Wiretapped Commitment over Binary Channels

Anuj Yadav
EPFL

Joint work with:

Manideep Mamindlapally

CWI, University of Amsterdam

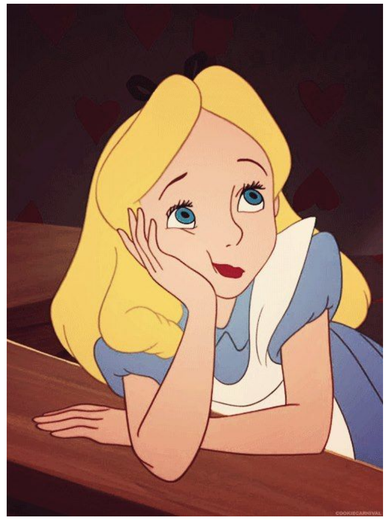
Amitalok Budkuley

IIT Kharagpur

The Game of Chess

Problem

Bed time, who play's the last move?

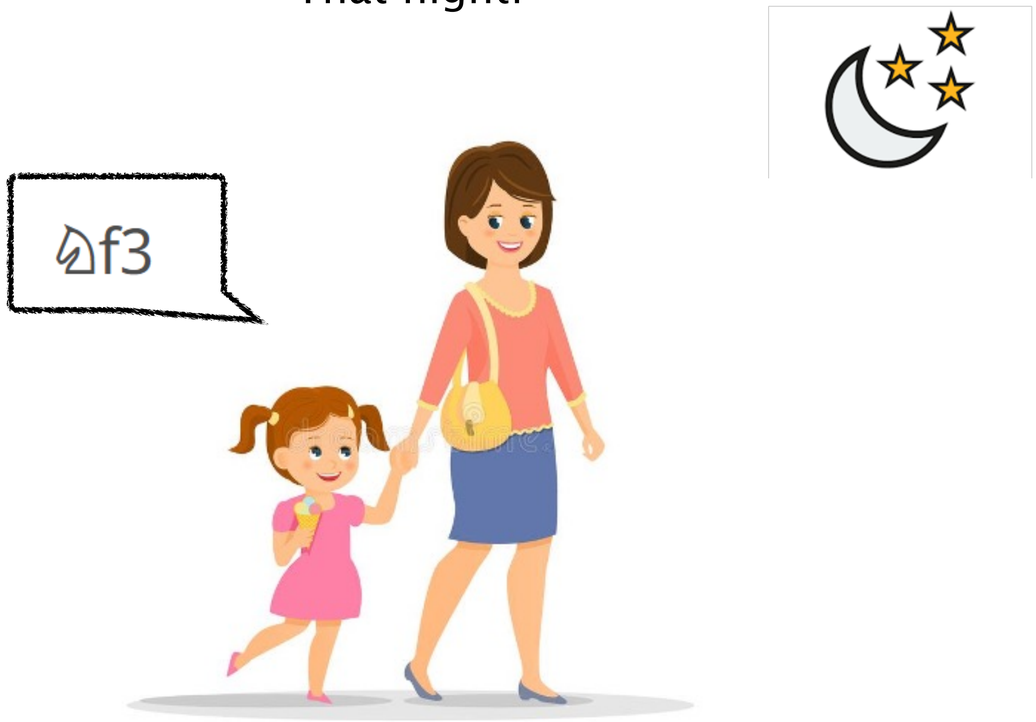


Alice (or Bob) can think about the next move for the whole night.

The Game of Chess

Solution – Trusted third party !!

That night:



Alice ‘commits’ her move to Mom.

Guarantee: The move is hidden from Bob.

Next Morning:

The move is ‘revealed’ to Bob.

Guarantee: Alice is bound to play the same move.

The Game of Chess

Without trusted third party ?

That night:

Next Morning:

What if there's no **Trusted third party ?** —— **"Bit Commitment"**

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

Introduction

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

- Security Guarantees: **Soundness**
  Concealment
  Bindingness

- **Applications:** Zero-Knowledge Proofs (ZKPs), Secure Multiparty Computation (MPC), Coin tossing, etc.

Commitment

History

- [Blum ’83]: Commitment – Interactive exchange of messages **(noiseless)**

Computationally secure

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

Commitment

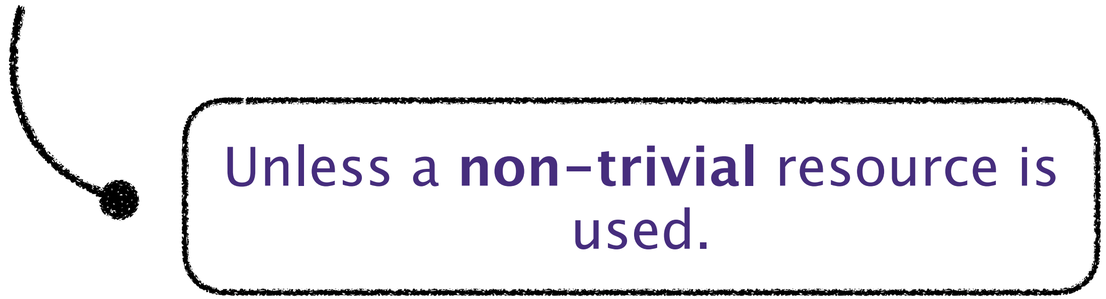
History

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

Commitment

History

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

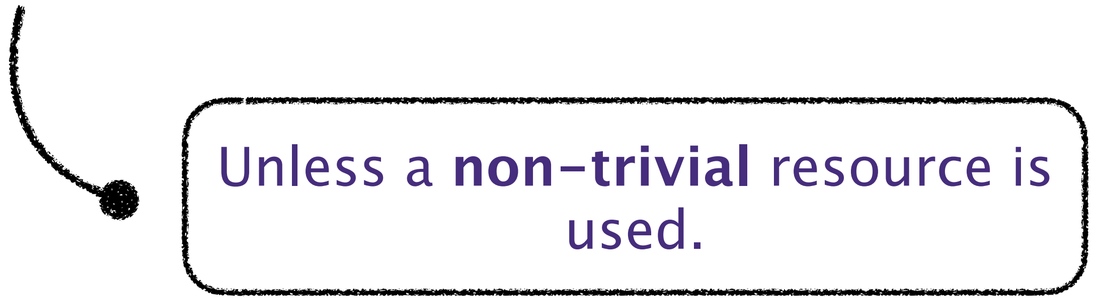


- [A. D. Wyner ’75]: The wire-tap channel.

Commitment

History

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

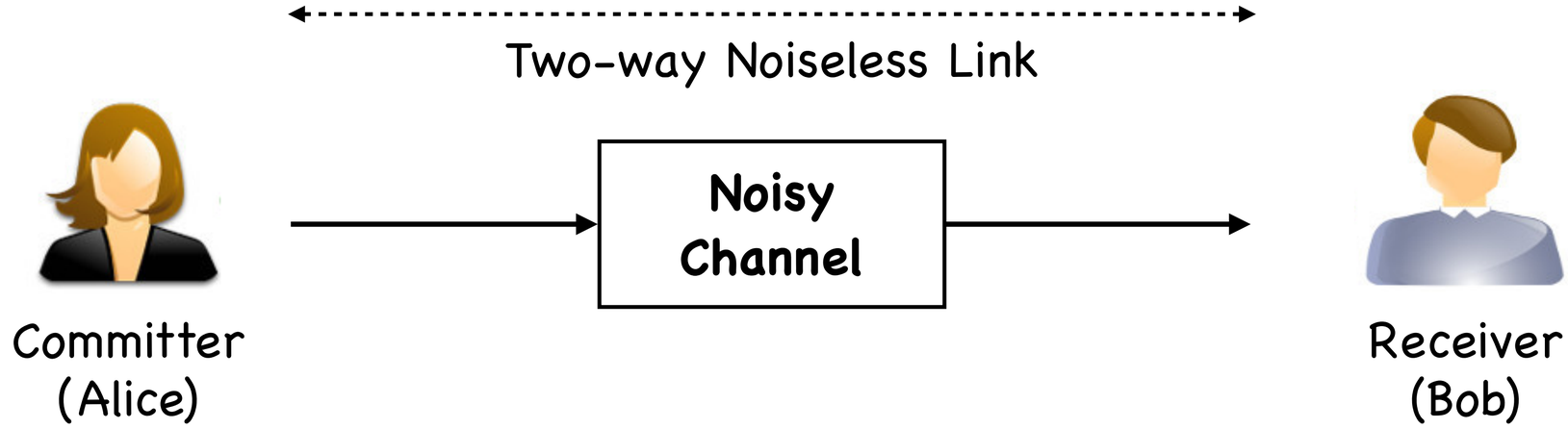


- [A. D. Wyner ’75]: The wire-tap channel.
- [Crepeau et al. ’88]: **Unconditionally secure** Commitment based on **Noisy** resource (Binary symmetric channel)

Unconditionally Secure Commitment

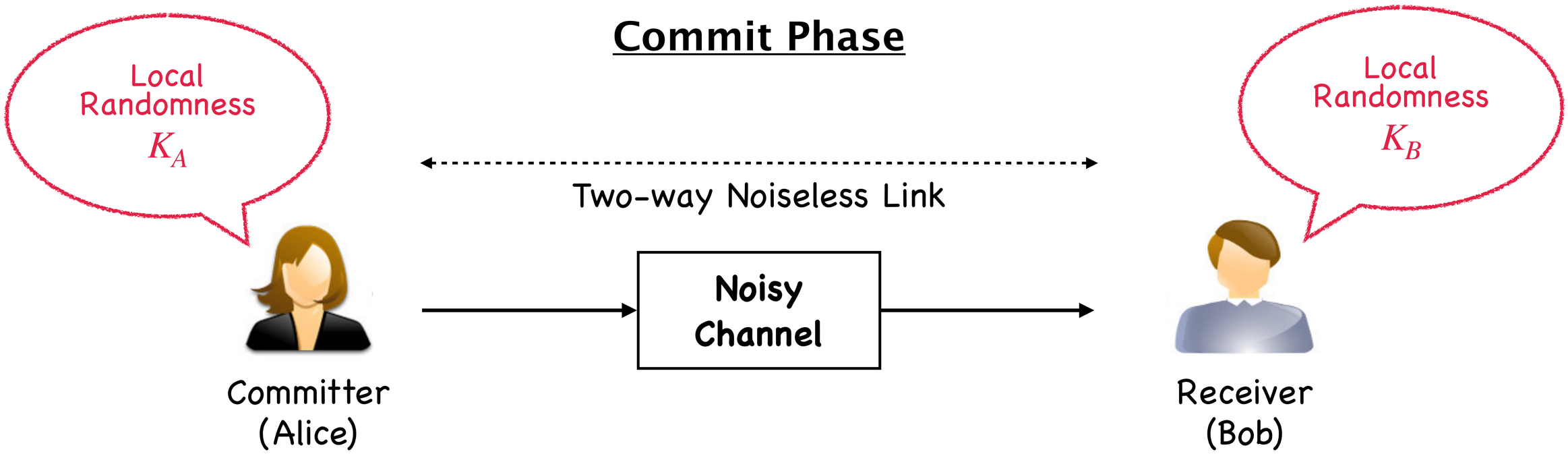
General Problem Setup

Commit Phase



Unconditionally Secure Commitment

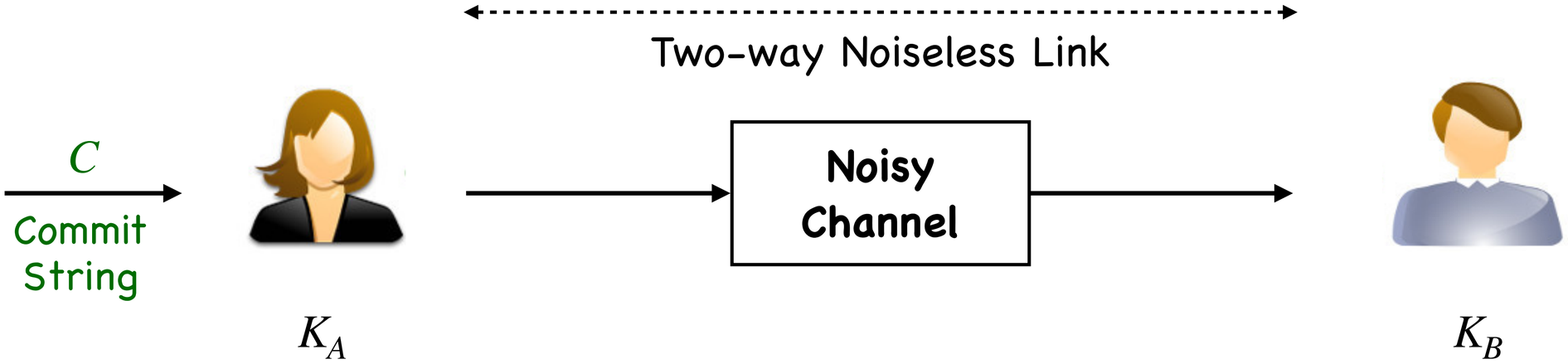
General Problem Setup



Unconditionally Secure Commitment

General Problem Setup

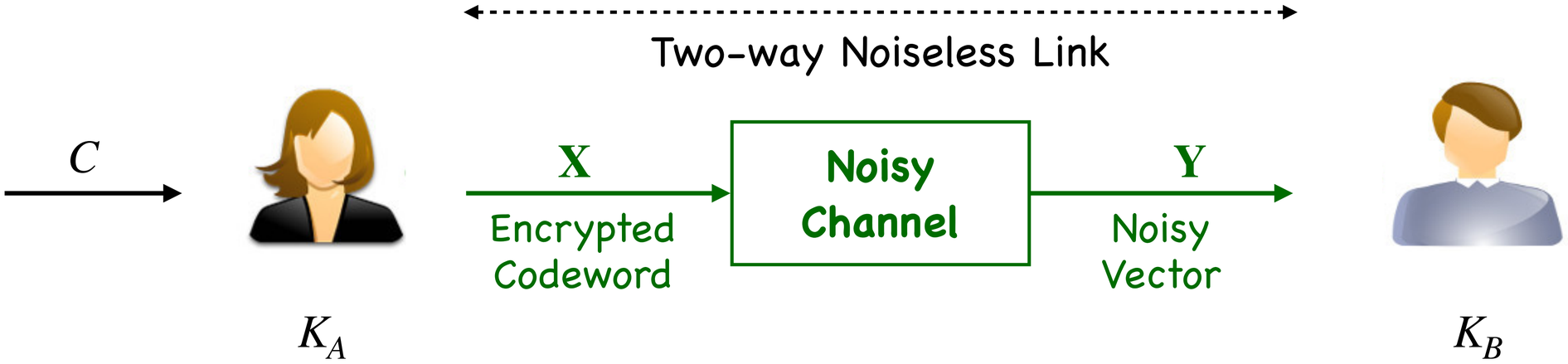
Commit Phase



Unconditionally Secure Commitment

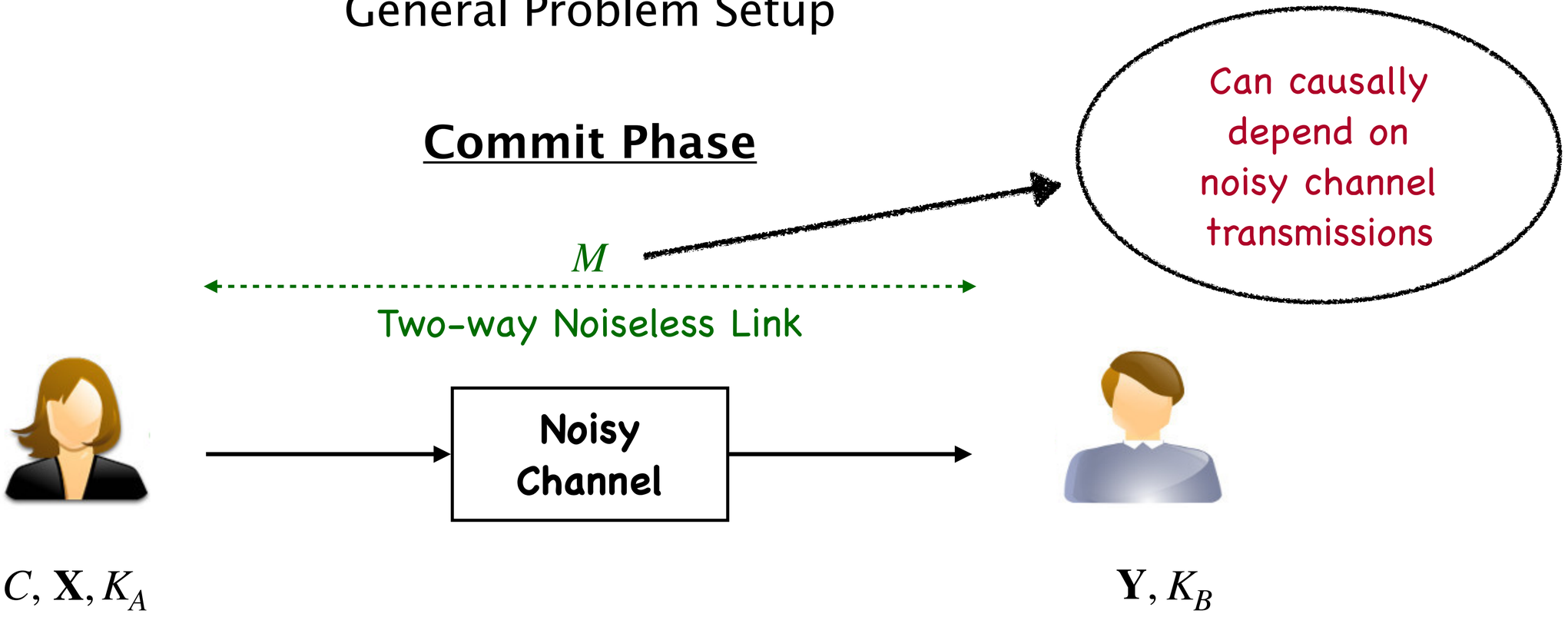
General Problem Setup

Commit Phase



Unconditionally Secure Commitment

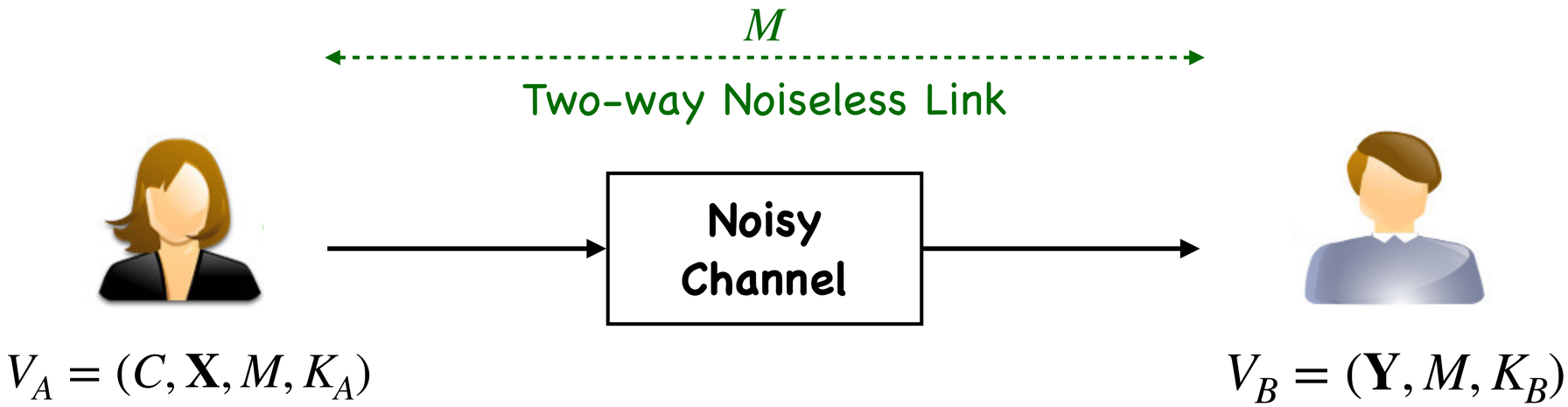
General Problem Setup



Unconditionally Secure Commitment

General Problem Setup

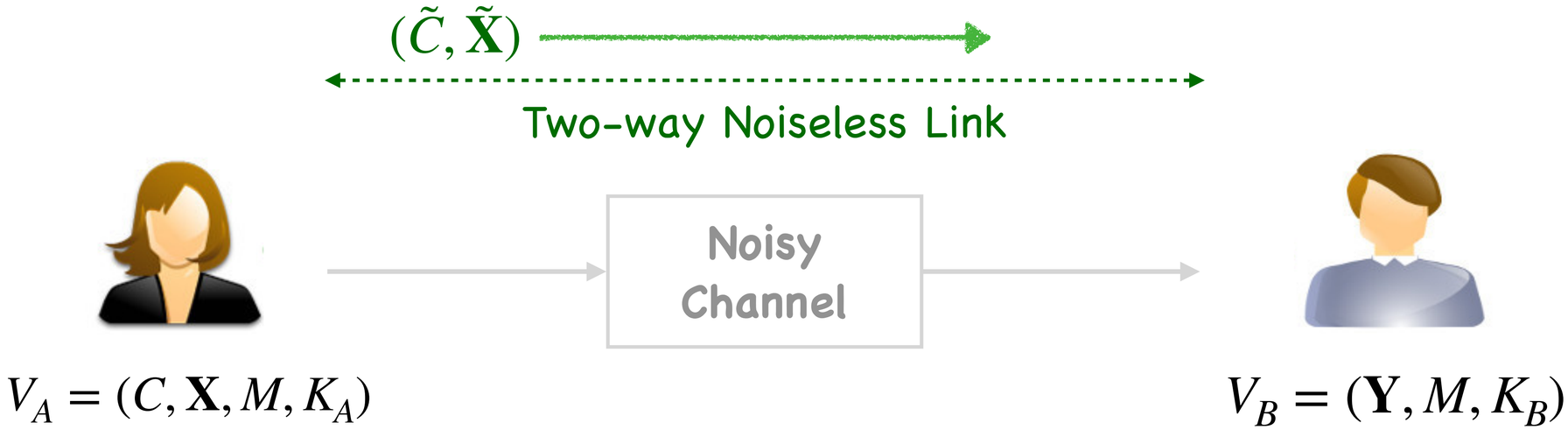
Commit Phase



Unconditionally Secure Commitment

General Problem Setup

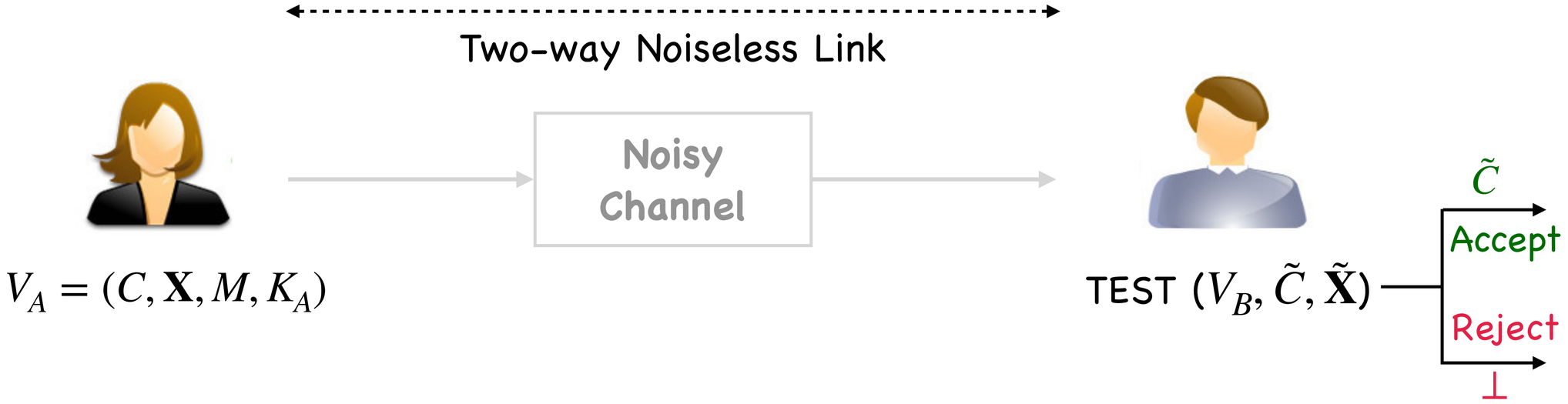
Reveal Phase



Unconditionally Secure Commitment

General Problem Setup

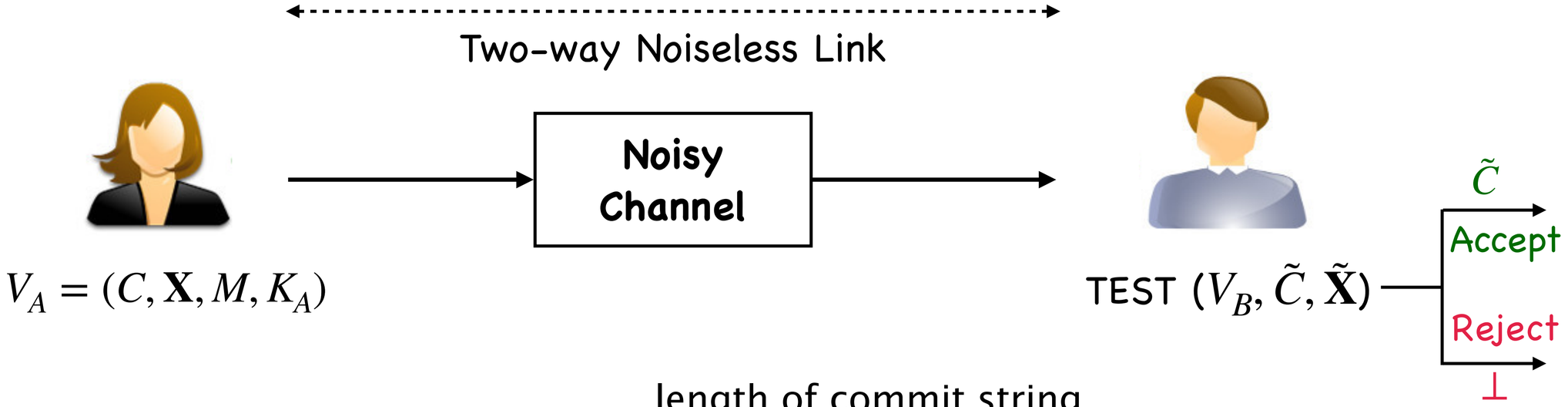
Reveal Phase



Unconditionally Secure Commitment

General Problem Setup

Commitment Rate



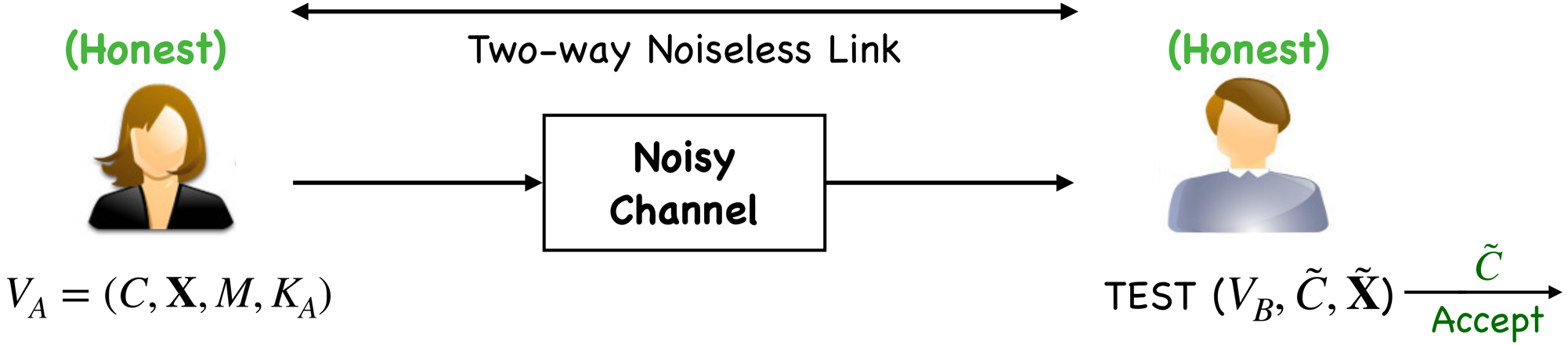
$$\text{Commitment Rate} := \frac{\text{length of commit string}}{\text{No. of uses of noisy channel}}$$

Unconditionally Secure Commitment

General Problem Setup – Security Guarantees

Soundness

(In reveal phase)



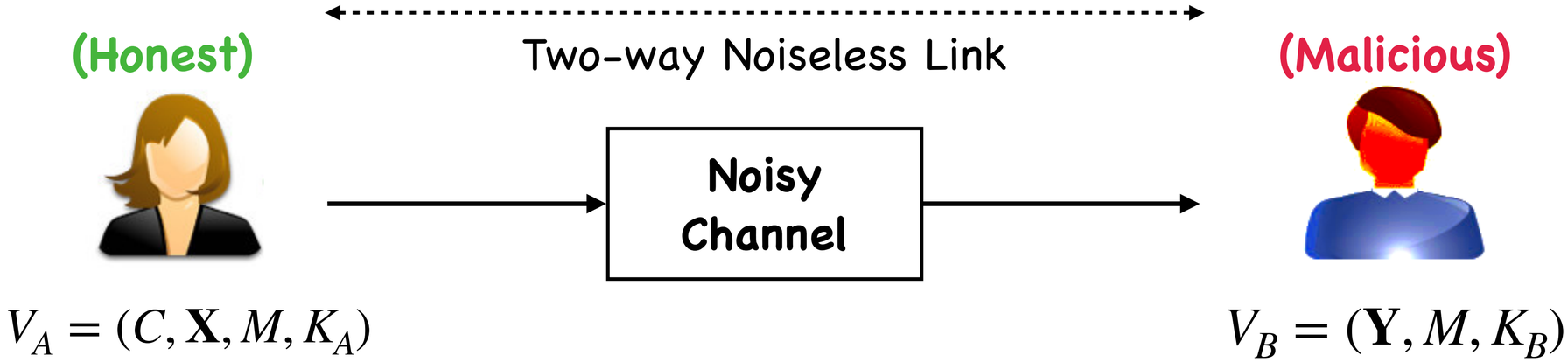
P (TEST $(V_B, \tilde{C}, \tilde{\mathbf{X}})$ = reject) $\leq \epsilon$

Unconditionally Secure Commitment

General Problem Setup – Security Guarantees

1-Concealment

(In commit phase)



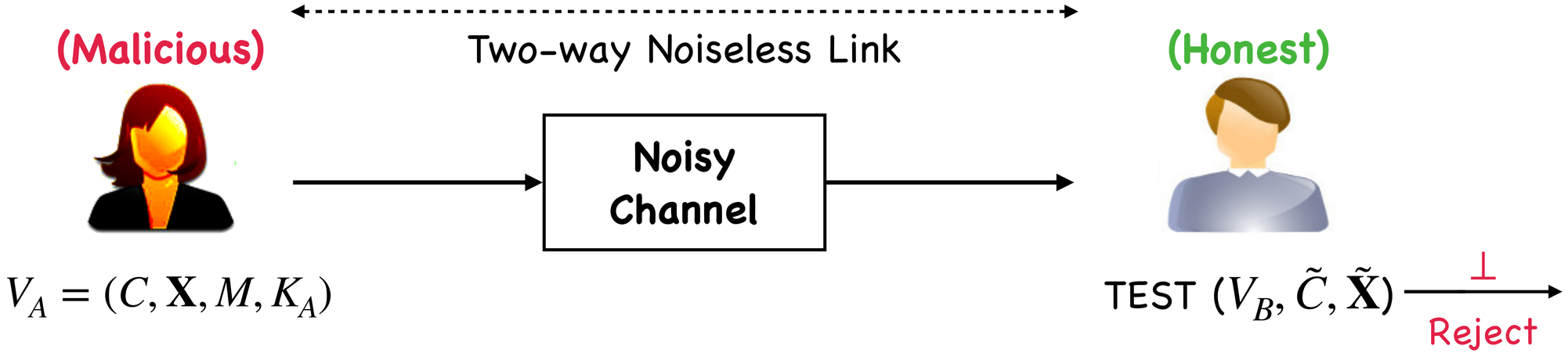
$$I(C; V_B) \leq \epsilon$$

Unconditionally Secure Commitment

General Problem Setup – Security Guarantees

1-Bindingness

(In reveal phase)



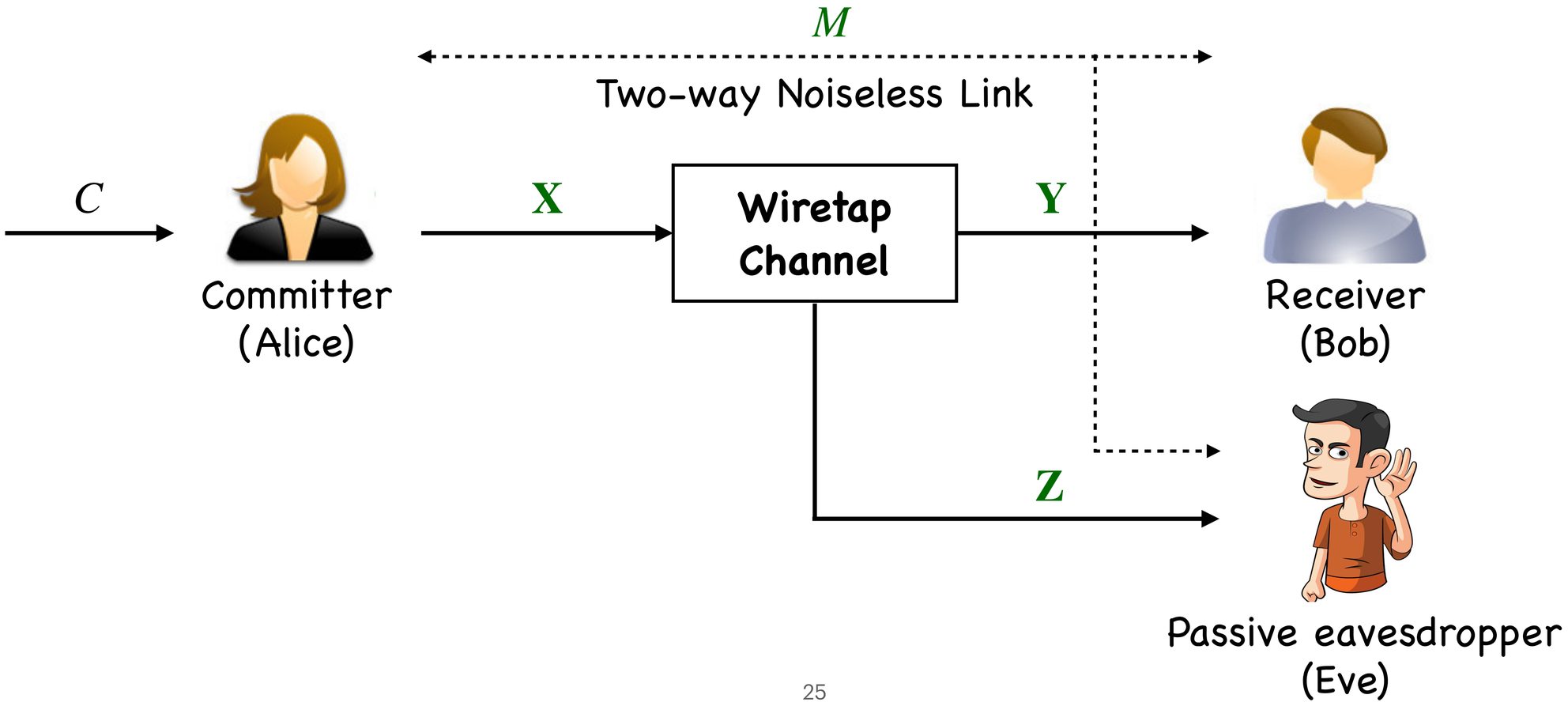
$$\mathbf{P}\ \{(\text{TEST}\ (V_B, \tilde{C}, \tilde{\mathbf{X}}) = \text{accept})\ \&\ (\text{TEST}\ (V_B, \hat{C}, \hat{\mathbf{X}}) = \text{accept})\} \leq \epsilon$$

$$\forall (\tilde{C}, \tilde{X}), (\hat{C}, \hat{X}) = \mathcal{A}(V_A)$$

Wiretapped Commitment

General Problem Setup

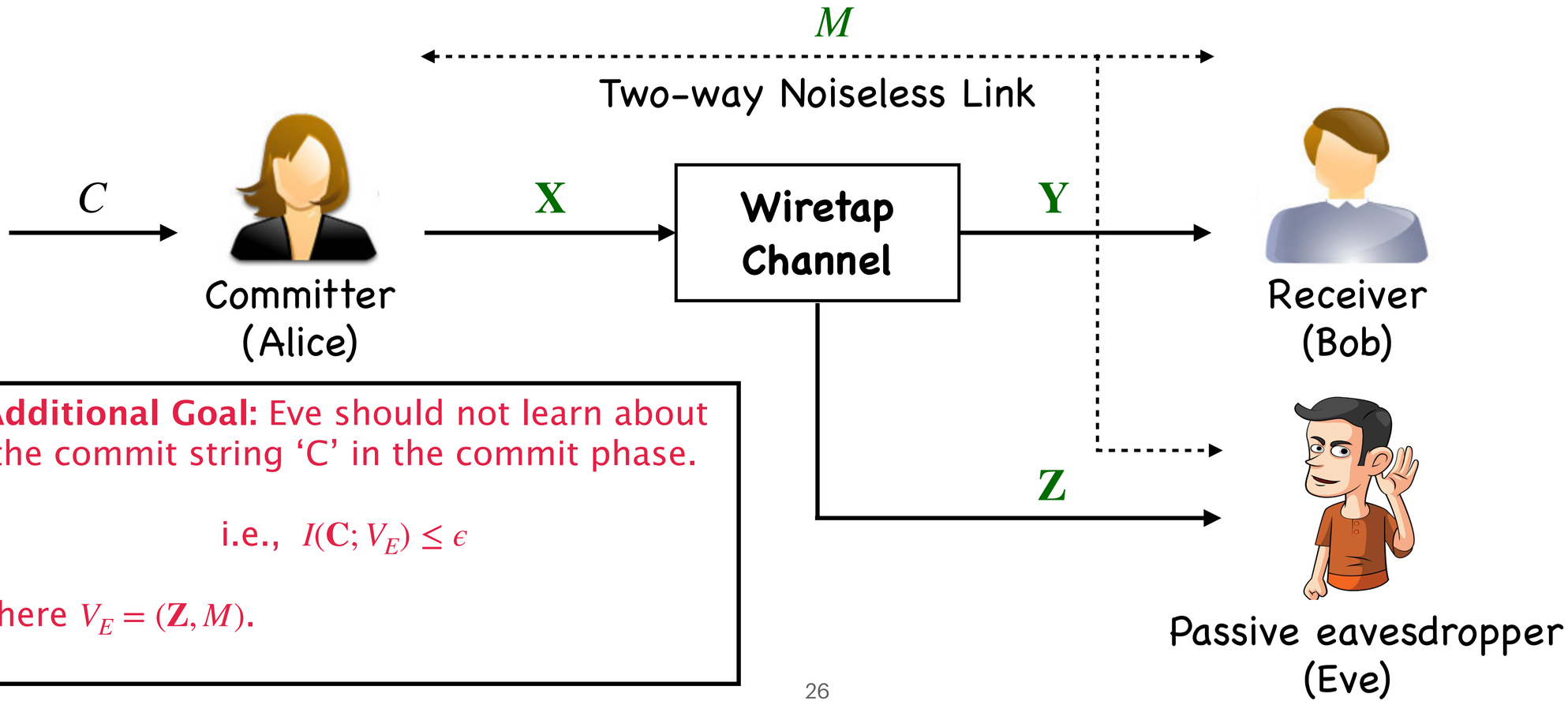
Commit & Reveal Phase



Wiretapped Commitment

General Problem Setup

Security against Eve



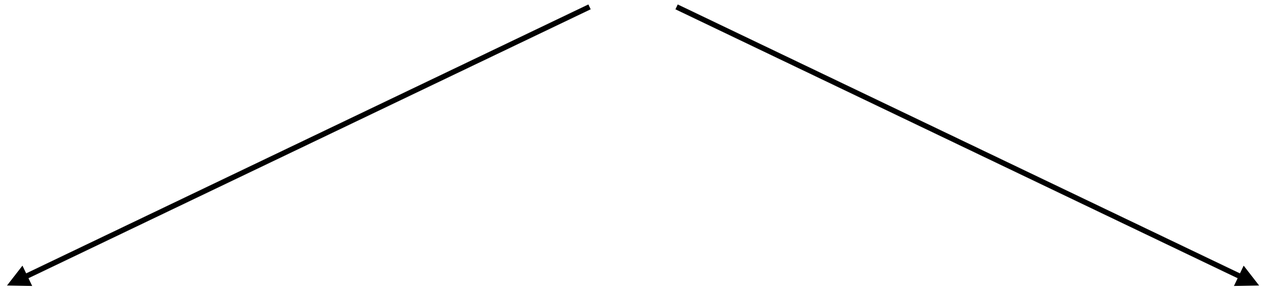
Additional Goal: Eve should not learn about the commit string 'C' in the commit phase.

i.e., $I(\mathbf{C}; V_E) \leq \epsilon$

Where $V_E = (\mathbf{Z}, M)$.

Wiretapped Commitment

Privacy Settings w.r.t Eavesdropper



1- Privacy Setting

- No collusion is allowed between the **legitimate users** and the **eavesdropper**.

2- Privacy Setting

- Collusion is allowed between a malicious **legitimate user** and the **eavesdropper**.

Wiretapped Oblivious Transfer - [Mishra, Dey, Prabhakaran, Diggavi '16]

Wiretapped Commitment

Security Guarantees under 1-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	1-Bindingness against Alice; Security against Eve
Honest	Malicious	Malicious	1-Concealment against Bob; Security against Eve
Malicious	Malicious	Malicious	No guarantee required

Wiretapped Commitment

Security Guarantees under 1-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	1-Bindingness against Alice; Security against Eve
Honest	Malicious	Malicious	1-Concealment against Bob; Security against Eve
Malicious	Malicious	Malicious	No guarantee required

Any commitment protocol must satisfy: **soundness**, **1- concealment**, **1-bindingness**, and **security against Eve.**

Wiretapped Commitment

Security Guarantees under 2-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve

Wiretapped Commitment

Security Guarantees under 2-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	

Wiretapped Commitment

Security Guarantees under 2-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	

Collusion

Wiretapped Commitment

Security Guarantees under 2-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	2-bindingness against Alice & Eve

Collusion

2-Bindingness:

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

$$\forall (\tilde{C}, \tilde{X}), (\hat{C}, \hat{X}) = \mathscr{A}(V_A, V_E)$$

Wiretapped Commitment

Security Guarantees under 2-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	2-bindingness against Alice & Eve
Honest	Malicious	Malicious	

Collusion

Wiretapped Commitment

Security Guarantees under 2-Privacy

Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	2-bindingness against Alice & Eve
Honest	Malicious	Malicious	2-concealment against Bob & Eve

Collusion

2- Concealment: $I(\mathbf{C}; V_B, V_E) \leq \epsilon$

Wiretapped Commitment

Security Guarantees under 2-Privacy

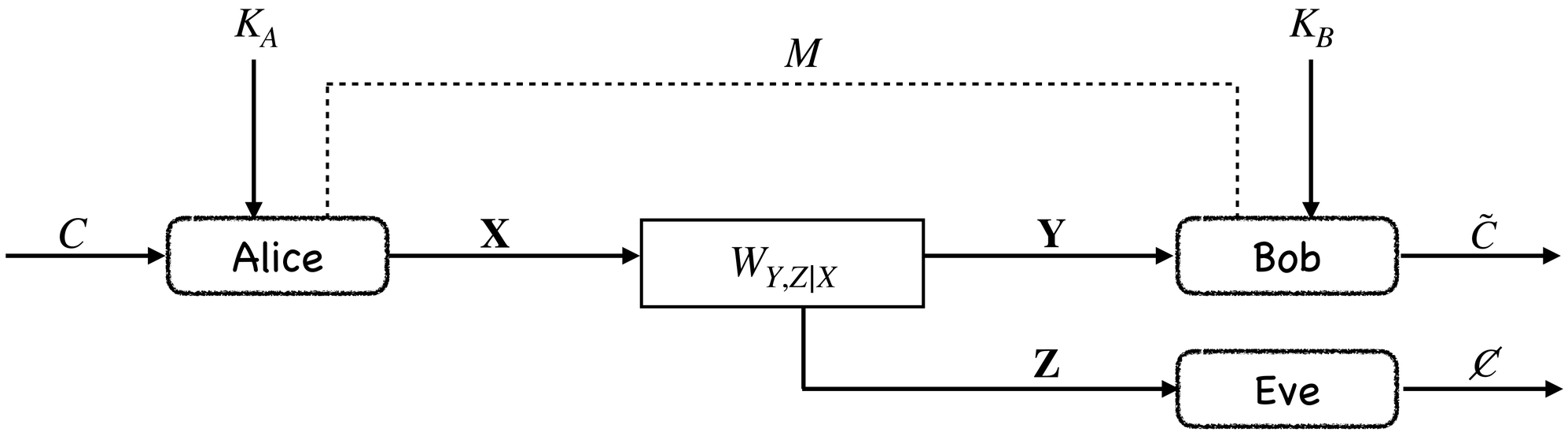
Alice	Bob	Eve	Security Guarantees
Honest	Honest	Malicious	Soundness; Security against Eve
Malicious	Honest	Malicious	2-bindingness against Alice & Eve
Honest	Malicious	Malicious	2-concealment against Bob & Eve
Malicious	Malicious	Malicious	No guarantee required

Any commitment protocol must satisfy: **soundness**, **2- concealment**, **2-bindingness**, and **security against Eve.**

Wiretapped Commitment

The Wiretap Channel Model

Binary Symmetric Broadcast Channel: BS-BC(p,q)



- $[W_{Y,Z|X}]_{Y|X} := W_{Y|X} \sim \text{BSC (p)}$
- $[W_{Y,Z|X}]_{Z|X} := W_{Z|X} \sim \text{BSC (q)}$

Wiretapped Commitment

Main Result - I

1-privacy capacity of BS-BC(p,q)

The 1-privacy commitment capacity of a BS-BC(p,q) is

$$\mathbb{C}_1 = \min\{H(p), H(q)\} .$$

Wiretapped Commitment

Corollary

1-privacy capacity of BS-BC(p,q)

The 1-privacy commitment capacity of a BS-BC(p,q) is

$$\mathbb{C}_1 = \min\{H(p), H(q)\}\ .$$

Case 1: $(q = 0, p \in (0,1/2))$:-

The channel to the eavesdropper Eve is a noiseless channel.

$$\mathbb{C}_1 = 0.$$

Wiretapped Commitment

Corollary

1-privacy capacity of BS-BC(p,q)

The 1-privacy commitment capacity of a BS-BC(p,q) is

$$\mathbb{C}_1 = \min\{H(p), H(q)\}\ .$$

Case 2: $(q = 1/2, p \in (0,1/2))$:-

The output at Eve is independent of Alice's transmission.

$$\mathbb{C}_1 = H(p)$$

Wiretapped Commitment

Corollary

1-privacy capacity of BS-BC(p,q)

The 1-privacy commitment capacity of a BS-BC(p,q) is

$$\mathbb{C}_1 = \min\{H(p), H(q)\} .$$

Case 2: $(q = 1/2, p \in (0,1/2))$:-

The output at Eve is independent of Alice's transmission.

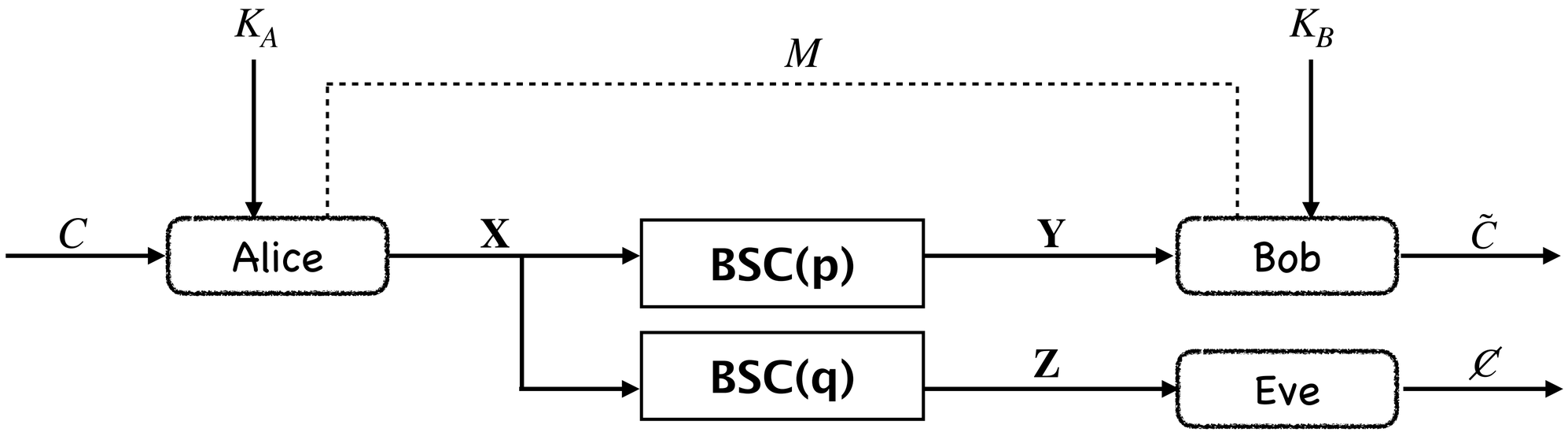
$$\mathbb{C}_1 = H(p)$$

commitment capacity of a BSC(p). [Winter et al. '03]

Wiretapped Commitment

Classes of BS-BC (p,q)

Independent Binary Symmetric Broadcast Channel: I-BS-BC(p,q)

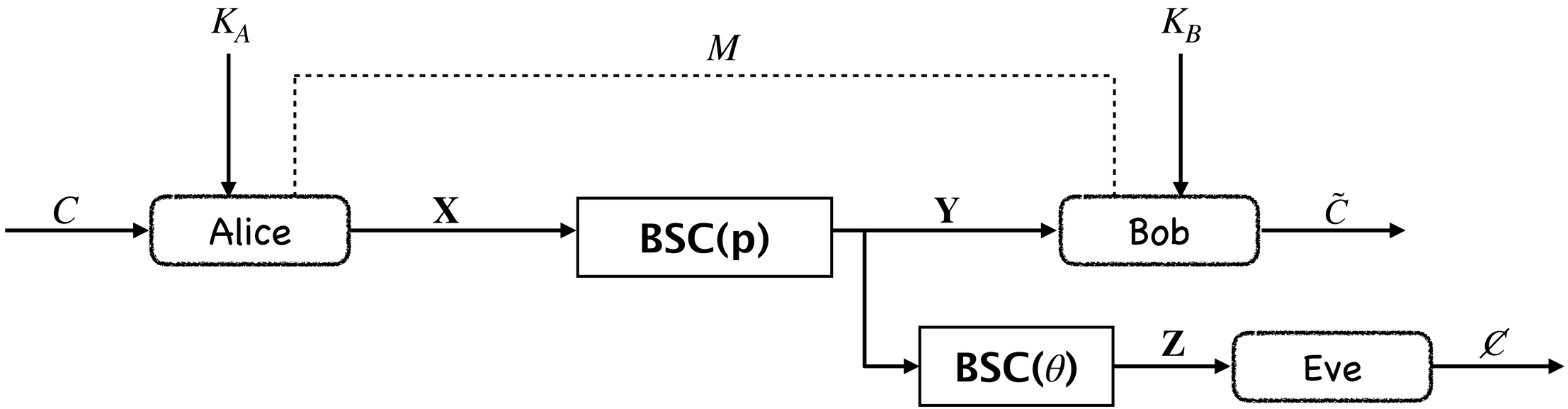


- Markov chain: $Y - X - Z$

Wiretapped Commitment

Classes of BS-BC (p,q)

Degraded Binary Symmetric Broadcast Channel: D-BS-BC(p,q)



- where $q = p \circledast \theta;\ (q > p)$
- Markov chain: $X - Y - Z$

Wiretapped Commitment

Corollary: 1- privacy capacity

1-privacy capacity of D-BS-BC(p,q)

The 1-privacy commitment capacity of a D-BS-BC(p,q) is

$$\mathbb{C}_1 = H(p)\,.$$

1-privacy capacity of I-BS-BC(p,q)

The 1-privacy commitment capacity of a I-BS-BC(p,q) is

$$\mathbb{C}_1 = \min\{H(p), H(q)\}\,.$$

Wiretapped Commitment

Main Result - II

2-privacy capacity of I-BS-BC(p,q)

The 2-privacy commitment capacity of a I-BS-BC(p,q) is

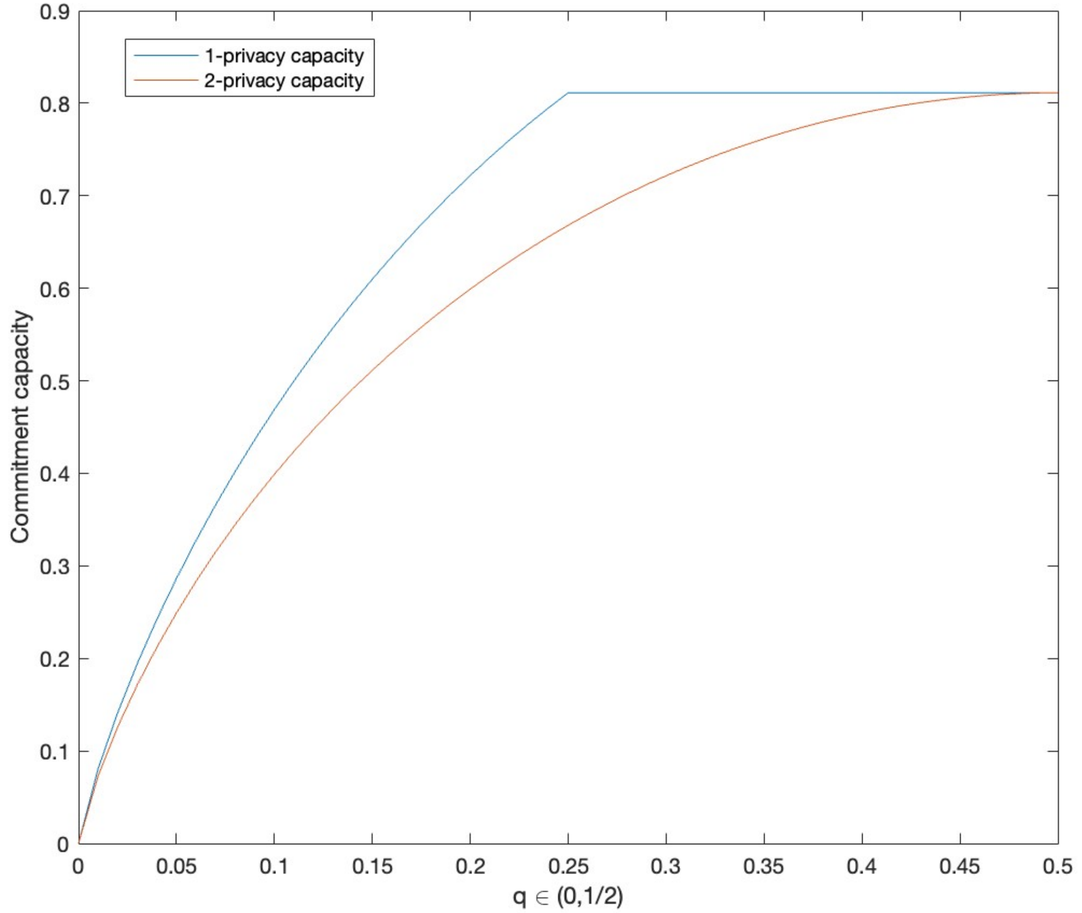
$$\mathbb{C}_2 = H(p) + H(q) - H(p \circledast q)\,.$$

Where $\circledast$ represents binary convolution i.e., $p \circledast q = p(1-q) + q(1-p)$.

Wiretapped Commitment

Comparison Example

1- privacy VS 2-privacy capacity for I-BS-BC (p = 0.25,q)



$$\mathbb{C}_1 \leq \mathbb{C}_2$$

Wiretapped Commitment

Conjecture

2-privacy capacity of D-BS-BC(p,q)

The 2-privacy commitment capacity of a D-BS-BC(p,q) is

$$\mathbb{C}_2 = H(p) - H\left(\frac{p-s}{1-2s}\right).$$

Where $s \in (0,1/2)$ is such that , $H(s) = H(p) + H(\theta) - H(q)$.

and $\theta = \frac{q-p}{1-2p}$.

Wiretapped Commitment

Achievability – Protocol overview – Commit Phase

- Alice wants to commit to a string, say C.
- Picks $\mathbf{X} \in \{0,1\}^n \sim$ ber $(1/2)$ i.i.d
- Transmits $\mathbf{X}$ over the BS-BC; Bob receives $\mathbf{Y}$ and Eve receives $\mathbf{Z}$.

BS-BC(p, q)

Wiretapped Commitment

Achievability – Protocol overview – Commit Phase

- Alice wants to commit to a string, say C.
- Picks $\mathbf{X} \in \{0,1\}^n \sim$ ber $(1/2)$ i.i.d
- Transmits $\mathbf{X}$ over the BS-BC; Bob receives $\mathbf{Y}$ and Eve receives $\mathbf{Z}$.

BS-BC(p, q)

- 'Single' or 'Double' round of Hash challenge from Bob to Alice.

Two-way Noiseless Link

Wiretapped Commitment

Achievability – Protocol overview – Commit Phase

- Alice wants to commit to a string, say C.
- Picks $\mathbf{X} \in \{0,1\}^n \sim$ ber $(1/2)$ i.i.d
- Transmits $\mathbf{X}$ over the BS-BC; Bob receives $\mathbf{Y}$ and Eve receives $\mathbf{Z}$.

BS-BC(p, q)

- 'Single' or 'Double' round 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

Wiretapped Commitment

Achievability – Protocol overview – Reveal Phase

- Alice reveals $(\tilde{c}, \tilde{u}^m)$ to Bob.
- Bob performs tests to accept / reject $\tilde{c}$.
  - ⟶ Typicality Test
  - ⟶ Hash Challenge Test
  - ⟶ OTP Test

Two-way
Noiseless Link

Wiretapped Commitment

Achievability – Protocol overview – Commit Phase

- Alice wants to commit to a string, say C.
- Picks $\mathbf{X} \in \{0,1\}^n \sim$ ber $(1/2)$ i.i.d
- Transmits $\mathbf{X}$ over the BS-BC; Bob receives $\mathbf{Y}$ and Eve receives $\mathbf{Z}$.

- Single round of Hash challenge from Bob to Alice.

Guarantees **Bindingness** against malicious Alice (possibly in collusion with Eve).

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

Wiretapped Commitment

Achievability – Protocol overview – Commit Phase

- Alice wants to commit to a string, say C.
- Picks $\mathbf{X} \in \{0,1\}^n \sim$ ber $(1/2)$ i.i.d
- Transmits $\mathbf{X}$ over the BS-BC; Bob receives $\mathbf{Y}$ and Eve receives $\mathbf{Z}$.

- Single round of Hash challenge from Bob to Alice.

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

Guarantees **Concealment** against malicious Bob (possibly in collusion with Eve).

Wiretapped Commitment

Summary

- Proposed the wiretapped commitment problem in presence of a passive eavesdropper.
- Studied under 2 settings, namely, **1-privacy** and **2-privacy**.

- Completely characterized the commitment capacity of BS-BC channels under 1-privacy.
- Commitment capacity of I-BS-BC channels under 2-privacy.
- Conjecture on the commitment capacity of D-BS-BC channels under 2-privacy.