On the (Im)possibility of Commitment over Gaussian Unfair Noisy Channels

Anuj Yadav
LINX
EPFL

Joint work with:

Amitalok Budkuley
IIT Kharagpur

Manideep Mamindlapally
TIFR Mumbai

Pranav Joshi
Independent Researcher

EPFL Information Processing Group

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**

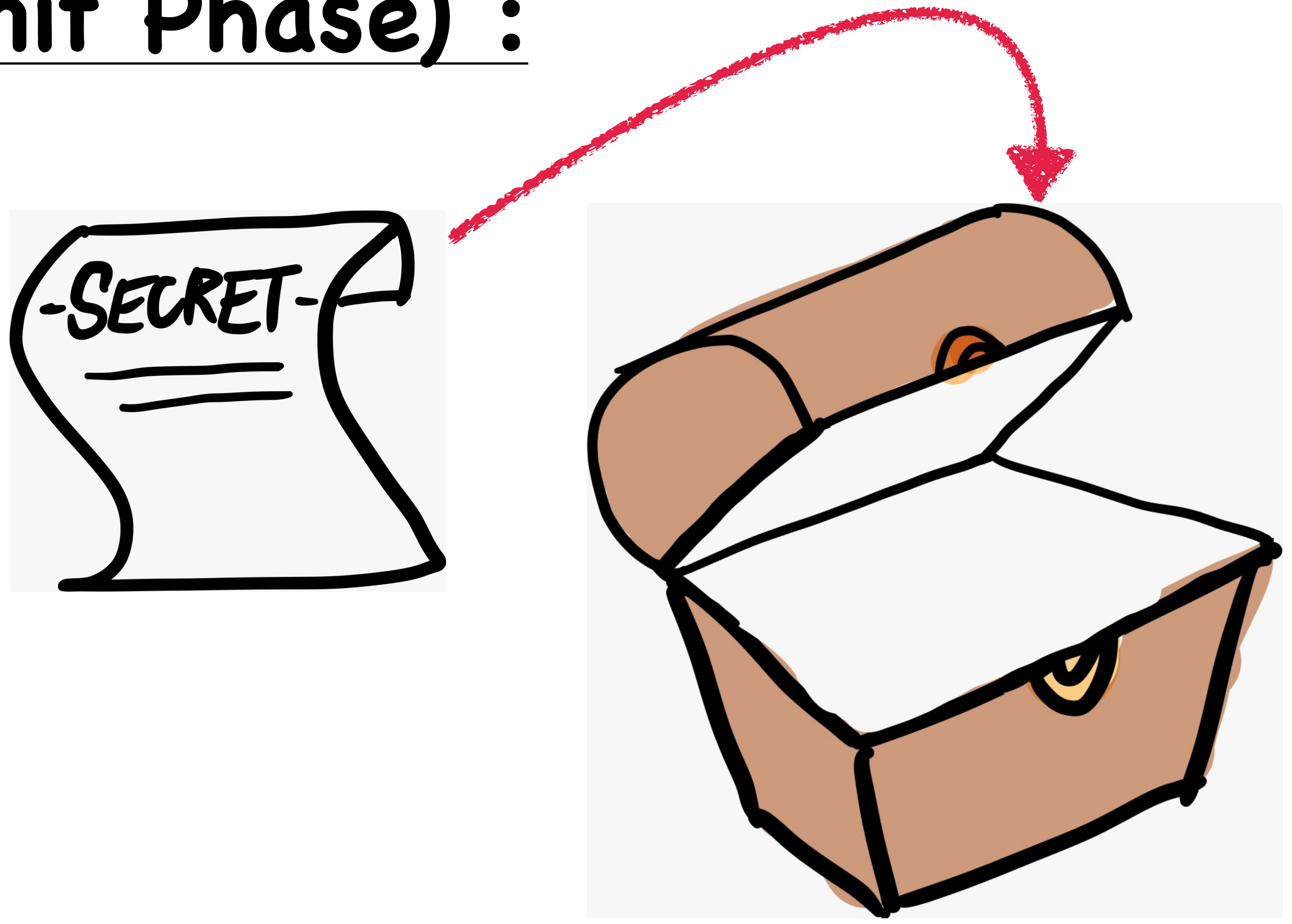
Commitment

Introduction

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

- **PHASE I (Commit Phase) :**

Alice
(Bidder)



Bob
(Auctioneer)

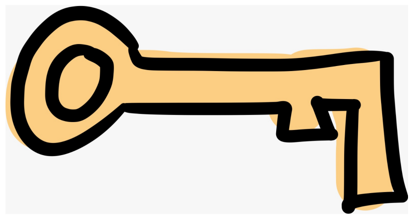
Commitment

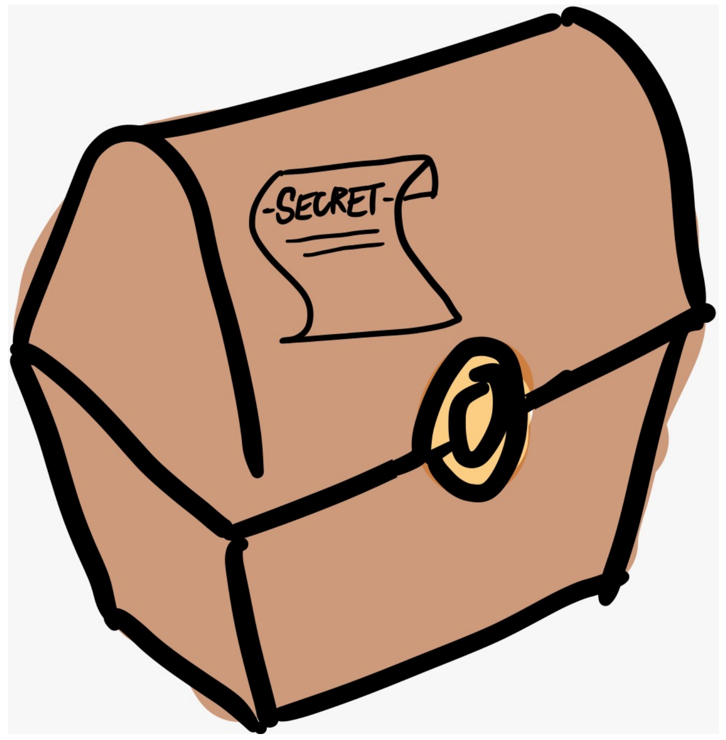
Introduction

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

- **<u>PHASE I (Commit Phase) :</u>**

Alice





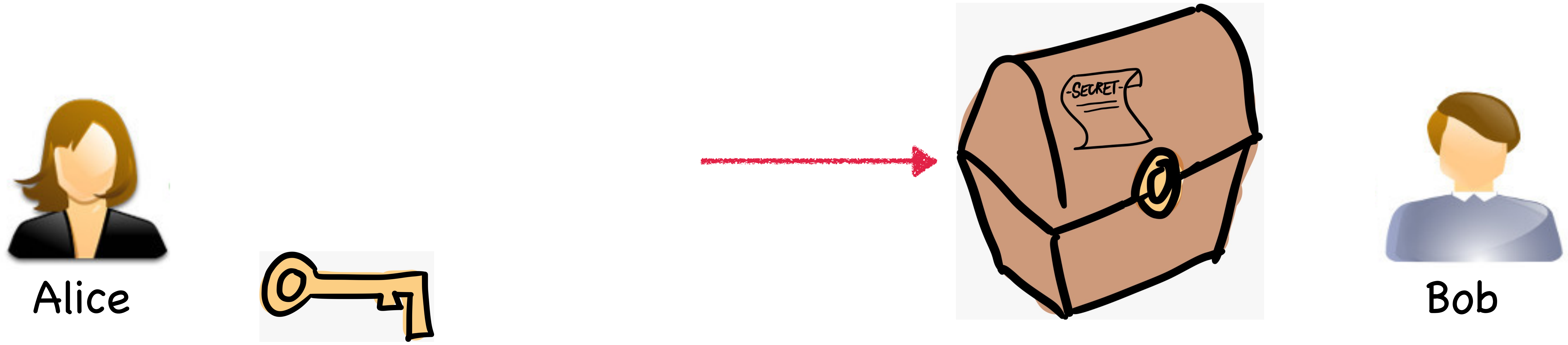
Bob

Commitment

Introduction

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

- **PHASE I (Commit Phase) :**

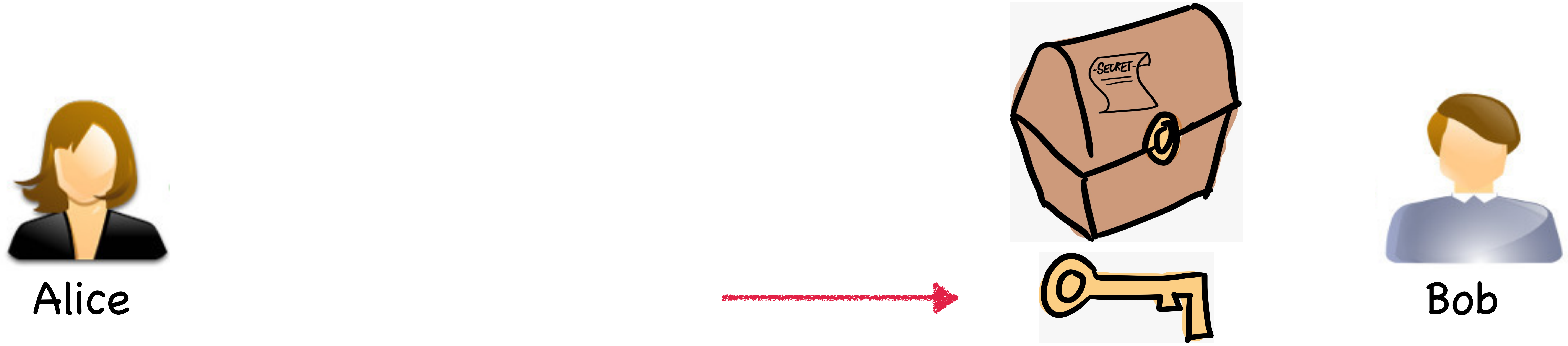


Commitment

Introduction

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

- **PHASE II (Reveal Phase) :**



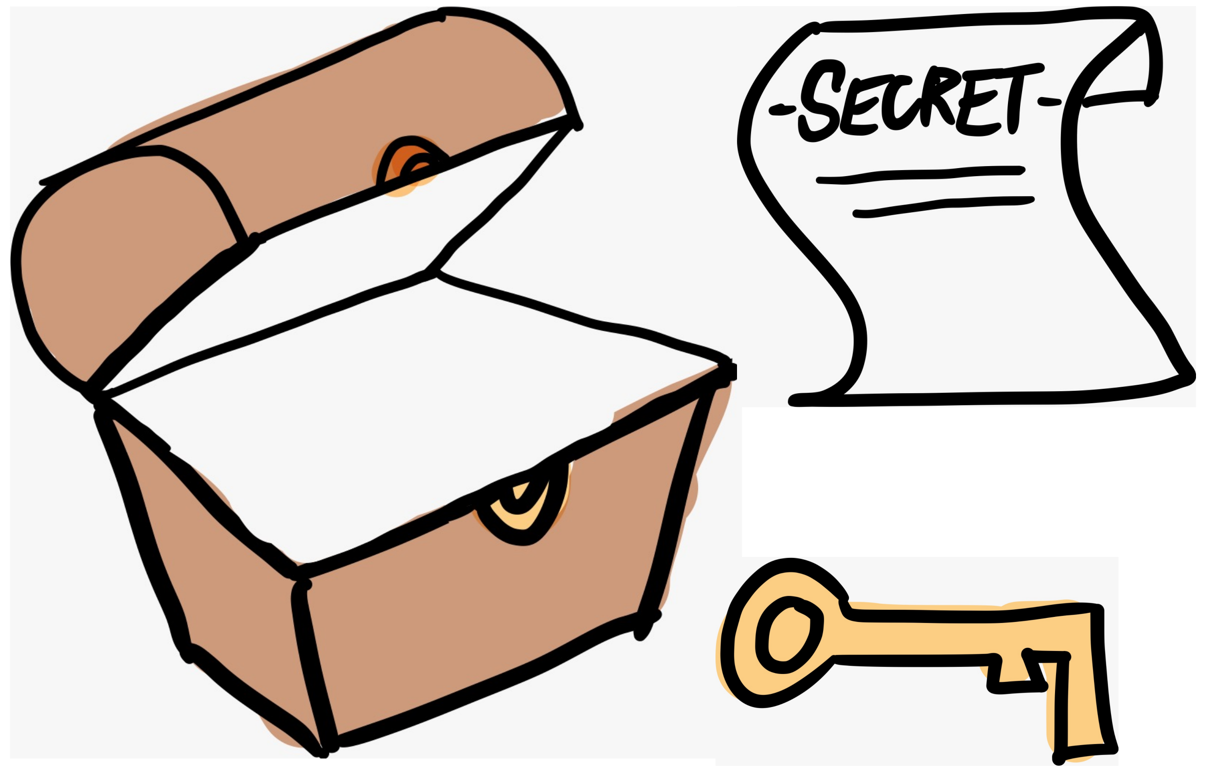
Commitment

Introduction

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

- **PHASE II (Reveal Phase) :**

Alice

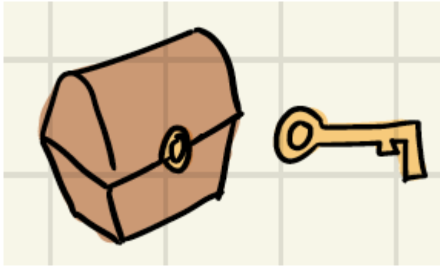


Bob

Commitment

Introduction

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

- Security Guarantees: **Soundness** **(Non-trivial resource:**  **)**
  Concealment
  Bindingness

Commitment

History

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

Computationally secure

(Secure under the assumption that users
are computationally bounded)

Commitment

History

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

Unless a **non-trivial** resource is used.

Commitment

History

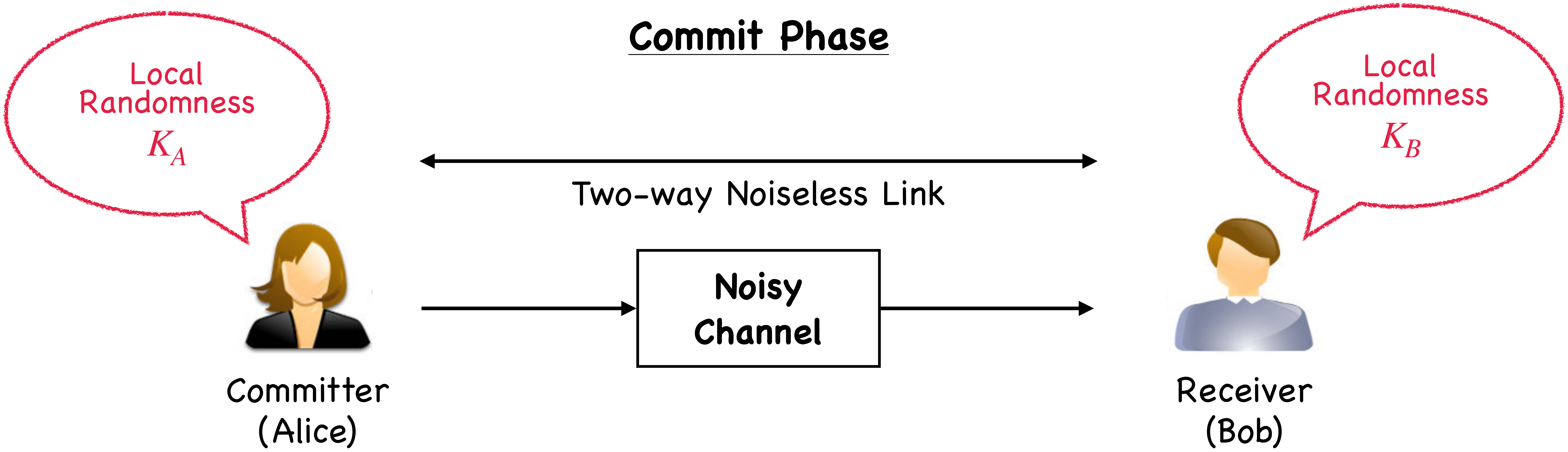
- [Blum '83] : Commitment - Interactive exchange of messages **(Computationally secure)**
- **Unconditionally secure** Commitment - IMPOSSIBLE

Unless a **non-trivial** resource is used.

- [Creapau et. al '88] : **Unconditionally secure** Commitment based on **Noisy** resource (Channel)

Unconditionally Secure Commitment

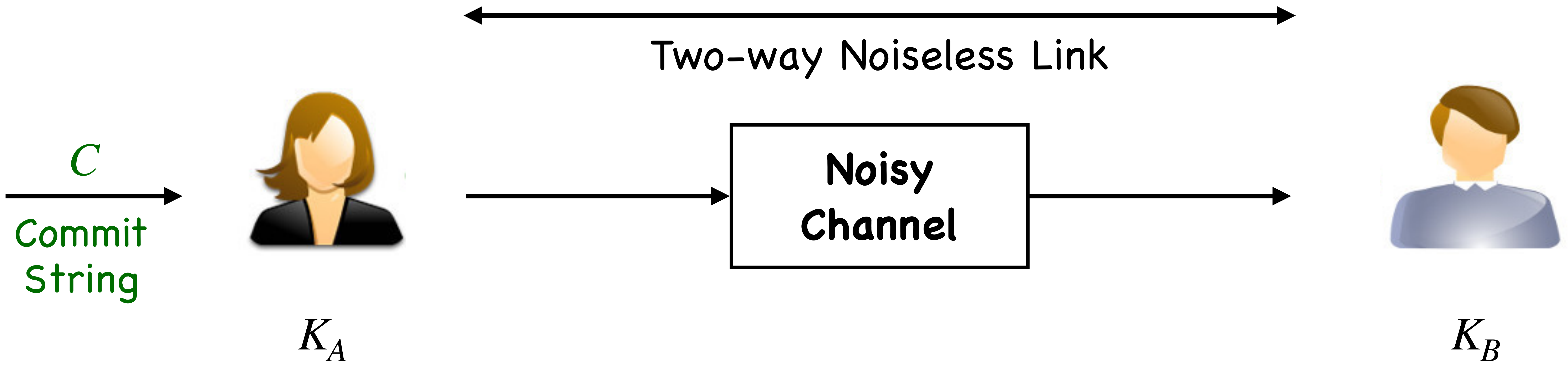
General Problem Setup



Unconditionally Secure Commitment

General Problem Setup

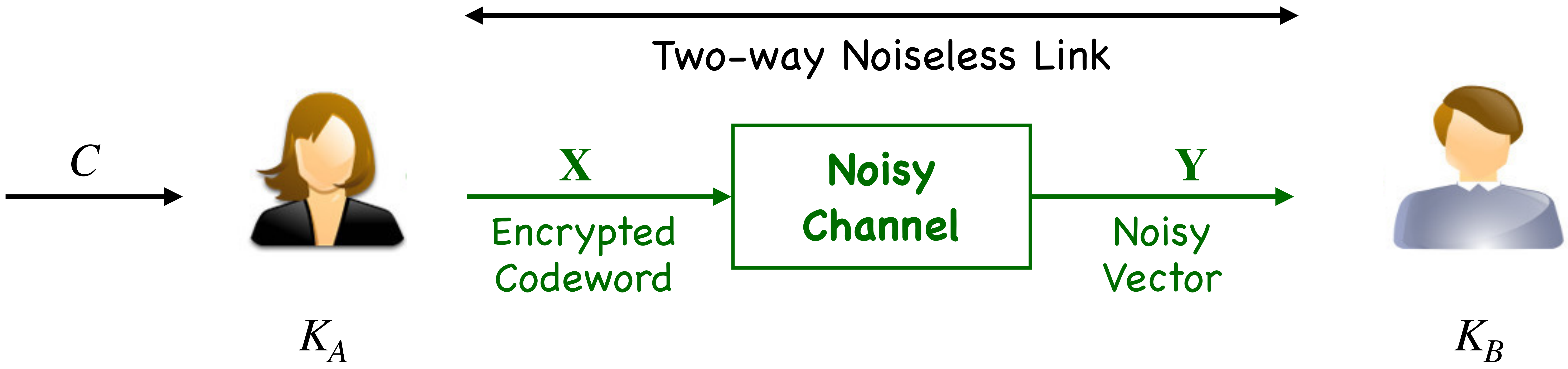
Commit Phase



Unconditionally Secure Commitment

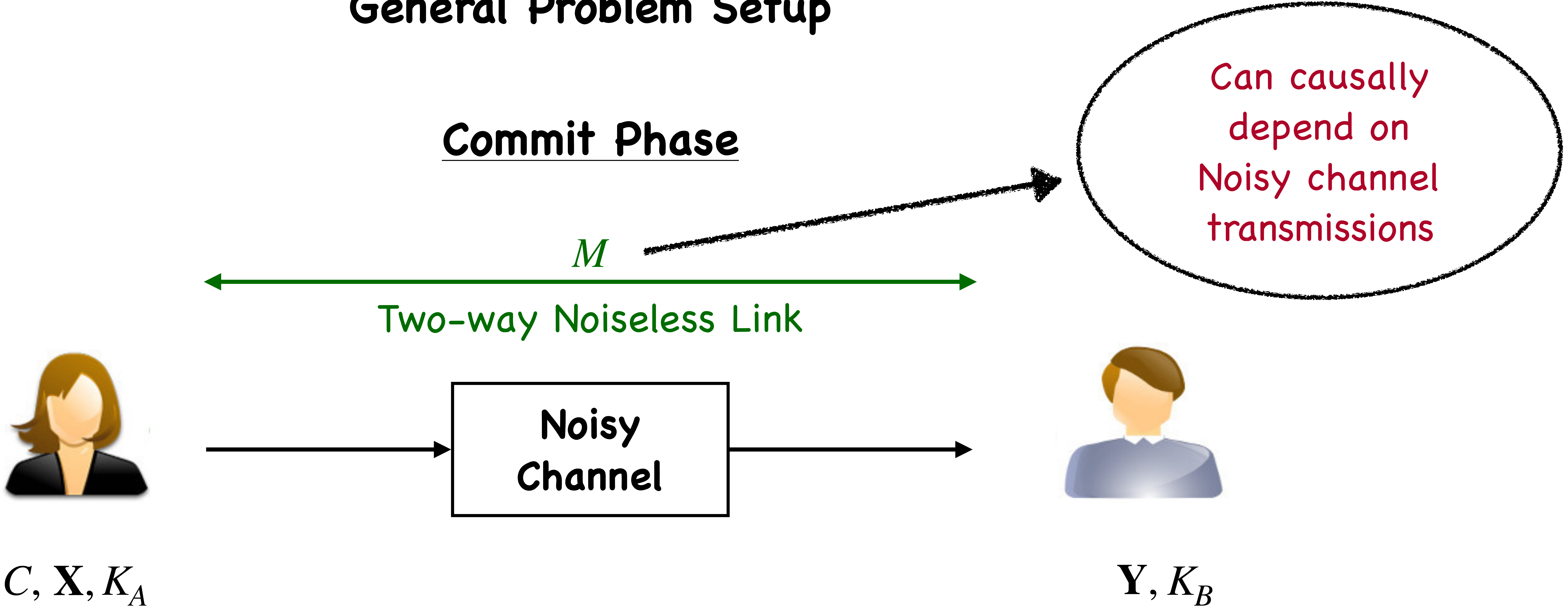
General Problem Setup

<u>Commit Phase</u>



Unconditionally Secure Commitment

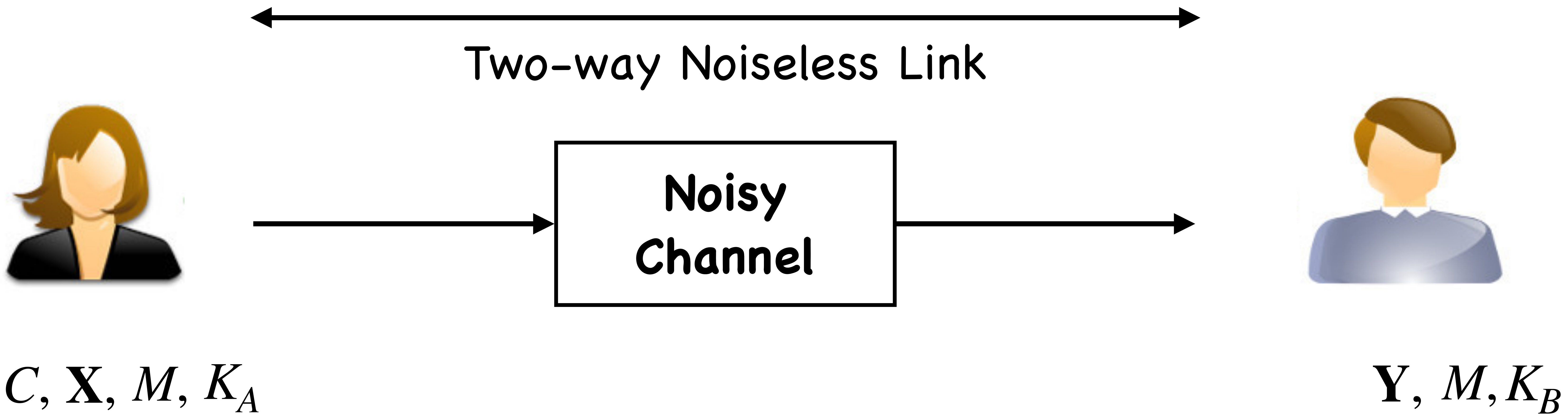
General Problem Setup



Unconditionally Secure Commitment

General Problem Setup

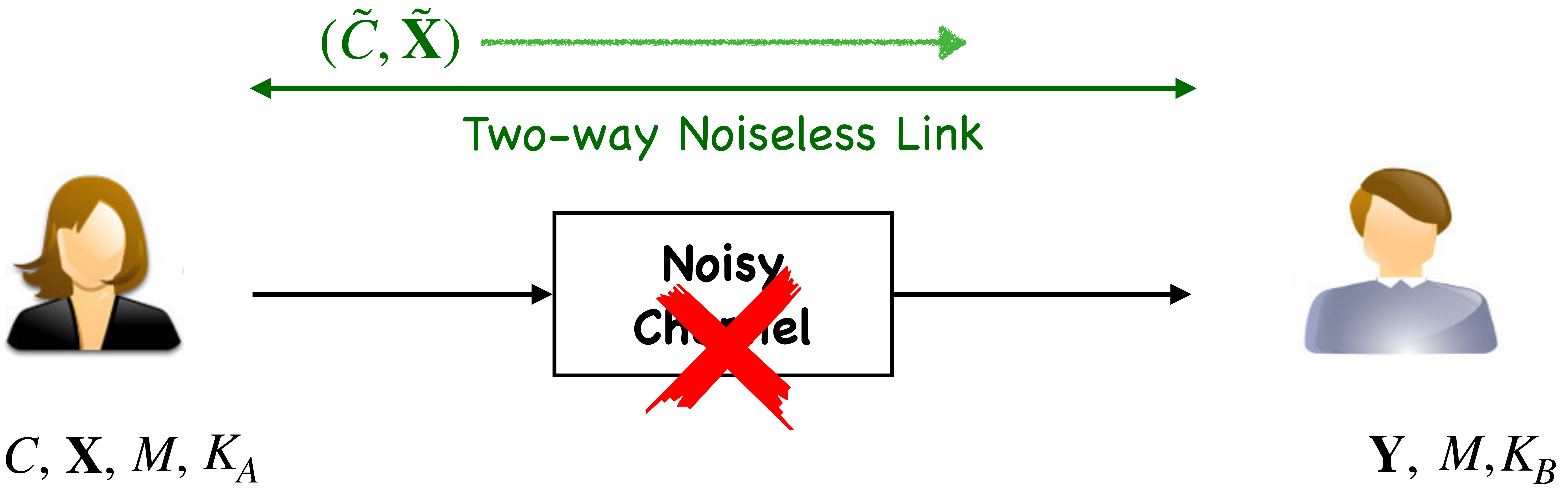
Commit Phase



Unconditionally Secure Commitment

General Problem Setup

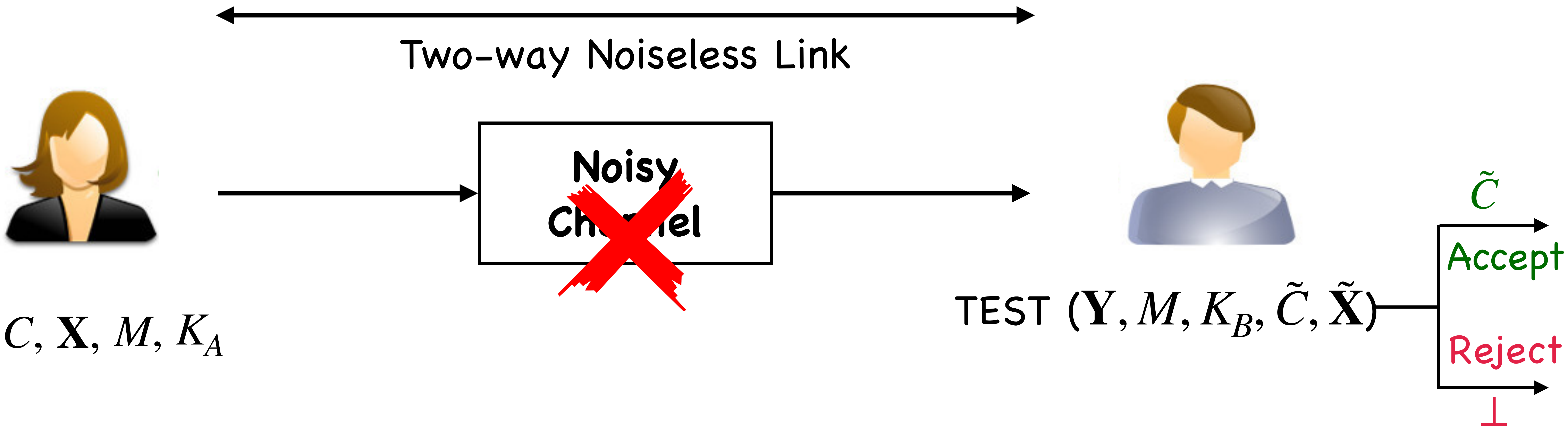
Reveal Phase



Unconditionally Secure Commitment

General Problem Setup

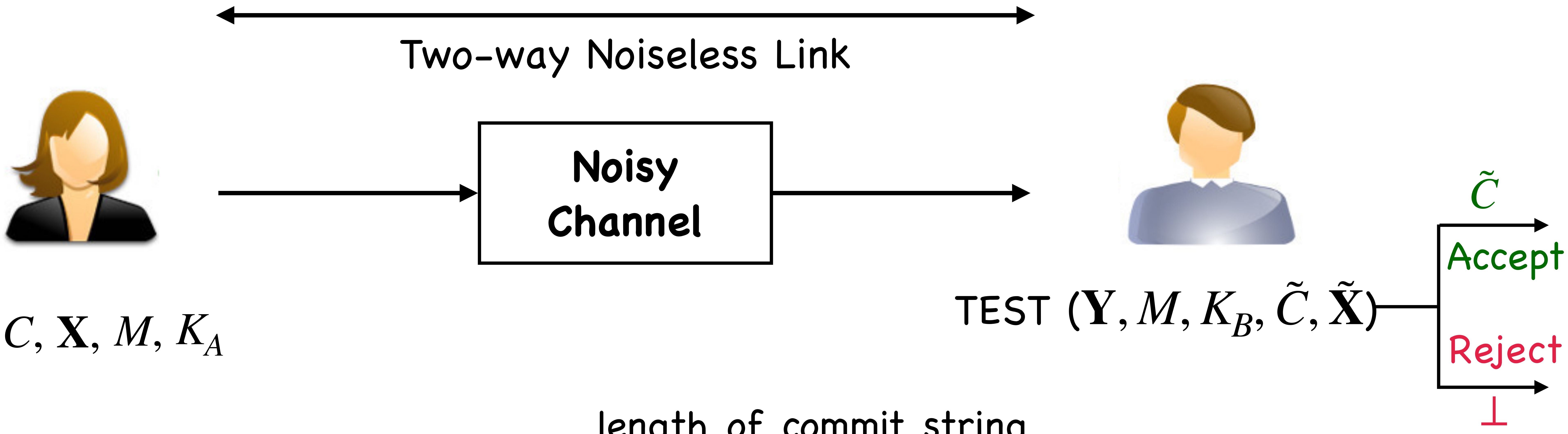
Reveal Phase



Unconditionally Secure Commitment

General Problem Setup - Commitment Rate

Reveal Phase



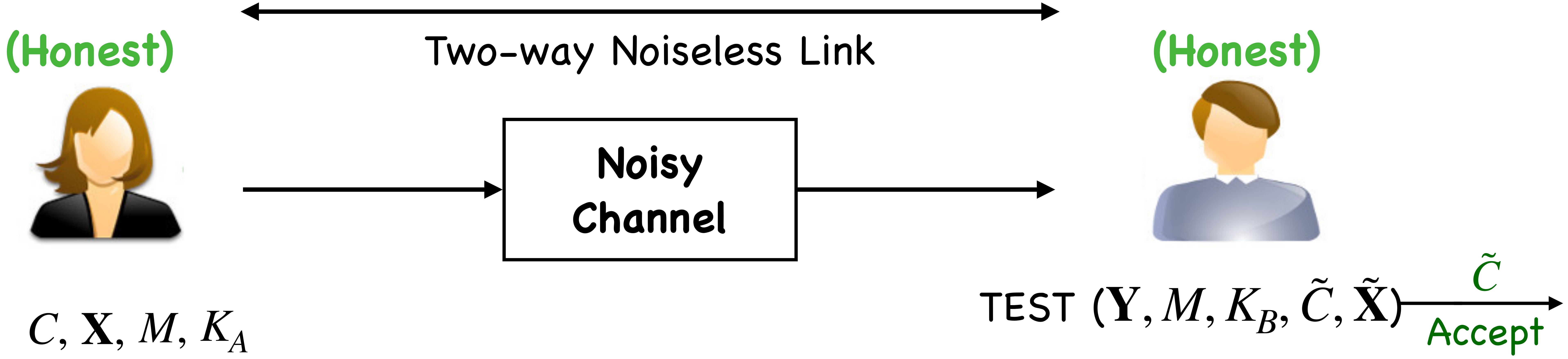
$$\text{Commitment Rate} := \frac{\text{length of commit string}}{\text{No. of uses of noisy channel}}$$

Unconditionally Secure Commitment

General Problem Setup - Security Guarantees

Soundness

(In reveal phase)



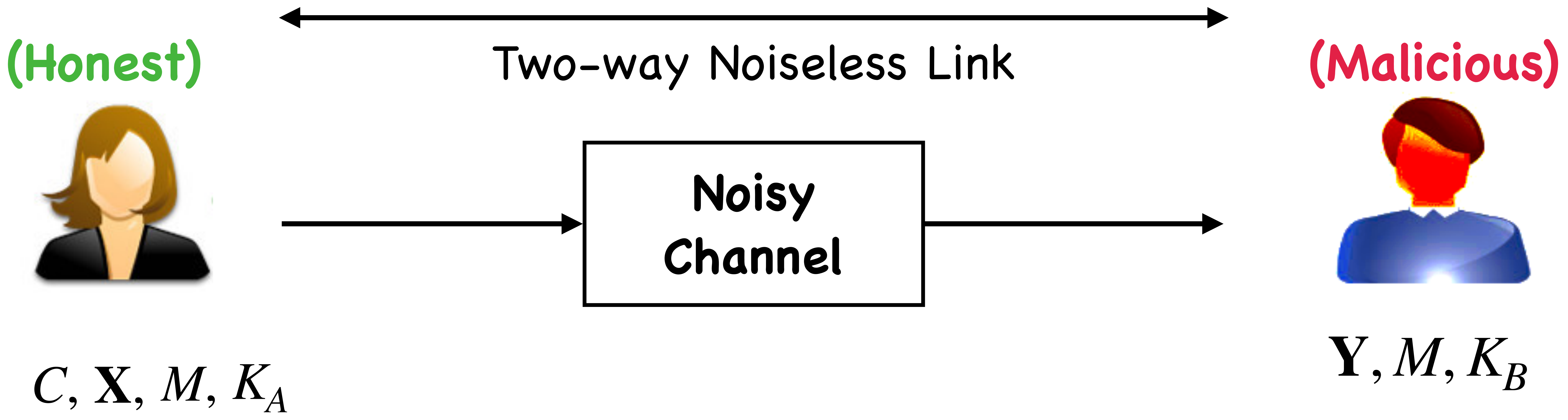
$\mathbf{P}$ (TEST $(\mathbf{Y}, M, K_B, \tilde{C}, \tilde{\mathbf{X}})$ = reject) $\leq \epsilon$

Unconditionally Secure Commitment

General Problem Setup - Security Guarantees

Concealment

(In commit phase)



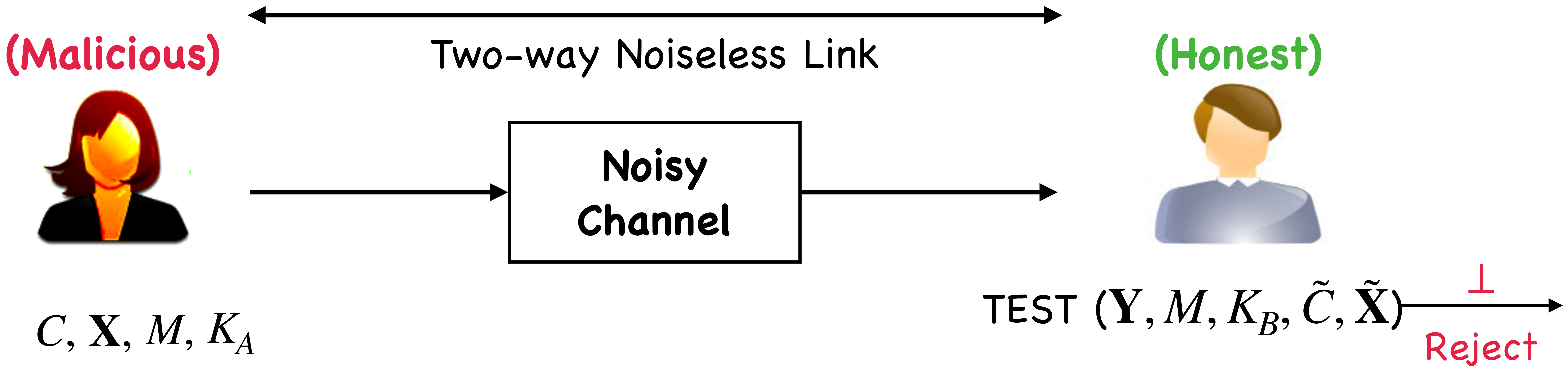
$$I(C; \mathbf{Y}, M, K_B) \leq \epsilon$$

Unconditionally Secure Commitment

General Problem Setup - Security Guarantees

Bindingness

(In reveal phase)



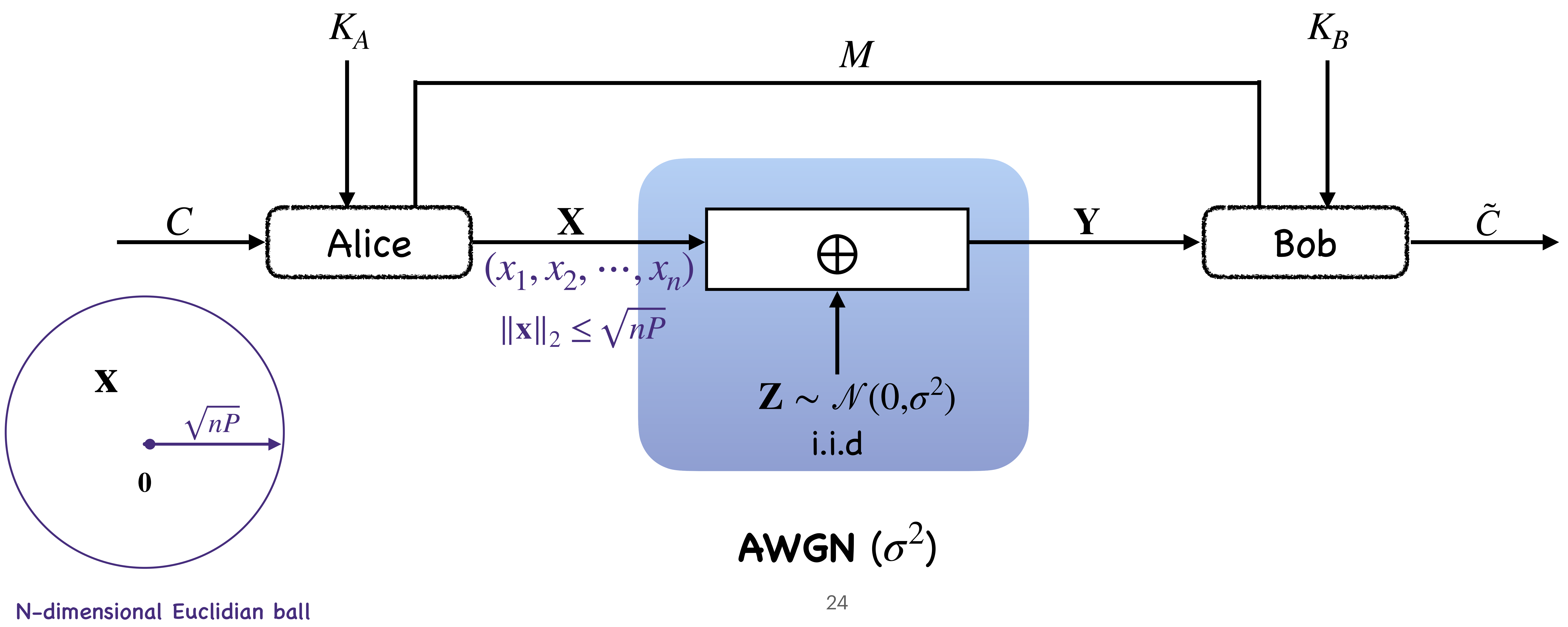
$$\mathrm{P}\left\{(\mathrm{TEST}\,(\mathbf{Y}, M, K_B, \tilde{C}, \tilde{\mathbf{X}}) = \text{accept})\ \&\ (\mathrm{TEST}\,(\mathbf{Y}, M, K_B, \hat{C}, \hat{\mathbf{X}}) = \text{accept})\right\} \leq \epsilon$$

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

Unconditionally Secure Commitment

Commitment over AWGN Channel

Setup



Unconditionally Secure Commitment

Commitment over AWGN Channel

Theorem:

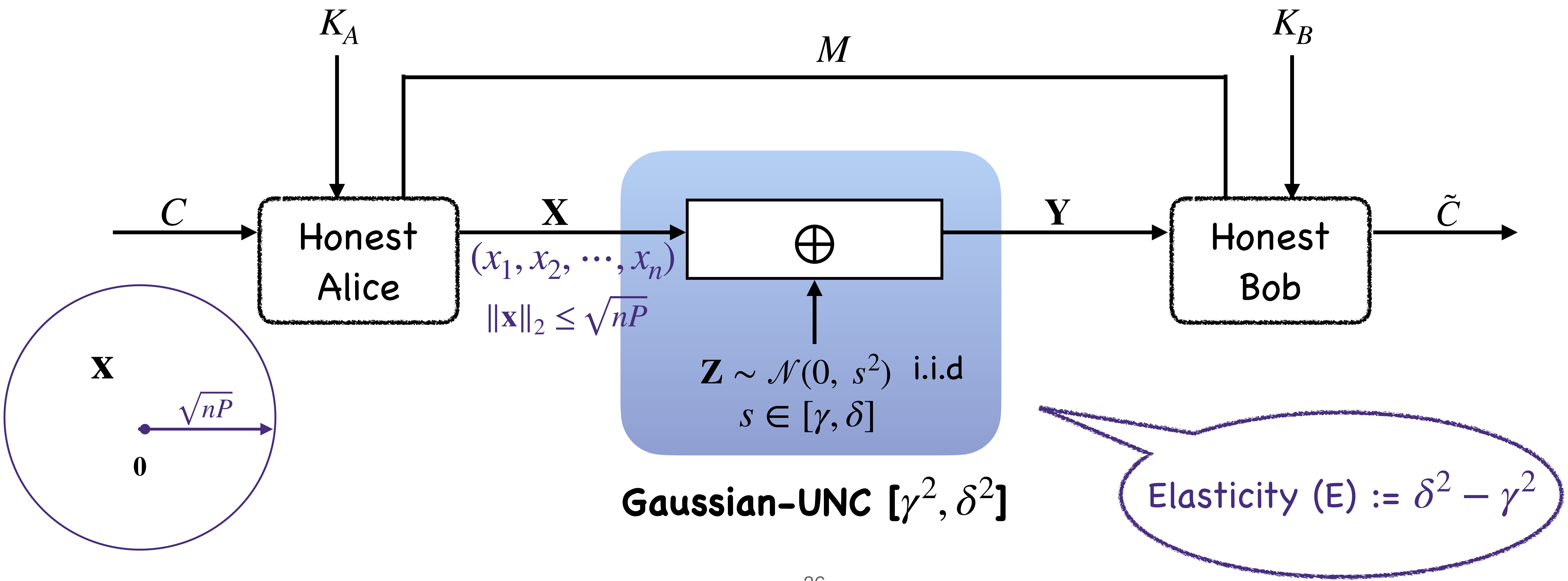
The Commitment Capacity of an AWGN channel is Infinite.

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)

Setup

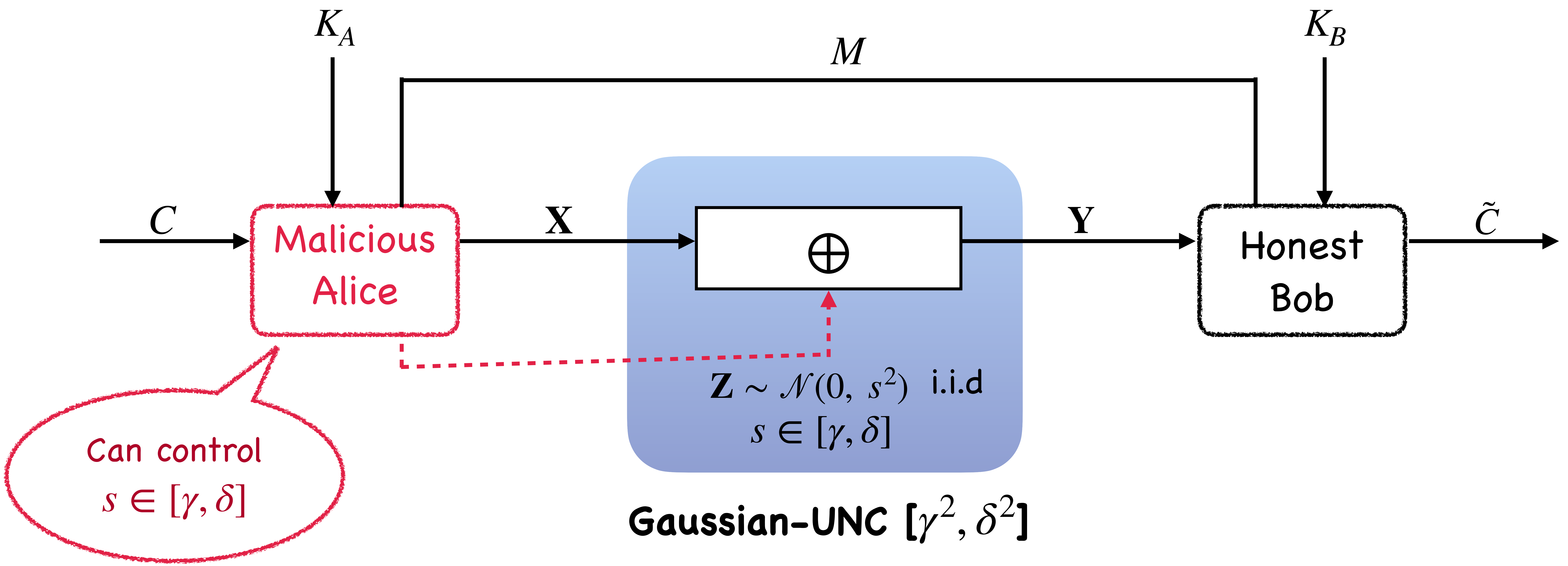


N-dimensional Euclidian ball

Unconditionally Secure Commitment

Gaussian Unfair Noisy Channel (Gaussian - UNC)

Setup

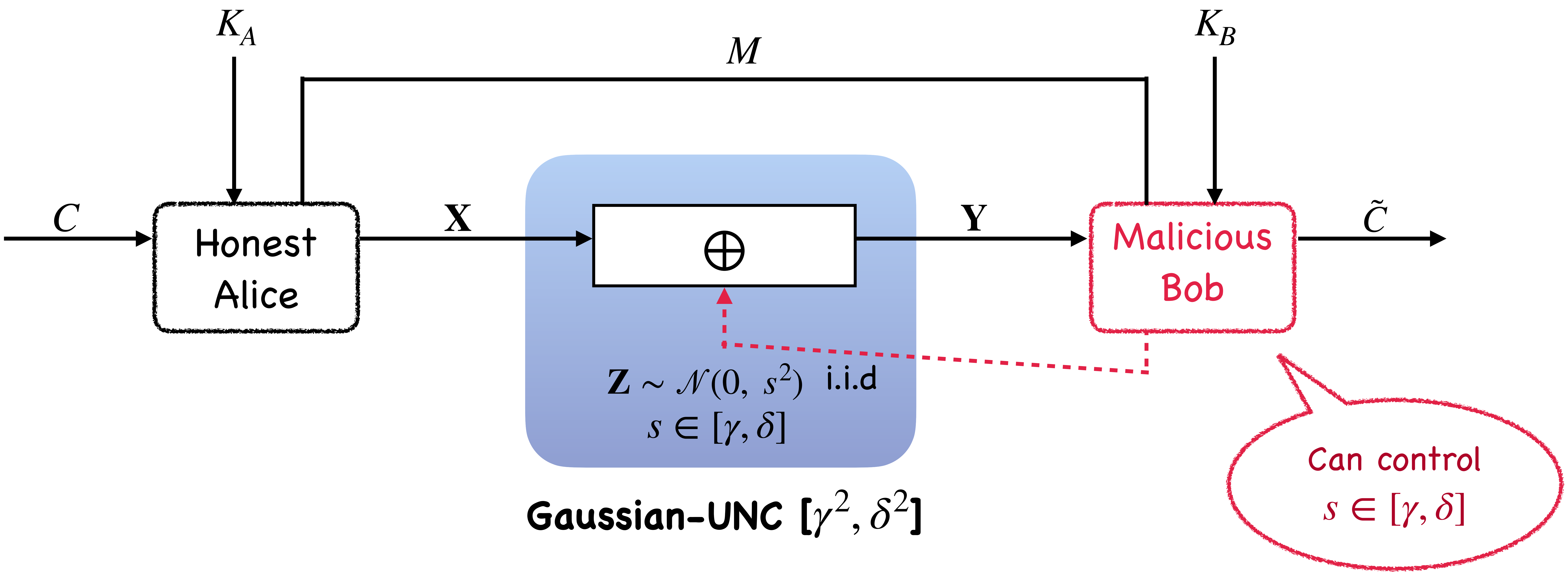


Gaussian-UNC $[\gamma^2, \delta^2]$

Unconditionally Secure Commitment

Gaussian Unfair Noisy Channel (Gaussian - UNC)

Setup



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

Commitment over Gaussian UNC

Main Result - Converse

Theorem:

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

Commitment over Gaussian UNC

Main Result - Achievability

Theorem:

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

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

and it 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 - Takeaways

Unconstrained Input

$(P \to \infty)$

Converse:

$\mathbb{C} = 0$, if

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

Achievability:

If $\delta^2 < \lim_{P\to\infty}\left(1 + \frac{P}{P+\gamma^2}\right)\gamma^2 = 2\gamma^2$

Then,

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

$$= \frac{1}{2}\log\left(\frac{\gamma^2}{E}\right)$$

Commitment over Gaussian UNC

Main Result - Takeaways

Unconstrained Input

$(P \to \infty)$

Converse:

$\mathbb{C} = 0$, if

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

Achievability:

If $\delta^2 < \lim_{P\to\infty} \left(1 + \frac{P}{P+\gamma^2}\right)\gamma^2 = 2\gamma^2$

Then,

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

$$= \frac{1}{2}\log\left(\frac{\gamma^2}{E}\right)$$

Positive rate commitment is possible if and only if $\delta^2 < 2\gamma^2$.

Commitment over Gaussian UNC

Main Result - Takeaways

Gaussian UNC with Zero Elasticity

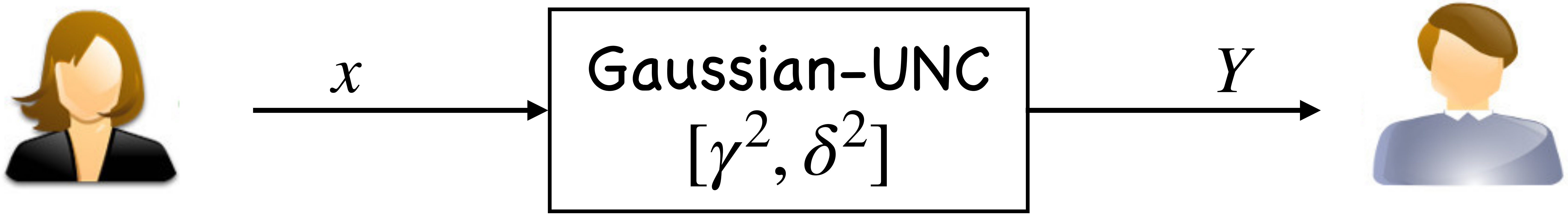
$(E := \delta^2 - \gamma^2 = 0)$

- Reduces to AWGN channel
- Our achievability result:

$$\mathbb{C} \geq \lim_{E \to 0} \left\{ \frac{1}{2} \log \left(\frac{P}{E} \right) - \frac{1}{2} \log \left(1 + \frac{P}{\gamma^2} \right) \right\} = \infty$$

Commitment over Gaussian UNC

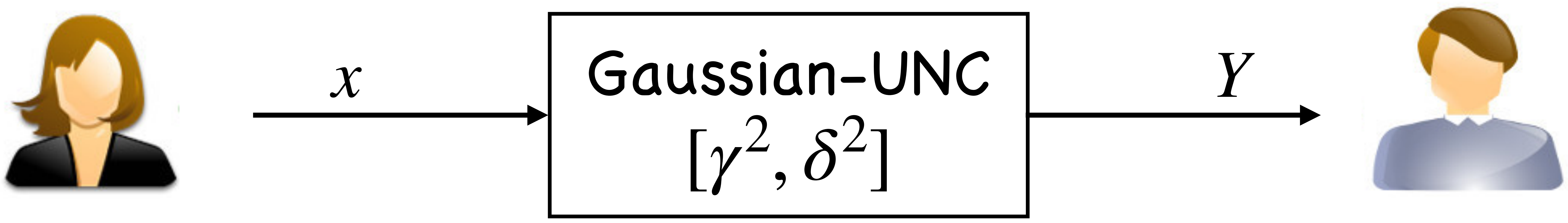
Zero rate Converse

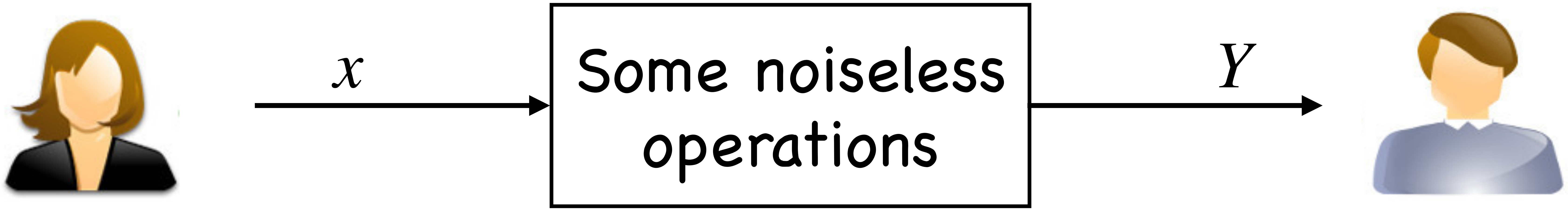


Ivan Damgård and Joe Kilian and Louis Salvail, "On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions", Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Springer 1999, pp. 56-73.

Commitment over Gaussian UNC

Zero rate Converse

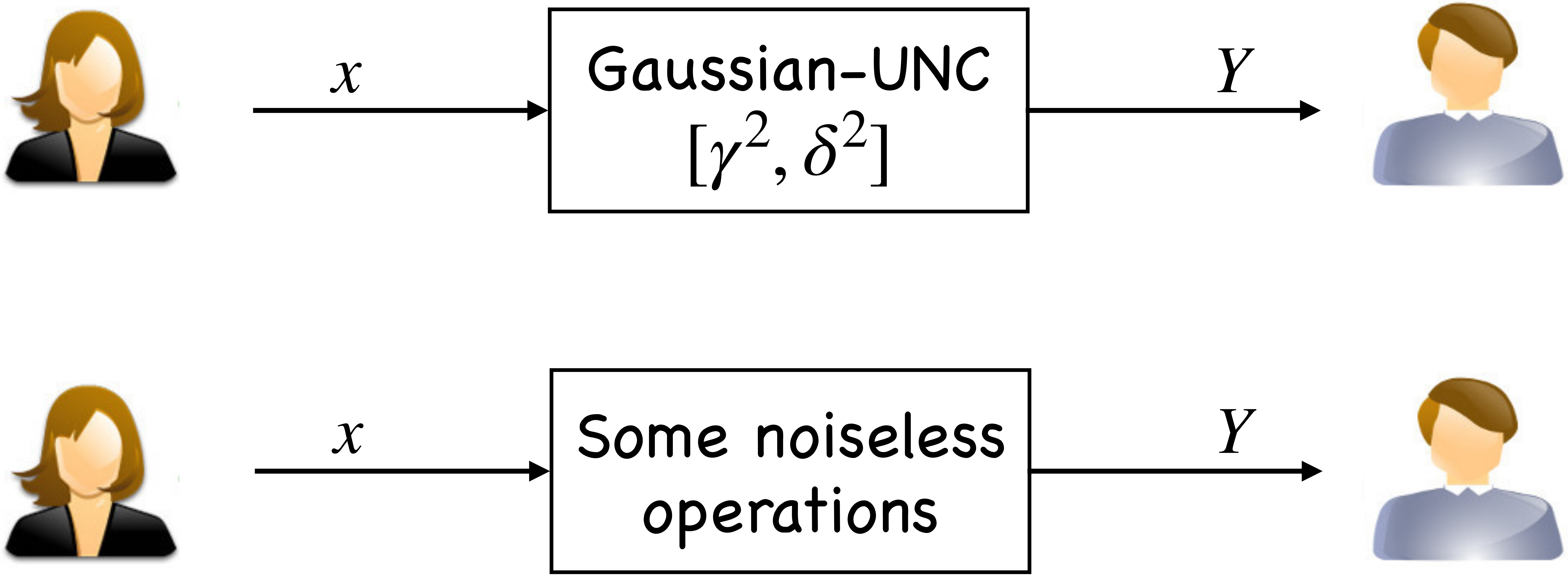




- Simulate an equivalent of an instantiation of the Gaussian UNC via purely noiseless operations.

Commitment over Gaussian UNC

Zero rate Converse



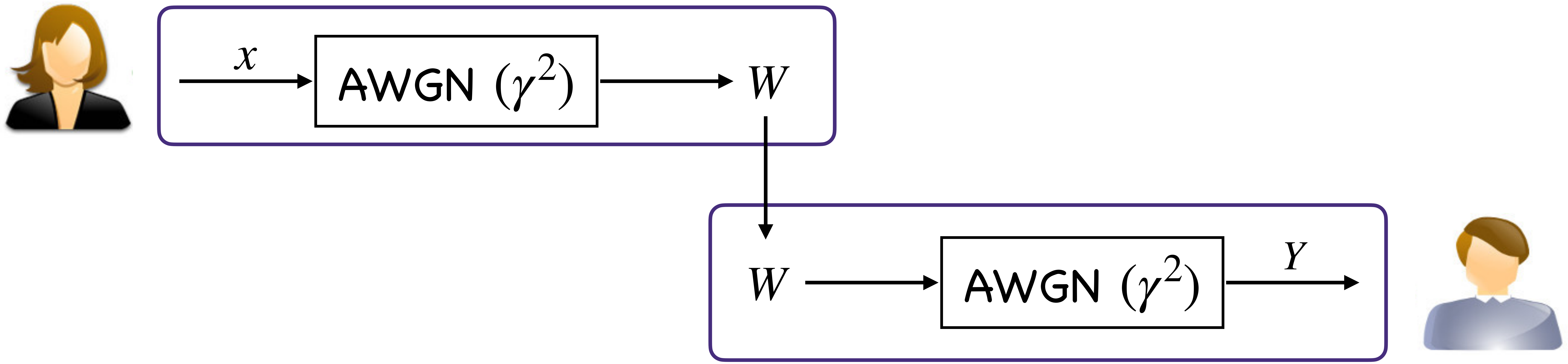
- Simulate an equivalent of an instantiation of the Gaussian UNC via purely noiseless operations.
- Commitment impossible over noiseless channels

==> Commitment impossible over Gaussian-UNC

Commitment over Gaussian UNC

Zero rate Converse

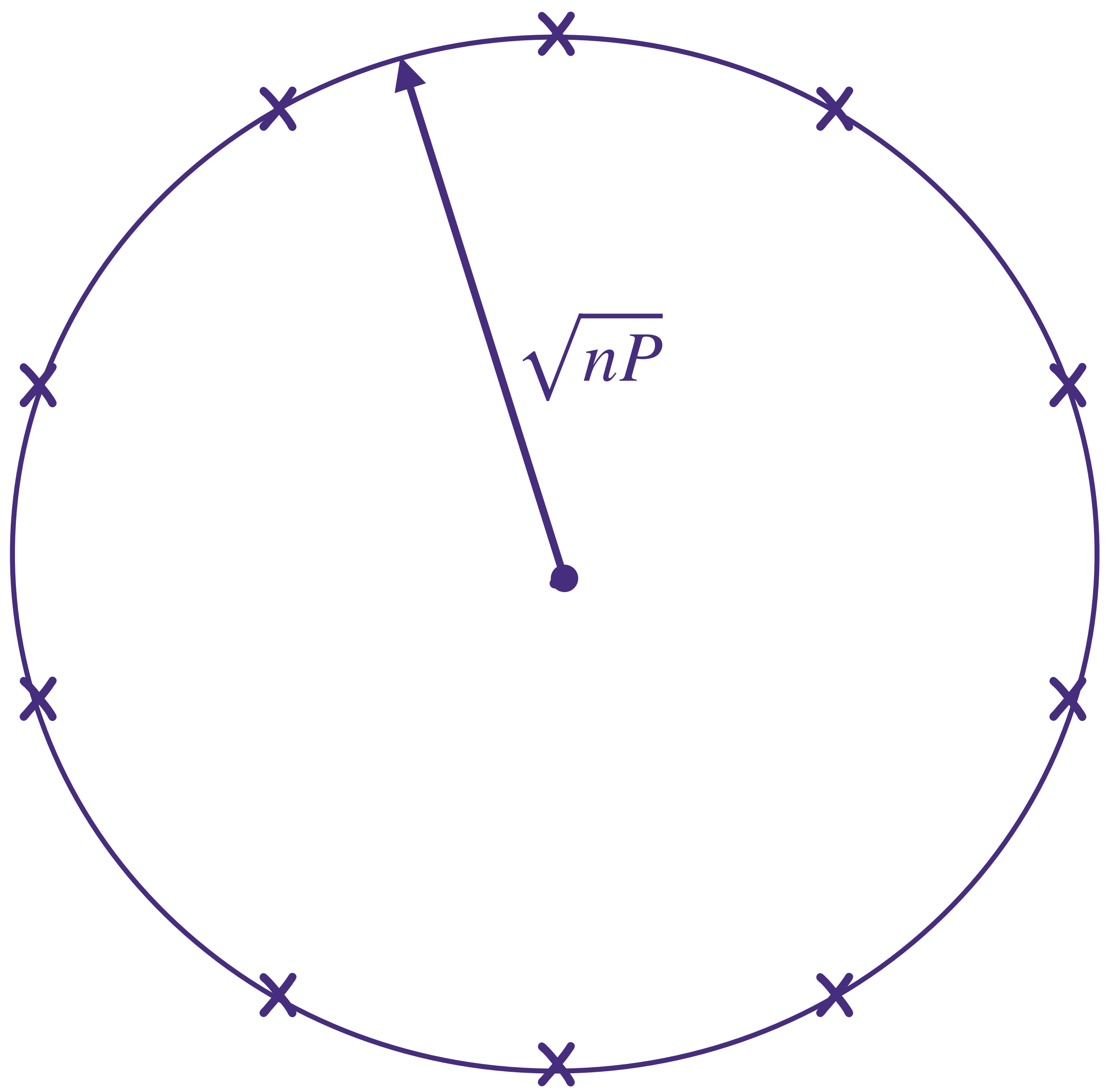
Instantiation: $s^2 = 2\gamma^2$



Commitment over Gaussian UNC

Achievability - Spherical code

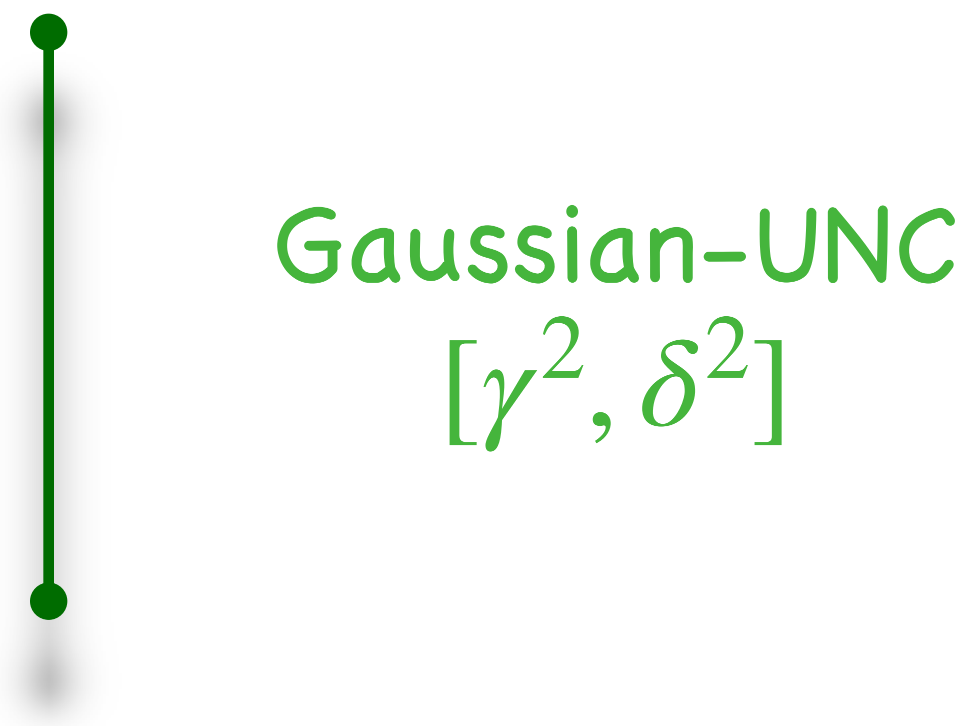
- Spherical code (ψ) with 'equi-normed' codewords
- On surface of hypersphere of radius $\approx \sqrt{nP}$



Commitment over Gaussian UNC

Achievability - Protocol - 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 $\mathbf{Y}$.



Commitment over Gaussian UNC

Achievability - Protocol - 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

Commitment over Gaussian UNC

Achievability - Protocol - 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

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

Two-way
Noiseless Link

Commitment over Gaussian UNC

Achievability - Protocol - Reveal Phase

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

$\longrightarrow$ Typicality Test

$\longrightarrow$ Hash Challenge Test

$\longrightarrow$ OTP Test

Two-way Noiseless Link

Commitment over Gaussian UNC

Achievability - Protocol - 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 $\mathbf{Y}$.

Guarantees
Bindingness against malicious
Alice

- 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 - Protocol - 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

Concluding Remarks

- Commitment capacity for AWGN channels is infinite.
- For Gaussian-UNC $[\gamma^2, \delta^2]$:
  - $\mathbb{C} = 0$, if $2\gamma^2 \leq \delta^2$.
  - $\mathbb{C} \geq \frac{1}{2}\log\left(\frac{\gamma^2}{E}\right)$, if $2\gamma^2 > \delta^2$.

Infinite power case

- For finite power constraint P, if $\delta^2 < \left(1 + \frac{P}{P+\gamma^2}\right)\gamma^2$ then:

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

Finite power constraint