Commitment Capacity under Cost Constraints

Anuj Kumar Yadav
IIT Patna

Joint work with:

Manideep Mamindlapally
IIT Kharagpur

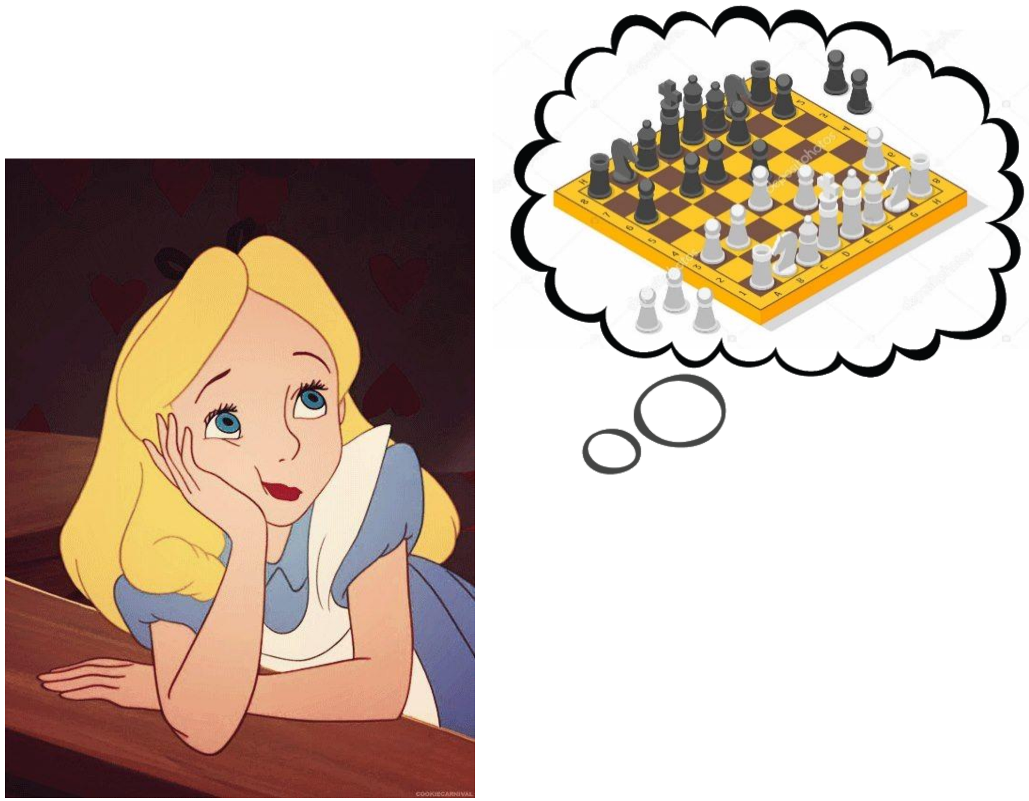
Manoj Mishra
NISER, HBNI

Amitalok J. Budkuley
IIT Kharagpur

Laboratoire ETIS
CY Cergy Paris Université, ENSEA, CNRS
France

The Problem

Alice's turn, but its bed time



Alice can think about her next move for the whole night

A Solution - Trusted Third Party

That night:

Alice **"commits"** move to Mom.

Guarantee: the move is **concealed** from Bob

The next morning:

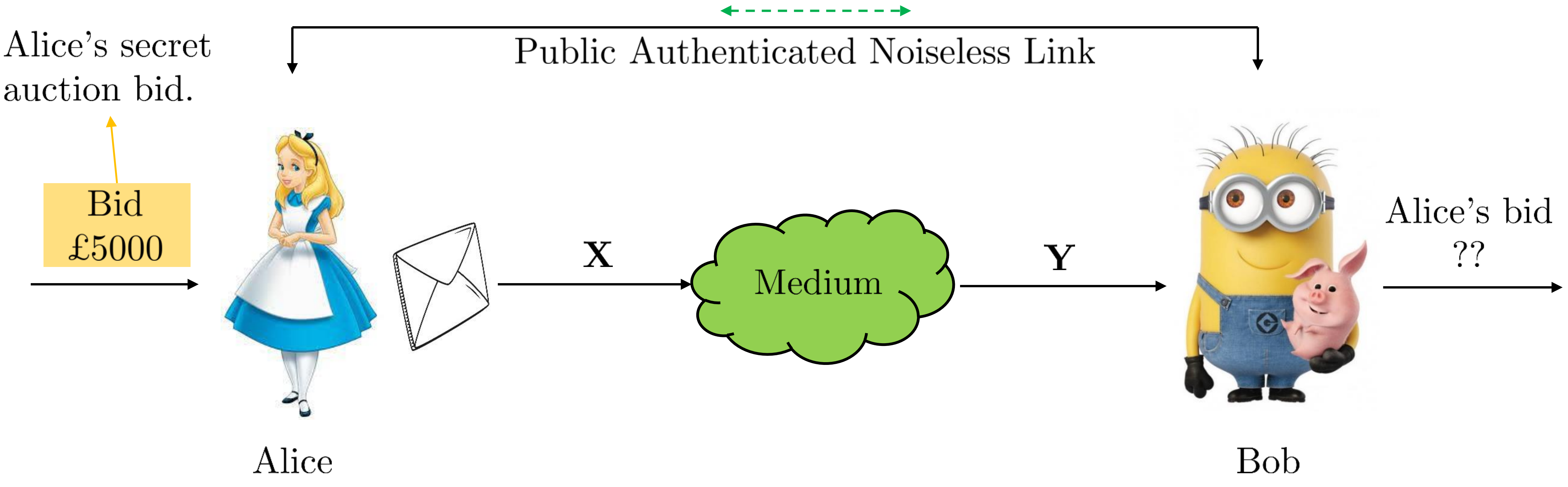
The move is **"revealed"** to Bob.

Guarantee: Alice is **bound** to her initial choice

What if there is no **Trusted Third Party**?

The Commit Phase

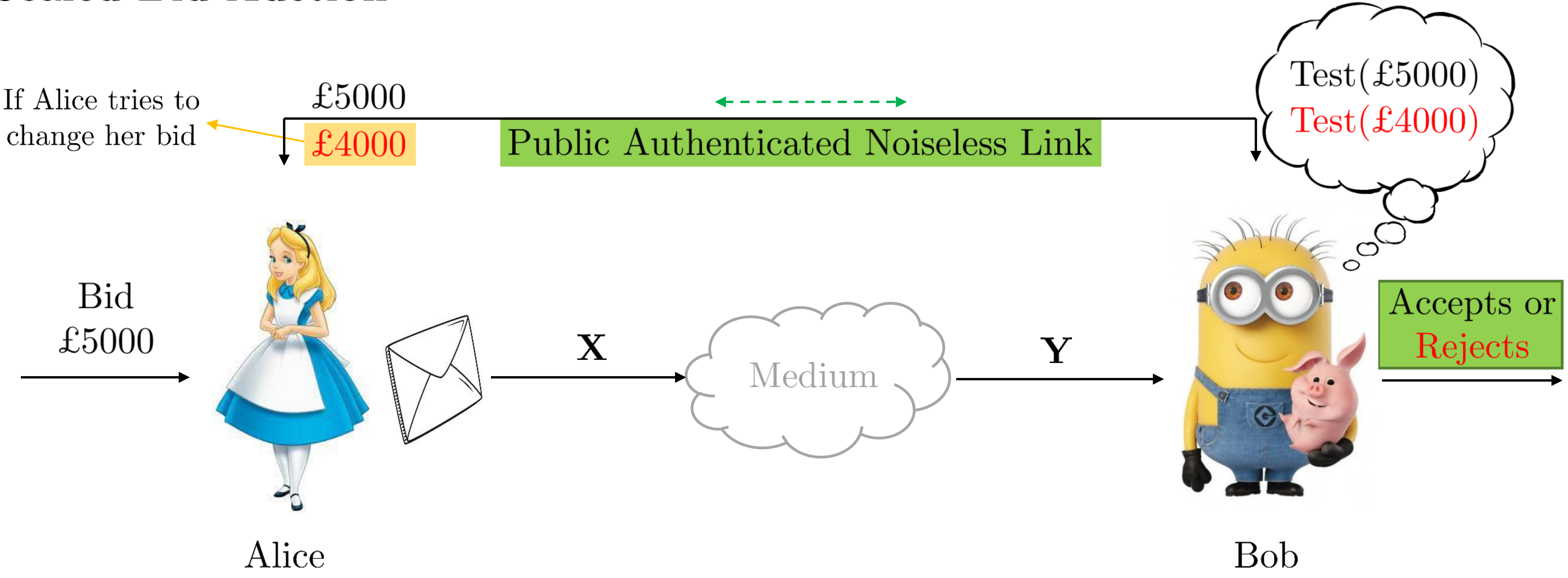
Sealed Bid Auction



Alice "commits" her message to Bob without him knowing what it is.

The Reveal Phase

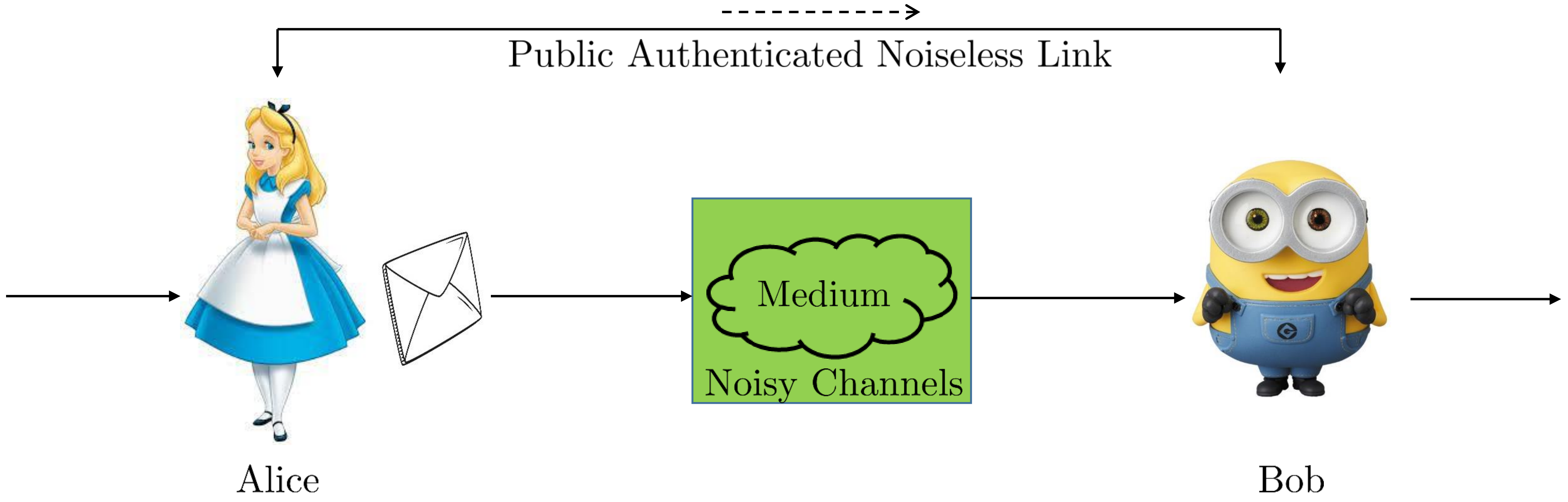
Sealed Bid Auction



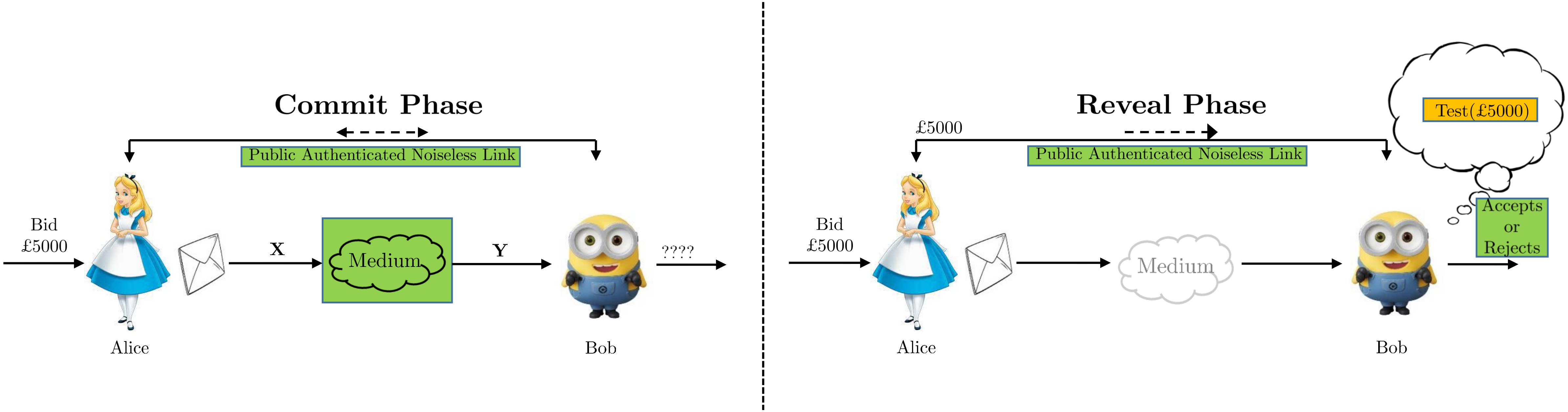
Alice “reveals” her choice to Bob and he decides whether or not she is being truthful

"Commitment" via Sealed bid Auction Example

- Introduced by [Blum '83] parties are computationally bounded i.e., *conditionally* secure.
- Commitment based on noisy channels can be *unconditionally* or *information-theoretically* secure [Crepéau-Kilian '88].
- Two phases viz., **Commit Phase** followed by **Reveal Phase**.



Commitment

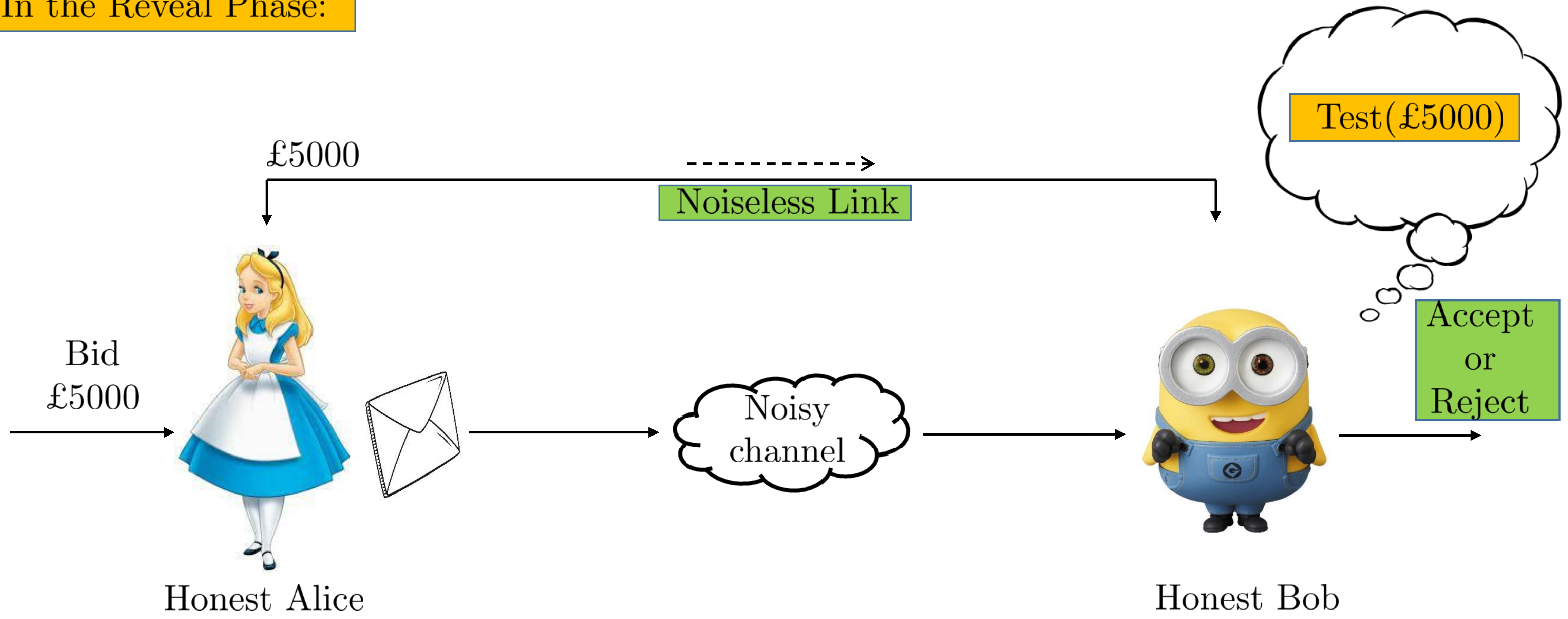


A good commitment protocol aims to be

- *sound*: when both Alice and Bob *honestly* follow the protocol
- *concealing*: when Alice *honestly* follows the protocol but a dishonest Bob may deviate
- *binding*: when Bob honestly follows the protocol but a *dishonest* Alice may deviate

Soundness

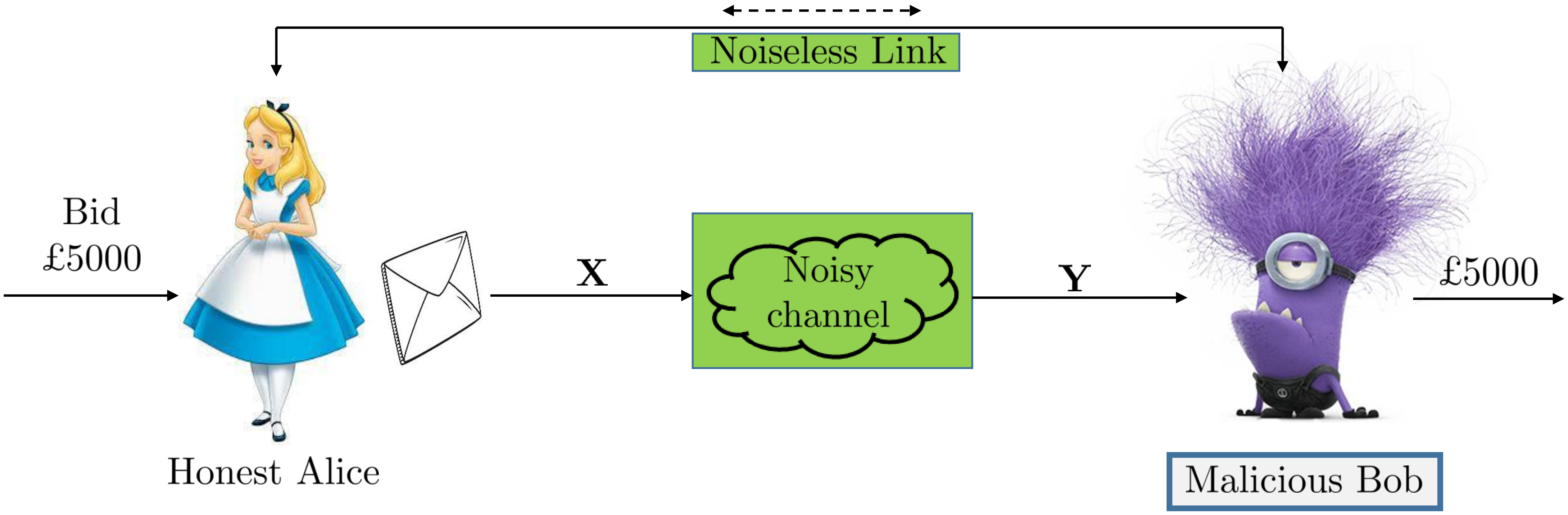
In the Reveal Phase:



Bob's Test always passes!

Concealment

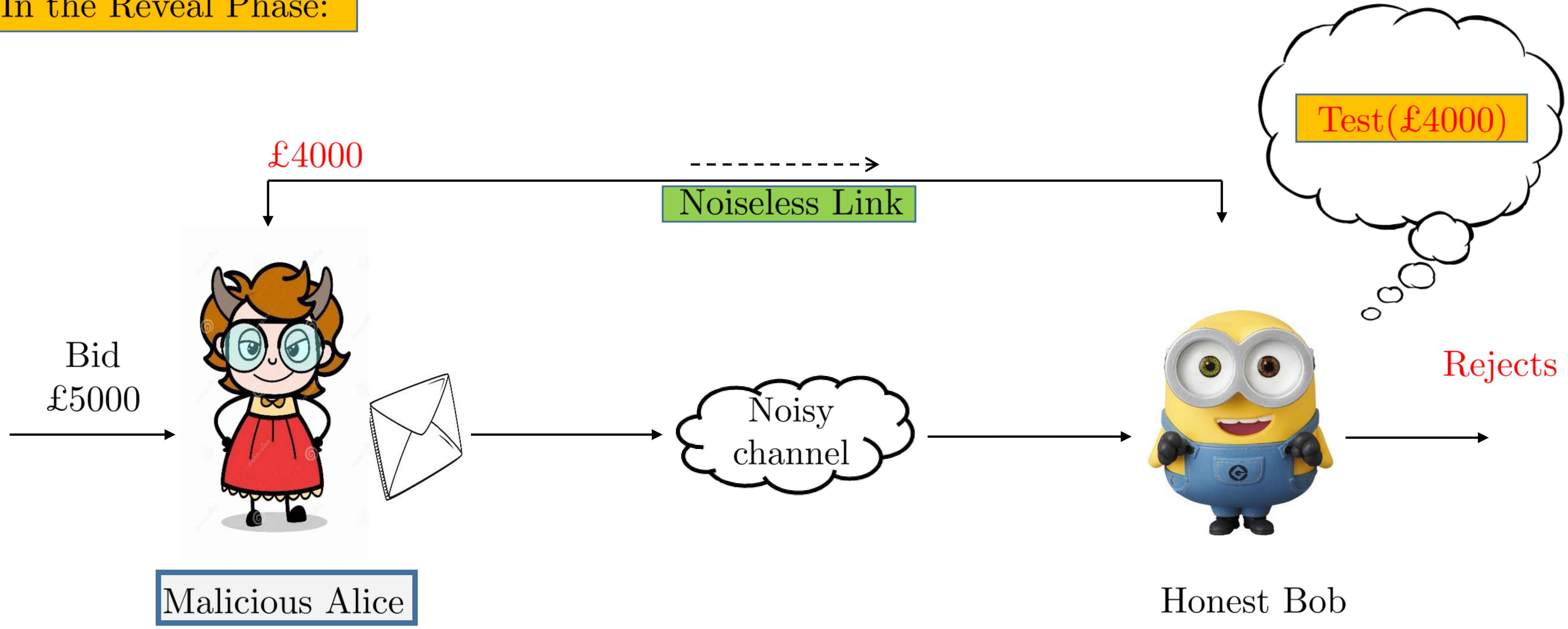
At the end of commit phase:



Malicious Bob can not learn Alice's Bid!

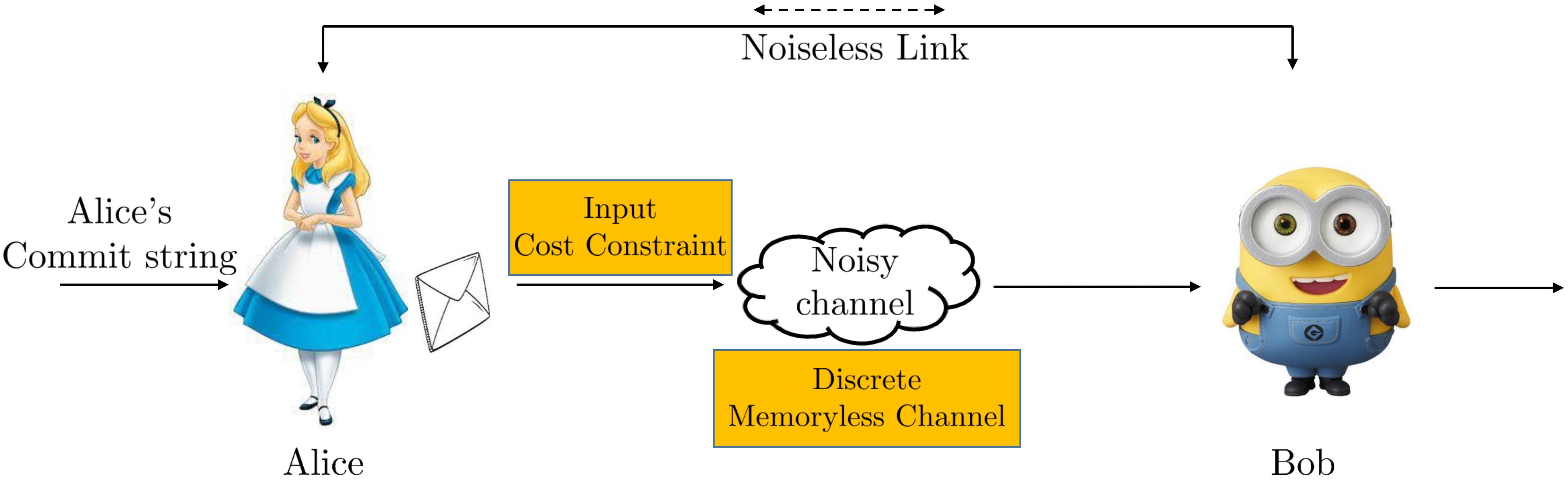
Bindingness

In the Reveal Phase:



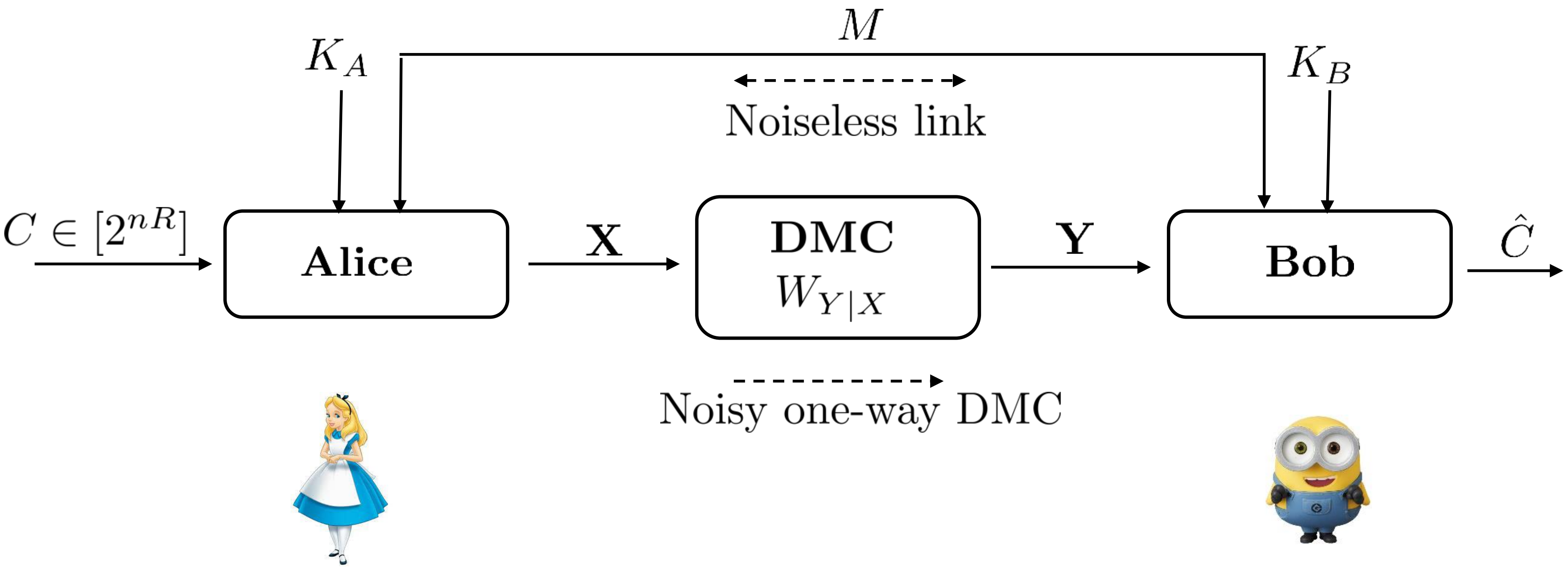
Bob's Test rejects dishonest Alice's cheating string

Commitment Capacity: DMCs with *constrained inputs*

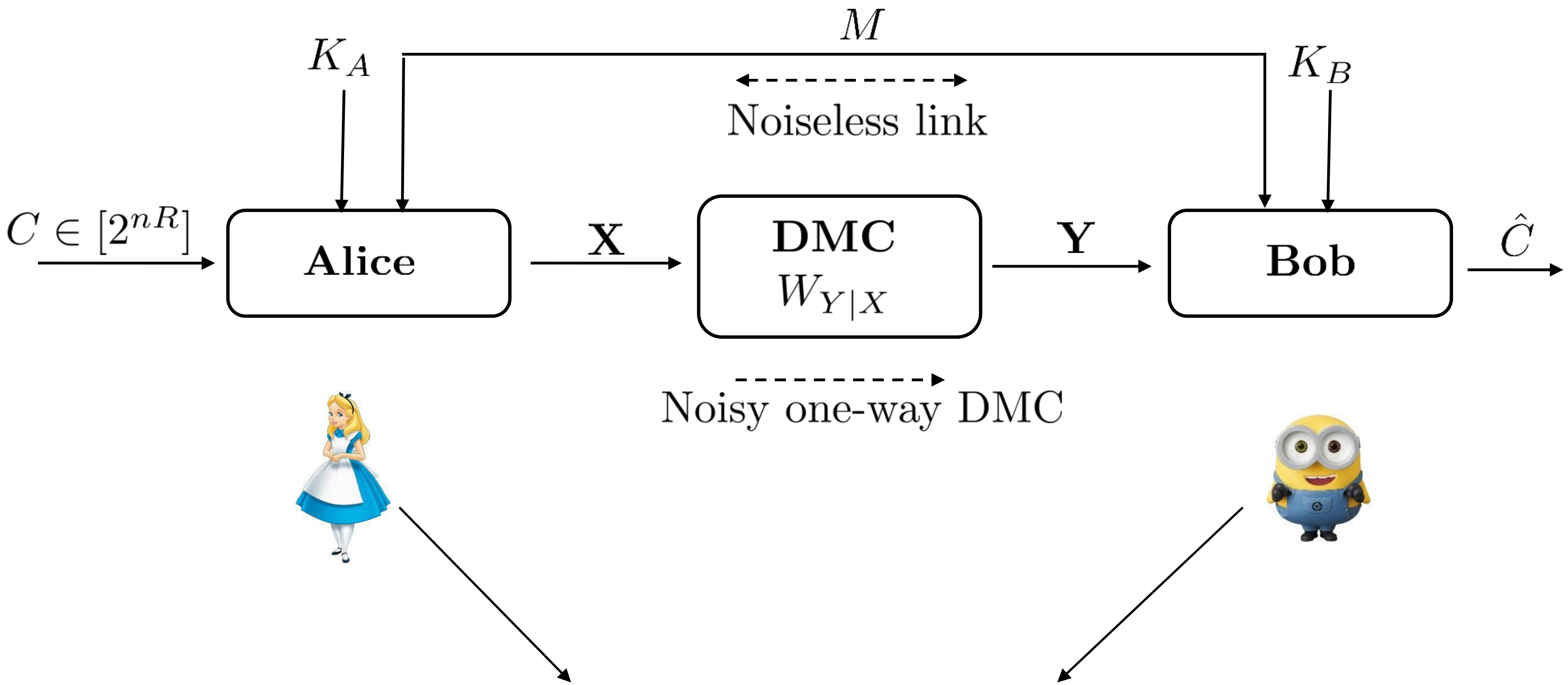


Goal: To characterize <u>Commitment Capacity</u> for cost constrained DMCs.

Problem Setup



Problem Setup

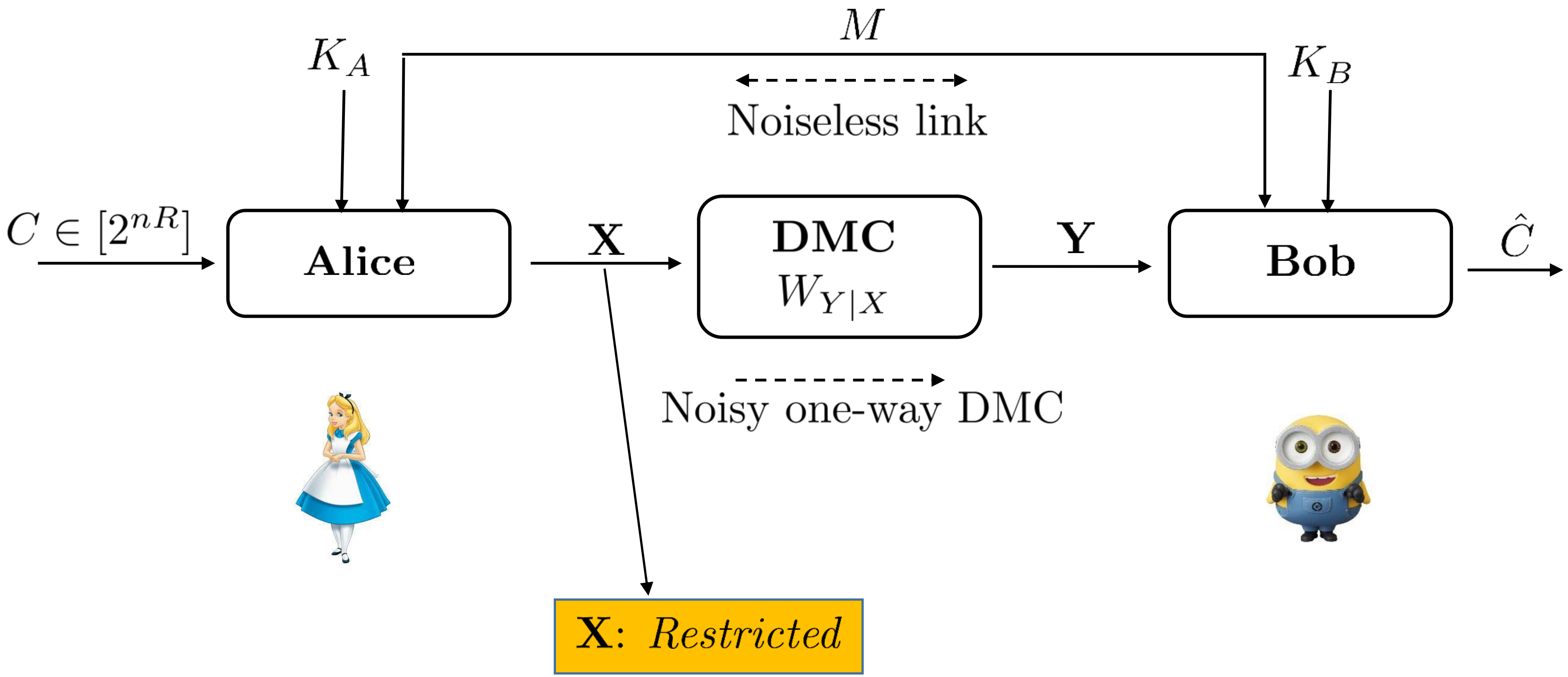


‘Alice’s view’ $V_A = (C, \mathbf{X}, K_A, M)$

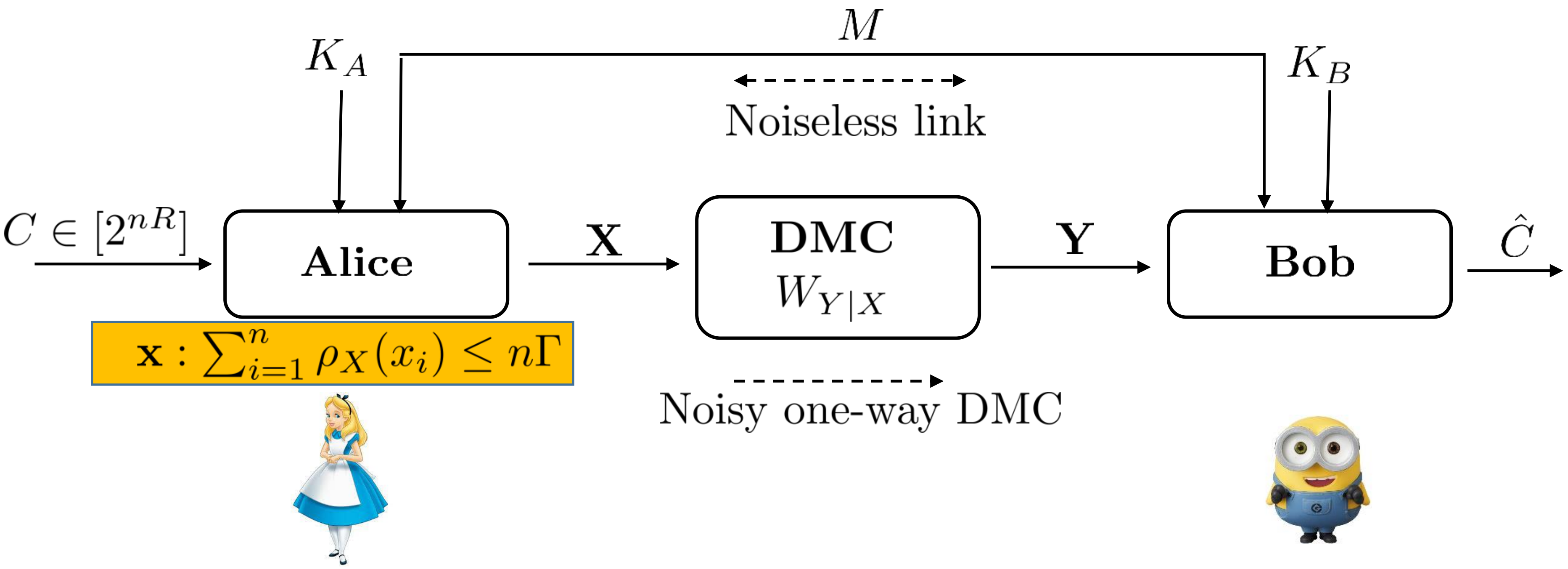
‘Bob’s view’ $V_B = (\mathbf{Y}, K_B, M)$

**View: collection at the *end of commit phase*

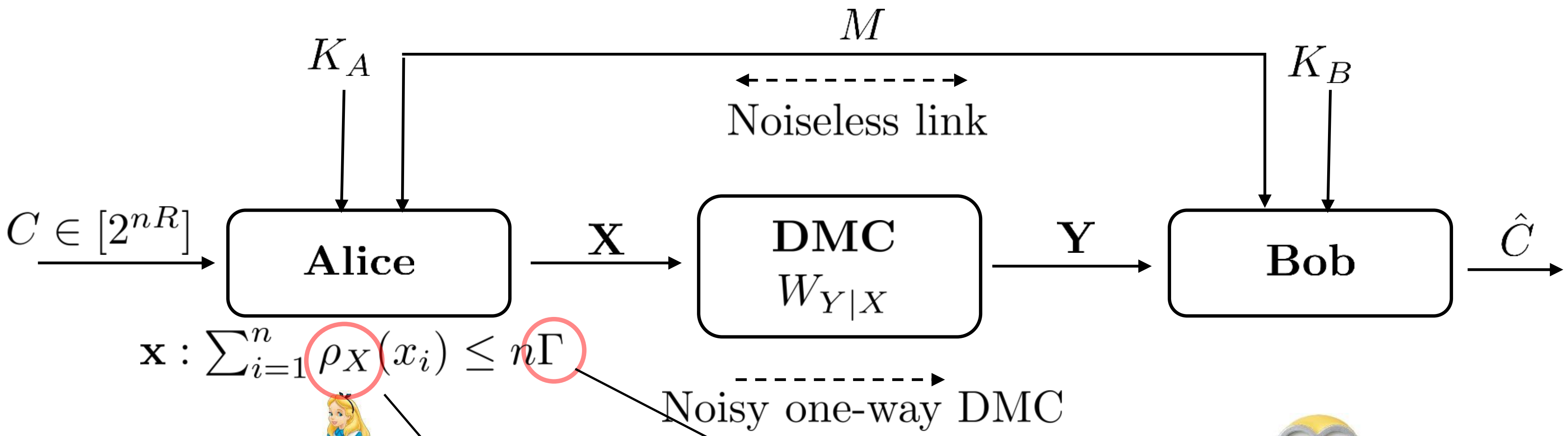
Problem Setup



Problem Setup



Problem Setup



$\mathbf{x} : \sum_{i=1}^{n} \rho_X(x_i) \leq n\Gamma$

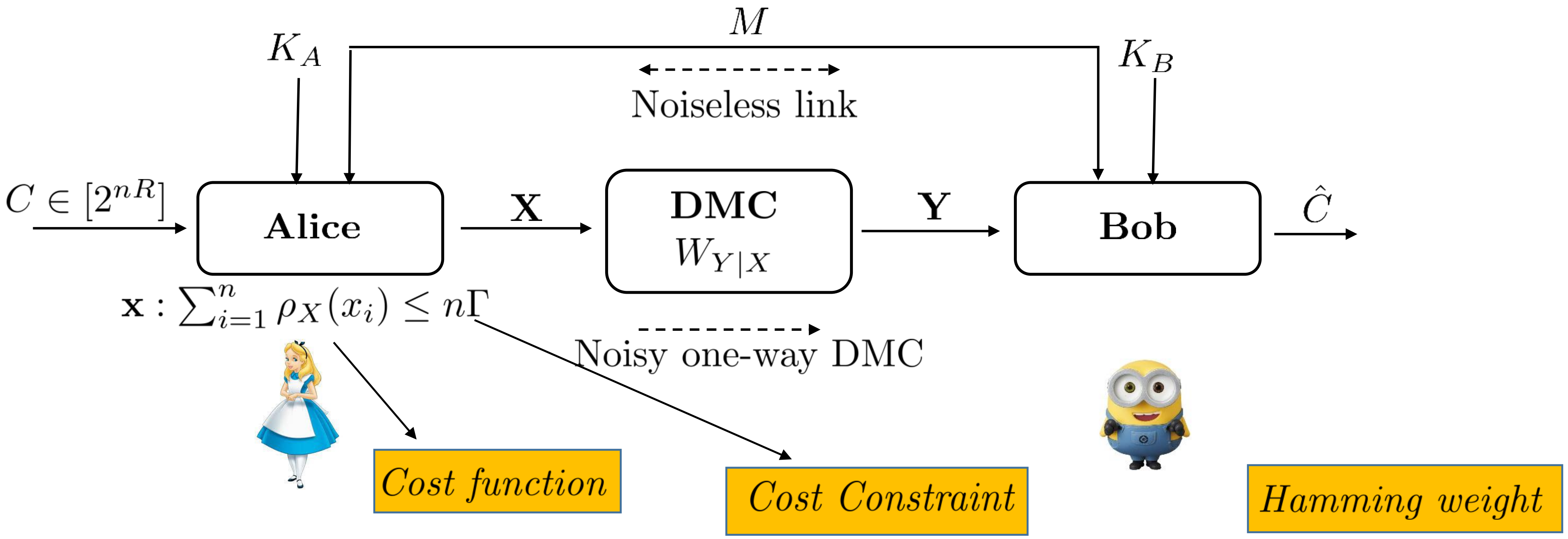
Cost function

$\rho_X : \mathcal{X} \to \mathbb{R}^+$

Cost Constraint

$\mathcal{S}(\Gamma) := \{\mathbf{x} : \sum_{i=1}^{n} \rho_X(x_i) \leq n\Gamma\}$

Problem Setup



Example: Let $\mathbf{x}$ be a bit string over binary space $\mathcal{X}^n = \{0,1\}^n$.

$$\rho_X(0) = 0$$

$$\rho_X(1) = 1$$

$$\xrightarrow[\textit{weight constraint}]{\Gamma}$$

$$\boxed{wt_H(\mathbf{x}) \leq n\Gamma}$$

Security guarantees

Let $\epsilon > 0$. Let $\mathcal{P}$ be a commitment protocol

ϵ-**sound**: When *both* Alice and Bob are honestly executing the protocol:

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

ϵ-**concealing**: For an honest Alice and under *any* dishonest strategy of Bob,

$$\boxed{I(C; V_B) \leq \epsilon}$$

ϵ-**binding**: For an honest Bob and under *any* dishonest strategy of Alice,

$$\mathbb{P}\left(T(\bar{c}, \bar{\mathbf{X}}, V_B) = ACCEPT \quad \& \quad T(\hat{c}, \hat{\mathbf{X}}, V_B) = ACCEPT\right) \leq \epsilon$$

$$\forall (\bar{c}, \bar{\mathbf{X}}), (\hat{c}, \hat{\mathbf{X}}) \ : \ \bar{c} \neq \hat{c}$$

Security guarantees

Let $\epsilon > 0$. Let $\mathcal{P}$ be a commitment protocol

ϵ-**sound**: When *both* Alice and Bob are honestly executing the protocol:

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

ϵ-**concealing**: For an honest Alice and under *any* dishonest strategy of Bob,

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

ϵ-**binding**: For an honest Bob and under *any* dishonest strategy of Alice,

$$\mathbb{P}\left(T(\bar{c}, \bar{\mathbf{X}}, V_B) = ACCEPT \quad \& \quad T(\hat{c}, \hat{\mathbf{X}}, V_B) = ACCEPT\right) \leq \epsilon$$

$$\forall (\bar{c}, \bar{\mathbf{X}}), (\hat{c}, \hat{\mathbf{X}}) \ : \ \bar{c} \neq \hat{c}$$

Rate $R > 0$ is "achievable" 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.

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

Main Results: Commitment Capacity for cost constraints

(ρ_X, Γ)-**non-redundant** DMCs

Primal Expression

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

- Generalisation of the result by [Winter *et. al*, '03] for general $\rho_X : \mathcal{X} \to \mathbb{R}^+$ function
- With stronger achievability : *stronger semantic security (concealment)*
- With stronger converse : *weaker average error condition*

Dual Expression

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

- Inspired by 'convex envelope of lines' approach [Csisźar-Korner '83]
- Computational aspect
- Unique optimising output distribution Q_Y

Main Results: Commitment Capacity for cost constraints

(ρ_X, Γ)-**non-redundant** DMCs

Primal Expression

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

- Generalisation of the result by [Winter *et. al*, '03] for general $\rho_X : \mathcal{X} \to \mathbb{R}^+$ function
- With stronger achievability : *stronger semantic security (concealment)*
- With stronger converse : *weaker average error condition*

Dual Expression

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

- Inspired by 'convex envelope of lines' approach [Csisźar-Korner '83]
- Computational aspect
- Unique optimising output distribution Q_Y

$P_1^* \neq P_2^*$

$P_1^* \to \boxed{\text{DMC } W_{Y|X}} \to Q_1^*$

$P_2^* \to \boxed{\text{DMC } W_{Y|X}} \to Q_2^*$

$Q_1^* = Q_2^*$

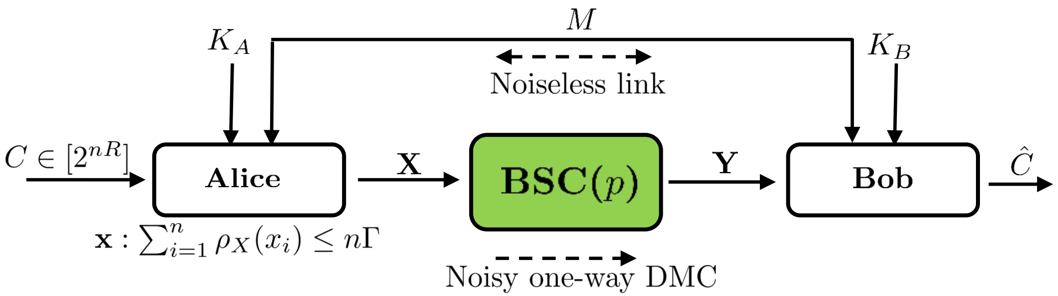
Main Results: Commitment Capacity for a cost constrained BSC example

$BSC(p)$ channel
Hamming weight cost function

Let $\mathbf{x}$ be a bit string over binary space $\mathcal{X}^n = \{0,1\}^n$.

$\rho_X(0) = 0$ $\qquad \xrightarrow[\textit{weight constraint}]{\Gamma} \qquad$ $wt_H(\mathbf{x}) \leq n\Gamma$ $\qquad \Gamma \in \mathbb{R}^+$

$\rho_X(1) = 1$



$$\boxed{\mathbb{C}(\Gamma) = H_2(p) + H_2(\Gamma) - H_2(p \circledast \Gamma)}$$

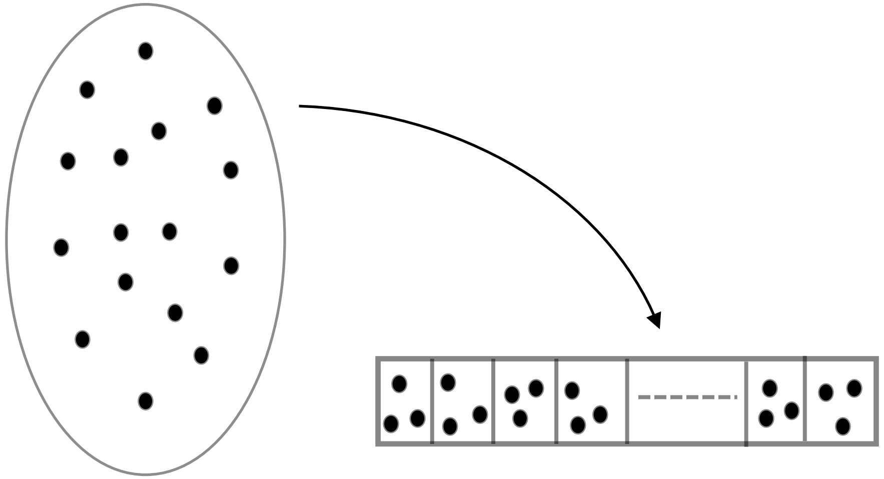
Achievability: Codebook Construction

- Uses the *random binning codebook* [Wyner '75, Winter *et al.* '03]
- Employs a stochastic encoding strategy by Alice

Binned codebook construction

For an $\varepsilon > 0$, fix:

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Binning Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$



$\mathcal{T}_\delta^{(n)}(P_X) \subseteq \mathcal{X}^n$

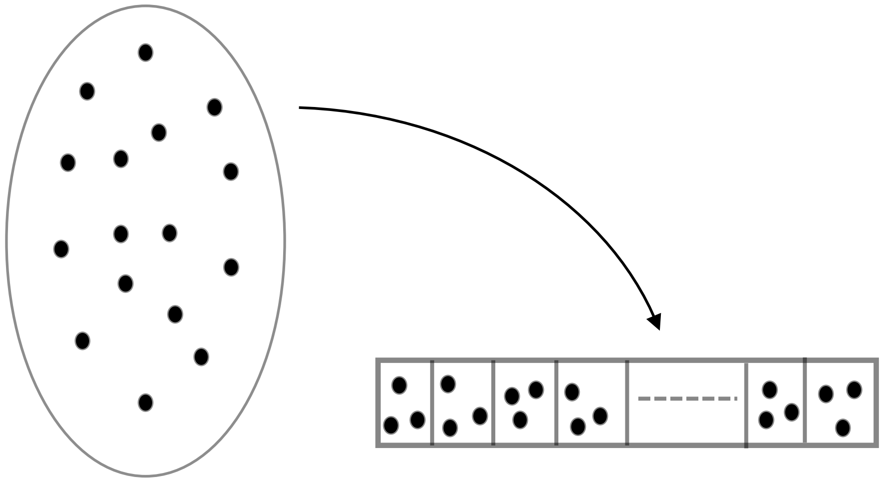
Achievability: Codebook Construction

- Uses the *random binning codebook* [Wyner '75, Winter *et al.* '03]
- Employs a stochastic encoding strategy by Alice

Binned codebook construction

For an $\varepsilon > 0$, fix:

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Binning Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$



$\mathcal{T}_\delta^{(n)}(P_X) \subseteq \mathcal{X}^n$

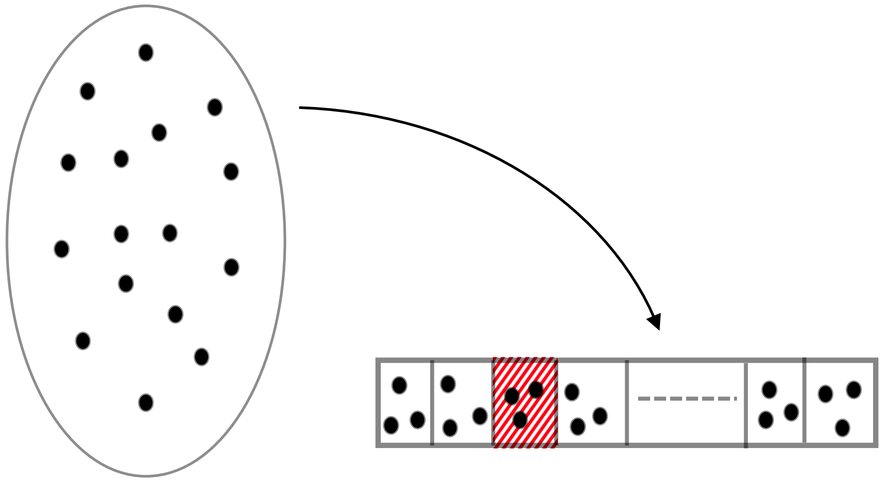
Achievability: Codebook Construction

- Uses the *random binning codebook* [Wyner '75, Winter *et al.* '03]
- Employs a stochastic encoding strategy by Alice

Binned codebook construction

For an $\varepsilon > 0$, fix:

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Binning Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$



$\mathcal{T}_\delta^{(n)}(P_X) \subseteq \mathcal{X}^n$

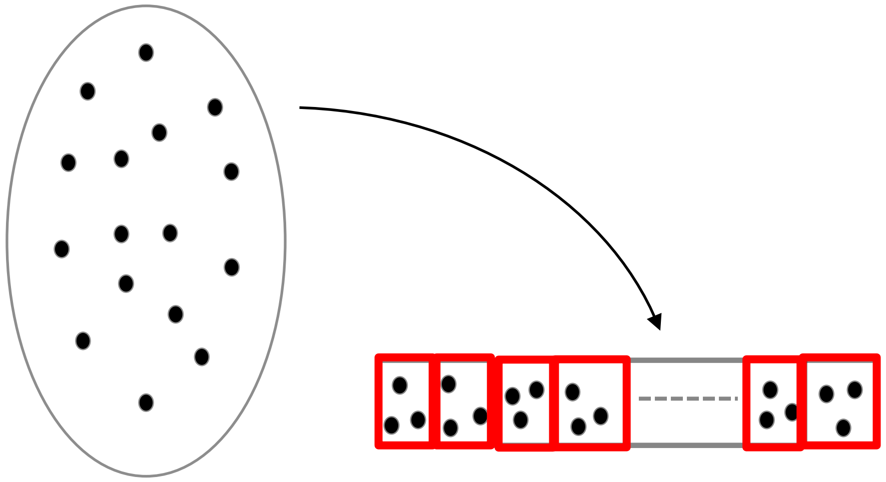
Achievability: Codebook Construction

- Uses the *random binning codebook* [Wyner '75, Winter *et al.* '03]
- Employs a stochastic encoding strategy by Alice

Binned codebook construction

For an $\varepsilon > 0$, fix:

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Binning Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$



$\mathcal{T}_\delta^{(n)}(P_X) \subseteq \mathcal{X}^n$

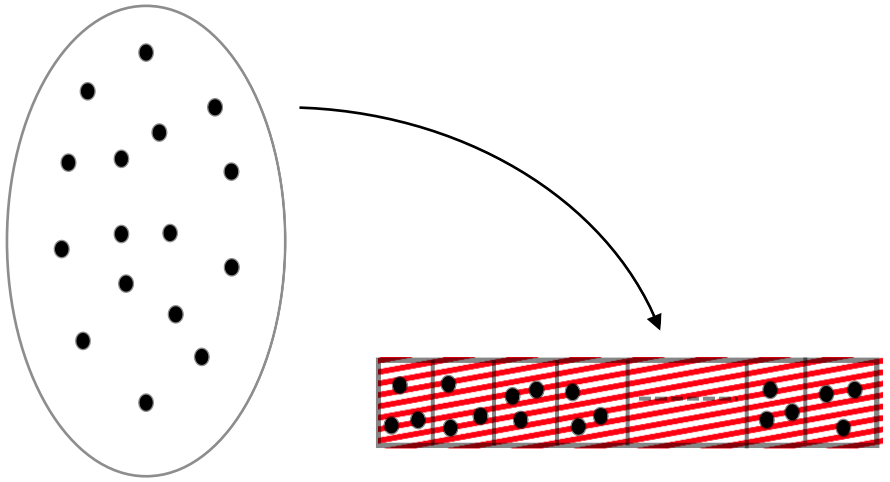
Achievability: Codebook Construction

- Uses the *random binning codebook* [Wyner '75, Winter *et al.* '03]
- Employs a stochastic encoding strategy by Alice

Binned codebook construction

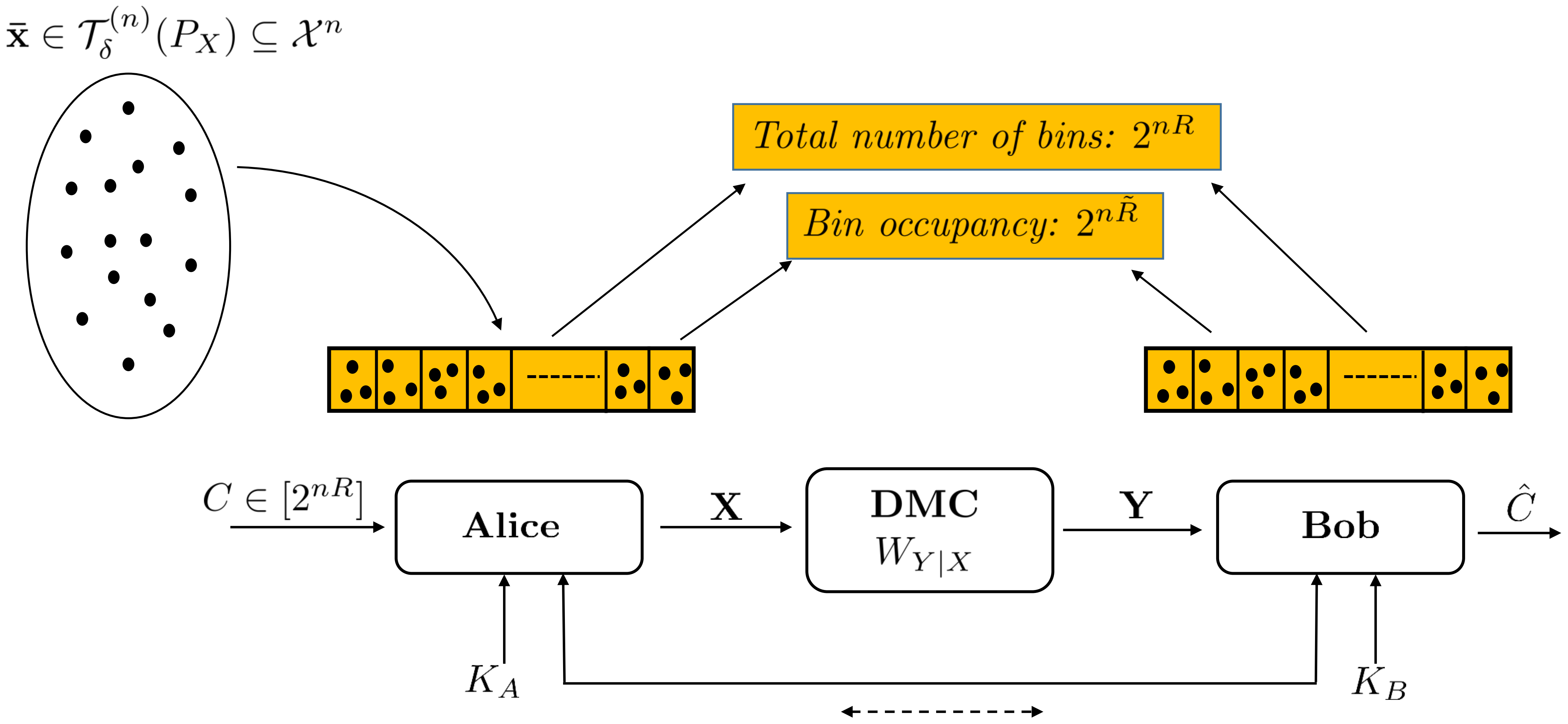
For an $\varepsilon > 0$, fix:

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Binning Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$

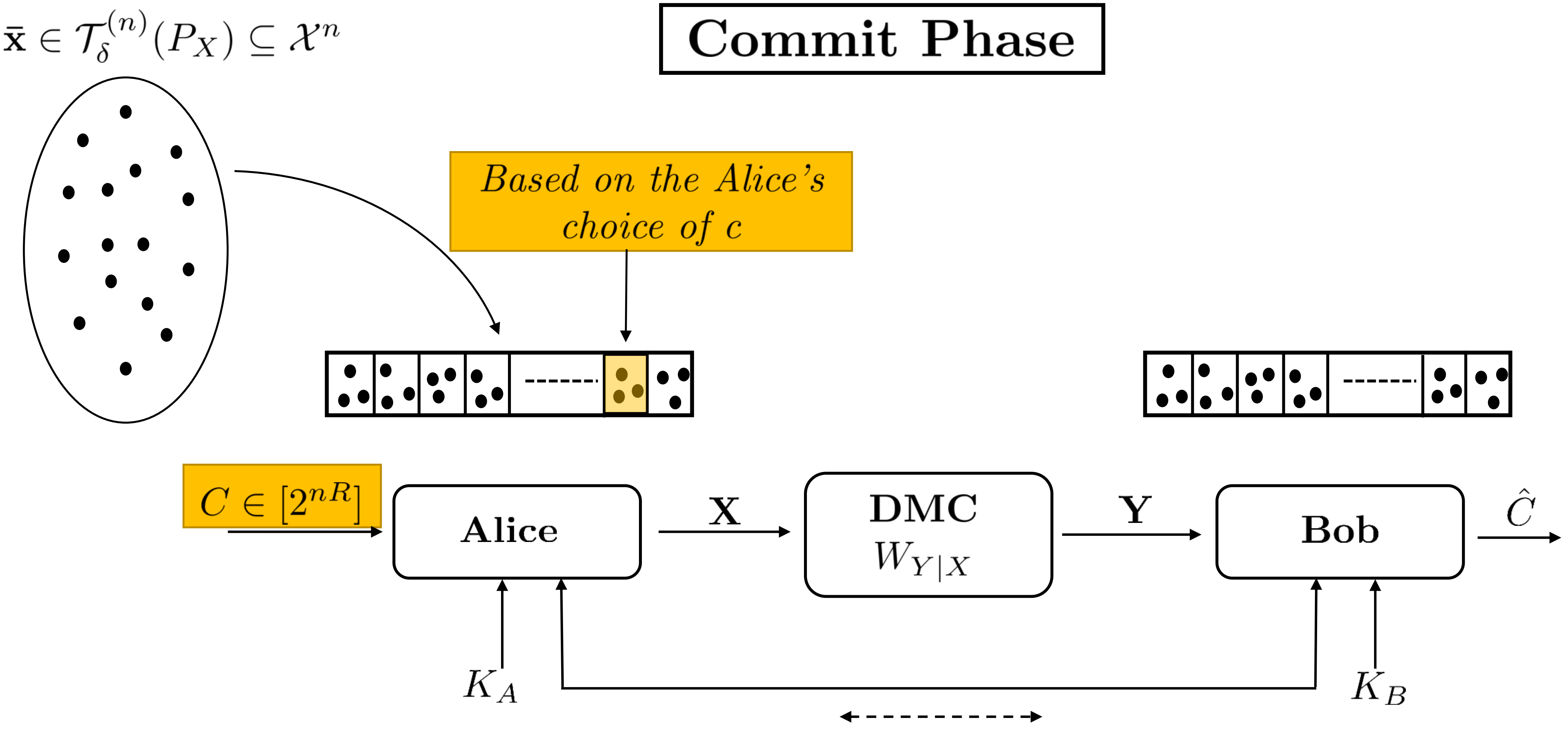


$\mathcal{T}_{\delta}^{(n)}(P_X) \subseteq \mathcal{X}^n$

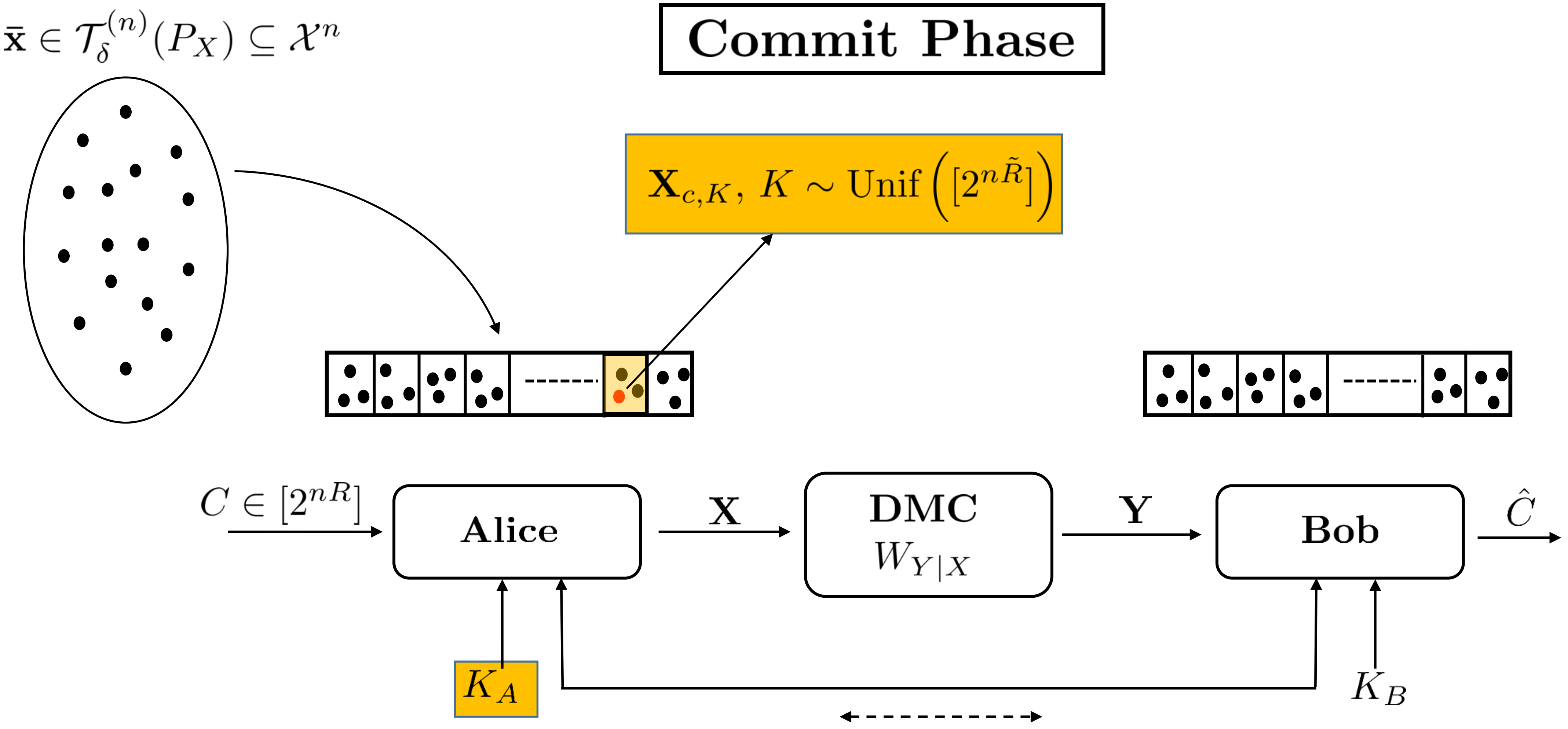
Achievability: Protocol



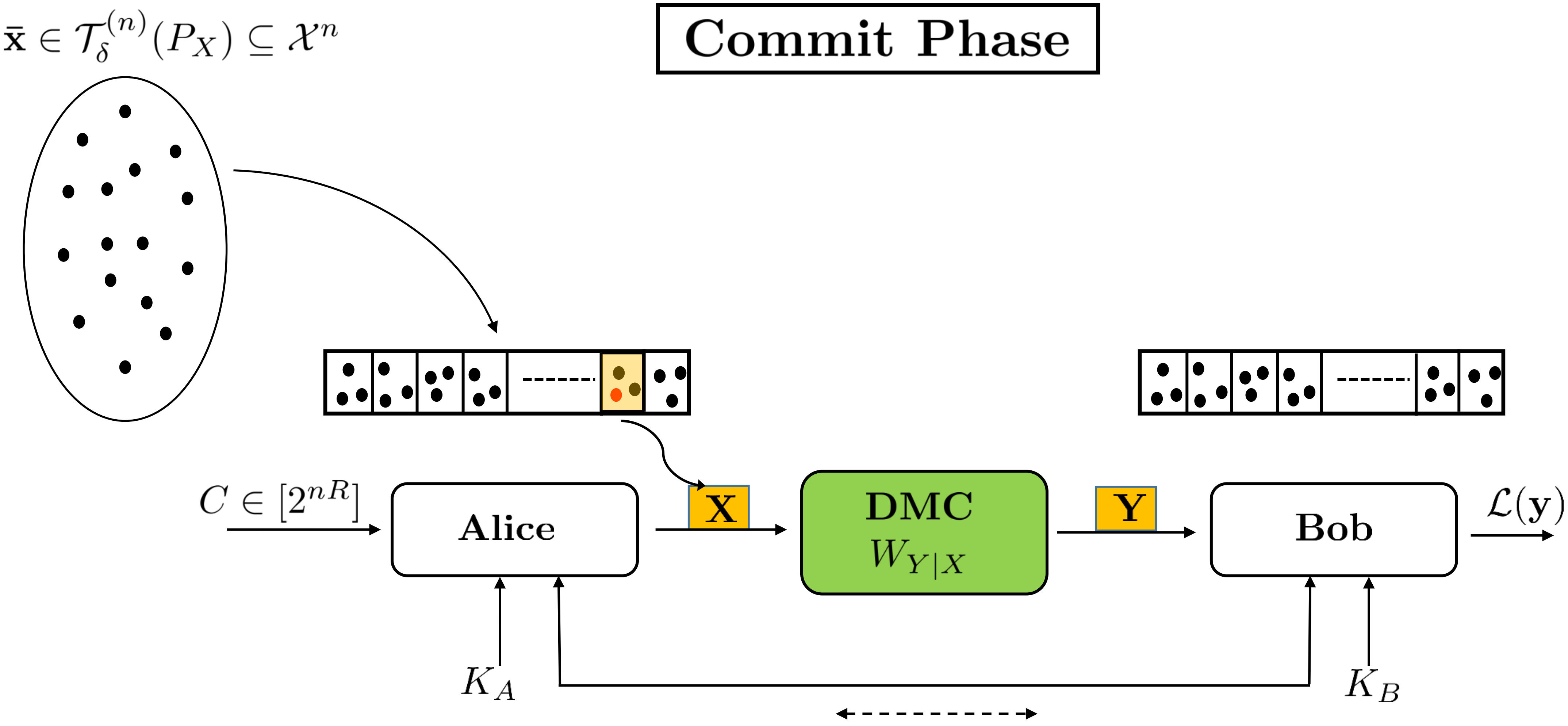
Achievability: Protocol



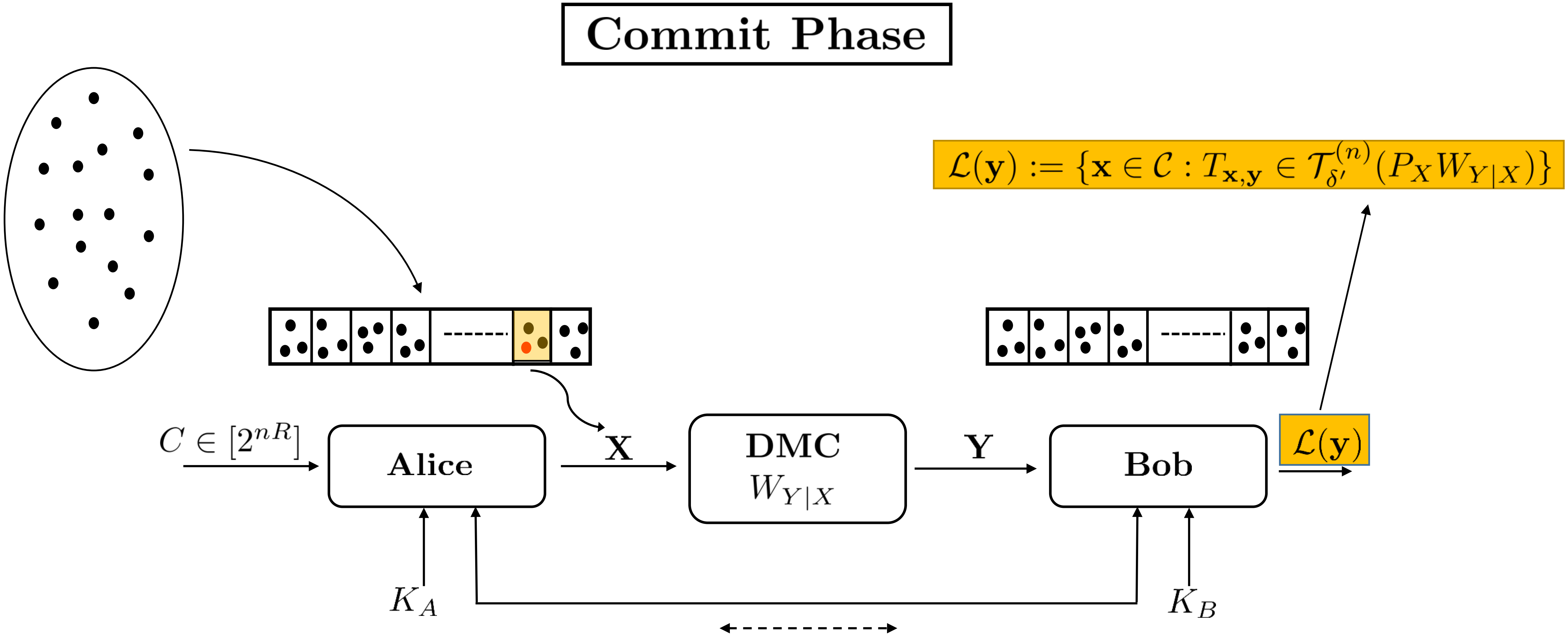
Achievability: Protocol



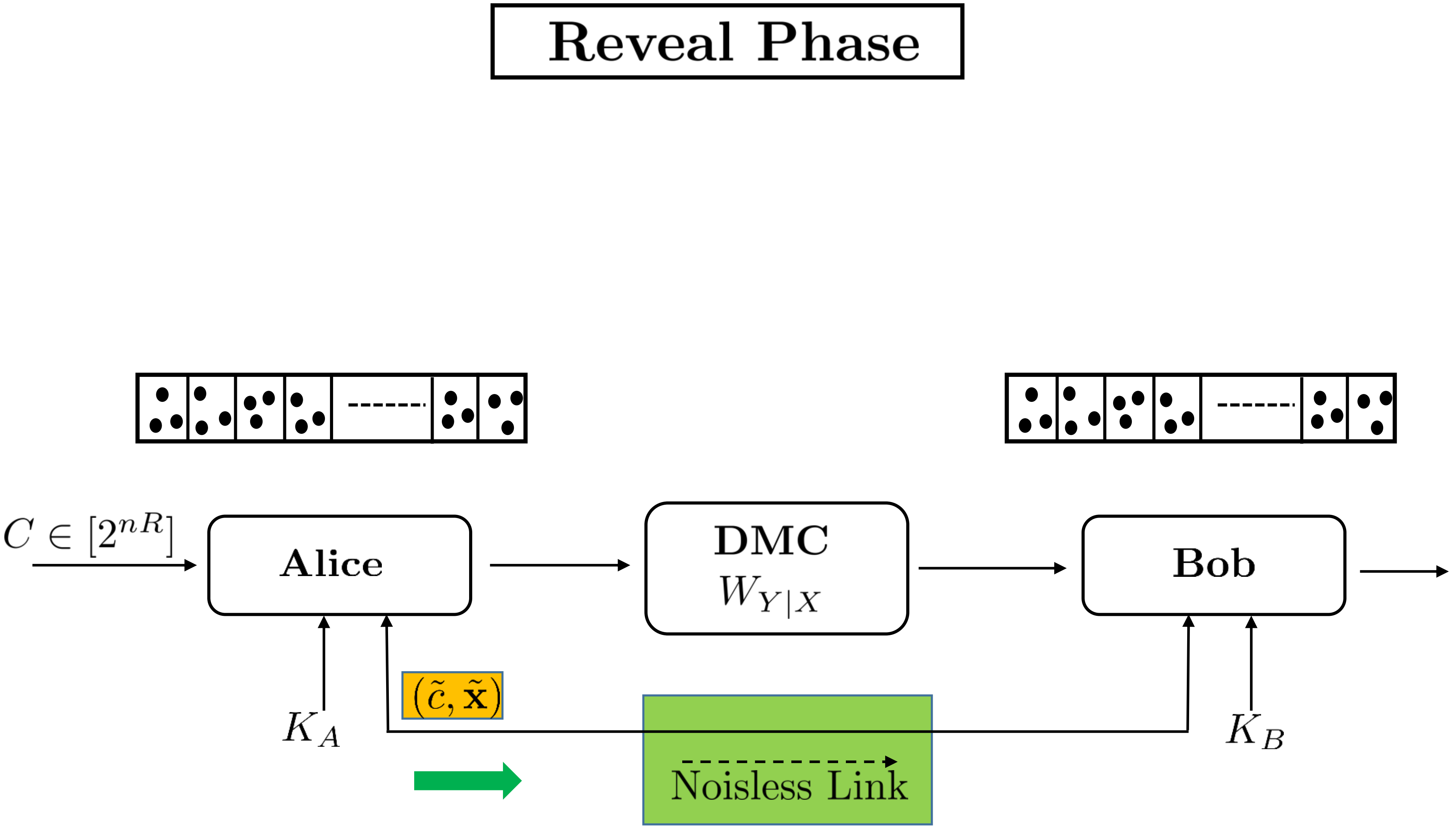
Achievability: Protocol



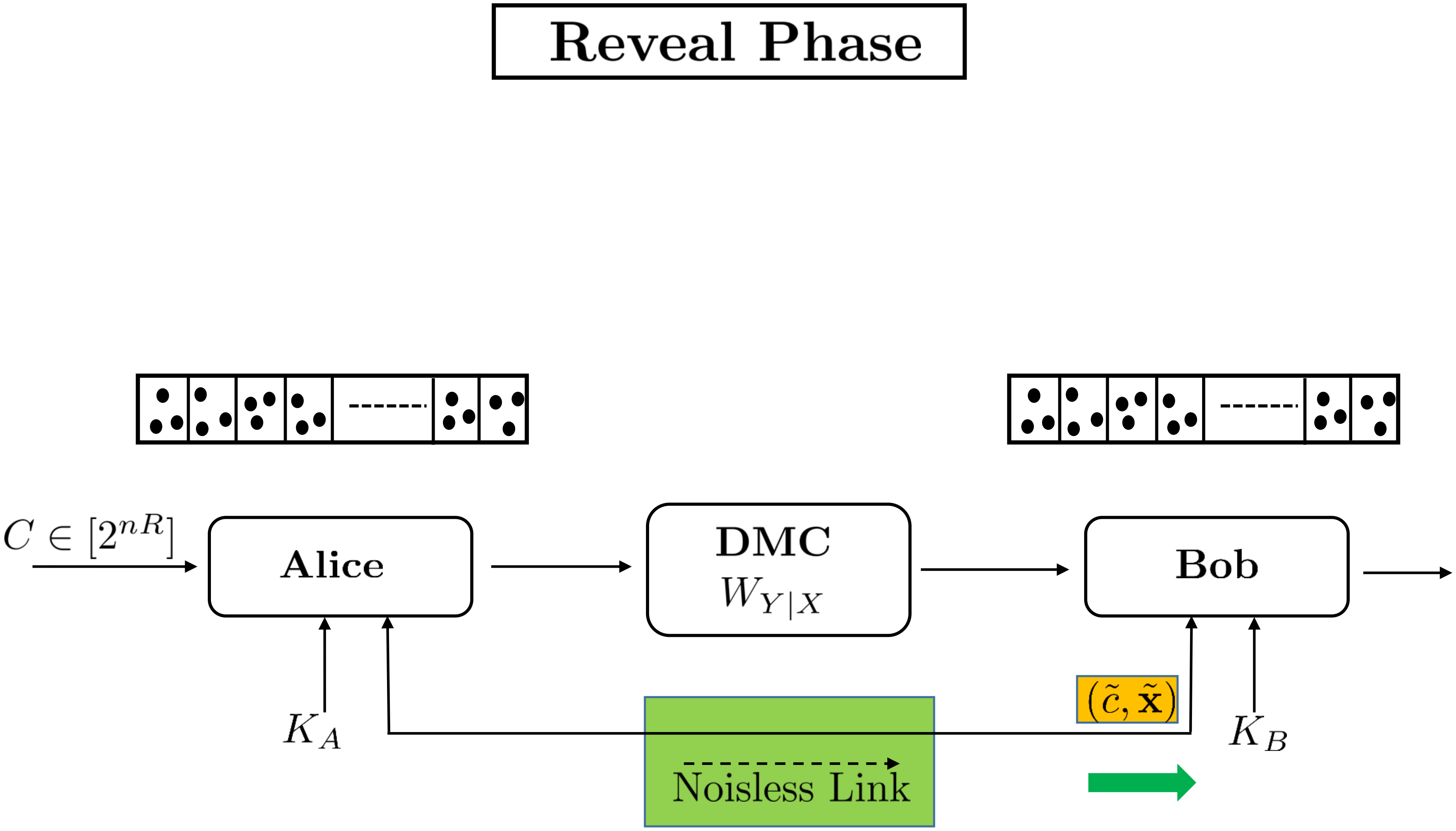
Achievability: Protocol



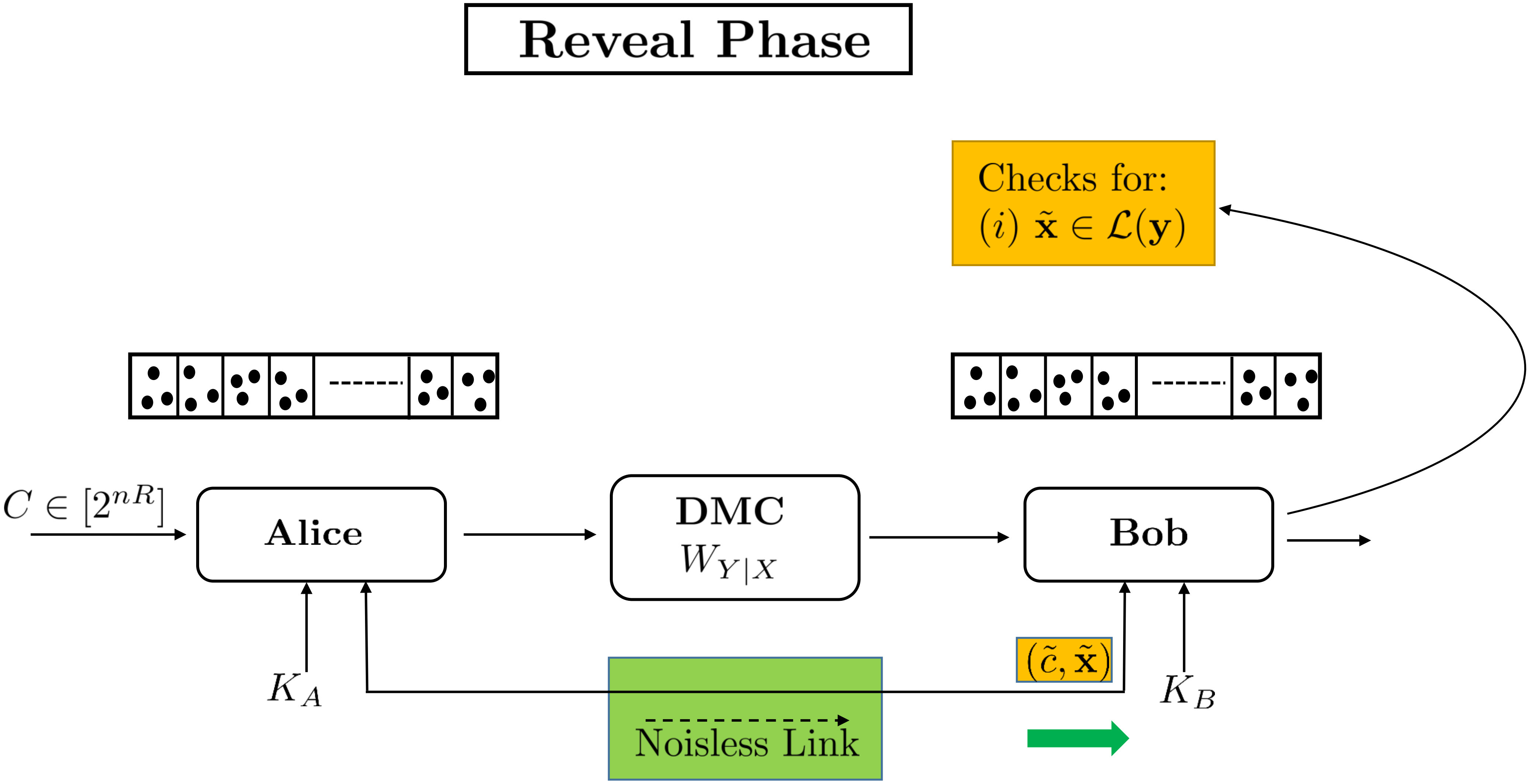
Achievability: Protocol



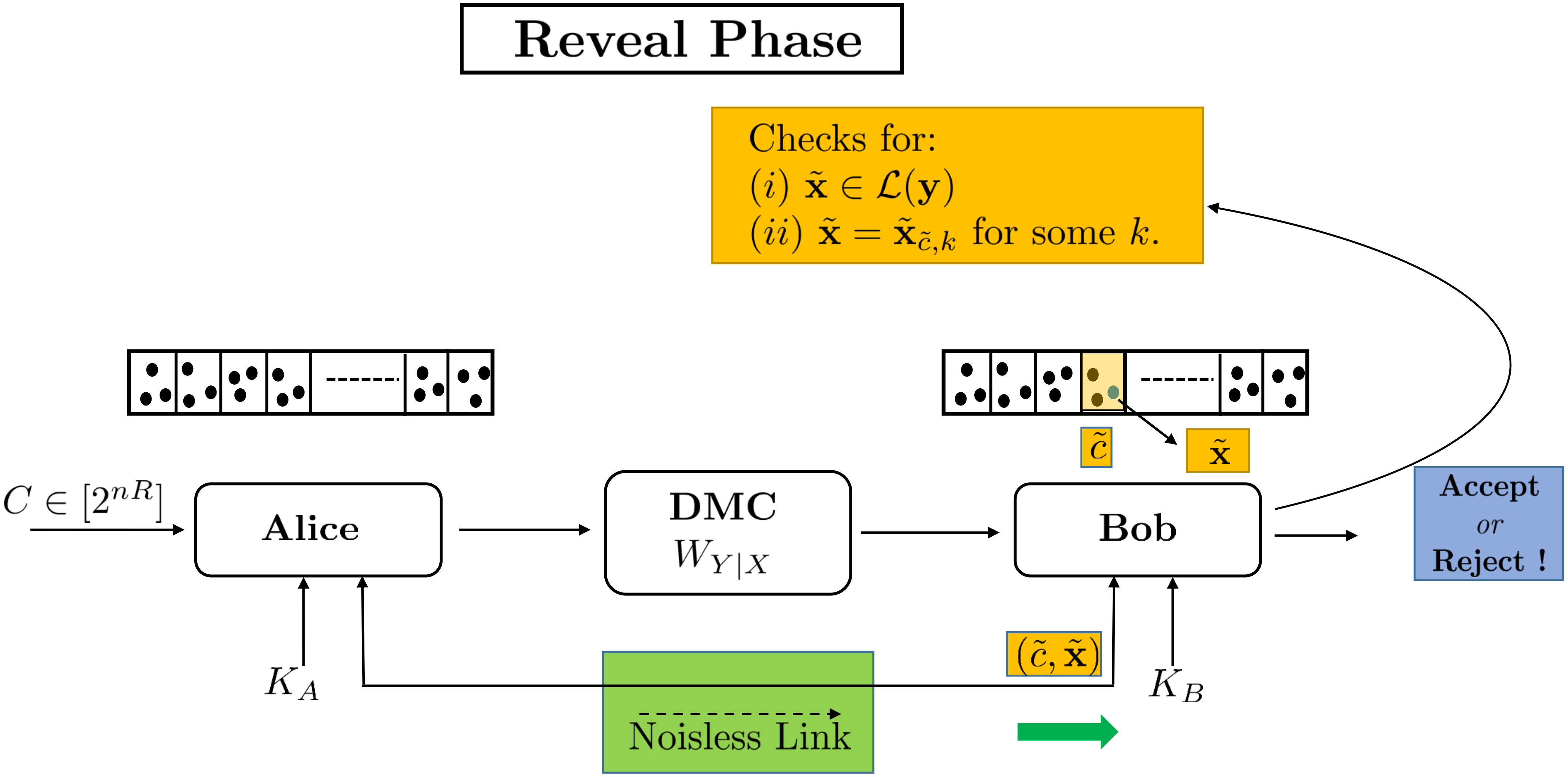
Achievability: Protocol



Achievability: Protocol



Achievability: Protocol



Achievability: Proof Analysis

Binned codebook construction

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Commitment Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$

Lemma (Codebook Construction)

$\exists$ a *binned codebook*: $\mathcal{A} = \{\bar{x}_{c,k}\}$, for $c \in [2^{nR}]$, $k \in [2^{n\tilde{R}}]$, where $|\mathcal{A}| = 2^{nR_{ov}}$ and $\bar{x}_{c,k} \in \mathcal{T}_{\delta}^{(n)}(P_X)$, such that:

(i) $d_H(\vec{x}_{c,k}, \vec{x}_{c',k'}) \geq 2n\eta$, $\forall c \neq c'$, $c, c' \in [2^{nR}]$, $k, k' \in [2^{n\tilde{R}}]$

(ii) for every $c \in [2^{nR}]$,

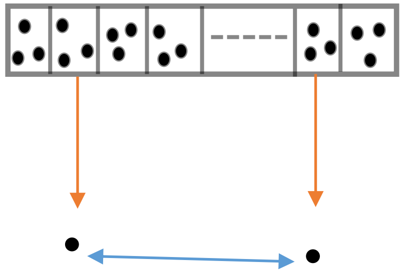
$$D\left(\frac{1}{2^{n\tilde{R}}}\sum_{k=1}^{2^{n\tilde{R}}} W_{Y|X}^{(n)}(\vec{y}|\vec{x}_{c,k}) \middle\| [P_X W_{Y|X}]_Y^{(n)}(\vec{y})\right) \leq e^{-n\alpha}$$

for some $\alpha(\delta) > 0$, where $\alpha \to 0$ as $\delta \to 0$.

Achievability: Proof Analysis

Binned codebook construction

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Commitment Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$



Lemma (Codebook Construction)

$\exists$ a *binned codebook*: $\mathcal{A} = \{\bar{x}_{c,k}\}$, for $c \in [2^{nR}]$, $k \in [2^{n\tilde{R}}]$, where $|\mathcal{A}| = 2^{nR_{ov}}$ and $\bar{x}_{c,k} \in \mathcal{T}_\delta^{(n)}(P_X)$, such that:

(i) $d_H(\vec{x}_{c,k}, \vec{x}_{c',k'}) \geq 2n\eta$, $\forall c \neq c'$, $c, c' \in [2^{nR}]$, $k, k' \in [2^{n\tilde{R}}]$

(ii) for every $c \in [2^{nR}]$,

$$D\left(\frac{1}{2^{n\tilde{R}}}\sum_{k=1}^{2^{n\tilde{R}}} W_{Y|X}^{(n)}(\vec{y}|\vec{x}_{c,k}) \middle\| [P_X W_{Y|X}]_Y^{(n)}(\vec{y})\right) \leq e^{-n\alpha}$$

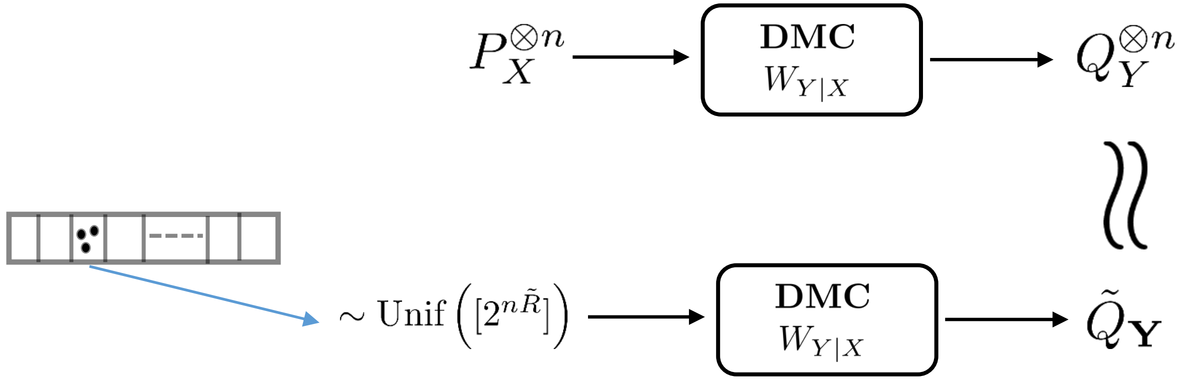
for some $\alpha(\delta) > 0$, where $\alpha \to 0$ as $\delta \to 0$.

"minimum distance *across bins* property"

Achievability: Proof Analysis

Binned codebook construction

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Commitment Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$



Lemma (Codebook Construction)

$\exists$ a *binned codebook*: $\mathcal{A} = \{\bar{x}_{c,k}\}$, for $c \in [2^{nR}]$, $k \in [2^{n\tilde{R}}]$, where $|\mathcal{A}| = 2^{nR_{ov}}$ and $\bar{x}_{c,k} \in \mathcal{T}_\delta^{(n)}(P_X)$, such that:

(i) $d_H(\vec{x}_{c,k}, \vec{x}_{c',k'}) \geq 2n\eta$, $\forall c \neq c'$, $c, c' \in [2^{nR}]$, $k, k' \in [2^{n\tilde{R}}]$

(ii) for every $c \in [2^{nR}]$,

$$D\left(\frac{1}{2^{n\tilde{R}}}\sum_{k=1}^{2^{n\tilde{R}}} W_{Y|X}^{(n)}(\vec{y}|\vec{x}_{c,k}) \Bigg|\Bigg| [P_X W_{Y|X}]_Y^{(n)}(\vec{y})\right) \leq e^{-n\alpha}$$

for some $\alpha(\delta) > 0$, where $\alpha \to 0$ as $\delta \to 0$.

Output distribution simulation property

Converse

A rate R scheme: $\epsilon_n - sound$, $\epsilon_n - concealing$ and $\epsilon_n - binding$

$$
\begin{aligned}
nR = H(C) &= H(C|V_B) + I(C;V_B) \\
&\leq H(C|\mathbf{Y}, M, K_B) + \epsilon_n \\
&\leq H(C, \mathbf{X}|\mathbf{Y}, M, K_B) + \epsilon_n \\
&= H(\mathbf{X}|\mathbf{Y}, M, K_B) + H(C|\mathbf{X}, \mathbf{Y}, M, K_B) \\
&\qquad + \epsilon_n \\
&\leq H(\mathbf{X}|\mathbf{Y}) + H(C|\mathbf{X}, V_B) + \epsilon_n \\
&\boxed{\leq \sum_{i=1}^{n} H(X_i|Y_i) + n\epsilon'_n + \epsilon_n} \\
&= n\left(\sum_{i=1}^{n} \frac{1}{n} H(X_i|Y_i)\right) + n\epsilon'_n + \epsilon_n
\end{aligned}
$$

$\epsilon_n - concealing$

$I(C;V_B) \leq \epsilon_n$

Lemma :

$H(C|\mathbf{X}, V_B) \leq n\epsilon'_n, \quad \epsilon'_n \to 0$ as $\epsilon_n \to 0$

Proof: $\epsilon_n - soundness$, $\epsilon_n - bindingness$, and Fano's Inequality

Converse

A rate R scheme: $\epsilon_n - sound$, $\epsilon_n - concealing$ and $\epsilon_n - binding$

$$
\begin{aligned}
nR = H(C) &= H(C|V_B) + I(C;V_B) \\
&\leq n\left(\sum_{i=1}^{n}\frac{1}{n}H(X_i|Y_i)\right) + n\epsilon_n' + \epsilon_n \\
&\leq n\left(\sum_{i=1}^{n}\frac{1}{n}\mathbb{C}(\mathbb{E}[\rho_X(X_i)])\right) + n\epsilon_n' + \epsilon_n \\
&\leq n\mathbb{C}\left(\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}[\rho_X(X_i)]\right) + n\epsilon_n' + \epsilon_n \\
&\leq n\mathbb{C}\left(\Gamma\right) + n\epsilon_n' + \epsilon_n
\end{aligned}
$$

From definition,

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

Lemma:

$\mathbb{C}(\Gamma)$ is *non-decreasing* in Γ

$\mathbb{C}(\Gamma)$ is *concave* in Γ

$$\sum_{i=1}^{n}\mathbb{E}[\rho_X(X_i)] \leq n\Gamma$$

as $n \to \infty$,

$$R \leq \mathbb{C}(\Gamma)$$

Dual Expression

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

Recall, $\mathbb{C}(\Gamma)$: non-decreasing, concave in Γ

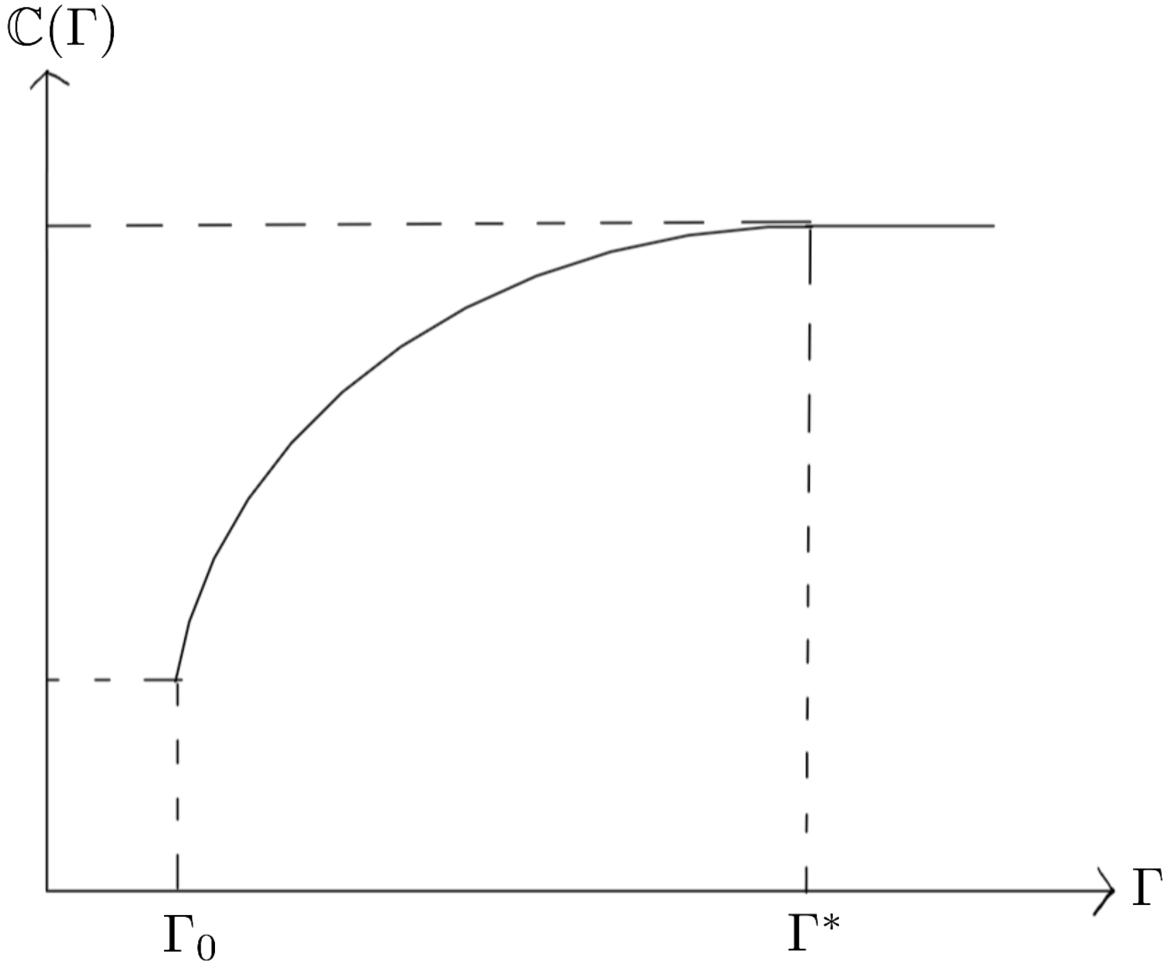


Fig: Plot of $\mathbb{C}(\Gamma)$ vs Γ

Dual Expression

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

Recall, $\mathbb{C}(\Gamma)$: non-decreasing, concave in Γ

Important Parameters

- $\Gamma_0 := \min_x \rho_X(x)$
- $\Gamma^* := \min\{\Gamma : \mathbb{C}(\Gamma) = \mathbb{C}(\infty)\}$

$\mathbb{C}(\Gamma)$ only studied for $\Gamma \in [\Gamma_0, \Gamma^*]$

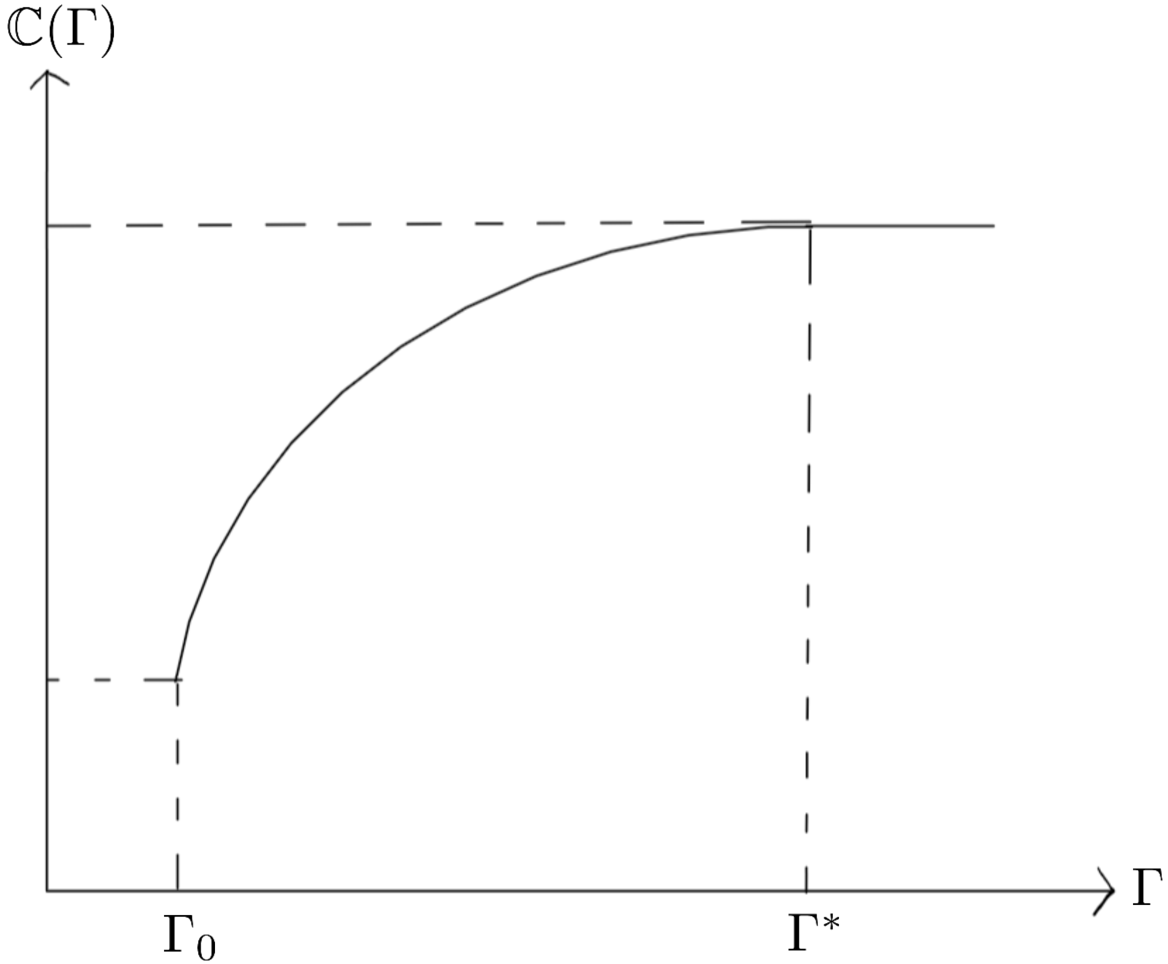


Fig: Plot of $\mathbb{C}(\Gamma)$ vs Γ

Dual Expression

For $\Gamma_1 \in [\Gamma_0, \Gamma^*]$

γ_1 : slope of the tangent to $\mathbb{C}(\Gamma)$ at Γ_1

$F(\gamma_1)$: corresponding $y-$intercept

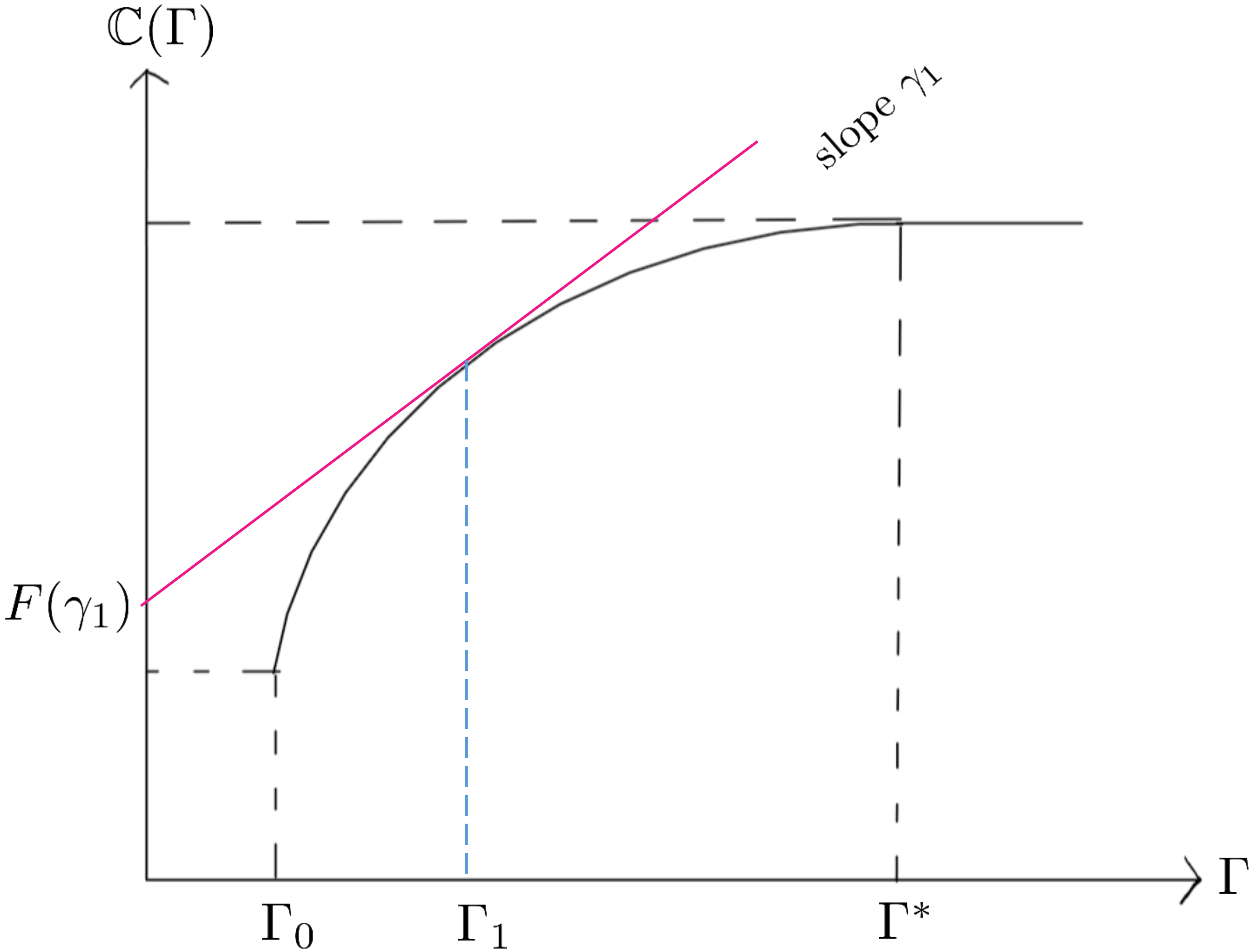


Fig: Plot of $\mathbb{C}(\Gamma)$ vs Γ

Dual Expression

For $\Gamma_1 \in [\Gamma_0, \Gamma^*]$

γ_1 : slope of the tangent to $\mathbb{C}(\Gamma)$ at Γ_1

$F(\gamma_1)$: corresponding $y-$intercept

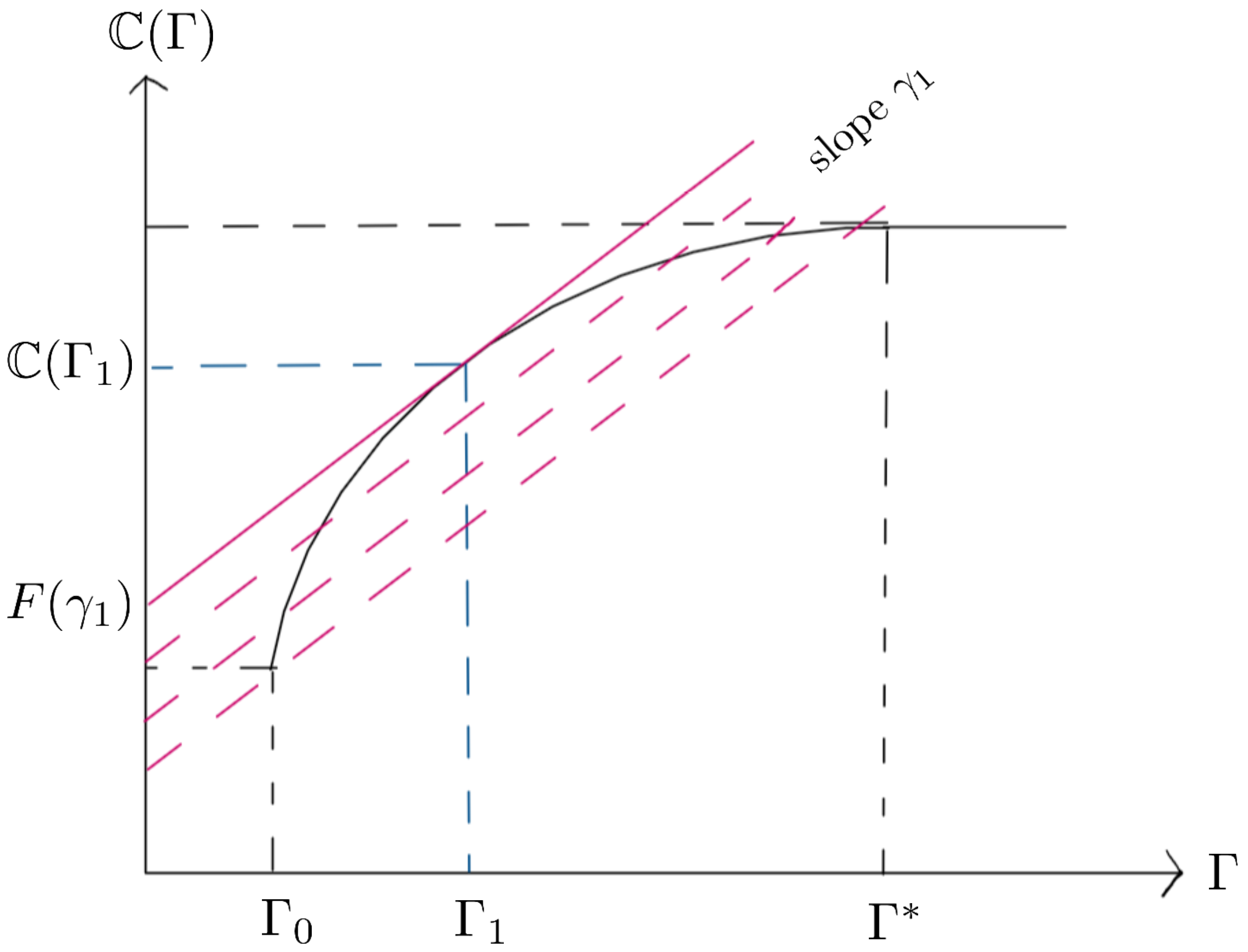


Fig: Plot of family of γ_1-sloped lines over $\mathbb{C}(\Gamma)$ curve

Dual Expression

For $\Gamma_1 \in [\Gamma_0, \Gamma^*]$

γ_1 : slope of the tangent to $\mathbb{C}(\Gamma)$ at Γ_1

$F(\gamma_1)$: corresponding $y-$intercept

$$F(\gamma_1) = \max_{\Gamma} \left[\mathbb{C}(\Gamma_1) - \gamma_1 \Gamma\right]$$

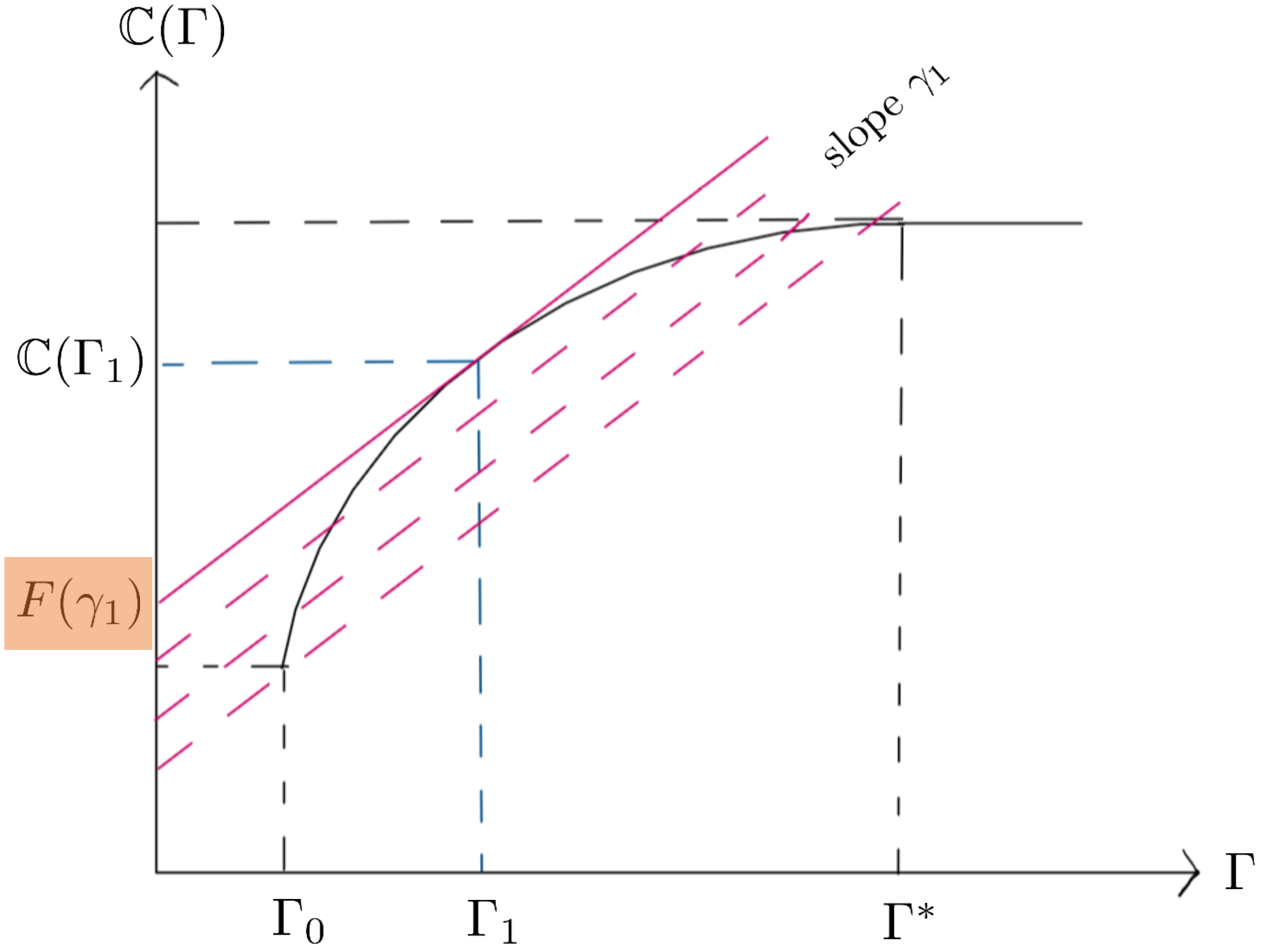


Fig: Plot of family of γ_1-sloped lines over $\mathbb{C}(\Gamma)$ curve

Dual Expression

$\mathbb{C}(\Gamma)$ can be reconstructed from the concave envelope of its tangents

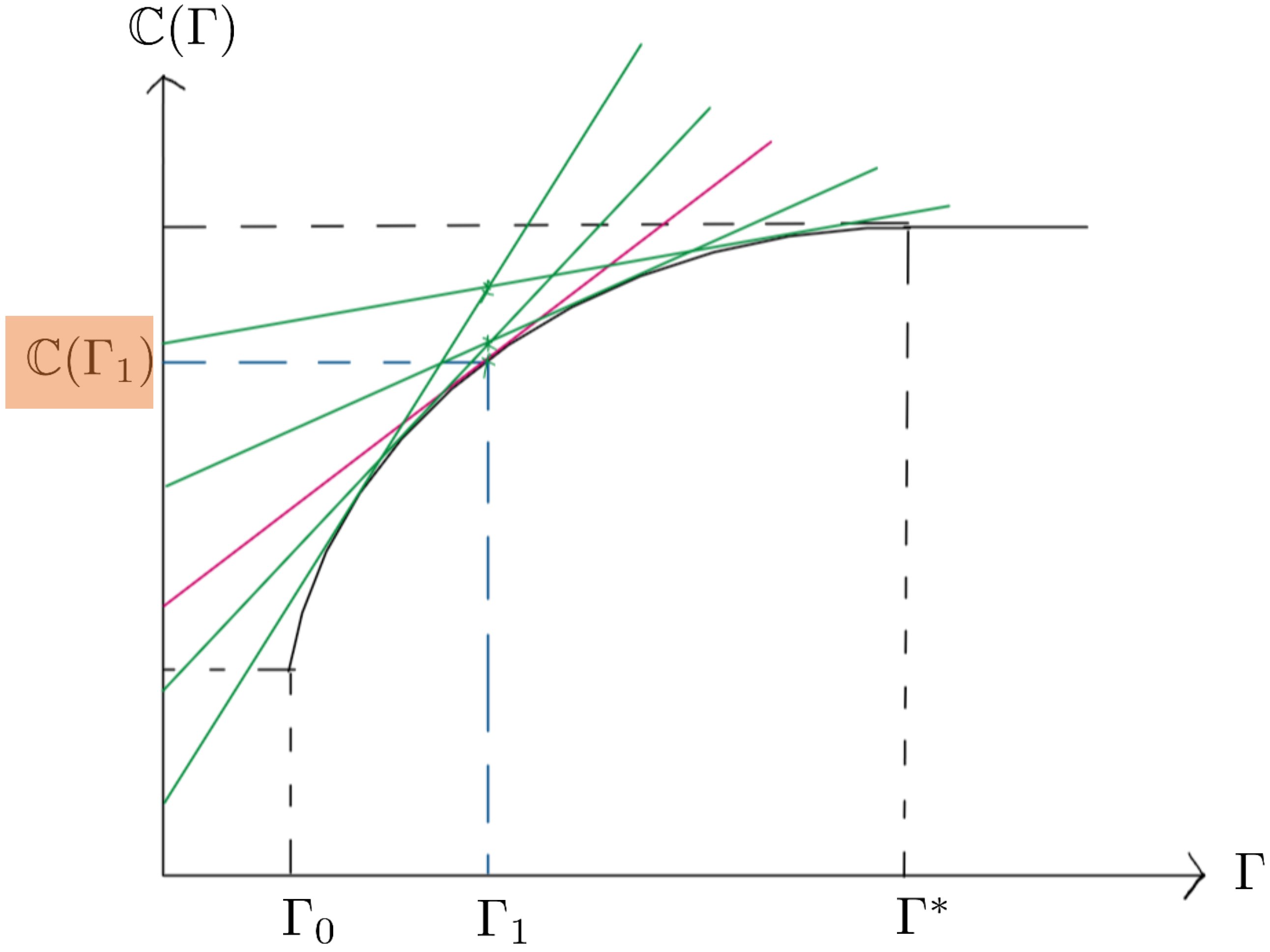


Fig: Plot of family of tangents to $\mathbb{C}(\Gamma)$ curve

Dual Expression

$$\mathbb{C}(\Gamma_1) = \min_{\gamma \geq 0} \left[F(\gamma) + \gamma\Gamma_1\right]$$

$\mathbb{C}(\Gamma)$ can be reconstructed from the concave envelope of its tangents

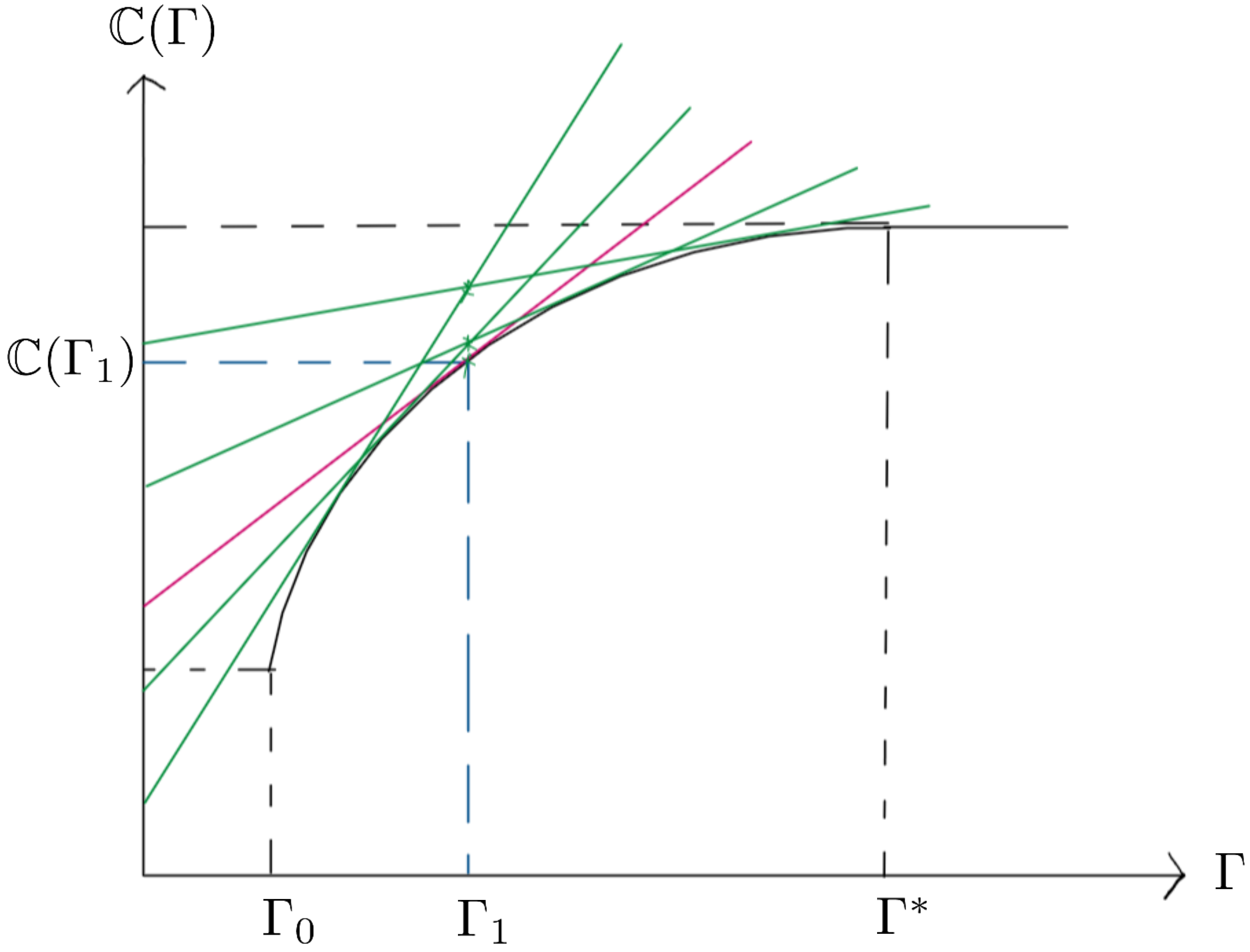


Fig: Plot of family of tangents to $\mathbb{C}(\Gamma)$ curve

Dual Expression

For given Γ

$$F(P_X, Q_Y) := H(P_X) - I(P_X, W_{Y|X}) - D(P_X W_{Y|X} || Q_Y) - \gamma \rho_X(P_X)$$

$$\max_{P_X} \max_{Q_Y} F(P_X, Q_Y) = F(\gamma)$$

$$\max_{Q_Y} \max_{P_X} F(P_X, Q_Y) = \max_{Q_Y} \Big[\log \Big(\sum_{x \in \mathcal{X}} \exp(-D(W_{Y|X}(\cdot|x) || Q_Y) - \gamma \rho_X(x)) \Big) \Big]$$

$$\max_{P_X} \max_{Q_Y} F(P_X, Q_Y) = \max_{Q_Y} \max_{P_X} F(P_X, Q_Y)$$

$$\Rightarrow F(\gamma) = \max_{Q_Y} \Big[\log \Big(\sum_{x \in \mathcal{X}} \exp(-D(W_{Y|X}(\cdot|x) || Q_Y) - \gamma \rho_X(x)) \Big) \Big]$$

Lemma:

$$\max_{Q_Y} F(P_X, Q_Y) = H(P_X) - I(P_X, W_{Y|X}) - \gamma \rho_X(P_X)$$

$$\max_{P_X} F(P_X, Q_Y) = \log \left(\sum_{x \in \mathcal{X}} \exp(-D(W_{Y|X}(\cdot|x) || Q_Y) - \gamma \rho_X(x)) \right)$$

$$\boxed{\mathbb{C}(\Gamma) = \min_{\gamma \geq 0} [F(\gamma) + \gamma \Gamma] = \min_{\gamma \geq 0} \Big[\max_{Q_Y} \log \Big(\sum_{x \in \mathcal{X}} \exp[-D(W_{Y|X}(\cdot|x) || Q_Y) - \gamma \rho_X(x)] \Big) + \gamma \Gamma \Big]}$$

*exponent and logarithm to the same base

Conclusion

In Summary...

- Commitment capacity of DMCs under general input constraints
- Dual characterization of commitment capacity
- Capacity achieving output distribution is unique for every optimizing input distribution.

Thank you !!