On the Use of Secret Keys in Broadcast Channels with Receiver Side Information

Rafael Schaefer

PRINCETON UNIVERSITY

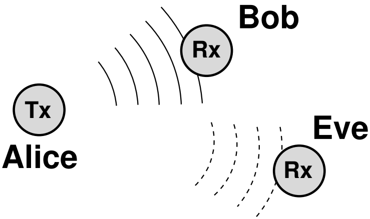
joint work with
Ashish Khisti (University of Toronto)
Holger Boche (Technische Universität München)

SS4: Signal Processing for Cyber-Security and Privacy

May 7, 2014

Motivation

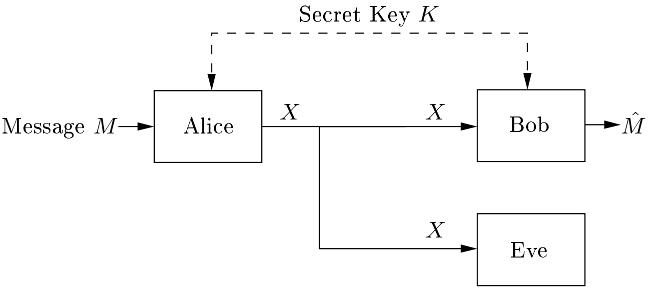
- Signal is received by legitimate users but also eavesdropped by **non-legitimate users**
  - ➠ Need of secure communication systems



- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers
  - ➠ **Use of information theoretic secrecy concepts**

Information Theoretic Secrecy

Shannon ’49

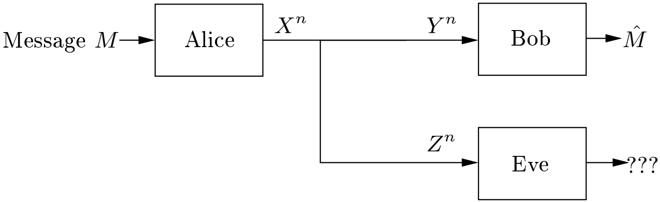


- Perfect secrecy $P(M|X) = P(M)$
- Key size = message length

➠ **One-time pad**

Wiretap Channel

Wyner ’75



- Reliability constraint : $\Pr(M \neq \hat{M}) \xrightarrow{n} 0$
- Secrecy Constraint : $I(M; Z^n) \xrightarrow{n} 0$

➠ **Secrecy Capacity**

Wiretap Channel - Extensions

MIMO Channels (Spatial Diversity)

Negi-Goel (2008), Khisti-Wornell (2010), Oggier-Hassibi (2011), Liu-Shamai (2009), Shafiee-Liu-Ulukus (2009), Liu-Bustin-Shamai-Poor (2010), He-Khisti-Yener (2011), Loyka-Charalambous (2012), Mukherjee-Swindlehurst (2011), Shi-Ritcey (2010)

Fading Channels (Power and Rate Control)

Liang-Poor-Shamai (2008), Lai-Gopala-ElGamal (2008), Khisti-Tchamkerten-Wornell (2008), Bloch-Barros- Rodrigues-McLaughlin (2011), Li-Petropulu (2011), Tang-Liu-Spasojevic (2009), Khalil-Youssef-Koyluoglu-ElGamal (2009)

Multiuser Channels and Cooperative Communications

Oohama (2006), Liang-Poor (2008), Lai-ElGamal (2008), Liu-Maric-Spasojevic-Yates (2008), Koyluoglu-ElGamal-Lai (2011), Liu-Prabhakaran-Vishwanath (2008), Tang-Liu-Spasojevic (2011), Lai-ElGamal-Poor (2008), Xu-Gao-Chen (2009)

Coding Techniques

Thangaraj-Dihidar-Calderbank-McLaughlin-Merolla (2007), Liu-Liang-Poor (2007), Klinc-Ha-McLaughlin-Barros (2011), Koyluoglu-ElGamal (2011), Mahdavifar-Vardy (2011), Hof-Shamai (2010), Oggier-Sole-Belfiore (2011), Andersson (2013)

Problem Setup

Broadcast Channel with Receiver Side Information and Independent Secret Keys

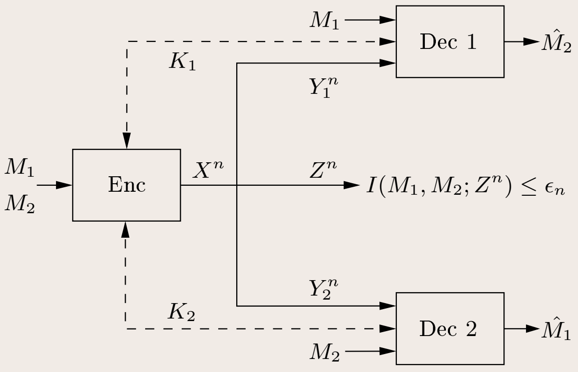
Problem Setup:

- One transmitter
- Two users
- One eavesdropper
- BC: $P_{Y_1 Y_2 Z|X}$
- Receiver side information

Secret Keys:

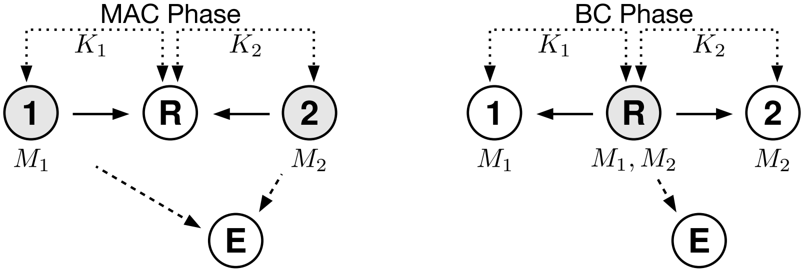
- $K_1, K_2 \in [1, 2^{nR_K}]$
- Independent keys
- $R_K \to \infty$

Channel Model



Decode-and-Forward Bidirectional Relaying

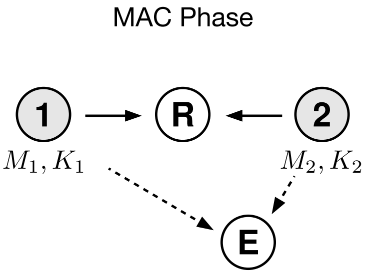
Secret Key Available Prior to Transmission

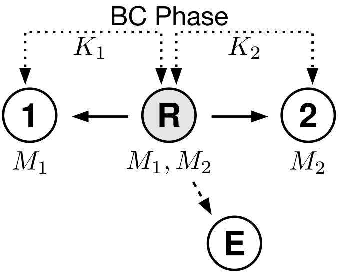


- MAC Phase: use secret keys as one-time pads – results in classical MAC with known capacity region [Ahlswede (1971), Liao (1972)]
- BC Phase: corresponds exactly to the BC with receiver side information and independent secret keys

Decode-and-Forward Bidirectional Relaying

Creating Secret Key in MAC Phase

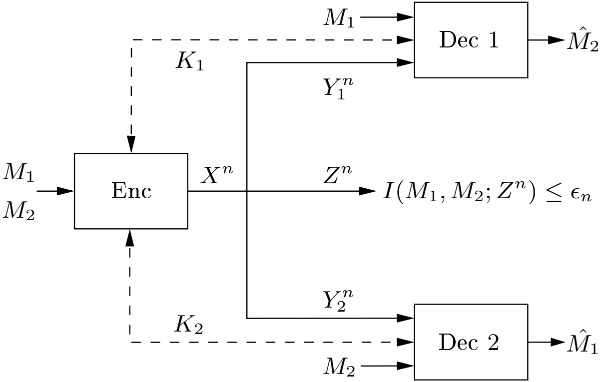




- MAC Phase: MAC wiretap channel – well understood [Liang-Poor (2008), Ekrem-Ulukus (2008), Tekin-Yener (2008), Wiese-Boche (2013), ...]
- BC Phase: corresponds exactly to the BC with receiver side information and independent secret keys

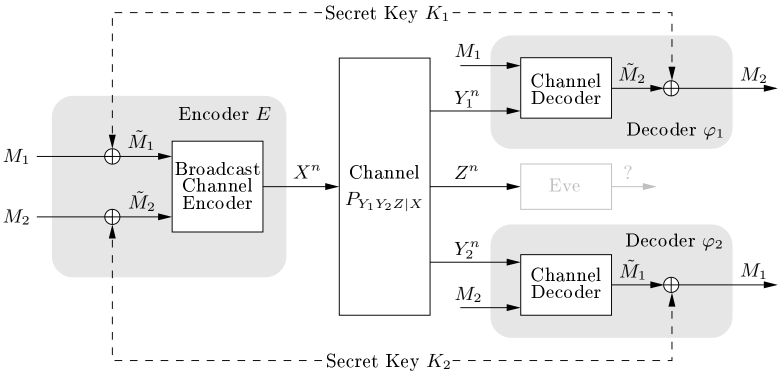
Back to our Problem

BC Phase of D&F Bidirectional Relaying



Approach 1

Secret-Keys as One Time Pad



- Two one-time pads: $\tilde{M}_i = M_i \oplus K_i, i = 1, 2$
- Broadcast channel encoder with two independent messages
- Interference between two receivers
  - ➠ Reduce to the classical BC with two independent messages

One-Time Pad Achievable Rate Region

- One-time pads immediately guarantees secrecy
  - ➠ Allows to apply classical strategies for reliability

Proposition: Superposition Coding

An *achievable secrecy rate region* is given by:

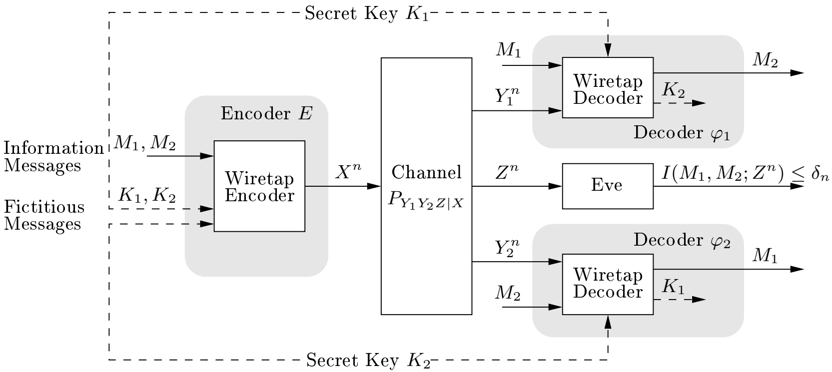
$$\begin{aligned} R_1 &\leq I(X;Y_1|U) \\ R_2 &\leq I(U;Y_2) \\ R_1 + R_2 &\leq I(X;Y_1) \end{aligned}$$

for random variables satisfying $U - X - (Y_1, Y_2)$.

- However, this approach does not exploit the noisy channel...

Approach 2

Secret-Keys as Fictitious Messages in Wiretap Code



- Wiretap code: fictitious messages (K_1, K_2) for randomization
- Receiver 1: Decode (M_2, K_2), has side-information (M_1, K_1)
- Receiver 2: Decode (M_1, K_1), has side-information (M_2, K_2)

Main Result

Degraded Eavesdropper

Theorem: Degraded Eavesdropper Channel

Suppose the BC $P_{Y_1 Y_2 Z|X}$ satisfies

$$X - Y_1 - Z$$
$$X - Y_2 - Z$$

The *secrecy capacity* is given by:

$$\begin{aligned} R_1 &\leq I(X;Y_1) \\ R_2 &\leq I(X;Y_2) \\ R_1 + R_2 &\leq I(X;Y_1) + I(X;Y_2) - I(X;Z). \end{aligned}$$

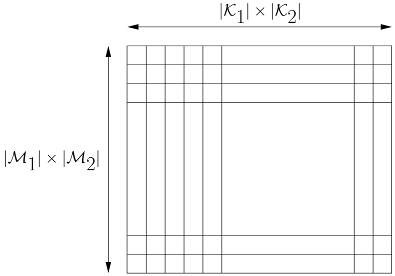
➠ The capacity is achieved using secret-keys as fictitious messages in a wiretap code (Approach 2).

Achievability

Alternative Capacity Expression

$$\bigcup_{0\leq\alpha\leq 1} \left\{ \begin{array}{l} R_1 \leq I(X;Y_1) - \alpha I(X;Z) \\ R_2 \leq I(X;Y_2) - (1-\alpha) I(X;Z) \end{array} \right\}$$

Wiretap codebook



$$|\mathcal{K}_1| > 2^{n((1-\alpha)I(X;Z)+\epsilon)}$$

$$|\mathcal{K}_2| > 2^{n(\alpha I(X;Z)+\epsilon)}$$

$$|\mathcal{M}_2| < 2^{n(I(X;Y_1)-\alpha I(X;Z)-2\epsilon)}$$

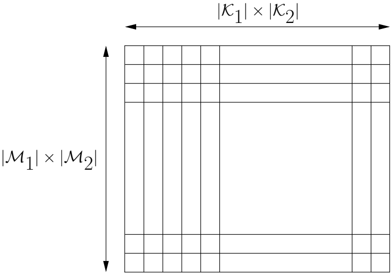
$$|\mathcal{M}_1| < 2^{n(I(X;Y_2)-(1-\alpha)I(X;Z)-2\epsilon)}$$

Achievability

Alternative Capacity Expression

$$\bigcup_{0\leq\alpha\leq 1} \left\{ \begin{array}{l} R_1 \leq I(X;Y_1) - \alpha I(X;Z) \\ R_2 \leq I(X;Y_2) - (1-\alpha) I(X;Z) \end{array} \right\}$$

Wiretap codebook



(Secrecy) : $\frac{1}{n}\log(|\mathcal{K}_1||\mathcal{K}_2|) > I(X;Z)$

(Rcv. 1) : $|\mathcal{M}_2||\mathcal{K}_2| \leq 2^{n(I(X;Y_1)-\epsilon)}$

(Rcv. 2) : $|\mathcal{M}_1||\mathcal{K}_1| \leq 2^{n(I(X;Y_2)-\epsilon)}$

Converse

$$R_1 \leq I(X;Y_1)$$
$$R_2 \leq I(X;Y_2)$$
$$R_1 + R_2 \leq I(X;Y_1) + I(X;Y_2) - I(X;Z)$$

- Key steps:

$$n(R_1 + R_2) \leq \underbrace{I(M_2;Y_1^n|M_1,K_1)}_{\text{Fano}} + \underbrace{I(M_1;Y_2^n|M_2,K_2)}_{\text{Fano}} - \underbrace{I(M_1,M_2;Z^n)}_{\text{Secrecy}}$$

Converse

$$R_1 \leq I(X;Y_1)$$
$$R_2 \leq I(X;Y_2)$$
$$R_1 + R_2 \leq I(X;Y_1) + I(X;Y_2) - I(X;Z)$$

- Key steps:

$$n(R_1+R_2) \leq \underbrace{I(M_2;Y_1^n|M_1,K_1)}_{\text{Fano}} + \underbrace{I(M_1;Y_2^n|M_2,K_2)}_{\text{Fano}} - \underbrace{I(M_1,M_2;Z^n)}_{\text{Secrecy}}$$
$$\leq I(M_{12},K_1;Y_1^n) + I(M_{12},K_2;Y_2^n) - I(M_{12};Z^n)$$

Converse

$$R_1 \leq I(X;Y_1)$$
$$R_2 \leq I(X;Y_2)$$
$$R_1 + R_2 \leq I(X;Y_1) + I(X;Y_2) - I(X;Z)$$

- Key steps:

$$n(R_1+R_2) \leq \underbrace{I(M_2;Y_1^n|M_1,K_1)}_{\text{Fano}} + \underbrace{I(M_1;Y_2^n|M_2,K_2)}_{\text{Fano}} - \underbrace{I(M_1,M_2;Z^n)}_{\text{Secrecy}}$$
$$\leq I(M_{12},K_1;Y_1^n) + I(M_{12},K_2;Y_2^n) - I(M_{12};Z^n)$$
$$\leq I(M_{12},K_1,K_2;Y_1^n) + I(M_{12},K_1,K_2;Y_2^n) - I(M_{12},K_1,K_2;Z^n)$$

Converse

$$R_1 \leq I(X;Y_1)$$
$$R_2 \leq I(X;Y_2)$$
$$R_1 + R_2 \leq I(X;Y_1) + I(X;Y_2) - I(X;Z)$$

- Key steps:

$$n(R_1+R_2) \leq \underbrace{I(M_2;Y_1^n|M_1,K_1)}_{\text{Fano}} + \underbrace{I(M_1;Y_2^n|M_2,K_2)}_{\text{Fano}} - \underbrace{I(M_1,M_2;Z^n)}_{\text{Secrecy}}$$
$$\leq I(M_{12},K_1;Y_1^n) + I(M_{12},K_2;Y_2^n) - I(M_{12};Z^n)$$
$$\leq I(M_{12},K_1,K_2;Y_1^n) + I(M_{12},K_1,K_2;Y_2^n) - I(M_{12},K_1,K_2;Z^n)$$
$$\leq I(M_{12},K_1,K_2;Y_1^n|Z^n) + I(M_{12},K_1,K_2;Y_2^n)$$

Converse

$$R_1 \leq I(X;Y_1)$$
$$R_2 \leq I(X;Y_2)$$
$$R_1 + R_2 \leq I(X;Y_1) + I(X;Y_2) - I(X;Z)$$

- Key steps:

$$n(R_1+R_2) \leq \underbrace{I(M_2;Y_1^n|M_1,K_1)}_{\text{Fano}} + \underbrace{I(M_1;Y_2^n|M_2,K_2)}_{\text{Fano}} - \underbrace{I(M_1,M_2;Z^n)}_{\text{Secrecy}}$$
$$\leq I(M_{12},K_1;Y_1^n) + I(M_{12},K_2;Y_2^n) - I(M_{12};Z^n)$$
$$\leq I(M_{12},K_1,K_2;Y_1^n) + I(M_{12},K_1,K_2;Y_2^n) - I(M_{12},K_1,K_2;Z^n)$$
$$\leq I(M_{12},K_1,K_2;Y_1^n|Z^n) + I(M_{12},K_1,K_2;Y_2^n)$$
$$\leq I(X^n;Y_1^n|Z^n) + I(X^n;Y_2^n)$$

Converse

$$R_1 \leq I(X;Y_1)$$
$$R_2 \leq I(X;Y_2)$$
$$R_1 + R_2 \leq I(X;Y_1) + I(X;Y_2) - I(X;Z)$$

- Key steps:

$$n(R_1+R_2) \leq \underbrace{I(M_2;Y_1^n|M_1,K_1)}_{\text{Fano}} + \underbrace{I(M_1;Y_2^n|M_2,K_2)}_{\text{Fano}} - \underbrace{I(M_1,M_2;Z^n)}_{\text{Secrecy}}$$
$$\leq I(M_{12},K_1;Y_1^n) + I(M_{12},K_2;Y_2^n) - I(M_{12};Z^n)$$
$$\leq I(M_{12},K_1,K_2;Y_1^n) + I(M_{12},K_1,K_2;Y_2^n) - I(M_{12},K_1,K_2;Z^n)$$
$$\leq I(M_{12},K_1,K_2;Y_1^n|Z^n) + I(M_{12},K_1,K_2;Y_2^n)$$
$$\leq I(X^n;Y_1^n|Z^n) + I(X^n;Y_2^n)$$
$$\leq nI(X;Y_1) + nI(X;Y_2) - nI(X;Z)$$

Conclusions

Secure transmission to two users using independent secret keys

- Approach 1: Secret keys as one-time pads, independent messages
- Approach 2: Secret keys as fictitious messages in the wiretap code
- Degraded eavesdropper channel: Approach 2 is optimal
- Reversely degraded channel: Approach 2 does not work anymore. Approach 1 establishes secure communication

Thank you for your attention!

Conclusions

Secure transmission to two users using independent secret keys

- Approach 1: Secret keys as one-time pads, independent messages
- Approach 2: Secret keys as fictitious messages in the wiretap code
- Degraded eavesdropper channel: Approach 2 is optimal
- Reversely degraded channel: Approach 2 does not work anymore. Approach 1 establishes secure communication

Thank you for your attention!