# Commitment Capacity of Reverse Elastic Channels

Pranav Joshi
IIT Kharagpur

Pranav Joshi
IIT Kharagpur

Manideep Mamindlapally
IIT Kharagpur

Anuj Kumar Yadav
IIT Patna

Manoj Mishra
NISER, HBNI

Amitalok J. Budkuley
IIT Kharagpur

# 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

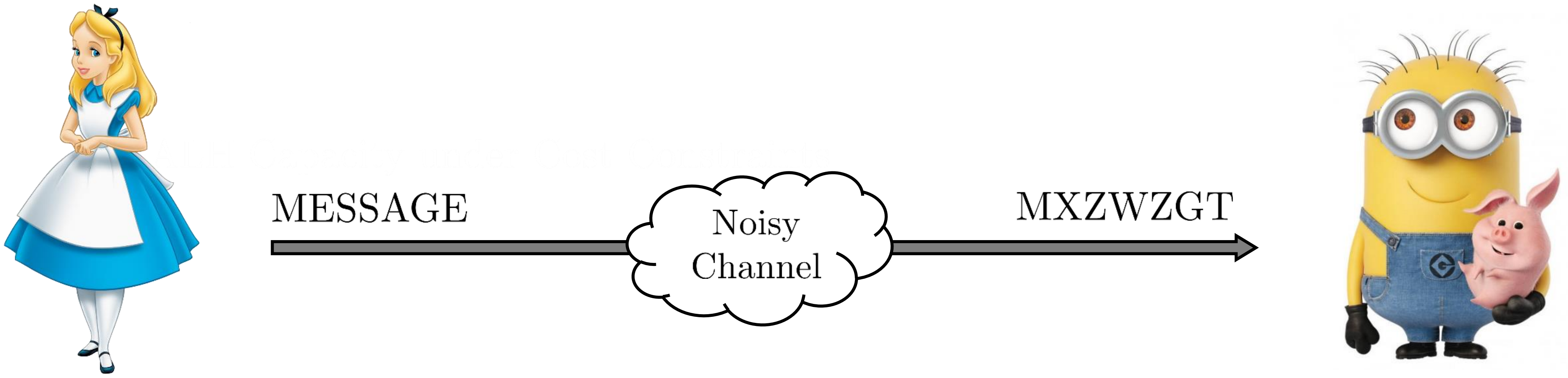
The next morning:


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

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

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

# A Solution - Noisy Channels

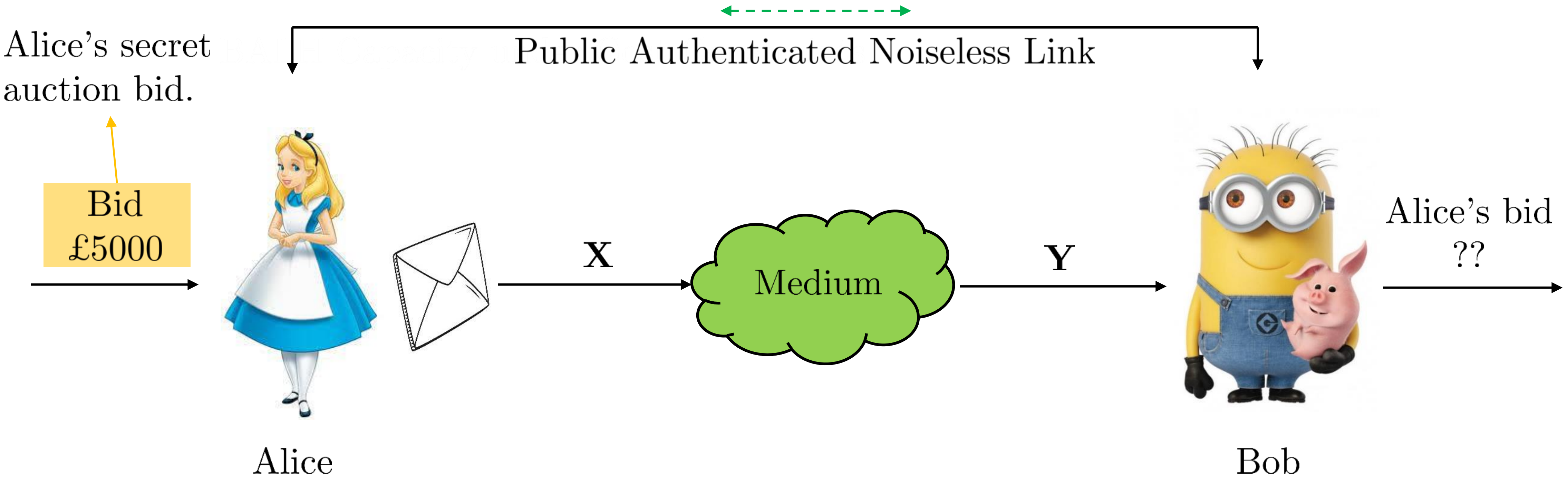



If used cleverly:
It jumbles the message just enough to **conceal** from Bob, and little enough for Bob to catch Alice if she cheats.

The Protocol occurs in two phases, the **Commit** and **Reveal** phases.

# The Commit Phase

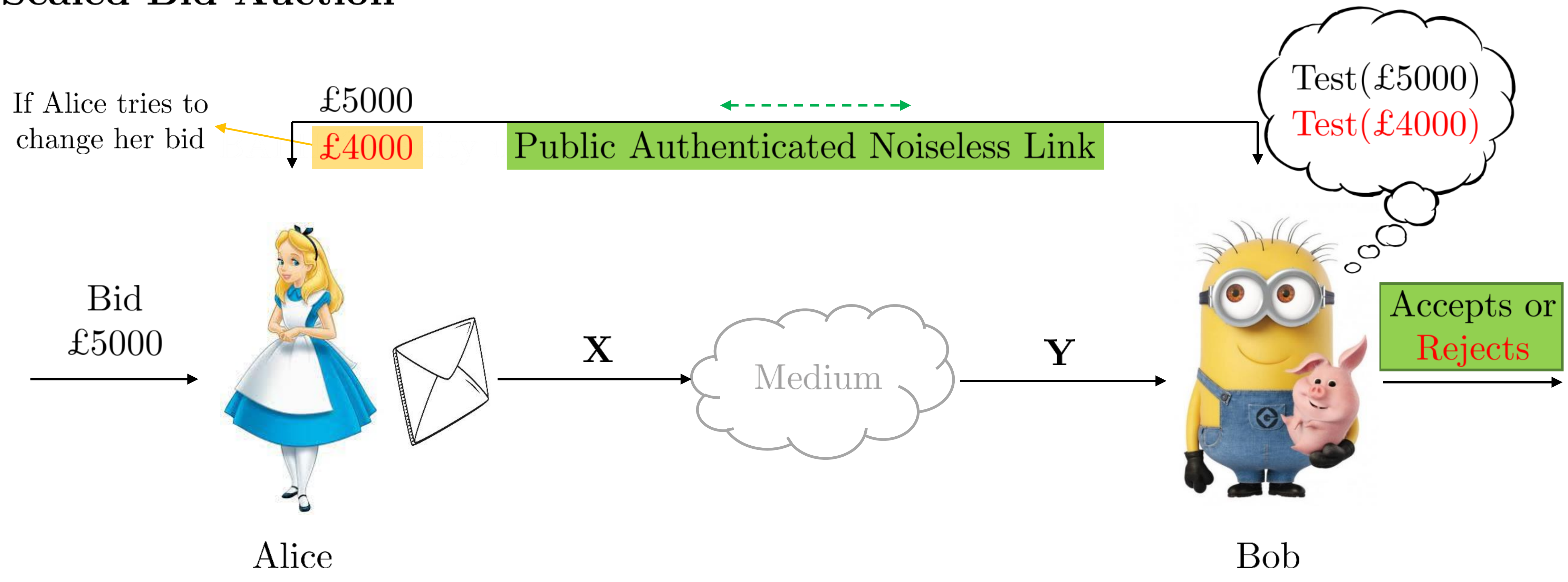
**Sealed Bid Auction**




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

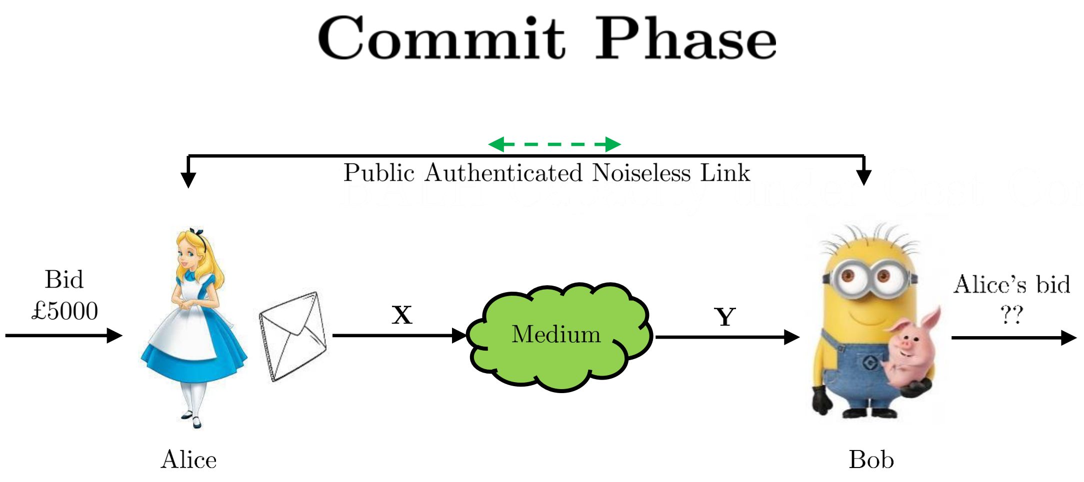
# The Reveal Phase

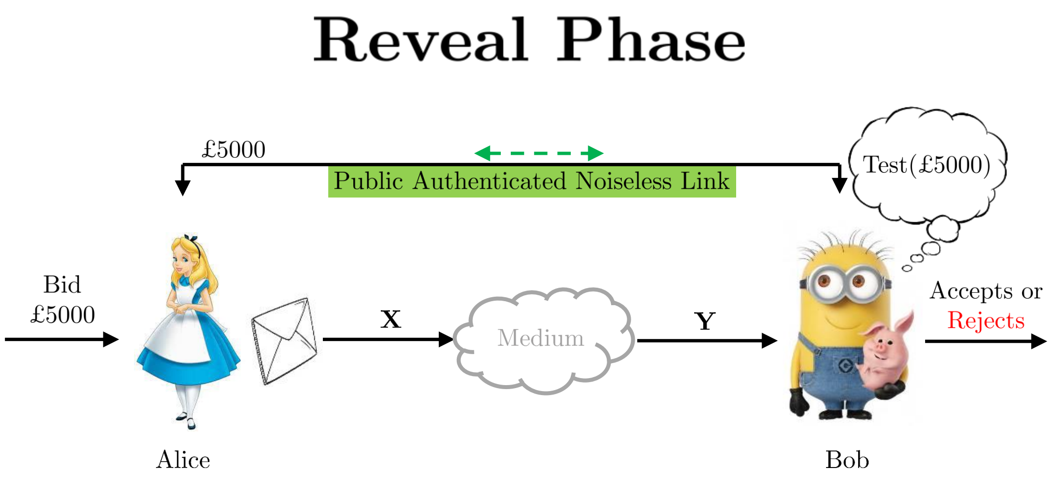
## Sealed Bid Auction




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

# Commitment



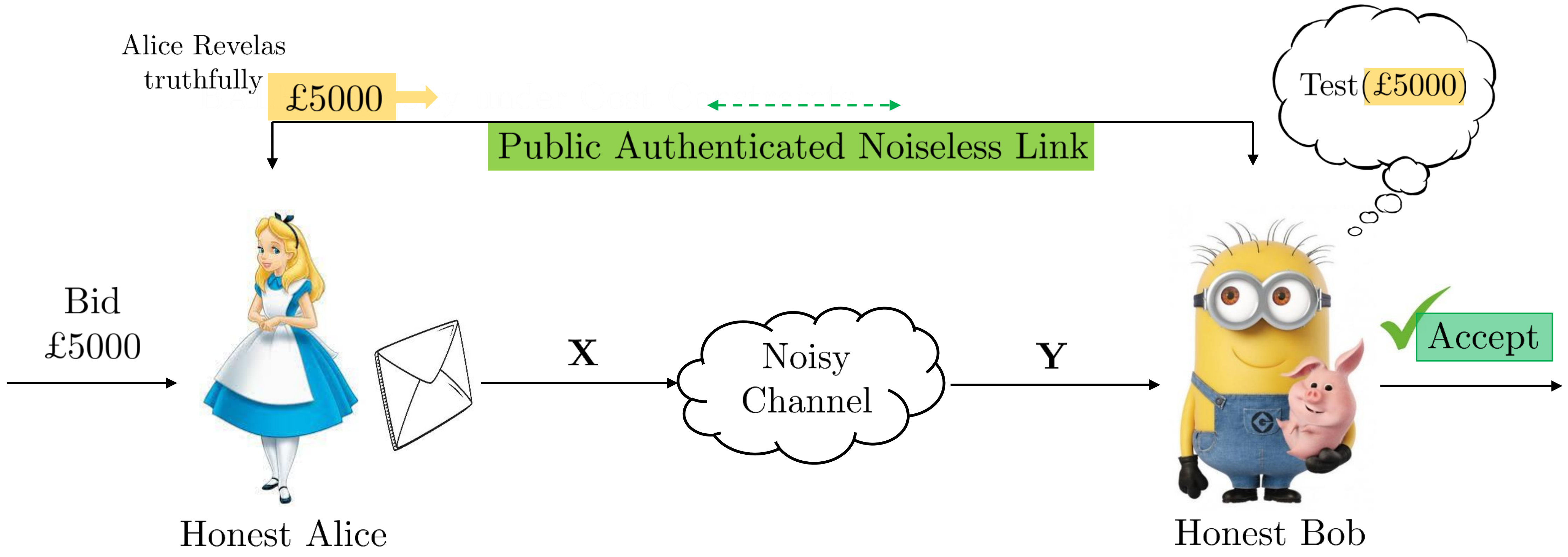




A good commitment protocol aims to be

- **sound** for two *honest* participants.
- **concealing** from *dishonest* Bob, when Alice *honestly* follows the protocol.
- **binding**: on a *dishonest* Alice, when Bob *honestly* follows the protocol

# Soundness

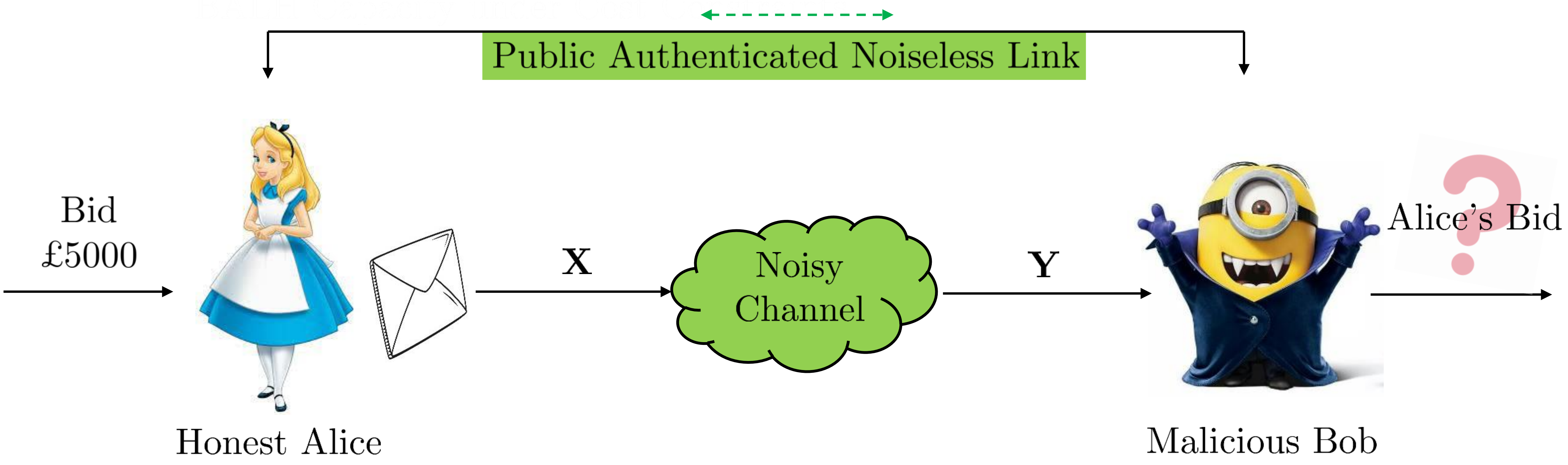
In the **Reveal Phase**:




**Sound Protocol:** A truthful reveal will never be rejected by Bob.

# Concealment

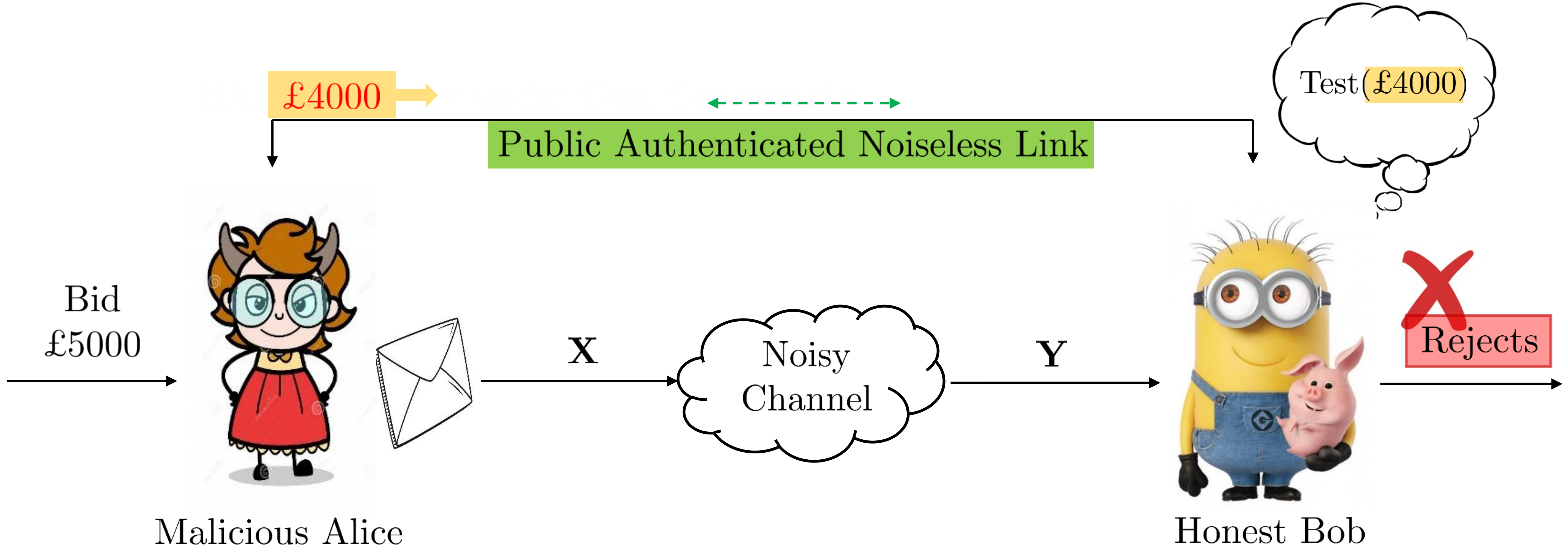
At the end of the **Commit Phase**:




**Concealing Protocol:** Bob can never learn Alice's bid until she reveals.

# Bindingness

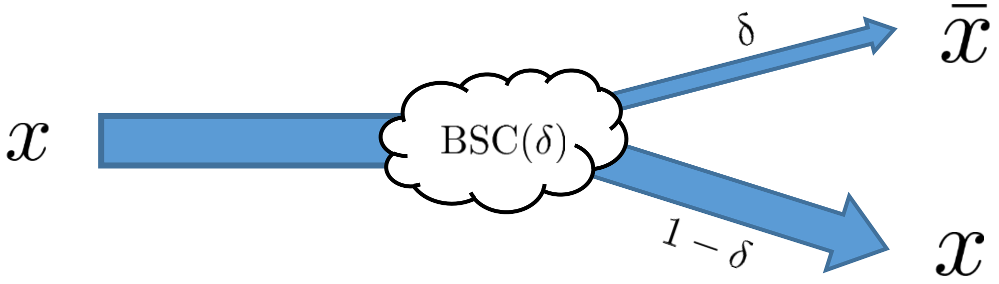
**In the Reveal Phase:**




**Binding Protocol:** Alice cannot change her bid without Bob realising.

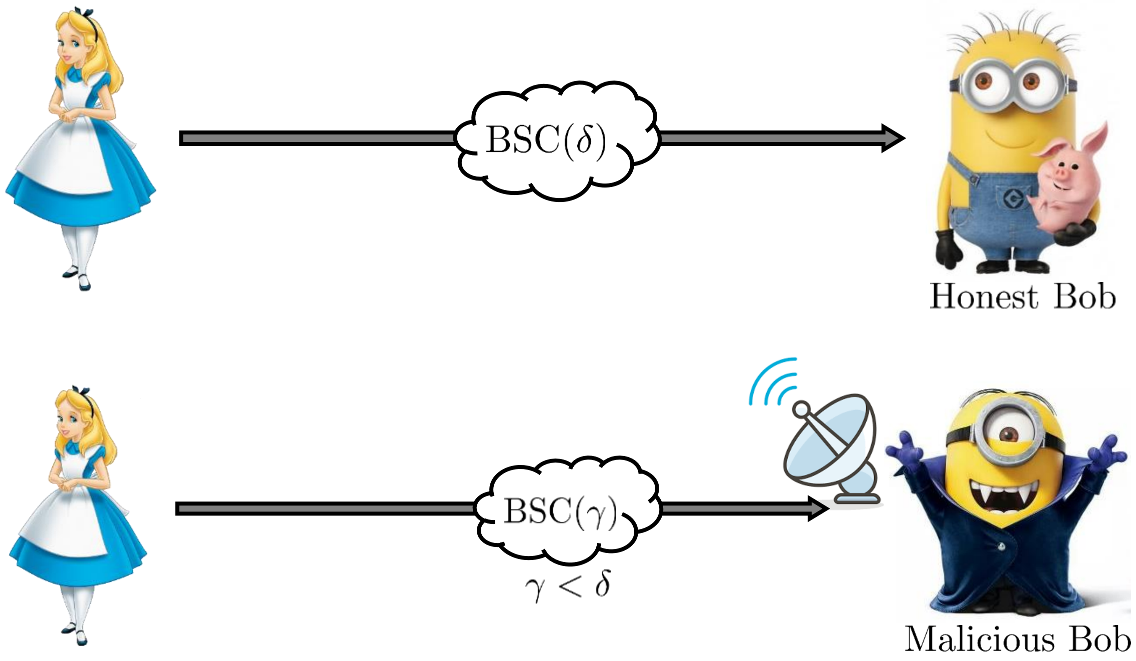
# Unreliable Noisy Channels

**Regular BSC:**




BSCs can be used for commitment, but not all channels are as *reliable*.
Real world channels may be influenced by malicious adversaries

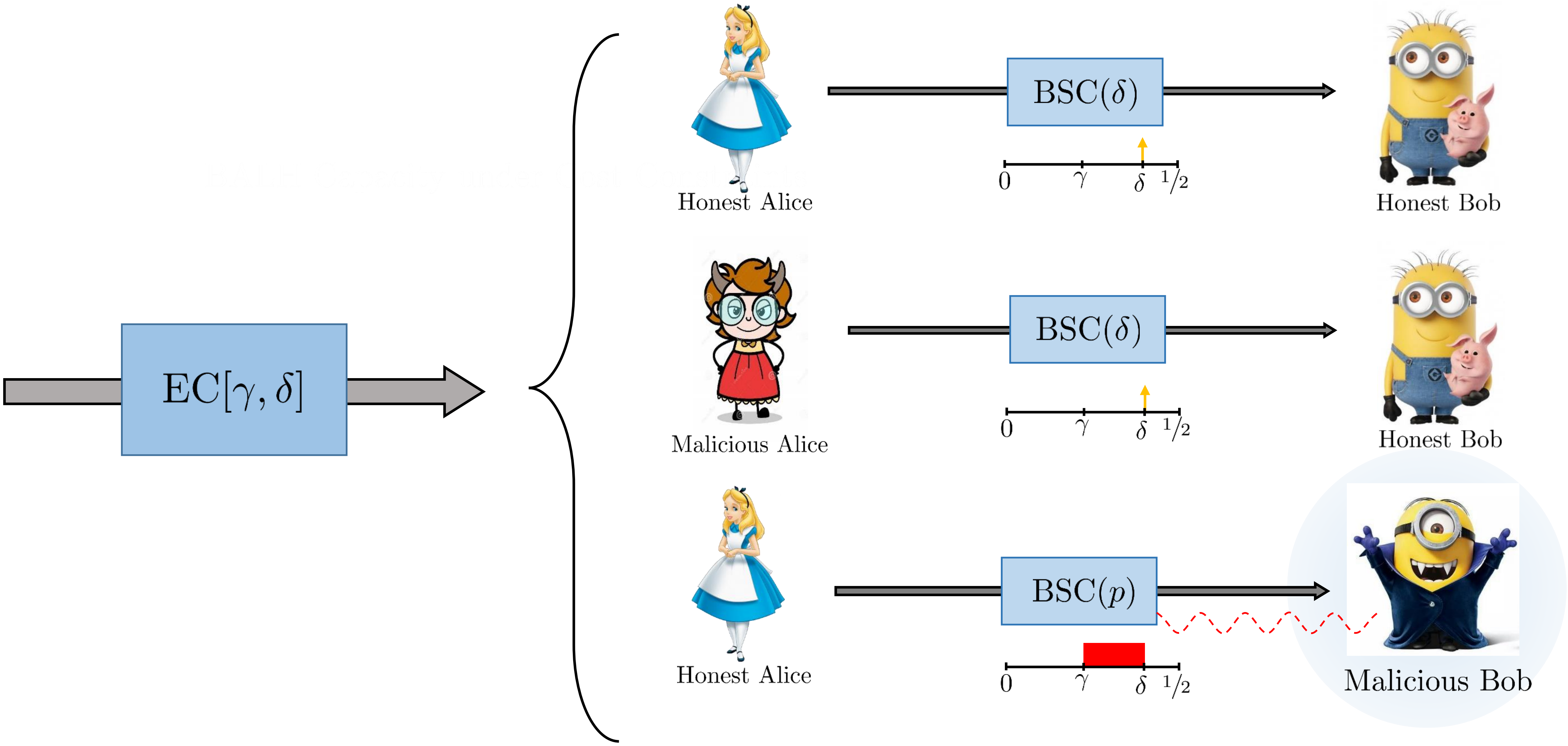
**Potential for Malicious Action:**



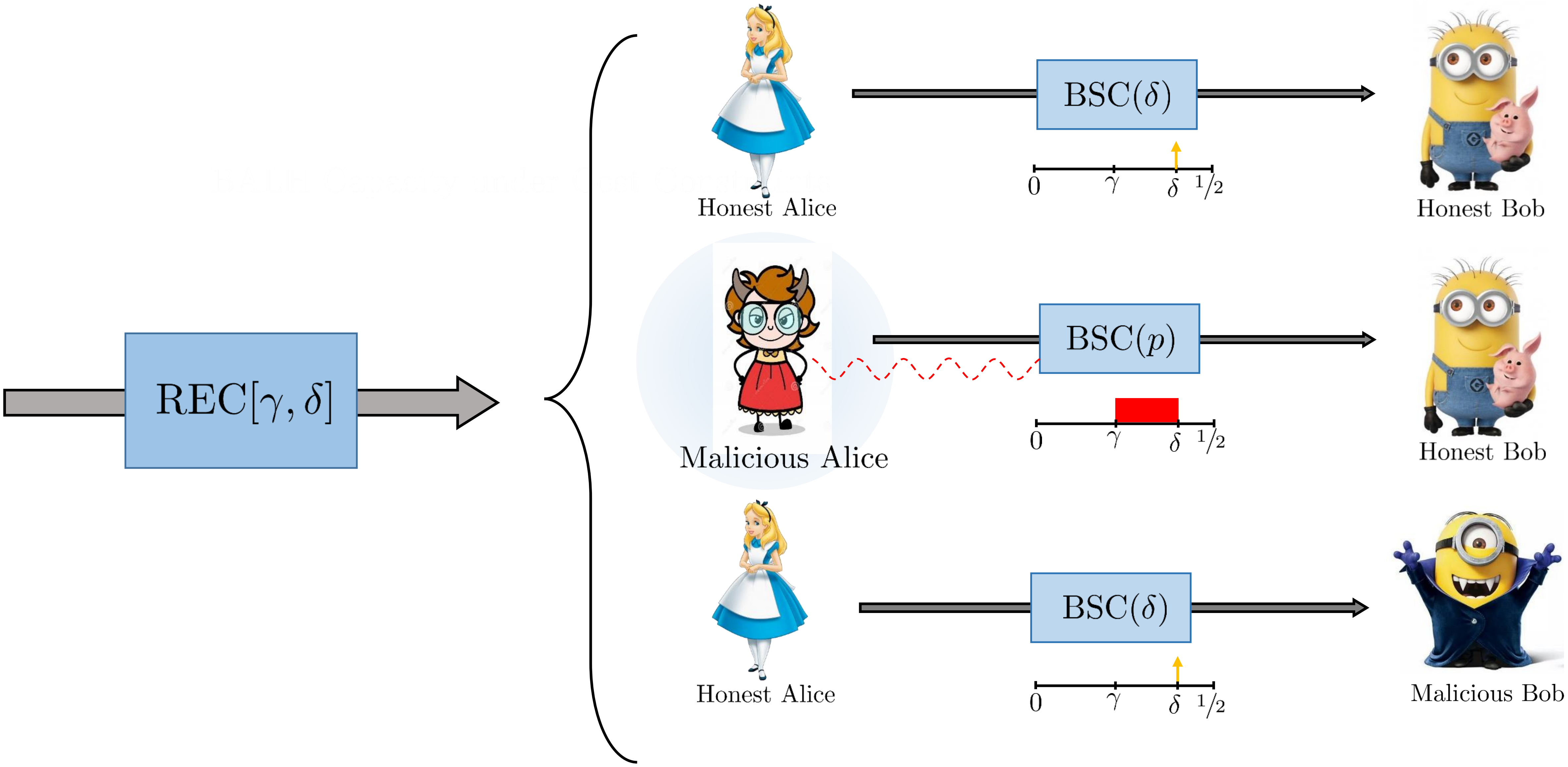

A better antenna lets Bob receive on a cleaner channel, unknown to Alice

# Elastic Noisy Channel

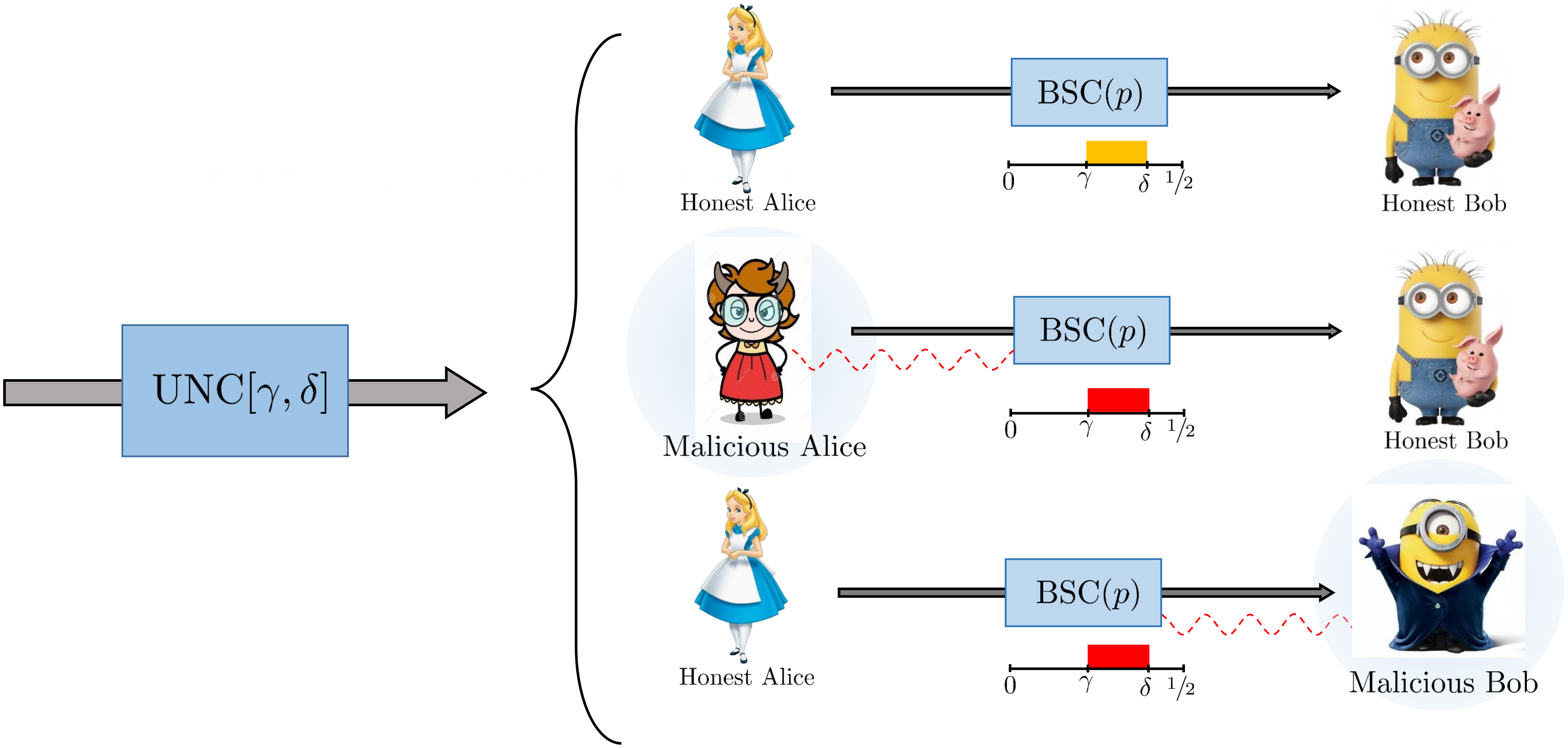
[Khurana et al, ‘16]



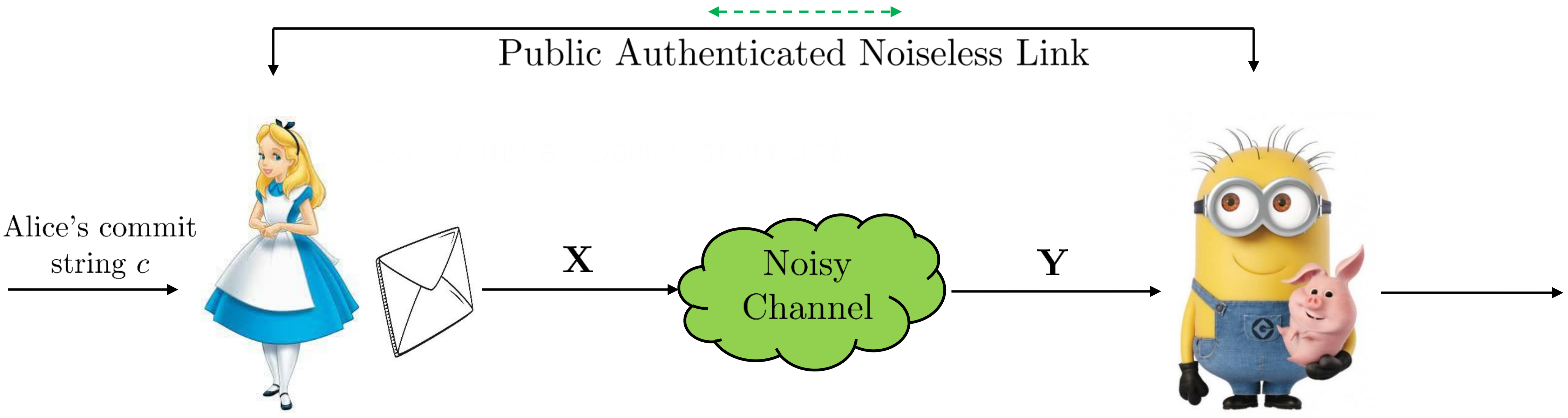
# Reverse Elastic Channel [Khurana et al, ‘16]



# Unfair Noisy Channel [Damgard et al, '98]



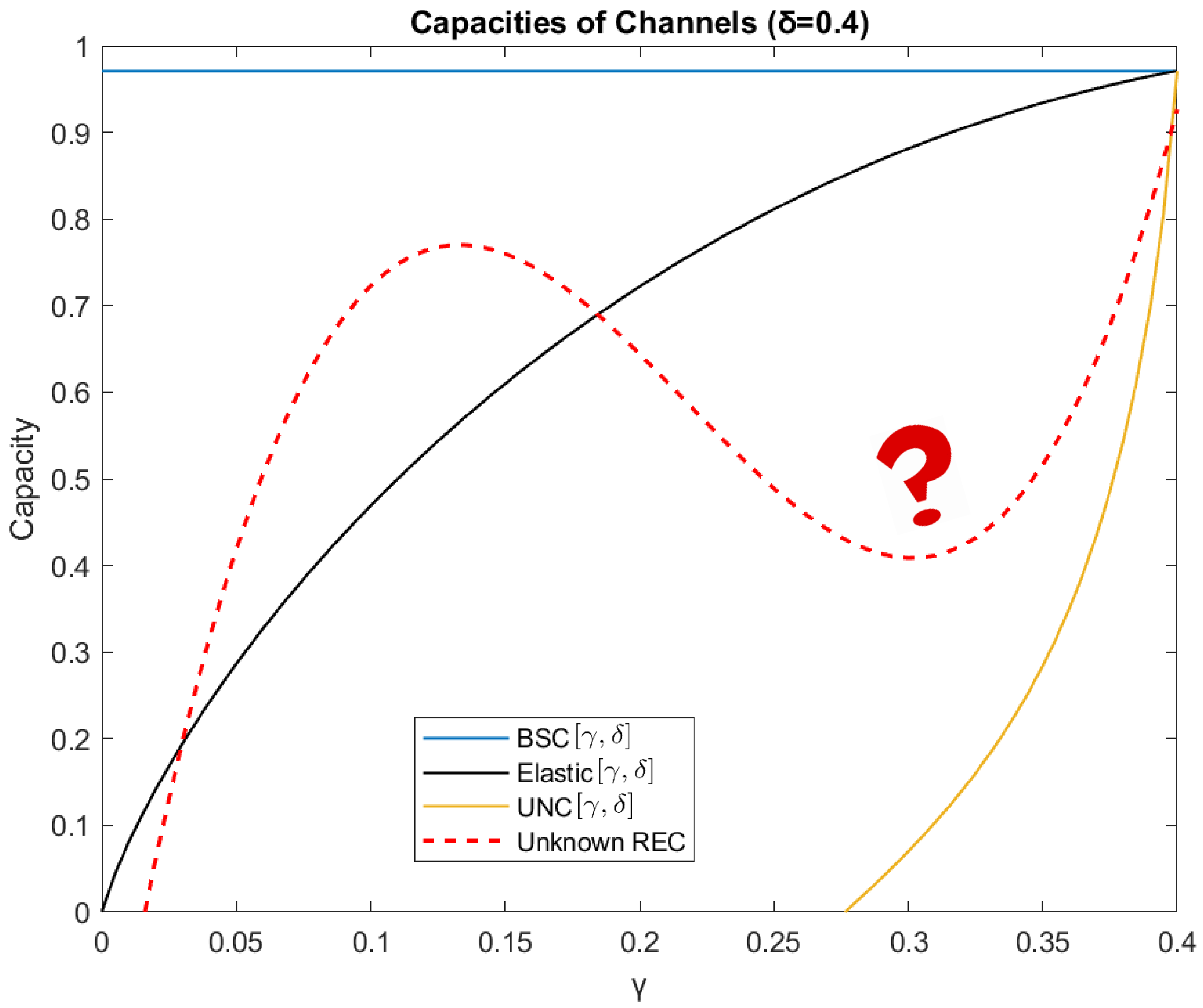
# Commitment Capacity




Maximise the length of $c$ given $n$ uses of the channel.

**Commitment Capacity:** measure of commitment throughput, i.e. how long we can make $c$

# Our Goal

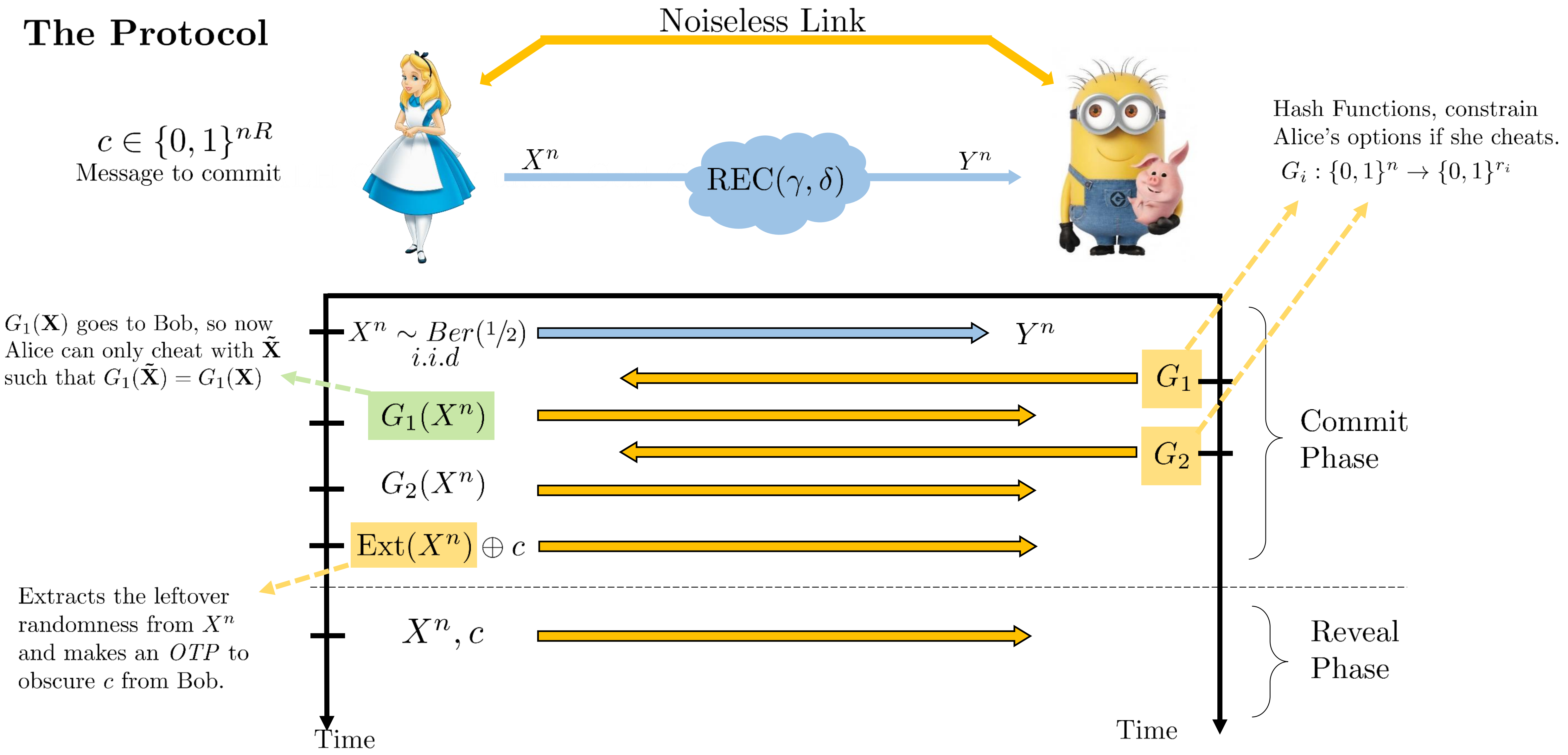



Known capacities of Channels:

- $C_{BSC} = \mathrm{H}(\delta)$
- $C_{ENC} = \mathrm{H}(\gamma)$
- $C_{UNC} = \mathrm{H}(\gamma)$ - $\mathrm{H}(\frac{\delta-\gamma}{1-2\gamma})$

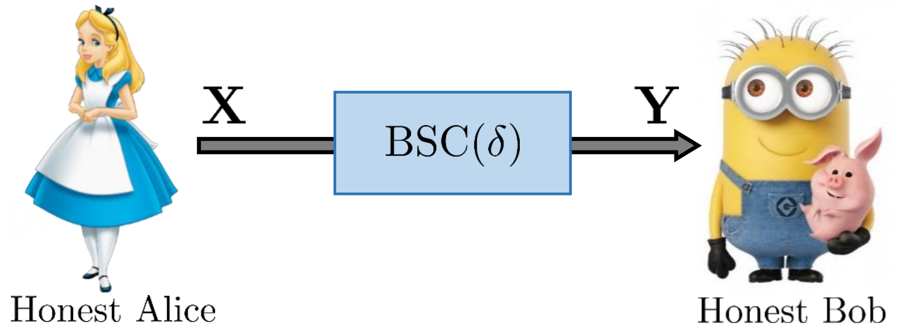
We wish to find the commitment capacity of REC.

# Achievability



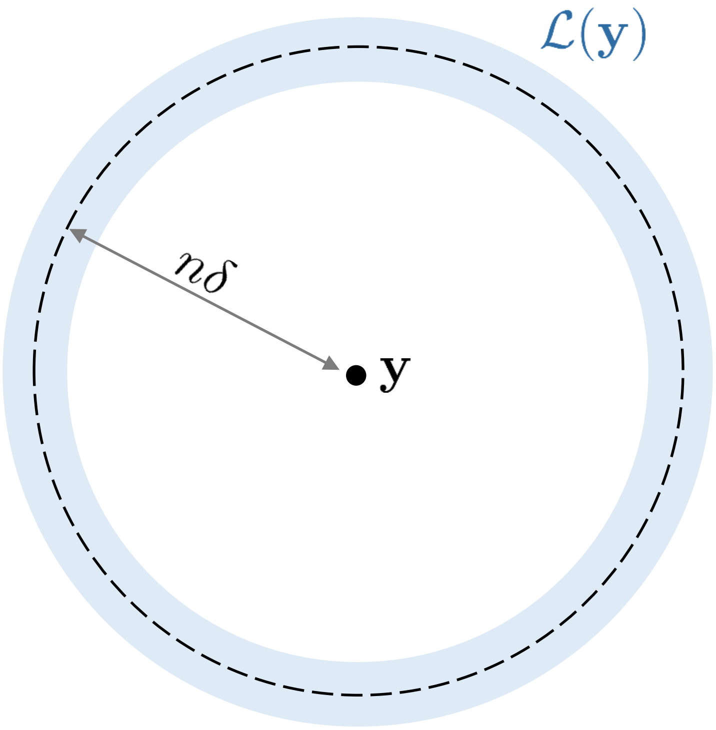
# Achievability

## Proof of Soundness




Bob prepares a list

$$\mathcal{L}(\mathbf{y}) = \left\{ \mathbf{x} \in \{0,1\}^n : d_H(\mathbf{x}, \mathbf{y}) \approx n\delta \right\}$$



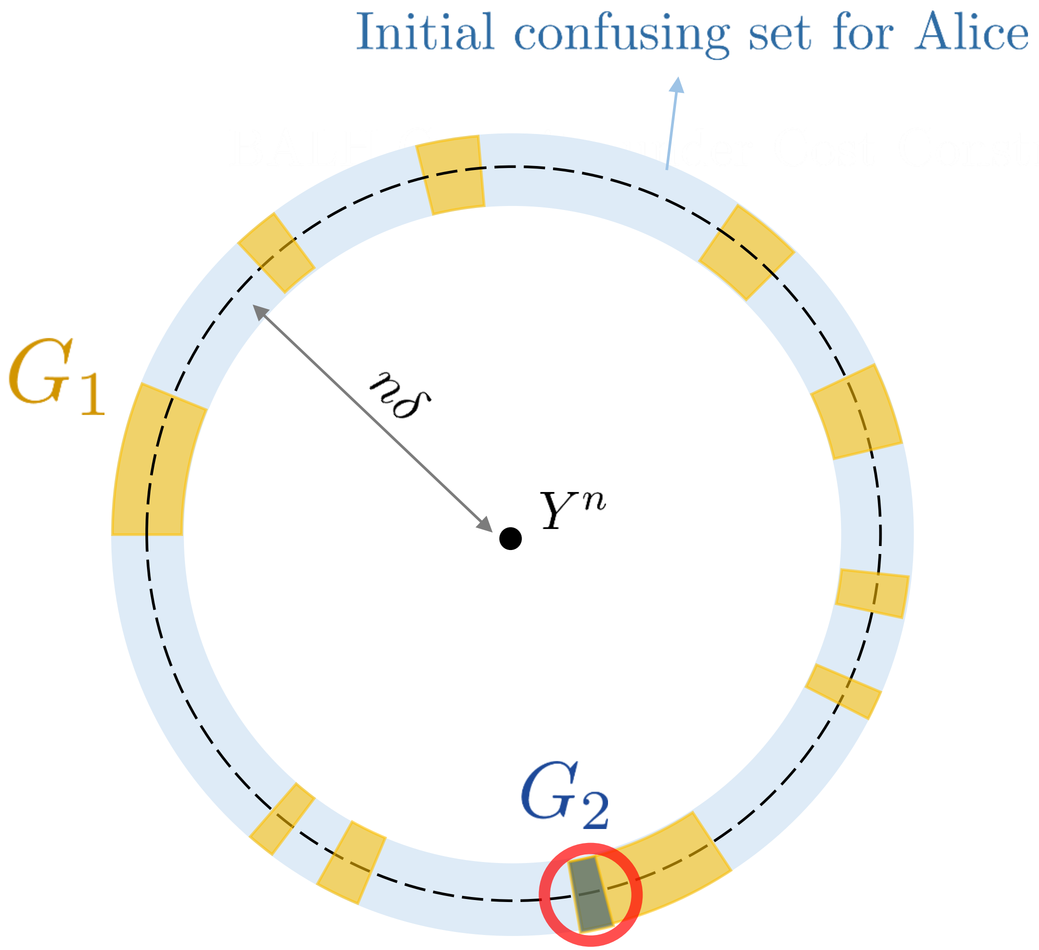

Protocol is sound if $\mathbf{X} \in \mathcal{L}(\mathbf{y})$ with high probability

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

$$P\big(\mathbf{X} \notin \mathcal{L}(\mathbf{y})\big) \xrightarrow{n \to \infty} 0$$

# Achievability

## Proof of Bindingness




The *one* remaining $X^n$ Alice can use

Bob knows $G_1(X^n)$ and $G_2(X^n)$, so Alice cannot “spoof” with any $X^n$ she wants

$G_1$ and $G_2$ limit the **number of strings Alice can cheat with:**

- Initially *exponential* in $n$.
- $G_1$: Constrains to *polynomial* in $n$.
- $G_2$: Constrains to *one* string.

## Proof of Concealment

$$\begin{aligned}
&H_\infty(\mathbf{X}|\mathbf{Y}, G_1(\mathbf{X}), G_1, G_2(\mathbf{X}), G_2) \\
&\quad \geq H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, G_1(\mathbf{X}), G_1, G_2(\mathbf{X}), G_2) \\
&\quad \geq (H(\mathbf{X}|\mathbf{Y}) - \zeta') - H_0(G_1(\mathbf{X})|G_2(\mathbf{X}), \mathbf{Y}, G_1, G_2) \\
&\qquad\quad - H_0(G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2) - \log(\epsilon_1^{-1}) \\
&\quad \geq n(H(\delta) - \zeta - H(\kappa) - \beta_1 - \beta_2) - \log(\epsilon_1^{-1})
\end{aligned}$$

*Chain rules of mutual entropy*
*Properties of Hash Functions*
*Continuity of smooth-min-entropy*

$\Downarrow$

$$\left| P_{\mathrm{Ext}(\mathbf{X}),\mathrm{Ext},\mathbf{Y},G_1(\mathbf{X}),G_1,G_2(\mathbf{X}),G_2} - P_{U_l,\mathrm{Ext},\mathbf{Y},G_1(\mathbf{X}),G_1,G_2(\mathbf{X}),G_2} \right| \leq 2^{-n\alpha_3}$$

*Generalised Leftover Hash Lemma*

$\Downarrow$

**Bias-based** secrecy $\Longrightarrow$ **Capacity-based** secrecy

# Converse

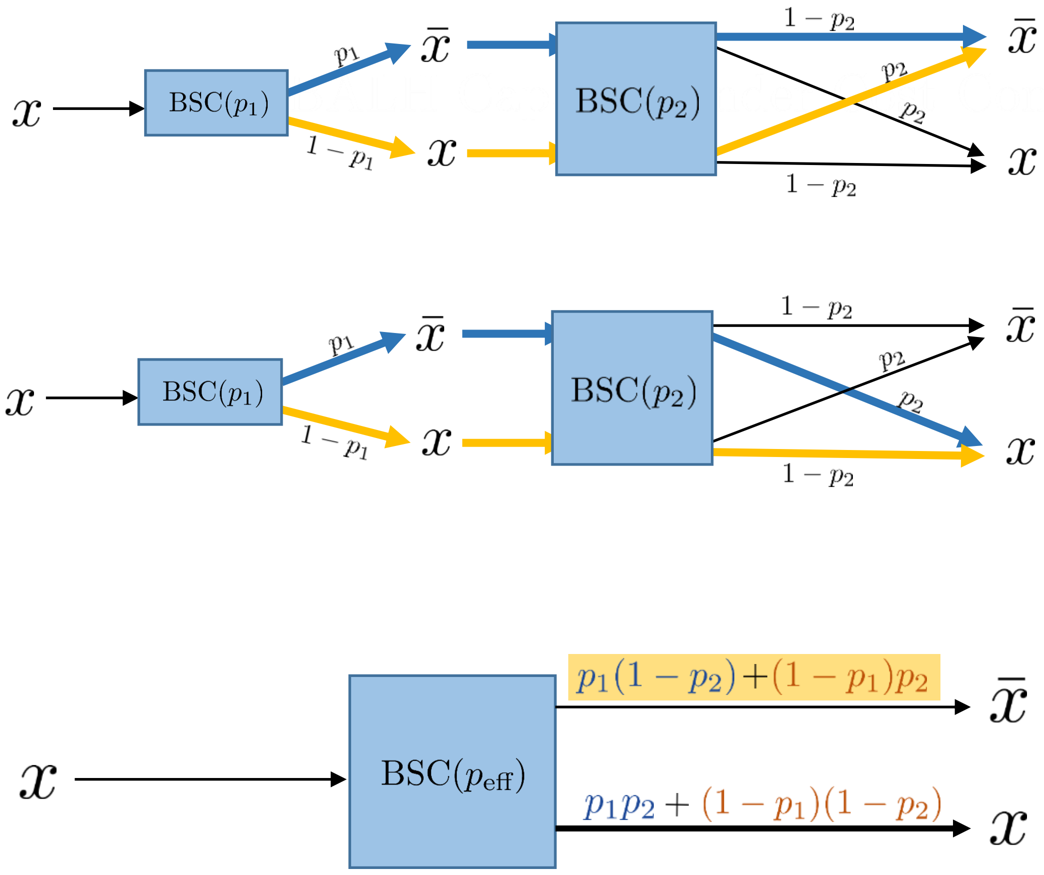
- Achievability: Prove rate $R \le h(\delta) - h(\theta)$ is possible
- Converse: Prove rate $R > h(\delta) - h(\theta)$ is **impossible**

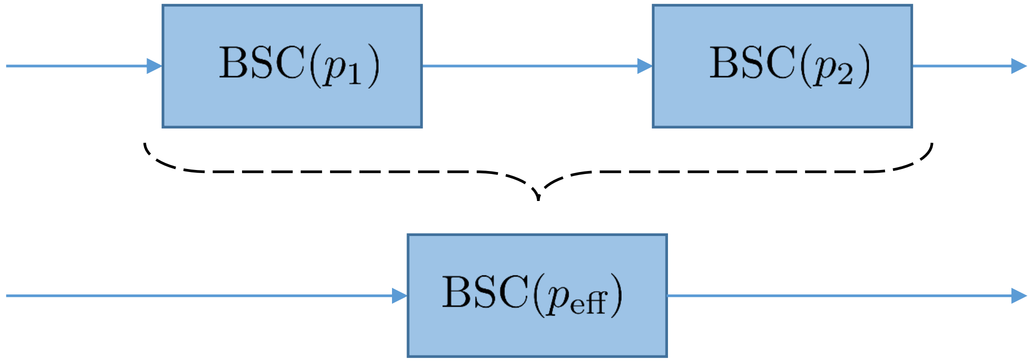
Pick a *specific cheating strategy* for Alice,
and see which rates we cannot achieve

Maybe put an achievability-impossibility curve here?

# Converse

## BSCs in Series



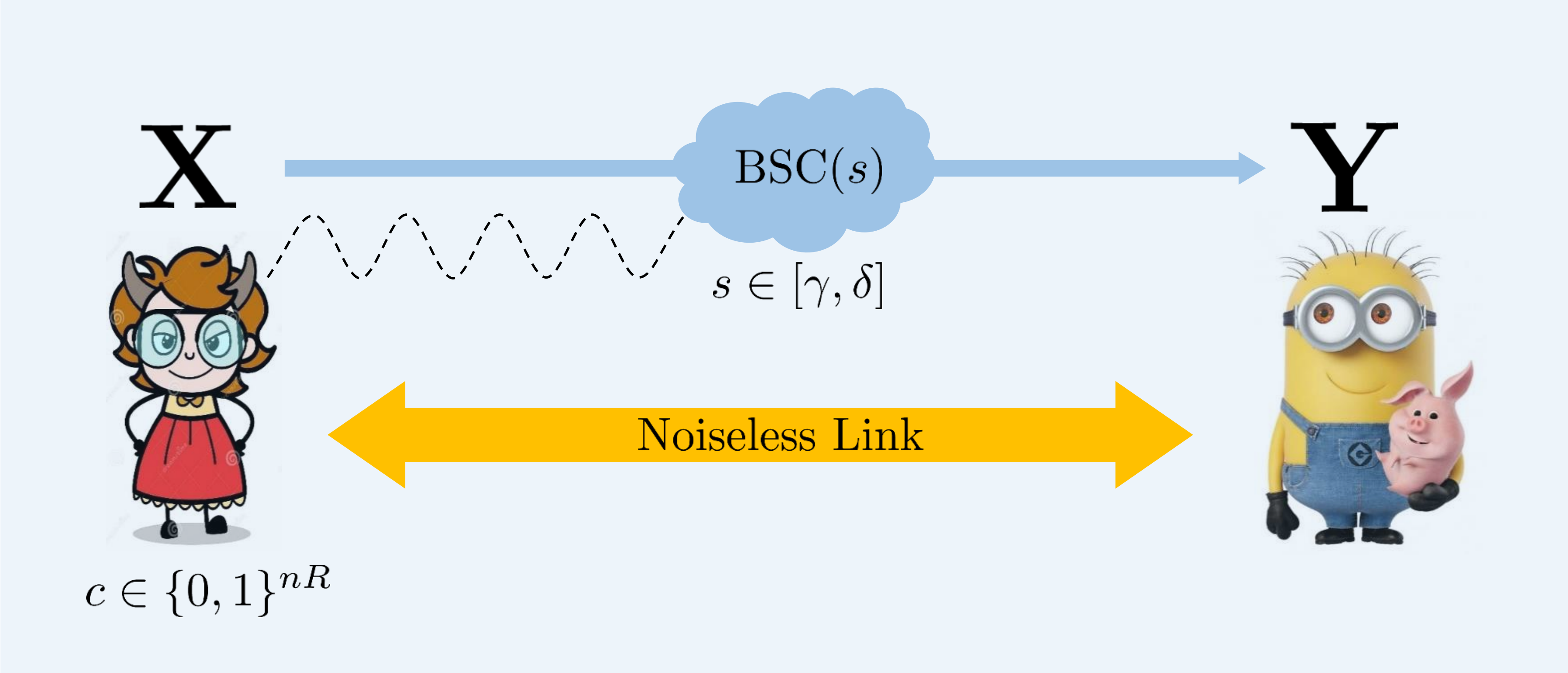

Where

$$p_{\text{eff}} = p_1 \circledast p_2 = p_1(1-p_2) + (1-p_1)p_2$$

$$p_2 = \frac{p_{\text{eff}} - p_1}{1 - 2p_1}$$

### Alice's Cheating Strategy

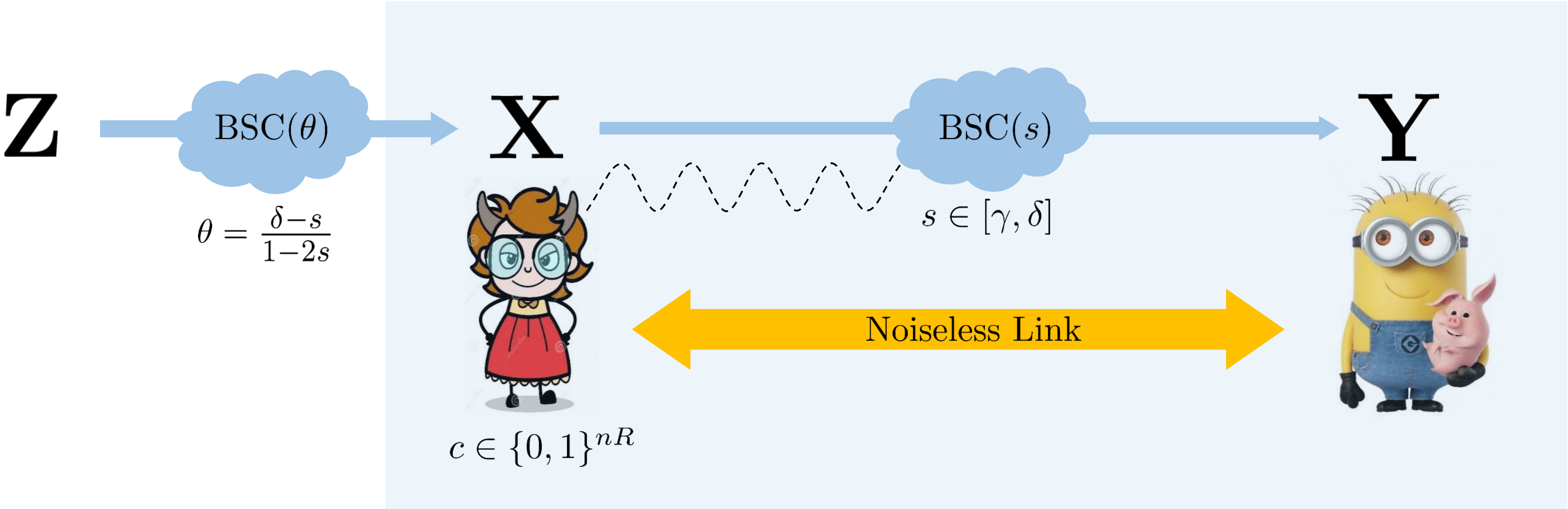
Alice sets the channel to be a BSC($s$), $s \in [\gamma, \delta]$
This allows her some room to cheat



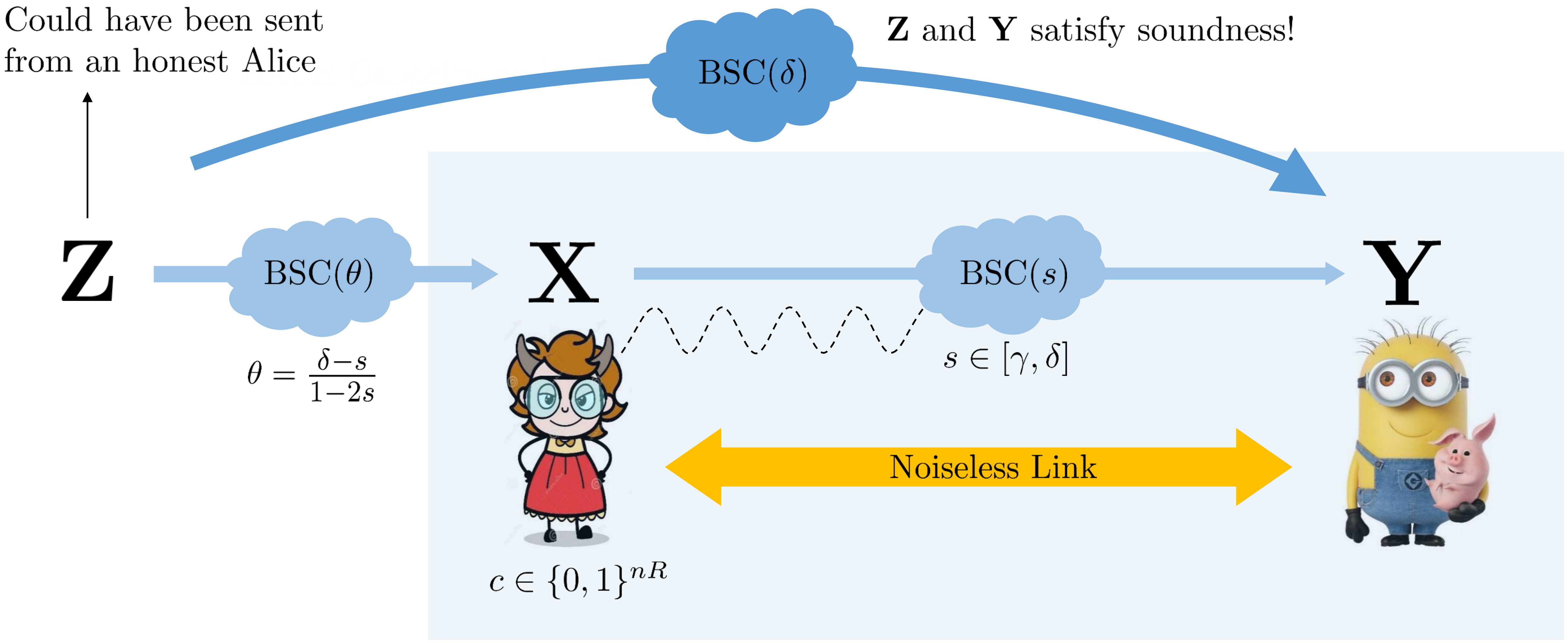
# Converse

### Alice's Cheating Strategy

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



**Alice's Cheating Strategy**



# Converse

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

$nR = H(C)$

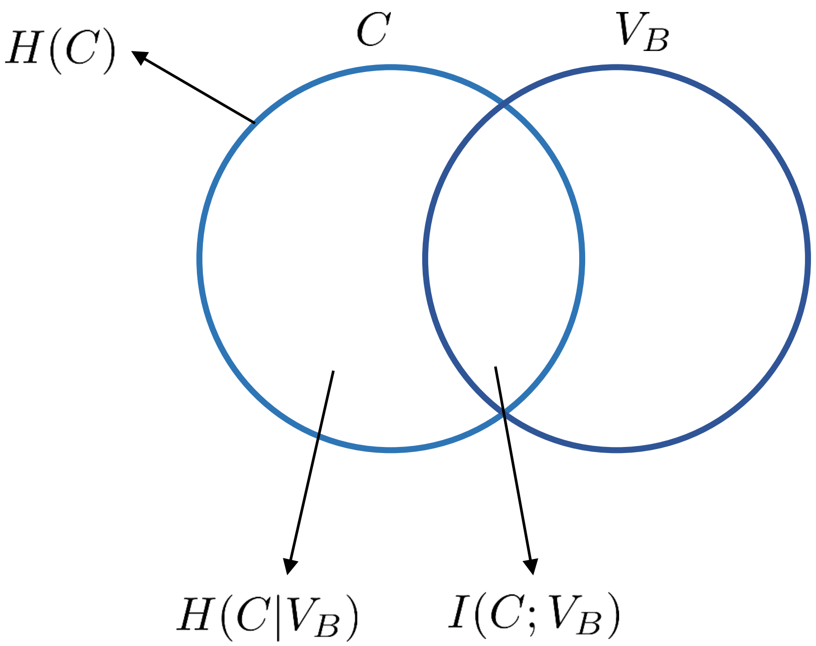
Because $C \in \{0,1\}^{nR}$

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

# Converse

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

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



# Converse

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

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

# Converse

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

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

Adding and subtracting

# Converse

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

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

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

# Converse

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

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

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

# Converse

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

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

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

# Converse

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

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

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

# Converse

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

$$nR = H(C)$$

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

# Converse

A rate $R$ scheme: $\epsilon_n$ – *sound*, $\epsilon_n$ – *concealing* and $\epsilon_n$ – *binding* $\left(\epsilon_n \xrightarrow{n\to\infty} 0\right)$

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

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

Using the result from Czisar and Korner:

# Converse

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

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

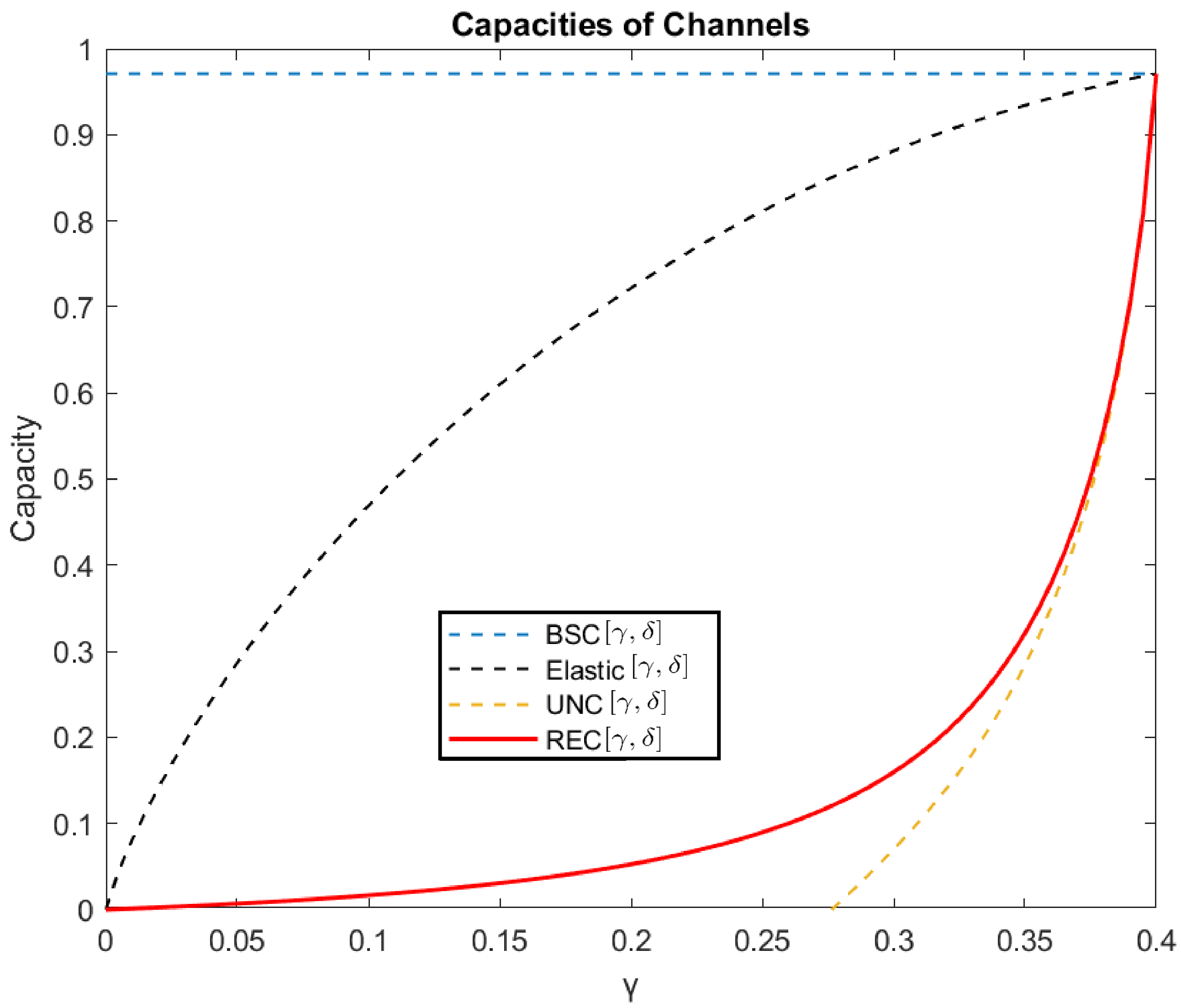
$$\implies R \leq I(\mathbf{X};\tilde{\mathbf{Z}}) - I(\mathbf{X};\mathbf{Y}) + \frac{\epsilon''}{n} + \frac{\epsilon}{n}$$

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

Let n grow sufficiently large.

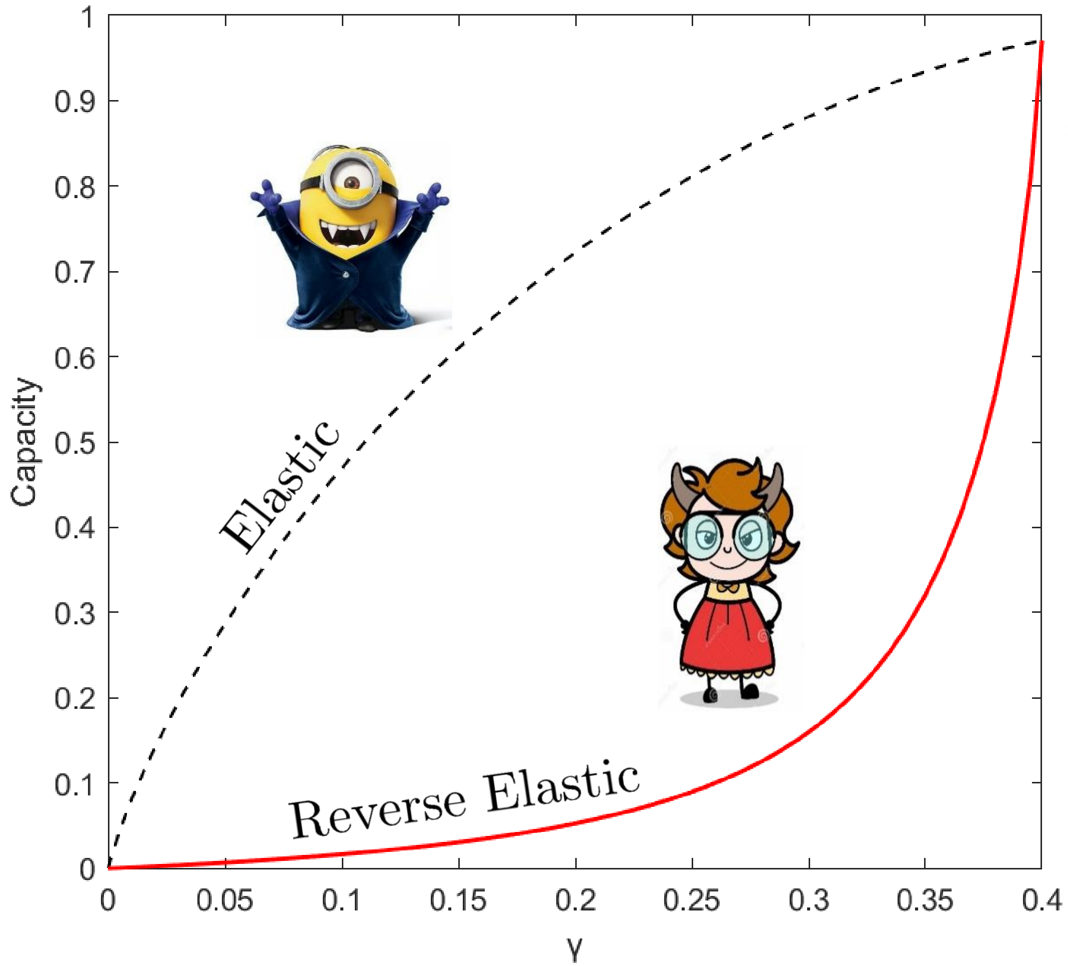
Because the inequality holds for *all* cheating behaviours of Alice, it must also hold for the minimum

# Result




$$C_{REC} = H(\delta) - H(\theta)$$

# Insights




Malicious Alice affects commitment capacity more than malicious Bob

The commitment problem is such that a malicious Bob can't really do much besides set the channel parameter because **Bob is not the one committing anything.**

END