Information-theoretically Secure Bit Commitment over Noisy Channels

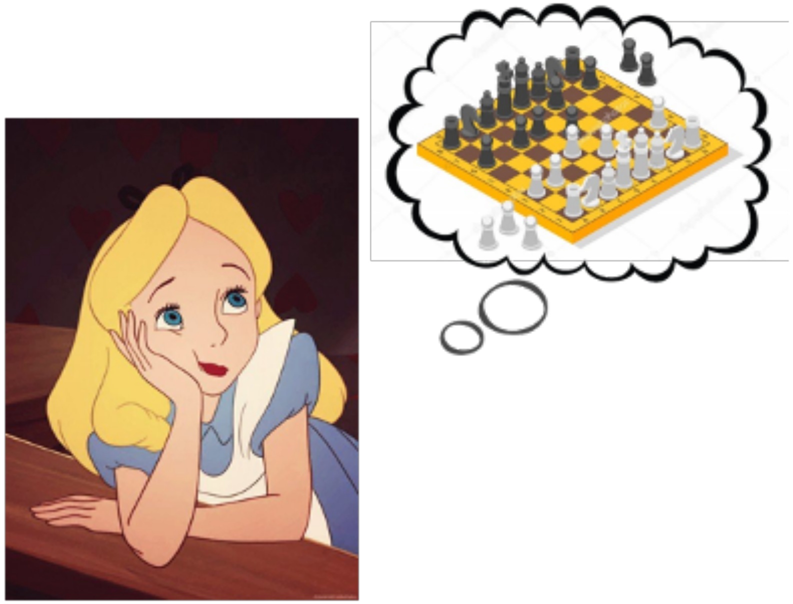
Anuj K. Yadav
LINX
EPFL

EPFL Information Processing Group

The Game of Chess

A problem!

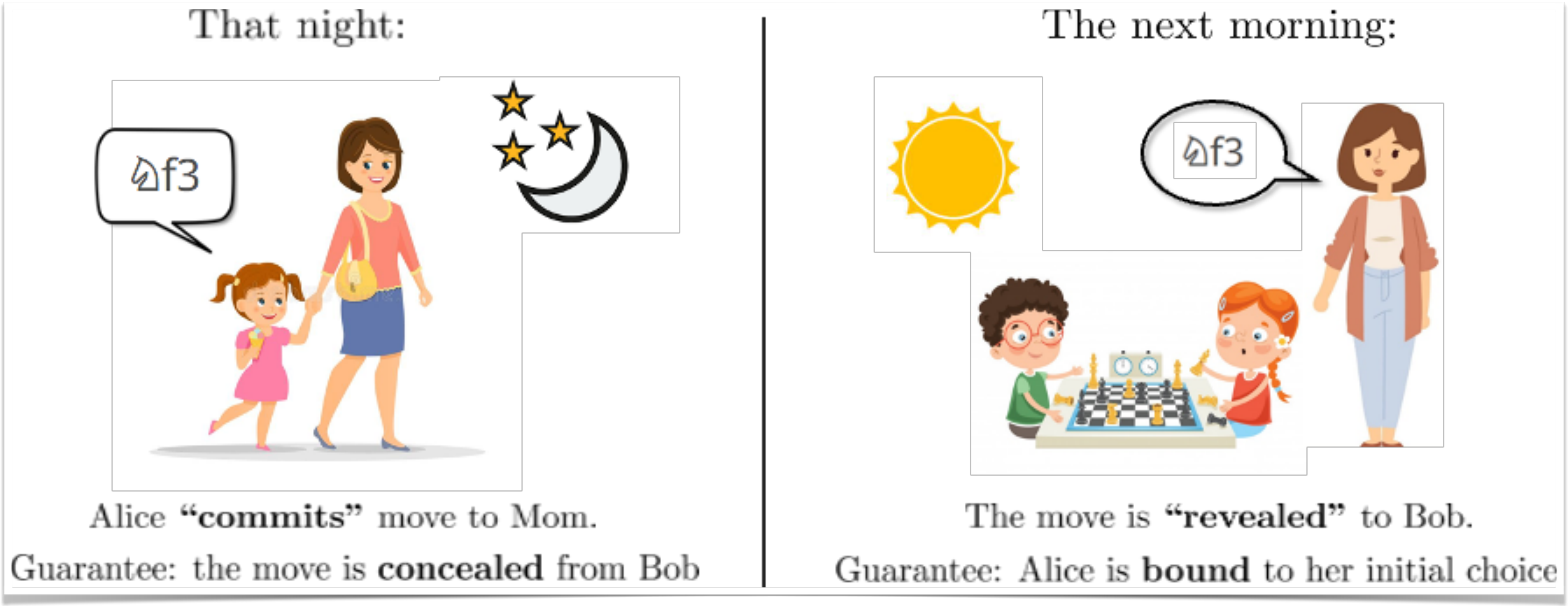
Alice's turn, but its bed time



Alice can think about her next move for the whole night

The Game of Chess

Potential Solution!



"Question" : What if no such **Trusted third Party** is available?

Answer :

Commitment Protocol!

What is Commitment?

- **Security Protocol**
- **Two users:** sender/committer *(<u>Alice</u>)* and a receiver/verifier *(<u>Bob</u>)*
- **Two Phases:** *"Commit Phase"* followed by a *"Reveal phase"*
- **Security Guarantees:** Soundness
  Concealment
  Bindingness
- **Applications:** Secure Multiparty Computation
  Zero-Knowledge Proofs
  Coin Tossing

Computational Security (CS)
VS
Information-theoretic Security (ITS)

- [Blum '83] — Introduced Commitment
- [Brassard et. al]— (comp. binding and IT concealing)
- [Ostrovksy et. al] — (comp. concealing and IT binding)

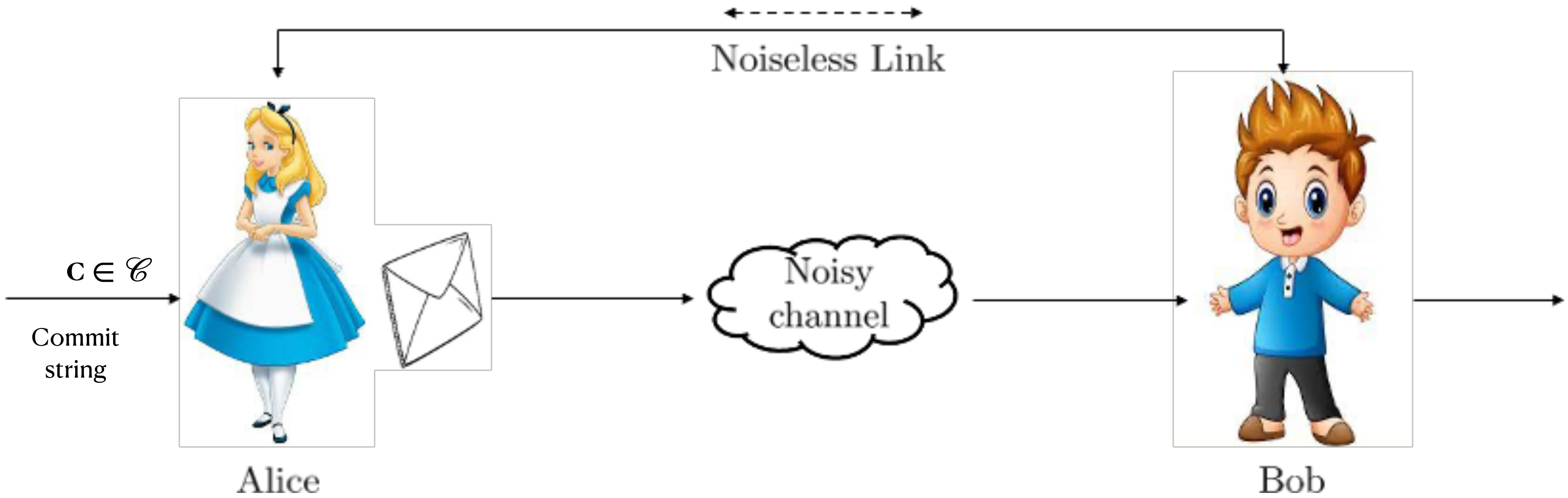
And many others....

What if both the users are "computationally unbounded" ?

- Noisy Communication Channel comes as a relief ! — [Creapau & Kilian '88]

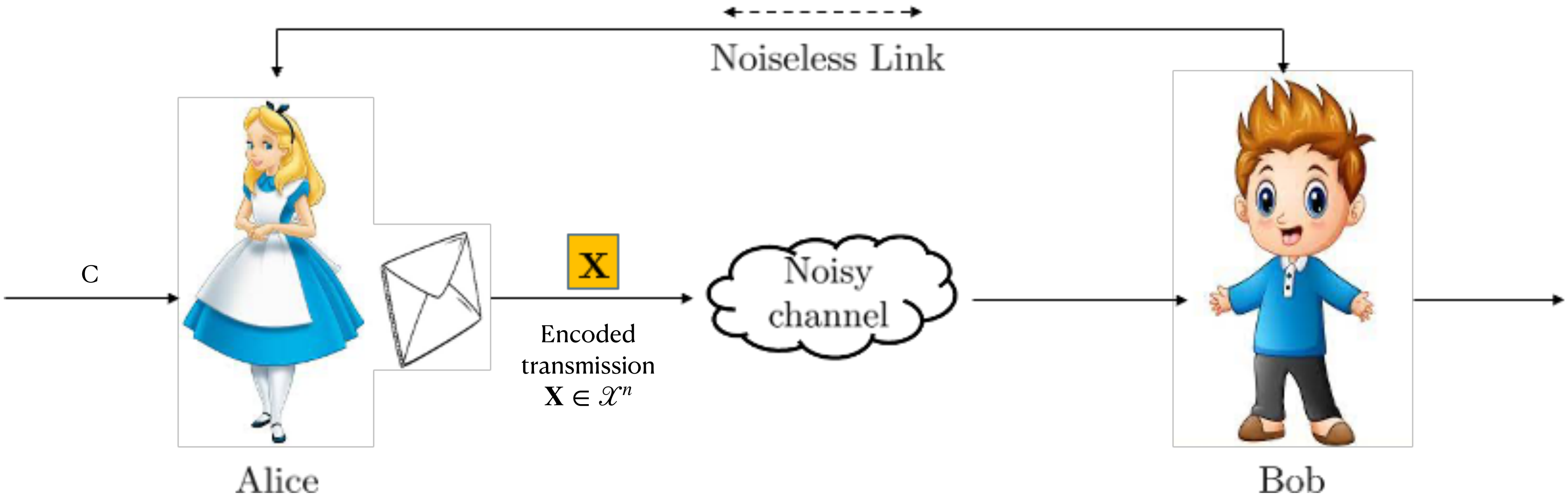
Commitment over Noisy Channels

Model



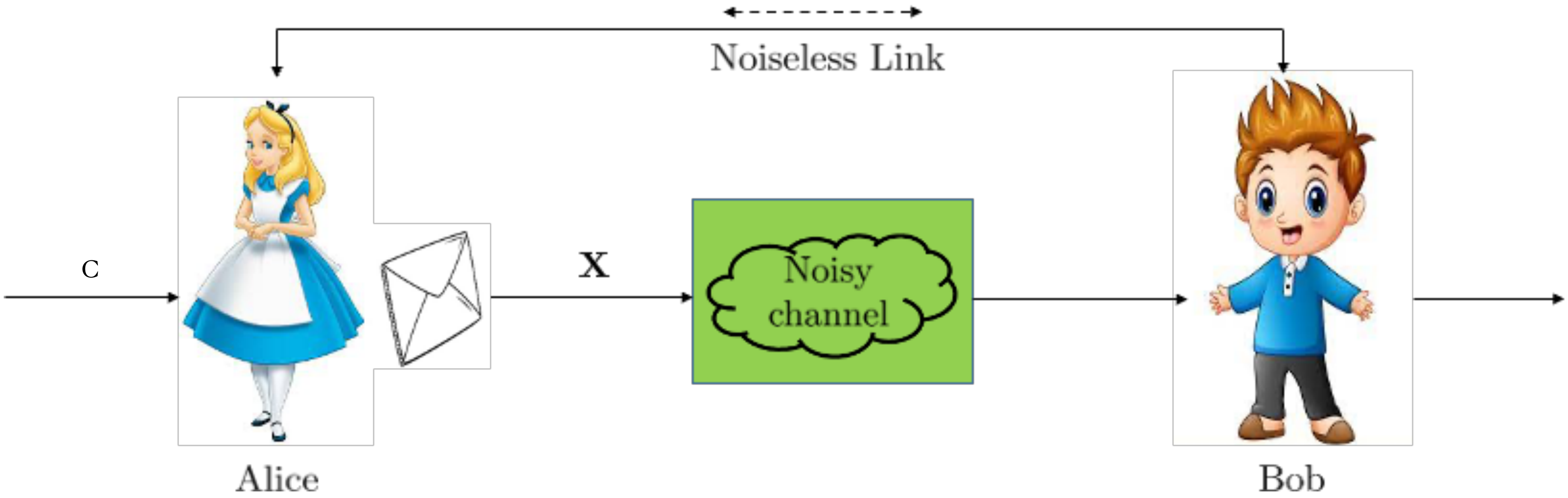
Commitment over Noisy Channels

Commit Phase



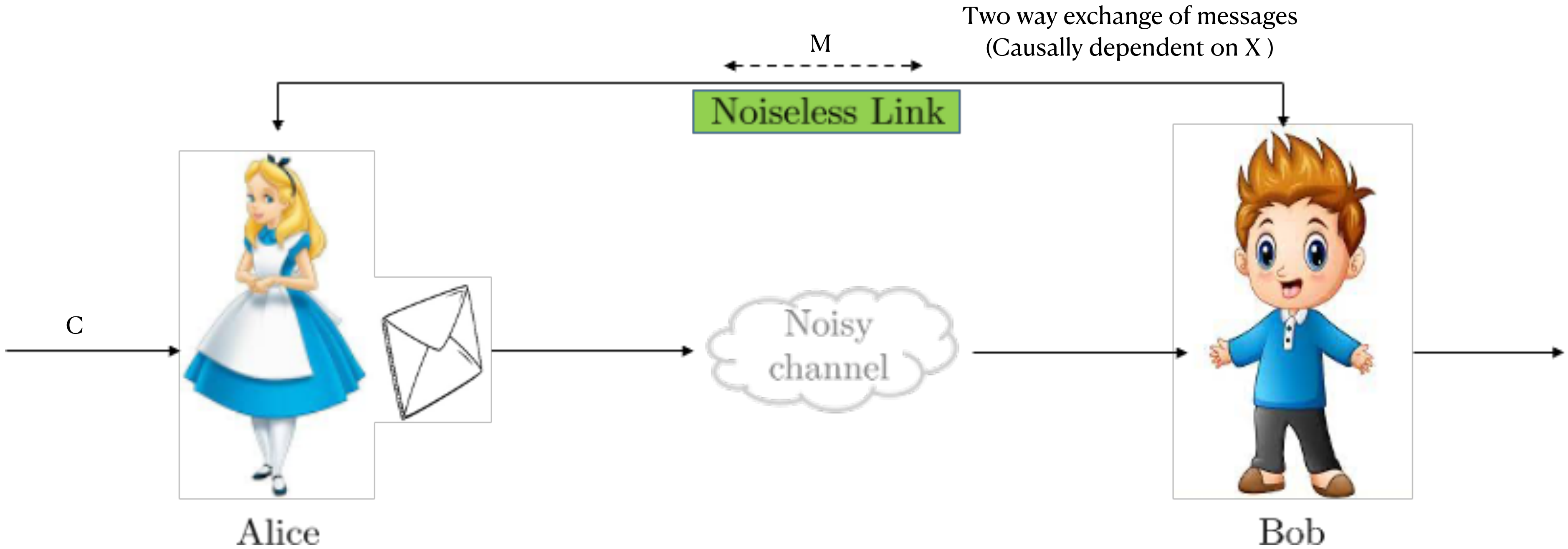
Commitment over Noisy Channels

Commit Phase



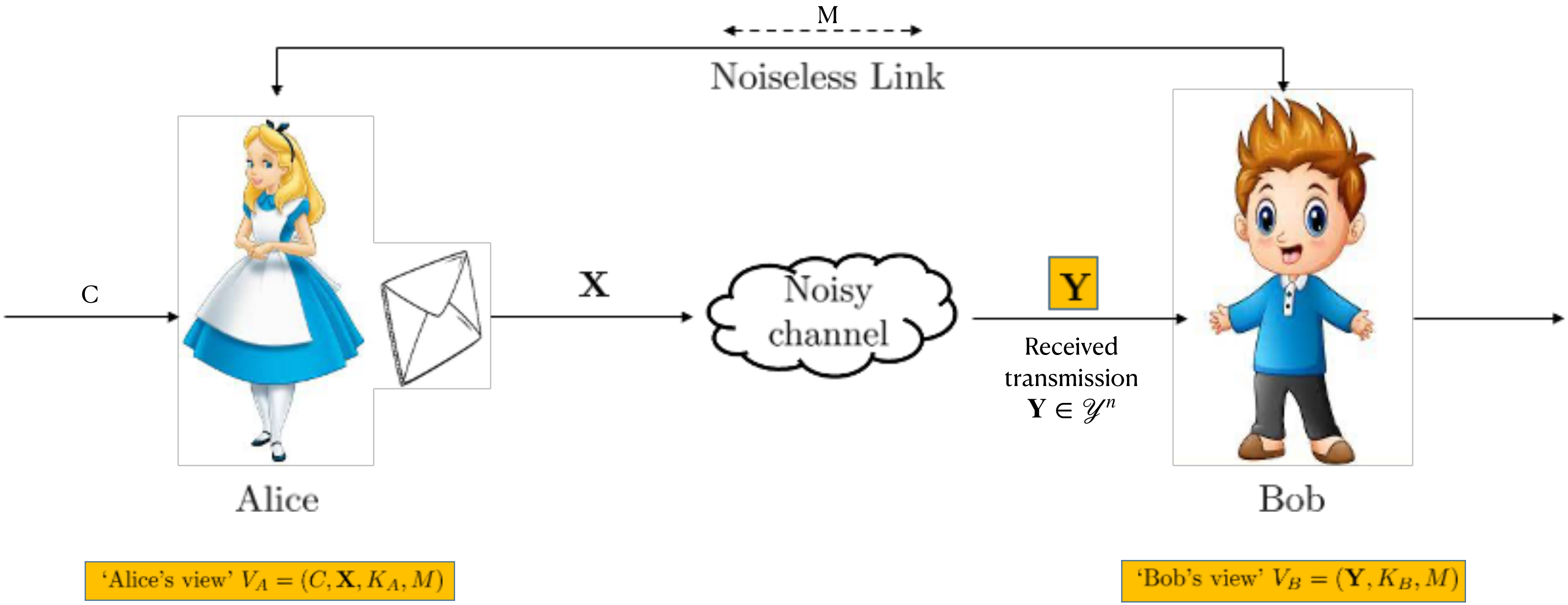
Commitment over Noisy Channels

Commit Phase



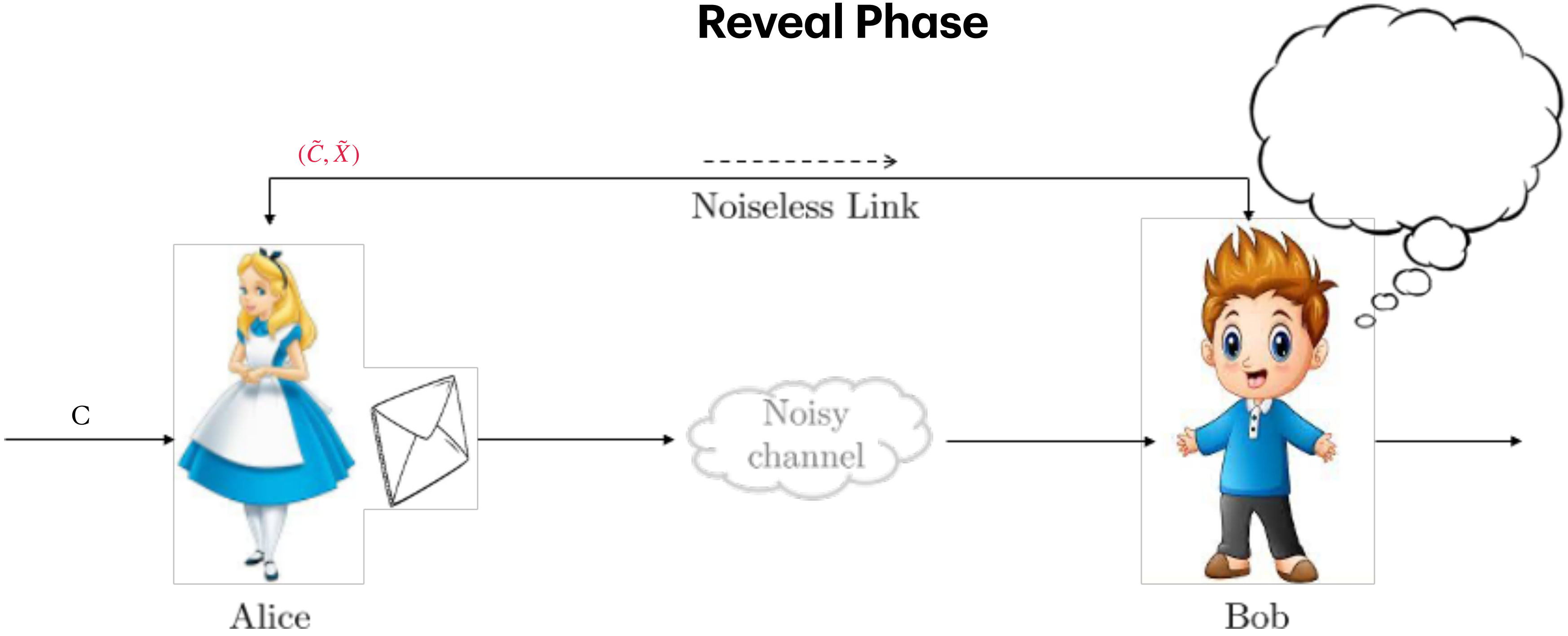
Commitment over Noisy Channels

Commit Phase



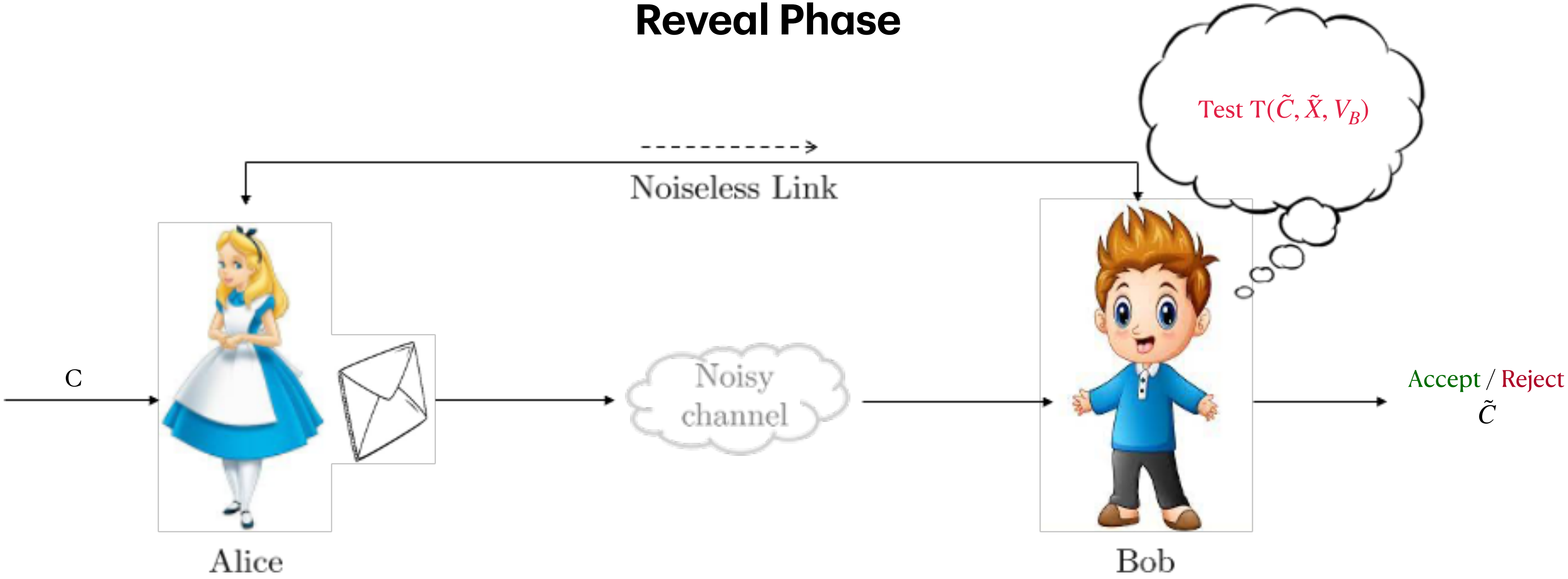
Commitment over Noisy Channels

Reveal Phase



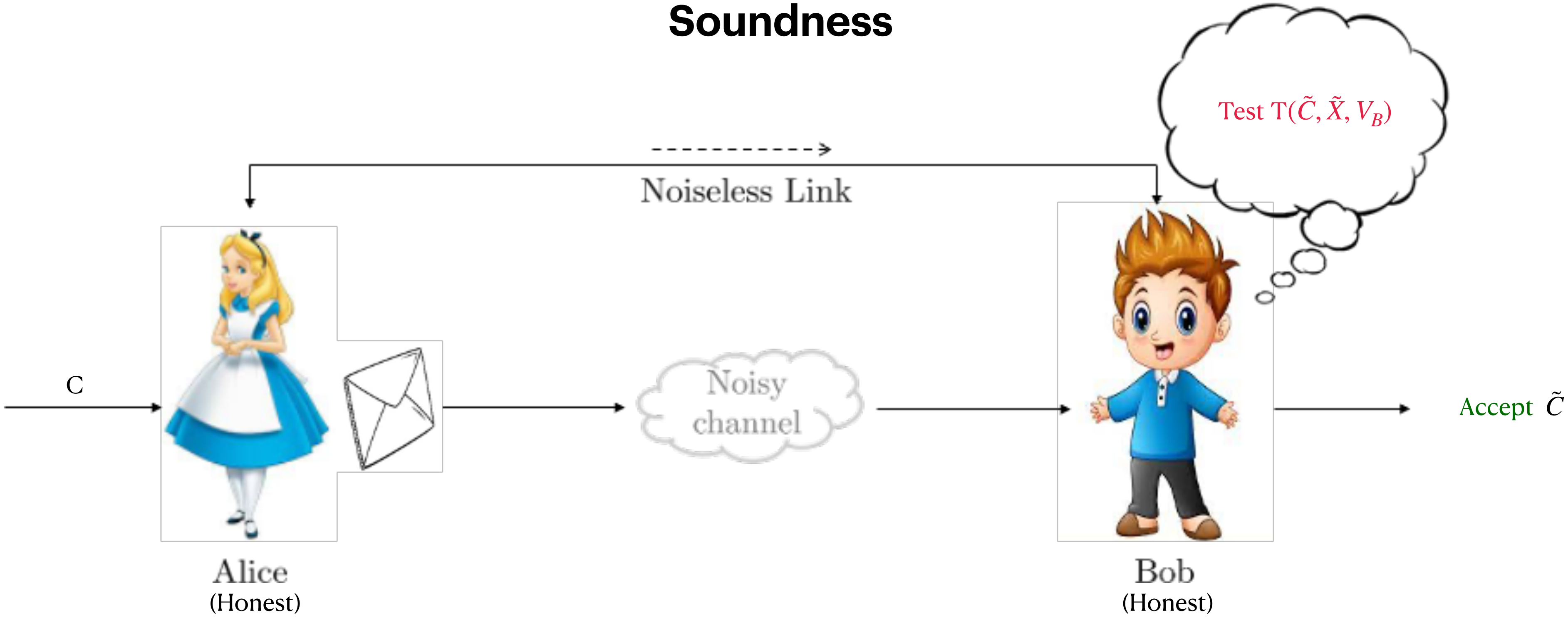
Commitment over Noisy Channels

Reveal Phase



Security Guarantees

Soundness

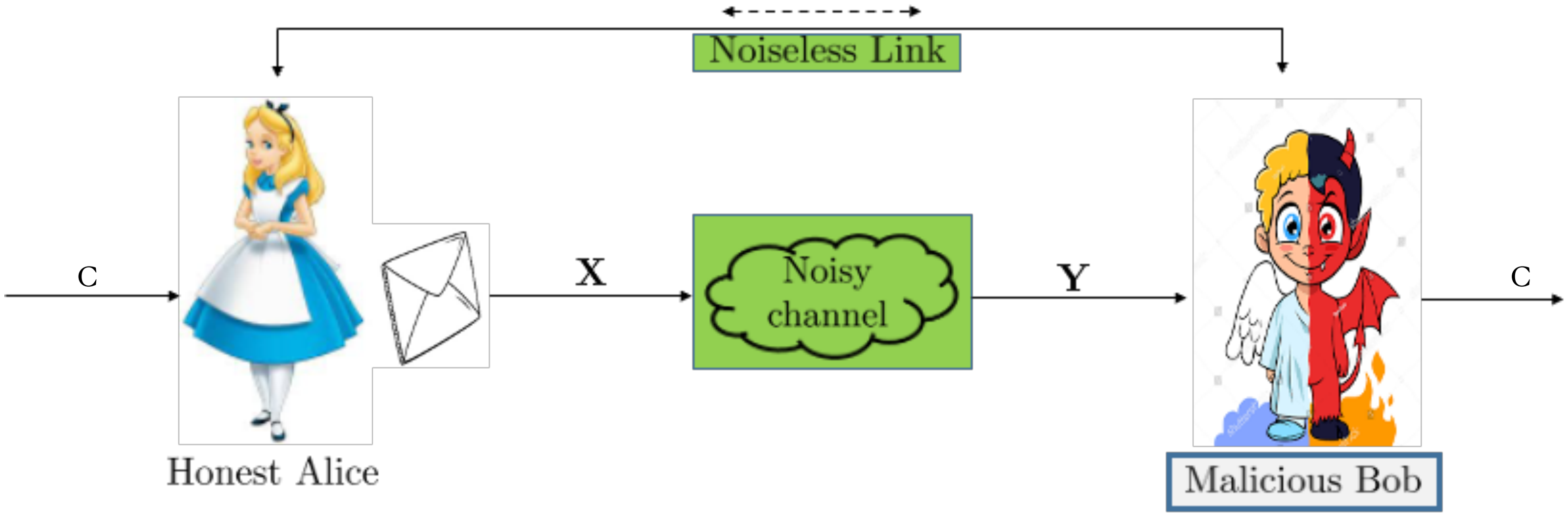


$$\mathbb{P}(T(C, X, V_B) = \text{REJECT}) \leq \epsilon(n)$$

Security Guarantees

Concealment

At the end of Commit Phase:



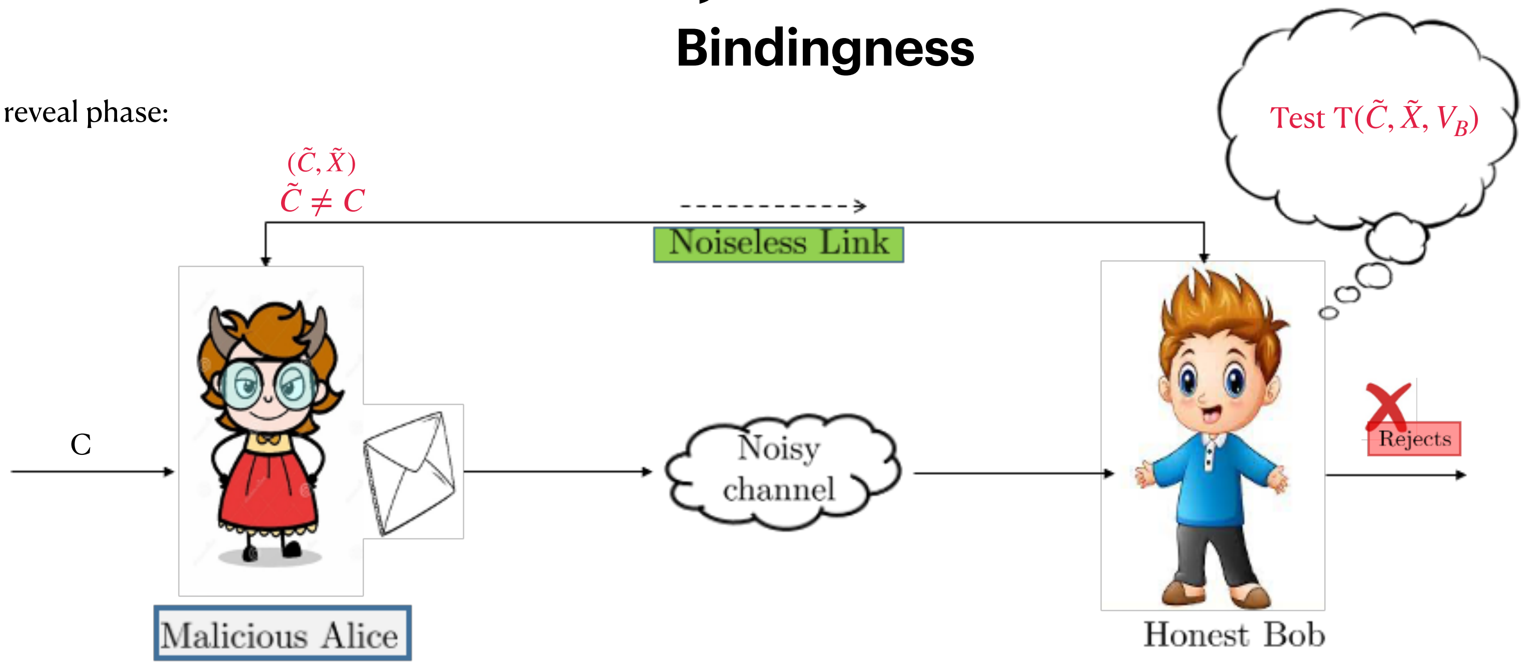
Malicious Bob can not learn Alice's Bid!

$$I(C; V_B) \leq \epsilon(n)$$

Security Guarantees

Bindingness

In the reveal phase:



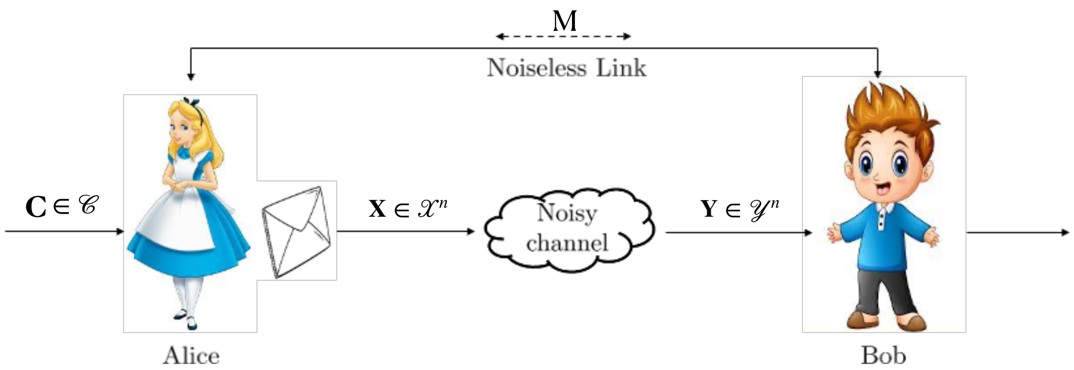
Bob's Test rejects dishonest Alice's cheating string

$$\mathbb{P}\left(T(\hat{C}, \hat{X}, V_B) = \text{"Accept"} \;\&\; T(\tilde{C}, \tilde{X}, V_B) = \text{"Accept"} \right) \leq \epsilon(n)$$

$$\forall (\hat{C}, \hat{X}),\ (\tilde{C}, \tilde{X}) : \hat{C} \neq \tilde{C}$$

Commitment over Noisy Channels

Commitment Rate & Capacity



Commitment Rate (R) $:= \dfrac{\log |\mathscr{C}|}{n}$

Rate $R > 0$ is <u>"achievable"</u> if $\forall\ \epsilon > 0, \forall n$ sufficiently large. $\exists$ an $(n; R)-$commitment protocol $\mathcal{P}\ : \mathcal{P}$ is $\epsilon-$sound, $\epsilon-$ binding and $\epsilon-$concealing.

$$\mathbb{C} := \sup\{R : R \text{ is achievable }\}$$

Commitment over Noisy Channels

Commitment Capacity

Noisy Channels

Reliable
Noisy Channels

- Perfectly characterised by a fixed transition function
- Examples: DMC($W_{Y|X}$), BSC(p), BEC(p), AWGN(0,σ^2) , etc..

Unreliable
Noisy Channels

- Poorly characterised Channels
- Users are unaware of the precise channel behaviour.
- Examples: Compound DMC ($\{W_{Y|X}\}_{s\in\mathcal{S}}$), AVC($W_{Y|X,S}$), **UNC**$[\gamma,\delta]$, **Elastic Channel (EC)-**$[\gamma,\delta]$, **Reverse Elastic Channels (REC)-**$[\gamma,\delta]$.

Commitment over Noisy Channels

Known Results on Capacity over Channels

<u>Discrete Memoryless Channels (DMC)</u> $\{W_{Y|X}\}$

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

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

[Winter et. al '04 (IMA ICCC)]

<u>Cost-Constrained DMC</u> $\{\rho_X, \Gamma, W_{Y|X}\}$**:**

$$C(\Gamma) = \max_{P_X : \mathbb{E}[\rho_X(X) \leq \Gamma]} H(X \mid Y)$$

$$C(\Gamma) = \min_{\gamma \geq 0} \max_{Q_Y} \log \left[\sum_{x \in \mathcal{X}} 2^{-D(W_{Y|X}(\cdot|x)||Q_Y(\cdot)) + \gamma(\Gamma - \rho_X(x))} \right]$$

[MYBM '21 (ISIT)]

<u>Compound- Discrete Memoryless Channels (C-DMC)</u> $\{W_{Y|X}\}_{s \in \mathcal{S}}$

$$C_{C-DMC} = \max_{P_X} \min_{s \in \mathcal{S}} H(X \mid Y)$$

$$C_{BSC[p,q]} = H(p)$$

[YMBM'21 (NCC)]

<u>State-aware compound channels (honest-but-curious users):</u>

Receiver is state-aware:

$$C_{C-DMC} = \max_{P_X} \min_{s \in \mathcal{S}} H(X \mid Y)$$

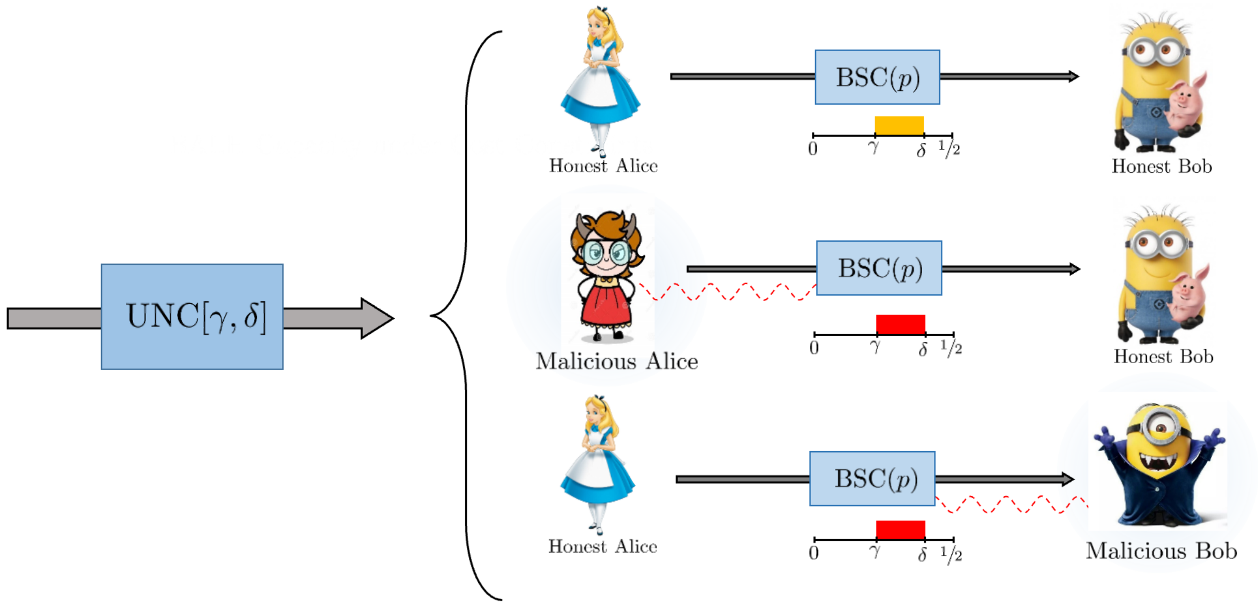
Sender is state-aware:

$$C_{C-DMC} = \min_{P_X} \max_{s \in \mathcal{S}} H(X \mid Y)$$

[YMBM'22 (COMSNETS)]

Unreliable Noisy Channels

Unfair Noisy Channel (UNC)-$[\gamma, \delta]$
[Damgard et. al '99 (EUROCRYPT)]

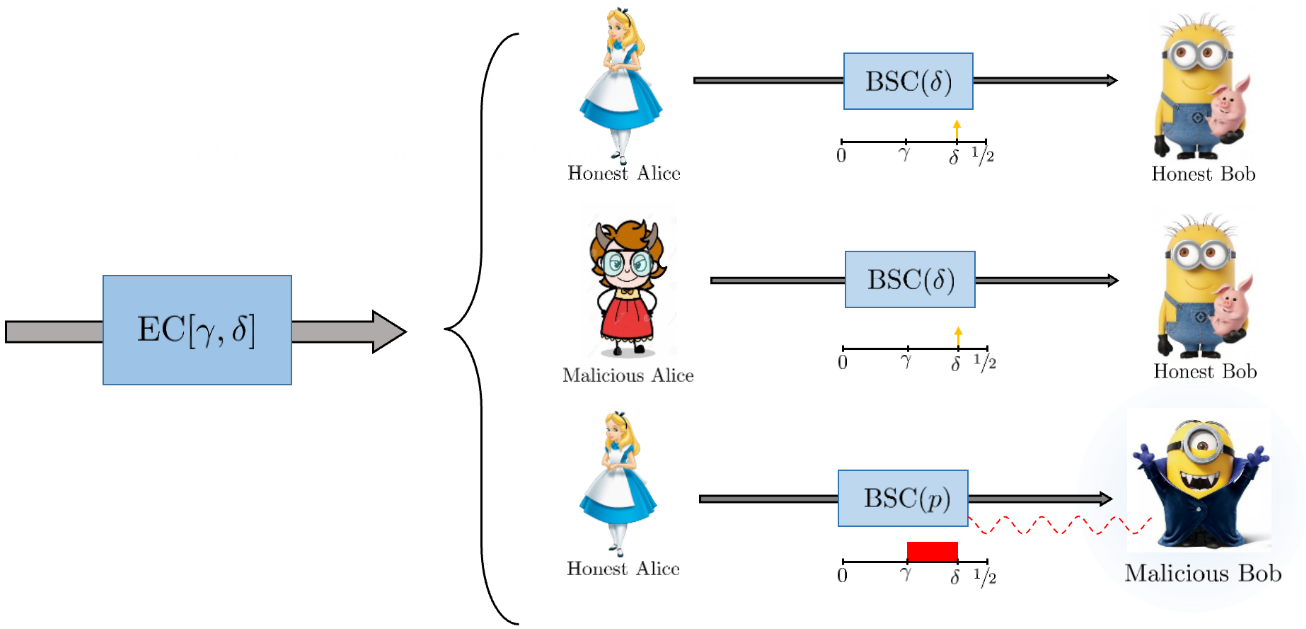


If $\delta \geq \gamma * \gamma = 2\gamma(1-\gamma)$. Then, $C_{UNC} = 0$. [Damgard et. al '99]

If $\delta < 2\gamma(1-\gamma)$. Then, $C_{UNC} = H(\gamma) - H\left(\frac{\delta - \gamma}{1 - 2\gamma}\right)$ [Crepeau et. al '20 (Trans. IT)]

Unreliable Noisy Channels

Elastic Channel (EC) -$[\gamma, \delta]$
[Khurana et. al '16 (EUROCRYPT)]

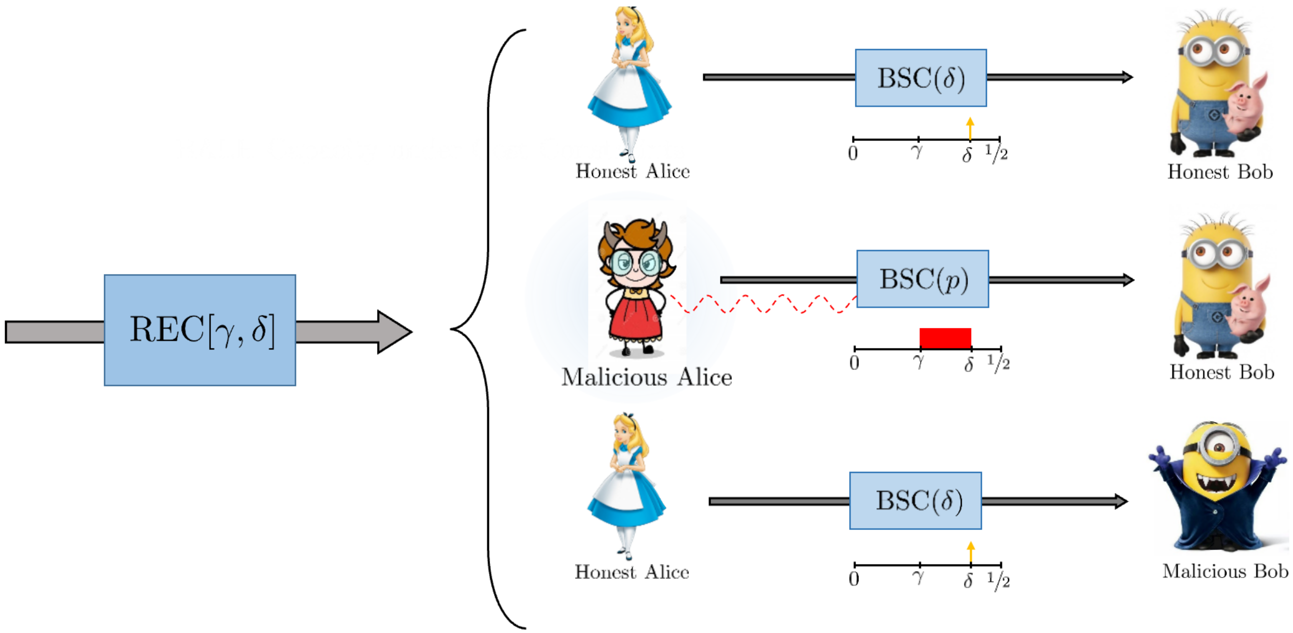


$C_{EC} \geq 0$ [Khurana et. al '16]

$C_{EC} = H(\gamma)$ [Crepeau et. al '20]

Unreliable Noisy Channels

Reverse Elastic Channel (EC) -$[\gamma, \delta]$



$$C_{REC} = H(\delta) - H\left(\frac{\delta - \gamma}{1 - 2\gamma}\right)$$

Conjectured by [Crepeau et. al '20]

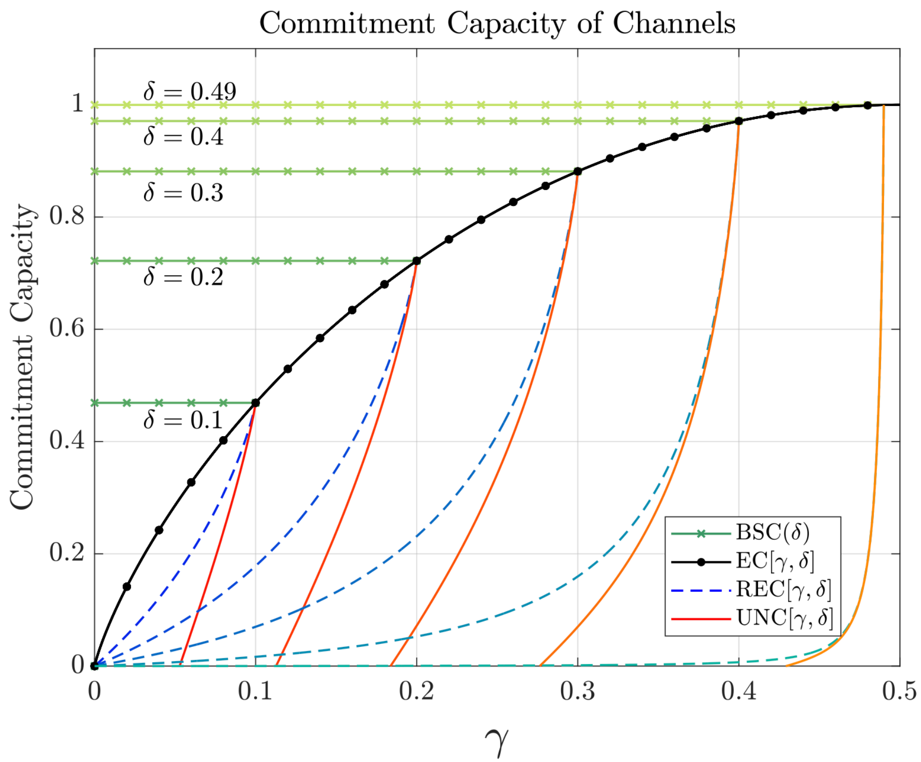
Commitment Capacity of REC-$[\gamma, \delta]$

Key results from [BJMY '22 (JSAC)]

- $C_{REC} \geq 0.\ \forall\ 0 < \gamma < \delta < 1/2$
- $C_{REC} = H(\delta) - H\left(\dfrac{\delta - \gamma}{1 - 2\gamma}\right)$
- $C_{REC} \leq C_{EC}$ i.e., Asymmetry in Commitment Capacity in channels with one-sided elasticity.
- For honest-but-curious users, we have $C_{REC} = C_{EC}$

Comparison of Commitment Capacities

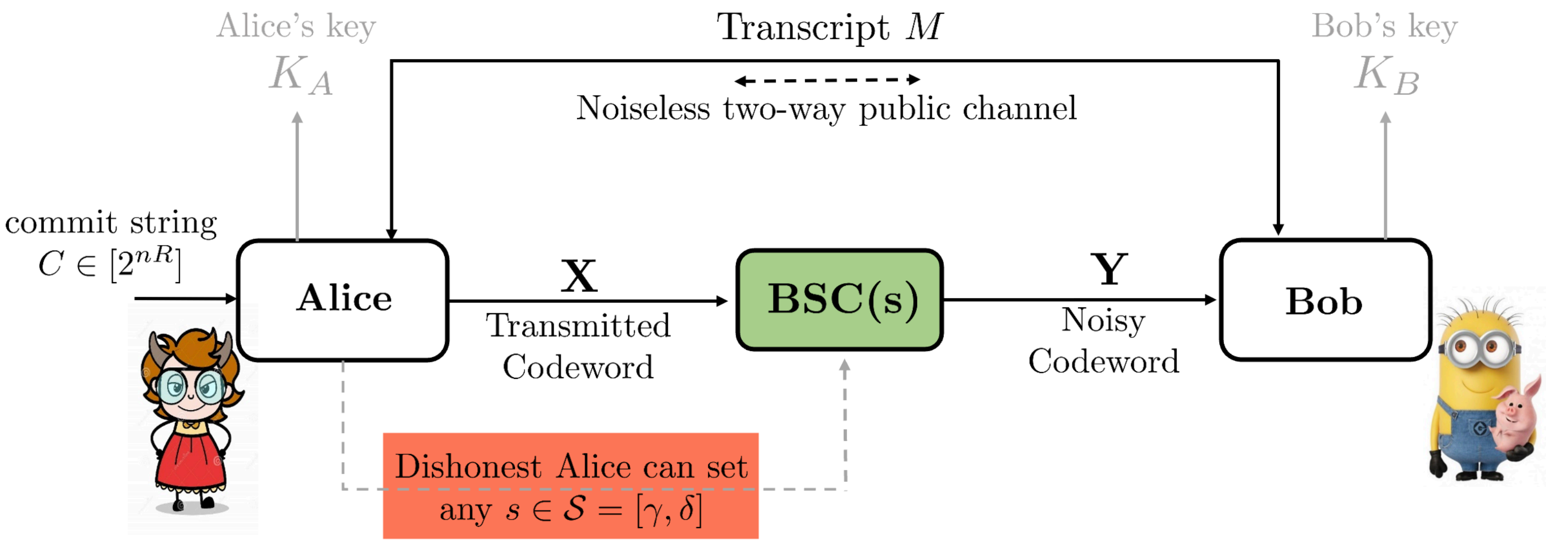
Key results



$$C_{BSC(\delta)} \geq C_{EC[\gamma,\delta]} \geq C_{REC[\gamma,\delta]} \geq C_{UNC[\gamma,\delta]}$$

Commitment over REC-$[\gamma, \delta]$

Revisiting Problem Setup



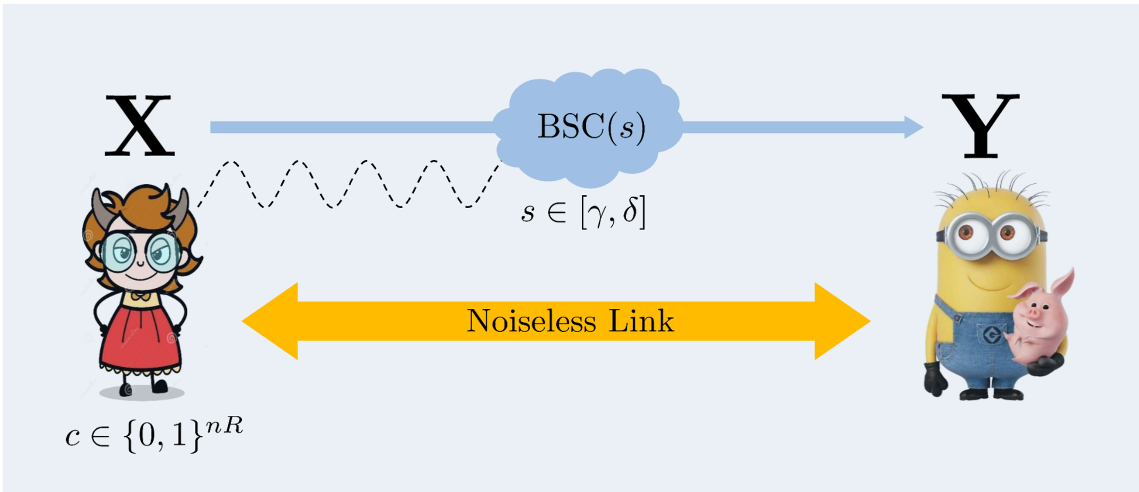
Reverse Elastic channel EC$[\gamma, \delta]$
$(0 < \gamma < \delta < \frac{1}{2})$

Commitment over REC-$[\gamma, \delta]$

Converse

Alice's Cheating Strategy

Alice sets the channel to be a BSC(s), $s \in [\gamma, \delta]$
This allows her some room to cheat

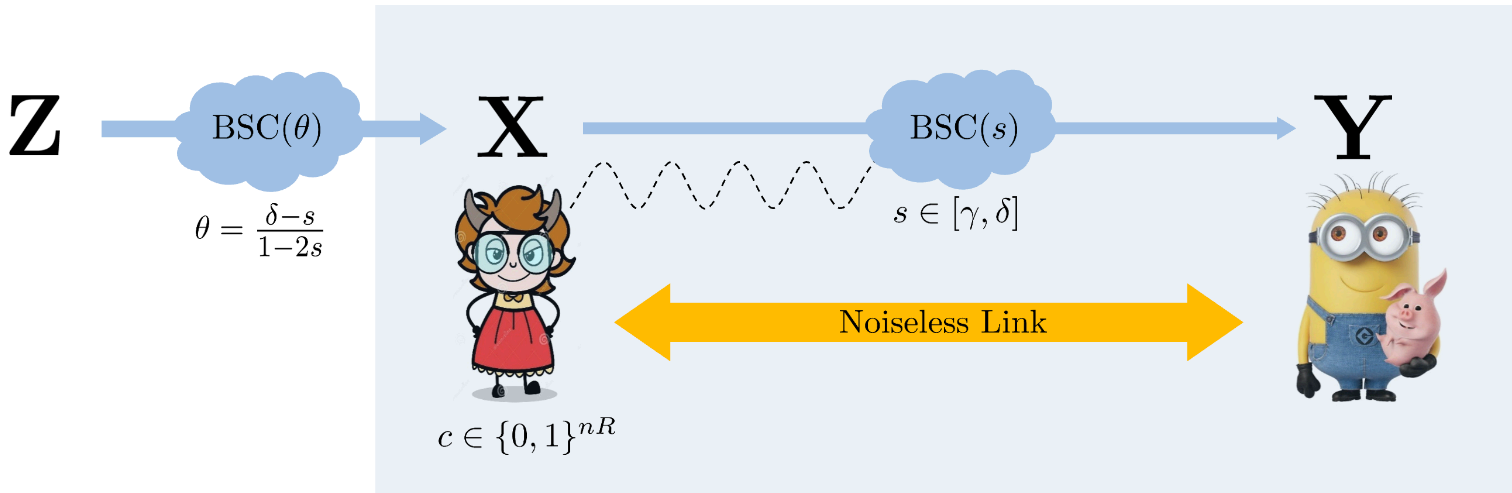


Commitment over REC-$[\gamma, \delta]$

Converse

Alice's Cheating Strategy

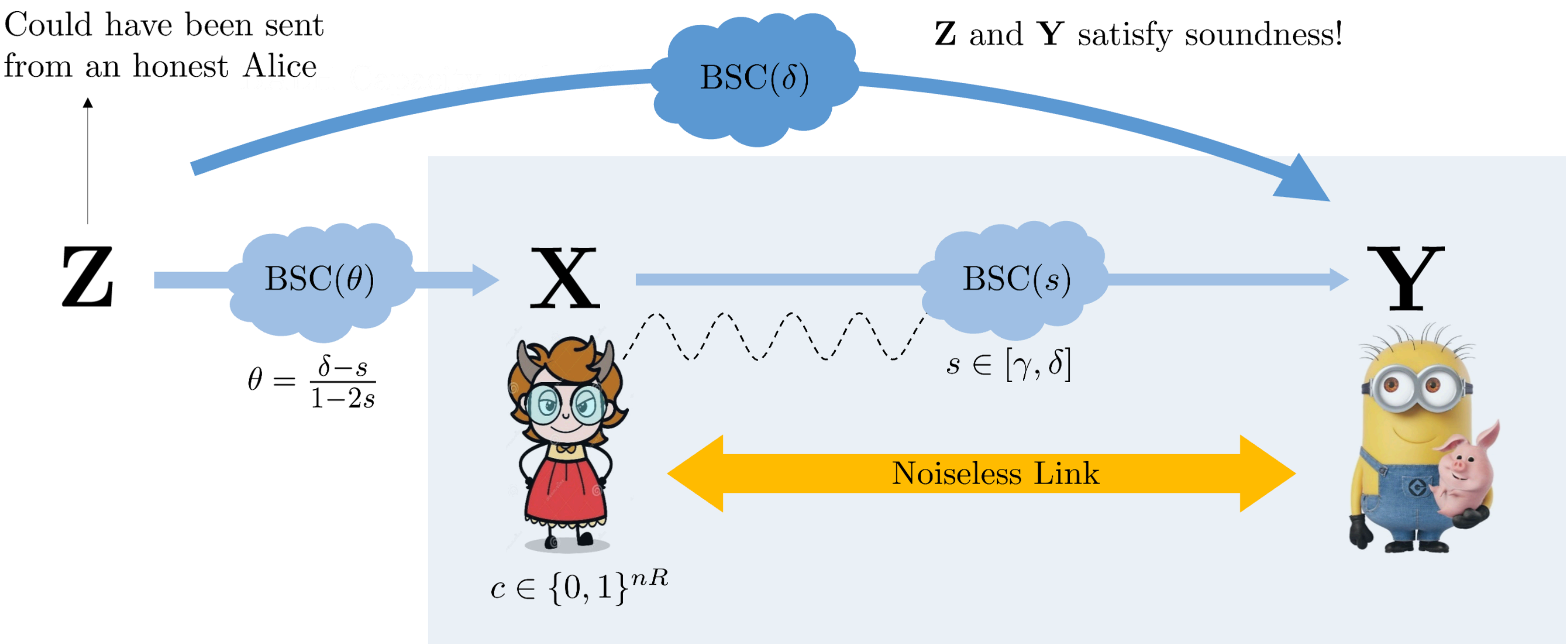
Alice sets the channel to be a BSC(s), $s \in [\gamma, \delta]$
This allows her some room to cheat



Commitment over REC-$[\gamma, \delta]$

Converse

Alice's Cheating Strategy



Commitment over REC-$[\gamma, \delta]$

Converse

A rate R scheme: $\epsilon_n - sound$, $\epsilon_n - concealing$ and $\epsilon_n - binding$ $\left(\epsilon_n \overset{n \to \infty}{\longrightarrow} 0\right)$

$nR = H(C)$

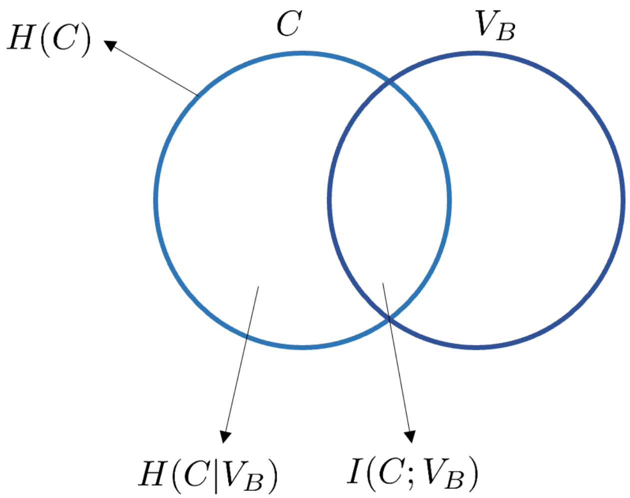
Because $C \in \{0,1\}^{nR}$

Now, we analyse this expression **assuming Alice executes the cheating strategy described previously**

Commitment over REC-[γ, δ]

Converse

$$
\begin{aligned}
nR &= H(C) \\
&\boxed{= H(C|V_B) + I(C;V_B)} \\
&\leq H(C|\mathbf{Y}, M, K_B) + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon_n \\
&\leq H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon'' + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|M, K_B) + \epsilon'' + \epsilon_n \\
&= I(C; \mathbf{YZ}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon \\
&= I(C; \tilde{\mathbf{Z}}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon
\end{aligned}
$$



Commitment over REC-[γ, δ]

Converse

$$
\begin{aligned}
nR &= H(C) \\
&= H(C|V_B) + I(C;V_B) \\
&\boxed{\le H(C|\mathbf{Y}, M, K_B) + \epsilon_n} \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon_n \\
&\le H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon'' + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|M, K_B) + \epsilon'' + \epsilon_n \\
&= I(C; \mathbf{Y}\mathbf{Z}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon \\
&= I(C; \tilde{\mathbf{Z}}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon
\end{aligned}
$$

$I(C;V_B) \le \epsilon_n$ by concealment

Commitment over REC-$[\gamma, \delta]$

Converse

$$
\begin{aligned}
nR &= H(C) \\
&= H(C|V_B) + I(C; V_B) \\
&\leq H(C|\mathbf{Y}, M, K_B) + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon_n \\
&\leq H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon'' + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|M, K_B) + \epsilon'' + \epsilon_n \\
&= I(C; \mathbf{Y}\mathbf{Z}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon \\
&= I(C; \tilde{\mathbf{Z}}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon
\end{aligned}
$$

Adding and subtracting

Commitment over REC-[γ, δ]

Converse

$$
\begin{aligned}
nR &= H(C) \\
&= H(C|V_B) + I(C;V_B) \\
&\leq H(C|\mathbf{Y}, M, K_B) + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon_n \\
&\boxed{\leq H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon'' + \epsilon_n} \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|M, K_B) + \epsilon'' + \epsilon_n \\
&= I(C;\mathbf{YZ}|M, K_B) - I(C;\mathbf{Y}|M, K_B) + \epsilon'' + \epsilon \\
&= I(C;\tilde{\mathbf{Z}}|M, K_B) - I(C;\mathbf{Y}|M, K_B) + \epsilon'' + \epsilon
\end{aligned}
$$

$H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \leq \epsilon''$

Commitment over REC-[γ, δ]

Converse

$$
\begin{aligned}
nR &= H(C) \\
&= H(C|V_B) + I(C;V_B) \\
&\leq H(C|\mathbf{Y},M,K_B) + \epsilon_n \\
&= H(C|\mathbf{Y},M,K_B) - H(C|\mathbf{Y},\mathbf{Z},M,K_B) \\
&\qquad\qquad + H(C|\mathbf{Y},\mathbf{Z},M,K_B) + \epsilon_n \\
&\leq H(C|\mathbf{Y},M,K_B) - H(C|\mathbf{Y},\mathbf{Z},M,K_B) + \epsilon'' + \epsilon_n \\
&= H(C|\mathbf{Y},M,K_B) - H(C|M,K_B) - H(C|\mathbf{Y},\mathbf{Z},M,K_B) \\
&\qquad\qquad + H(C|M,K_B) + \epsilon'' + \epsilon_n \\
&= I(C;\mathbf{YZ}|M,K_B) - I(C;\mathbf{Y}|M,K_B) + \epsilon'' + \epsilon \\
&= I(C;\tilde{\mathbf{Z}}|M,K_B) - I(C;\mathbf{Y}|M,K_B) + \epsilon'' + \epsilon
\end{aligned}
$$

Adding and subtracting $H(C|M,K_B)$

Commitment over REC-$[\gamma, \delta]$

Converse

$$
\begin{aligned}
nR &= H(C) \\
&= H(C|V_B) + I(C;V_B) \\
&\leq H(C|\mathbf{Y}, M, K_B) + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon_n \\
&\leq H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon'' + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|M, K_B) + \epsilon'' + \epsilon_n \\
&\boxed{= I(C; \mathbf{YZ}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon} \\
&= I(C; \tilde{\mathbf{Z}}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon
\end{aligned}
$$

Grouping 3^{rd} with 4^{th} term and 1^{st} with 2^{nd} term

Commitment over REC-$[\gamma, \delta]$

Converse

$$
\begin{aligned}
nR &= H(C) \\
&= H(C|V_B) + I(C; V_B) \\
&\leq H(C|\mathbf{Y}, M, K_B) + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon_n \\
&\leq H(C|\mathbf{Y}, M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) + \epsilon'' + \epsilon_n \\
&= H(C|\mathbf{Y}, M, K_B) - H(C|M, K_B) - H(C|\mathbf{Y}, \mathbf{Z}, M, K_B) \\
&\qquad\qquad + H(C|M, K_B) + \epsilon'' + \epsilon_n \\
&= I(C; \mathbf{YZ}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon \\
&\boxed{= I(C; \tilde{\mathbf{Z}}|M, K_B) - I(C; \mathbf{Y}|M, K_B) + \epsilon'' + \epsilon}
\end{aligned}
$$

Denoting the pair of random variables $(\mathbf{Y}, \mathbf{Z})$ as $\tilde{\mathbf{Z}}$

Commitment over REC-$[\gamma, \delta]$

Converse

$$nR = H(C)$$

$$= I(C;\tilde{\mathbf{Z}}|M,K_B) - I(C;\mathbf{Y}|M,K_B) + \epsilon'' + \epsilon$$

$$\implies \boxed{R \leq I(\mathbf{X};\tilde{\mathbf{Z}}) - I(\mathbf{X};\mathbf{Y}) + \frac{\epsilon''}{n} + \frac{\epsilon}{n}}$$

Using the result from seminal work [Csizar and Korner '78]
Followed by few non-trivial information-theoretic reductions

Commitment over REC-$[\gamma, \delta]$

Converse

$$
\begin{aligned}
nR &= H(C) \\
&= I(C;\tilde{\mathbf{Z}}|M,K_B) - I(C;\mathbf{Y}|M,K_B) + \epsilon'' + \epsilon
\end{aligned}
$$

$$
\implies R \leq I(\mathbf{X};\tilde{\mathbf{Z}}) - I(\mathbf{X};\mathbf{Y}) + \frac{\epsilon''}{n} + \frac{\epsilon}{n}
$$

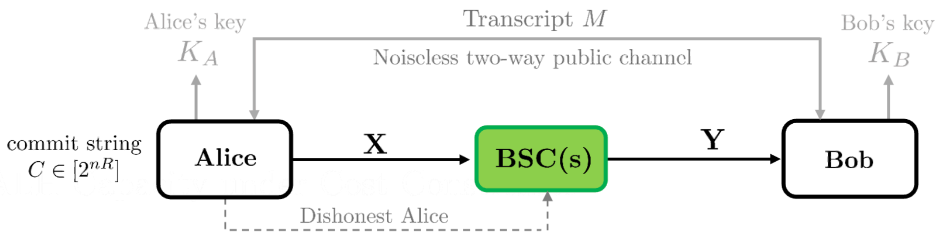
$$
\begin{aligned}
\implies \boxed{R \leq \min_{s\in[\gamma,\delta]} \Big[I(\mathbf{X};\tilde{\mathbf{Z}}) - I(\mathbf{X};\mathbf{Y}) \Big]} \\
\leq \max_{P_X} \min_{s\in[\gamma,\delta]} \Big[I(\mathbf{X};\tilde{\mathbf{Z}}) - I(\mathbf{X};\mathbf{Y}) \Big] \\
\leq H(\delta) - H(\theta)
\end{aligned}
$$

Because the inequality holds for *all* cheating behaviours of Alice, it must also hold for the minimum

Commitment over REC-$[\gamma, \delta]$

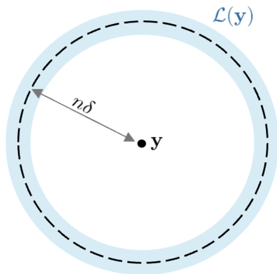
Achievability: Protocol: Commit phase

The Protocol



$\mathbf{X} \sim Ber(1/2)$ *i.i.d* $\qquad \mathbf{Y} \longrightarrow \mathcal{L}(\mathbf{y})$

$$\mathcal{L}(\mathbf{y}) = \left\{ \mathbf{x} \in \{0,1\}^n : d_H(\mathbf{x}, \mathbf{y}) \in [n(\delta - \epsilon), n(\delta + \epsilon)] \right\}$$



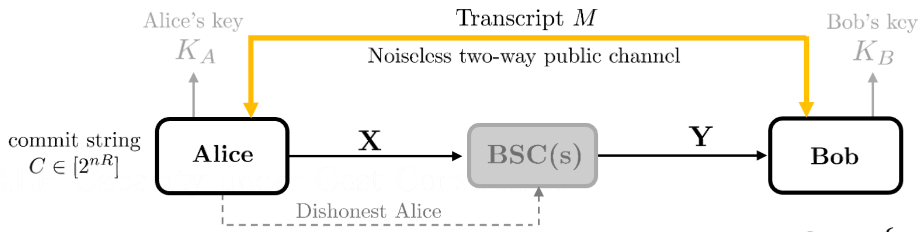
Time

Time

Commitment over REC-$[\gamma, \delta]$

Achievability: Protocol: Commit phase

The Protocol



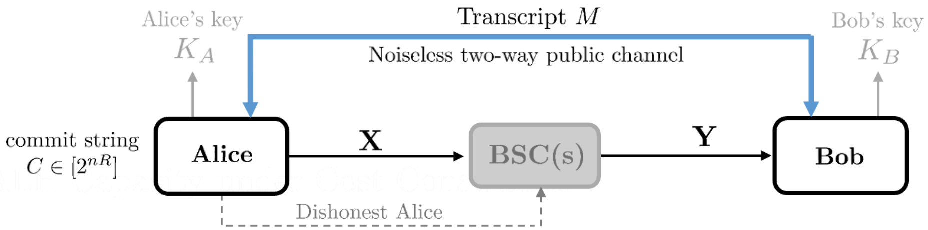
where $\kappa := \dfrac{\delta - \gamma}{1 - 2\gamma}$

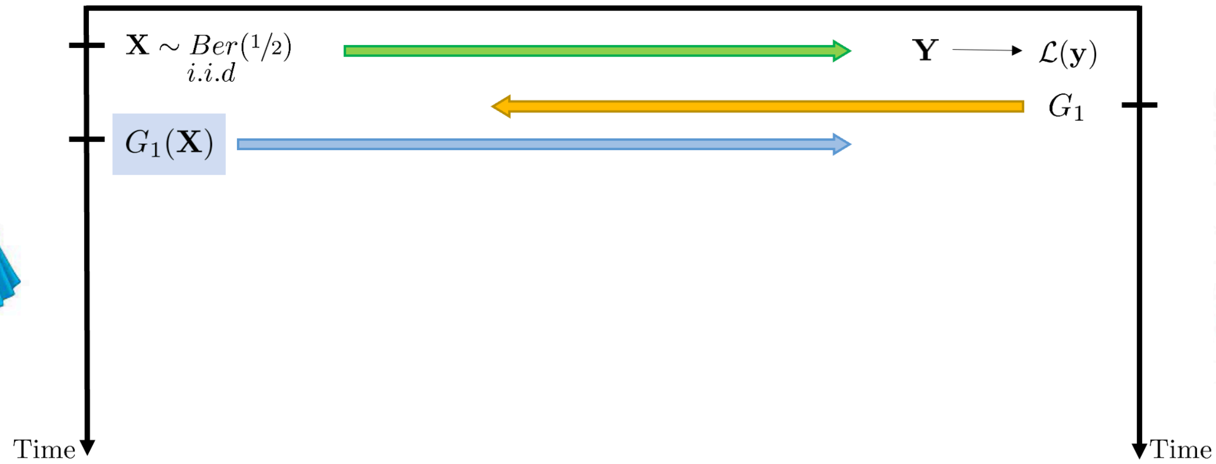
$$\mathcal{G}_1 := \left\{ g_1 : \{0,1\}^n \to \{0,1\}^{n(H(s)+\beta_1)} \right\}$$

Commitment over REC-$[\gamma, \delta]$

Achievability: Protocol: Commit phase

The Protocol

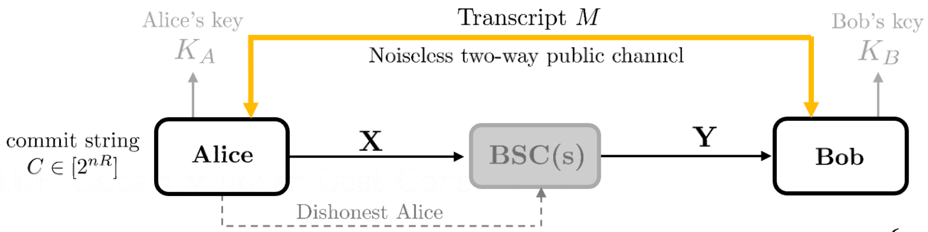




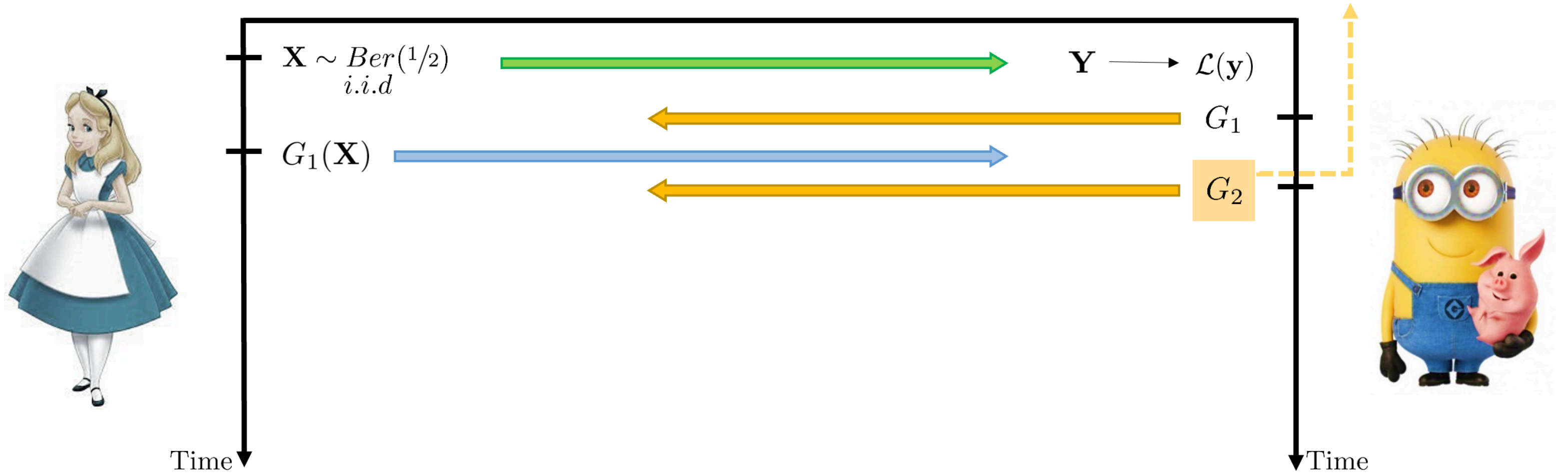
Commitment over REC-$[\gamma, \delta]$

Achievability: Protocol: Commit phase

The Protocol



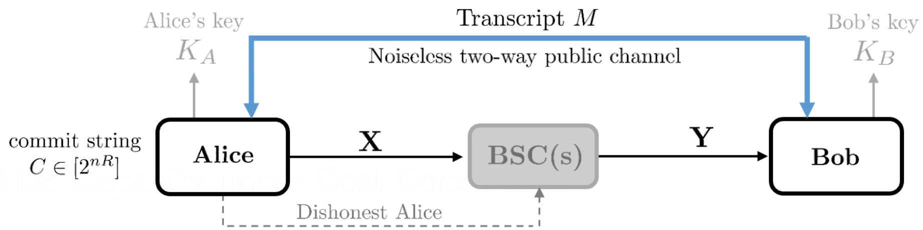
$\mathcal{G}_2 := \{g_2 : \{0,1\}^n \to \{0,1\}^{n\beta_2)}\}$

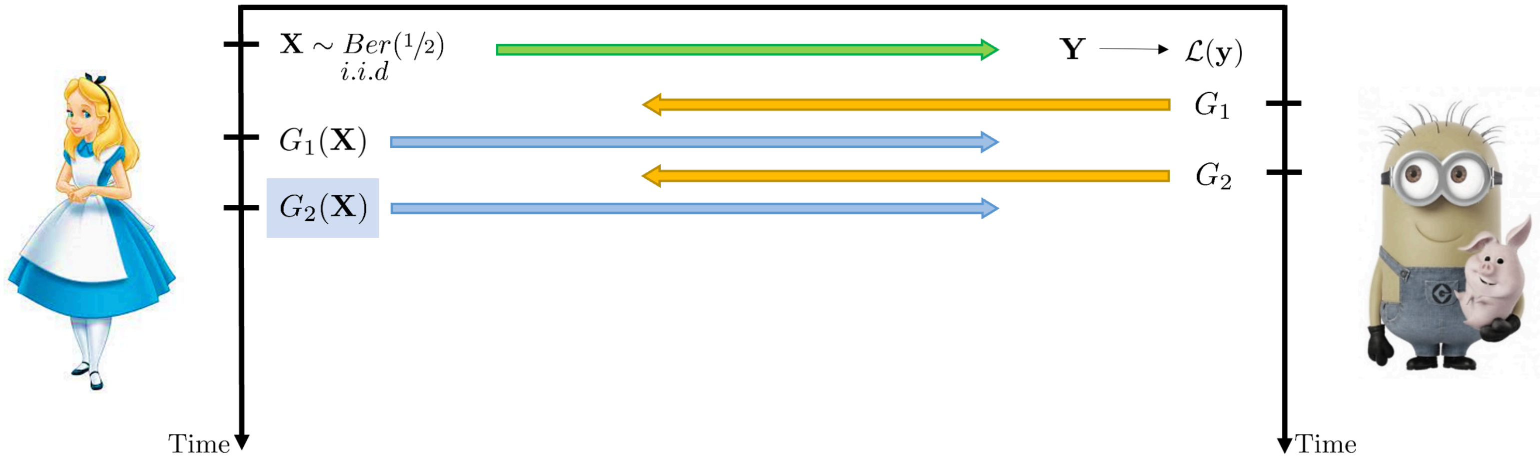


Commitment over REC-$[\gamma, \delta]$

Achievability: Protocol: Commit phase

The Protocol

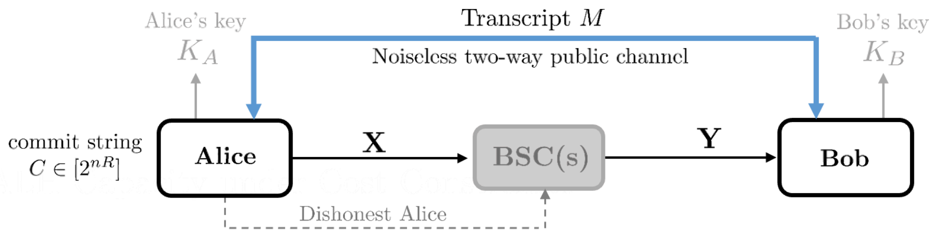


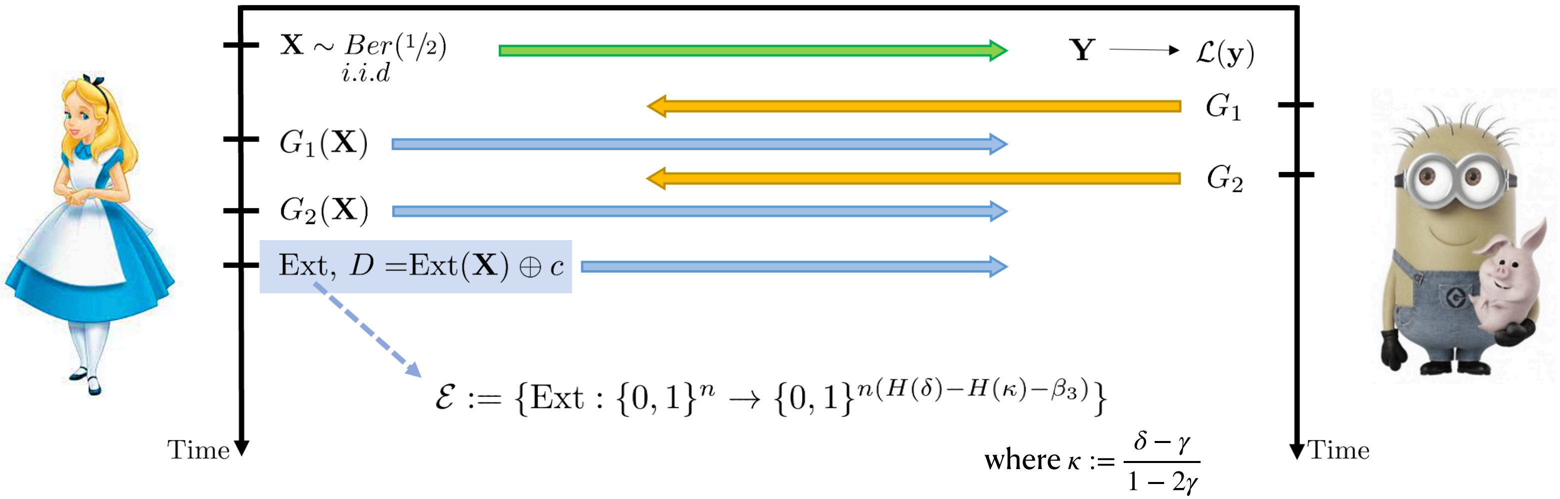


Commitment over REC-$[\gamma, \delta]$

Achievability: Protocol: Commit phase

The Protocol

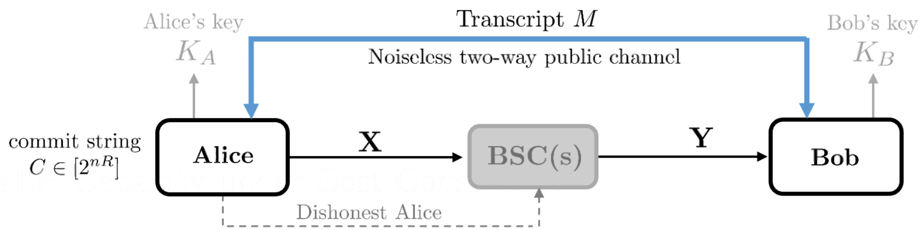


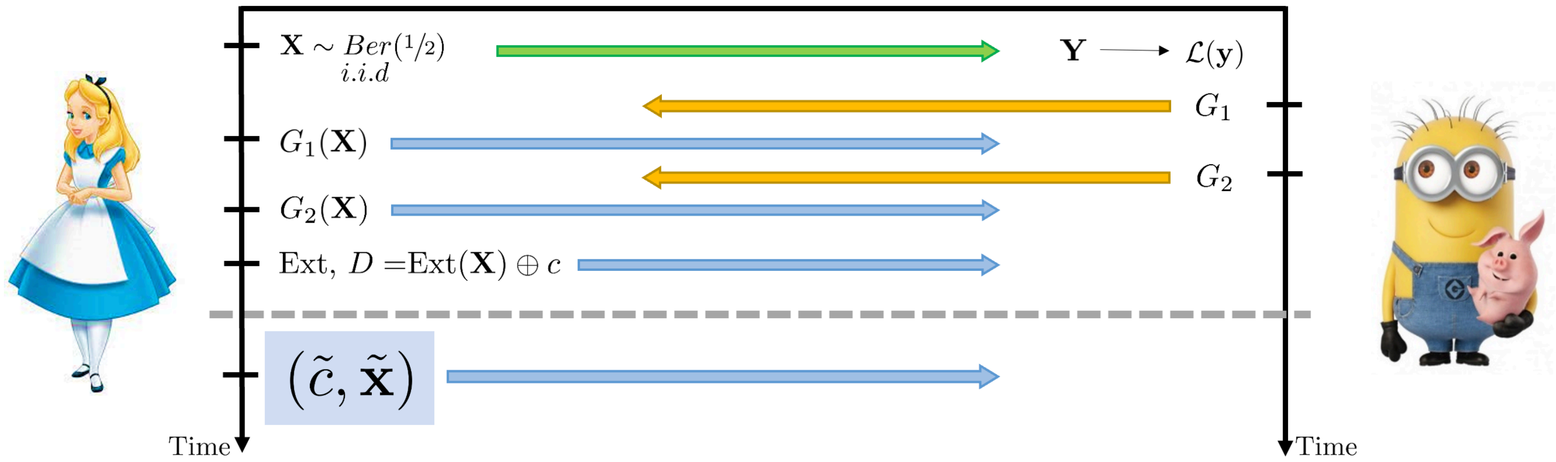


Commitment over REC-$[\gamma, \delta]$

Achievability: Protocol: Reveal phase

The Protocol

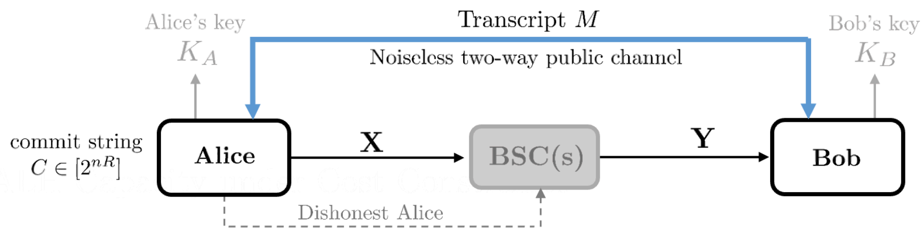


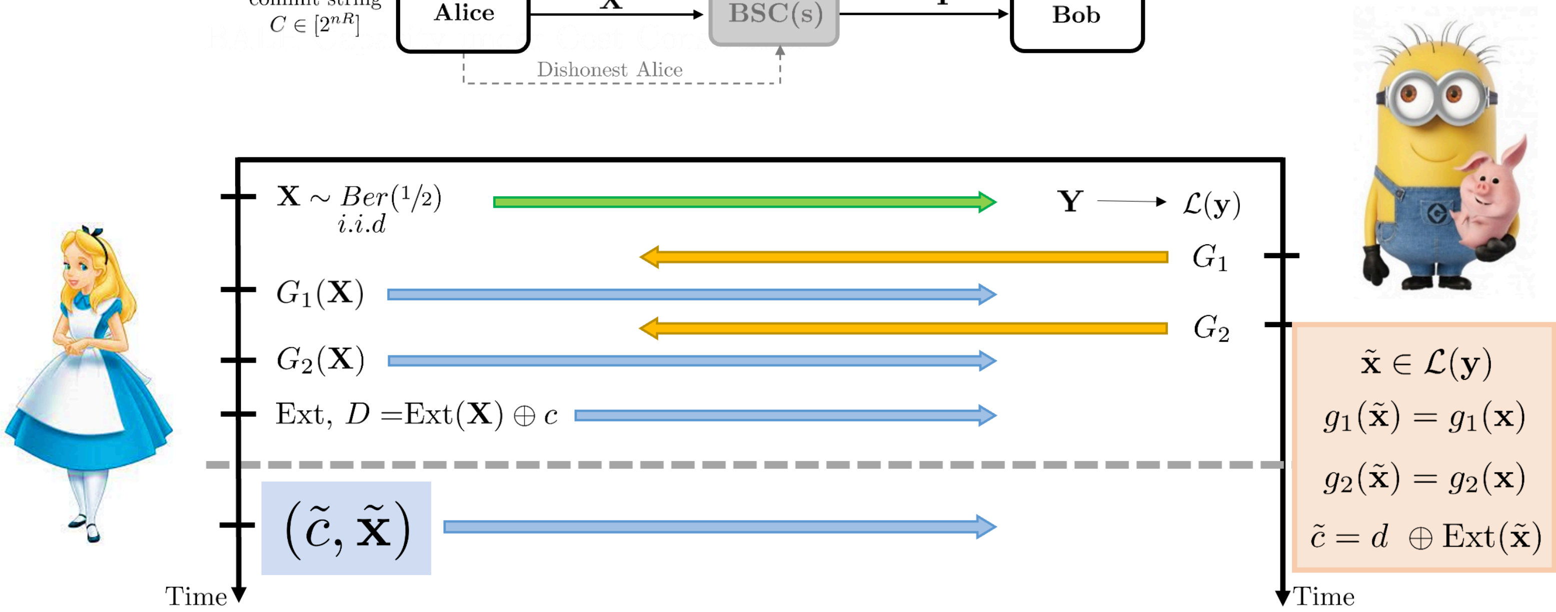


Commitment over REC-[γ, δ]

Achievability: Protocol: Reveal phase

The Protocol



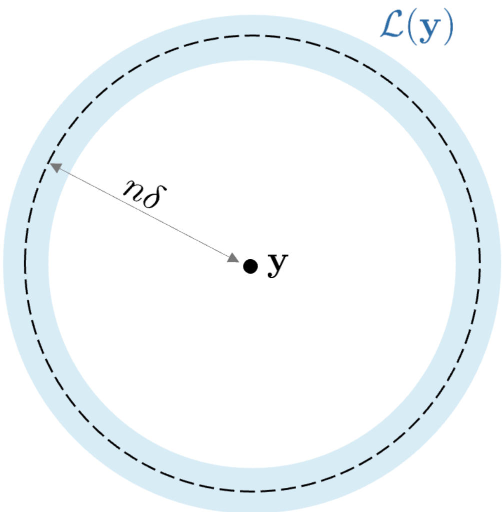


Commitment over REC-$[\gamma, \delta]$

Security Guarantees: $\epsilon-$soundness

Bob prepares a list

$$\mathcal{L}(\mathbf{y}) = \Big\{\mathbf{x} \in \{0,1\}^n : d_H(\mathbf{x},\mathbf{y}) \in [n(\delta-\epsilon), n(\delta+\epsilon)]\Big\}$$



Protocol is sound if $\mathbf{X} \in \mathcal{L}(\mathbf{y})$ with high probability

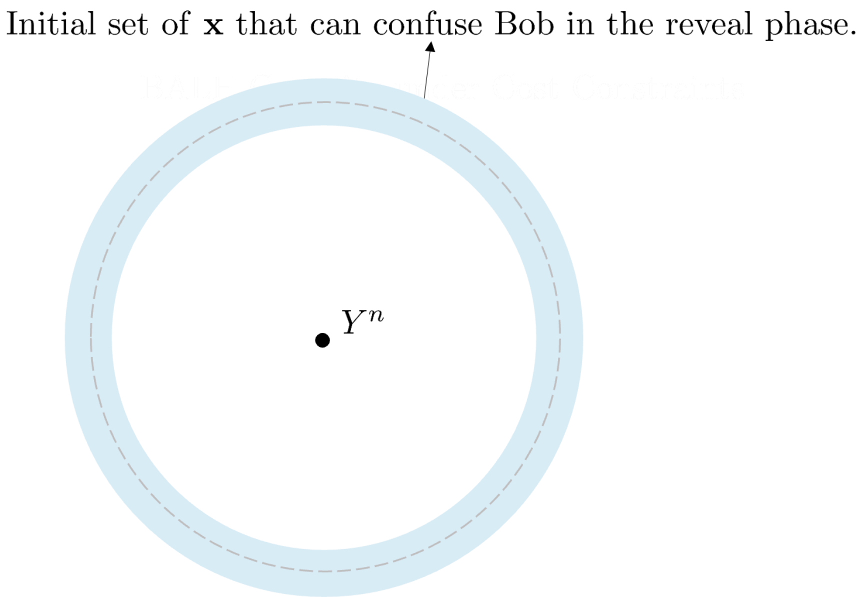
Using the Chernoff Bound, and the fact that $\mathbf{X}$ and $\mathbf{Y}$ are connected via a BSC(δ), we can show:

$$\boxed{P\big(\mathbf{X} \notin \mathcal{L}(\mathbf{y})\big) \leq \epsilon'(n)}$$

$\epsilon'(n) \to 0$ as $n \to \infty$

Commitment over REC-$[\gamma, \delta]$

Security Guarantees: $\epsilon-$bindingness

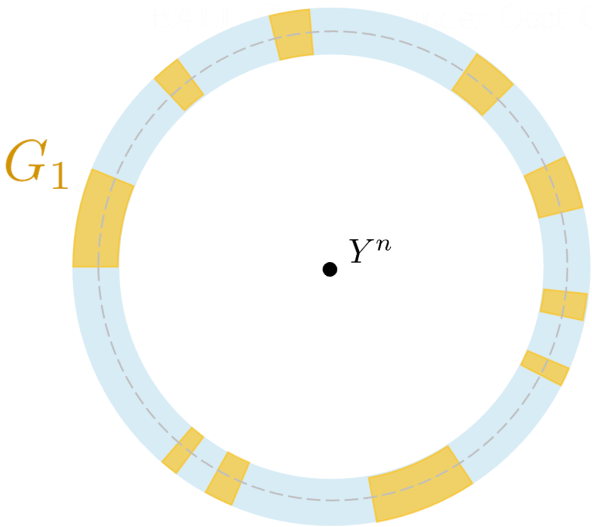


Exponential (in n)

Commitment over REC-[γ, δ]

Security Guarantees: $\epsilon-$bindingness

Alice sends $G_1(X)$



Exponential (in n)

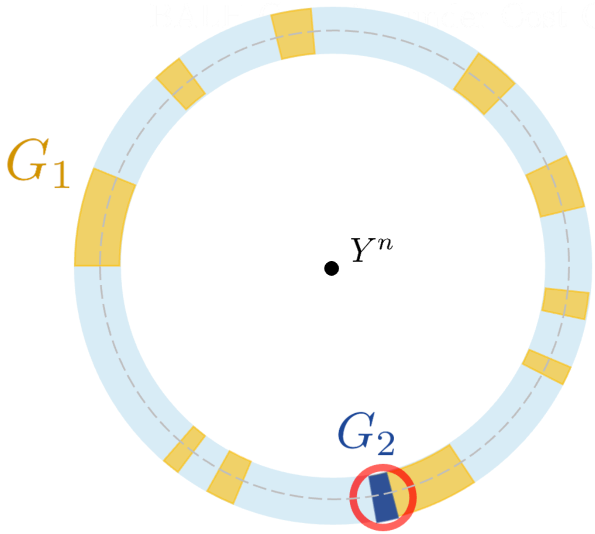
$\Big\downarrow G_1$

Polynomial (in n)

Commitment over REC-$[\gamma, \delta]$

Security Guarantees: $\epsilon-$bindingness

Alice sends $G_2(X)$



The *one* remaining $\mathbf{x}$ Alice can use.

Exponential (in n)

$\Big\downarrow G_1$

Polynomial (in n)

$\Big\downarrow G_2$

Unique

Two rounds of hash challenges bind Alice to a single $\mathbf{x}$

Commitment over REC-$[\gamma, \delta]$

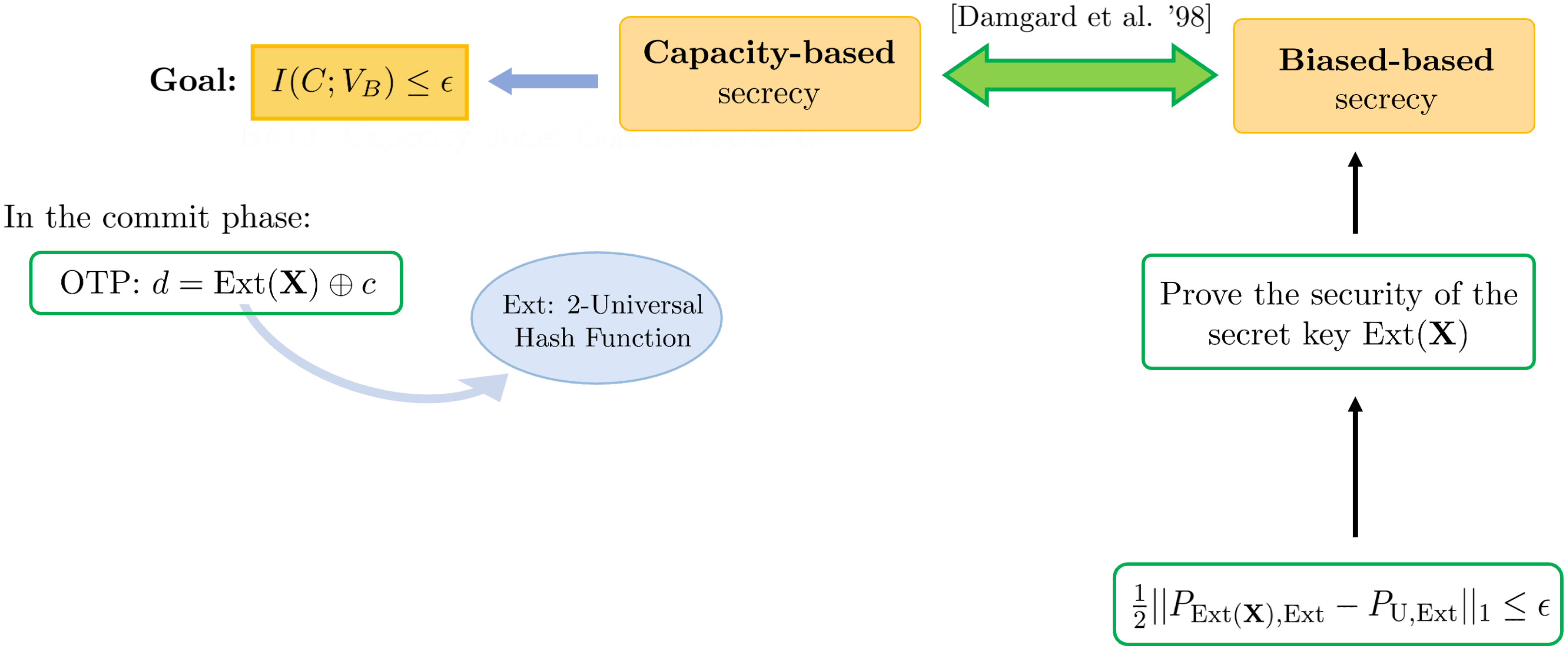
Security Guarantees: $\epsilon-$concealment

Goal: $I(C; V_B) \leq \epsilon$ ← **Capacity-based** secrecy ⟷ **Biased-based** secrecy

[Damgard et al. '98]

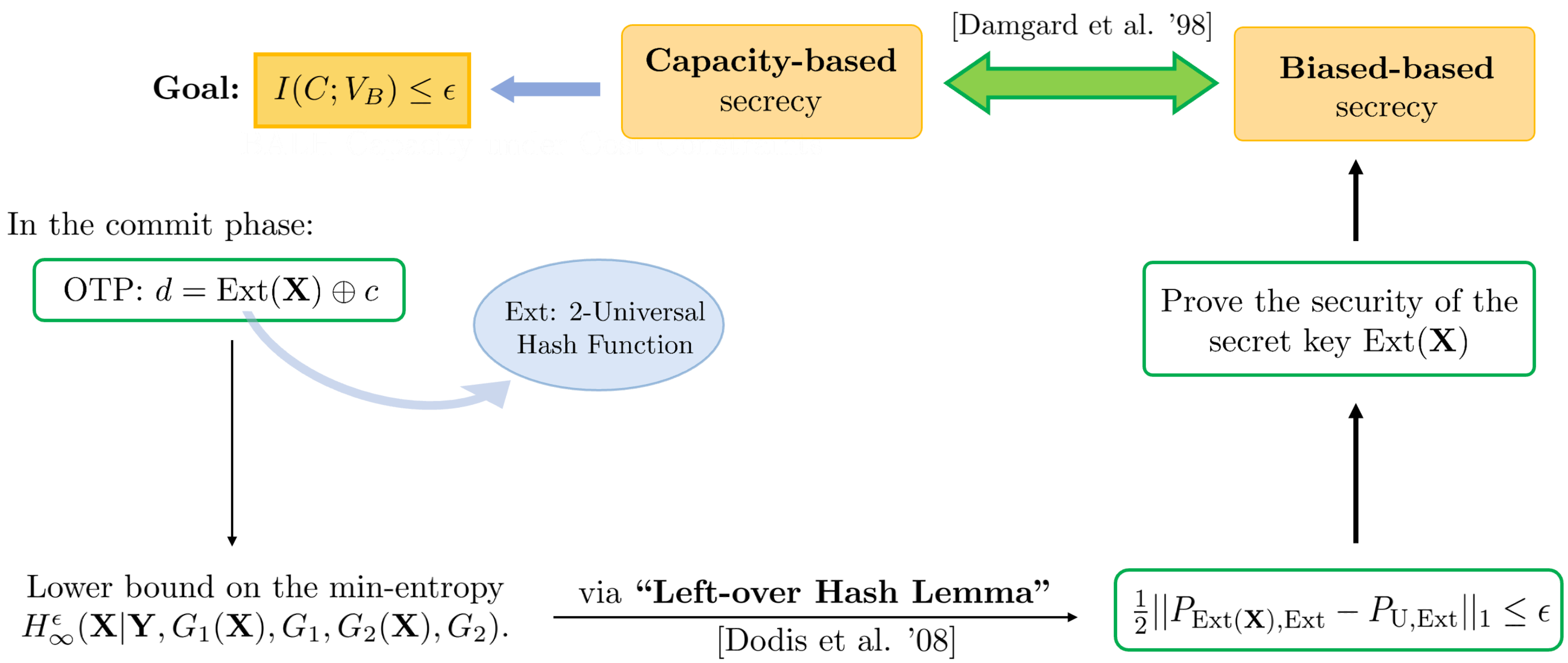
Commitment over REC-$[\gamma, \delta]$

Security Guarantees: $\epsilon-$concealment



Commitment over REC-$[\gamma, \delta]$

Security Guarantees: $\epsilon-$concealment



Commitment over Noisy Channels

Other Interesting Results:

- Commitment Capacity of AWGN channels is "Infinite". **[Nascimento et.al (Trans. IT '08)]**

- UNC version of Gaussian Channels may have finite capacity. It has zero commitment capacity if $\delta^2 \geq 2\gamma^2$, even under infinite input power. and other results.. **[BJMY (ISIT '23)]**

- Bit commitment over Multiple-access channels. **[Chou and Bloch (Allerton '22)]**