Wiretap Channels with Side Information

Rafael Wyrembelski

joint work with Holger Boche

Technische Universität München

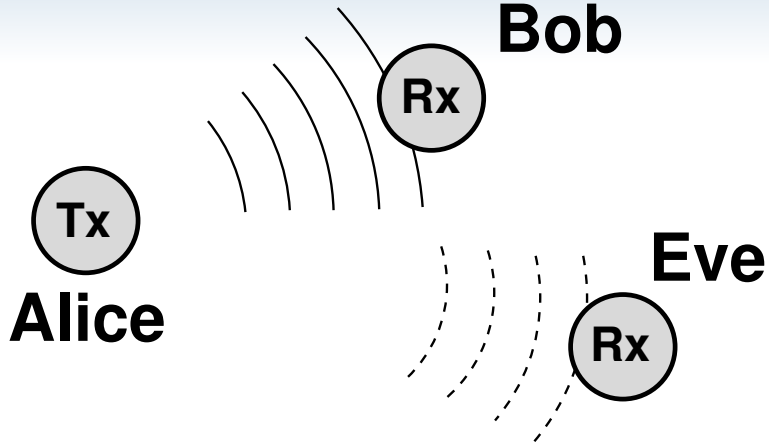
Lehrstuhl für Theoretische Informationstechnik

University of Toronto

May 2, 2013

Motivation

- Signal is received by legitimate users but also eavesdropped by **non-legitimate users**



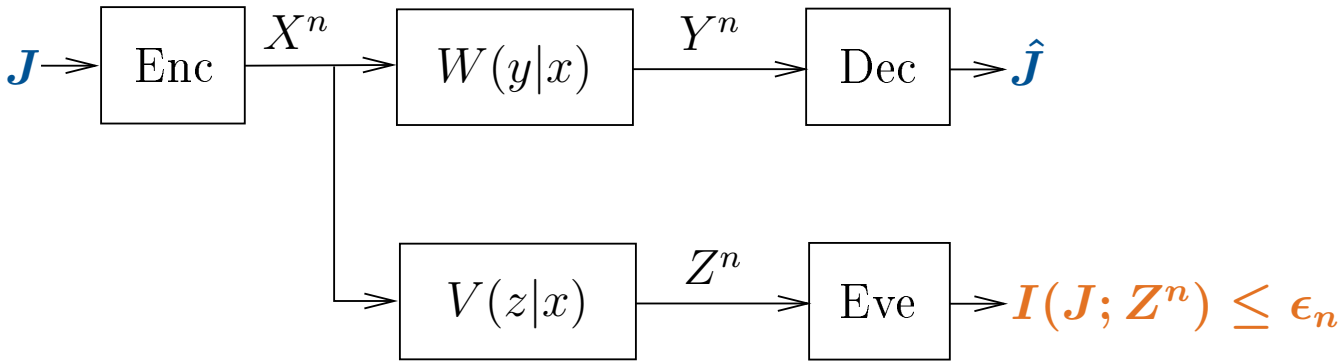
➠ Need of secure communication systems

- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers

  ➠ **Use of information theoretic secrecy concepts**

- Eve may have **side information about the transmitted message** available due to
  - prior transmissions, certain network structure, helping wiretappers, ...

Wiretap Channel



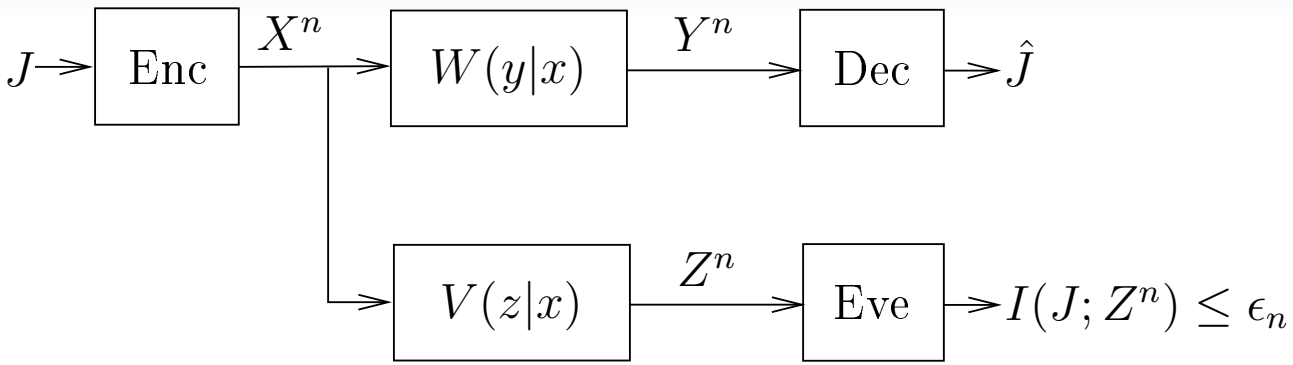
- **Goal:** Transmit message $J \in \mathcal{J}_n$ **reliably** to the legitimate receiver while keeping the wiretapper Eve **ignorant** of it

- **Strong secrecy** requirement on J, i.e.,

$$I(J;Z^n) \leq \epsilon_n$$

➠ Total amount of information leaked to Eve has to be small

Secrecy Capacity



Theorem 1: Secrecy Capacity [Wyner '75, Csiszár/Körner '78]

The *secrecy capacity* C_S of the wiretap channel is

$$C_S = \max_{U-X-(Y,Z)} \big(I(U;Y) - I(U;Z)\big)$$

for random variables $U - X - (Y, Z)$ forming a Markov chain.

A. D. Wyner, ''The Wire-Tap Channel,'' *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975

I. Csiszár and J. Körner, ''Broadcast Channels with Confidential Messages,'' *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978

Implications of Strong Secrecy

Theorem 2: Decoding Error [Bjelaković/Boche/Sommerfeld '13]

If $I(J;Z^n) \leq \epsilon_n$, then the average probability $\bar{e}_{n,Eve}$ (and therewith also the maximum probability) of decoding error at Eve satisfies

$$\bar{e}_{n,Eve} \geq 1 - c\sqrt{\epsilon_n}$$

for some constant $c > 0$.

- Decoding error approaches

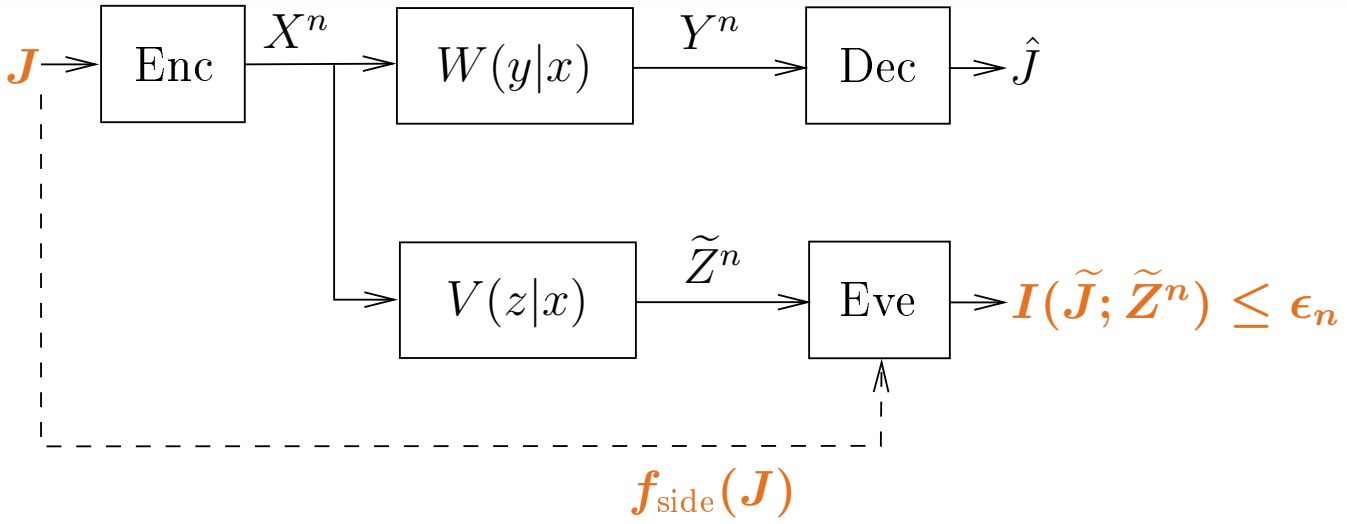
  $$\bar{e}_{n,Eve} \to 1 \quad \text{(exponentially fast)}$$

  since $I(J;Z^n) \leq \epsilon_n = 2^{-n\beta}$, $\beta > 0$
- Important signal processing interpretation:

  ➠ Regardless of the **post-processing** at Eve, it always results in the **worst** behavior of decoding performance!

I. Bjelaković, H. Boche, and J. Sommerfeld, ''Secrecy Results for Compound Wiretap Channels,'' *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013

Wiretap Channel with Side Information



- Eve has side information $f_{\text{side}}(J)$ about the message J
  - ➠ Eve can restrict the message to a certain subset $\widetilde{\mathcal{J}} \subseteq \mathcal{J}_n$

➠ Strong secrecy requirement becomes

$$I(\widetilde{J};\widetilde{Z}^n) \leq \epsilon_n \qquad \text{for all } \widetilde{\mathcal{J}} \subseteq \mathcal{J}_n \text{ with } |\widetilde{\mathcal{J}}| \geq 2$$

How does the side information at the wiretapper influence the

➠ **secrecy capacity?**

➠ **decoding performance of Eve?**

Vanishing Output Variation

- To answer these questions we need the following concept:

Definition 1: Vanishing Output Variation

A code for the wiretap channel (with side information) with stochastic encoder $E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n)$ has exponentially fast *vanishing output variation at the wiretapper* if there is a measure ϑ on $\mathcal{Z}^n$ and some $\beta > 0$ such that for all $j \in \mathcal{J}_n$ and

$$\overline{V}^n(z^n|j) = \sum_{x^n \in \mathcal{X}^n} V^n(z^n|x^n) E(x^n|j)$$

it holds

$$\left\| \overline{V}^n(\cdot|j) - \vartheta \right\| \leq 2^{-n\beta}.$$

Implications of Vanishing Output Variation

Proposition 1: Implications [Boche/Wyrembelski '13]

If $\|\overline{V}^n(\cdot|j) - \vartheta\| \leq 2^{-n\beta}$ for all $j \in \mathcal{J}_n$, then

- the strong secrecy criterion satisfies

$$I(\widetilde{J}; \widetilde{Z}^n) \leq \epsilon_n$$

- the average probability $\bar{e}_{n,Eve}$ of decoding error at Eve satisfies

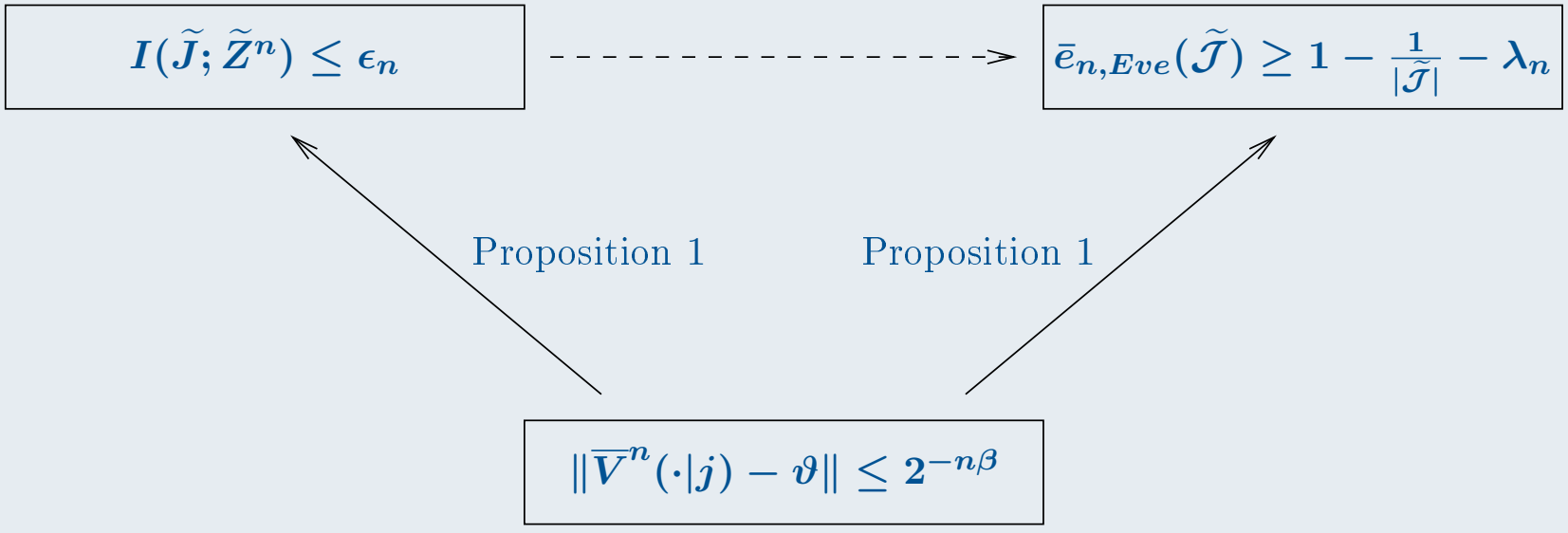
$$\bar{e}_{n,Eve} \geq 1 - \frac{1}{|\widetilde{\mathcal{J}}|} - \lambda_n$$

with $\epsilon_n, \lambda_n \to 0$ as $n \to \infty$ exponentially fast.

- Eavesdropped signal is **useless** (Eve does not learn anything new)
  - Eve can choose one message at random based on her side information (with success probability $1/|\widetilde{\mathcal{J}}|$)
- Again worst behavior of decoding performance at Eve!

Optimal Pre-processing

If the code has vanishing output variation according to Definition 1, then



- Vanishing output variation is **sufficient** for strong secrecy and maximum uncertainty.

H. Boche and R. F. Wyrembelski, ‘‘Optimal Transceiver Design for Wiretap Channels with Side Information,’’ in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, Vancouver, Canada, May 2013

Secrecy Capacity

Theorem 3: Secrecy Capacity [Boche/Wyrembelski '13]

The *strong secrecy capacity* $C_{S,side}^{strong}$ of the wiretap channel with side information is

$$C_{S,side}^{strong} = C_S,$$

➠ Side information at Eve does not decrease secrecy capacity!

Key ideas for proof:

- Converse $C_{S,side}^{strong} \leq C_S$ follows immediately, since side information cannot increase capacity.
- Achievability follows from [Bjelaković/Boche/Sommerfeld '13] which provides a wiretap code achieving C_S with vanishing output variation. Proposition 1 ensures that $I(\widetilde{J};\widetilde{Z}^n) \leq \epsilon_n$ is satisfied.

I. Bjelaković, H. Boche, and J. Sommerfeld, ''Secrecy Results for Compound Wiretap Channels,'' *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013

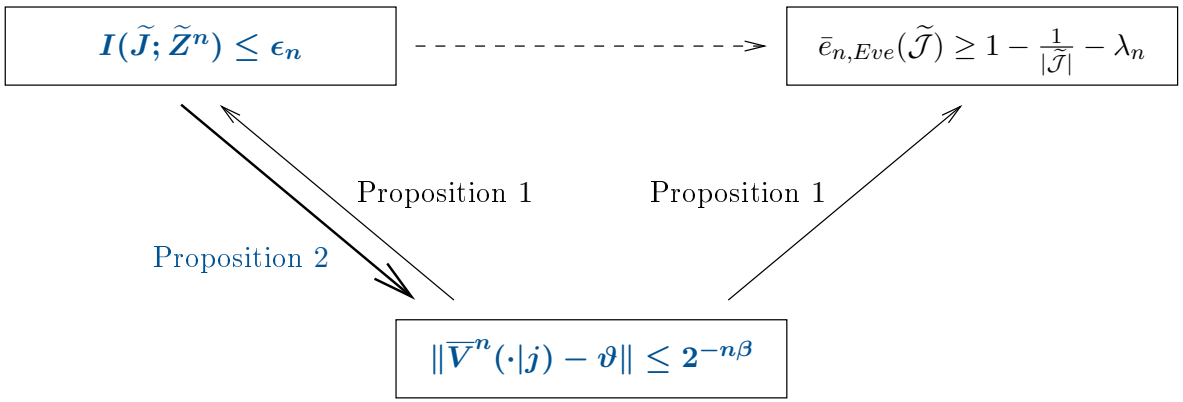
H. Boche and R. F. Wyrembelski, ''On the Strong Secrecy Capacity of Wiretap Channels with Side Information,'' in *Proc. IEEE Int. Conf. Commun.*, Budapest, Hungary, Jun. 2013

Optimal Pre-processing

Proposition 2: Optimal Pre-processing [Boche/Wyrembelski '13]

For wiretap codes achieving the strong secrecy capacity $C_{S,side}^{strong}$, there exists a measure ϑ on $\mathcal{Z}^n$ and some $\beta > 0$ such that for all $j \in \mathcal{J}_n$ it holds $\|\overline{V}^n(\cdot|j) - \vartheta\| \leq 2^{-n\beta}$. This means, **the optimal code has the vanishing output variation property**.

- Vanishing output variation is also **necessary** for strong secrecy.



Maximum Uncertainty

- For $C_{S,Side}^{strong}$ under the strong secrecy criterion $I(\widetilde{J};\widetilde{Z}^n) \leq \epsilon_n$ for all $\widetilde{\mathcal{J}} \subseteq \mathcal{J}_n$ with $|\widetilde{\mathcal{J}}| \geq 2$, we have maximum uncertainty at Eve, i.e.,

$$\bar{e}_{n,Eve} \geq 1 - \frac{1}{|\widetilde{\mathcal{J}}|} - \lambda_n$$

➠ Desirable, since it is the worst behavior we can hope for

Why do we require strong secrecy and not maximum uncertainty?

What changes if we directly **require maximum uncertainty**?

Secrecy Capacity

- Instead of requiring strong secrecy, we directly require maximum uncertainty at Eve!

Theorem 4: Secrecy Capacity [Boche/Wyrembelski '13]

The *secrecy capacity with maximum uncertainty* $C_{S,side}^{uncert}$ of the wiretap channel with side information is

$$C_{S,side}^{uncert} = C_S.$$

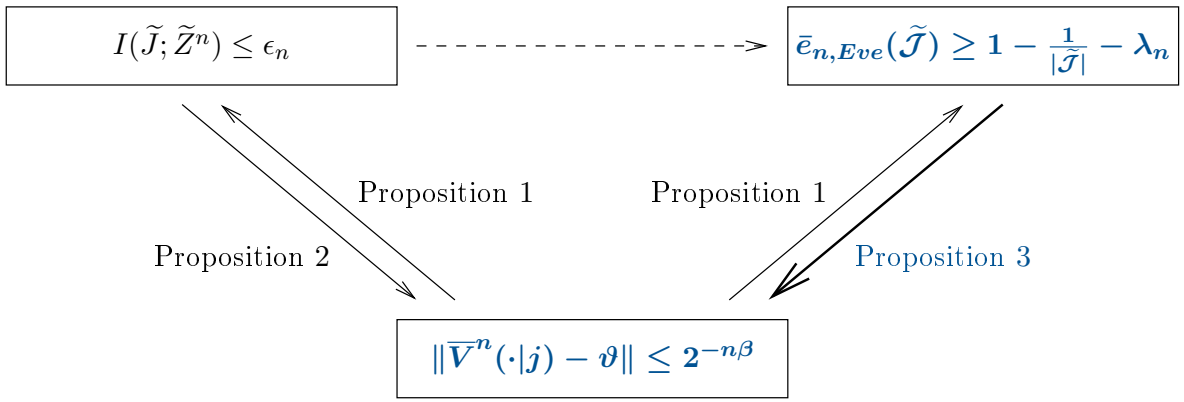
➠ Maximum uncertainty yields the same secrecy capacity as strong secrecy, i.e., $C_{S,side}^{uncert} = C_{S,side}^{strong} = C_S$!

Optimal Pre-processing

Proposition 3: Optimal Pre-processing Boche/Wyrembelski '13

For wiretap codes achieving the secrecy capacity with maximum uncertainty $C_{S,side}^{uncert}$, there exists a measure ϑ on $\mathcal{Z}^n$ and some $\beta > 0$ such that for all $j \in \mathcal{J}_n$ it holds $\|\overline{V}^n(\cdot|j) - \vartheta\| \leq 2^{-n\beta}$. This means, **the optimal code has the vanishing output variation property**.

- Vanishing output variation is also **necessary** for maximum uncertainty.



Concluding Remarks

- Classical wiretap channel
  - Information theoretic criterion of strong secrecy
  - ➠ Implies that decoding error at Eve goes to 1!

- Wiretap channel with **side information**
  - Information theoretic criterion of strong secrecy
  - Signal processing inspired criterion of maximum uncertainty
  - ➠ No loss in secrecy capacity due to side information
  - ➠ Equivalence of strong secrecy and maximum uncertainty in terms of secrecy capacity

Thank you for your attention!

Concluding Remarks

- Classical wiretap channel
  - Information theoretic criterion of strong secrecy
  - ➠ Implies that decoding error at Eve goes to 1!

- Wiretap channel with **side information**
  - Information theoretic criterion of strong secrecy
  - Signal processing inspired criterion of maximum uncertainty
  - ➠ No loss in secrecy capacity due to side information
  - ➠ Equivalence of strong secrecy and maximum uncertainty in terms of secrecy capacity

Thank you for your attention!

Concluding Remarks

- Classical wiretap channel
  - Information theoretic criterion of strong secrecy
  - ➠ Implies that decoding error at Eve goes to 1!

- Wiretap channel with **side information**
  - Information theoretic criterion of strong secrecy
  - Signal processing inspired criterion of maximum uncertainty
  - ➠ No loss in secrecy capacity due to side information
  - ➠ Equivalence of strong secrecy and maximum uncertainty in terms of secrecy capacity

Thank you for your attention!

References I

- A. D. Wyner, ‘‘The Wire-Tap Channel,’’ *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
- I. Csiszár and J. Körner, ‘‘Broadcast Channels with Confidential Messages,’’ *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- I. Bjelaković, H. Boche, and J. Sommerfeld, ‘‘Secrecy Results for Compound Wiretap Channels,’’ *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.
- H. Boche and R. F. Wyrembelski, ‘‘Optimal Transceiver Design for Wiretap Channels with Side Information,’’ in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, Vancouver, Canada, May 2013.
- H. Boche and R. F. Wyrembelski, ‘‘On the Strong Secrecy Capacity of Wiretap Channels with Side Information,’’ in *Proc. IEEE Int. Conf. Commun.*, Budapest, Hungary, Jun. 2013.