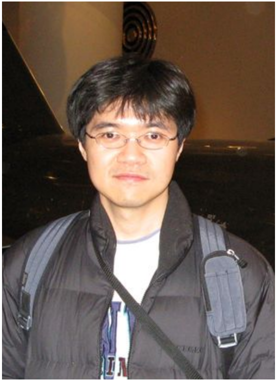
The Sender-Excited Secret Key Agreement Model: Capacity and Error Exponents

Tzu-Han Chou, **Vincent Y. F. Tan**, Stark C. Draper

Department of Electrical and Computer Engineering,
University of Wisconsin-Madison

Allerton (Sep 2011)

Joint work with



Tzu-Han Chou
Qualcomm

Stark C. Draper
UW-Madison

Introduction

- Consider the fundamental limits of the secret key generation problem

Introduction

- Consider the fundamental limits of the secret key generation problem
- There is a noiseless public discussion channel

Introduction

- Consider the fundamental limits of the secret key generation problem
- There is a noiseless public discussion channel
- Source is randomly excited by the sender

Introduction

- Consider the fundamental limits of the secret key generation problem
- There is a noiseless public discussion channel
- Source is randomly excited by the sender
- Motivated by
  - Key generation [Maurer, Ahlswede and Csiszár]
  - Key generation with external excitation [Chou, Draper and Sayeed]

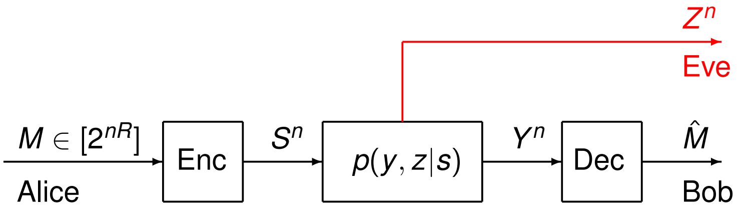
Introduction

- Consider the fundamental limits of the secret key generation problem
- There is a noiseless public discussion channel
- Source is randomly excited by the sender
- Motivated by
  - Key generation [Maurer, Ahlswede and Csiszár]
  - Key generation with external excitation [Chou, Draper and Sayeed]
  - Channels with action-dependent states [Weissman]

Introduction

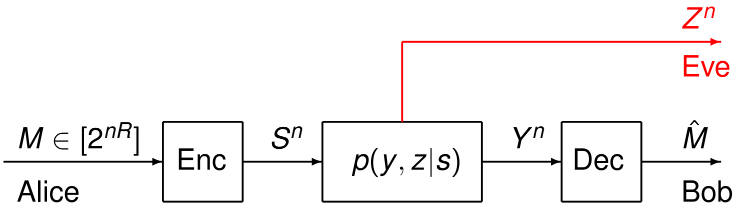
- Consider the fundamental limits of the secret key generation problem
- There is a noiseless public discussion channel
- Source is randomly excited by the sender
- Motivated by
  - Key generation [Maurer, Ahlswede and Csiszár]
  - Key generation with external excitation [Chou, Draper and Sayeed]
  - Channels with action-dependent states [Weissman]
- Main contributions:
  - Secret key capacity
  - Inner bound for rate-reliability-secrecy-exponent region

Wiretap Channel [Wyner, Csiszár and Körner]



- Want to transmit message reliably to Bob but keep Eve ignorant
- $\mathbb{P}(\hat{M} \neq M) \to 0$ and $\frac{1}{n} I(M; Z^n) \to 0$

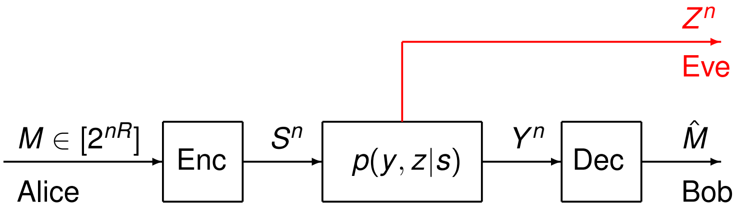
Wiretap Channel [Wyner, Csiszár and Körner]



- Want to transmit message reliably to Bob but keep Eve ignorant
- $\mathbb{P}(\hat{M} \neq M) \to 0$ and $\frac{1}{n} I(M; Z^n) \to 0$
- Wiretap channel capacity

$$C_{\text{wiretap}} = \max_{U - S - (Y,Z)} \{ I(U; Y) - I(U; Z) \}$$

Wiretap Channel [Wyner, Csiszár and Körner]

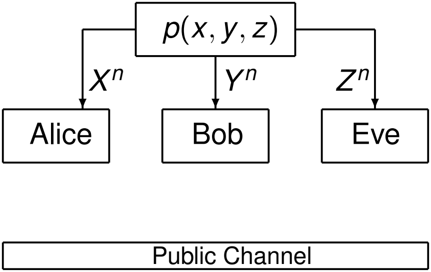


- Want to transmit message reliably to Bob but keep Eve ignorant
- $\mathbb{P}(\hat{M} \neq M) \to 0$ and $\frac{1}{n} I(M; Z^n) \to 0$
- Wiretap channel capacity

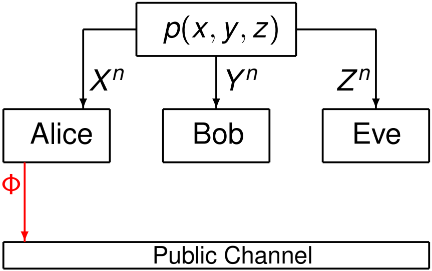
$$C_{\text{wiretap}} = \max_{U-S-(Y,Z)} \{I(U;Y) - I(U;Z)\}$$

- Channel-type model

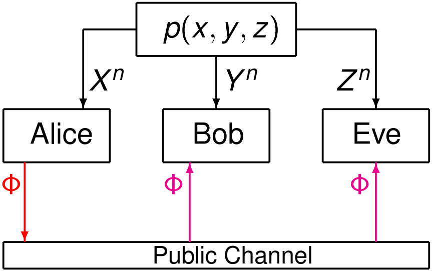
Secret Key Generation [Maurer, Ahlswede & Csiszár]



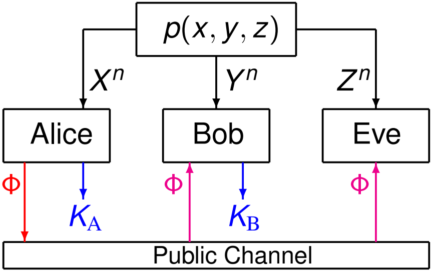
Secret Key Generation [Maurer, Ahlswede & Csiszár]



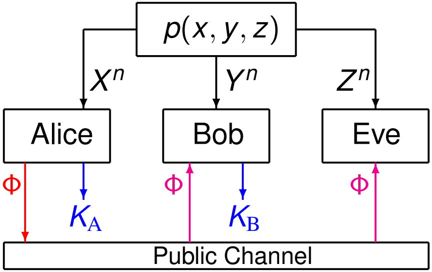
Secret Key Generation [Maurer, Ahlswede & Csiszár]



Secret Key Generation [Maurer, Ahlswede & Csiszár]

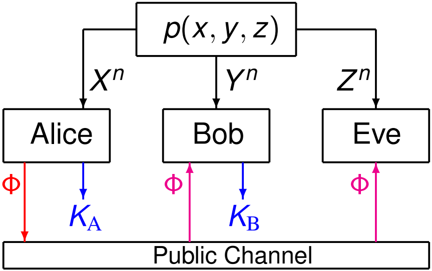


Secret Key Generation [Maurer, Ahlswede & Csiszár]



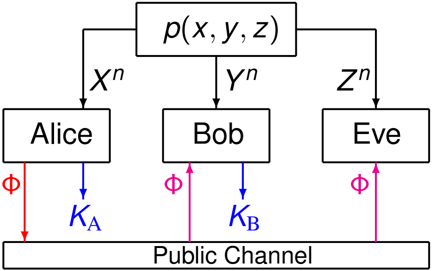
- Secret keys are generated from dependent sources X, Y, Z

Secret Key Generation [Maurer, Ahlswede & Csiszár]



- Secret keys are generated from dependent sources X, Y, Z
- $\mathbb{P}(K_A \neq K_B) \to 0$ and $\frac{1}{n} I(K_A; Z^n, \Phi) \to 0$

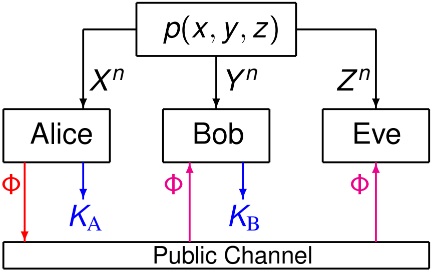
Secret Key Generation [Maurer, Ahlswede & Csiszár]



- Secret keys are generated from dependent sources X, Y, Z
- $\mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \to 0$ and $\frac{1}{n} I(K_{\mathrm{A}}; Z^n, \Phi) \to 0$
- Secret key capacity

$$C_{\mathrm{SK}} = \max_{W - U - X - (Y,Z)} \{ I(U; Y|W) - I(U; Z|W) \}$$

Secret Key Generation [Maurer, Ahlswede & Csiszár]

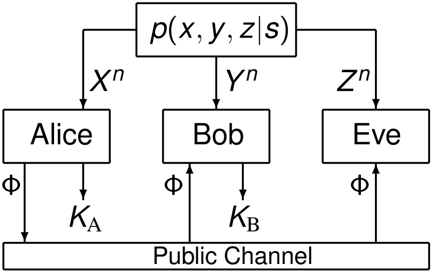


- Secret keys are generated from dependent sources X, Y, Z
- $\mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \to 0$ and $\frac{1}{n} I(K_{\mathrm{A}}; Z^n, \Phi) \to 0$
- Secret key capacity

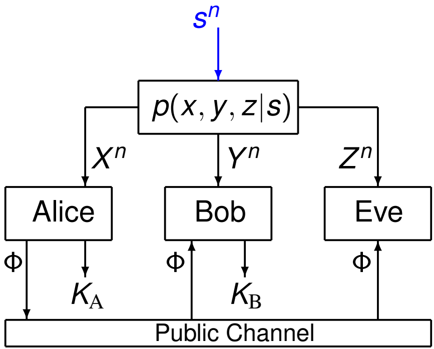
$$C_{\mathrm{SK}} = \max_{W - U - X - (Y,Z)} \{I(U; Y|W) - I(U; Z|W)\}$$

- Source-type model

Key Generation with External Excitation [Chou et al.]

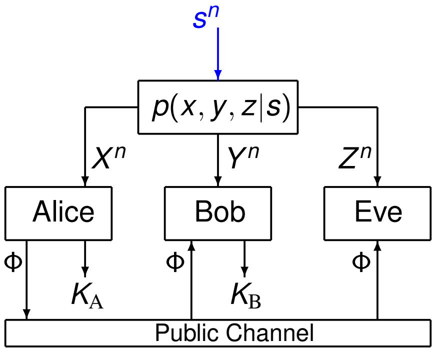


Key Generation with External Excitation [Chou et al.]



- Wireless channels $\Rightarrow$ auxiliary randomness
- Due to multipath fading
- Transmissions are bi-directional $\Rightarrow$ X, Y, Z generated by transmitting prearranged sounding signals.

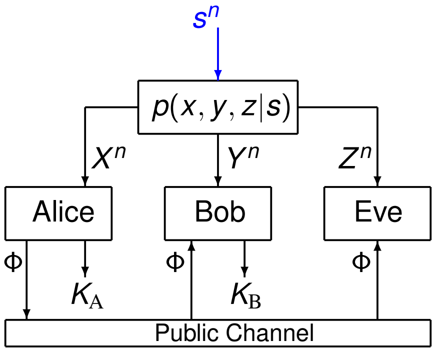
Key Generation with External Excitation [Chou et al.]



- Wireless channels $\Rightarrow$ auxiliary randomness
- Due to multipath fading
- Transmissions are bi-directional $\Rightarrow X, Y, Z$ generated by transmitting prearranged sounding signals.

- External excitation via a deterministic sounding signal s^n

Key Generation with External Excitation [Chou et al.]

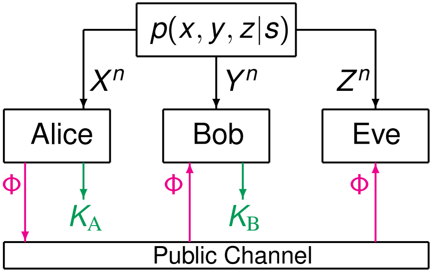


- Wireless channels $\Rightarrow$ auxiliary randomness
- Due to multipath fading
- Transmissions are bi-directional $\Rightarrow X, Y, Z$ generated by transmitting prearranged sounding signals.

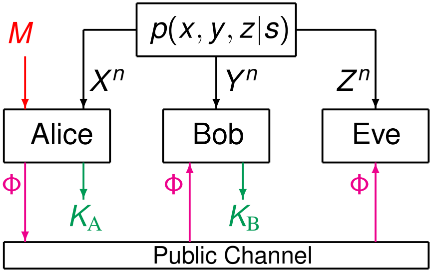
- External excitation via a deterministic sounding signal s^n
- Secret key capacity

$$C_{\text{SK}} = \max_{p(w,u|s),p(x|u,s),p(s)} \{I(U; Y|W, S) - I(U; Z|W, S)\}$$

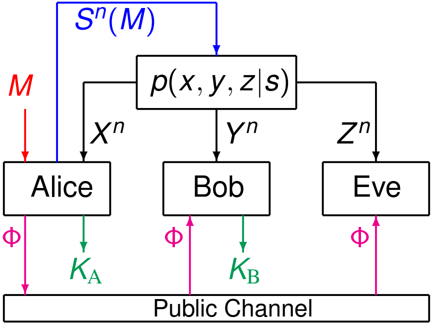
Our model: Sender-Excited Secret Key Agreement



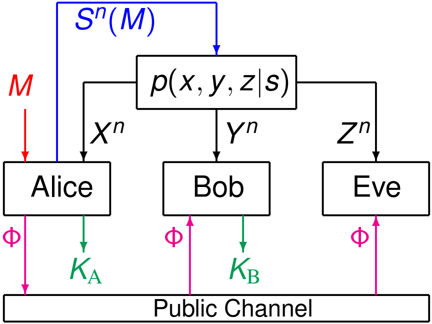
Our model: Sender-Excited Secret Key Agreement



Our model: Sender-Excited Secret Key Agreement

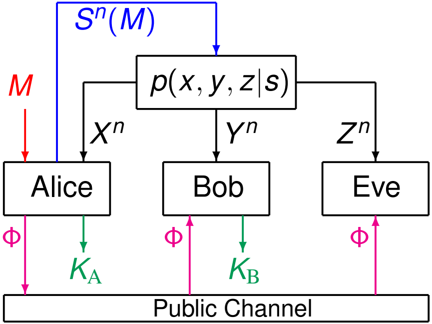


Our model: Sender-Excited Secret Key Agreement



A $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ code consists of a uniform $M \in [2^{nR_M}]$ and

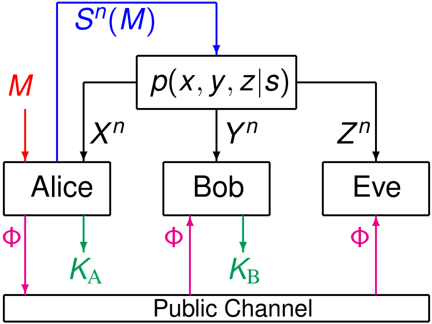
Our model: Sender-Excited Secret Key Agreement



A $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ code consists of a uniform $M \in [2^{nR_M}]$ and

- Channel Excitation: $s^n = s^n(m)$ such that $\frac{1}{n}\sum_{i=1}^{n} \Lambda(s_i(m)) \leq \Gamma$

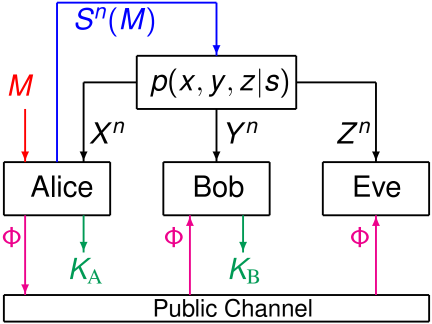
Our model: Sender-Excited Secret Key Agreement



A $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ code consists of a uniform $M \in [2^{nR_M}]$ and

- Channel Excitation: $s^n = s^n(m)$ such that $\frac{1}{n}\sum_{i=1}^n \Lambda(s_i(m)) \leq \Gamma$
- One-way Public Discussion: Alice generates a public message $\phi = \phi(m, x^n) \in [2^{nR_\Phi}]$ and transmits it over a noiseless channel

Our model: Sender-Excited Secret Key Agreement



A $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ code consists of a uniform $M \in [2^{nR_M}]$ and

- Channel Excitation: $s^n = s^n(m)$ such that $\frac{1}{n}\sum_{i=1}^{n} \Lambda(s_i(m)) \le \Gamma$
- One-way Public Discussion: Alice generates a public message $\phi = \phi(m, x^n) \in [2^{nR_\Phi}]$ and transmits it over a noiseless channel
- Key Generation: $k_{\mathrm{A}} = k_{\mathrm{A}}(m, x^n) \in \mathbb{N}$ and $k_{\mathrm{B}} = k_{\mathrm{B}}(\phi, y^n) \in \mathbb{N}$

Motivation for our model

- Combine the source-type model with the wiretap channel model to extract higher SK rate?

Motivation for our model

- Combine the source-type model with the wiretap channel model to extract higher SK rate?

- Can parties (or sender) excite the source with private source of randomness M?

Motivation for our model

- Combine the source-type model with the wiretap channel model to extract higher SK rate?
- Can parties (or sender) excite the source with private source of randomness M?
- Our model is also inspired by
  - Channels with action-dependent states [Weissman 2010]
  - Probing capacity [Asnani et al. 2010]

Motivation for our model

- Combine the source-type model with the wiretap channel model to extract higher SK rate?
- Can parties (or sender) excite the source with private source of randomness M?
- Our model is also inspired by
  - Channels with action-dependent states [Weissman 2010]
  - Probing capacity [Asnani et al. 2010]
  - Key generation when encoder and decoder have state information [Khisti, Diggavi, Wornell 2011]

Weak Achievability

The rate R_{SK} is weakly-achievable if there exists a sequence of $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ codes such that

$$\lim_{n\to\infty} \mathbb{P}(K_\mathrm{A} \neq K_\mathrm{B}) = 0$$

$$\lim_{n\to\infty} \frac{1}{n} I(K_\mathrm{A}; Z^n, \Phi) = 0$$

$$\liminf_{n\to\infty} \frac{1}{n} H(K_\mathrm{A}) \geq R_{\mathrm{SK}}$$

Weak Achievability

The rate R_{SK} is weakly-achievable if there exists a sequence of $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ codes such that

$$\lim_{n\to\infty} \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) = 0$$

$$\lim_{n\to\infty} \quad \frac{1}{n} I(K_{\mathrm{A}}; Z^n, \Phi) = 0$$

$$\liminf_{n\to\infty} \quad \frac{1}{n} H(K_{\mathrm{A}}) \geq R_{\mathrm{SK}}$$

Definition ((Weak)-Secret key capacity)

$C_{\mathrm{SK}}(\Gamma) := \sup\{R_{\mathrm{SK}} : R_{\mathrm{SK}} \text{ weakly-achievable}\}$

Weak Achievability

The rate R_{SK} is weakly-achievable if there exists a sequence of $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ codes such that

$$\lim_{n\to\infty} \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) = 0$$

$$\lim_{n\to\infty} \frac{1}{n} I(K_{\mathrm{A}}; Z^n, \Phi) = 0$$

$$\liminf_{n\to\infty} \frac{1}{n} H(K_{\mathrm{A}}) \geq R_{\mathrm{SK}}$$

Definition ((Weak)-Secret key capacity)

$C_{\mathrm{SK}}(\Gamma) := \sup\{R_{\mathrm{SK}} : R_{\mathrm{SK}} \text{ weakly-achievable}\}$

But weak secrecy $\frac{1}{n} I(K_{\mathrm{A}}; Z^n, \Phi) \to 0$ is usually not good enough

[Maurer & Wolf 2000], [Watanabe et al. 2009], [Bloch & Barros 2011], [Bloch & Laneman 2011],

Strong Achievability

The rate-exponent triple (R_{SK}, E, F) is achievable if there exists a sequence of $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ codes such that

$$\liminf_{n\to\infty} -\frac{1}{n}\log \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \geq E, \quad \Leftrightarrow \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \stackrel{.}{\leq} 2^{-nE}$$

$$\liminf_{n\to\infty} -\frac{1}{n}\log I(K_{\mathrm{A}}; Z^n, \Phi) \geq F, \quad \Leftrightarrow \quad I(K_{\mathrm{A}}; Z^n, \Phi) \stackrel{.}{\leq} 2^{-nF}$$

$$\liminf_{n\to\infty} \frac{1}{n}H(K_{\mathrm{A}}) \geq R_{\mathrm{SK}}$$

Strong Achievability

The rate-exponent triple (R_{SK}, E, F) is achievable if there exists a sequence of $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ codes such that

$$\liminf_{n\to\infty} \quad -\frac{1}{n}\log \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \geq E, \qquad \Leftrightarrow \qquad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \stackrel{.}{\leq} 2^{-nE}$$

$$\liminf_{n\to\infty} \quad -\frac{1}{n}\log I(K_{\mathrm{A}}; Z^n, \Phi) \geq F, \qquad \Leftrightarrow \qquad I(K_{\mathrm{A}}; Z^n, \Phi) \stackrel{.}{\leq} 2^{-nF}$$

$$\liminf_{n\to\infty} \quad \frac{1}{n}H(K_{\mathrm{A}}) \geq R_{\mathrm{SK}}$$

Definition (Capacity-reliability-secrecy region)

$$\mathcal{R}^*(p(x,y,z|s)) := \overline{\left\{(R_{\mathrm{SK}}, E, F) \in \mathbb{R}_+^3 \;:\; (R_{\mathrm{SK}}, E, F) \text{ achievable}\right\}}$$

Strong Achievability

The rate-exponent triple (R_{SK}, E, F) is achievable if there exists a sequence of $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$ codes such that

$$\liminf_{n\to\infty} \quad -\frac{1}{n}\log \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \geq E, \quad \Leftrightarrow \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \dot{\leq} 2^{-nE}$$

$$\liminf_{n\to\infty} \quad -\frac{1}{n}\log I(K_{\mathrm{A}}; Z^n, \Phi) \geq F, \quad \Leftrightarrow \quad I(K_{\mathrm{A}}; Z^n, \Phi) \dot{\leq} 2^{-nF}$$

$$\liminf_{n\to\infty} \quad \frac{1}{n} H(K_{\mathrm{A}}) \geq R_{\mathrm{SK}}$$

Definition (Capacity-reliability-secrecy region)

$$\mathcal{R}^*(p(x,y,z|s)) := \overline{\left\{(R_{\mathrm{SK}}, E, F) \in \mathbb{R}^3_+ \ : \ (R_{\mathrm{SK}}, E, F) \text{ achievable}\right\}}$$

Definition (Strong-achievability)

R_{SK} is strongly-achievable if (R_{SK}, E, F) is achievable for some $E, F > 0$

Capacity Result

Theorem (Secret Key Capacity for Sender-Excited Model)

The secret key capacity is

$$C_{\mathrm{SK}}(\Gamma) = \max \left\{ I(U, V; Y|W) - I(U, V; Z|W) \right\}$$

where the max is over all joints

$$p(w, u, v, s, x, y, z) = p(w, u)p(s|u)p(v|w, u, x)p(x, y, z|s)$$

such that $\mathbb{E}\Lambda(S) \leq \Gamma$.

Remarks on Capacity Result

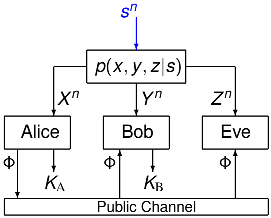
- $C_{\mathrm{SK}}(\Gamma) = \max\{I(U, V; Y|W) - I(U, V; Z|W)\}$

- $C_{\mathrm{SK}}(\Gamma) = \max\{I(U,V;Y|W) - I(U,V;Z|W)\}$
- Rate can be written as $R_{\mathrm{ch}} + R_{\mathrm{src}}$ where

$$R_{\mathrm{ch}} = I(U;Y|W) - I(U;Z|W),$$
$$R_{\mathrm{src}} = I(V;Y|W,U) - I(V;Y|W,U)$$

- $R_{\mathrm{ch}} =$ Confidential message rate of wiretap channel $p(y,z|s)$
- $R_{\mathrm{src}} =$ Secret key rate of excited source $p(x,y,z|s)$ [Chou et al.]
    - Sounding signal s^n deterministic
    - Roughly, $p(s)$ chosen to max

$$I(V;Y|W,S) - I(V;Z|W,S)$$



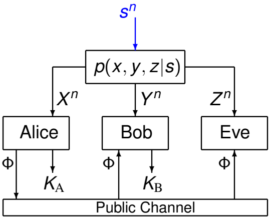
Remarks on Capacity Result

- $C_{\mathrm{SK}}(\Gamma) = \max\{I(U,V;Y|W) - I(U,V;Z|W)\}$
- Rate can be written as $R_{\mathrm{ch}} + R_{\mathrm{src}}$ where

$$R_{\mathrm{ch}} = I(U;Y|W) - I(U;Z|W),$$
$$R_{\mathrm{src}} = I(V;Y|W,U) - I(V;Y|W,U)$$

- R_{ch} = Confidential message rate of wiretap channel $p(y,z|s)$
- R_{src} = Secret key rate of excited source $p(x,y,z|s)$ [Chou et al.]
  - Sounding signal s^n deterministic
  - Roughly, $p(s)$ chosen to max

$$I(V;Y|W,S) - I(V;Z|W,S)$$



- Capacity: Find optimal sum rate $R_{\mathrm{ch}} + R_{\mathrm{src}}$

Degradedness

We say that the DM-BC $p(x, y, z|s)$ is degraded if

$$(X, S) - Y - Z$$

Degradedness

We say that the DM-BC $p(x, y, z|s)$ is degraded if

$$(X, S) - Y - Z$$

Theorem (Secret Key Capacity for Degraded Sender-Excited Model)

If the DM-BC $p(x, y, z|s)$ is degraded the secret key capacity is

$$C_{\mathrm{SK}}(\Gamma) = C_{\mathrm{SK}}^{(\mathrm{Weak})}(\Gamma) = \max_{p(s):\mathbb{E}\Lambda(S)\le\Gamma} \{I(X, S; Y) - I(X, S; Z)\}$$

Also, $C_{\mathrm{SK}}^{(\mathrm{Weak})}(\Gamma) = C_{\mathrm{SK}}^{(\mathrm{Strong})}(\Gamma)$

Degradedness

We say that the DM-BC $p(x, y, z|s)$ is degraded if

$$(X, S) - Y - Z$$

Theorem (Secret Key Capacity for Degraded Sender-Excited Model)

If the DM-BC $p(x, y, z|s)$ is degraded the secret key capacity is

$$C_{\mathrm{SK}}(\Gamma) = C_{\mathrm{SK}}^{(\mathrm{Weak})}(\Gamma) = \max_{p(s):\mathbb{E}\Lambda(S)\le\Gamma} \{I(X, S; Y) - I(X, S; Z)\}$$

Also, $C_{\mathrm{SK}}^{(\mathrm{Weak})}(\Gamma) = C_{\mathrm{SK}}^{(\mathrm{Strong})}(\Gamma)$

$$R_{\mathrm{ch}} = I(S; Y) - I(S; Z), \qquad R_{\mathrm{src}} = I(X; Y|S) - I(X; Z|S)$$

Binary Example

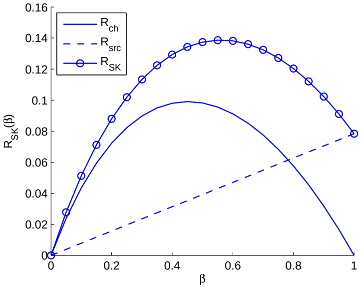
Consider the case where $S, X, Y, Z \in \mathbb{F}_2$:

$$X = (H \cdot S) \oplus N_1, \qquad Y = (H \cdot S) \oplus N_2, \qquad Z = (\tilde{H} \cdot H \cdot S) \oplus N_3$$

Binary Example

Consider the case where $S, X, Y, Z \in \mathbb{F}_2$:

$$X = (H \cdot S) \oplus N_1, \qquad Y = (H \cdot S) \oplus N_2, \qquad Z = (\tilde{H} \cdot H \cdot S) \oplus N_3$$

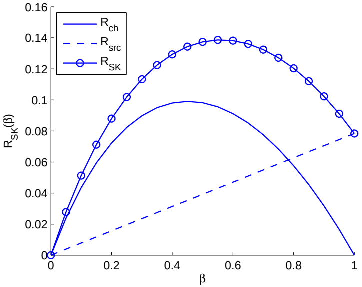


- Noises N_i indep
- H and $\tilde{H}$ indep
- $S \sim \mathrm{Bern}(\beta)$
- $R_{\mathrm{ch}} = I(S; Y) - I(S; Z)$
- $R_{\mathrm{src}} = I(X; Y|S) - I(X; Z|S)$

Binary Example

Consider the case where $S, X, Y, Z \in \mathbb{F}_2$:

$$X = (H \cdot S) \oplus N_1, \qquad Y = (H \cdot S) \oplus N_2, \qquad Z = (\tilde{H} \cdot H \cdot S) \oplus N_3$$



- Noises N_i indep
- H and $\tilde{H}$ indep
- $S \sim \mathrm{Bern}(\beta)$
- $R_{\mathrm{ch}} = I(S; Y) - I(S; Z)$
- $R_{\mathrm{src}} = I(X; Y|S) - I(X; Z|S)$

- Interplay between common randomness and wiretap rate

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \stackrel{.}{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \stackrel{.}{\leq} 2^{-nF}$$

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \ge n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \ne K_{\mathrm{B}}) \,\dot{\le}\, 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \,\dot{\le}\, 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M) := \max_{0 \le \rho \le 1} \rho(-R_M + R_\Phi) - \log \sum_y \left[\sum_{s,x} p(s) p(x, y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \dot{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \dot{\leq} 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$

$$:= \max_{0\leq\rho\leq 1} \rho(-R_M + R_\Phi) - \log \sum_y \left[\sum_{s,x} p(s) p(x, y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

$$:= \max_{0\leq\rho\leq 1} -\rho R_M + \rho R_\Phi - \log \sum_y \left[\sum_{s,x} p(s) p(y|s)^{\frac{1}{1+\rho}} p(x|y,s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \stackrel{.}{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \stackrel{.}{\leq} 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$

$$:= \max_{0\leq\rho\leq 1} \rho(-R_M + R_\Phi) - \log \sum_y \left[\sum_{s,x} p(s)p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

$$:= \max_{0\leq\rho\leq 1} -\rho R_M + \rho R_\Phi - \log \sum_y \left[\sum_{s,x} p(s)p(y|s)^{\frac{1}{1+\rho}} p(x|y,s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

- Gallager's channel coding exponent [Gallager's Book Ch. 5]

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \dot{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \dot{\leq} 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$

$$:= \max_{0 \leq \rho \leq 1} \rho(-R_M + R_\Phi) - \log \sum_y \left[\sum_{s,x} p(s)p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

$$:= \max_{0 \leq \rho \leq 1} -\rho R_M + \rho R_\Phi - \log \sum_y \left[\sum_{s,x} p(s)p(y|s)^{\frac{1}{1+\rho}} p(x|y,s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

- Gallager's source coding with side information exponent [1976]

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \ge n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \ne K_{\mathrm{B}}) \,\dot{\le}\, 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \,\dot{\le}\, 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$
$$:= \max_{0\le\rho\le 1} \rho(-R_M + R_\Phi) - \log \sum_y \left[\sum_{s,x} p(s) p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \dot{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \dot{\leq} 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$
$$:= \max_{0 \leq \rho \leq 1} \rho(R_\Phi - R_M) - \log \sum_y \left[\sum_{s,x} p(s) p(x, y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

- Define secrecy exponent given $p(s), R_{\mathrm{SK}}, R_\Phi, R_M$

$$F_{\mathrm{o}}(p(s), R_{\mathrm{SK}}, R_\Phi, R_M)$$
$$:= \sup_{0 < \alpha \leq 1} -\alpha(R_{\mathrm{SK}} + R_\Phi - R_M) - \log \sum_{x,z,s} p(x, z, s) \left[\frac{p(x, z|s)}{p(z)} \right]^\alpha$$

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \stackrel{.}{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \stackrel{.}{\leq} 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$
$$:= \max_{0 \leq \rho \leq 1} \rho(R_\Phi - R_M) - \log \sum_y \left[\sum_{s,x} p(s) p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

- Define secrecy exponent given $p(s), R_{\mathrm{SK}}, R_\Phi, R_M$

$$F_{\mathrm{o}}(p(s), R_{\mathrm{SK}}, R_\Phi, R_M)$$
$$:= \sup_{0 < \alpha \leq 1} -\alpha(R_{\mathrm{SK}} + R_\Phi - R_M) - \log \sum_{x,z,s} p(x,z,s) \left[p(x|z,s) \frac{p(z|s)}{p(z)} \right]^\alpha$$

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \dot{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \dot{\leq} 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$
$$:= \max_{0 \leq \rho \leq 1} \rho(R_\Phi - R_M) - \log \sum_y \left[\sum_{s,x} p(s) p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

- Define secrecy exponent given $p(s), R_{\mathrm{SK}}, R_\Phi, R_M$

$$F_{\mathrm{o}}(p(s), R_{\mathrm{SK}}, R_\Phi, R_M)$$
$$:= \sup_{0 < \alpha \leq 1} -\alpha(R_{\mathrm{SK}} + R_\Phi - R_M) - \log \sum_{x,z,s} p(x,z,s) \left[p(x|z,s) \frac{p(z|s)}{p(z)} \right]^{\alpha}$$

Error Exponents: Setup

- Recall that (R_{SK}, E, F) is achievable if

$$H(K_{\mathrm{A}}) \geq n(R_{\mathrm{SK}} - \epsilon), \quad \mathbb{P}(K_{\mathrm{A}} \neq K_{\mathrm{B}}) \dot{\leq} 2^{-nE}, \quad I(K_{\mathrm{A}}; Z^n, \Phi) \dot{\leq} 2^{-nF}$$

- Define reliability exponent given $p(s), R_\Phi, R_M$

$$E_{\mathrm{o}}(p(s), R_\Phi, R_M)$$
$$:= \max_{0\leq\rho\leq 1} \rho(R_\Phi - R_M) - \log \sum_y \left[\sum_{s,x} p(s)p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}$$

- Define secrecy exponent given $p(s), R_{\mathrm{SK}}, R_\Phi, R_M$

$$F_{\mathrm{o}}(p(s), R_{\mathrm{SK}}, R_\Phi, R_M)$$
$$:= \sup_{0<\alpha\leq 1} -\alpha(R_{\mathrm{SK}} + R_\Phi - R_M) - \log \sum_{x,z,s} p(x,z,s) \left[\frac{p(x,z|s)}{p(z)} \right]^\alpha$$

Error Exponents: Result

Theorem (Inner bound to Capacity-Reliability-Secrecy Region)

Let $\mathcal{R}(p(s), R_\Phi, R_M) := \big\{(R_{\mathrm{SK}}, E, F) \in \mathbb{R}_+^3 :$

Error Exponents: Result

Theorem (Inner bound to Capacity-Reliability-Secrecy Region)

Let $\mathcal{R}(p(s), R_\Phi, R_M) := \big\{(R_{\mathrm{SK}}, E, F) \in \mathbb{R}_+^3 : E \leq E_{\mathrm{o}}(p(s), R_\Phi, R_M),$

Error Exponents: Result

Theorem (Inner bound to Capacity-Reliability-Secrecy Region)

Let $\mathcal{R}(p(s), R_\Phi, R_M) := \big\{(R_{\mathrm{SK}}, E, F) \in \mathbb{R}_+^3 : E \le E_{\mathrm{o}}(p(s), R_\Phi, R_M), F \le F_{\mathrm{o}}(p(s), R_{\mathrm{SK}}, R_\Phi, R_M)\big\}.$

Theorem (Inner bound to Capacity-Reliability-Secrecy Region)

Let $\mathcal{R}(p(s), R_\Phi, R_M) := \big\{(R_{\mathrm{SK}}, E, F) \in \mathbb{R}_+^3 : E \leq E_{\mathrm{o}}(p(s), R_\Phi, R_M),$
$F \leq F_{\mathrm{o}}(p(s), R_{\mathrm{SK}}, R_\Phi, R_M)\big\}$. *Then,*

$$\bigcup_{p(s), R_\Phi, R_M} \mathcal{R}(p(s), R_\Phi, R_M) \subset \mathcal{R}^*(p(x, y, z|s))$$

Error Exponents: Result

Theorem (Inner bound to Capacity-Reliability-Secrecy Region)

Let $\mathcal{R}(p(s), R_\Phi, R_M) := \big\{(R_{\mathrm{SK}}, E, F) \in \mathbb{R}_+^3 : E \le E_{\mathrm{o}}(p(s), R_\Phi, R_M),$ $F \le F_{\mathrm{o}}(p(s), R_{\mathrm{SK}}, R_\Phi, R_M)\big\}$. *Then,*

$$\bigcup_{p(s), R_\Phi, R_M} \mathcal{R}(p(s), R_\Phi, R_M) \subset \mathcal{R}^*(p(x, y, z|s))$$

- Reliability exponent E:
  - Gallager's channel coding exponent [1968]
  - Gallager's source coding with side information exponent [1976]
- Secrecy exponent F:
  - Hayashi's wiretap channel exponents [2006, 2011]
  - Chou's key agreement model with external excitation [In Press]
- Strongly-achievable rates for degraded case [Preprint]

Error Exponents: Binary Example

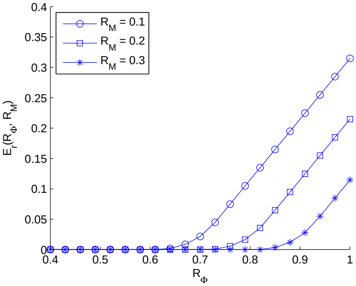
R_M: Rate of Alice's Private mess.

R_Φ: Rate of Public mess.

R_{SK}: Secret key rate

Error Exponents: Binary Example

R_M: Rate of Alice's Private mess. R_Φ: Rate of Public mess.
R_{SK}: Secret key rate

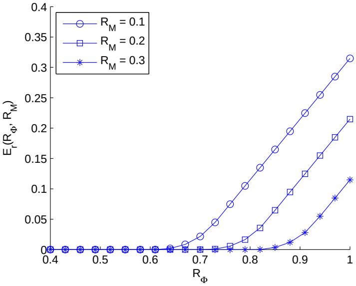


- When $R_M \uparrow$ rel. exp. $\downarrow$
- When $R_\Phi \uparrow$ rel. exp. $\uparrow$

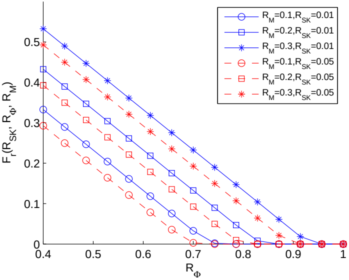
Error Exponents: Binary Example

R_M: Rate of Alice's Private mess.
$R_{\rm SK}$: Secret key rate

R_Φ: Rate of Public mess.



- When $R_M \uparrow$ rel. exp. $\downarrow$
- When $R_\Phi \uparrow$ rel. exp. $\uparrow$



- When $R_M \uparrow$ sec. exp. $\uparrow$
- When $R_\Phi \uparrow$ sec. exp. $\downarrow$
- When $R_{\rm SK} \uparrow$ sec. exp. $\downarrow$

Conclusions and Open Problems

- Proposed the sender-excited model for key agreement

Conclusions and Open Problems

- Proposed the sender-excited model for key agreement
- Derived the capacity and an inner bound to the capacity-reliability-secrecy region

Conclusions and Open Problems

- Proposed the sender-excited model for key agreement
- Derived the capacity and an inner bound to the capacity-reliability-secrecy region
- Inner bound for multi-way discussion? Strictly better?

Conclusions and Open Problems

- Proposed the sender-excited model for key agreement
- Derived the capacity and an inner bound to the capacity-reliability-secrecy region
- Inner bound for multi-way discussion? Strictly better?
- Outer bound to capacity-reliability-secrecy region?