capacity of unfair noisy channels,” IEEE Transactions on Information Theory, vol. 66, no. 6, pp. 3745–3752, 2020.

A. J. Budkuley, P. Joshi, M. Mamindlapally, and A. K. Yadav, “On re- verse elastic channels and the asymmetry of commitment capacity under channel elasticity,” IEEE Journal on Selected Areas in Communications, vol. 40, no. 3, pp. 862–870, 2022.