20/October/2021

Some Topics on Information Theoretic Security

Yasutada Oohama

University of Electro-Communications

Introduction

- In this plenary talk we present our previous works on information theoretic security consisting of three miscellaneous topics.

I. Relay channel with confidential messages (RCC)

II. Broadcast channel with confidential messages (BCC) with randomness constraints

III. Information theoretic analysis of Shannon cipher system under side-channel attacks

Introduction

- In this plenary talk we present our previous works on information theoretic security consisting of three miscellaneous topics.
- Those topics provide some specific but interesting problems arising inherently in communication systems with security requirement.

I. Relay channel with confidential messages (RCC)

$\sim$ *Interplay between the two roles of the relay as a "helper" and as an "eavesdropper"*

II. Broadcast channel with confidential messages (BCC) with randomness constraints

$\sim$ *Relationship between randomness and security*

III. Information theoretic analysis of Shannon cipher system under side-channel attacks

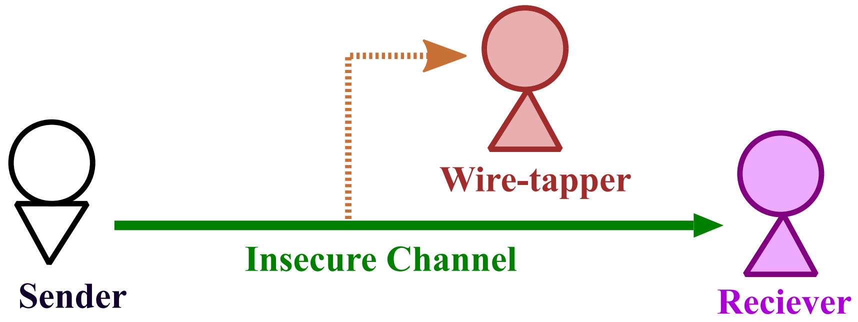
$\sim$ *Relationship between the privacy amplification and the strong converse theorem for one helper source coding system*

I. Relay Channel with Confidential Messages

Presentation Overview

Introduction

Security of Communication Systems



☐ Information Theoretical Analysis of Secure Systems

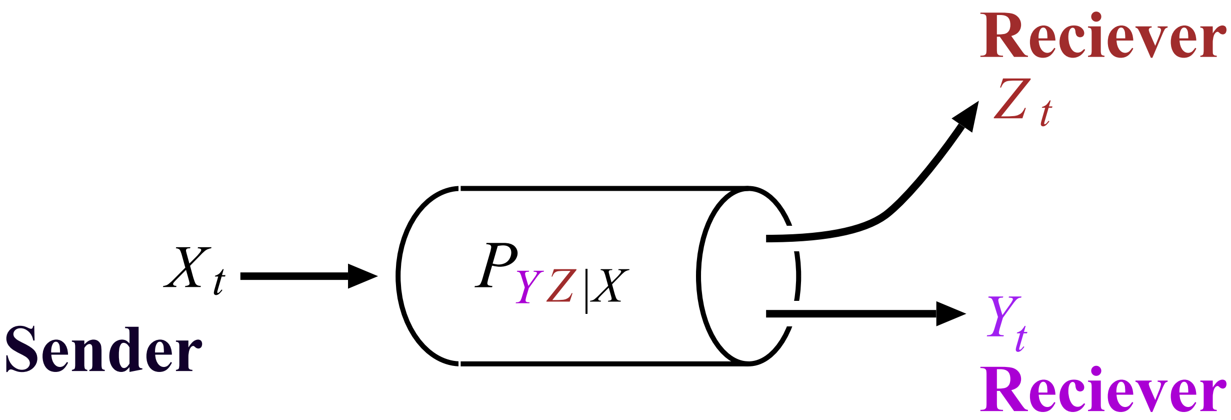
- "Wire-Tap Channels"(Wyner, IT 75)
- "Broadcast Channels with Confidential Messages" (Csiszár and Körner, IT 78)

Multiuser Communication Networks

$\Downarrow$

Secure communication for unauthorized users

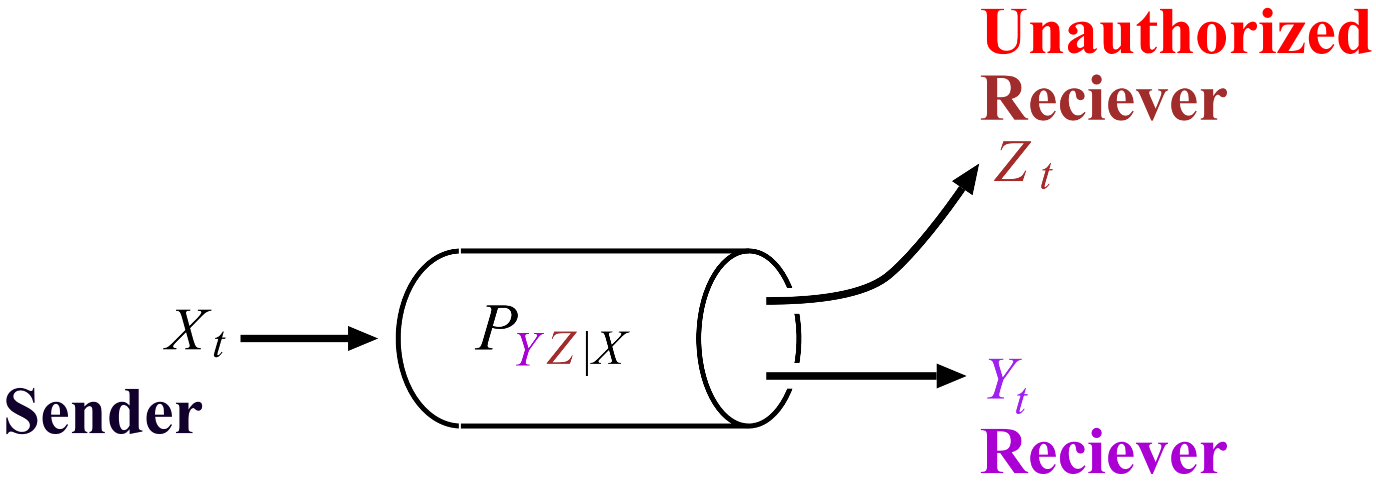
Broadcast Channel



Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The broadcast channel is defined by a discrete memoryless channel specified with

$$P_{YZ|X} = \{P_{YZ|X}(y, z|x)\}_{(x,y,z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}} \, .$$

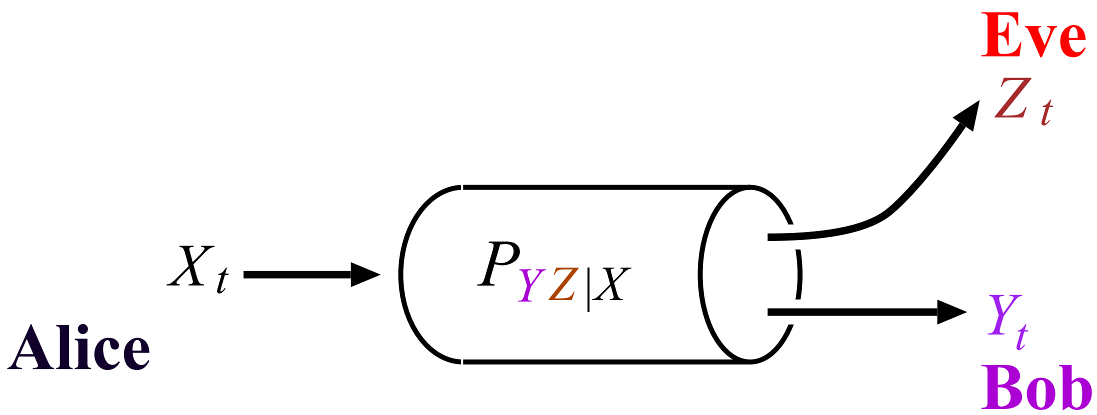
Broadcast Channel



Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The broadcast channel is defined by a discrete memoryless channel specified with

$$P_{YZ|X} = \{P_{YZ|X}(y, z|x)\}_{(x,y,z)\in\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}} \,.$$

Broadcast Channel

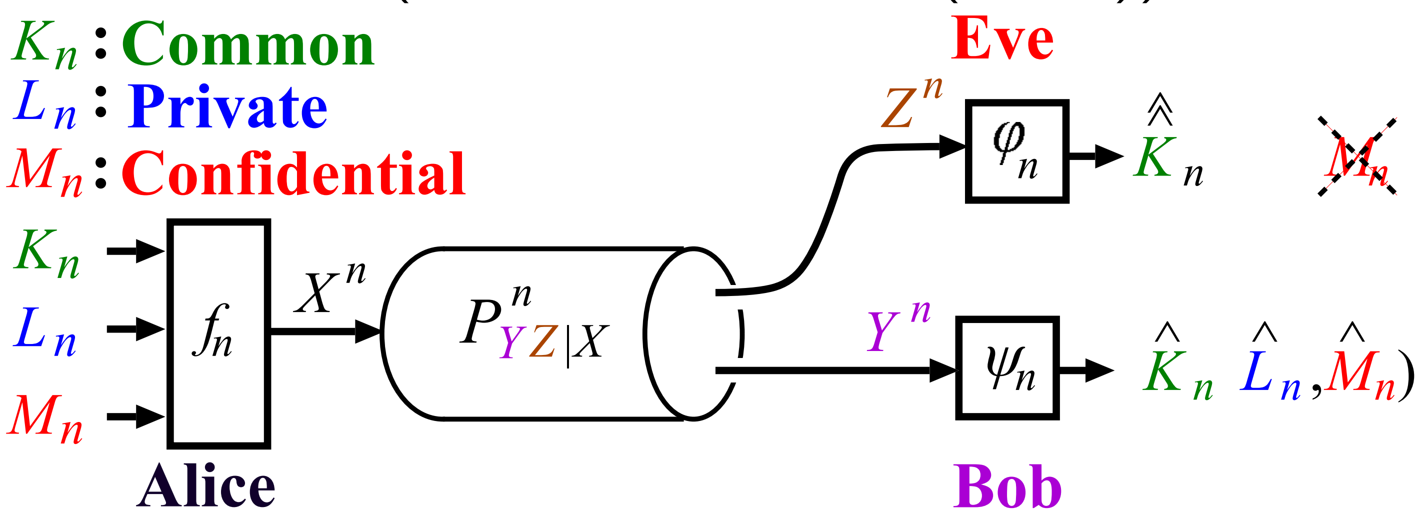


Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The broadcast channel is defined by a discrete memoryless channel specified with

$$P_{YZ|X} = \{P_{YZ|X}(y, z|x)\}_{(x,y,z)\in\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}} .$$

Broadcast Channels with Confidential Messages

BCC(Csiszár and Körner(IT 78))



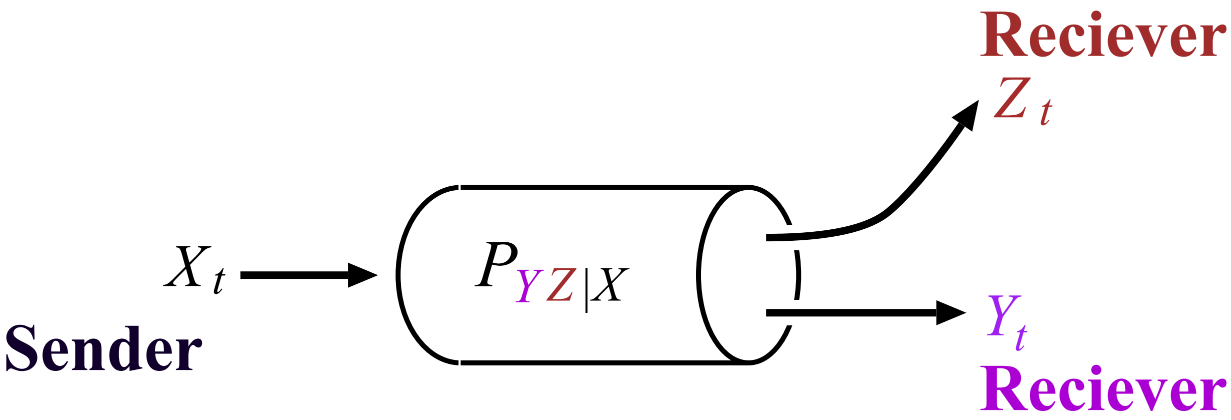
☐ Information Leakage on Confidential Messages

- $D_n := I(M_n; Z^n)$

$$\limsup_{n\to\infty} \frac{1}{n} D_n = \limsup_{n\to\infty} \frac{1}{n} I(M_n; Z^n) = 0, \text{ (weak secrecy criterion)}$$

$$\limsup_{n\to\infty} D_n = \limsup_{n\to\infty} I(M_n; Z^n) = 0. \text{ (strong secrecy criterion)}$$

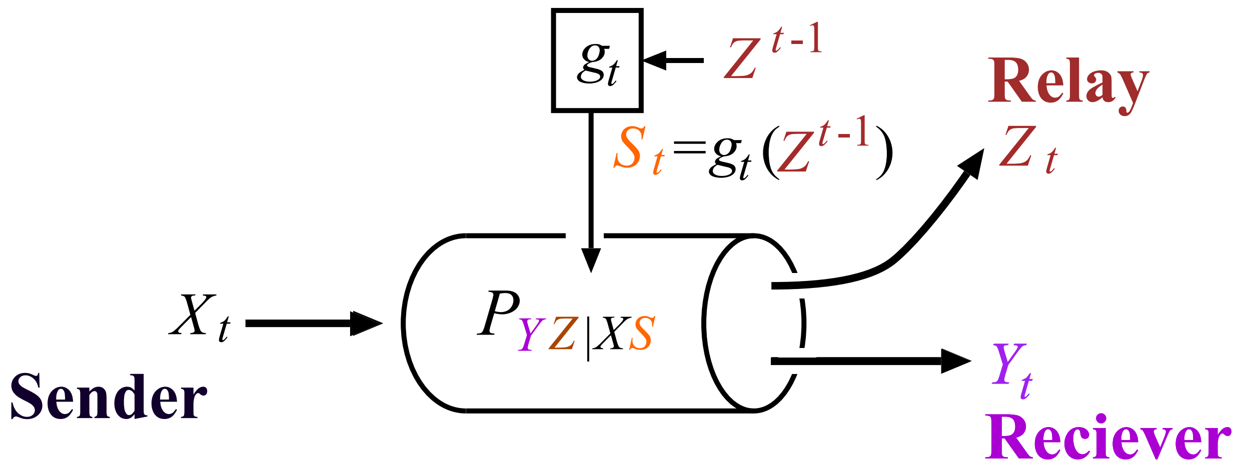
Broadcast Channel and Relay Channel



Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The broadcast channel is defined by a discrete memoryless channel specified with

$$P_{YZ|X} = \{P_{YZ|X}(y, z|x)\}_{(x,y,z)\in\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}} \,.$$

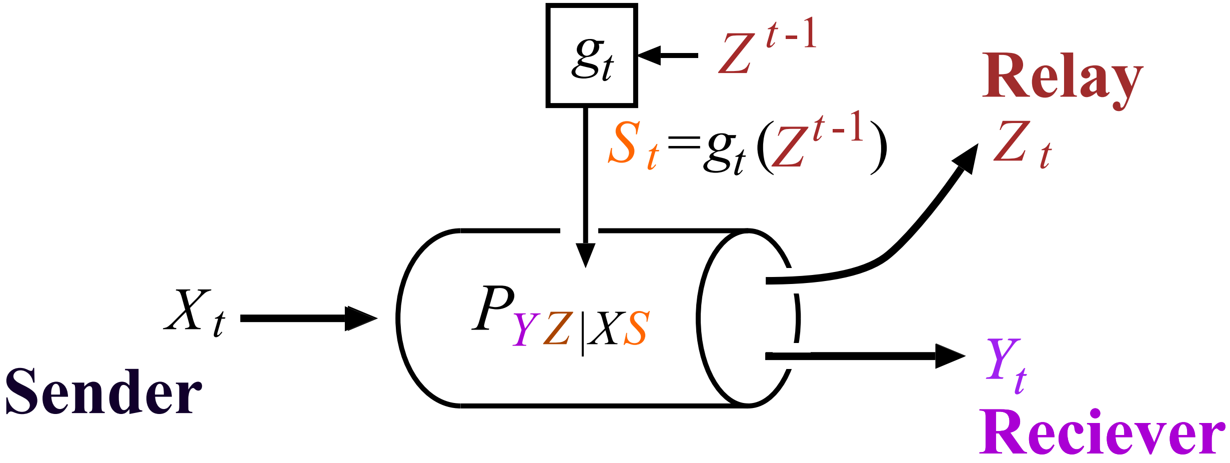
Broadcast Channel and Relay Channel



Let $\mathcal{X}, \mathcal{S}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The relay channel is defined by a discrete memoryless channel specified with

$$P_{YZ|XS} = \{P_{YZ|XS}(y, z|x, s)\}_{(x,s,y,z)\in\mathcal{X}\times\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}.$$

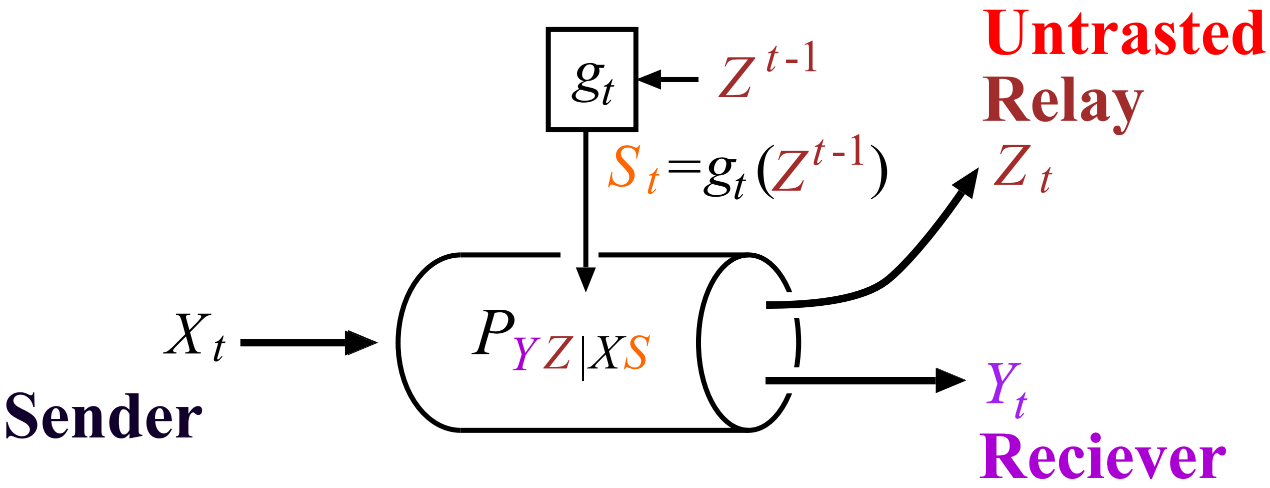
Relay Channel



Let $\mathcal{X}, \mathcal{S}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The relay channel is defined by a discrete memoryless channel specified with

$$P_{YZ|XS} = \{P_{YZ|XS}(y, z|x, s)\}_{(x,s,y,z)\in\mathcal{X}\times\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}} \, .$$

Relay Channel

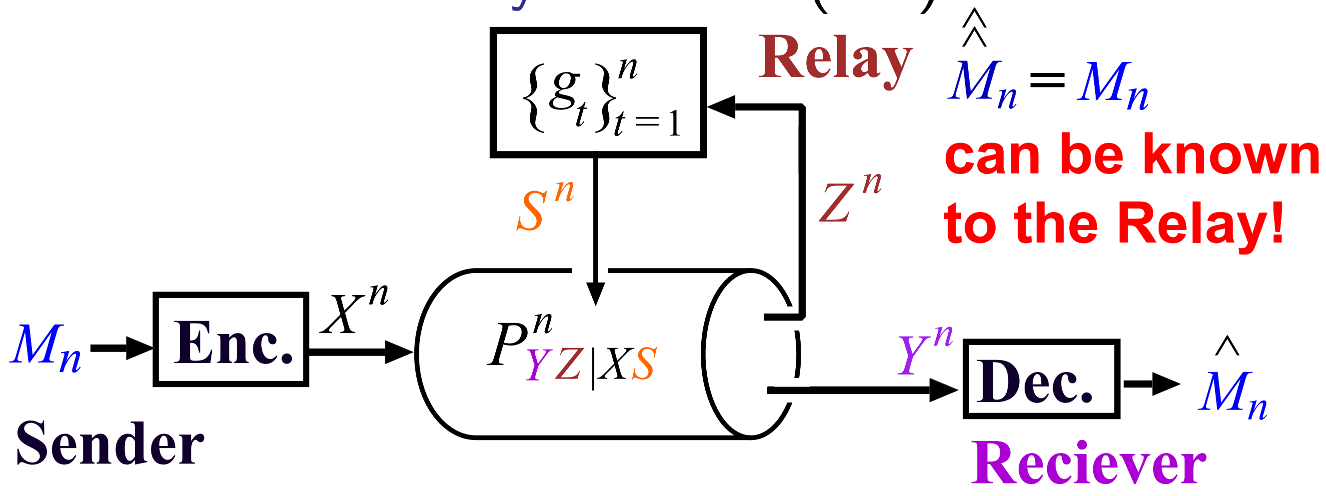


Let $\mathcal{X}, \mathcal{S}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The relay channel is defined by a discrete memoryless channel specified with

$$P_{YZ|XS} = \{P_{YZ|XS}(y, z|x, s)\}_{(x,s,y,z)\in\mathcal{X}\times\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}} .$$

Security of Relay Channels

Relay Channel (RC)



☐ Coding strategy of Cover and El Gamal(IT 79) for the RC

- Relay obtains all messages flowing through the channel.

☐ Security of RC should be studied.

- Some messages should be confidential to the relay.
- Comm. Syst. with Confidential Messages

⇓ Oohama (ITW 01, Cairns)

Relay Channels with Confidential Messages (RCC)

Works on RCC or the Security of Relay Channels

- Relay Channels with Confidential Messages
  by Oohama (ISIT 07, Nice)
- Relay-Eavesdropper Channel
  by Lai and El Gamal (IT 08)
- Cooperation with an Untrusted Relay: A Secrecy Perspective
  by He and A. Yener (IT 10)
- Refine and extensions of Oohama (ITW 01, ISIT 07) by Oohama and Watanabe (SITA 10)

Refine and Extensions of Oohama (ITW 01)

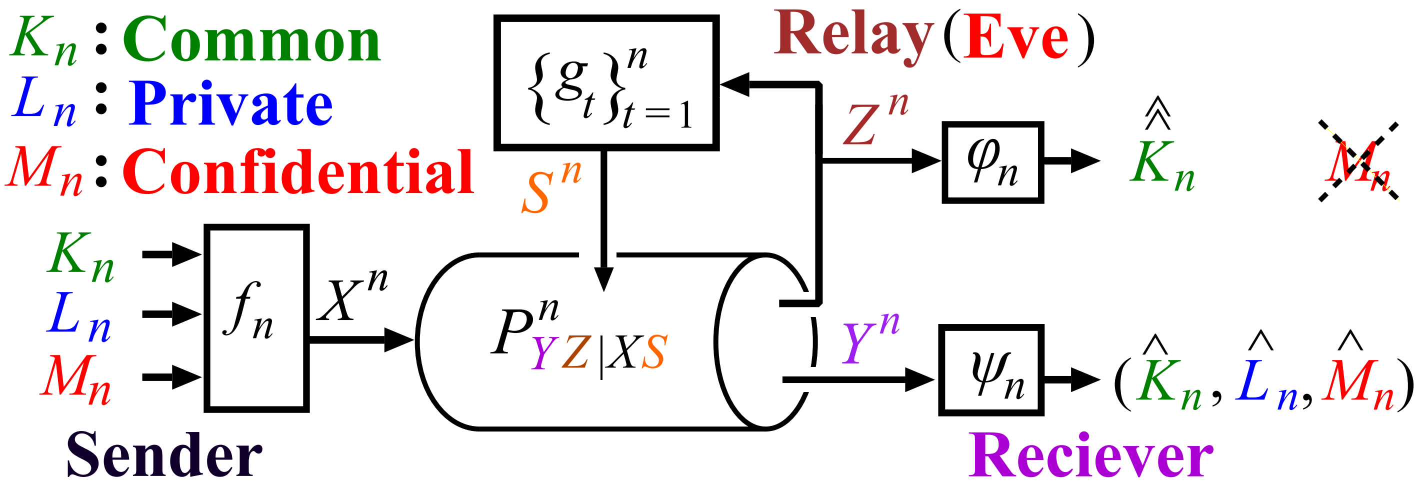
- Refine or extensions of Oohama (ITW 01) were given by Oohama (ISIT 07), Oohama and Watanabe (SITA 10).
  1. Definitions of rate regions in two cases; deterministic/stochastic encoders
  2. Inner bounds and outer bounds of the rate regions
  3. The case where inner and outer bounds match.
     $\rightarrow$ Reversely degraded relay channels, semi deterministic relay channels

Refine and Extensions of Oohama (ITW 01)

- Refine or extensions of Oohama (ITW 01) were given by Oohama (ISIT 07), Oohama and Watanabe (SITA 10).

1. Definitions of rate regions in two cases; deterministic/stochastic encoders
2. **2.** Inner bounds and outer bounds of the rate regions
3. **3.** The case where inner and outer bounds match.
   $\rightarrow$ Reversely degraded relay channels, Semi deterministic relay channels

Problem Setting of RCC



Encoder $f_n : \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{M}_n \to \mathcal{X}^n,$

Receiver Decoder $\psi_n : \mathcal{Y}^n \to \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{M}_n$

Relay Encoder $\{g_t\}_{t=1}^n, \; S^n = \{g_t(Z^{t-1})\}_{t=1}^n$

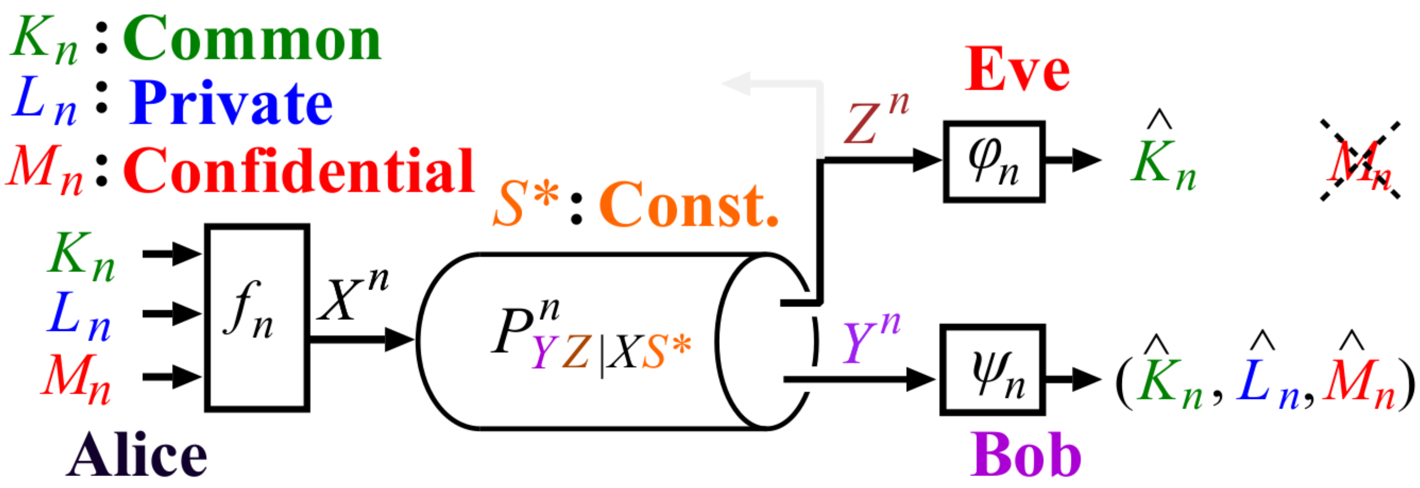
Relay Decoder $\varphi_n : \mathcal{Z}^n \to \mathcal{K}_n$

Receiver Error Prob. $\lambda_1^{(n)} := \Pr\{(\hat{K}_n, \hat{L}_n, \hat{M}_n) \neq (K_n, L_n, M_n)\}$

Relay Error Prob. $\lambda_2^{(n)} := \Pr\{\hat{\hat{K}}_n \neq K_n\}$

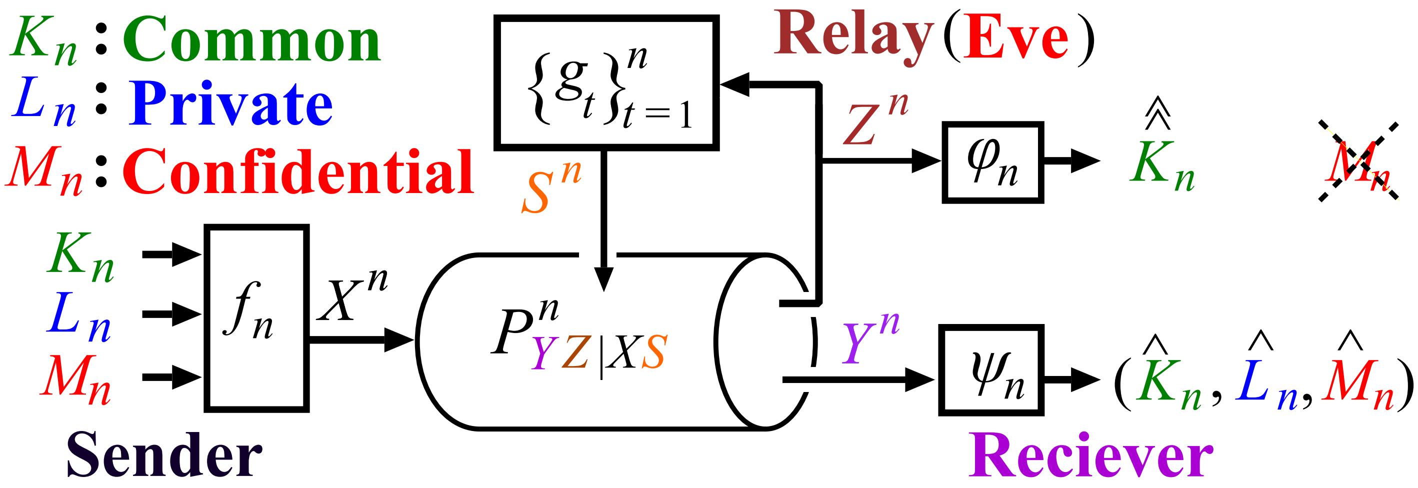
Security $D_n := D(P_{M_n Z^n} || P_{M_n} \times P_{Z^n}) = I(M_n; Z^n)$

Relation between RCC and BCC



RCC includes the BCC as a special case by letting $|\mathcal{S}| = 1$.

Rate Region of RCC



(R_0, R_1, R_s) is *achievable* $\overset{\mathrm{def}}{\Leftrightarrow} \exists\{(f_n, \{g_t\}_{t=1}^n, \psi_n, \varphi_n)\}_{n=1}^\infty$ s.t.

$$\lim_{n\to\infty} \lambda_i^{(n)} = 0, i = 1, 2, \ \limsup_{n\to\infty} \frac{D_n}{n} = 0 \text{ (weak secrecy criterion)}$$

$$\liminf_{n\to\infty} \frac{\log|\mathcal{K}_n|}{n} \geq R_0, \ \lim_{n\to\infty} \frac{\log|\mathcal{L}_n|}{n} = R_1, \ \liminf_{n\to\infty} \frac{\log|\mathcal{M}_n|}{n} \geq R_\mathrm{s}.$$

For simplicity of notation set $\Gamma := P_{YZ|XS}$.

$$\mathcal{R}_\mathrm{rcc}(\Gamma) = \{(R_0, R_1, R_\mathrm{s}) : (R_0, R_1, R_\mathrm{s}) \text{ is achievable.}\}$$

A Pair of Inner and Outer Bounds of $\mathcal{R}_{\rm rcc}(\Gamma)$

$$\mathcal{P}_1 := \{(U,X,S) \in \mathcal{U}\times\mathcal{X}\times\mathcal{S} : |\mathcal{U}| \le |\mathcal{X}||\mathcal{S}|+3,\ U \leftrightarrow XS \leftrightarrow YZ\},$$

$$\begin{aligned}\tilde{\mathcal{R}}^{(\rm in)}(\Gamma) := \{(R_0,R_1,R_{\rm s}) : \exists (U,X,S)\in\mathcal{P}_1 \text{ s.t. } & \\ R_0 &\le \min\{I(Y;US), I(Z;U|S)\},\\ R_1+R_{\rm s} &\le I(X;Y|US),\\ R_{\rm s} &\le \boxed{I(X;Y|US)-I(X;Z|US)}\},\end{aligned}$$

$$\begin{aligned}\tilde{\mathcal{R}}^{(\rm out)}(\Gamma) := \{(R_0,R_1,R_{\rm s}) : \exists (U,X,S)\in\mathcal{P}_1 \text{ s.t. } & \\ R_0 &\le \min\{I(Y;US), I(Z;U|S)\},\\ R_1+R_{\rm s} &\le I(X;YZ|US),\\ R_0+R_1+R_{\rm s} &\le I(XS;Y),\\ R_{\rm s} &\le \boxed{I(X;Y|ZUS)}\}.\end{aligned}$$

Theorem 1 For any relay channel Γ,

$$\tilde{\mathcal{R}}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm rcc}(\Gamma) \subseteq \tilde{\mathcal{R}}^{(\rm out)}(\Gamma).$$

Reversely Degraded Relay Channel

An essential difference between $\tilde{\mathcal{R}}_{\mathrm{d}}^{(\mathrm{in})}(\Gamma)$ and $\tilde{\mathcal{R}}_{\mathrm{d}}^{(\mathrm{out})}(\Gamma)$ is a gap Δ given by

$$\Delta := I(X;Y|ZUS) - [I(X;Y|US) - I(X;Z|US)]$$
$$= I(X;ZY|US) - I(X;Y|US) = I(X;Z|YUS)\,.$$

Important Fact

$\Delta = 0$ if Γ satisfies the following

$$\Gamma(z,y|x,s) = \Gamma(z|y,s)\Gamma(y|x,s),\ (x,s,y,z) \in \mathcal{X} \times \mathcal{S} \times \mathcal{Y} \times \mathcal{Z}$$
$$\Longleftrightarrow X \leftrightarrow SY \leftrightarrow Z\,.$$

Cover and El. Gamal(IT 81) called the above Γ reversely degraded relay channel.

Degraded Relay Channel

Cover and El. Gamal(IT 81) called the relay channel is degraded if Γ satisfies

$$\Gamma(z,y|x,s) = \Gamma(y|z,s)\Gamma(z|x,s),\ (x,s,y,z) \in \mathcal{X} \times \mathcal{S} \times \mathcal{Y} \times \mathcal{Z}$$
$$\Longleftrightarrow X \leftrightarrow SZ \leftrightarrow Y$$

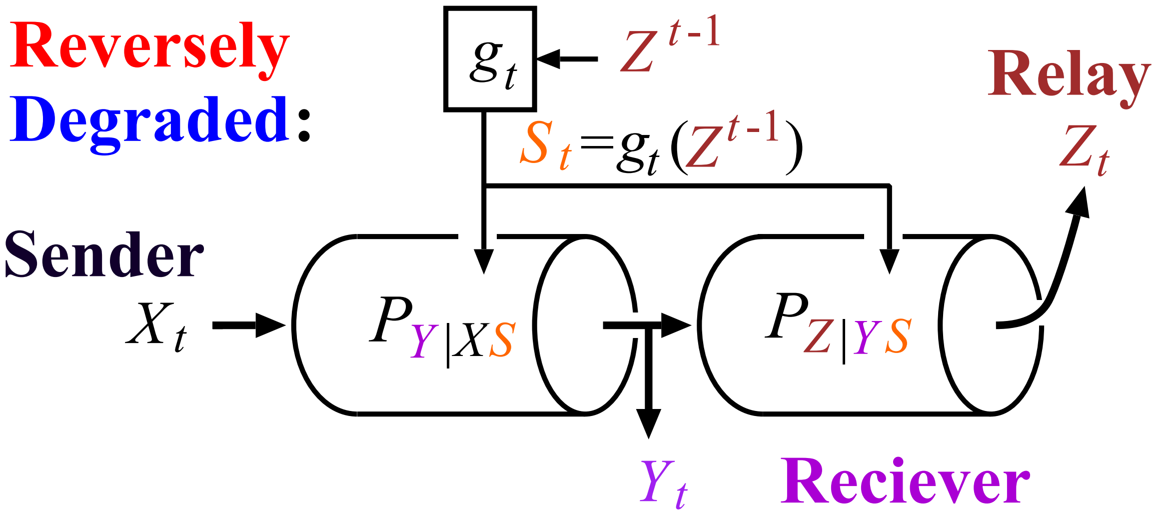
Important Fact

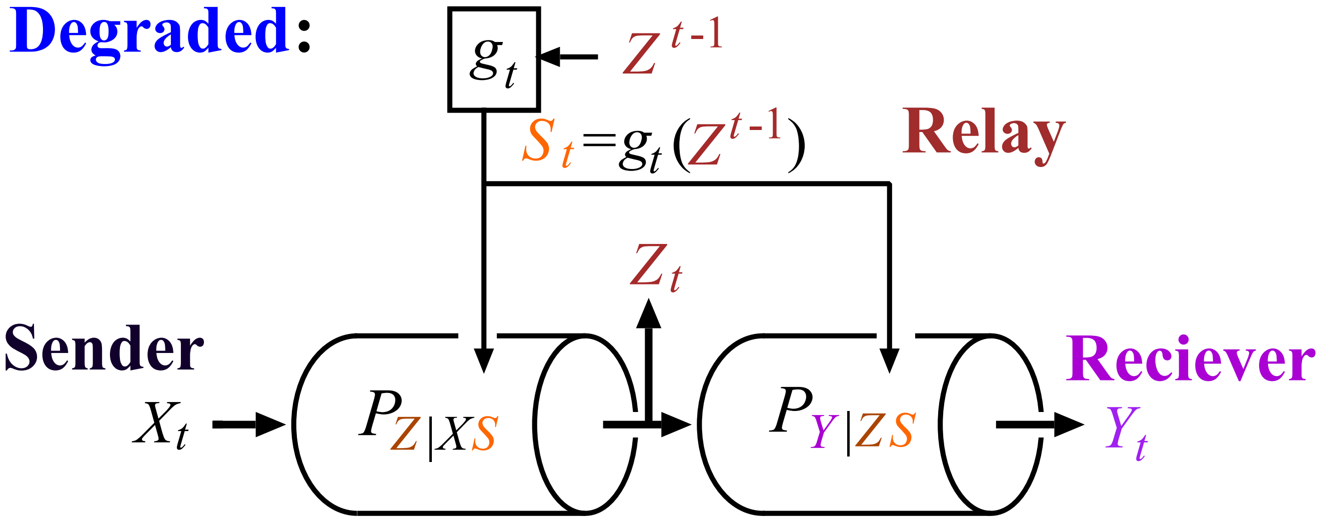
If the relay channel is degraded, then $I(X;Y|ZUS) = 0$.

→ R_{s} must be zero.

→ No security on the private messages is guaranteed!

Two Degraded Relay Channels





Results on the Two Degraded Cases

Corollary 1 For the reversely degraded relay channel Γ,

$$\tilde{\mathcal{R}}^{(\mathrm{in})}(\Gamma) = \mathcal{R}_{\mathrm{rcc}}(\Gamma) = \tilde{\mathcal{R}}^{(\mathrm{out})}(\Gamma) \, .$$

Corollary 2 When the relay channel Γ is degraded, no security on the private messages is guaranteed.

Some remarks on the two corollaries:

- Corollary 1 implies that the coding strategy attaining $\tilde{\mathcal{R}}_{\mathrm{d}}^{(\mathrm{in})}(\Gamma)$ in Theorem 1 is optimal in the case of reversely degraded relay channels.
- Corollary 2 meets our intuition in the sense that if the relay channel is degraded, the relay can do anything that the destination can.

Another Pair of Inner and Outer Bounds of $\mathcal{R}_{\mathrm{rcc}}(\Gamma)$

$$\mathcal{Q}_1 := \{(U, V, X, S) : |\mathcal{U}| \le |\mathcal{X}||\mathcal{S}| + 3, |\mathcal{V}| \le (|\mathcal{X}||\mathcal{S}|)^2 + 4|\mathcal{X}||\mathcal{S}| + 3, \underline{U \leftrightarrow V \leftrightarrow XS \leftrightarrow YZ}, US \leftrightarrow V \leftrightarrow X\},$$

$$\mathcal{Q}_2 := \{(U, V, X, S) : |\mathcal{U}| \le |\mathcal{Z}||\mathcal{X}||\mathcal{S}| + 3, |\mathcal{V}| \le (|\mathcal{Z}||\mathcal{X}||\mathcal{S}|)^2 + 4|\mathcal{Z}||\mathcal{X}||\mathcal{S}| + 3, \underline{U \leftrightarrow V \leftrightarrow XSZ \leftrightarrow Y}, \underline{US \leftrightarrow VX \leftrightarrow Z}, US \leftrightarrow V \leftrightarrow X\}.$$

$\mathcal{R}^{(\mathrm{in})}(\Gamma) := \{(R_0, R_1, R_{\mathrm{s}}) : \exists (U, V, X, S) \in \mathcal{Q}_1$ s.t.

$$R_0 \le \min\{I(Y; US), I(Z; U|S)\},$$
$$R_0 + R_1 + R_{\mathrm{s}} \le I(V; Y|US) + \min\{I(Y; US), I(Z; U|S)\},$$
$$R_{\mathrm{s}} \le I(V; Y|US) - I(V; Z|US)\}.$$

Theorem 2 For any relay channel Γ,

$$\mathcal{R}^{(\mathrm{in})}(\Gamma) \subseteq \mathcal{R}_{\mathrm{rcc}}(\Gamma)$$

Another Pair of Inner and Outer Bounds of $\mathcal{R}_{\rm rcc}(\Gamma)$

$$\mathcal{Q}_1 := \{(U,V,X,S) : |\mathcal{U}| \le |\mathcal{X}||\mathcal{S}|+3, |\mathcal{V}| \le (|\mathcal{X}||\mathcal{S}|)^2 + 4|\mathcal{X}||\mathcal{S}|+3, \underline{U \leftrightarrow V \leftrightarrow XS \leftrightarrow YZ}, US \leftrightarrow V \leftrightarrow X\},$$

$$\mathcal{Q}_2 := \{(U,V,X,S) : |\mathcal{U}| \le |\mathcal{Z}||\mathcal{X}||\mathcal{S}|+3, |\mathcal{V}| \le (|\mathcal{Z}||\mathcal{X}||\mathcal{S}|)^2 + 4|\mathcal{Z}||\mathcal{X}||\mathcal{S}|+3, \underline{U \leftrightarrow V \leftrightarrow XSZ \leftrightarrow Y}, \underline{US \leftrightarrow VX \leftrightarrow Z}, US \leftrightarrow V \leftrightarrow X\}.$$

$\mathcal{R}^{(\rm out)}(\Gamma) := \{(R_0, R_1, R_{\rm s}) : \exists (U,V,X,S) \in \mathcal{Q}_2$ s.t.

$$R_0 \le \min\{I(Y;US), I(Z;U|S)\},$$
$$R_0 + R_1 + R_{\rm s} \le I(V;Y|US) + \min\{I(Y;US), I(Z;U|S)\},$$
$$R_{\rm s} \le I(V;Y|US) - I(V;Z|US)\}.$$

Theorem 2 For any relay channel Γ,

$$\mathcal{R}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm rcc}(\Gamma) \subseteq \mathcal{R}^{(\rm out)}(\Gamma).$$

Semi Deterministic Relay Channels

We say that Γ is semi deterministic if Z is a function of (X, S).

Corollary 3 If Γ is semi deterministic

$$\mathcal{R}^{(\mathrm{in})}(\Gamma) = \mathcal{R}_{\mathrm{rcc}}(\Gamma) = \mathcal{R}^{(\mathrm{out})}(\Gamma)\,.$$

Some Comments (1/2)

1. For derivations of the inner bounds we use the decode and forward scheme. Derivations of the ourter bounds are standard.
2. If Γ is semi deterministic, then

$$C_{\mathrm{rcc}}(\Gamma) := \sup R_{\mathrm{s}} : (0,0,R_{\mathrm{s}}) \in \mathcal{R}_{\mathrm{rcc}}(\Gamma)$$
$$= \max_{(U,V,X,S)\in\mathcal{Q}_1} \left[I(V;Y|US) - I(V;Z|US) \right].$$

   a) We can show that $C_{\mathrm{rcc}}(\Gamma)$ can be attained by $S = s^*$, where $s^* \in \mathcal{S}$ is the best input alphabet which maximizes the secrecy rate

$$\max_{(V,U,X,S=s^*)\in\mathcal{Q}_1} \{ I(V;Y|US=s^*) - I(V;Z|US=s^*) \}.$$

   b) This implies that the improvement of $C_{\mathrm{rcc}}(\Gamma)$ limited when Γ is semi deterministic.
   c) We have a similar result when Γ is reversely degraded.

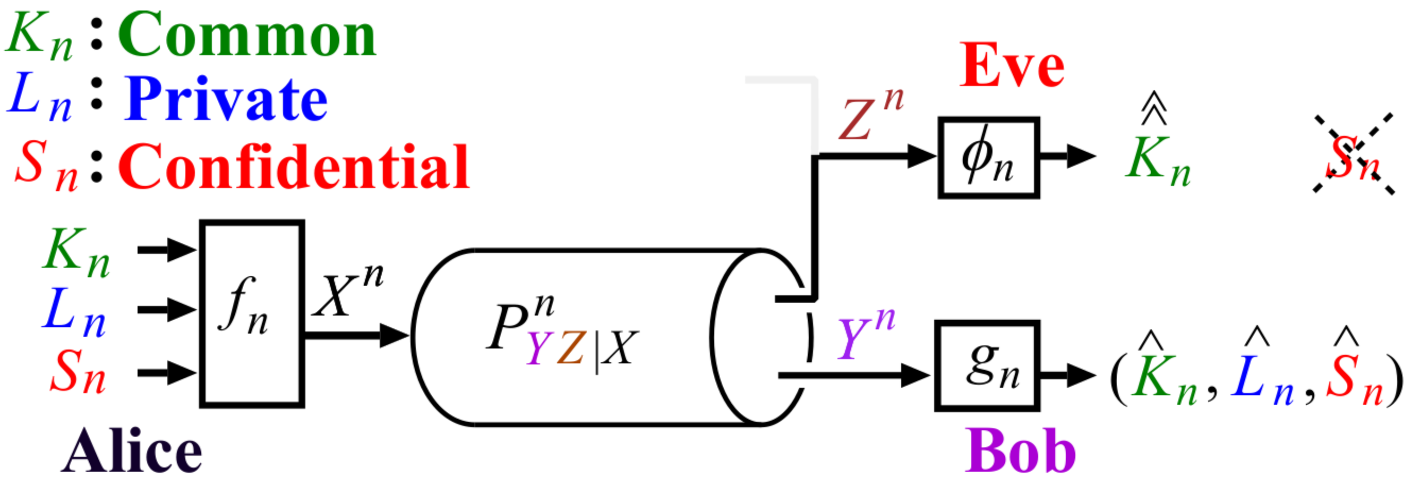
Some Comments (2/2)

3. Cover and El Gamal (IT 81) introduced the compress-and-forward scheme, where the relay transmits a quantized version of its received signal.
4. He and Yener (IT 10) derived lower bound of $C_{\mathrm{rcc}}(\Gamma)$ for general Γ in the case where the relay employs the compress-and-forward scheme to show that the relay may improve the secrecy capacity.

II. Broadcast Channel with Confidential Messages (BCC) with Randomness Constraints

Contents

Problem Setting of BCC



(Stochastic) Encoder $f_n : \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{S}_n \to \mathcal{X}^n$

Bob's Decoder $g_n : \mathcal{Y}^n \to \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{S}_n$

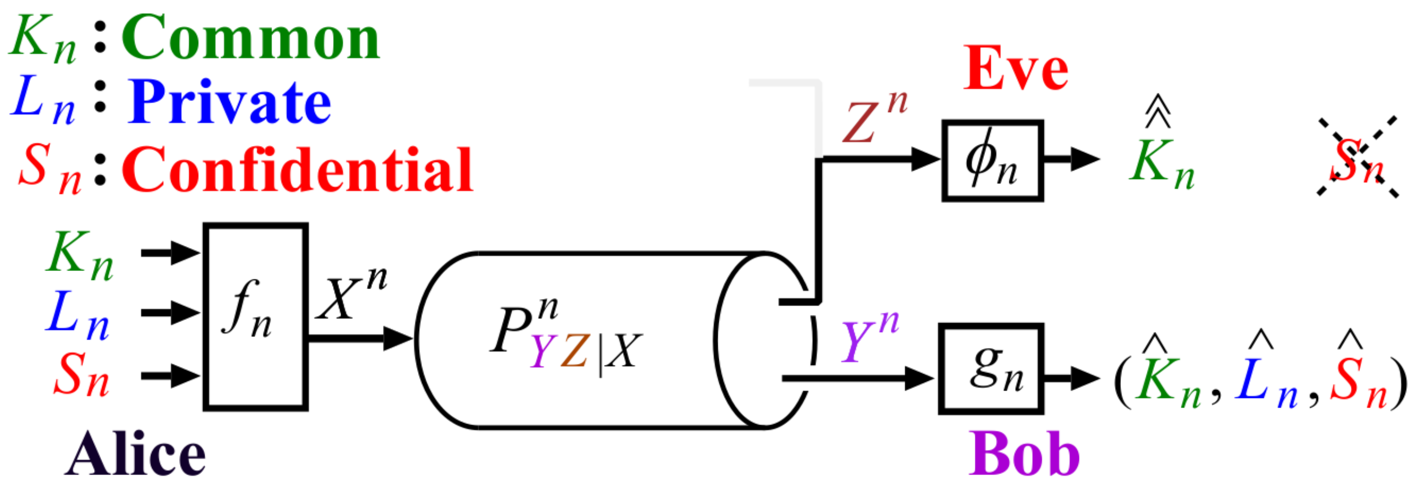
Eve's Decoder $\phi_n : \mathcal{Z}^n \to \mathcal{K}_n$

Bob's. Error Prob. $\lambda_1^{(n)} := \Pr\{(\hat{K}_n, \hat{L}_n, \hat{S}_n) \neq (K_n, L_n, S_n)\}$

Eve's Error Prob. $\lambda_2^{(n)} := \Pr\{\hat{\hat{K}}_n \neq K_n\}$

Security $D_n := D(P_{S_n Z^n} || P_{S_n} \times P_{Z^n}) = I(S_n; Z^n)$

Problem Setting of BCC



(R_0, R_1, R_s) is *achievable* $\overset{\text{def}}{\Leftrightarrow} \exists \{(f_n, g_n, \phi_n)\}_{n=1}^{\infty}$ s.t.

$$\lim_{n\to\infty} \lambda_i^{(n)} = 0, i = 1, 2, \ \limsup_{n\to\infty} D_n = 0 \text{ (strong secrecy criterion)}$$

$$\liminf_{n\to\infty} \frac{\log |\mathcal{K}_n|}{n} \geq R_0, \ \lim_{n\to\infty} \frac{\log |\mathcal{L}_n|}{n} = R_1, \ \liminf_{n\to\infty} \frac{\log |\mathcal{S}_n|}{n} \geq R_s.$$

Coding Theorem of BCC

Theorem [Csiszár and Körner (IT 78)] (R_0, R_1, R_s) is achievable iff. $\exists P_{UVX}$ s.t.

$$U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y, Z)$$

$$R_0 \leq \min\{I(Y;U), I(Z;U)\}$$

$$R_0 + R_1 + R_s \leq I(V;Y|U) + \min\{I(Y;U), I(Z;U)\}$$

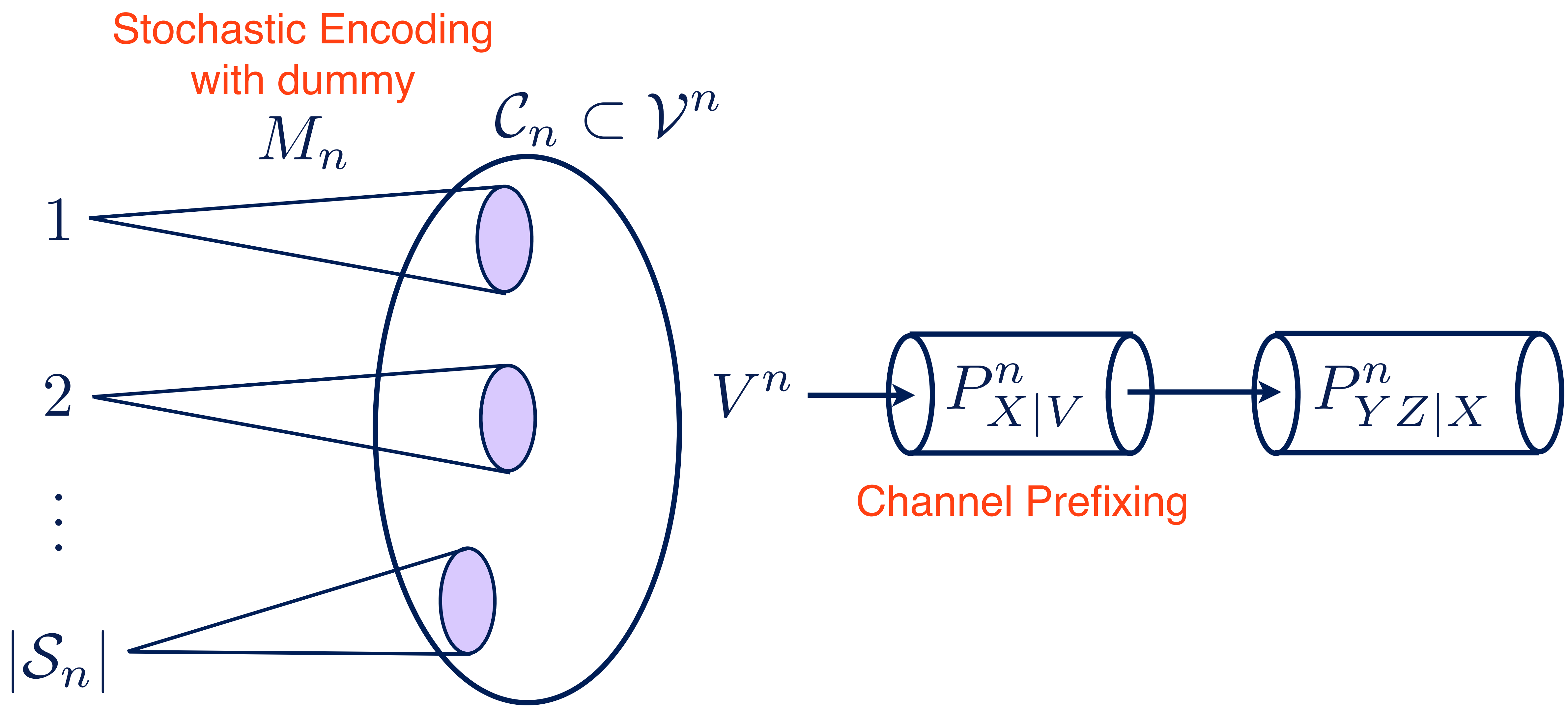
$$R_s \leq I(V;Y|U) - I(V;Z|U)$$

$R_0 = R_1 = 0$ Wiretap Channel

Corollary [Csiszár and Körner (IT 78), Wyner (IT 75)] R_s is achievable iff.

$$R_\mathrm{s} \leq C_\mathrm{s} = \max_{V \leftrightarrow X \leftrightarrow (Y, Z)} [I(V;Y) - I(V;Z)]$$

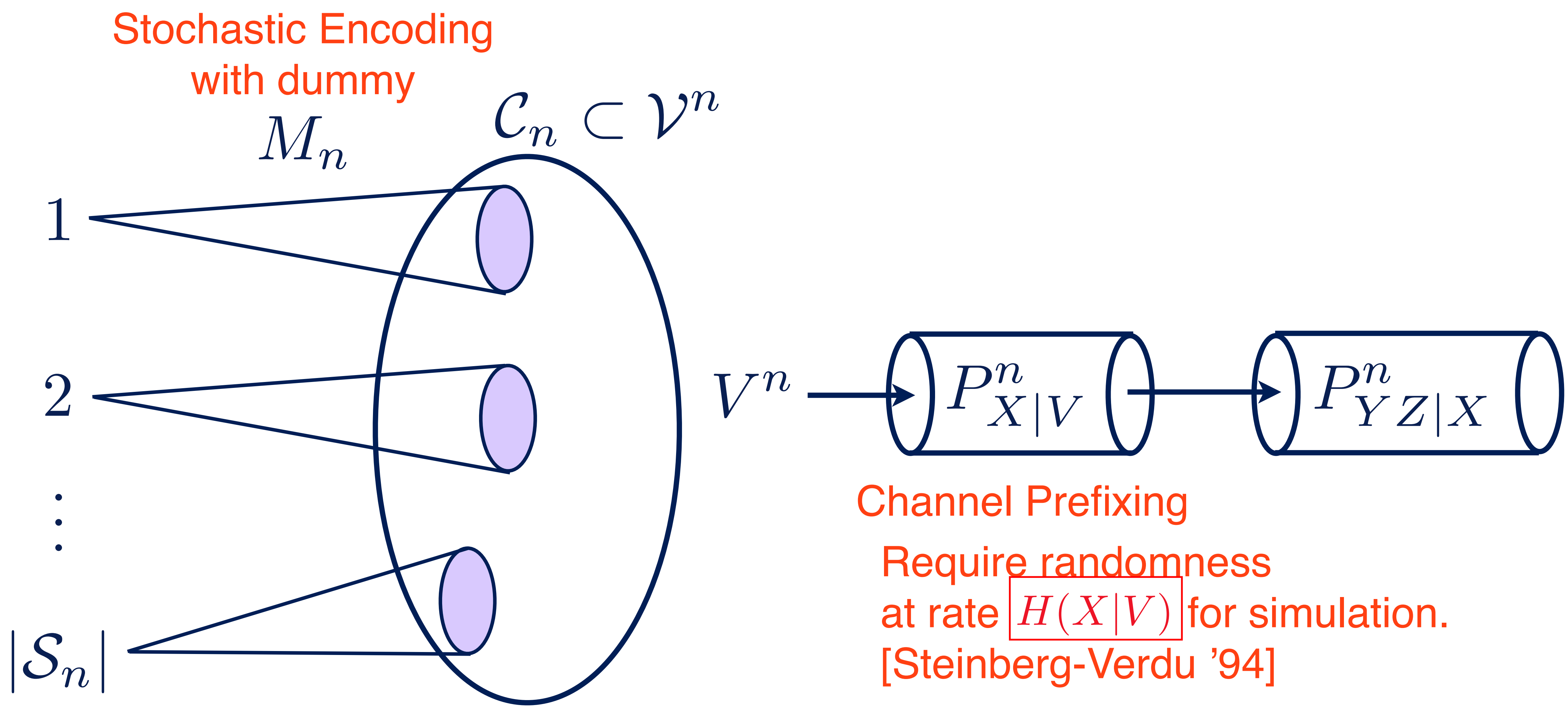
Achievability Scheme of C_s



Bob decodes S_n and M_n.

If $\frac{1}{n} \log |\mathcal{M}_n| > I(V;Z)$, then $D_n \to 0$.

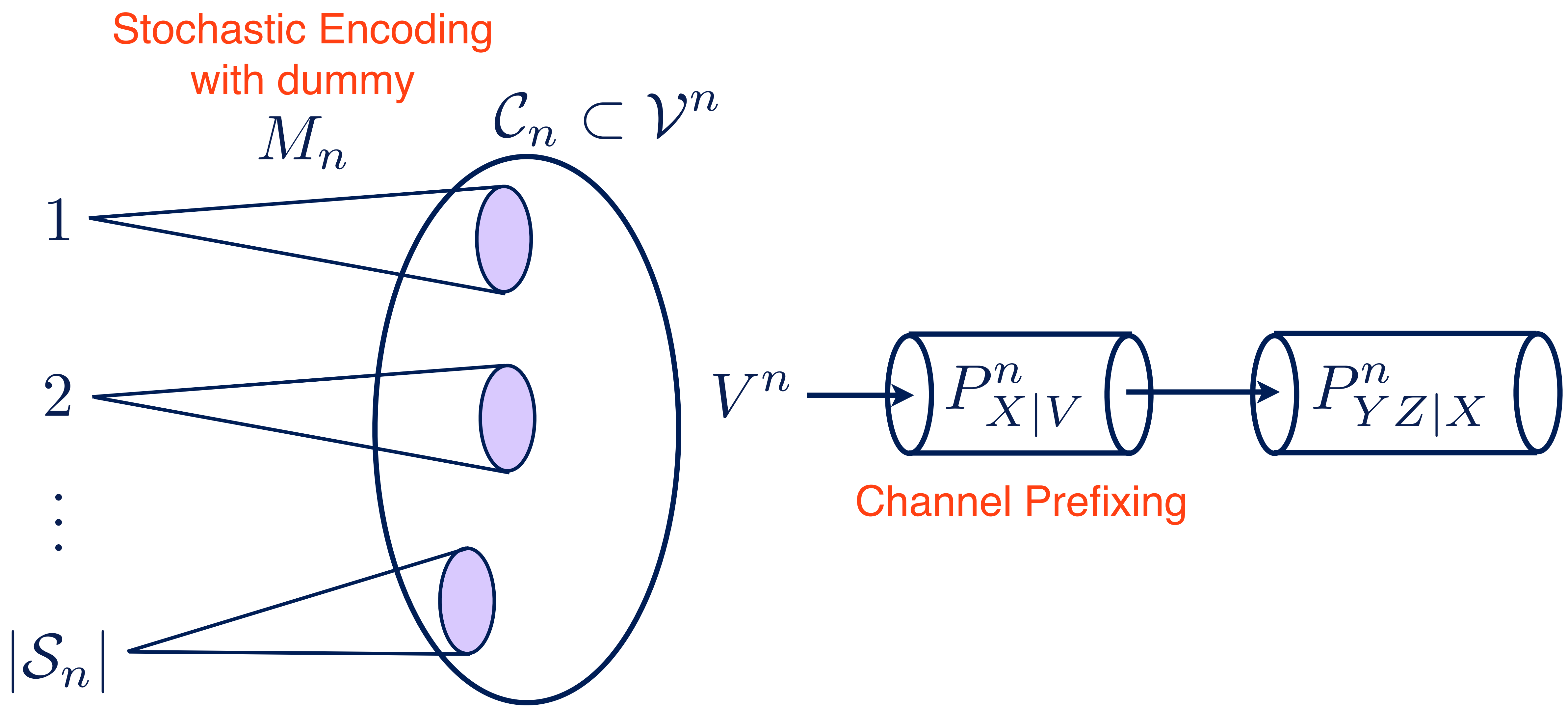
Achievability Scheme of C_s



Bob decodes S_n and M_n.

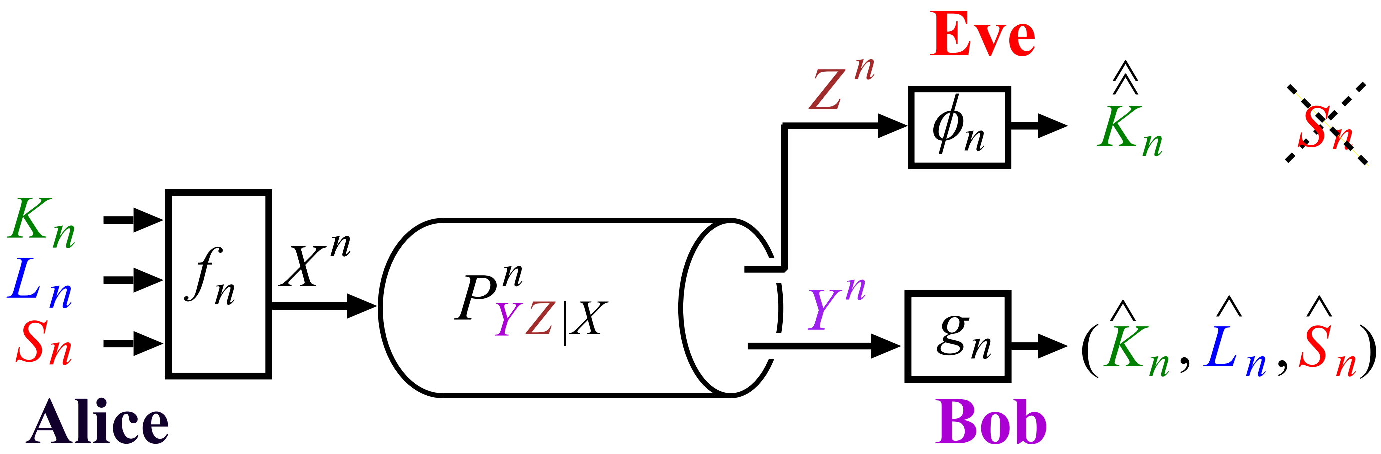
If $\frac{1}{n} \log |\mathcal{M}_n| > I(V;Z)$, then $D_n \to 0$.

Achievability Scheme of C_s



Huge amount of randomness is needed for the stochastic encoding and for simulating the channel prefixing.
What is the optimal scheme if we take in to account the amount of randomness.

Old Problem Setting



(Stochastic) Encoder $f_n : \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{S}_n \to \mathcal{X}^n$

Bob's Decoder $g_n : \mathcal{Y}^n \to \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{S}_n$

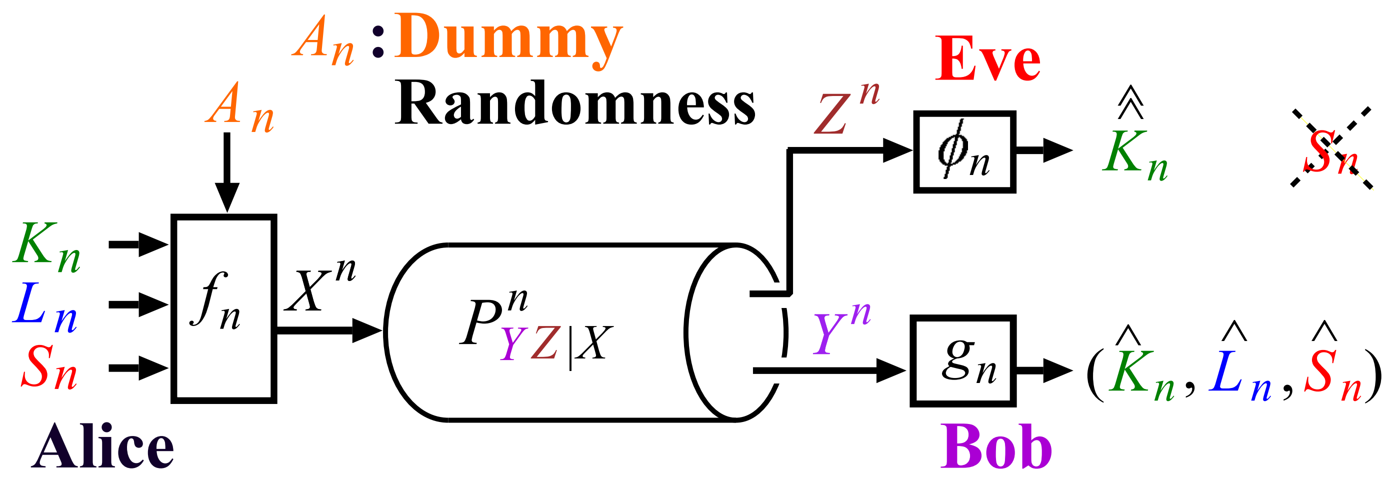
Eve's Decoder $\phi_n : \mathcal{Z}^n \to \mathcal{K}_n$

Bob's. Error Prob. $\lambda_1^{(n)} := \Pr\{(\hat{K}_n, \hat{L}_n, \hat{S}_n) \neq (K_n, L_n, S_n)\}$

Eve's Error Prob. $\lambda_2^{(n)} := \Pr\{\hat{\hat{K}}_n \neq K_n\}$

Security $D_n := D(P_{S_n Z^n} || P_{S_n} \times P_{Z^n}) = I(S_n; Z^n)$

New Problem Setting by W.O. (IT 15)



(Deterministic) Encoder $f_n : \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{S}_n \times \mathcal{A}_n \to \mathcal{X}^n$

Bob's Decoder $g_n : \mathcal{Y}^n \to \mathcal{K}_n \times \mathcal{L}_n \times \mathcal{S}_n$

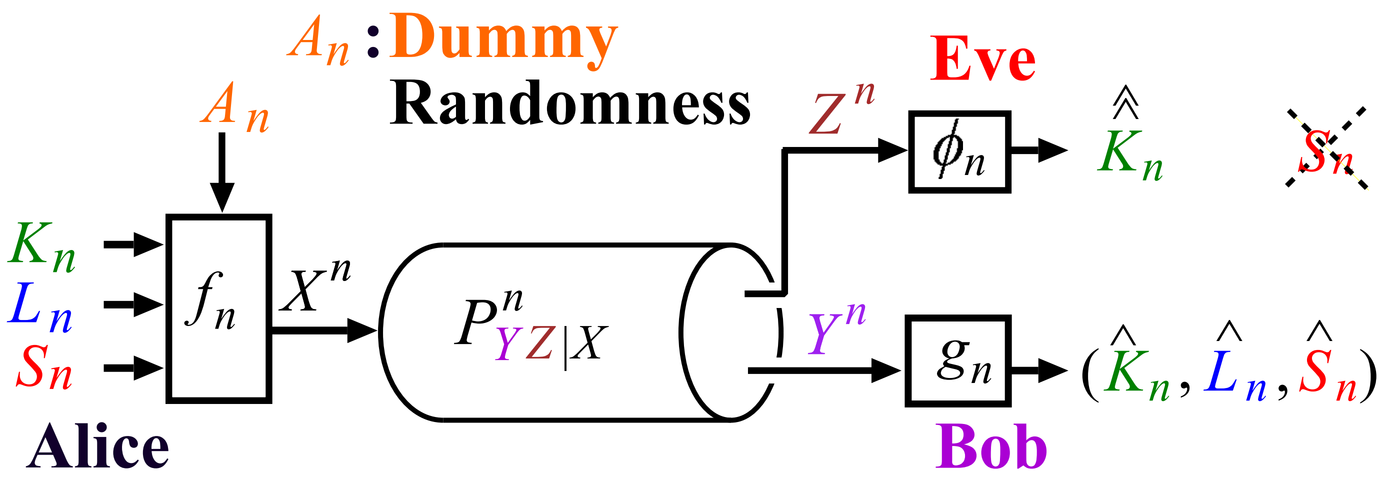
Eve's Decoder $\phi_n : \mathcal{Z}^n \to \mathcal{K}_n$

Bob's. Error Prob. $\lambda_1^{(n)} := \Pr\{(\hat{K}_n, \hat{L}_n, \hat{S}_n) \neq (K_n, L_n, S_n)\}$

Eve's Error Prob. $\lambda_2^{(n)} := \Pr\{\hat{\hat{K}}_n \neq K_n\}$

Security $D_n := D(P_{S_n Z^n} || P_{S_n} \times P_{Z^n}) = I(S_n; Z^n)$

New Problem Setting by W.O. (IT 15)



$(R_\mathrm{d}, R_0, R_1, R_\mathrm{s})$ is *achievable* $\overset{\text{def}}{\Leftrightarrow} \exists\{(f_n, g_n, \phi_n)\}_{n=1}^{\infty}$ s.t.

$$\lim_{n\to\infty} \lambda_i^{(n)} = 0, i = 1, 2, \ \limsup_{n\to\infty} D_n = 0 \text{ (strong secrecy criterion)}$$

$$\liminf_{n\to\infty} \frac{\log|\mathcal{K}_n|}{n} \geq R_0, \ \lim_{n\to\infty} \frac{\log|\mathcal{L}_n|}{n} = R_1, \ \liminf_{n\to\infty} \frac{\log|\mathcal{S}_n|}{n} \geq R_\mathrm{s}$$

$$\liminf_{n\to\infty} \frac{\log|\mathcal{A}_n|}{n} \leq R_\mathrm{d}$$

Main Theorem

Theorem [Watanabe and Oohama (IT 15)] $(R_{\mathrm{d}}, R_0, R_1, R_{\mathrm{s}})$ is achievable iff. $\exists P_{UVX}$ s.t.

$$U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y, Z)$$

$$R_0 \leq \min\{I(Y;U), I(Z;U)\}$$

$$R_0 + R_1 + R_{\mathrm{s}} \leq I(V;Y|U) + \min\{I(Y;U), I(Z;U)\}$$

$$R_{\mathrm{s}} \leq I(V;Y|U) - I(V;Z|U)$$

$$R_1 + R_{\mathrm{d}} \geq I(X;Z|U)$$

$$R_{\mathrm{d}} \geq I(X;Z|V)$$

Main Theorem

Theorem [Watanabe and Oohama (IT 15)] $(R_{\mathrm{d}}, R_0, R_1, R_{\mathrm{s}})$ is achievable iff. $\exists P_{UVX}$ s.t.

$$U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y, Z)$$

$$R_0 \le \min\{I(Y;U), I(Z;U)\}$$

$$R_0 + R_1 + R_{\mathrm{s}} \le I(V;Y|U) + \min\{I(Y;U), I(Z;U)\}$$

$$R_{\mathrm{s}} \le I(V;Y|U) - I(V;Z|U)$$

$$R_1 + R_{\mathrm{d}} \ge I(X;Z|U)$$

$$R_{\mathrm{d}} \ge I(X;Z|V)$$

(New Inequalities)

Ideas of Coding Scheme

Superposition coding scheme proposed by Chia and El Gamal is employed instead of the channel simulation.

1. For common message k_n , randomly generate code word $u^n_{k_n}$ according to P^n_U .
2. For each k_n and for private and confidential messages (ℓ_n, s_n), randomly generate $v^n_{k_n \ell_n s_n}$ according to $P^n_{V|U}(\cdot|u^n_{k_n})$.
3. For each (k_n, ℓ_n, s_n) and for dummy randomness a_n , randomly generate $x^n_{k_n \ell_n s_n a_n}$ according to $P^n_{X|V}(\cdot|v^n_{k_n \ell_n s_n})$.

Error Analysis

1. Bob decodes (k_n, ℓ_n, s_n) by looking for unique

$$(v^n_{k_n \ell_n s_n}, y^n) \in \mathcal{T}^n_1$$

2. Eve decodes k_n by looking for unique

$$(u^n_{k_n}, z^n) \in \mathcal{T}^n_2$$

Analysis of error probability is almost same as that of the BC with degraded message set.

Security Analysis

The channel resolvability with the superposition coding is used to analyze the security.

Lemma (Superposition Resolvability)

If $R_1 > I(V;Z)$ and $R_d > I(X;Z|V)$,

$$\lim_{n\to\infty} D(P_{Z^n|S_n}(\cdot|s_n)\|P_Z^n) = 0$$

Note that $I(V;Z) + I(X;Z|V) = I(X;Z)$, which is the randomness needed to simulate P_Z^n via $P_{Z|X}^n$.

The lemma shows the strong security of Chia and El Gamal's superposition scheme.

The lemma is proved by extending a result in [Hayashi '11].

When $R_\mathrm{d} = \infty$

Main Theorem implies ...

Corollary [Csiszár and Körner (IT 78)] $(\infty, R_0, R_1, R_\mathrm{s})$ is achievable iff. $\exists P_{UVX}$ s.t.

$$U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y, Z)$$

$$R_0 \leq \min\{I(Y;U), I(Z;U)\}$$

$$R_0 + R_1 + R_\mathrm{s} \leq I(V;Y|U) + \min\{I(Y;U), I(Z;U)\}$$

$$R_\mathrm{s} \leq I(V;Y|U) - I(V;Z|U)$$

When $R_{\mathrm{d}} = 0$

Corollary [Oohama and Watanabe (SITA 10)] $(0, R_0, R_1, R_{\mathrm{s}})$ is achievable iff. $\exists P_{UVX}$ s.t.

$$U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y, Z)$$

$$R_0 \leq \min\{I(Y;U), I(Z;U)\}$$

$$R_0 + R_1 + R_{\mathrm{s}} \leq I(V;Y|U) + \min\{I(Y;U), I(Z;U)\}$$

$$R_{\mathrm{s}} \leq I(V;Y|U) - I(V;Z|U)$$

$$R_1 \geq I(X;Z|U)$$

When $R_0 = R_1 = 0$

Main Theorem implies ...

Corollary [Watanabe and Oohama (IT 15)] $(R_\mathrm{d}, R_\mathrm{s})$ is achievable iff. $\exists P_{UVX}$ s.t.

$$U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y, Z)$$

$$R_\mathrm{s} \le I(V;Y|U) - I(V;Z|U)$$

$$R_\mathrm{d} \ge \underline{I(X;Z|U)}$$

U is just a time-sharing R.V..

When $R_0 = R_1 = 0$

Region achieved by channel simulation is...

Proposition $(R_{\mathrm{d}}, R_{\mathrm{s}})$ is achievable iff. $\exists P_{UVX}$ s.t.

$$U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y, Z)$$

$$R_{\mathrm{s}} \leq I(V;Y|U) - I(V;Z|U)$$

$$R_{\mathrm{d}} \geq \underline{I(V;Z|U)} + \boxed{H(X|V)}$$

Note that

$$\underline{I(X;Z|U)} = \underline{I(V;Z|U)} + \underline{I(X;Z|V)} < \underline{I(V;Z|U)} + \boxed{H(X|V)}$$

in general.

When $R_0 = R_1 = 0$

When $P_{Y|X}$ is more capable than $P_{Z|X}$...

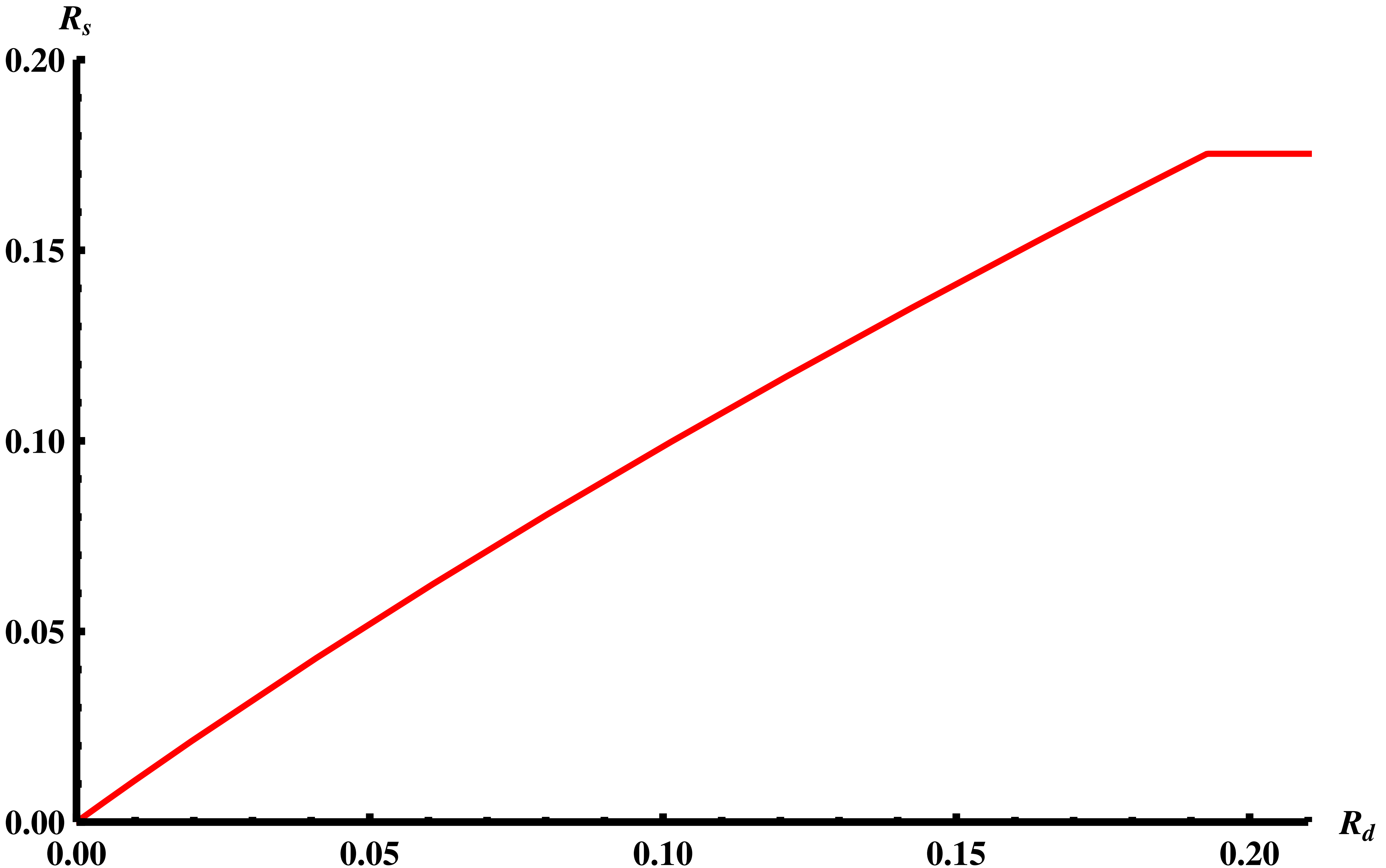
Corollary $(R_\mathrm{d}, R_\mathrm{s})$ is achievable iff. $\exists P_{UX}$ s.t.

$$
\begin{aligned}
U \leftrightarrow X \leftrightarrow (Y, Z) \\
R_\mathrm{s} \le I(X;Y|U) - I(X;Z|U) \\
R_\mathrm{d} \ge I(X;Z|U)
\end{aligned}
$$

- Independently solved by Bloch and Kliewer (Arxiv 12).
- Channel prefixing is not needed.

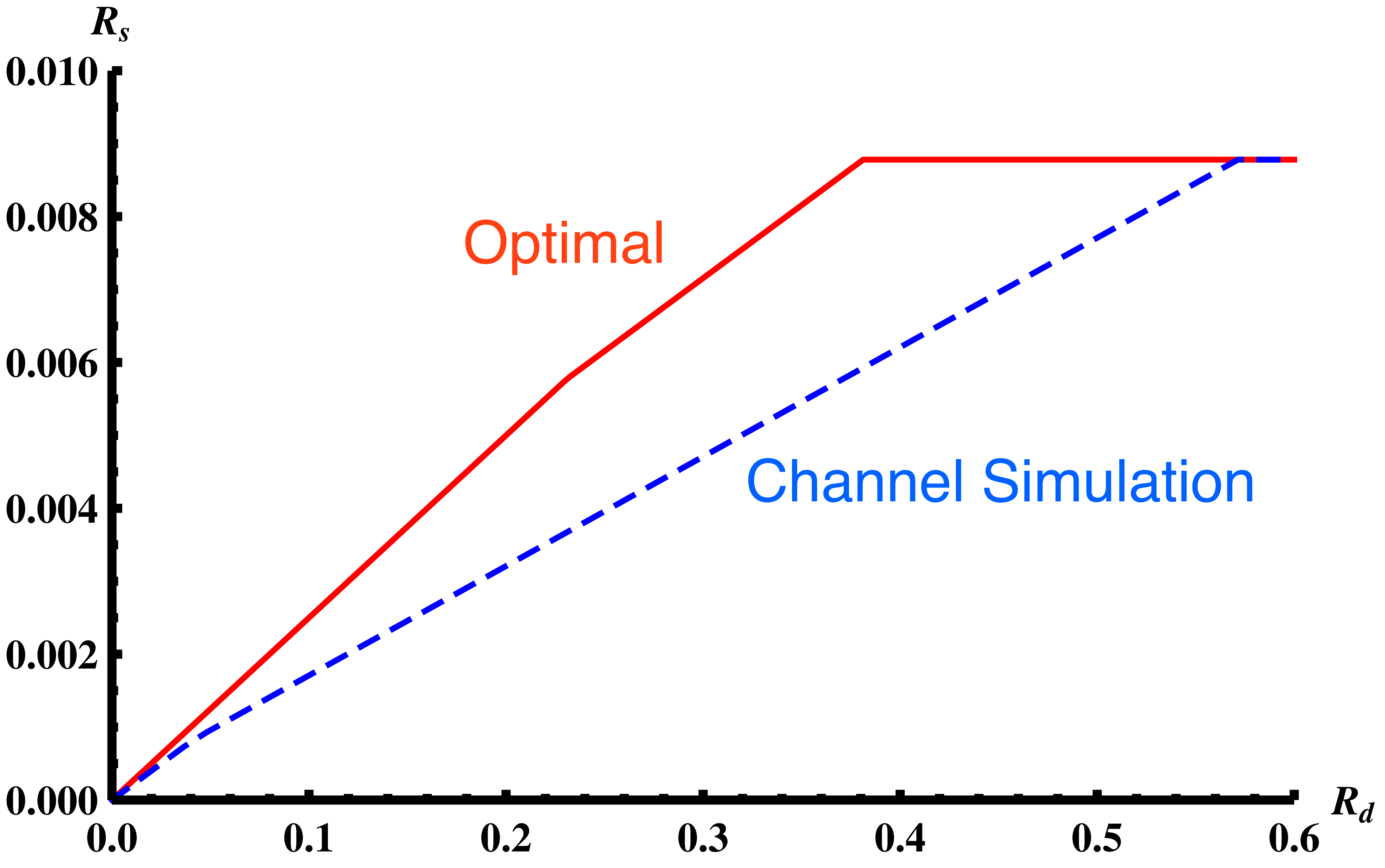
Numerical Example 1

When $P_{Y|X} = \mathrm{BSC}(0.1)$ and $P_{Z|X} = \mathrm{BSC}(0.2)$ ...



Numerical Example 2

When $P_{Y|X} = \mathrm{BSC}(0.11)$ and $P_{Z|X} = \mathrm{BEC}(0.45)$...



Conclusions

- New setting of BCC was proposed.
- Optimal region was clarified.
- The channel simulation scheme turned out to be suboptimal

III. Information Theoretic Analysis of Shannon Cipher System under Side-channel Attacks

Basic Definitions and Notations (Part 1/2)

Random Source of Information and Key:

$\mathcal{X}$: Finite set, $X \in \mathcal{X}$, $X \sim p_X = \{p_X(x)\}_{x\in\mathcal{X}}$

$\{X_t\}_{t=1}^{\infty}$: Stationary Discrete Memoryless Source(SDMS), $X_t \sim p_X$, $t = 1, 2, \ldots$ The SDMS $\{X_t\}_{t=1}^{\infty}$ is specified with p_X.

$K \in \mathcal{X}$, $K \sim p_K = \{p_K(k)\}_{k\in\mathcal{X}}$

$\{K_t\}_{t=1}^{\infty}$: SDMS, $K_t \sim p_K$. We assume that p_K is the uniform distribution over $\mathcal{X}$.

Random Variables and Sequences:

We write $X^n := X_1 X_2 \cdots X_n \in \mathcal{X}^n$. Similarly, we write $x^n := x_1 x_2 \cdots x_n \in \mathcal{X}^n$. For $x^n \in \mathcal{X}^n$, $p_{X^n}(x^n)$ stands for the probability of the occurrence of x^n. Since $\{X_t\}_{t=1}^{\infty}$ is SDMS specified with p_X, we have

$$p_{X^n}(x^n) = \prod_{t=1}^{n} p_X(x_t).$$

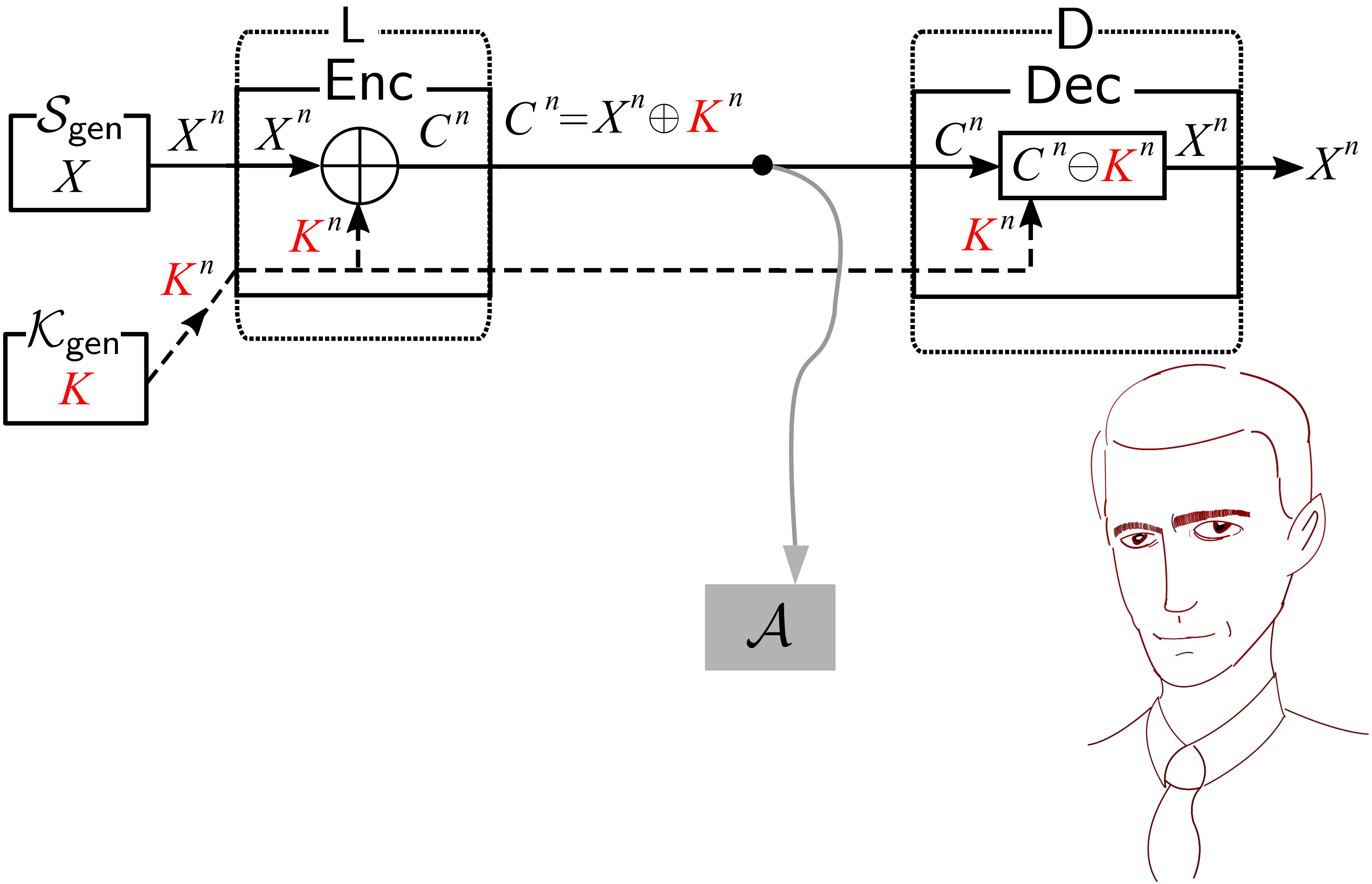
In this case we write $p_{X^n}(x^n)$ as $p_X^n(x^n)$. Similar notations are used for other random variables and sequences.

Basic Definitions and Notations (Part 2/2)

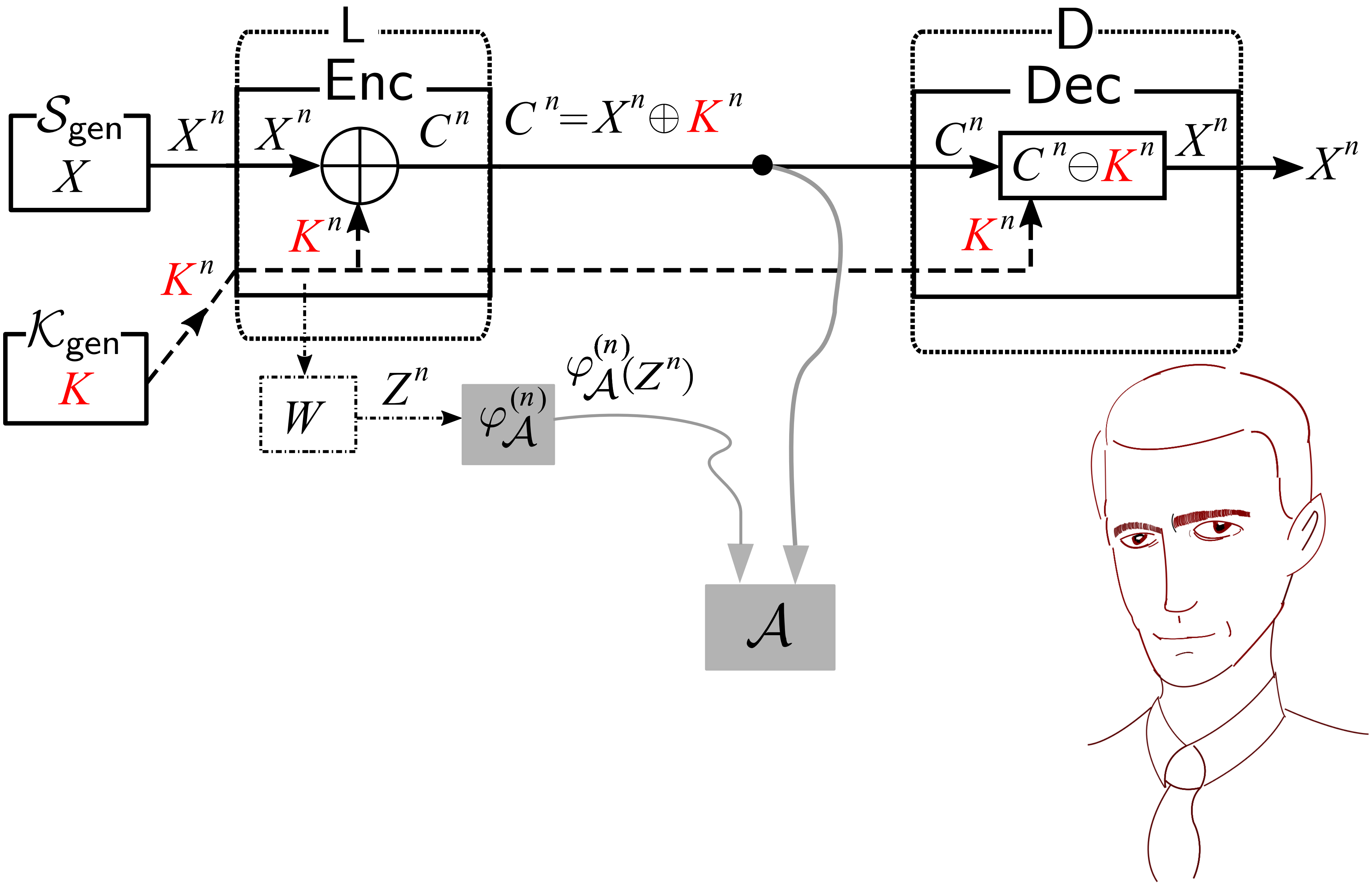
Finite Field and the Addition Operation:

- We assume that $\mathcal{X}$ is a finite field.
- The notation $\oplus$ is used to denote the field addition operation, while the notation $\ominus$ is used to denote the field subtraction operation, i.e., $a \ominus b = a \oplus (-b)$ for any elements $a, b \in \mathcal{X}$.

Shannon Cipher System



Side-Channel Attacks to Shannon Cipher System



Leakage of Key Data by Side-Channel Attacks

- Let $W : \mathcal{K} \to \mathcal{Z}$ be noisy channel.
- Let Z be a channel output r.v. from W for the input r.v. K.
- We consider the discrete memoryless channel(DMC) specified with W. Let $Z^n \in \mathcal{Z}^n$ be a random variable from W the channel output by connecting $K^n \in \mathcal{X}^n$ to the input of channel. We write a conditional distribution on Z^n given K^n as

$$W^n = \{W^n(z^n|k^n)\}_{(k^n,z^n)\in\mathcal{K}^n\times\mathcal{Z}^n} \cdot$$

Since the channel is memoryless, we have

$$W^n(z^n|k^n) = \prod_{t=1}^{n} W(z_t|k_t). \qquad (1)$$

Assumption on the Adversary $\mathcal{A}$

Let

$$\varphi_{\mathcal{A}}^{(n)} : \mathcal{Z}^n \to \mathcal{M}_{\mathcal{A}}^{(n)}, \quad R_{\mathcal{A}}^{(n)} := \frac{1}{n} \log |\mathcal{M}_{\mathcal{A}}^{(n)}|.$$

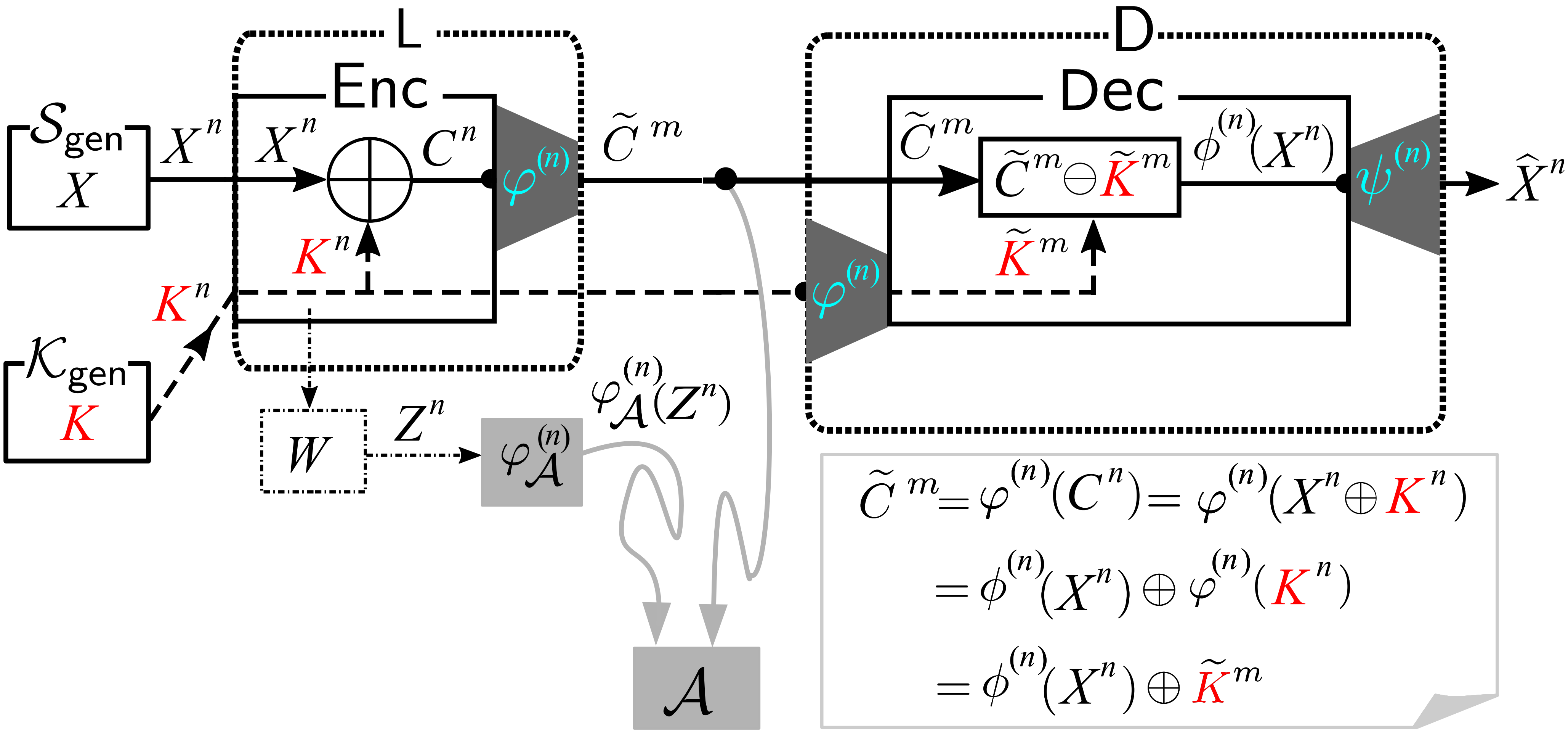
For $R_{\mathcal{A}} > 0$, we set $\mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}}) := \{\varphi_{\mathcal{A}}^{(n)} : R_{\mathcal{A}}^{(n)} \leq R_{\mathcal{A}}\}$.

- The adversary $\mathcal{A}$, having accessed Z^n, obtains $\varphi_{\mathcal{A}}^{(n)}(Z^n)$. For each $n = 1, 2, \cdots$, the adversary $\mathcal{A}$ can design $\varphi_{\mathcal{A}}^{(n)}$.
- The adversary $\mathcal{A}$ must use $\varphi_{\mathcal{A}}^{(n)}$ such that for some $R_{\mathcal{A}}$ and for any sufficiently large n, $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$.

Validity of Our Theoretical Model:

- As a real situation of side channel attacks we have often the case where the noisy version Z^n of K^n can be regarded as *almost an analog random signal*.
- In this case, $|\mathcal{Z}|$ is sufficiently large. The adversary $\mathcal{A}$ can not obtain Z^n in a lossless form.

Affine Encoder as Privacy Amplifier



$$
\begin{aligned}
\widetilde{C}^m &= \varphi^{(n)}(C^n) = \varphi^{(n)}(X^n \oplus K^n) \\
&= \phi^{(n)}(X^n) \oplus \varphi^{(n)}(K^n) \\
&= \phi^{(n)}(X^n) \oplus \widetilde{K}^m
\end{aligned}
$$

Affine Encoder as Privacy Amplifier

For each $n = 1, 2, \cdots$, let $\phi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$ be a linear mapping. Define the mapping $\varphi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$ by

$$\varphi^{(n)}(k^n) := \phi^{(n)}(k^n) \oplus b^m = \underline{k^n A \oplus b^m}, \text{ for } k^n \in \mathcal{X}^n. \tag{2}$$

where A is a matrix with n rows and m columns. Entries of A are from $\mathcal{X}$. We fix $b^m \in \mathcal{X}^m$. By the definition (2) of $\varphi^{(n)}$, those satisfy the following affine structure:

$$\begin{aligned} \varphi^{(n)}(x^n \oplus k^n) &= (x^n \oplus k^n)A \oplus b^m = x^n A \oplus (k^n A \oplus b^m) \\ &= \underline{\boxed{\phi^{(n)}(x^n)} \oplus \varphi^{(n)}(k^n)}, \text{ for } x^n, k^n \in \mathcal{X}^n. \end{aligned} \tag{3}$$

Let $\psi^{(n)}$ be the corresponding decoder for $\phi^{(n)}$ such that $\psi^{(n)} : \mathcal{X}^m \to \mathcal{X}^n$.

Affine Encoder as Privacy Amplifier

Description of Proposed Procedure:

1. *Encoding of Ciphertext:* First, we use $\varphi^{(n)}$ to encode the ciphertext $C^n = X^n \oplus K^n$ Let $\widetilde{C}^m = \varphi^{(n)}(C^n)$. Then, instead of sending C^n, we send $\tilde{C}^m$ to the public communication channel. By the affine structure (3) of encoder we have that

$$\begin{aligned} \widetilde{C}^m &= \varphi^{(n)}(X^n \oplus K^n) \\ &= \phi^{(n)}(X^n) \oplus \varphi^{(n)}(K^n) = \widetilde{X}^m \oplus \widetilde{K}^m, \end{aligned} \tag{4}$$

where we set

$$\widetilde{X}^m := \phi^{(n)}(X^n), \widetilde{K}^m := \varphi^{(n)}(K^n).$$

Affine Encoder as Privacy Amplifier

2. *Decoding at Sink Node* D*:* First, using the linear encoder $\varphi^{(n)}$, D encodes the key K^n received through private channel into $\widetilde{K}^m$ =($\varphi^{(n)}(K^n)$. Receiving $\widetilde{C}^m$ from public communication channel, D computes $\widetilde{X}^m$ in the following way. From (4), we have that the decoder D can obtain $\widetilde{X}^m = \phi^{(n)}(X^n)$ by subtracting $\widetilde{K}^m = \varphi^{(n)}(K^n)$ from $\widetilde{C}^m$. Finally, D outputs $\widehat{X}^n$ by applying the decoder $\psi^{(n)}$ to $\widetilde{X}^m$ as follows:

$$\widehat{X}^n = \psi^{(n)}(\widetilde{X}^m) = \psi^{(n)}(\phi^{(n)}(X^n)). \tag{5}$$

Error Probability and Information Leakage

When $\varphi^{(n)}$ is an affine map, we have the following result.

On Reliability:

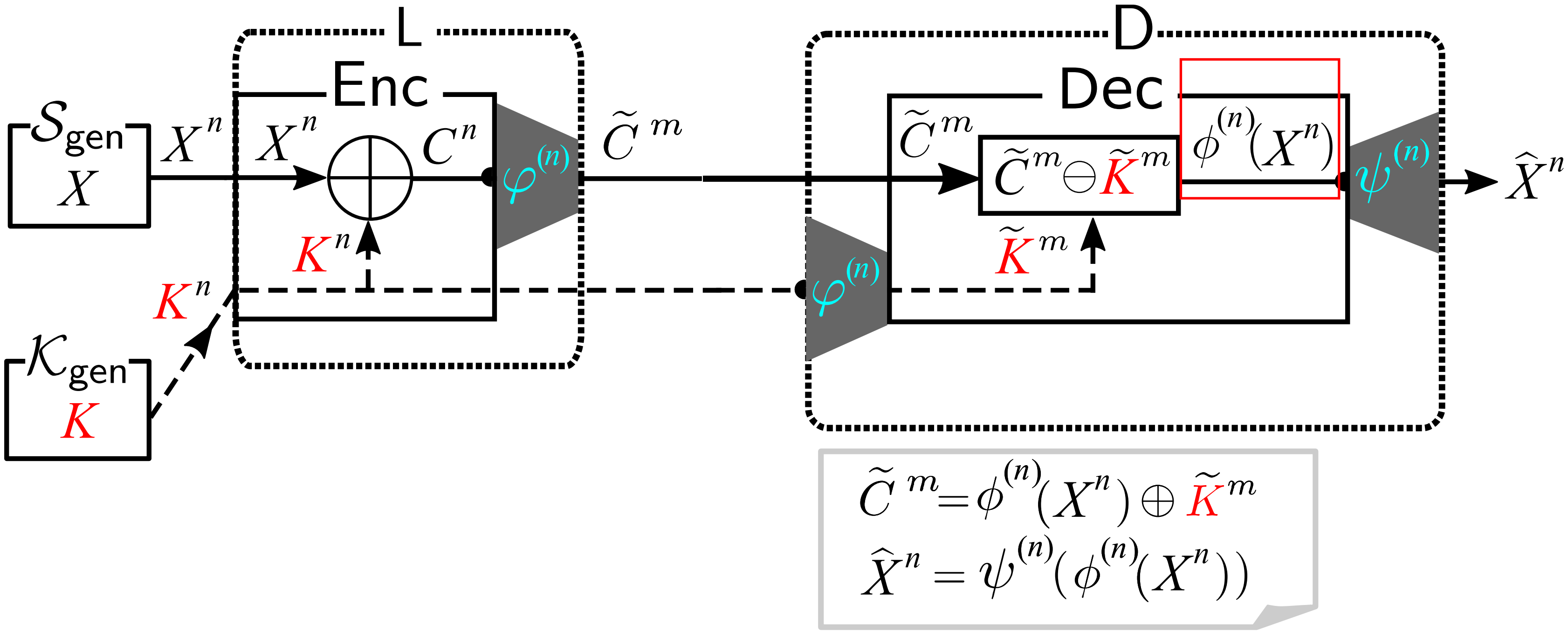
$$p_{\mathrm{e}} := \Pr[\widehat{X}^n \neq X^n] = \Pr[\psi^{(n)}(\phi^{(n)}(X^n)) \neq X^n]. \tag{6}$$

On Security:

$$\begin{aligned}\Delta^{(n)} :=& I(X^n; \widetilde{C}^m, \varphi_{\mathcal{A}}^{(n)}(Z^n)) \\ =& I(X^n; \varphi^{(n)}(X^n \oplus K^n), \varphi_{\mathcal{A}}^{(n)}(Z^n)) \leq D(p_{\tilde{K}^m | M_{\mathcal{A}}^{(n)}} || p_{V^m} | p_{M_{\mathcal{A}}^{(n)}}),\end{aligned}$$

where $M_{\mathcal{A}}^{(n)} := \varphi_{\mathcal{A}}^{(n)}(Z^n)$ and p_{V^m} is the uniform distribution on $\mathcal{X}^m$.

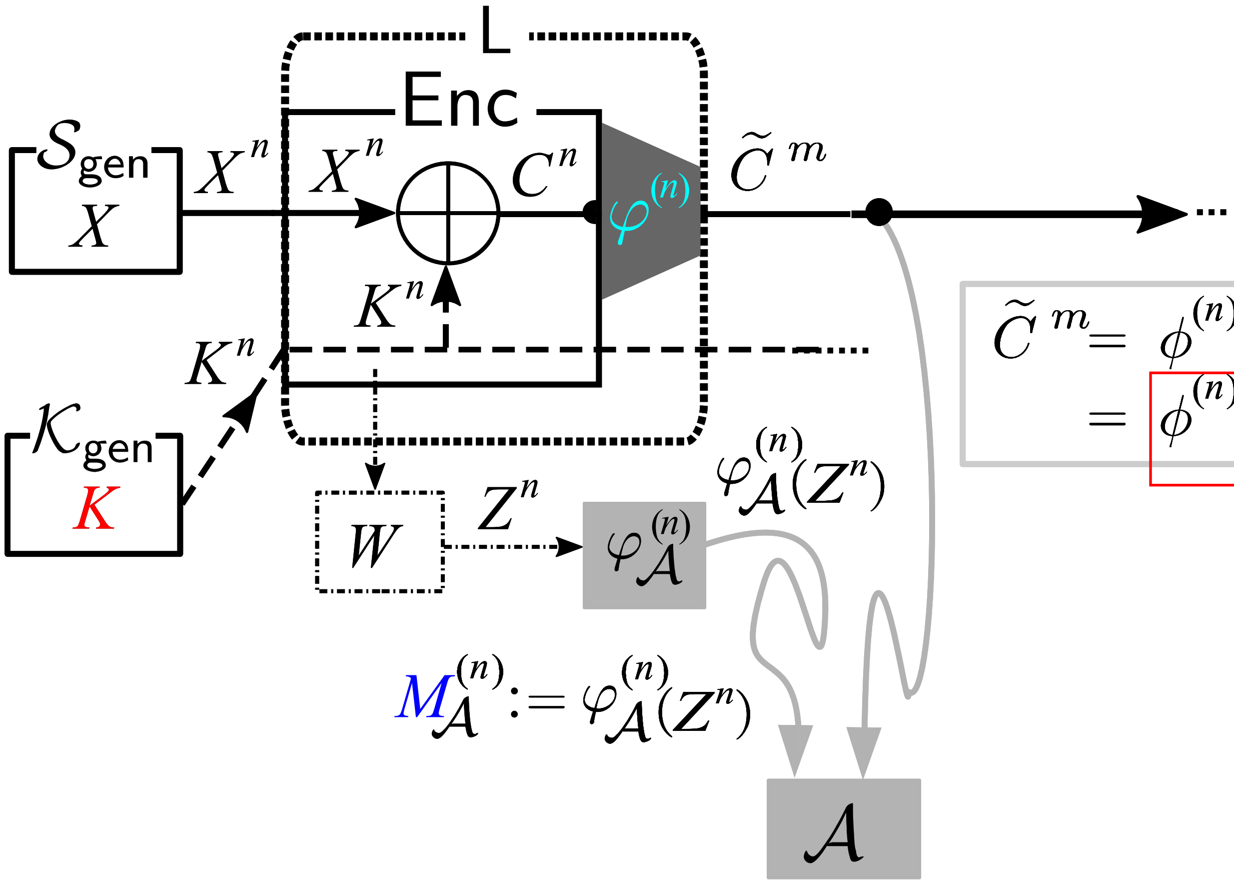
Analysis of $p_{\mathrm{e}} = \Pr[\widehat{X}^n \neq X^n]$



When $\varphi^{(n)}$ is an affine map, we have the following result.

$$p_{\mathrm{e}} = \Pr[\widehat{X}^n \neq X^n] = \Pr[\psi^{(n)}(\phi^{(n)}(X^n)) \neq X^n]. \tag{7}$$

Analysis of $\Delta_n = I(X^n; \widetilde{C}^m, \varphi_{\mathcal{A}}^{(n)}(Z^n))$



$$\widetilde{C}^m = \phi^{(n)}(X^n) \oplus \varphi^{(n)}(K^n) = \phi^{(n)}(X^n) \oplus \widetilde{K}^m$$

$$\Delta^{(n)} = I(X^n; \phi^{(n)}(X^n) \oplus \tilde{K}^m, M_{\mathcal{A}}^{(n)}) = I(X^n; \phi^{(n)}(X^n) \oplus \tilde{K}^m | M_{\mathcal{A}}^{(n)})$$

$$= H(\phi^{(n)}(X^n) \oplus \tilde{K}^m | M_{\mathcal{A}}^{(n)}) - H(\tilde{K}^m | M_{\mathcal{A}}^{(n)})$$

$$\leq m \log |\mathcal{X}| - H(\tilde{K}^m | M_{\mathcal{A}}^{(n)}) = D(p_{\tilde{K}^m | M_{\mathcal{A}}^{(n)}} || p_{V^m} | p_{M_{\mathcal{A}}^{(n)}}).$$

Definition for Upper Bound of Error Prob.

Let $\overline{X}$ be an arbitrary random variable over $\mathcal{X}$ and has a probability distribution $p_{\overline{X}}$. Let $\mathcal{P}(\mathcal{X})$ denote the set of all probability distributions on $\mathcal{X}$. For $R \geq 0$ and $p_X \in \mathcal{P}(\mathcal{X})$, we define the following function:

$$E(R|p_X) := \min_{p_{\overline{X}} \in \mathcal{P}(\mathcal{X})} \{[R - H(\overline{X})]^+ + D(p_{\overline{X}}||p_X)\}.$$

By definition we have

$$R > H(X) \Longleftrightarrow E(R|p_X) > 0.$$

Definition for Upper Bound of Security

$$\Xi(R, R_{\mathcal{A}}) := \inf_{\eta > 0} \left[\max_{\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(R_{\mathcal{A}})} p_{M_{\mathcal{A}}^{(n)} Z^n K^n} \left\{ R \geq \frac{1}{n} \log \frac{1}{p_{K^n | M_{\mathcal{A}}^{(n)}}(K^n | M_{\mathcal{A}}^{(n)})} - \eta \right\} + \mathrm{e}^{-n\eta} \right]. \quad (8)$$

Key Proposition

Proposition 1 For any $R_{\mathcal{A}}, R > 0$, and any (p_K, W), there exists a sequence of mappings $\{(\varphi^{(n)}, \psi^{(n)})\}_{n=1}^{\infty}$ such that for any $p_X \in \mathcal{P}(\mathcal{X})$,

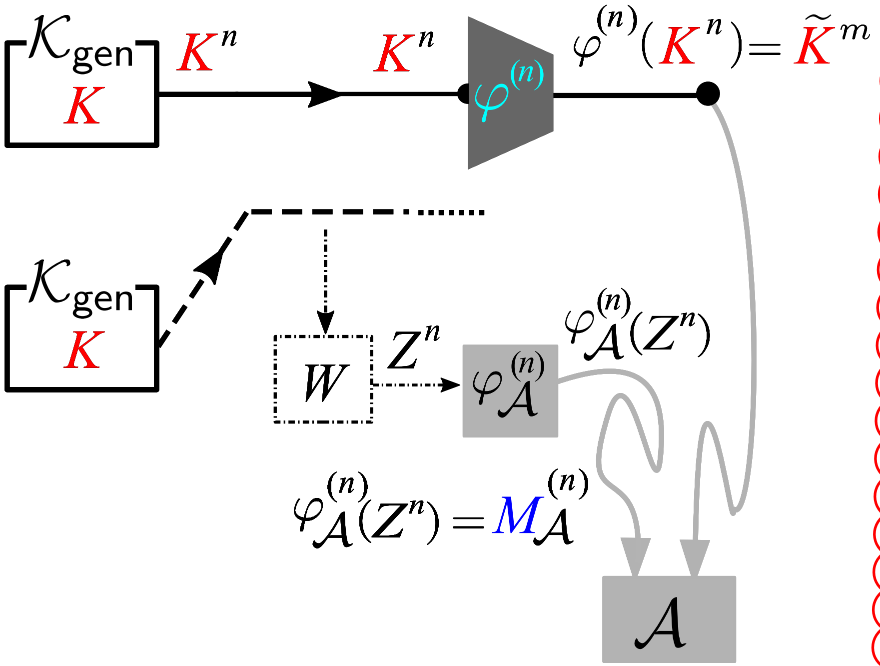
$$\frac{1}{n}\log|\mathcal{X}^m| = \frac{m}{n}\log|\mathcal{X}| \in \left[R - \frac{1}{n}, R\right],$$

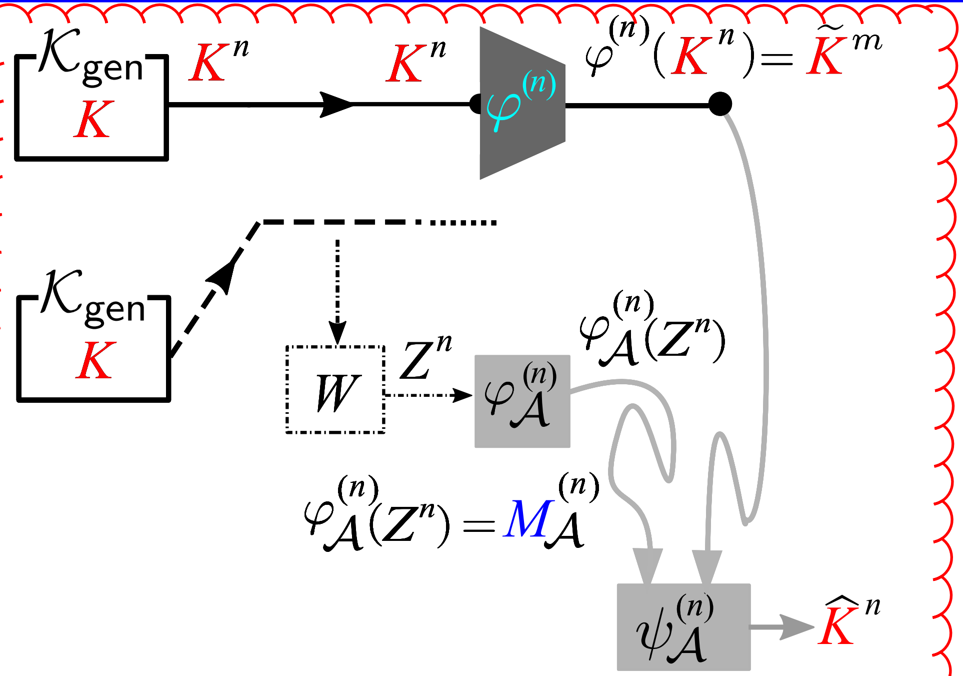
$$p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n) \leq \mathrm{e}(n+1)^{2|\mathcal{X}|}\{(n+1)^{|\mathcal{X}|}+1\} \times \mathrm{e}^{-n[E(R|p_X)]} \tag{9}$$

and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$,

$$\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n) \leq D(p_{\tilde{K}^m|M_{\mathcal{A}}^{(n)}}||p_{V^m}|p_{M_{\mathcal{A}}^{(n)}}) \leq \{(n+1)^{|\mathcal{X}|}+1\}(nR)\Xi(R, R_{\mathcal{A}}). \tag{10}$$

$\Xi(R, R_{\mathcal{A}})$ and One Helper Source Coding Problem





There exists $\{(\varphi^{(n)}, \psi^{(n)})\}_{n\geq 1}$ with $(n/m)\log|\mathcal{X}| \leq R$ such that for any $\{(\varphi_{\mathcal{A}}^{(n)}, \psi_{\mathcal{A}}^{(n)})\}_{n\geq 1}$ with $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(R_{\mathcal{A}})$,

$$\Delta^{(n)} \leq D(p_{\tilde{K}^m|M_{\mathcal{A}}^{(n)}} || p_{V^m} | p_{M_{\mathcal{A}}^{(n)}}) \leq (nR)\Xi(R, R_{\mathcal{A}}), \tag{11}$$

$$\Pr\{K^n = \psi_{\mathcal{A}}^{(n)}(\tilde{K}^m, M_{\mathcal{A}}^{(n)})\} \leq \Xi(R, R_{\mathcal{A}}). \tag{12}$$

Definition of the Region

Let U be an auxiliary random variable taking values in a finite set $\mathcal{U}$. We assume that the joint distribution of (U, Z, K) is

$$p_{UZK}(u, z, k) = p_U(u) p_{Z|U}(z|u) p_{K|Z}(k|z).$$

The above condition is equivalent to $U \leftrightarrow Z \leftrightarrow K$. Define the set of probability distribution $p = p_{UZK}$ by

$$\mathcal{P}(p_K, W) := \{p_{UZK} : |\mathcal{U}| \leq |\mathcal{Z}| + 1, U \leftrightarrow Z \leftrightarrow K\}.$$

Set

$$\mathcal{R}(p) := \{(R_{\mathcal{A}}, R) : R_{\mathcal{A}}, R \geq 0,\ R_{\mathcal{A}} \geq I(Z; U), R \geq H(K|U)\},$$

$$\mathcal{R}(p_K, W) := \bigcup_{p \in \mathcal{P}(p_K, W)} \mathcal{R}(p).$$

Property of $\mathcal{R}(p_K, W)$

Property 1

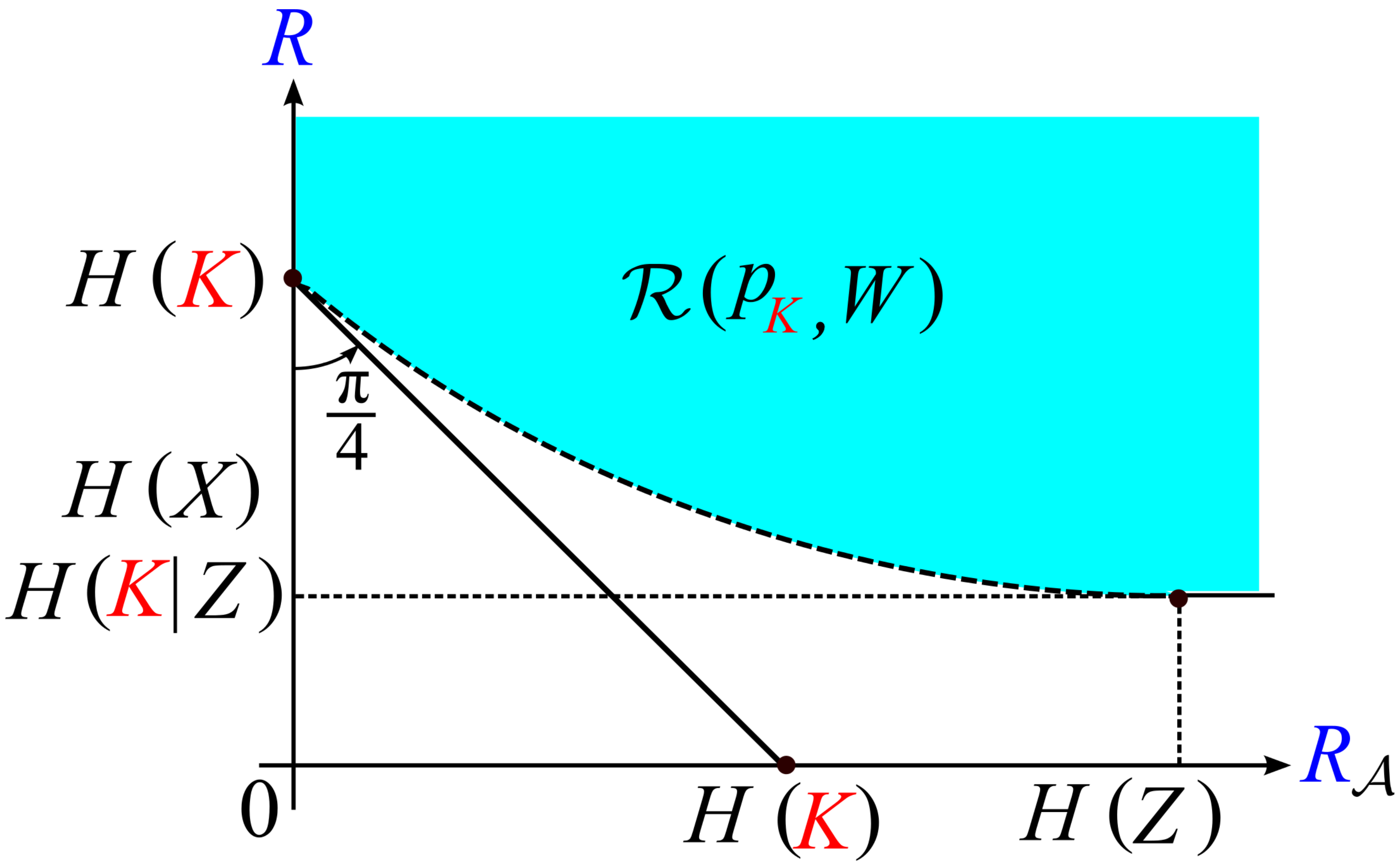
a) The region $\mathcal{R}(p_K, W)$ is a closed convex subset of $\mathbb{R}_+^2$.
b) For any (p_K, W), we have

$$\mathcal{R}(p_K, W) \subseteq \{(R_{\mathcal{A}}, R) : R_{\mathcal{A}} + R \geq H(K)\} \cap \mathbb{R}_+^2.$$

Furthermore, the point $(0, H(K))$ always belongs to $\mathcal{R}(p_K, W)$.

Property 1 part a) is a well known property. Proof of Property 1 part b) is easy. Proofs of Property 1 parts a) and b) are omitted.

Form of $\mathcal{R}(p_K, W)$



Definitions for Upper Bounds of $\Xi(R, R_{\mathcal{A}})$

Set

$$\mathcal{Q}(p_{K|Z}) := \{q = q_{UZK} : |\mathcal{U}| \leq |\mathcal{Z}|, U \leftrightarrow Z \leftrightarrow K, p_{K|Z} = q_{K|Z}\}.$$

For $(\mu, \alpha) \in [0,1]^2$, and for $q = q_{UZK} \in \mathcal{Q}(p_{K|Z})$, define

$$\omega_{q|p_Z}^{(\mu,\alpha)}(z,k|u) := \bar{\alpha} \log \frac{q_Z(z)}{p_Z(z)} + \alpha \left[\mu \log \frac{q_{Z|U}(z|u)}{p_Z(z)} + \log \frac{1}{q_{K|U}(k|u)} \right],$$

$$\Omega^{(\mu,\alpha)}(q|p_Z) := -\log \mathrm{E}_q \left[\exp \left\{ -\omega_{q|p_Z}^{(\mu,\alpha)}(Z,K|U) \right\} \right],$$

$$\Omega^{(\mu,\alpha)}(p_K, W) := \min_{q \in \mathcal{Q}(p_{K|Z})} \Omega^{(\mu,\alpha)}(q|p_Z),$$

$$F^{(\mu,\alpha)}(\mu R_{\mathcal{A}} + R | p_K, W) := \frac{\Omega^{(\mu,\alpha)}(p_K, W) - \alpha(\mu R_{\mathcal{A}} + R)}{2 + \alpha \bar{\mu}},$$

$$\boxed{F(R_{\mathcal{A}}, R | p_K, W)} := \sup_{\substack{(\mu,\alpha) \\ \in [0,1]^2}} F^{(\mu,\alpha)}(R_{\mathcal{A}}, R | p_K, W).$$

Property of $F(R_{\mathcal{A}}, R|p_K, W)$(1/2)

Property 2

a) The cardinality bound $|\mathcal{U}| \leq |\mathcal{Z}|$ in $\mathcal{Q}(p_{K|Z})$ is sufficient to describe the quantity $\Omega^{(\mu,\alpha)}(p_K, W)$.

b) Fix any $p = p_{UZK} \in \mathcal{P}_{\rm sh}(p_K, W)$ and $\mu \in [0,1]$. Define

$$\tilde{\omega}_p^{(\mu)}(z,k|u) := \mu \log \frac{p_{Z|U}(z|u)}{p_Z(z)} + \log \frac{1}{p_{K|U}(K|U)}.$$

For $\lambda \in [0, 1/2]$, define a probability distribution $p^{(\lambda)} = p_{UZK}^{(\lambda)}$ by

$$p^{(\lambda)}(u,z,k) := \frac{p(u,z,k) \exp\left\{-\lambda \tilde{\omega}_p^{(\mu)}(z,k|u)\right\}}{\mathrm{E}_p\left[\exp\left\{-\lambda \tilde{\omega}_p^{(\mu)}(Z,K|U)\right\}\right]}.$$

Property of $F(R_{\mathcal{A}}, R|p_K, W)$(2/2)

Property 2

b) (Cont.) For $(\mu, \lambda) \in [0,1] \times [0,1/2]$, define

$$\rho^{(\mu,\lambda)}(p_K, W) := \max_{\substack{(\nu,p)\in[0,\lambda] \\ \times \mathcal{P}_{\mathrm{sh}}(p_K,W): \\ \tilde{\Omega}^{(\mu,\lambda)}(p) \\ = \tilde{\Omega}^{(\mu,\lambda)}(p_K,W)}} \mathrm{Var}_{p^{(\nu)}}\left[\tilde{\omega}_p^{(\mu)}(Z,K|U)\right],$$

and set

$$\rho = \rho(p_K, W) := \max_{(\mu,\lambda)\in[0,1]\times[0,1/2]} \rho^{(\mu,\lambda)}(p_K, W).$$

Then we have $\rho(p_K, W) < \infty$. Furthermore, for every $\tau \in (0, (1/2)\rho(p_K, W))$, $(R_{\mathcal{A}}, R+\tau) \notin \mathcal{R}(p_K, W)$ implies

$$F(R_{\mathcal{A}}, R|p_K, W) > \frac{\rho(p_K,W)}{4} \cdot g^2\left(\frac{\tau}{\rho(p_K,W)}\right) > 0,$$

where g is the inverse function of $\vartheta(a) := a + (3/2)a^2, a \geq 0$.

Upper Bound of $\Xi(R, R_{\mathcal{A}})$ (1/2)

Lemma 1 For any $\eta > 0$ and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have

$$\Xi(R, R_{\mathcal{A}}) \leq p_{M_{\mathcal{A}}^{(n)} Z^n K^n} \left\{ 0 \geq \frac{1}{n} \log \frac{q_{Z^n}(Z^n)}{p_{Z^n}(Z^n)} - \eta, \right. \tag{13}$$

$$0 \geq \frac{1}{n} \log \frac{\hat{q}_{M_{\mathcal{A}}^{(n)} Z^n K^n}(M_{\mathcal{A}}^{(n)}, Z^n, K^n)}{p_{M_{\mathcal{A}}^{(n)} Z^n K^n}(M_{\mathcal{A}}^{(n)}, Z^n, K^n)} - \eta, \tag{14}$$

$$R_{\mathcal{A}} \geq \frac{1}{n} \log \frac{p_{Z^n|M_{\mathcal{A}}^{(n)}}(Z^n|M_{\mathcal{A}}^{(n)})}{p_{Z^n}(Z^n)} - \eta,$$

$$\left. R \geq \frac{1}{n} \log \frac{1}{p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta \right\} + 4\mathrm{e}^{-n\eta}. \tag{15}$$

Upper Bound of $\Xi(R, R_{\mathcal{A}})$ (2/2)

Lemma 1(Cont.) The probability distributions appearing in the two inequalities (13) and (14) in the right members of (15) have a property that we can select them arbitrary. In (13), we can choose any distribution q_{Z^n} on $\mathcal{Z}^n$. In (14), we can choose any probability distribution $\hat{q}_{M_{\mathcal{A}}^{(n)} Z^n K^n}$ on $\mathcal{M}_{\mathcal{A}}^{(n)} \times \mathcal{Z}^n \times \mathcal{X}^n$.

In a manner similar to the derivation of the exponential upper bound of the correct probability of decoding for one helper source coding problem we can derive the same exponential upper bound of $\Xi(R, R_{\mathcal{A}})$. This result is shown in the following proposition.

Proposition 2 For any $R, R_{\mathcal{A}} \geq 0$, we have

$$\Xi(R, R_{\mathcal{A}}) \leq 5 \cdot \mathrm{e}^{-nF(R_{\mathcal{A}}, R | p_K, W)}. \tag{16}$$

From Propositions 1, 2, and Lemma 1 we immediately obtain the following result.

Main Result

Theorem 1 (Santoso and Oohama (Entropy, 19)) For any $R_{\mathcal{A}}, R > 0$, and any (p_K, W) with $(R_{\mathcal{A}}, R) \in \mathcal{R}^{\mathrm{c}}(p_Z, W)$, there exists a sequence of mappings $\{(\varphi^{(n)}, \psi^{(n)})\}_{n=1}^{\infty}$ satisfying

$$\frac{1}{n}\log|\mathcal{X}^m| = \frac{m}{n}\log|\mathcal{X}| \in \left[R - \frac{1}{n}, R\right],$$

such that for any p_X with $R > H(X)$,

$$p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n) \leq \mathrm{e}^{-n[E(R|p_X)-\delta_{1,n}]} \tag{17}$$

and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$,

$$\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n) \leq \mathrm{e}^{-n[F(R_{\mathcal{A}}, R|p_K, W)-\delta_{2,n}]}, \tag{18}$$

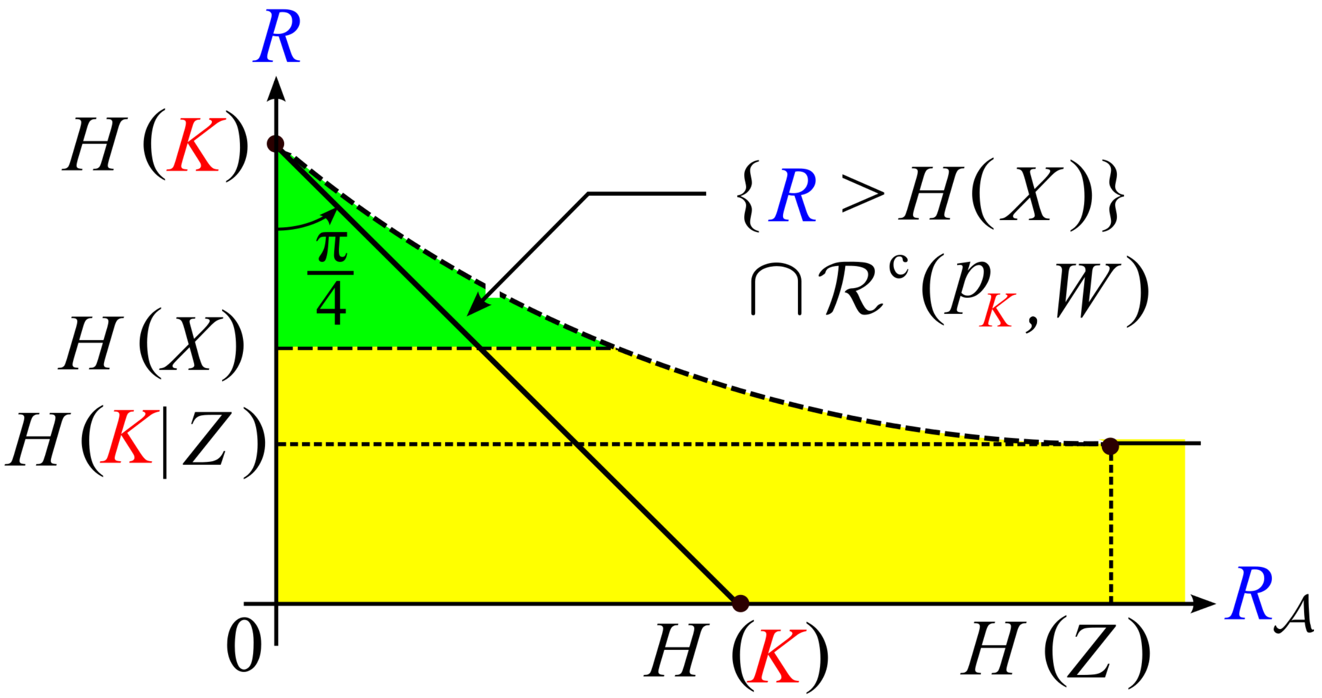
where $\delta_{i,n}, i = 1, 2$ are positive numbers satisfying $\delta_{i,n} \to 0$ as $n \to \infty$.

Implications of Theorem 1 (1/2)

We set

$$\mathcal{R}^{(\mathrm{in})}_{\mathsf{Sys}}(p_X, p_K, W) := \{R \geq H(X)\} \cap \mathrm{cl}\left[\mathcal{R}^{c}(p_K, W)\right],$$

where $\mathrm{cl}\left[\mathcal{R}^{\mathrm{c}}(p_K, W)\right]$ stands for the closure of the complement of $\mathcal{R}(p_K, W)$.



Implications of Theorem 1 (2/2)

By Theorem 1, under

$$(R_{\mathcal{A}}, R) \in \mathrm{int}\left[\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X, p_K, W)\right],$$

we have the followings:

- On the reliability, $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n)$ goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $E(R|p_X)$.
- On the security, for any $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(R_{\mathcal{A}})$, the information leakage $\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} |p_X^n, p_K^n, W^n)$ on X^n goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $F(R_{\mathcal{A}}, R|p_K, W)$.
- The code that attains the exponent functions $E(R|p_X)$ is the universal code that depends only on R not on the value of the distribution p_X.

Conclusions

Our Contribution:

1. We have formulated the problem of information theoretical analysis of side-channel attacks to the Shannon cipher system.
2. We have derived a sufficient condition of reliable and secure communication under the side-channel attacks.
3. To prove the exponential decrease of the information leakage we have used the author's technique of proving exponential strong converse to one helper source coding problem.

Future Works:

1. Derivation of the necessary and sufficient condition.
2. Extension to the case where Z is an analog random signal.
3. Extension to the case where we have several distributed side-channel attacks.

Finally...

- We have presented three topics in information theoretical security.
- Those are specific but provide new interesting problems raising in communication systems with security requirement.
- We think that in this fields we may have several such other interesting problems which remains to be investigated!