Information Theoretic Paths Forward in the Wireless Physical Layer

H. Vincent Poor
(poor@princeton.edu)

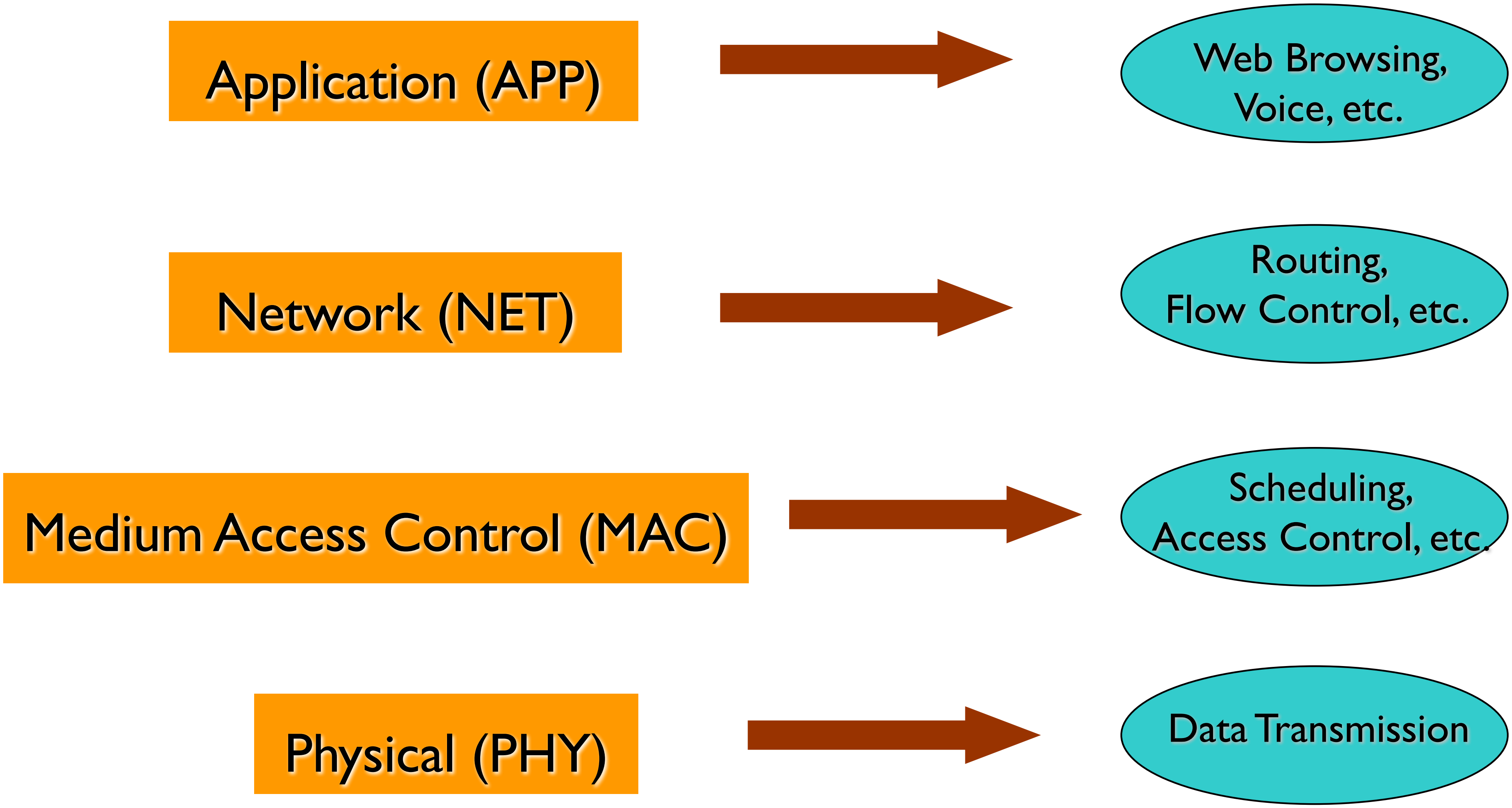
Thanks to the U.S. NSF under Grants CNS-1702808 and ECCS-1647198.

Outline of Today's Talk

- State of the Art and Emerging Challenges in the Wireless PHY
  - Key Enablers of the State of the Art: 4G
  - Challenges for the Emerging Generation: 5G & Beyond
  - Open Problems & Potential Solutions
- Two Fundamental Approaches
  - Physical Layer Security
  - Finite-Blocklength Fundamentals

State of the Art and Emerging Challenges in the Wireless PHY

Wireless Networks: Layers



Key Enablers of the State-of-the-Art

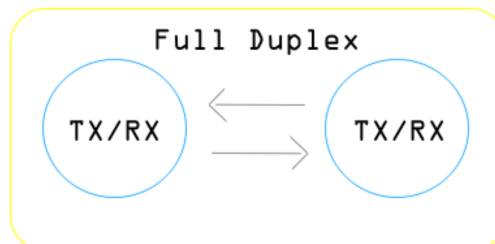
- Exploiting spatial diversity:
  - MIMO, cooperation & relaying
- Exploiting frequency diversity:
  - OFDMA
- Approaching the Shannon limit:
  - Iterative decoding (Turbo, LDPC)

Challenges for the Emerging Generation

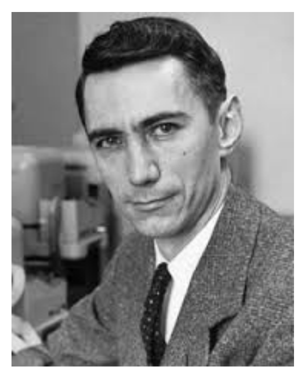
- Always capacity, reliability, and now, energy efficiency
- In the emerging generation, supporting:
  - Internet of Things (IoT):
    - 100's of billions of terminals, densification, low complexity
  - Autonomy & telecontrol:
    - low latency and very high reliability
  - Immersive experiences:
    - very high bandwidth streaming

Open Problems & Potential Solutions

- Densification & interference management:
  - C-RAN, massive MIMO, mmWave, energy harvesting
- Capacity enhancement:
  - Full duplex, NOMA, caching



- Security in IoT:
  - Physical layer security √
- Short packet transmission:
  - Finite-blocklength fundamentals √



Physical Layer Security

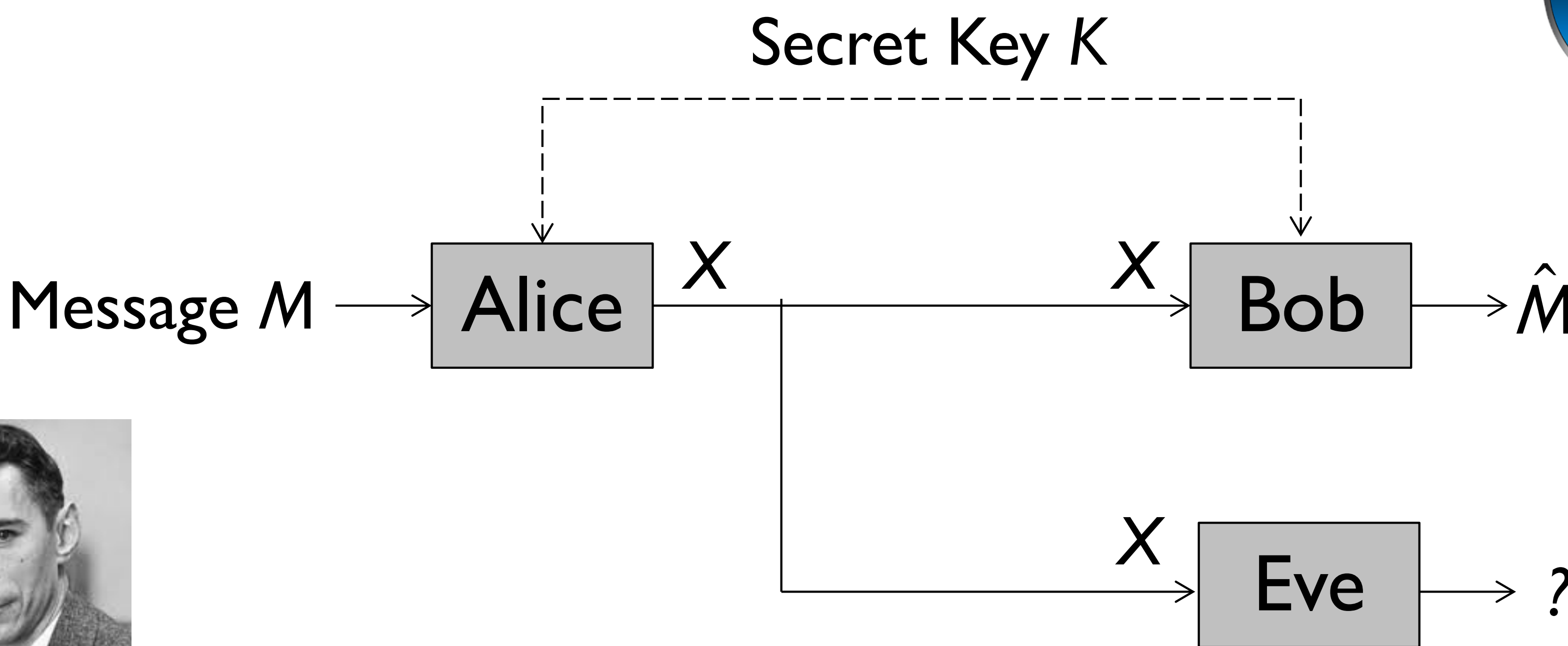
The PHY: From Foe to Friend

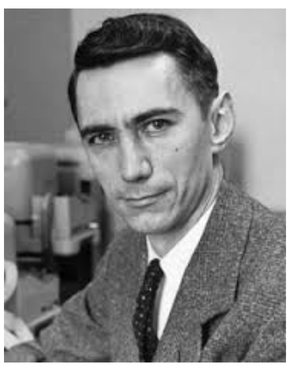
- Key Techniques for Improving Capacity & Reliability:
  - MIMO (Multiple-Antenna Systems)
  - Cooperation & Relaying
  - Cognitive Radio

The PHY: From Foe to Friend

- Key Techniques for Improving Capacity & Reliability:
  - MIMO (Multiple-Antenna Systems)
  - Cooperation & Relaying
  - Cognitive Radio
- What About Security?
  - Traditionally a higher-layer issue (e.g., APP)
  - Encryption can be complex and difficult without infrastructure
  - Information theoretic security examines the fundamental ability of the PHY to provide security (primarily secrecy – i.e., data confidentiality)

Information Theoretic Secrecy: Shannon's Model



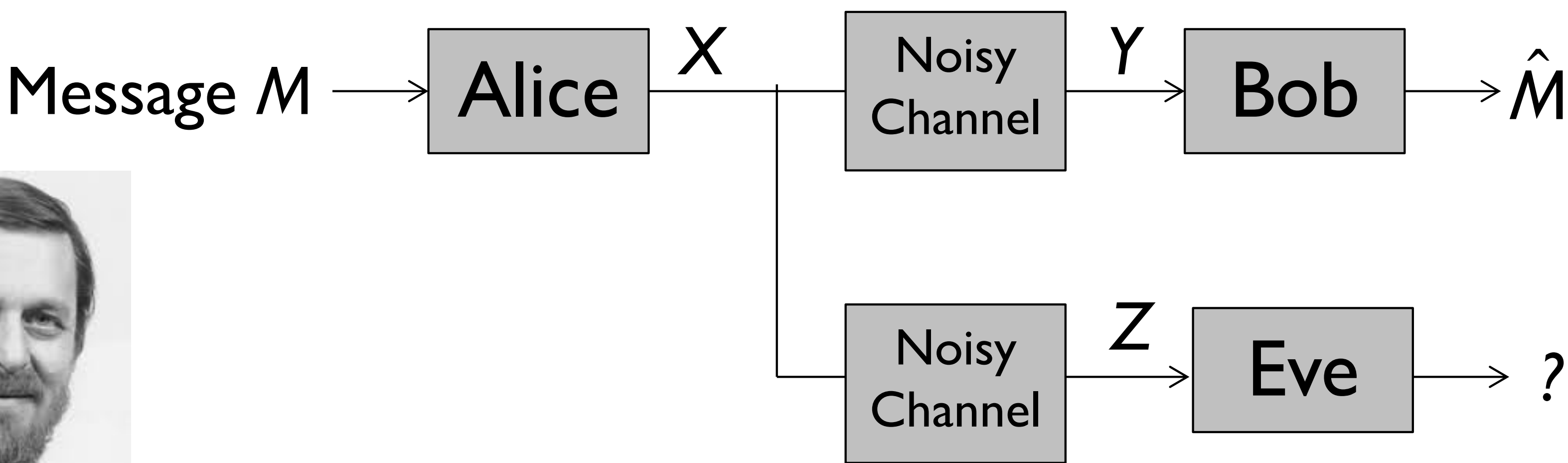


Shannon [1949]: For cipher, perfect secrecy requires a one-time pad.

[I.e., the entropy of the key must be at least the entropy of the source: $H(K) \geq H(M)$]

Information Theoretic Secrecy: Wyner's Model

"The Wiretap Channel"



- Tradeoff: reliable rate R to Bob vs. the "equivocation" $H(M|Z)$ at Eve
- Secrecy capacity = maximum R such that $R = H(M|Z)$
- Wyner [1975]: Secrecy capacity > 0 iff. Z is degraded relative to Y

Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in these ideas, as standard encryption is impractical for emerging wireless networking paradigms.

Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in these ideas, as standard encryption is impractical for emerging wireless networking paradigms.

- In general, the legitimate receiver needs an advantage over the eavesdropper – either a secret shared with the transmitter, or a better channel.

Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in these ideas, as standard encryption is impractical for emerging wireless networking paradigms.

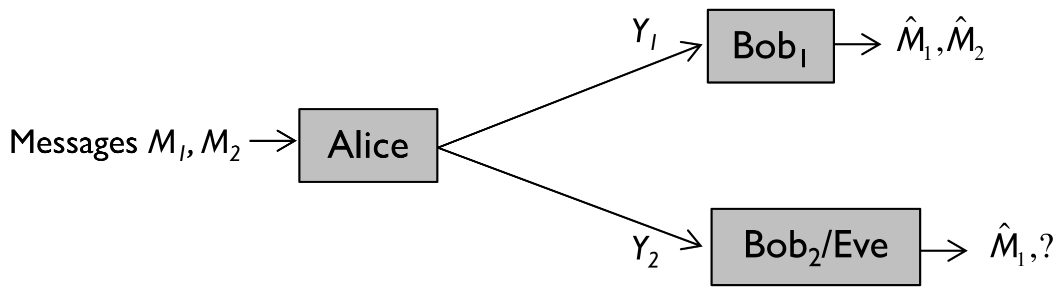
- In general, the legitimate receiver needs an advantage over the eavesdropper – either a secret shared with the transmitter, or a better channel.

- The physical properties of radio propagation (diffusion & superposition) provide opportunities for this, via
  - fading: provides natural degradedness over time
  - interference: allows active countermeasures to eavesdropping
  - spatial diversity (MIMO, relays): creates "secrecy degrees of freedom"
  - random channels: sources of common randomness for key generation

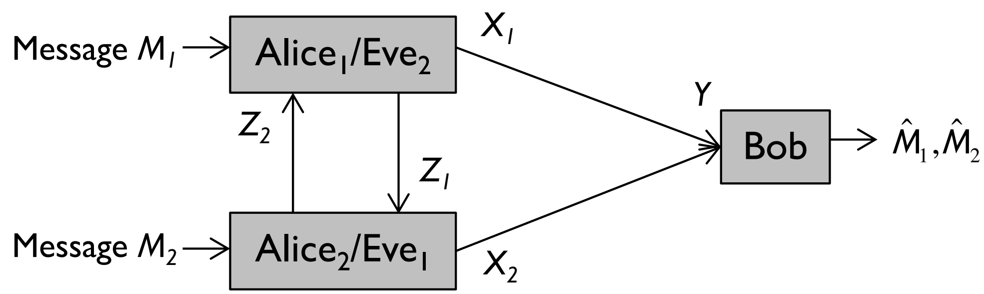
[Survey: Poor & Schaefer (2017) "Wireless Physical Layer Security," PNAS]

Secrecy in Fundamental Channel Models

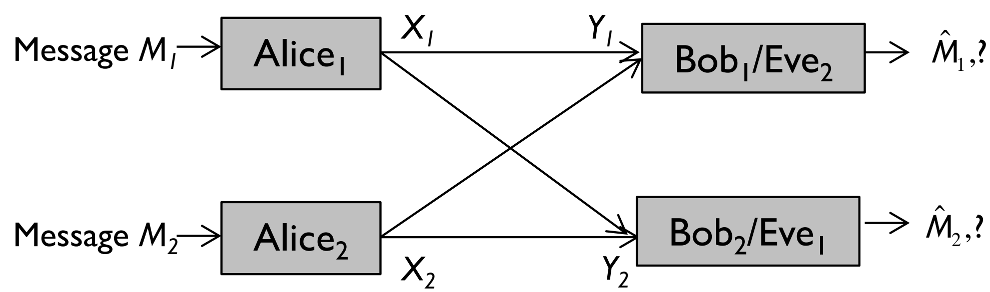
- Broadcast Channels:



- Multiple-Access Channels:



- Interference Channels:



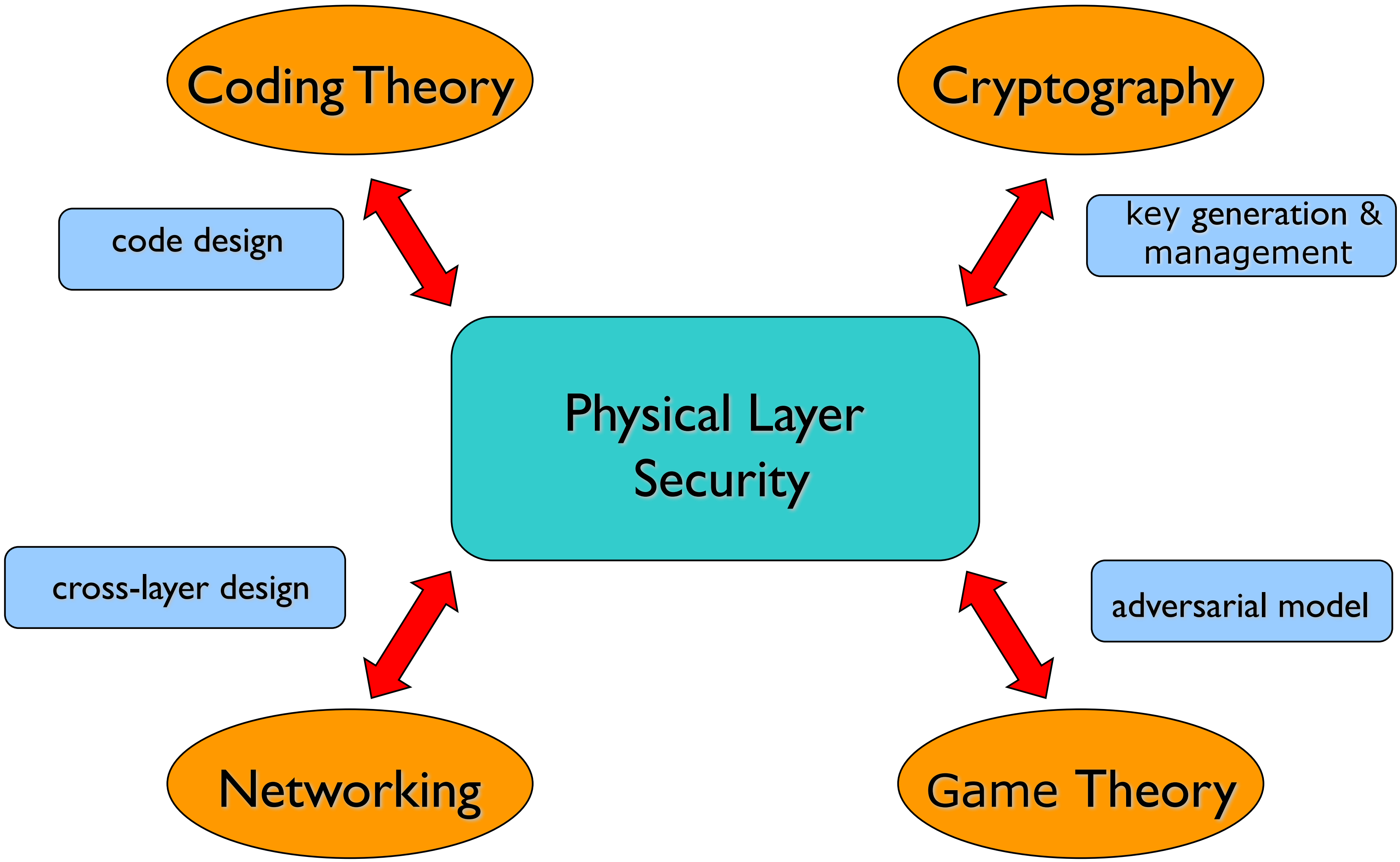
- Relay Channels: Relay cooperates to improve security; or relay is untrusted.
- MIMO Channels: Allows simultaneous secure transmission without rate penalty.

Key Generation from Common Randomness

- Passive Eavesdropper:
  - Public discussion (Ahlswede & Czizsár [1993], Mauer [1993])
  - Channel reciprocity: joint source-channel model
  - Relay assisted: trusted or oblivious
- Active Eavesdropper:
  - Channel reciprocity: joint source-channel model

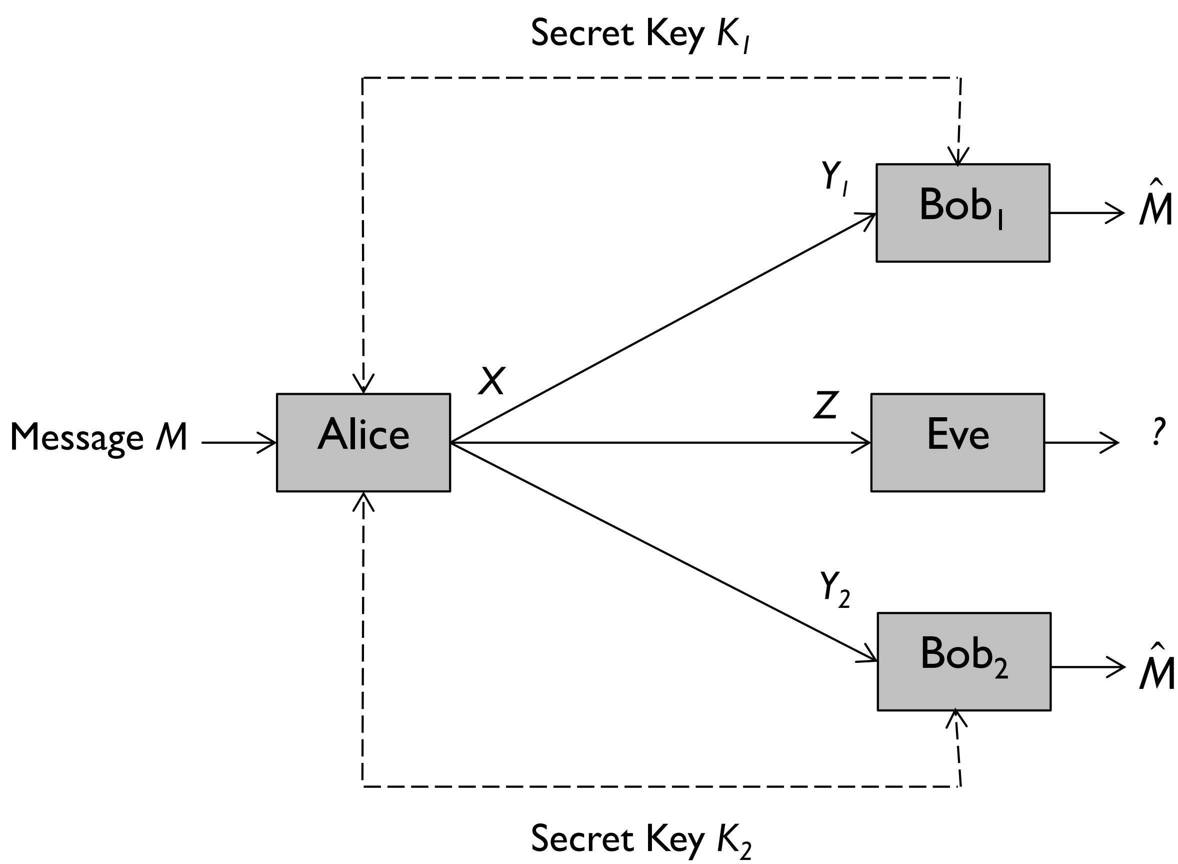
[Survey: Lai, et al. (2015) "Key Generation from Random Channels," in *Physical Layer Security in Wireless Communications*, Zhou & Song, Eds.]

A Rich Area



Coding Theory
Cryptography
code design
key generation & management
Physical Layer Security
cross-layer design
adversarial model
Networking
Game Theory

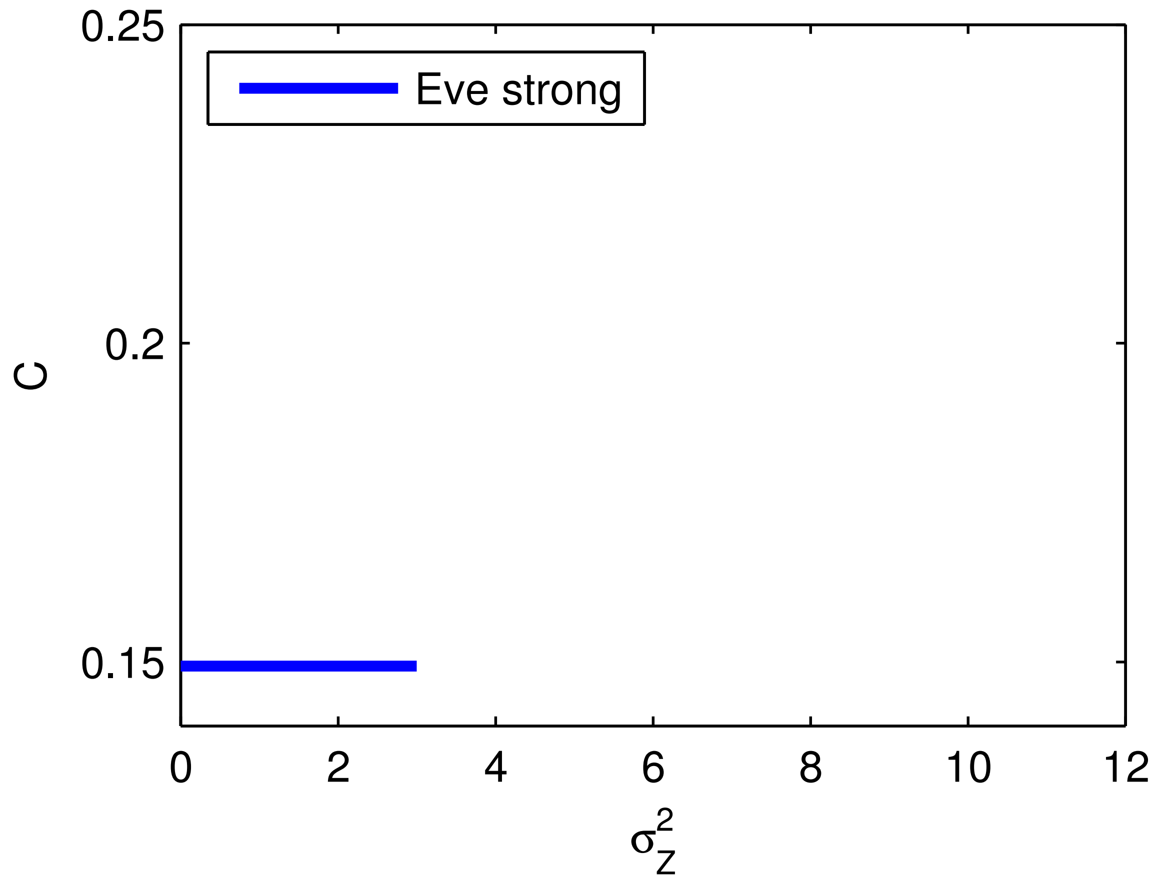
Augmentation of Traditional Encryption
Broadcast with Secret Keys



[Schaefer, Khisti & Poor (2018) – IEEE Trans. Commun.]

Augmentation of Traditional Encryption

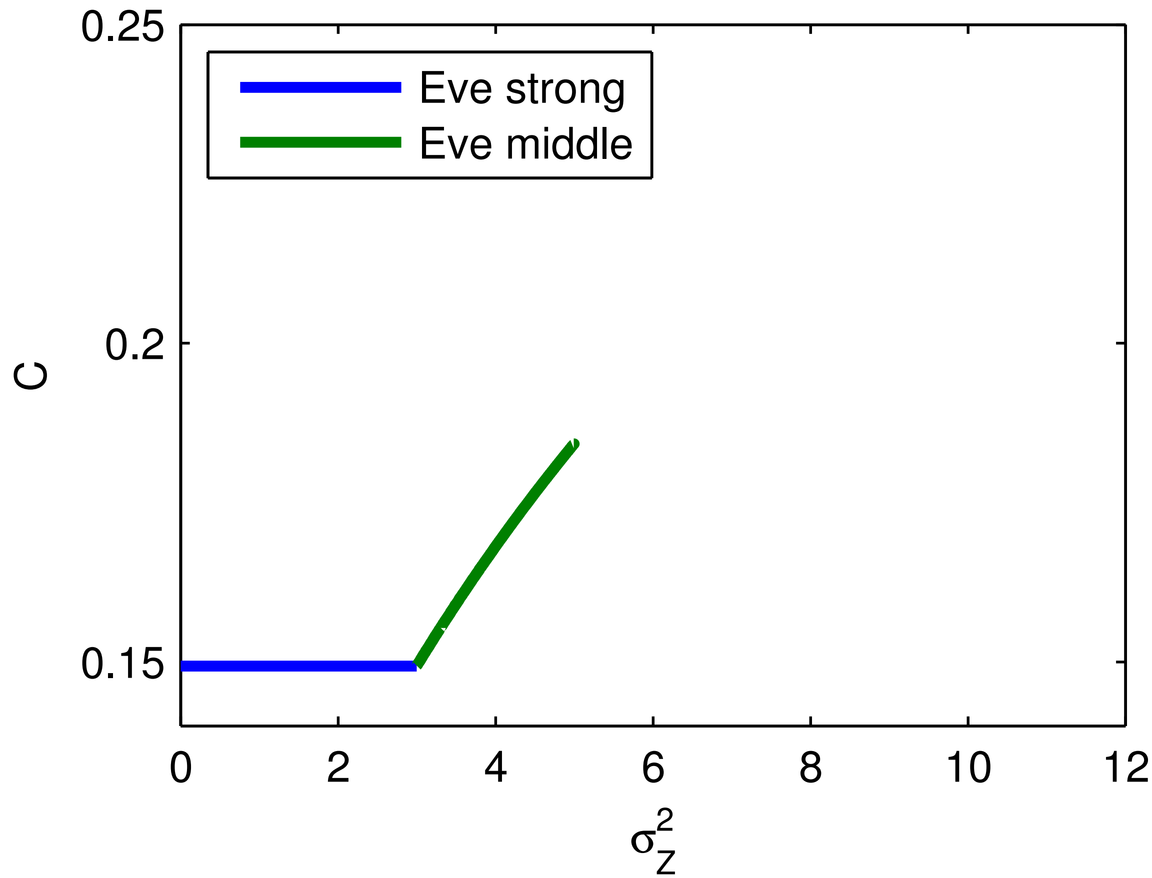
Example: AWGN Channel



[Schaefer, Khisti & Poor (2018) – IEEE Trans. Commun.]

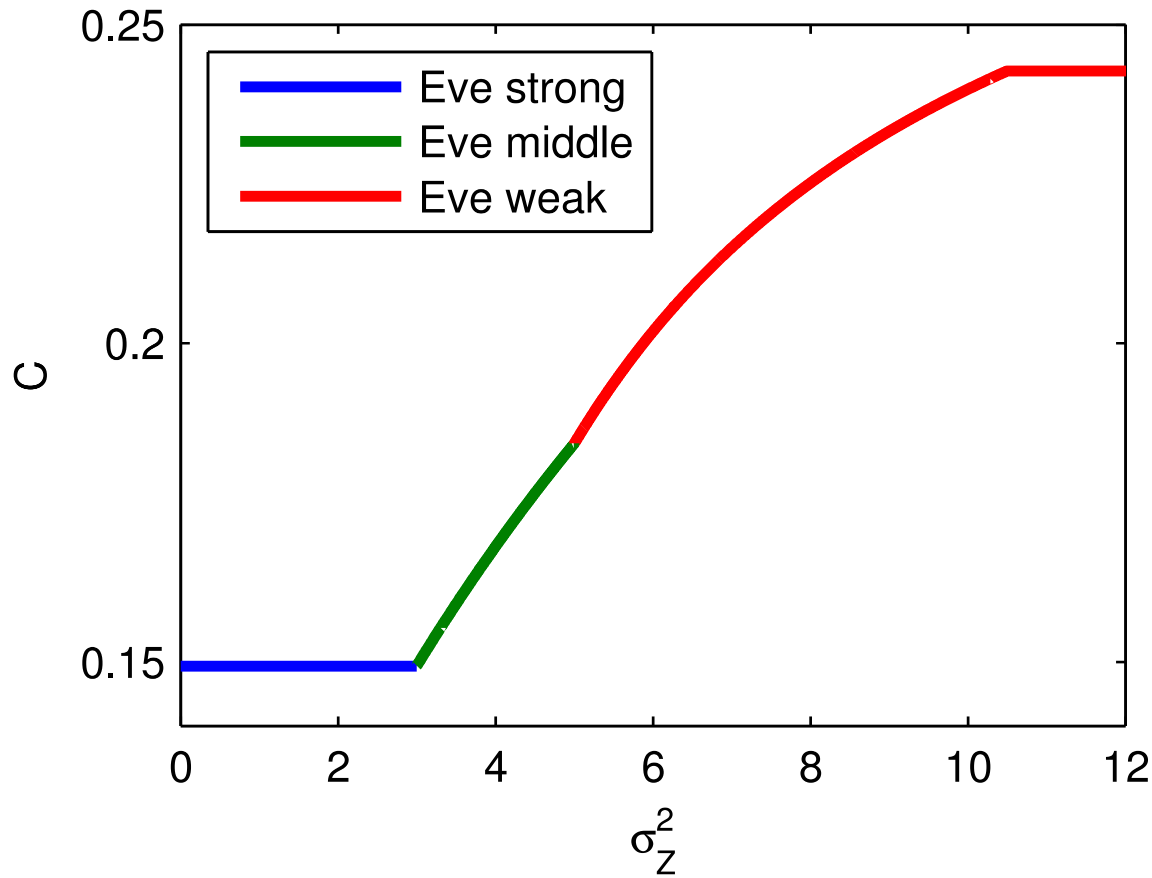
Augmentation of Traditional Encryption

Example: AWGN Channel



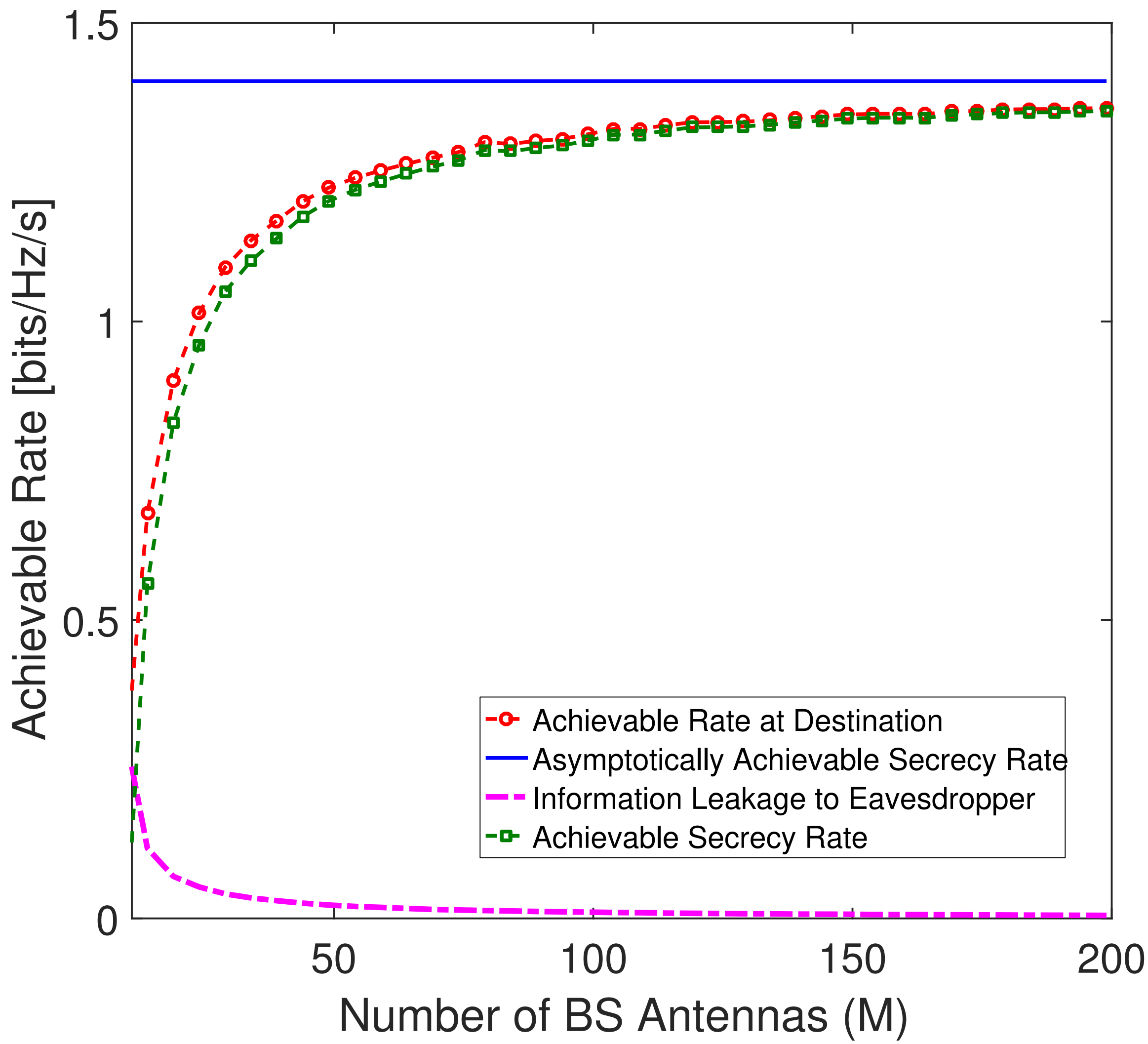
[Schaefer, Khisti & Poor (2018) – IEEE Trans. Commun.]

Augmentation of Traditional Encryption
Example: AWGN Channel



[Schaefer, Khisti & Poor (2018) – IEEE Trans. Commun.]

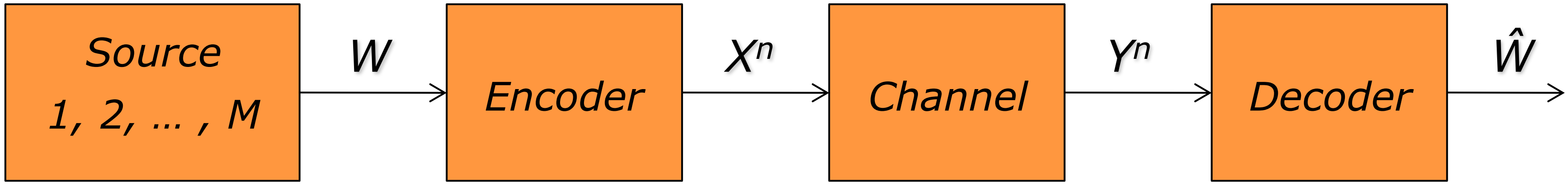
PHY Security in Massive MIMO Systems



[Amarasuriya, Schaefer & Poor (2017) – Proc. Asilomar Conf.]

Finite-Blocklength Fundamentals

A Fundamental Problem



- <u>(n,M,ε) code</u>: $P(W \neq \hat{W}) \leq \varepsilon$
- <u>Fundamental limit</u>: $M^*(n,\varepsilon) = \max\{M: \exists \text{ an } (n,M,\varepsilon) \text{ code}\}$
- <u>Shannon</u>: As $n \to \infty$, $\varepsilon \to 0$

$$\frac{\log M^*(n,\varepsilon)}{n} \to C \quad \text{(capacity)}$$

- In many situations (e.g., short packets) n and ε are <u>noticeably finite</u>.

Finite *n* and *ε*

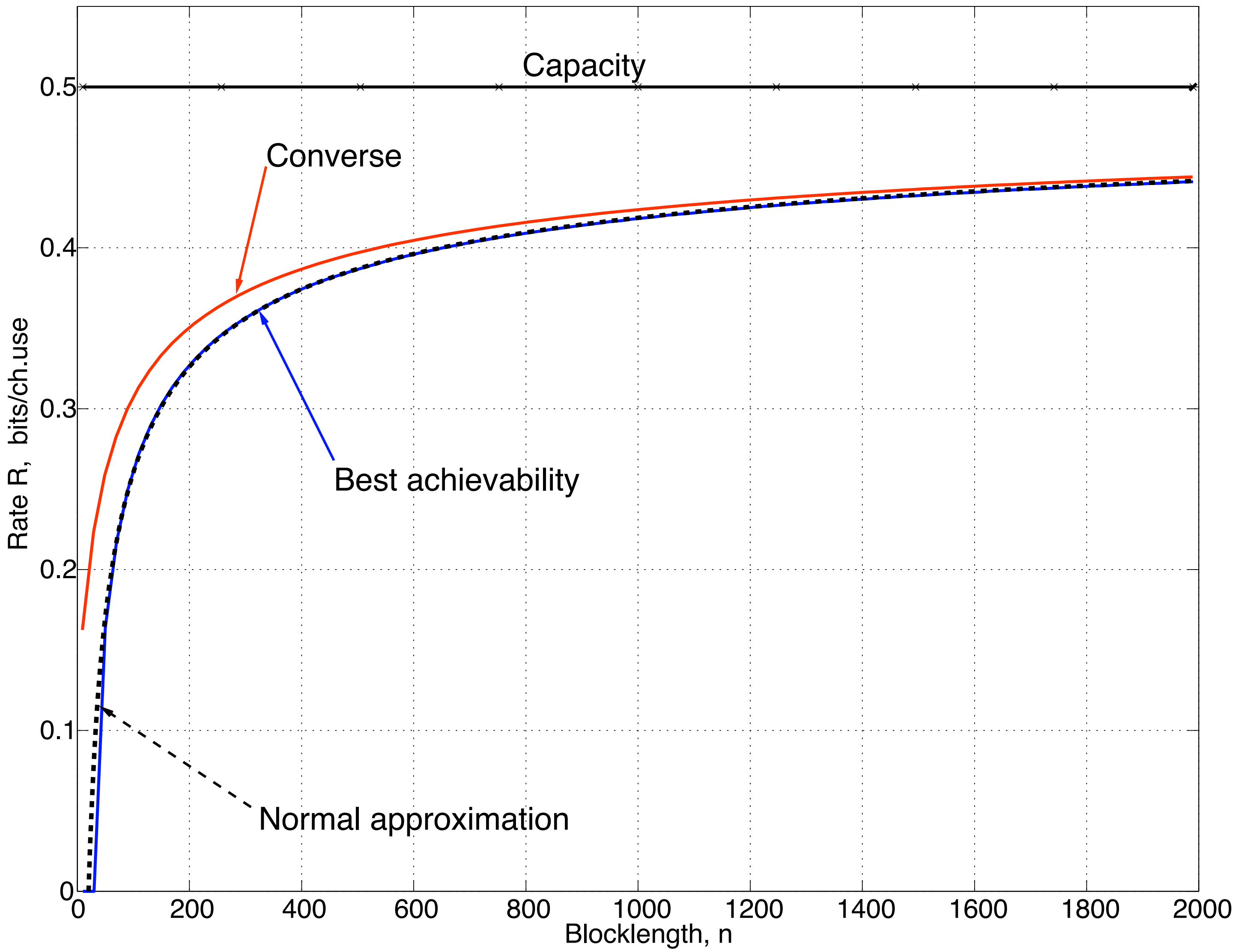
- Bounds:
  - Shannon-Feinstein (1954/57); Gallager (1965)
  - Random coding union; dependence testing
- Approximation:
  - Strassen (1962) – discrete memoryless channels
  - New bounds yield – sharper for DMCs; Gaussian; fading

$$\log M^*(n,\varepsilon) = n\,C - \sqrt{nV}\,Q^{-1}(\varepsilon) + O(\log n)$$

$V = \mathrm{Var}[i(X^*,Y^*)]$ ("dispersion")

[Polyanskiy, Poor & Verdu (2010, 2011) – IEEE Trans. Inf. Theory]

Example: AWGN (SNR = 0 dB; $\varepsilon = 10^{-3}$)

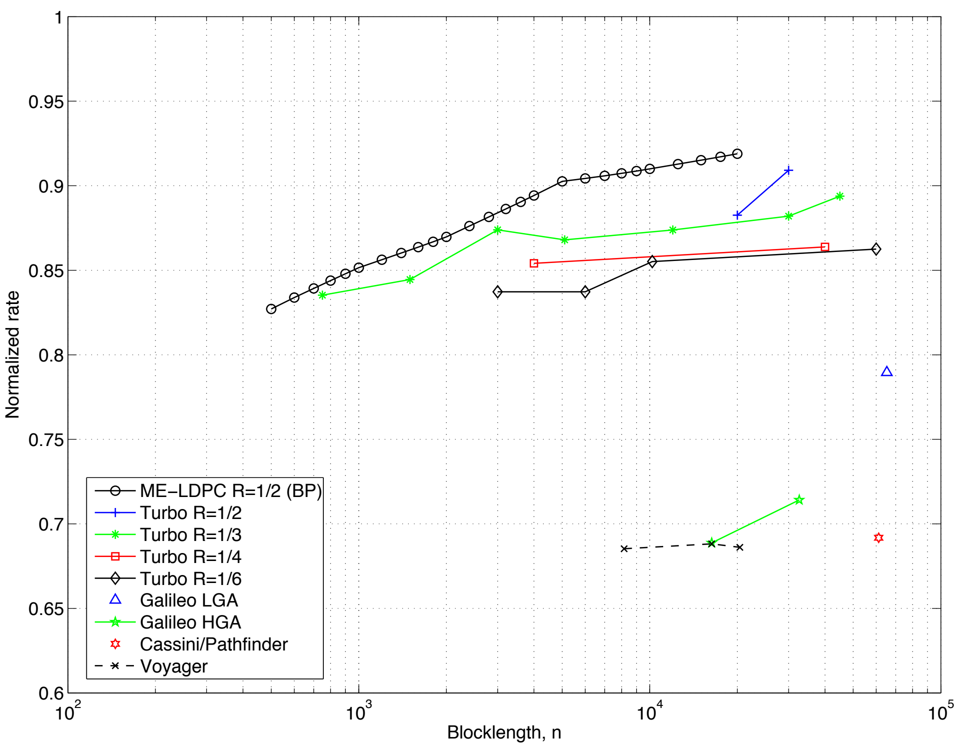


[Polyanskiy, Poor & Verdu (2010, 2011) – IEEE Trans. Inf. Theory]

Applications

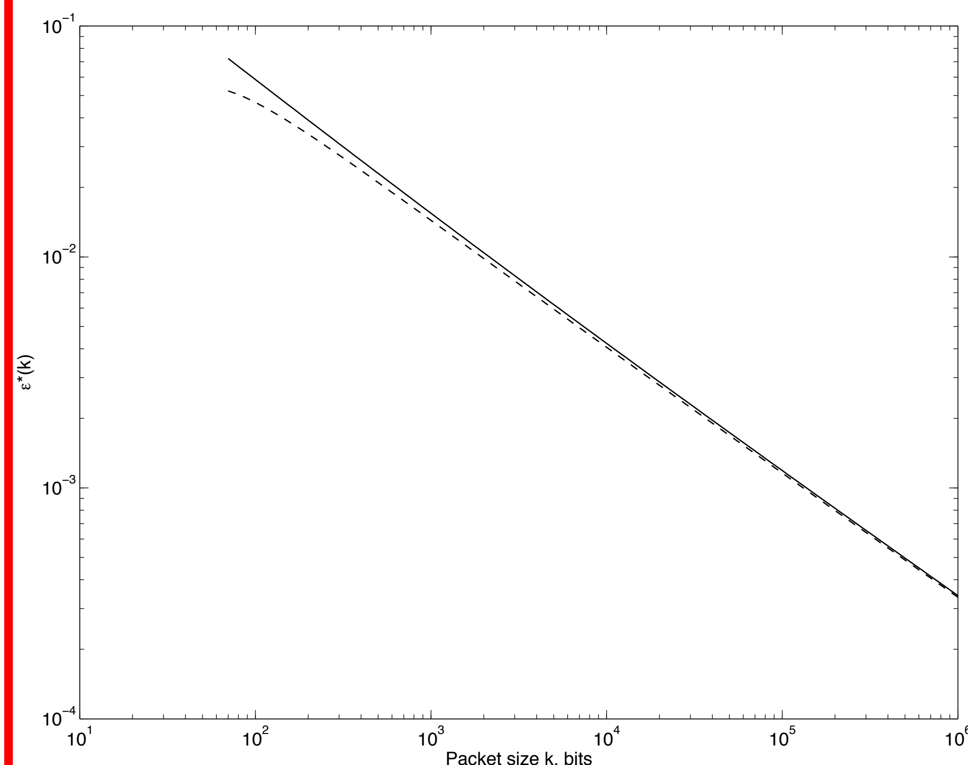
Analysis of Codes

(normalized to the approx.; ε = 10^{-4})

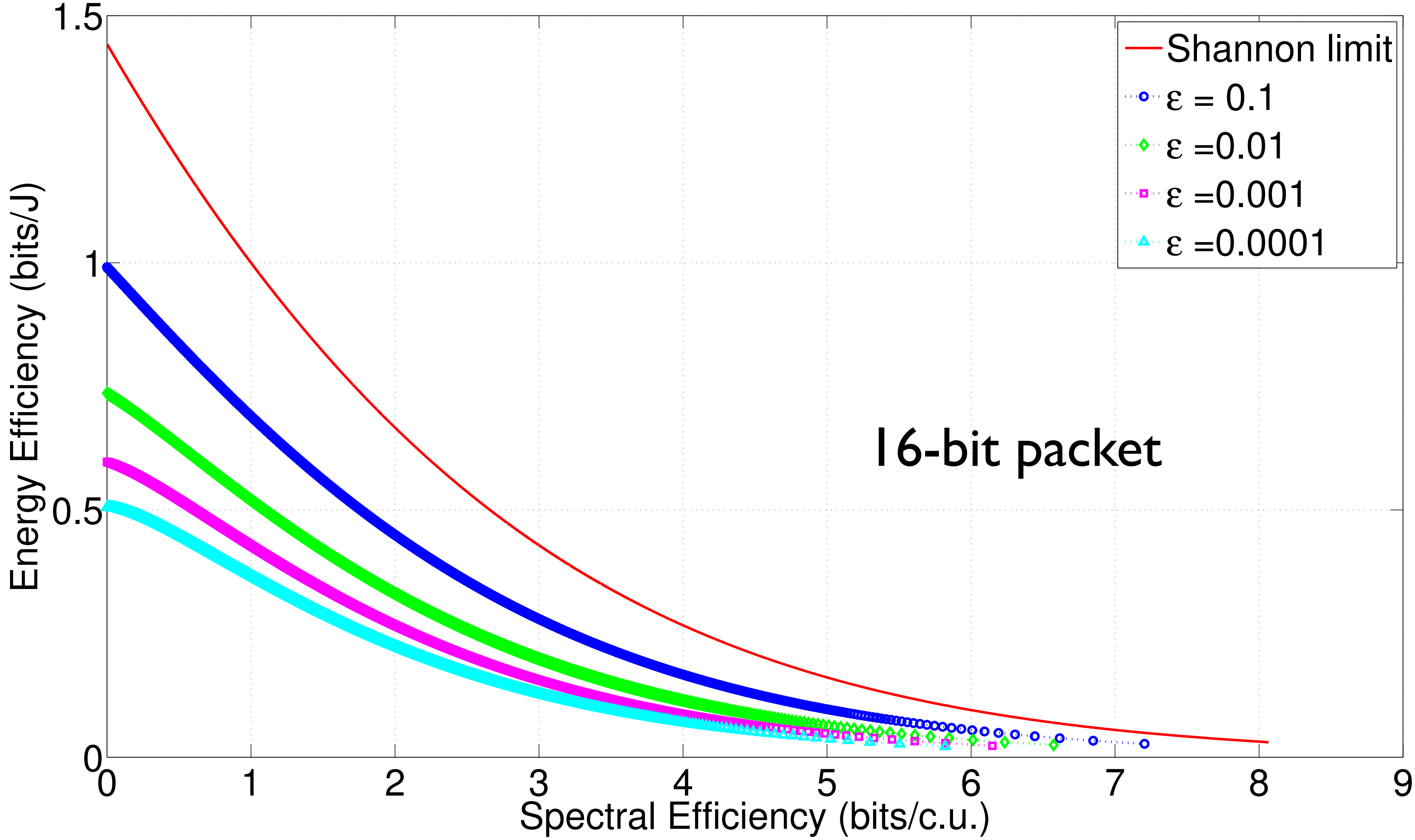


ARQ: Optimal *ε* vs. *n*

(AWGN; SNR = 0 dB)

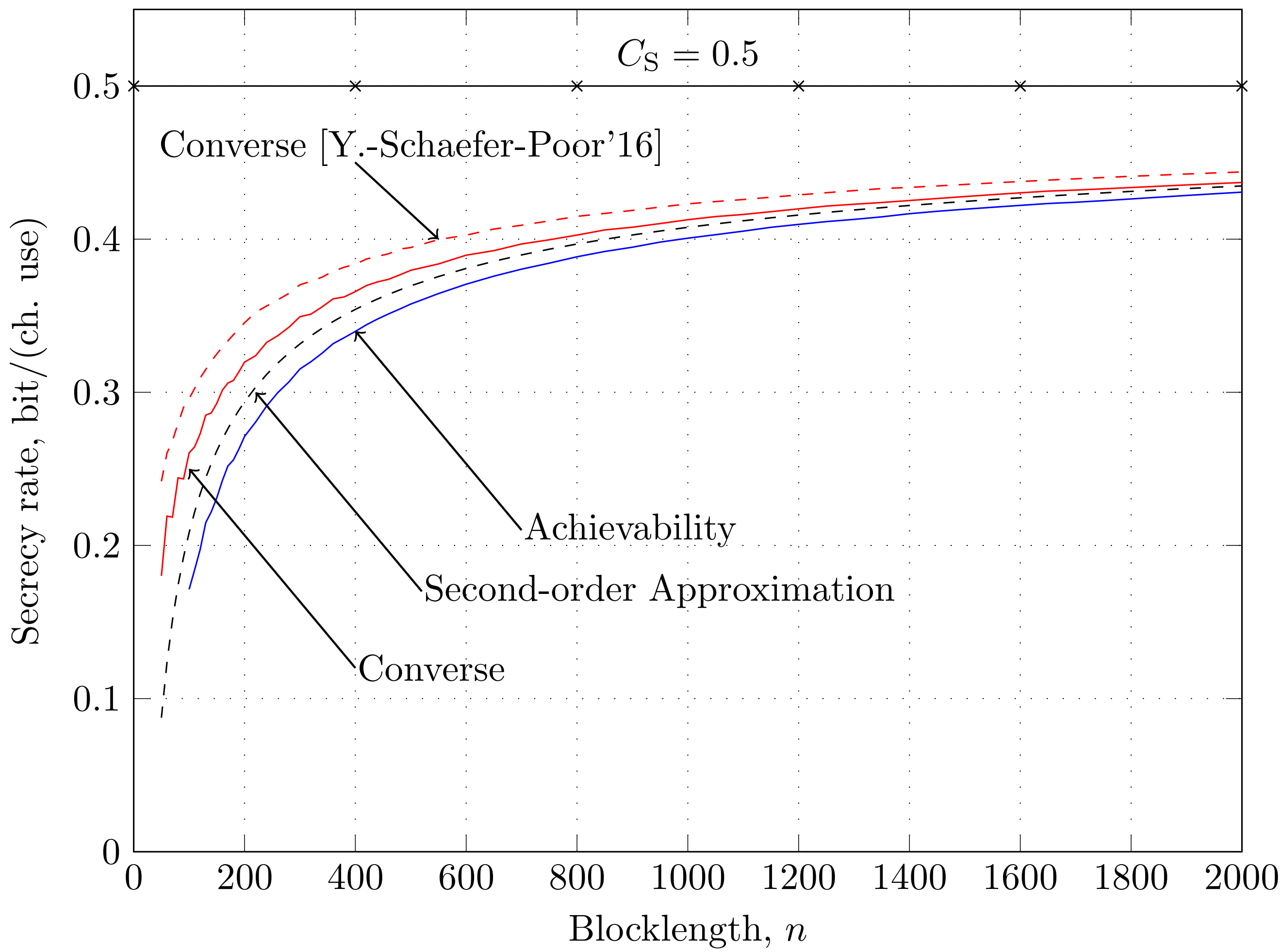


Short-Packet Energy/Spectral-Efficiency Tradeoff



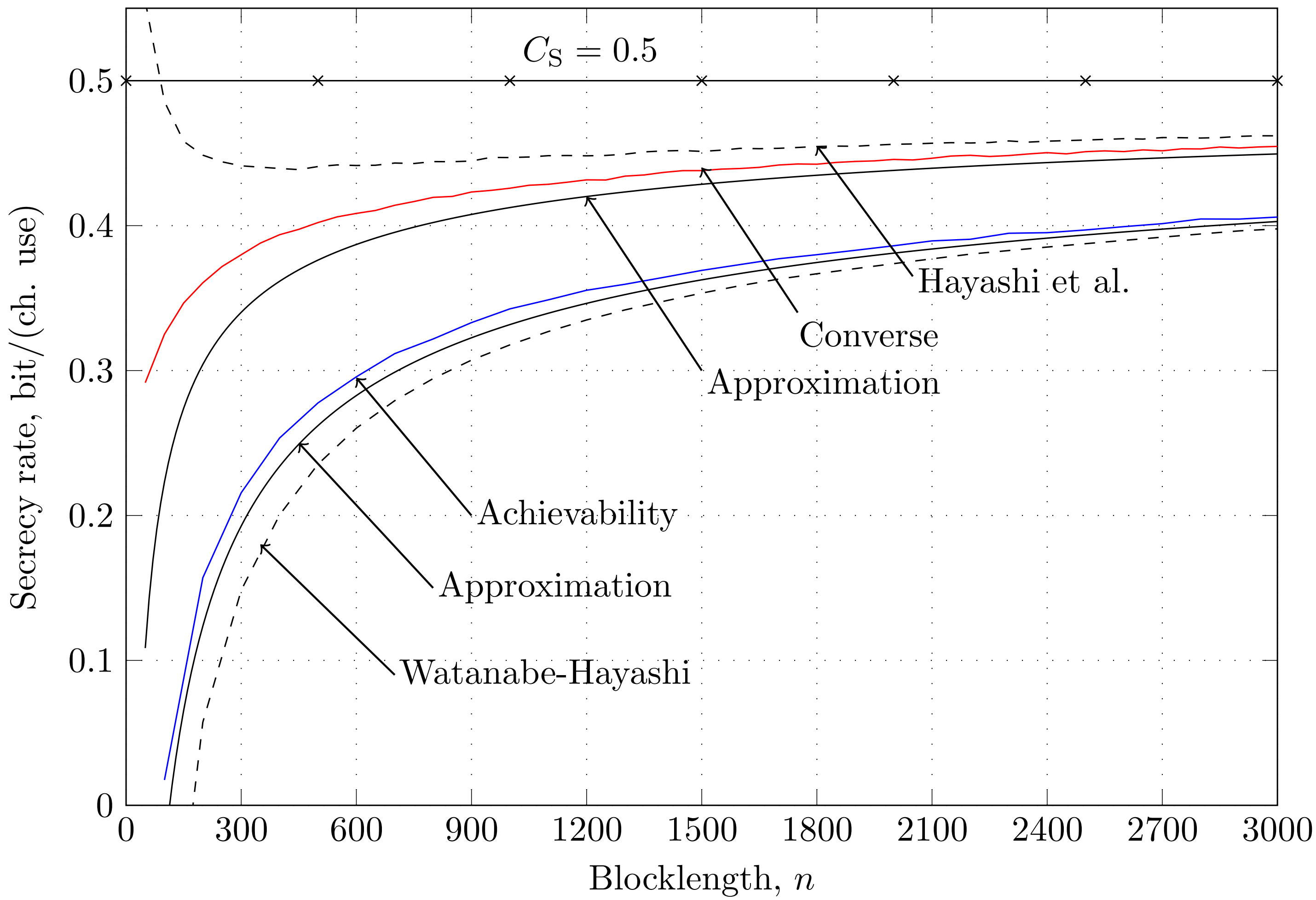
[Gorce, Kelif & Poor (2016) – Proc. IEEE Globecom]

Short-Packet Security
Semi-deterministic Wiretap Channel



[Yang, Schaefer & Poor (2017) – Proc. IEEE Int. Symp. Inf. Theory]

Short-Packet Security
Gaussian Wiretap Channel



[Yang, Schaefer & Poor (2017) – Proc. IEEE Int. Symp. Inf. Theory]

Summary

- State of the Art and Emerging Challenges in the Wireless PHY
  - Key Enablers of 4G: spatial diversity, OFDMA, iterative decoding, etc.
  - Challenges for 5G & Beyond: densification, low latency/high reliability, high data bandwidths, etc.
  - Potential Solutions: C-RAN, massive MIMO, mmWave, energy harvesting, full duplex, NOMA, caching, etc.
- Two Fundamental Approaches
  - Physical Layer Security (e.g., the Internet of Things)
  - Finite-Blocklength Fundamentals (e.g., optimal short-packet transmission)

Thank You!