ISWCS - Aachen
9 November 2011

Physical Layer Security in Wireless Networks

Vince Poor
(poor@princeton.edu)

Outline

1. Motivation & Background
2. Physical Layer Security in Basic Network Models
   - A Paradigm: The Broadcast Channel with Confidential Messages
   - Other Channels (Briefly)
3. Other Results & Open Issues
4. A Related Problem: Privacy (Briefly)

Motivation & Background

Exploiting the Wireless Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - *Multiple-Antenna Systems (MIMO)*
  - *Cooperation & Relaying*
  - *Cognitive Radio*

Exploiting the Wireless Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - *Multiple-Antenna Systems (MIMO)*
  - *Cooperation & Relaying*
  - *Cognitive Radio*
- What About Security?

Exploiting the Wireless Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - *Multiple-Antenna Systems (MIMO)*
  - *Cooperation & Relaying*
  - *Cognitive Radio*
- What About Security?
  - *Traditionally a higher-network-layer issue*

Exploiting the Wireless Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - *Multiple-Antenna Systems (MIMO)*
  - *Cooperation & Relaying*
  - *Cognitive Radio*
- What About Security?
  - *Traditionally a higher-network-layer issue*
  - *Encryption can be complex and difficult without infrastructure (e.g, in ad-hoc networks)*

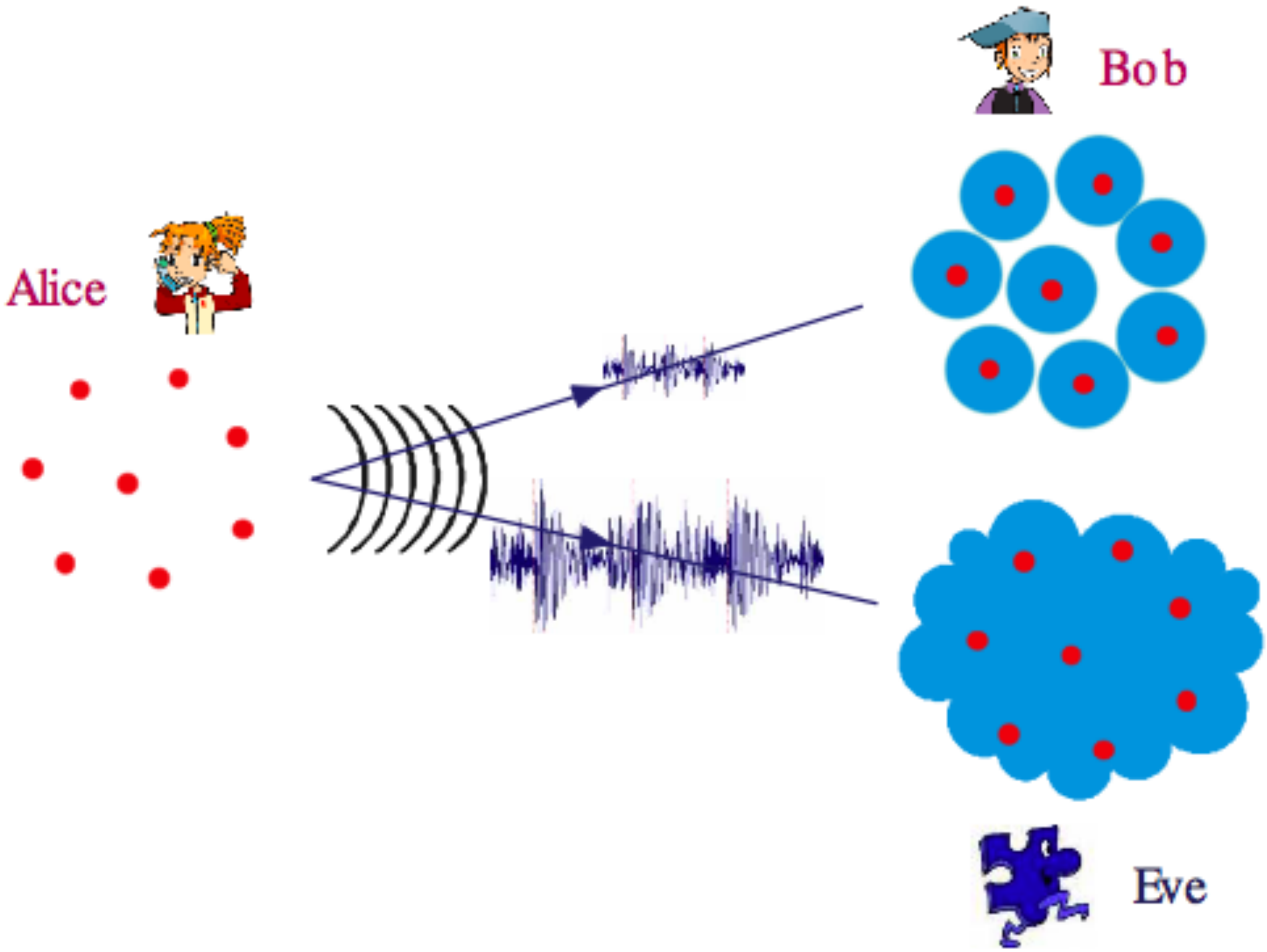
Exploiting the Wireless Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - *Multiple-Antenna Systems (MIMO)*
  - *Cooperation & Relaying*
  - *Cognitive Radio*
- What About Security?
  - *Traditionally a higher-network-layer issue*
  - *Encryption can be complex and difficult without infrastructure (e.g, in ad-hoc networks)*
  - *Information theoretic security characterizes the fundamental ability of the physical layer to provide security (confidentiality)*

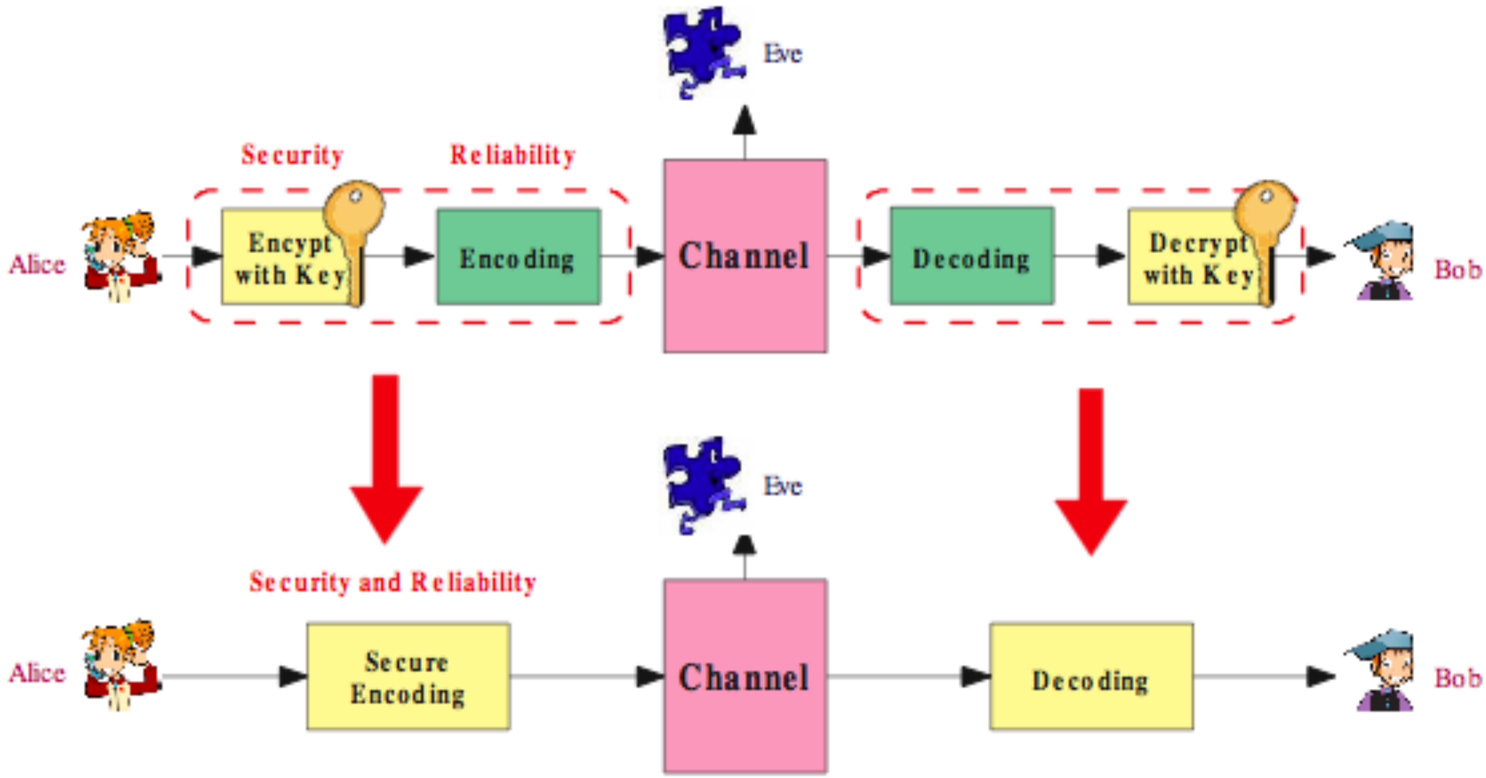
Exploiting the Wireless Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - *Multiple-Antenna Systems (MIMO)*
  - *Cooperation & Relaying*
  - *Cognitive Radio*
- What About Security?
  - *Traditionally a higher-network-layer issue*
  - *Encryption can be complex and difficult without infrastructure (e.g, in ad-hoc networks)*
  - *Information theoretic security characterizes the fundamental ability of the physical layer to provide security (confidentiality)*
  - *Caveat: This is still largely a theoretical issue*

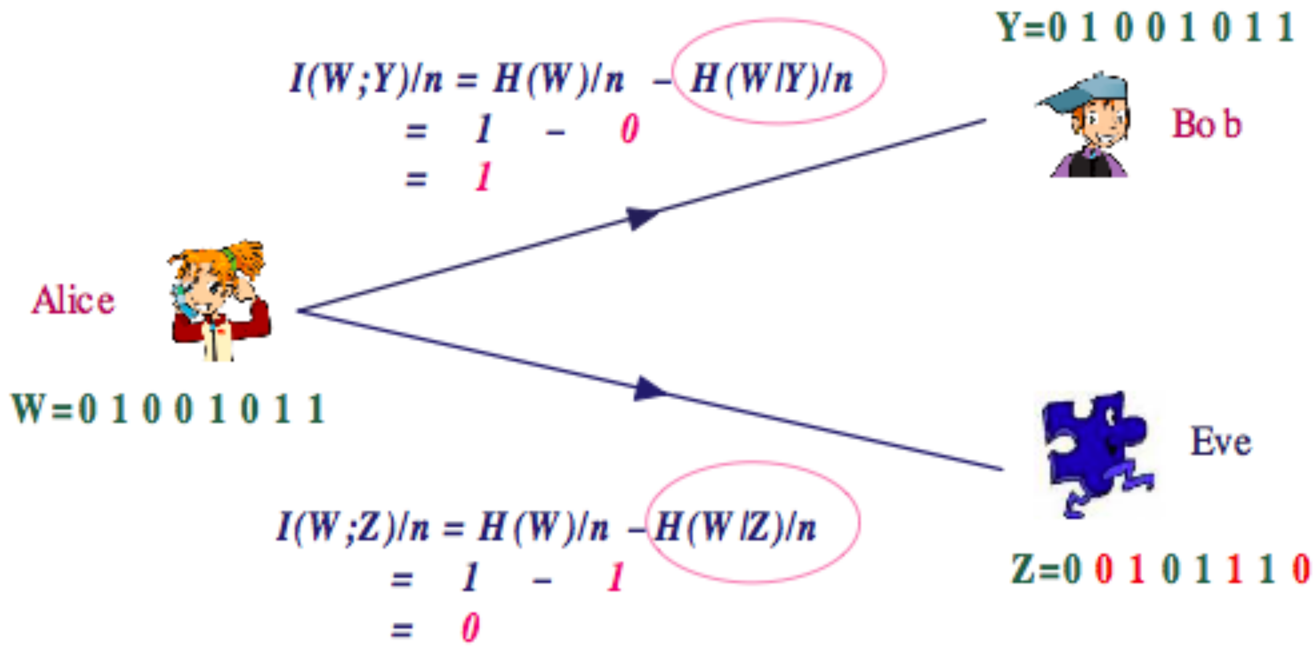
Physical Layer Security
Plausibility



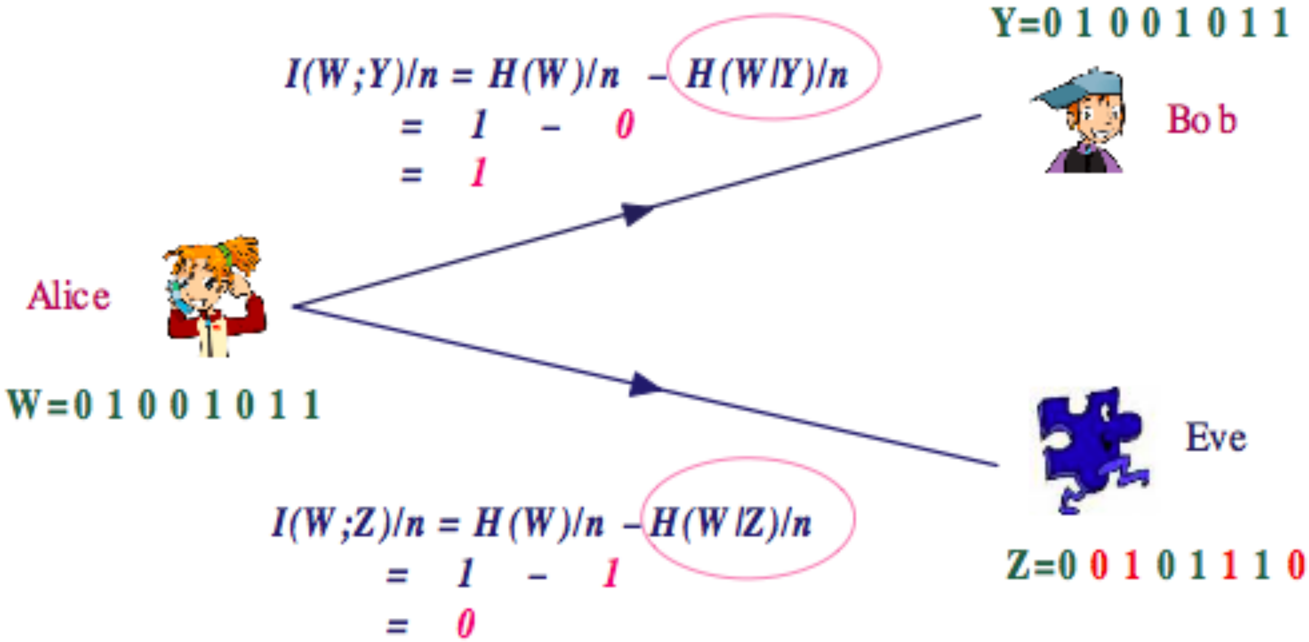
Physical Layer Security
Joint Security-Reliability Coding



Quantifying Security: Equivocation



Quantifying Security: Equivocation



Of interest:

- capacity-equivocation regions
- secrecy capacity regions (rate = equivocation)

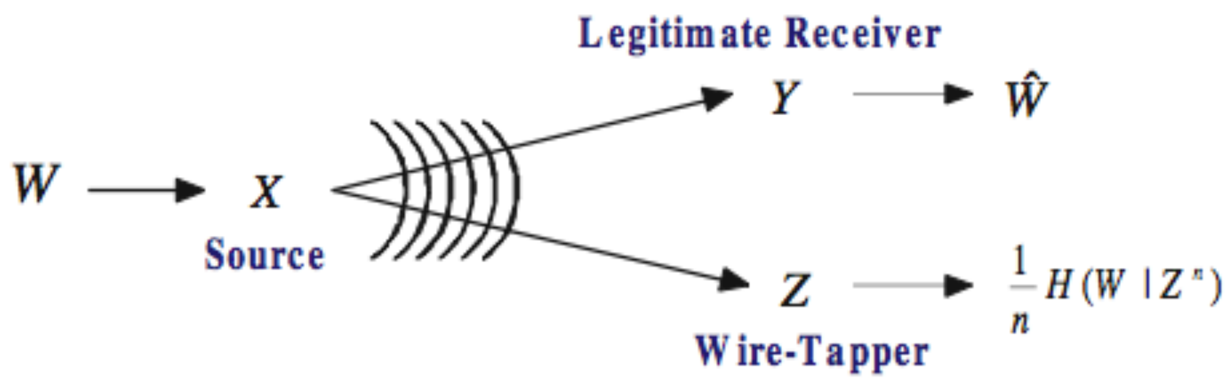
A (Very) Brief History

- Shannon [BSTJ'49]: For cipher, need *$H(K) > H(S)$.*

A (Very) Brief History

- Shannon [BSTJ'49]: For cipher, need $H(K) > H(S)$.

- Wyner [BSTJ'75]: For the wire-tap channel

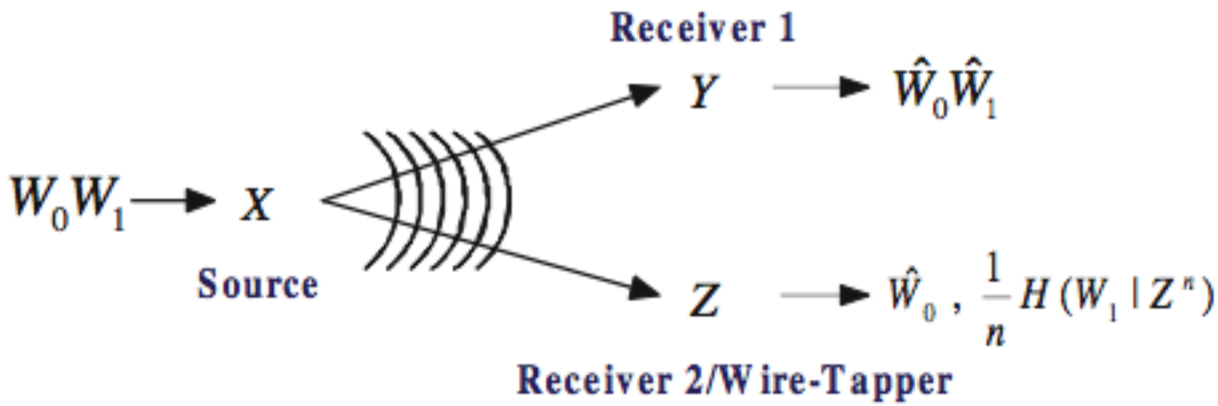


the wire-tapper must be degraded.

Physical Layer Security in Basic Network Models

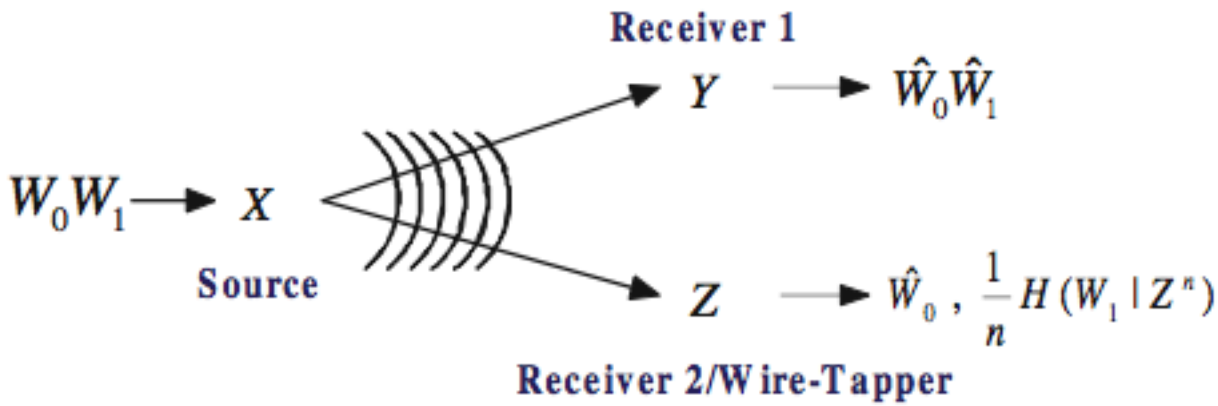
A Paradigm: The Broadcast Channel with Confidential Messages

Broadcast Channel with Confidential (BCC) Messages



Csiszár & Körner [IT'78]: Discrete Memoryless BCC

Broadcast Channel with Confidential (BCC) Messages

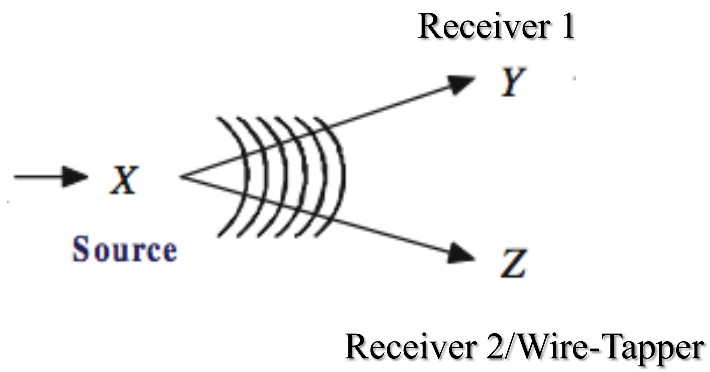


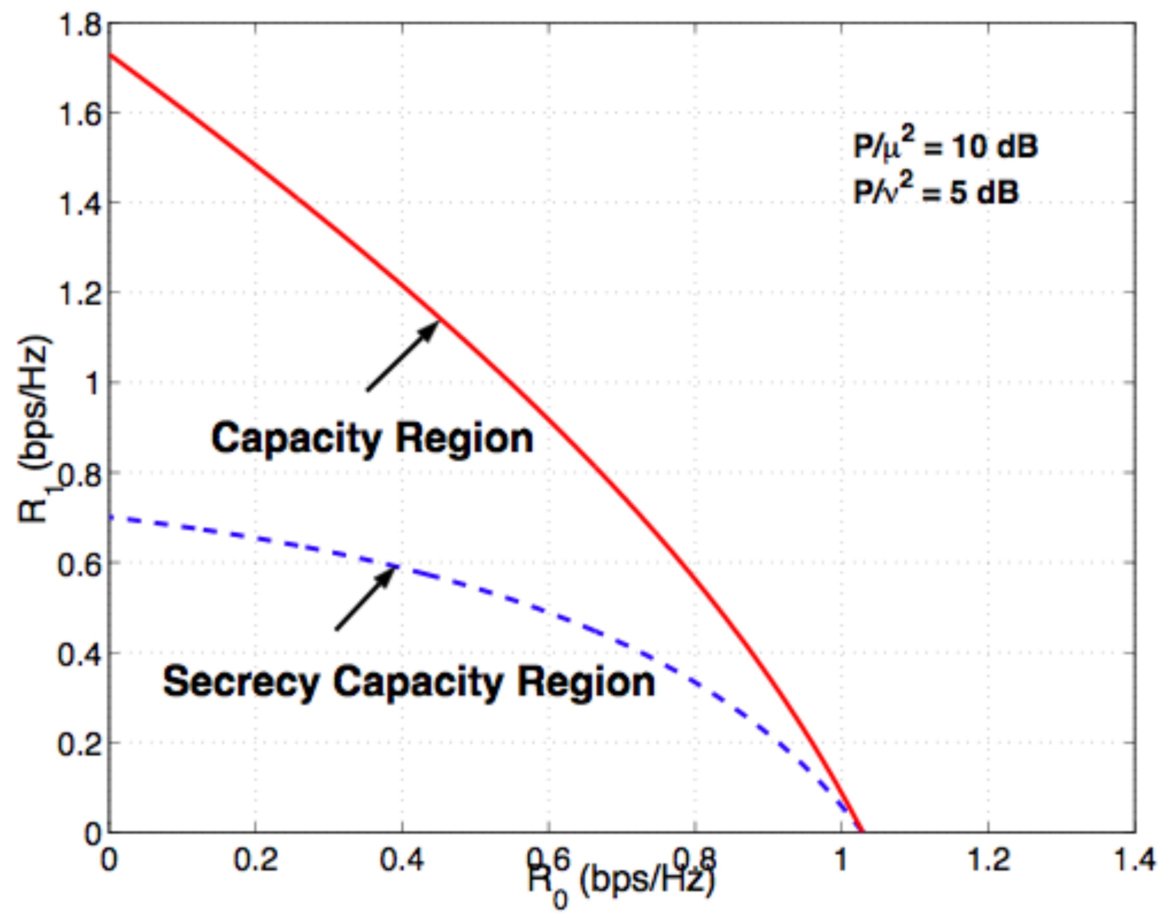
Csiszár & Körner [IT'78]: Discrete Memoryless BCC

Liang, Poor & Shamai [IT'08]:

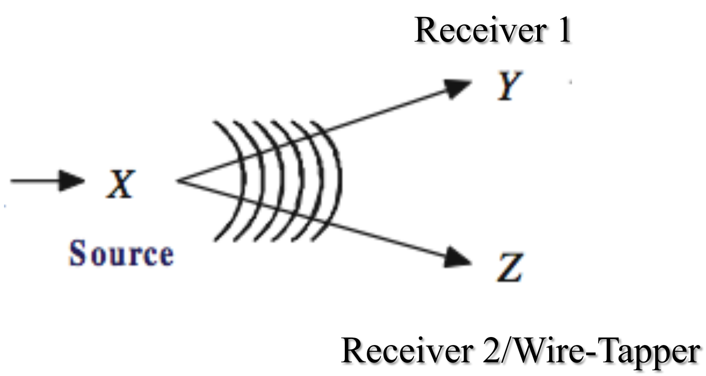
- Gaussian BCC
  - secrecy-capacity region
- Fading BCC
  - secrecy-capacity region
  - exploit fading to achieve secrecy

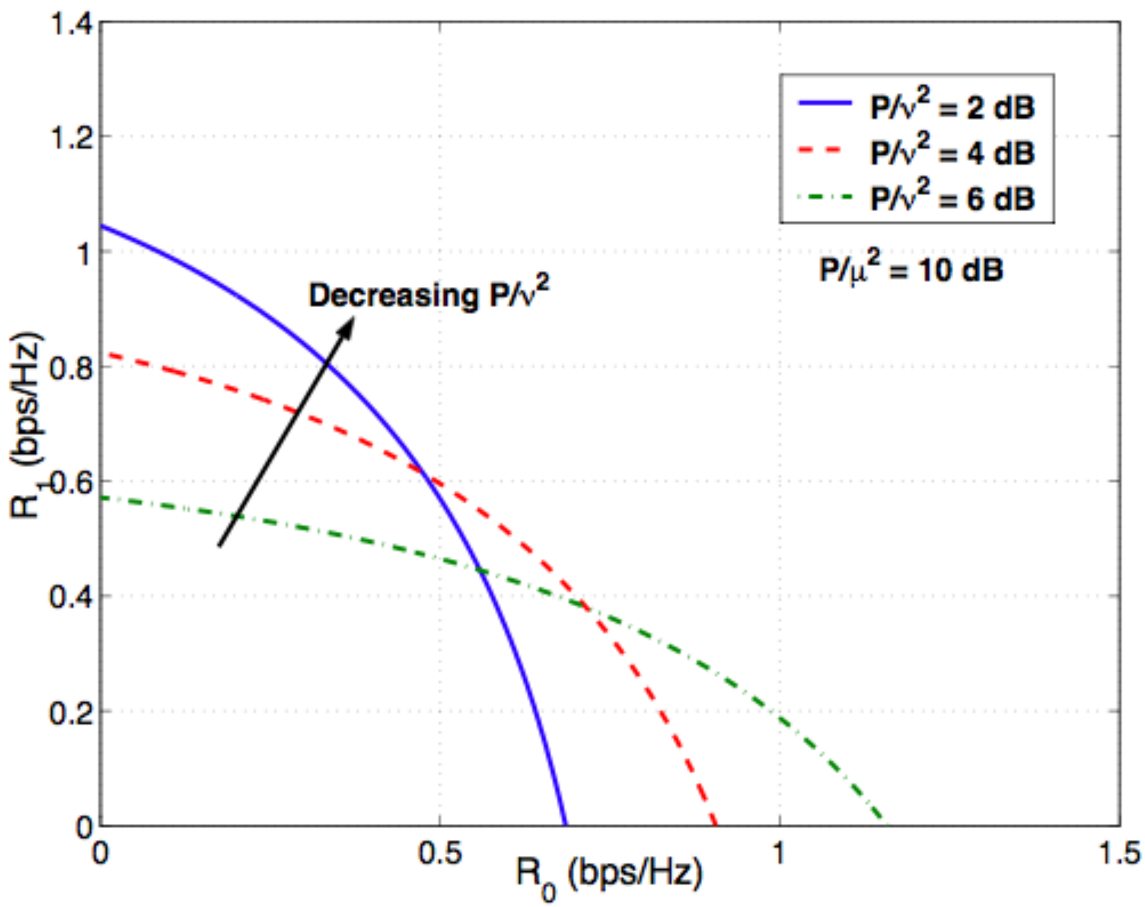
Gaussian BCC



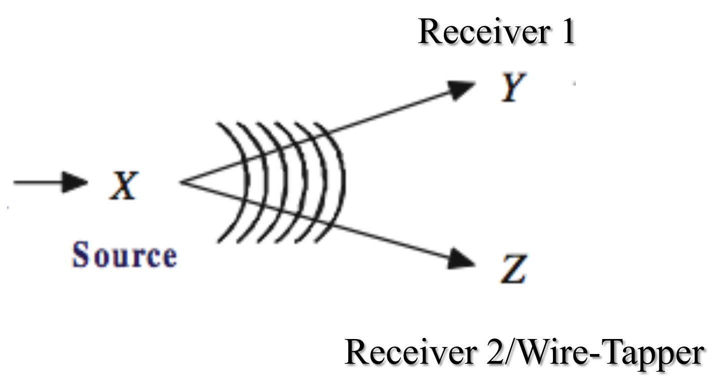


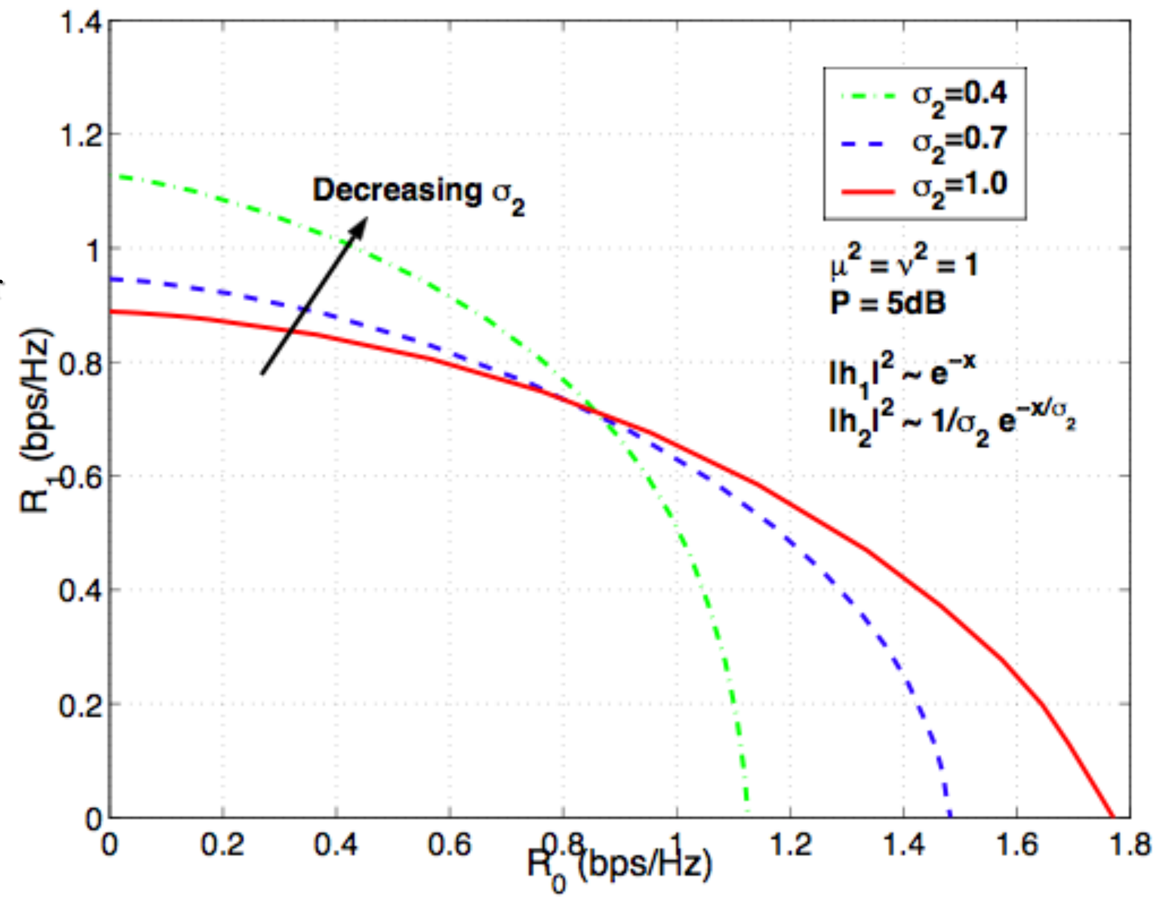
Gaussian BCC: Secrecy Capacity Regions



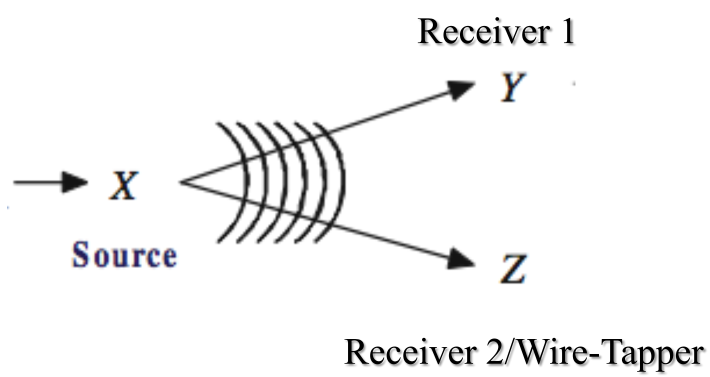


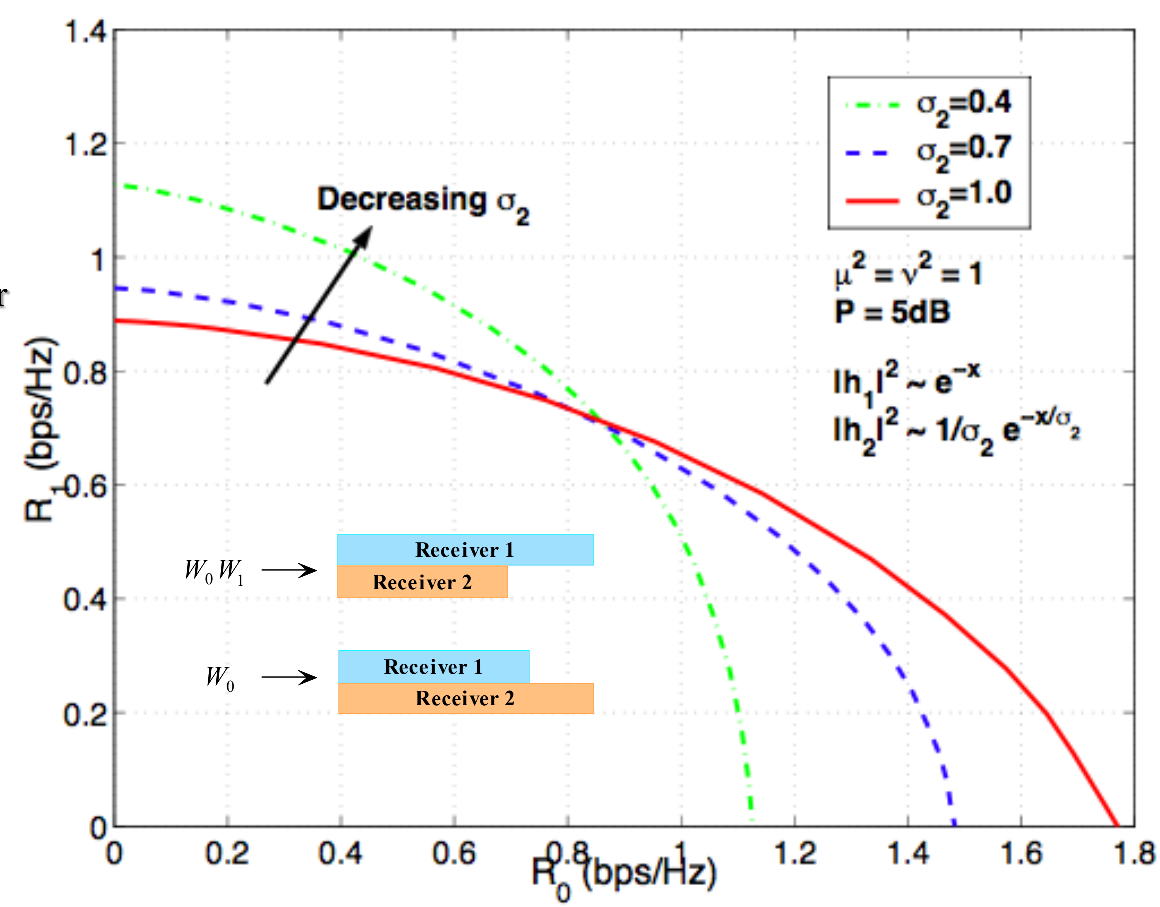
Fading BCC: Secrecy Capacity Regions





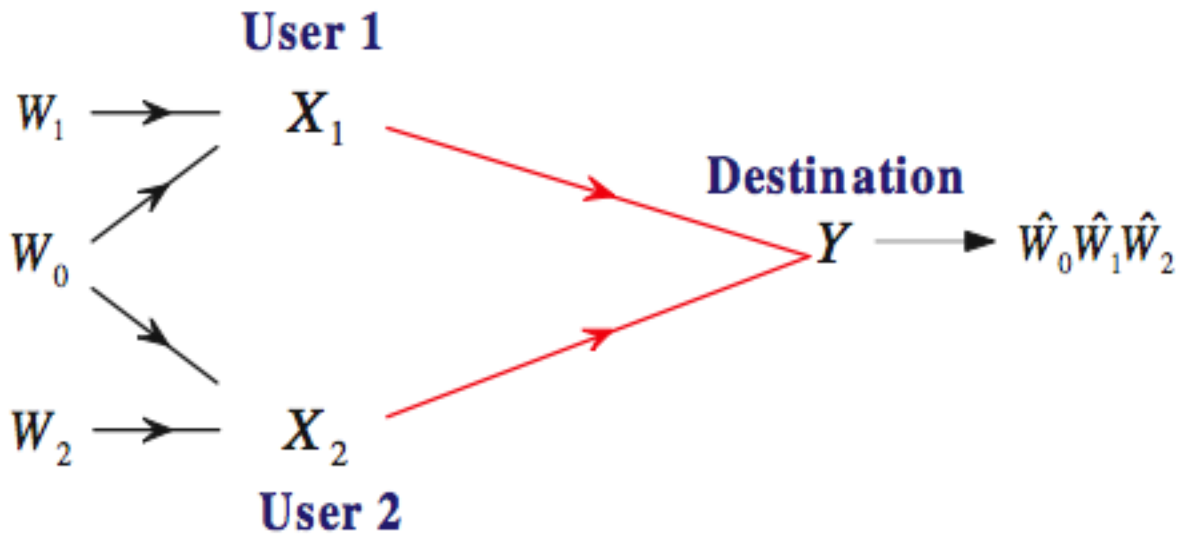
Fading BCC: Secrecy Capacity Regions





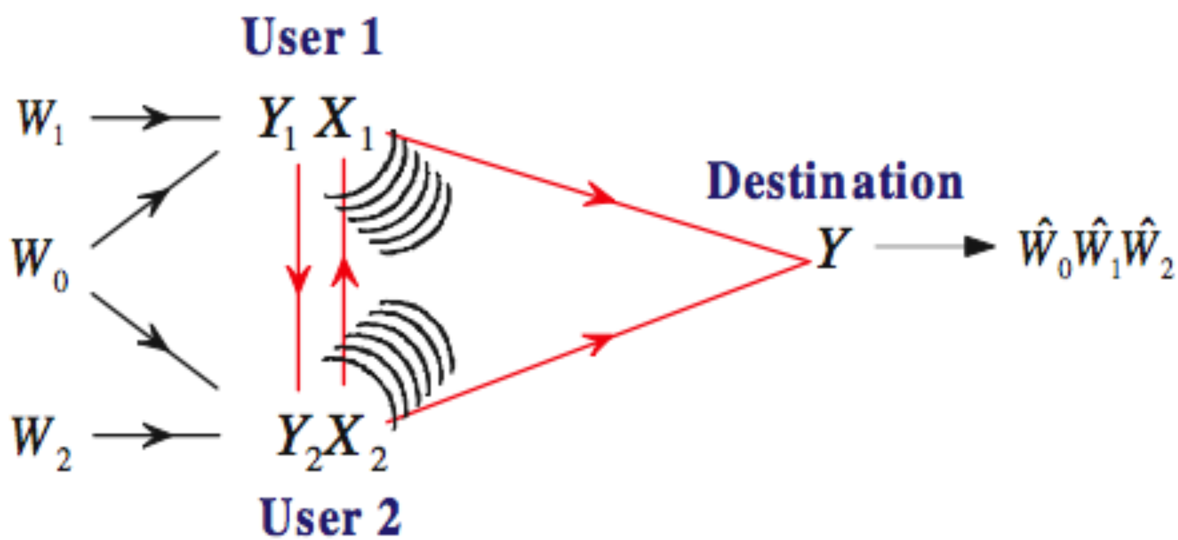
Other Channels of Interest

Multiple-Access Channel



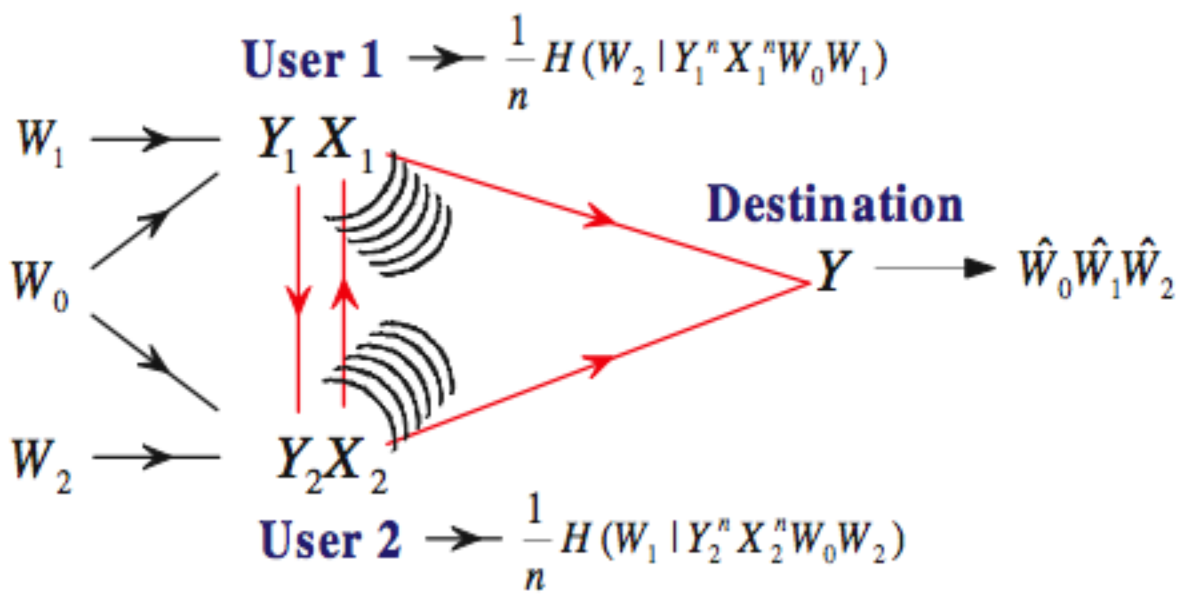
Multiple-Access Channel with Confidential Messages

Liang & Poor - IT'08 (AWGN) & Liu, Liang & Poor – IT'11 (fading)]

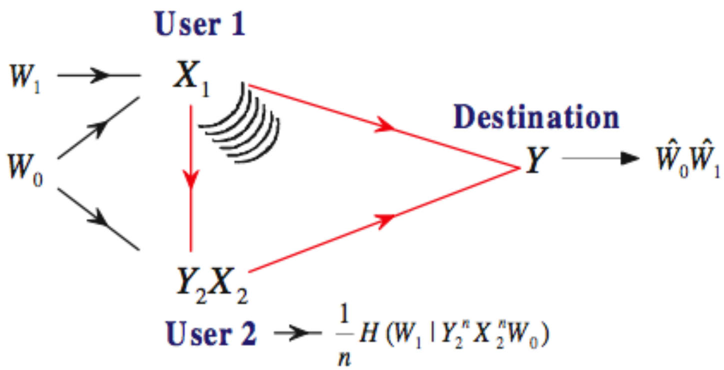


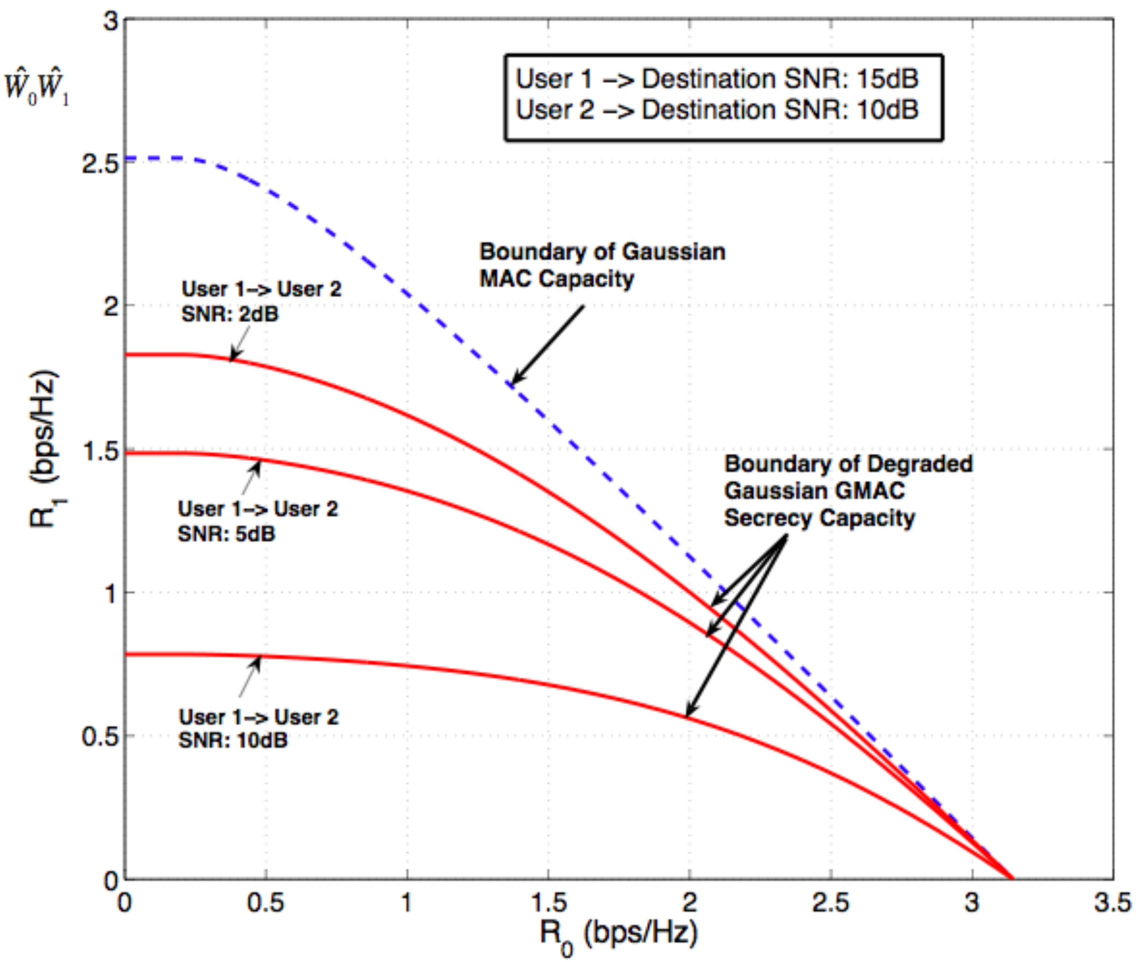
Multiple-Access Channel with Confidential Messages

Liang & Poor - IT'08 (AWGN) & Liu, Liang & Poor – IT'11 (fading)]

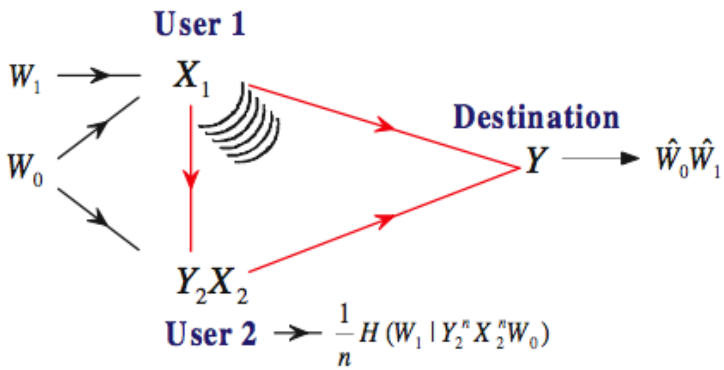


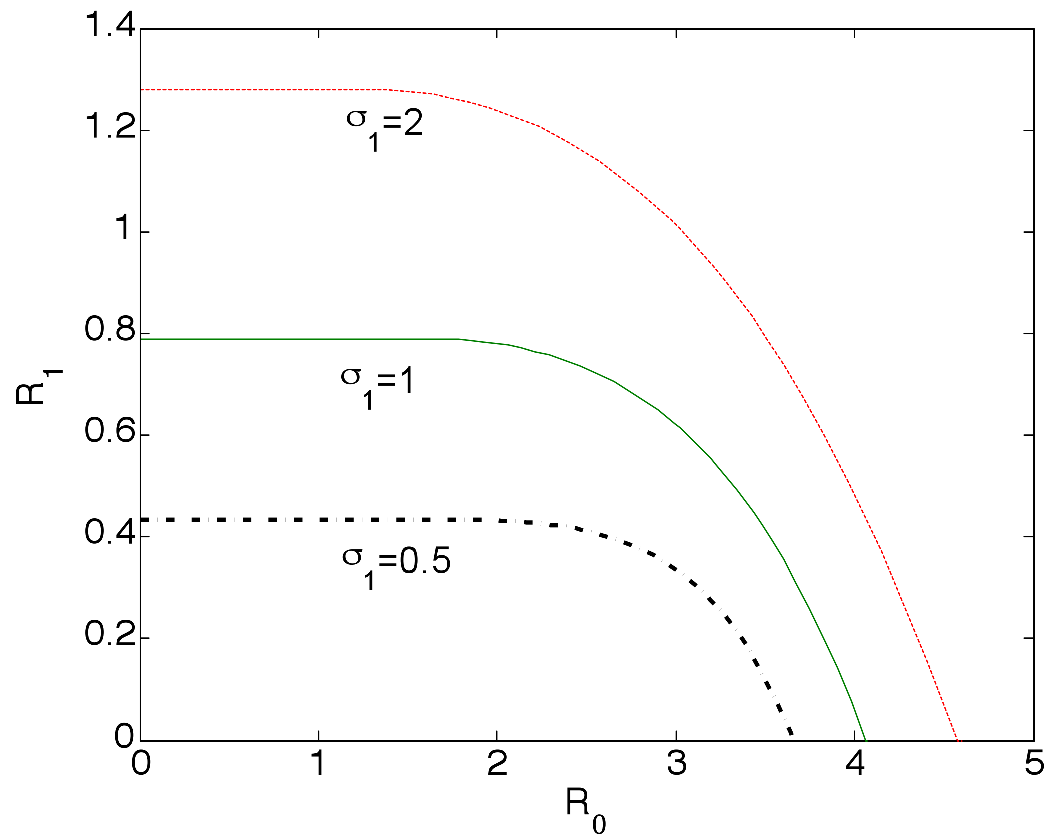
Multiple-Access Channel: AWGN





Multiple-Access Channel: Fading

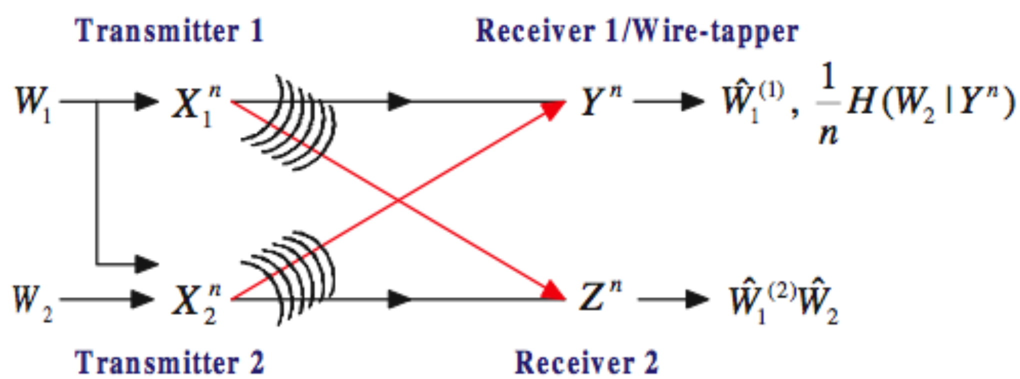




- $|h_1|^2$, $|h_2|^2$ and $|g_1|^2$ are exponentially distributed with means σ_1, $\sigma_2=1$ and $\sigma_3=1$
- power constraint $P_1=P_2=10$ dB, and Gaussian noise variance $\upsilon = u = 2$

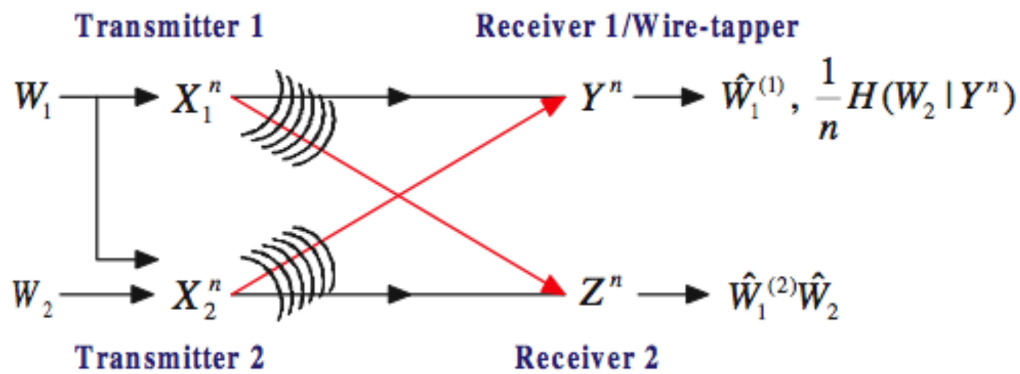
Other Channels of Interest

- Interference Channel [w/ Liang, Someck-Baruch, Shamai, Verdú - IT'09 (cognitive) & w/ Koyluoglu, El Gamal, Lai - IT'11 (interference alignment)]:



Other Channels of Interest

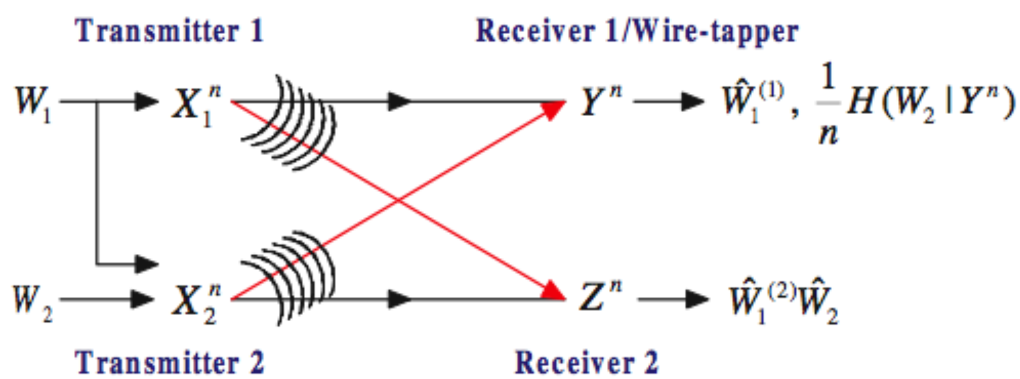
- Interference Channel [w/ Liang, Someck-Baruch, Shamai, Verdú - IT'09 (cognitive) & w/ Koyluoglu, El Gamal, Lai - IT'11 (interference alignment)]:



- Relay Channels [e.g., w/ Aggarwal, Sankar, Calderbank – JWCN'09 & w/ Kim – IT'11]: Source and relay cooperate to improve security.

Other Channels of Interest

- Interference Channel [w/ Liang, Someck-Baruch, Shamai, Verdú - IT'09 (cognitive) & w/ Koyluoglu, El Gamal, Lai - IT'11 (interference alignment)]:



- Relay Channels [e.g., w/ Aggarwal, Sankar, Calderbank – JWCN'09 & w/ Kim – IT'11]: Source and relay cooperate to improve security.

- MIMO [e.g., w/ Liu, Liu, Shamai – IT'10]: Use of multiple transmit & receive antennas allows simultaneous secure broadcast without rate penalty.

Other Results & Open Issues

Other Results of Interest

- Authentication [w/ Lai, El-Gamal – IT'09]: "Cheating" probability is characterized for authentication in noisy channels.

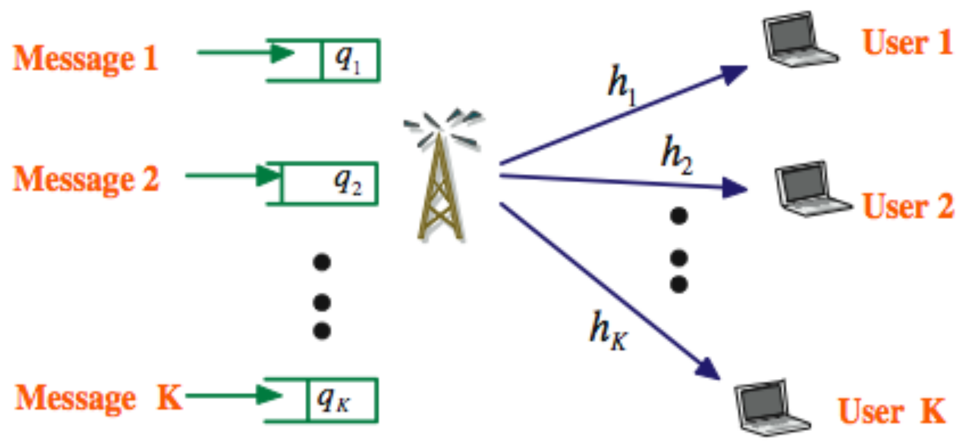
- Feedback [e.g., w/ Lai, El-Gamal – IT'08, w/ Liu, Tang, Spasojevic – IT'09 & w/ Kim – IT'10]: Judicious use of feedback enhances security.

- Code Design [e.g., w/ Liu, Liang, Spasojevic – IT (under review)]: Nested structure for secure error-control codes for the wire-tap channel.

- Cross Layer Design …

Scheduling of Secure Broadcast

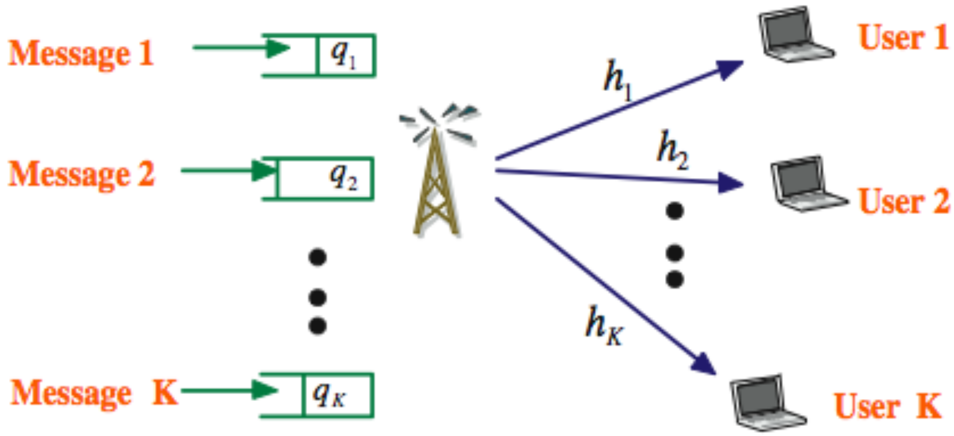
[Liang, Poor & Ying – IFS'11]



- Three objectives:
  - reliability (low error probability)
  - security (perfect secrecy)
  - stability (queues remain finite)

Scheduling of Secure Broadcast

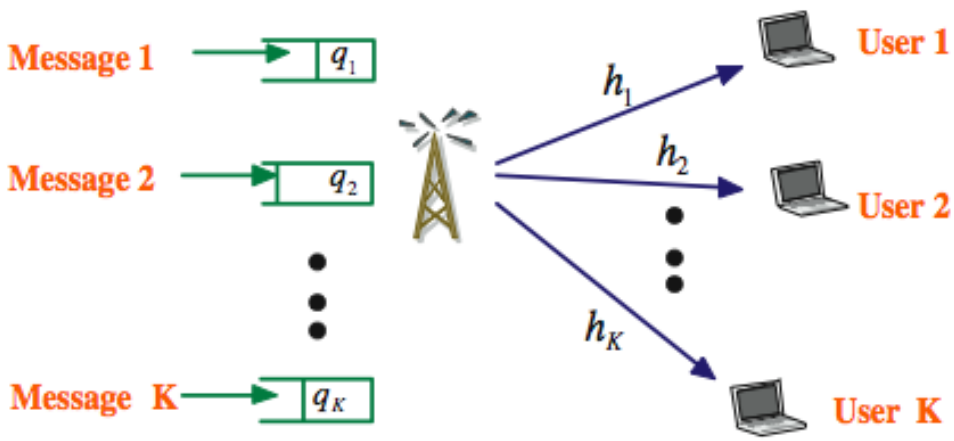
[Liang, Poor & Ying – IFS'11]



- Three objectives:
  - reliability (low error probability)
  - security (perfect secrecy)
  - stability (queues remain finite)
- Two time scales:
  - packet level (scheduling)
  - symbol level (power control)

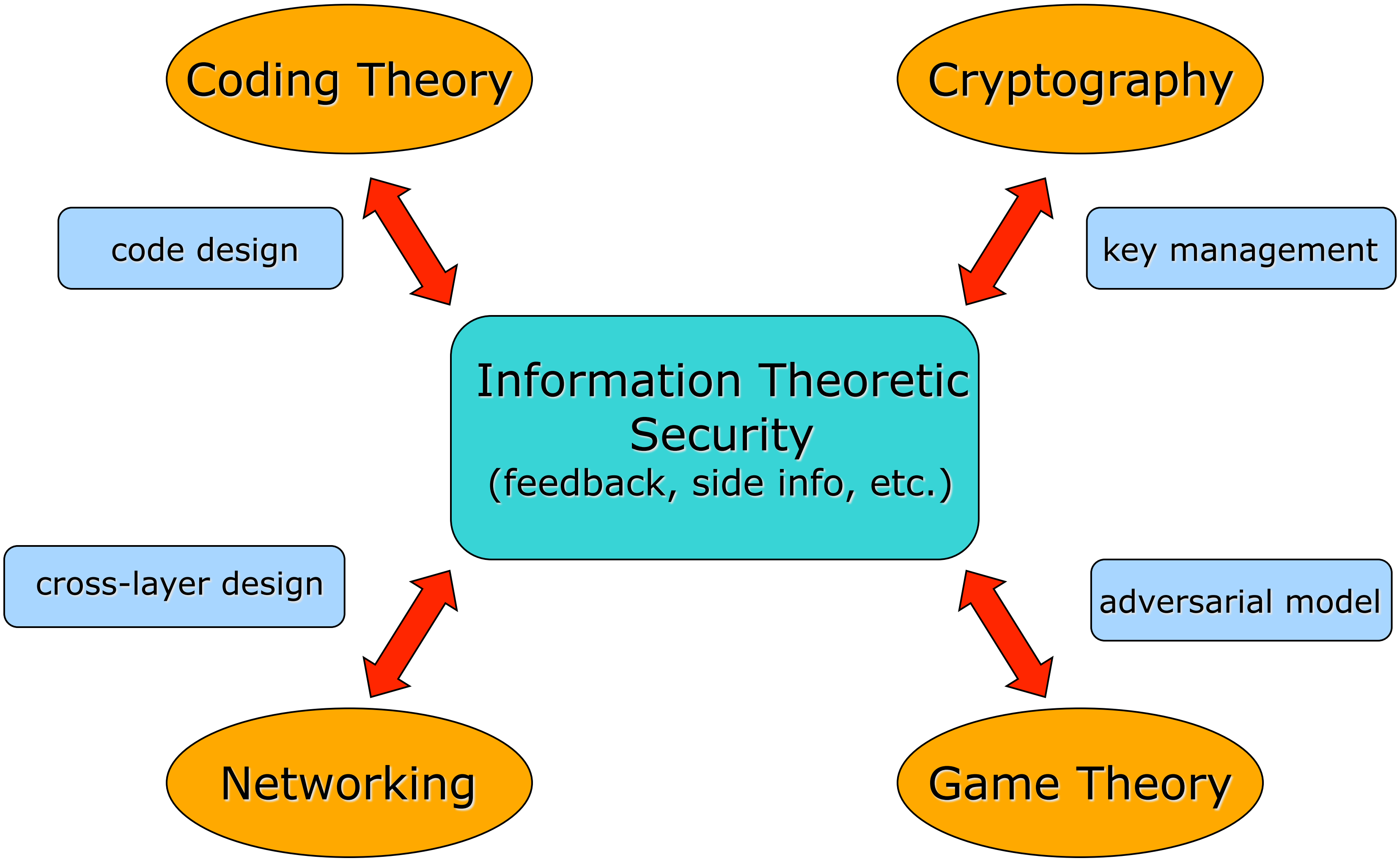
Scheduling of Secure Broadcast

[Liang, Poor & Ying – IFS'11]



- Three objectives:
  - reliability (low error probability)
  - security (perfect secrecy)
  - stability (queues remain finite)
- Two time scales:
  - packet level (scheduling)
  - symbol level (power control)
- Two eavesdropping models:
  - collaborative - MIMO wiretapper [Khisti & Wornell - IT'10]; achieve secrecy-throughput optimality via time division
  - non-collaborative - compound wiretapper [w/ Liang, Kramer, Shamai - JWCN'09]; time division is suboptimal, but can still stabilize

A Rich Area



Liang, Poor & Shamai, *Information Theoretic Security* (Now ’09)
Liu & Trappe, Eds., *Securing Wireless Communications at the Physical Layer* (Springer ’10)
Bloch & Barros, *Physical Layer Security* (CUP ’11)

A Related Problem: Privacy

The Privacy Problem

- Many electronic information sources are publicly accessible
  - Google, Facebook, open governance, census, etc.

U.S. Census Bureau

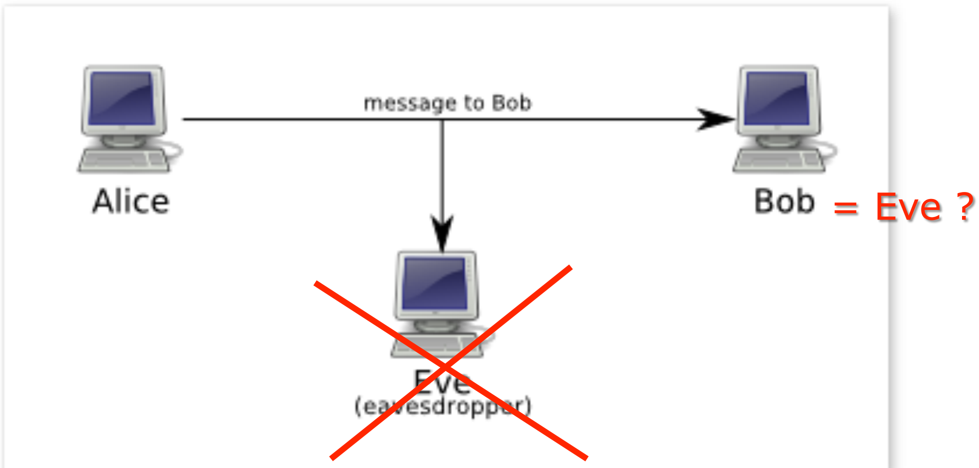
STATE OF NEW JERSEY
MOTOR VEHICLE COMMISSION

- The utility of these sources depends on their accessibility

- But, they can also leak private information

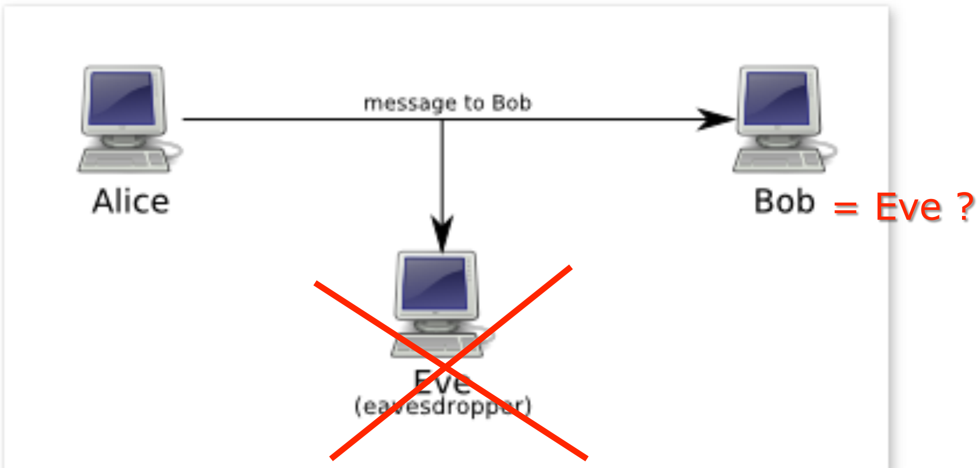
Privacy-Utility Tradeoff

- Privacy is not secrecy:



Privacy-Utility Tradeoff

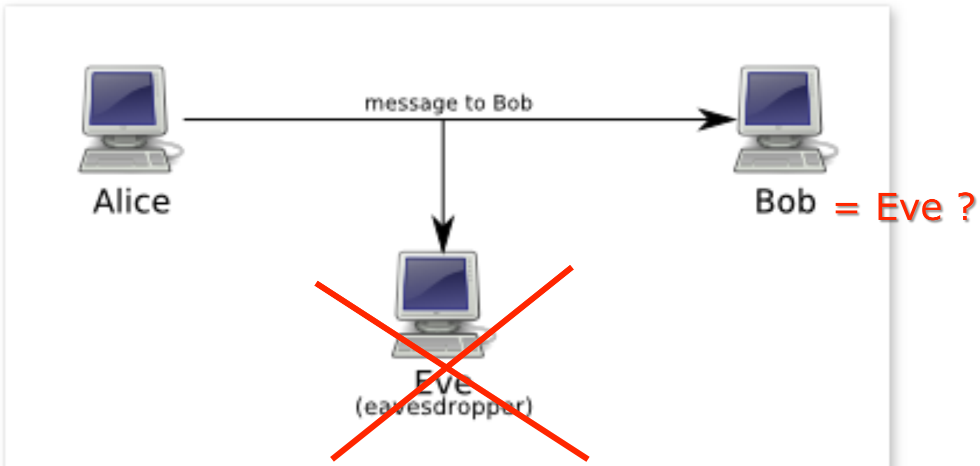
- Privacy is not secrecy:



- An information theoretic characterization: equivocation-distortion
  [w/ Sankar, Rajagopalan, IT (under review)]

Privacy-Utility Tradeoff

- Privacy is not secrecy:

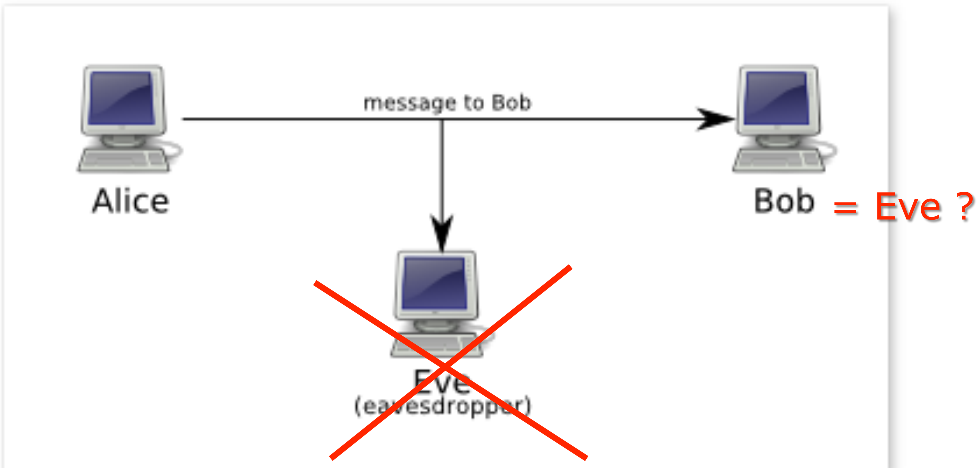


- An information theoretic characterization: equivocation-distortion
  [w/ Sankar, Rajagopalan, IT (under review)]

- Can consider multiple queries (successive disclosure) & multiple databases (side information)

Privacy-Utility Tradeoff

- Privacy is not secrecy:



- An information theoretic characterization: equivocation-distortion
  [w/ Sankar, Rajagopalan, IT (under review)]

- Can consider multiple queries (successive disclosure) & multiple databases (side information)

- Application to smart grid: competitive privacy & smart metering
  [w/ Sankar, Kar, Tandon & w/ Rajagopalan, Sankar, Mohajer – SmartGridComm'11]

Thank You!