CBCrypto
Eurocrypt 2025

Leveraging Spherical Codes for Commitment over Gaussian UNCs

Anuj K. Yadav
EPFL

Joint work with:

Amitalok Budkuley
IIT Kharagpur

Manideep Mamindlapally
QuSoft & University of Amsterdam

Commitment

Introduction

- Cryptographic Primitive
- Two Users - **Committer** *(Alice)* and **Verifier** *(Bob)*

Commitment

Introduction

- Cryptographic Primitive
- Two Users - **Committer** *(Alice)* and **Verifier** *(Bob)*
- Two Phases - **Commit Phase** followed by **Reveal Phase**

Commitment

Introduction

- Cryptographic Primitive
- Two Users - **Committer** *(Alice)* and **Verifier** *(Bob)*
- Two Phases - **Commit Phase** followed by **Reveal Phase**

- Security Guarantees: **Soundness**
  Concealment
  Bindingness

Commitment

History

- **[Blum '83]** : Commitment - Interactive exchange of messages **(Computationally secure)**

Computationally secure

(Secure under the assumption that
'atleast' one user
is computationally bounded)

Commitment

History

- **[Blum ’83]** : Commitment - Interactive exchange of messages **(Computationally secure)**
- Unconditionally secure Commitment - **IMPOSSIBLE**

Unless a **non-trivial** resource is used - noisy channel, shared randomness, etc.

Commitment

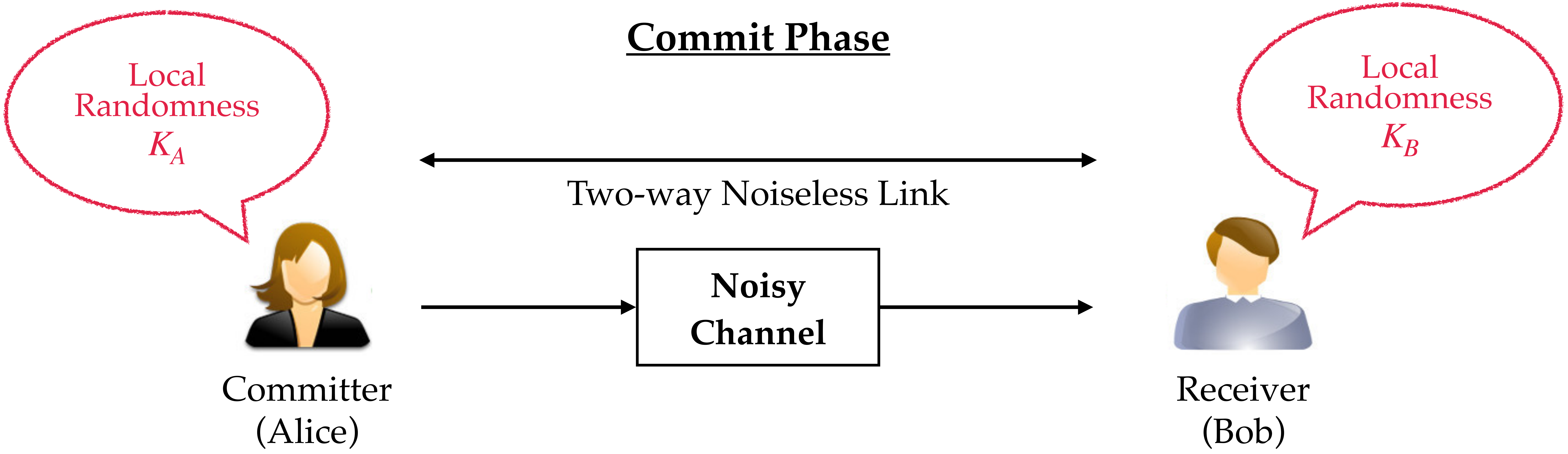
History

- **[Blum '83]** : Commitment - Interactive exchange of messages **(Computationally secure)**
- Unconditionally secure Commitment - via **NOISY CHANNELS**

- **[Crèpeau et al. '88]** : Unconditionally secure Commitment based on **Noisy** channel (BSC)
- **[Damgård et al. '99]** : Impossibility results on Commitment over Unfair Noisy Channel (UNC)
- **[Winter et al. '04]** : Characterized Commitment Capacity of Discrete Memoryless Channels
- **[Crèpeau et al. '20]** : Characterized Commitment Capacity of UNCs
- And others…

Unconditionally Secure Commitment

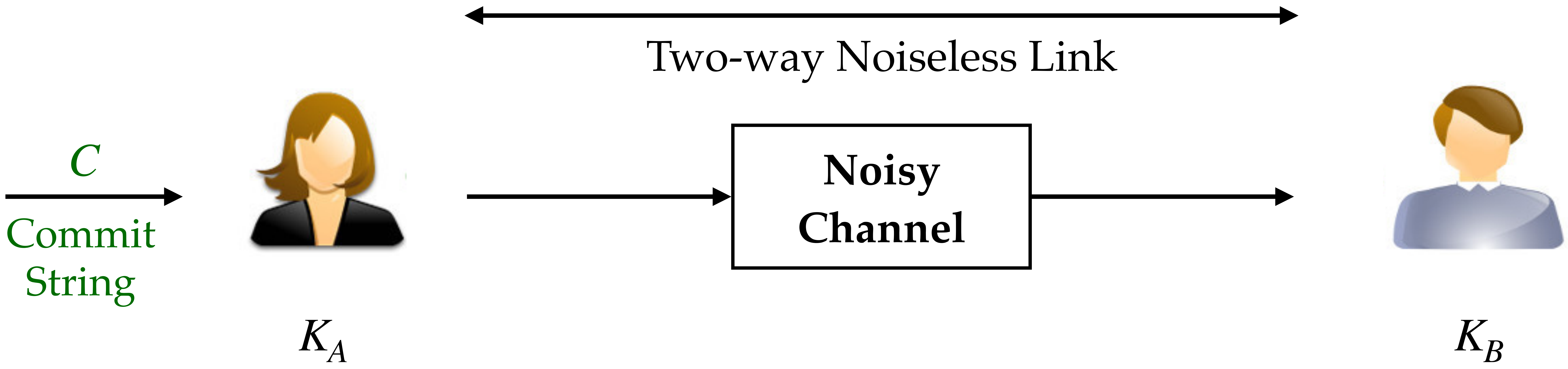
General Problem Setup



Unconditionally Secure Commitment

General Problem Setup

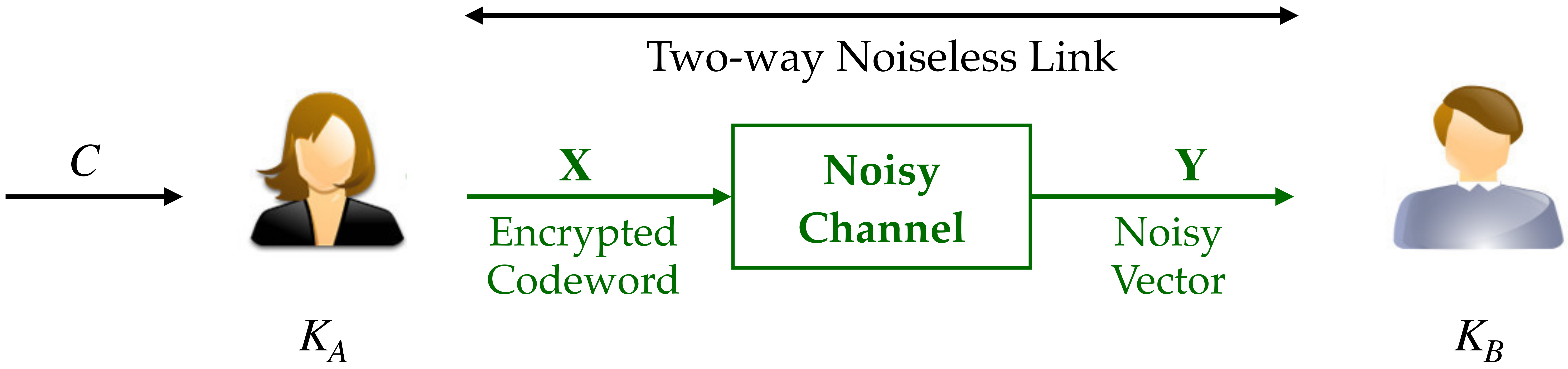
<u>Commit Phase</u>



Unconditionally Secure Commitment

General Problem Setup

Commit Phase

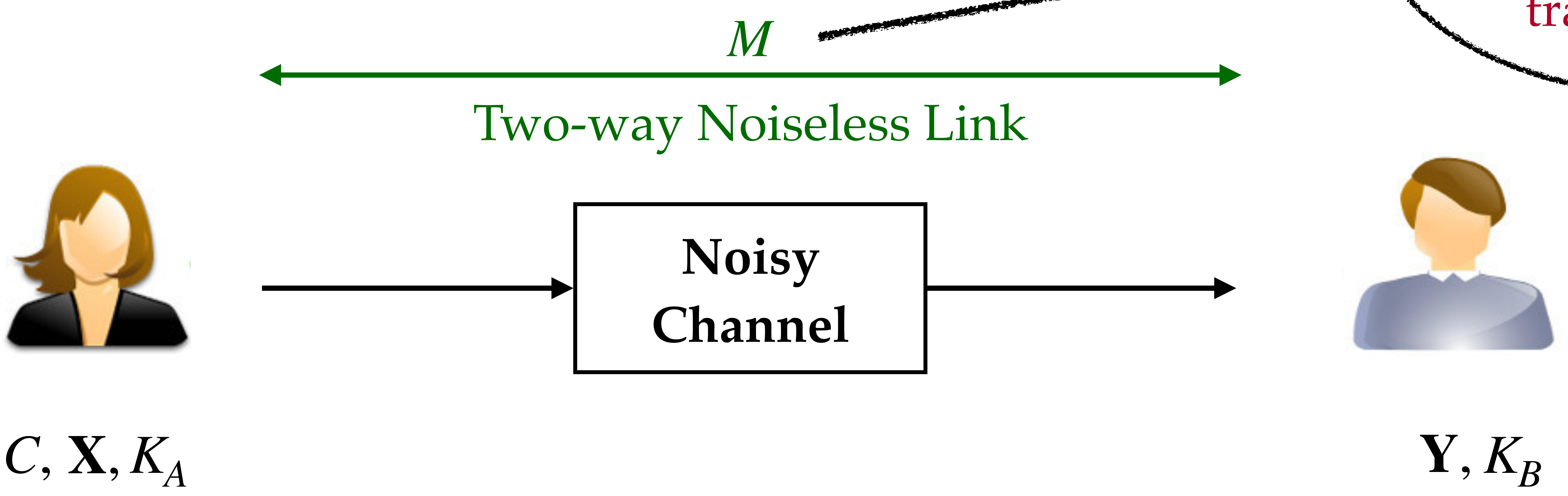


Unconditionally Secure Commitment

General Problem Setup

Can causally depend on noisy channel transmissions

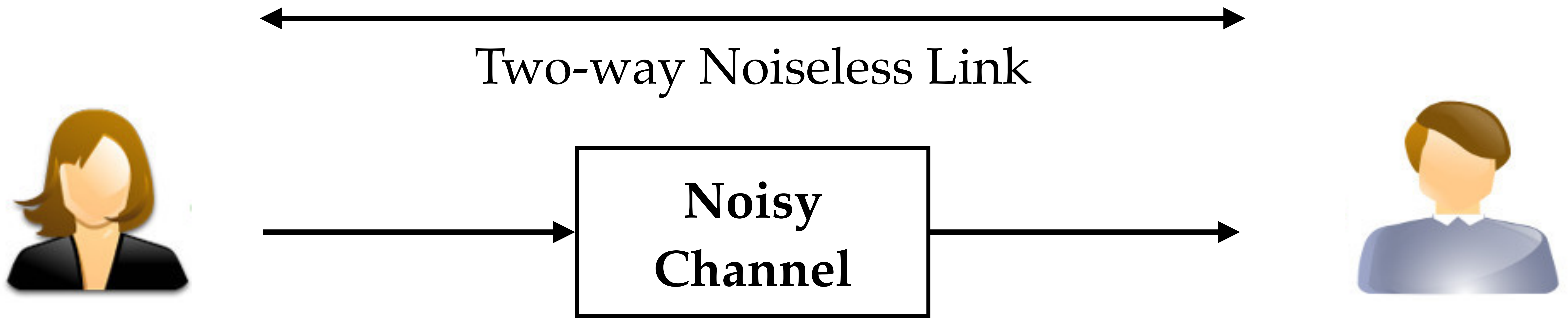
Commit Phase



Unconditionally Secure Commitment

General Problem Setup

Commit Phase

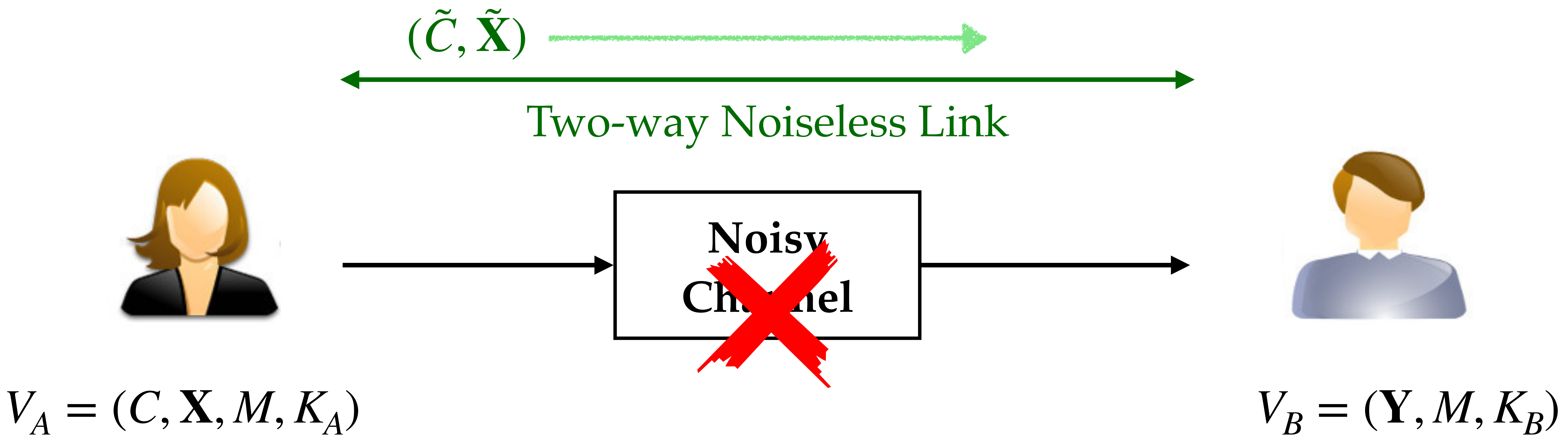


$V_A = (C, \mathbf{X}, M, K_A)$ $V_B = (\mathbf{Y}, M, K_B)$

Unconditionally Secure Commitment

General Problem Setup

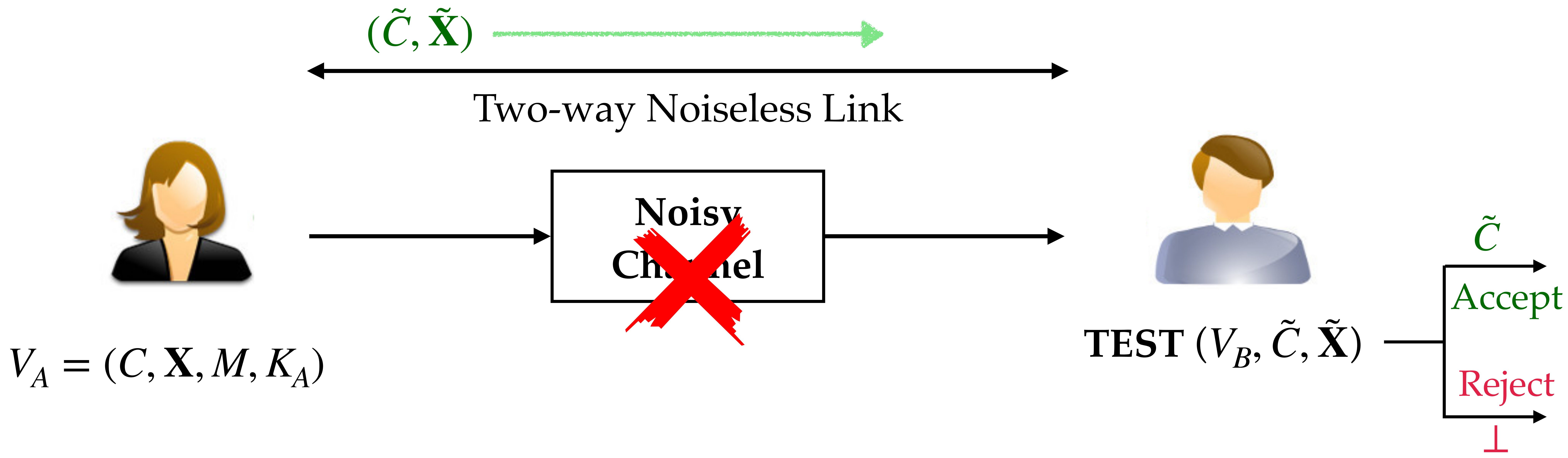
Reveal Phase



Unconditionally Secure Commitment

General Problem Setup

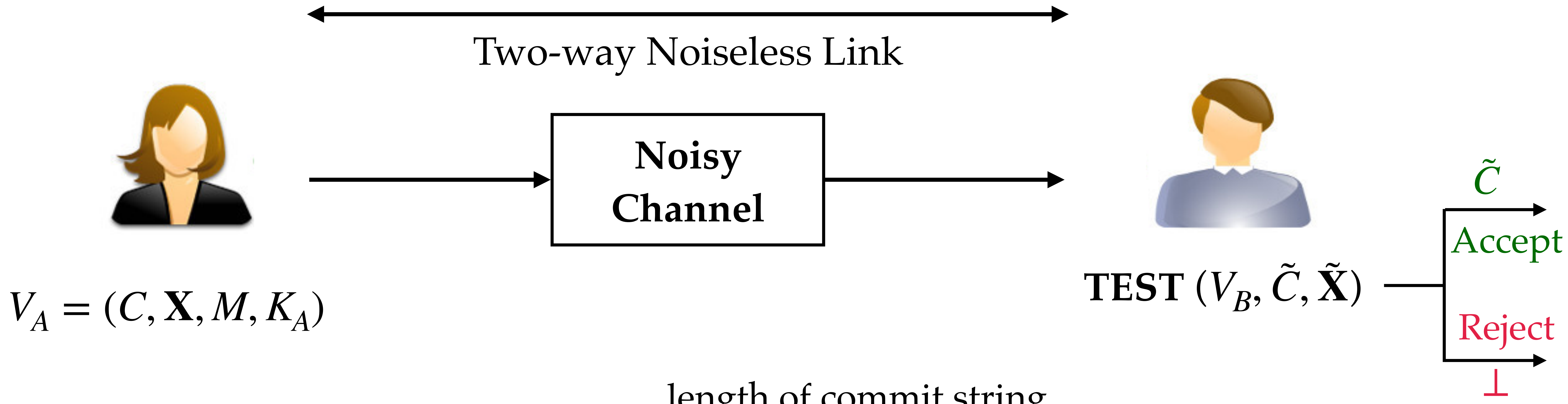
Reveal Phase



Unconditionally Secure Commitment

Commitment Rate

<u>Reveal Phase</u>



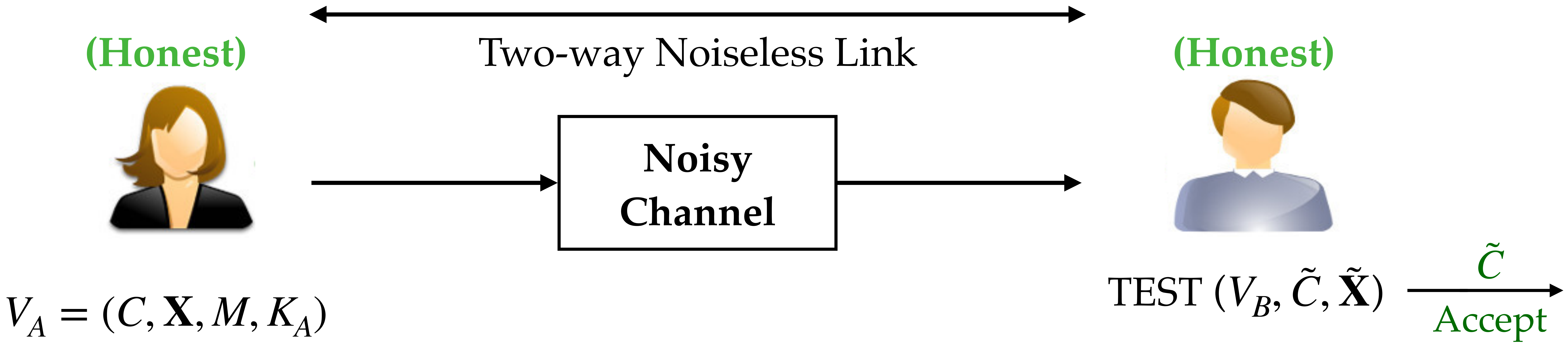
$$\text{Commitment Rate} := \frac{\text{length of commit string}}{\text{No. of uses of noisy channel}}$$

Unconditionally Secure Commitment

Security Guarantees

Soundness

(In reveal phase)



$$\mathbf{P}\left(\text{TEST}\,(V_B, \tilde{C}, \tilde{\mathbf{X}}) = \text{reject}\right) \leq \epsilon$$

Unconditionally Secure Commitment

Security Guarantees

<u>**Concealment**</u>

<u>(In commit phase)</u>

(Honest)

Two-way Noiseless Link

Noisy Channel

(Malicious)

$V_A = (C, \mathbf{X}, M, K_A)$

$V_B = (\mathbf{Y}, M, K_B)$

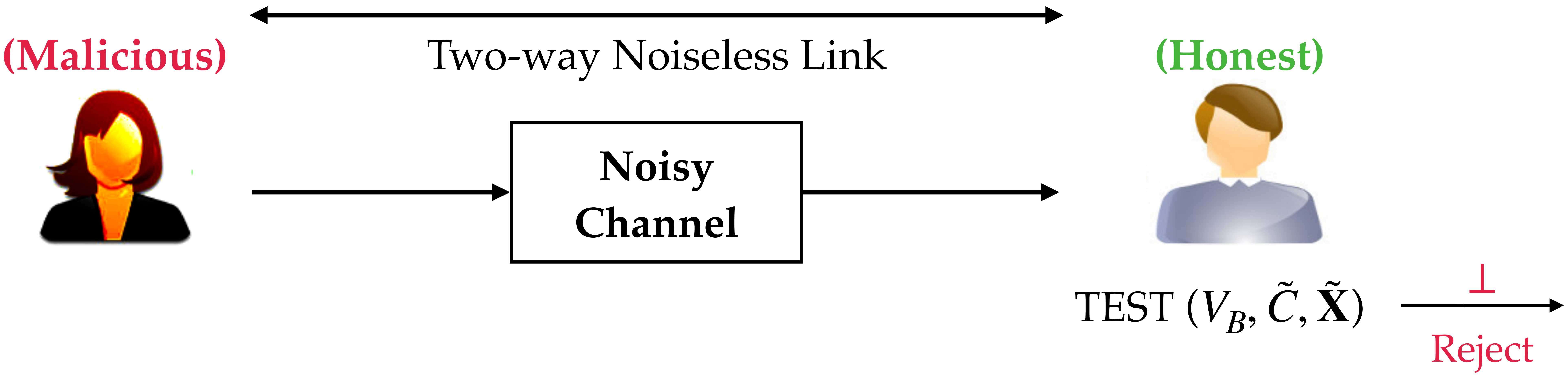
Mutual Information : $I(C; V_B) \leq \epsilon$

Unconditionally Secure Commitment

Security Guarantees

<u>Bindingness</u>

<u>(In reveal phase)</u>



$$\mathbf{P}\left\{(\text{TEST }(V_B, \tilde{C}, \tilde{\mathbf{X}}) = \text{accept}) \,\&\, (\text{TEST }(V_B, \hat{C}, \hat{\mathbf{X}}) = \text{accept})\right\} \leq \epsilon$$

$$\forall (\tilde{C}, \tilde{X}), (\hat{C}, \hat{X}) \text{ s.t. } \tilde{C} \neq \hat{C}$$

Unconditionally Secure Commitment

Our Goal : Commitment Capacity

- Recall, Commitment Rate $(\mathbb{R}) := \dfrac{\text{length of commit string}}{\text{No. of uses of noisy channel}}$

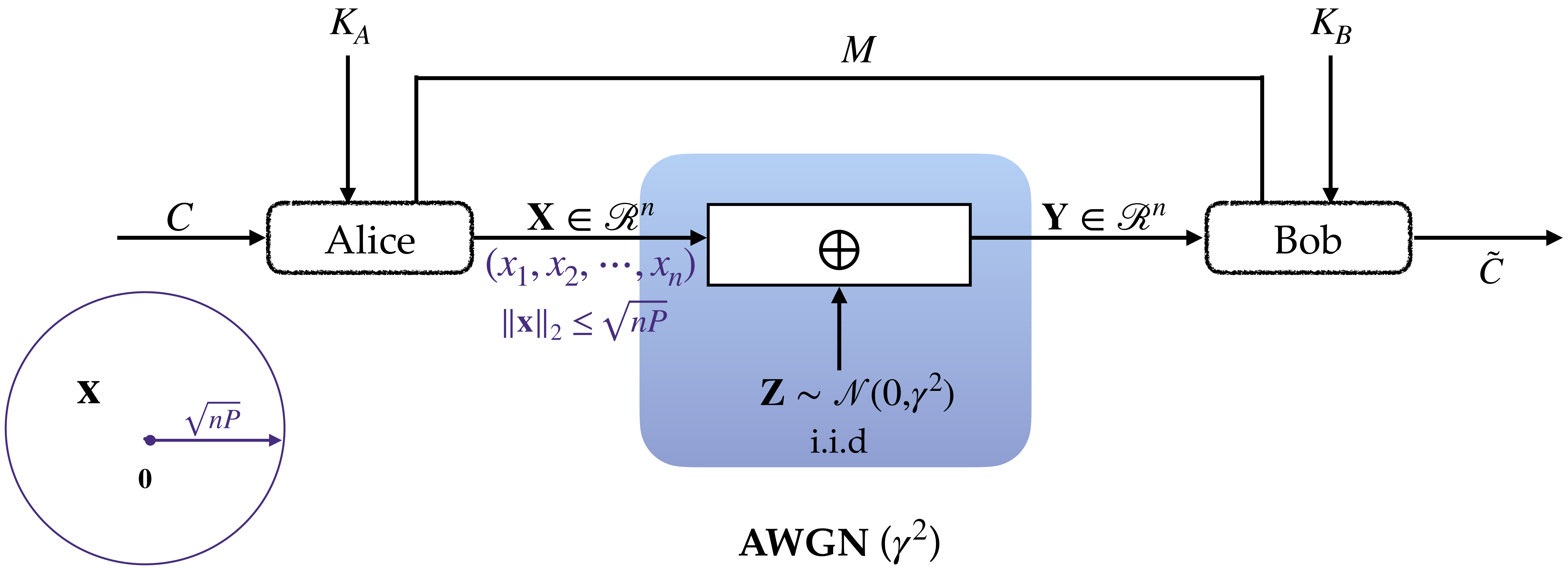
- Commitment Capacity $(\mathbb{C}) : = \sup \{ \mathbb{R} : \mathbb{R} \text{ is achievable} \}$
- A rate $\mathbb{R}$ is achievable if

  $\exists$ a commitment scheme with rate $\mathbb{R}$ that satisfies all the three security guarantees

- **Goal :** To study the 'possibility of commitment' and the 'commitment capacity' of Gaussian UNCs.

Unconditionally Secure Commitment

Commitment over AWGN Channel (with power constraint P)



N-dimensional Euclidean ball

Unconditionally Secure Commitment

Commitment over AWGN Channel

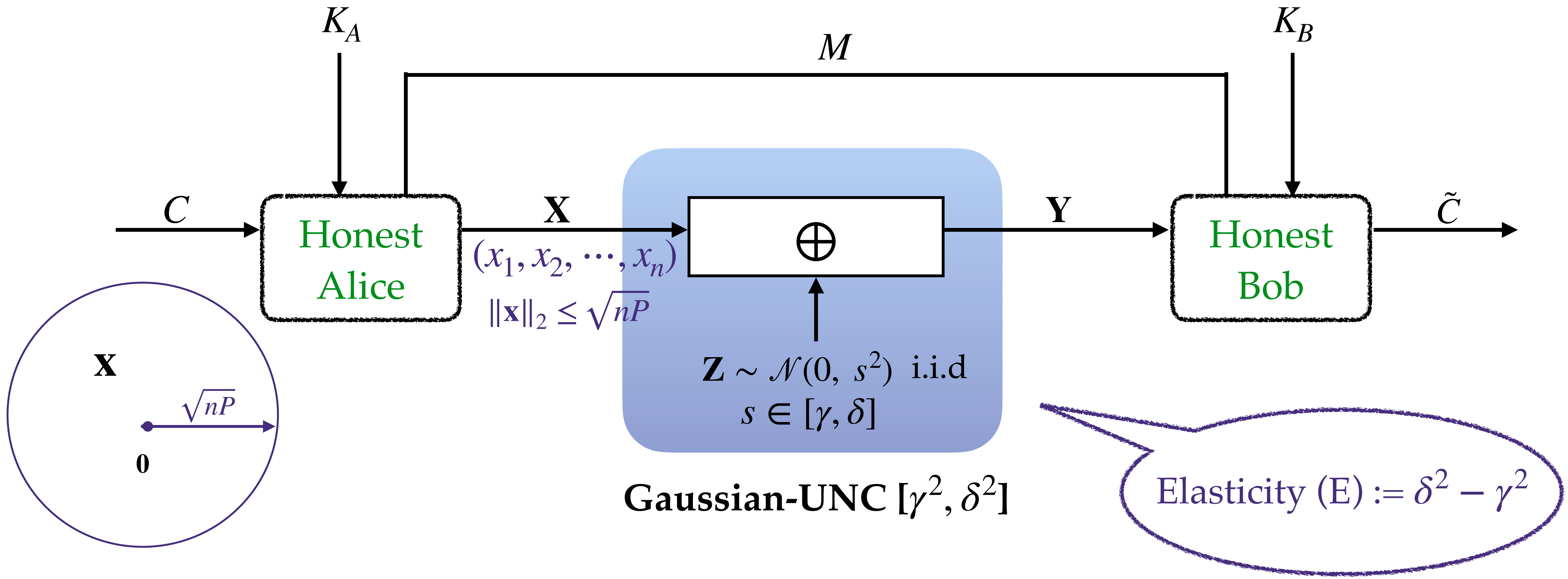
Theorem:

The Commitment Capacity of an AWGN channel (even with finite power constraint) is **Infinite**.

A. C. A. Nascimento, J. Barros, S. Skludarek and H. Imai, "The Commitment Capacity of the Gaussian Channel Is Infinite," in *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2785-2789, June 2008, doi: 10.1109/TIT.2008.921686.

Unconditionally Secure Commitment

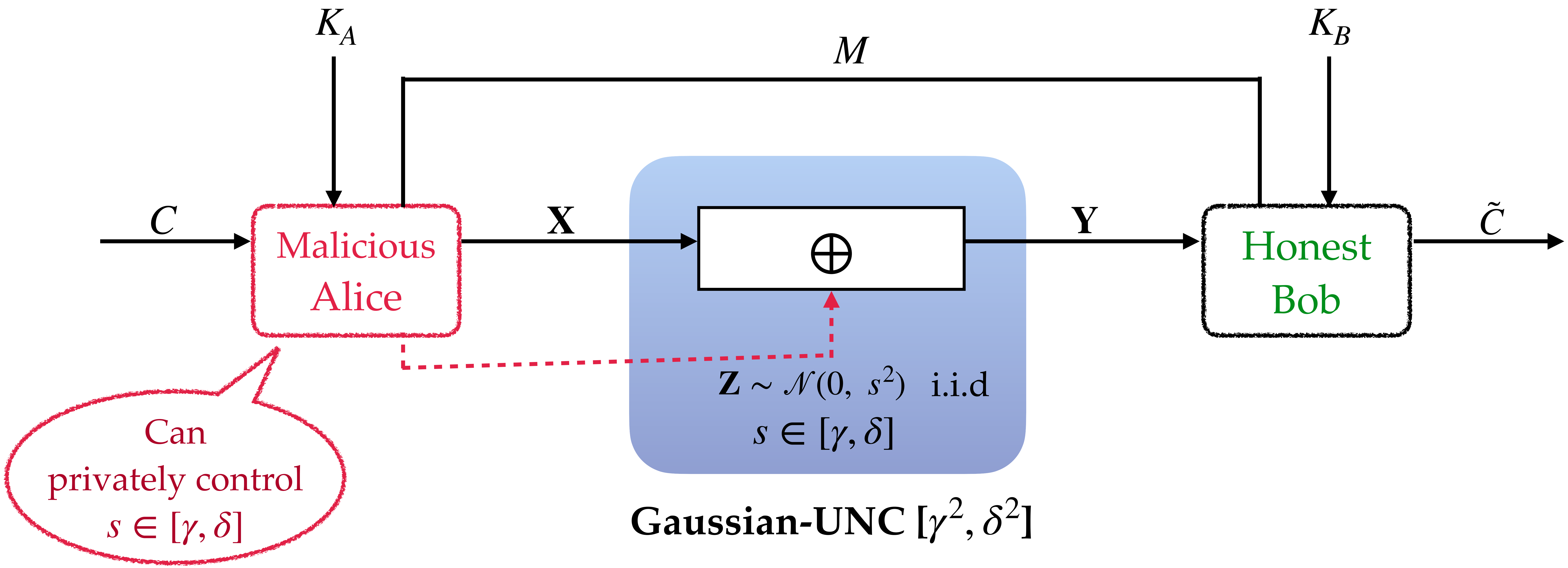
Gaussian Unfair Noisy Channel (Gaussian - UNC)



N-dimensional Euclidean ball

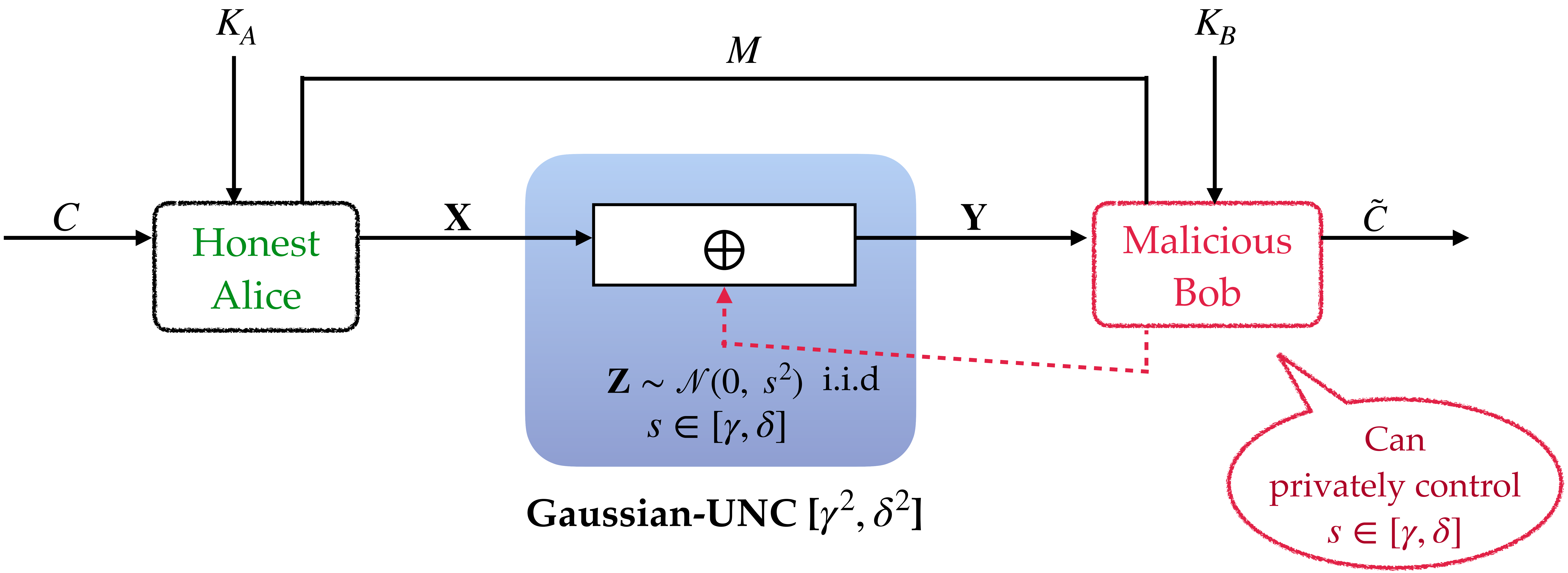
Unconditionally Secure Commitment

Gaussian Unfair Noisy Channel (Gaussian - UNC)



Unconditionally Secure Commitment

Gaussian Unfair Noisy Channel (Gaussian - UNC)



Commitment over Gaussian UNC

Main Result - Impossibility Result

<u>**Theorem:**</u>

> For Gaussian-UNC $[\gamma^2, \delta^2]$, with unconstrained input $P \to \infty$, the commitment capacity is zero (i.e., $\mathbb{C} = 0$), if $\delta^2 \geq 2\gamma^2$

Budkuley, A., Joshi, P., Mamindlapally, M. and Yadav, A.K., 2023, June. On the (im) possibility of commitment over gaussian unfair noisy channels. In *2023 IEEE International Symposium on Information Theory (ISIT)* (pp. 483-488).

Commitment over Gaussian UNC

Main Result - Achievability (Lower Bound)

Theorem:

For Gaussian-UNC $[\gamma^2, \delta^2]$, with $P > 0$, the positive rate commitment is possible if

$$\delta^2 < \left(1 + \frac{P}{P + \gamma^2}\right)\gamma^2$$

and the commitment capacity is lower bounded by:

$$\mathbb{C} \geq \mathbb{C}_L := \frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right)$$

Commitment over Gaussian UNC

Main Result - Converse (Upper Bound)

Theorem:

For Gaussian-UNC $[\gamma^2, \delta^2]$, with $P > 0$, the commitment capacity is upper bounded by

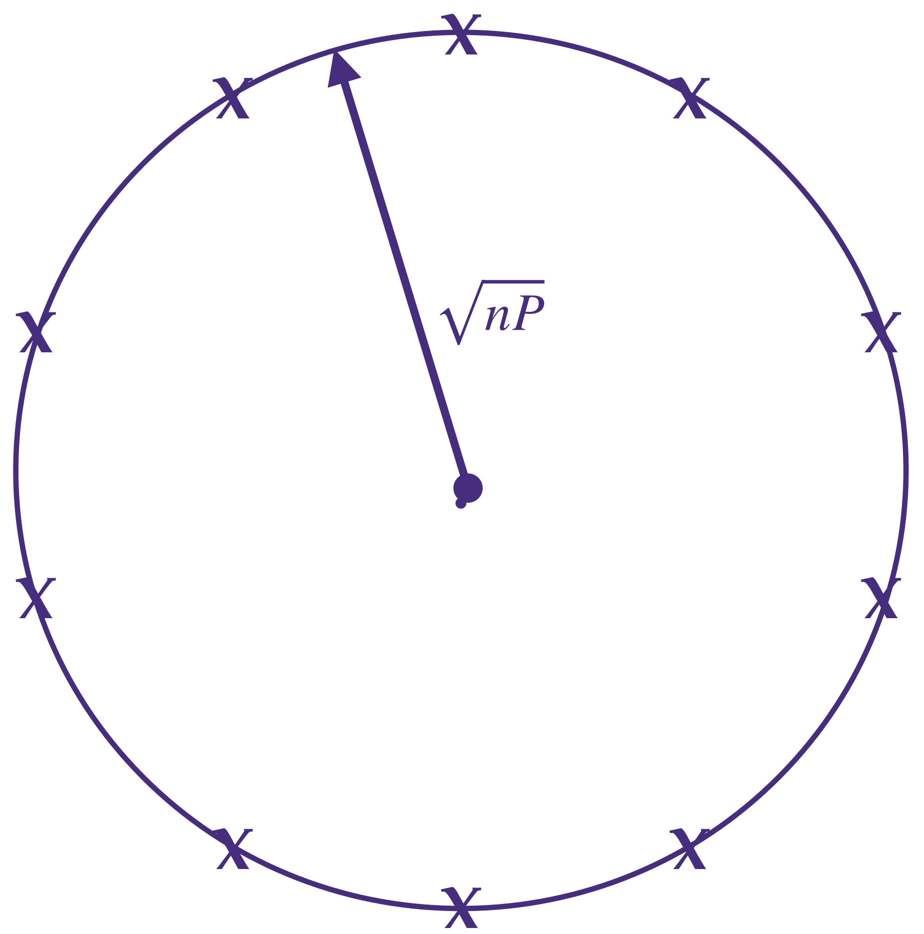
$$\mathbb{C} \leq \mathbb{C}_U := \frac{1}{2} \log \left(1 + \frac{P}{E} \right) - \frac{1}{2} \log \left(1 + \frac{P}{\gamma^2} \right)$$

if $\delta^2 < 2\gamma^2$.

Commitment over Gaussian UNC

Achievability Scheme - Spherical code

- For $0 < \alpha < 1$, $\exists$ a code $\mathscr{C} \subseteq \mathbb{R}^n$ s.t. :
  - $d_{min}(\mathscr{C}) = \alpha^2 nP$
  - $\bar{R} \geq \frac{1}{2}\log\left(\frac{1}{1-(1-\alpha/2)^2}\right)$



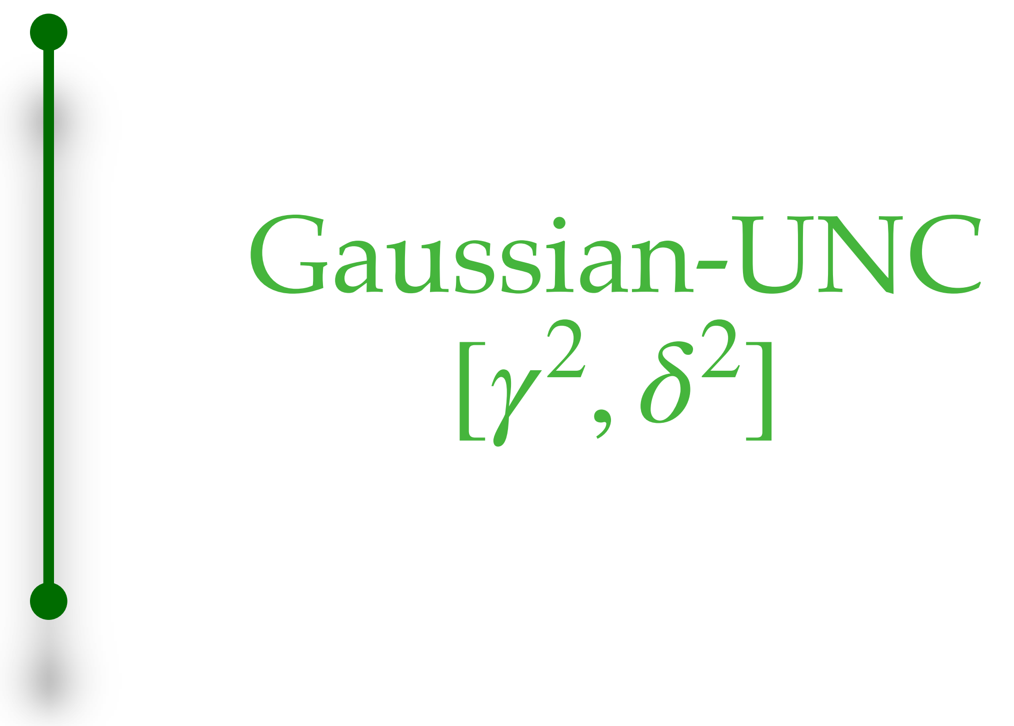
- Uniformly dist. codewords on the surface of a hypersphere
- Spherical code $(\mathscr{C}, \psi, \phi)$ with 'equi-normed' codewords
- $\mathscr{C} \subseteq \mathbb{R}^n, \psi : \{0,1\}^m \to \mathbb{R}^n, \phi : \mathbb{R}^n \to \{0,1\}^m \cup \{0\}$
- $(\mathscr{C}, \psi, \phi)$ - shared between both Alice and Bob

Commitment over Gaussian UNC

Achievability Scheme - Commit Phase

- Alice wants to commit to a string, say C
- Picks $U^m \in \{0,1\}^m \sim$ ber (1/2) i.i.d
- Transmits $\mathbf{X} = \psi(u^m)$ to Bob, he receives $\mathbf{Y}$.

  Bob creates a list $\mathscr{L}(y)$ of codewords :



$$\mathscr{L}(\mathbf{y}) := \{\mathbf{x} \in \mathscr{C} : n(\gamma^2 - \alpha_1) \leq \|\mathbf{x} - \mathbf{y}\|_2^2 \leq n(\delta^2 + \alpha_1)\}$$

Commitment over Gaussian UNC

Achievability Scheme - Commit Phase

- Alice wants to commit to a string, say C.
- Picks $U^m \in \{0,1\}^m \sim$ ber (1/2) i.i.d
- Transmits $\mathbf{X} = \psi(u^m)$ to Bob, he receives $\mathbf{Y}$.

Gaussian-UNC
$[\gamma^2, \delta^2]$

- Two rounds of Hash challenge from Bob to Alice.

Two-way
Noiseless Link

$G_1 : \{0,1\}^m \rightarrow \{0,1\}^{n(\bar{R}+\frac{1}{2}\log(\frac{E}{P})+\beta_1)}$

$G_1(u^m)$

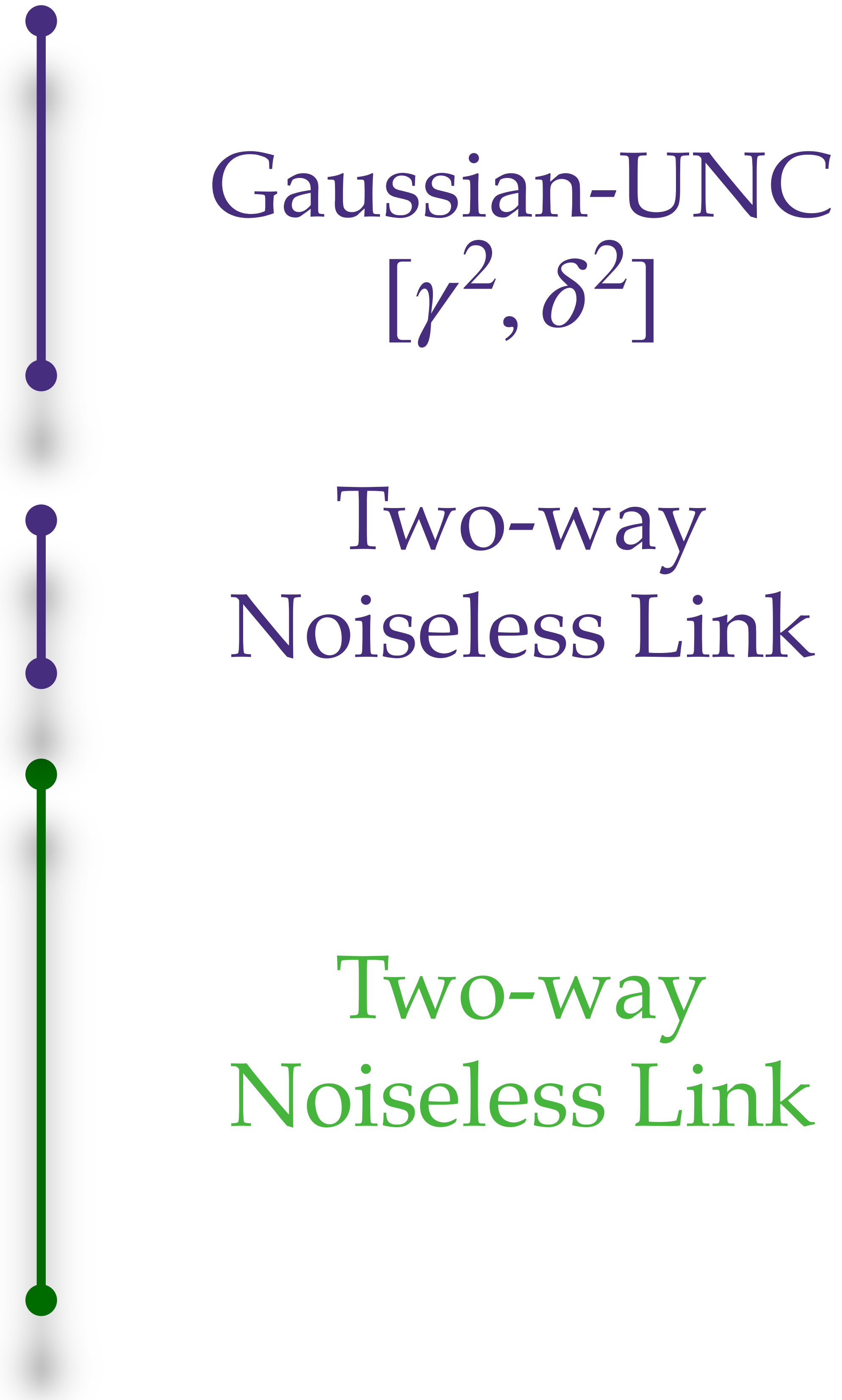
$G_2 : \{0,1\}^m \rightarrow \{0,1\}^{n\beta_2}$

$G_2(u^m)$

Commitment over Gaussian UNC

Achievability Scheme - Commit Phase

- Alice wants to commit to a string, say C.
- Picks $U^m \in \{0,1\}^m \sim$ ber $(1/2)$ i.i.d
- Transmits $\mathbf{X} = \psi(u^m)$ to Bob, he receives $\mathbf{Y}$.
- Two rounds of Hash challenge from Bob to Alice.
- Randomness Extractor (one-time pad with C) from Alice to Bob.

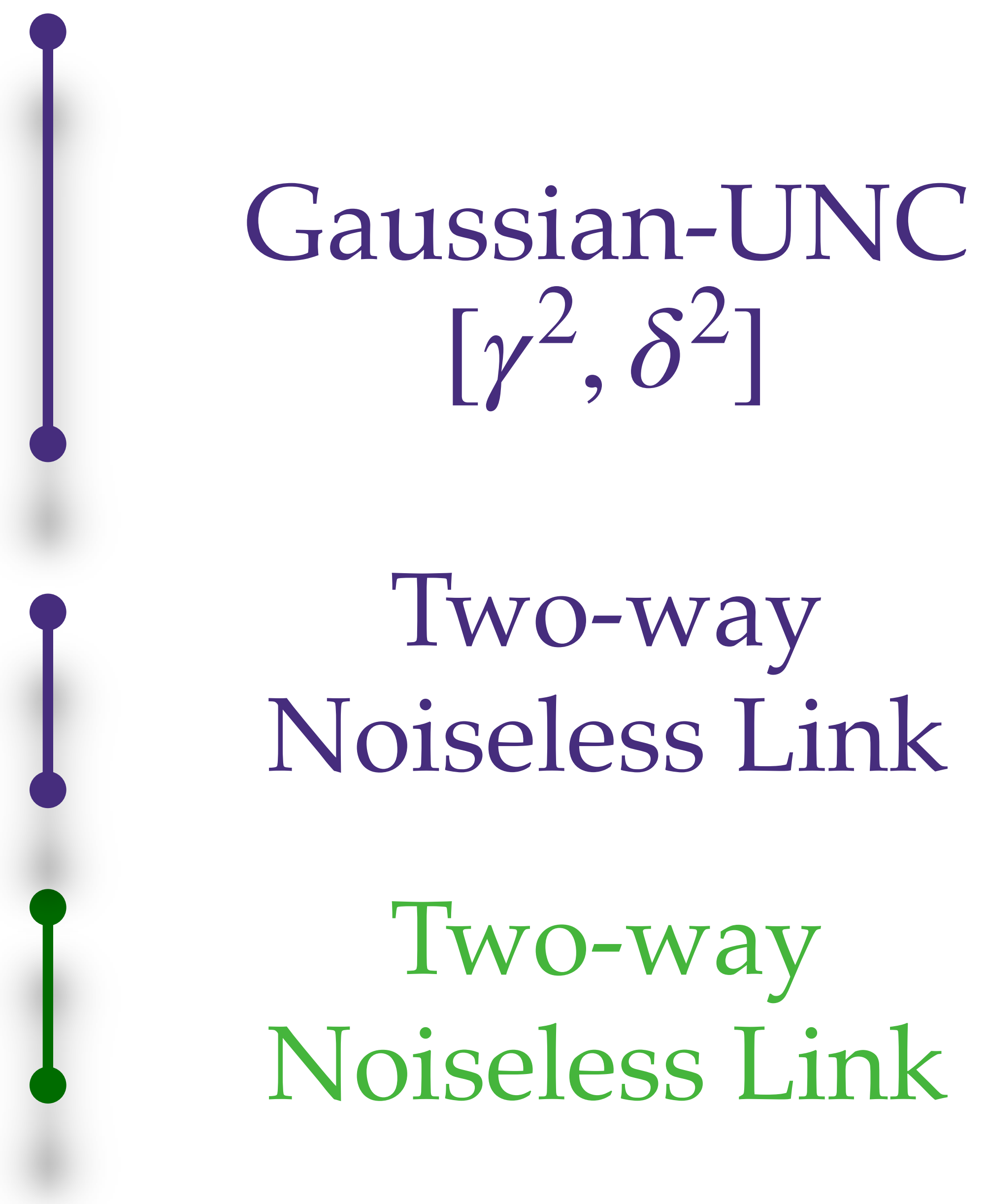


Commitment over Gaussian UNC

Achievability Scheme - Commit Phase

- Alice wants to commit to a string, say C.
- Picks $U^m \in \{0,1\}^m \sim$ ber $(1/2)$ i.i.d
- Transmits $\mathbf{X} = \psi(u^m)$ to Bob, he receives $\mathbf{Y}$.
- Two rounds of Hash challenge from Bob to Alice.
- Randomness Extractor (one-time pad with C) from Alice to Bob.

- $V_A = (c, u^m, \mathbf{x}, G_1, G_2, \text{Ext})$
- $V_B = (\mathbf{y}, G_1, G_1(u^m), G_2, G_2(u^m), \text{Ext}, Q)$



Commitment over Gaussian UNC

Achievability Scheme - Reveal Phase

- Alice reveals $(\tilde{c}, \tilde{u}^m)$ to Bob.
- Bob performs tests to accept / reject $\tilde{c}$.

Two-way Noiseless Link

$\longrightarrow$ **Typicality Test**

Check : $\psi(\tilde{u}^m) \in \mathscr{L}(\mathbf{y})$?

$\longrightarrow$ **Hash Challenge Test**

Check : $G_1(\tilde{u}^m) = G_1(u^m)$ and $G_2(\tilde{u}^m) = G_2(u^m)$?

$\longrightarrow$ **OTP Test**

Check : $\tilde{c} \oplus \mathrm{Ext}(\tilde{u}^m) = Q$?

Commitment over Gaussian UNC

Achievability Scheme - Security Guarantees

- Alice wants to commit to a string, say C.
- Picks $U^m \in \{0,1\}^m \sim$ ber (1/2) i.i.d
- Transmits $\mathbf{X} = \psi(u^m)$ to Bob, he receives $\mathbf{Y}$.
- Two rounds of Hash challenge from Bob to Alice.
- Randomness Extractor (one-time pad with C) from Alice to Bob.

Guarantees
Bindingness against
malicious Alice

Commitment over Gaussian UNC

Achievability Scheme - Security Guarantees

- Alice wants to commit to a string, say C.
- Picks $U^m \in \{0,1\}^m \sim$ ber (1/2) i.i.d
- Transmits $\mathbf{X} = \psi(u^m)$ to Bob, he receives $\mathbf{Y}$.

- Two rounds of Hash challenge from Bob to Alice.

- Randomness Extractor (one-time pad with C) from Alice to Bob.

Guarantees **Concealment** against malicious Bob

Commitment over Gaussian UNC

Summary of Results

Unconstrained Input

$(P \to \infty)$

$\delta^2 \geq 2\gamma^2$

Impossibility Result:

Commitment Capacity, $\mathbb{C} = 0$

$\delta^2 < 2\gamma^2$

Achievability:

$$\mathbb{C}_L = \lim_{P\to\infty} \left\{ \frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right) \right\}$$

Converse:

$$\mathbb{C}_U = \lim_{P\to\infty} \left\{ \frac{1}{2}\log\left(1 + \frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right) \right\}$$

Thus, $\mathbb{C} = \mathbb{C}_L = \mathbb{C}_U = \frac{1}{2}\log\left(\frac{\gamma^2}{E}\right)$

Commitment over Gaussian UNC

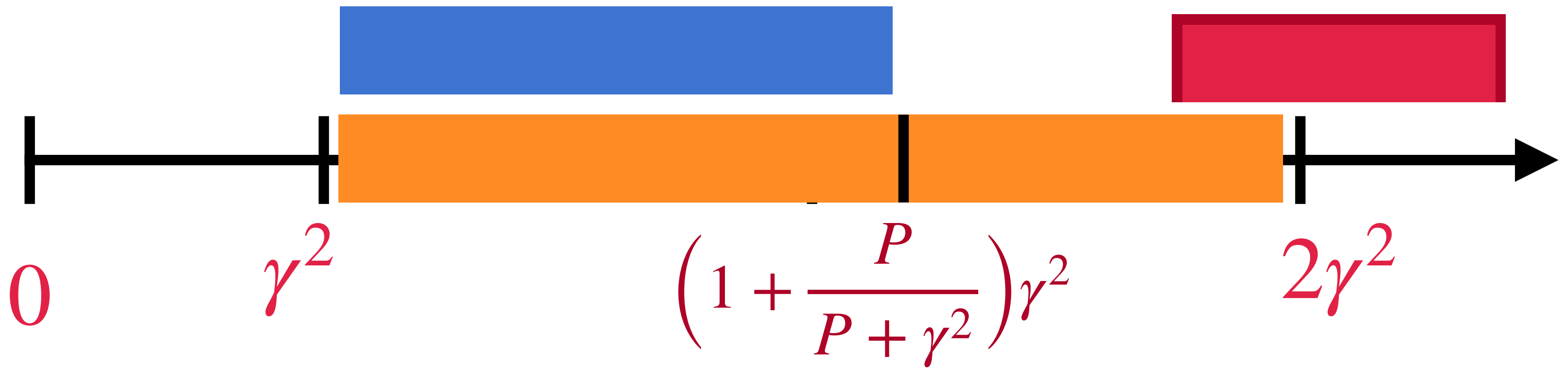
Summary of Results & Open Questions

Constrained Input

$(P < \infty)$

$\delta^2 \geq 2\gamma^2$

Impossibility Result



$\delta^2 < 2\gamma^2$

Converse:

$$\mathbb{C} \leq \frac{1}{2}\log\left(1 + \frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right)$$

$\delta^2 < \left(1 + \frac{P}{P+\gamma^2}\right)\gamma^2 < 2\gamma^2$

Achievability:

$$\mathbb{C} \geq \frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right)$$

Commitment over Gaussian UNC

Summary of Results

Gaussian UNC with Zero Elasticity

$$(E := \delta^2 - \gamma^2 = 0)$$

- Reduces to AWGN channel
- Our **achievability** result: $$\mathbb{C} \geq \lim_{E \to 0} \left\{ \frac{1}{2} \log\left(\frac{P}{E}\right) - \frac{1}{2} \log\left(1 + \frac{P}{\gamma^2}\right) \right\} = \infty$$
- Verifies the infinite capacity result of **[Nascimento et al. '08]** over AWGN channels.

Thank you !