Opportunistic Secret Communication

Zang Li

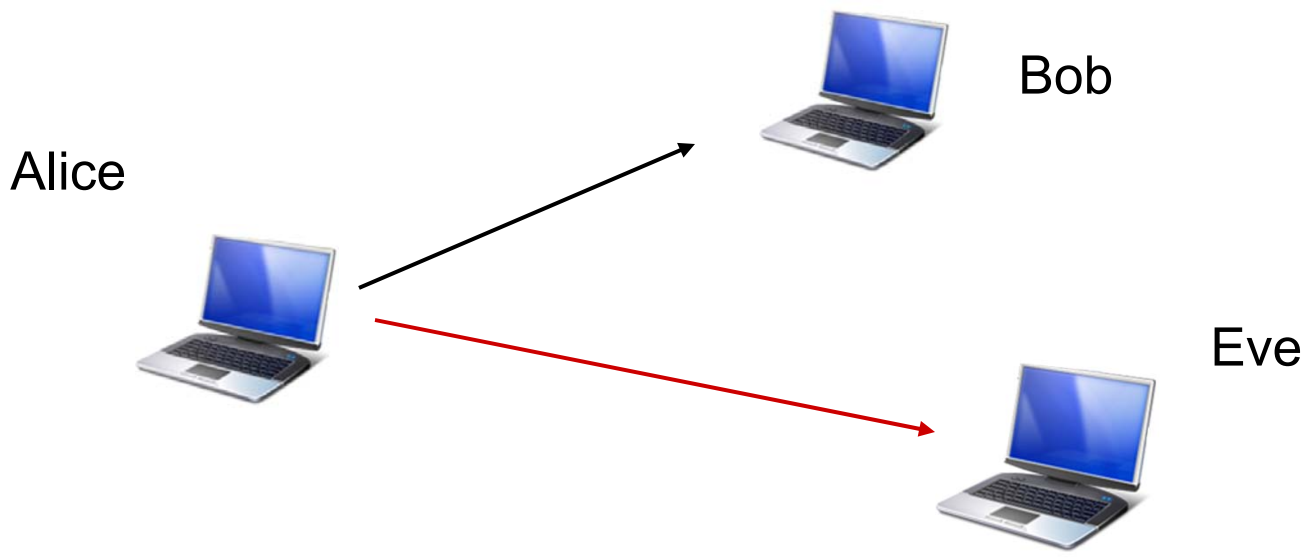
Advisors: Wade Trappe, **Roy Yates**

WINLAB Research Review,
Rutgers University
May19, 2009

Wireless $\Rightarrow$ New Security Challenges

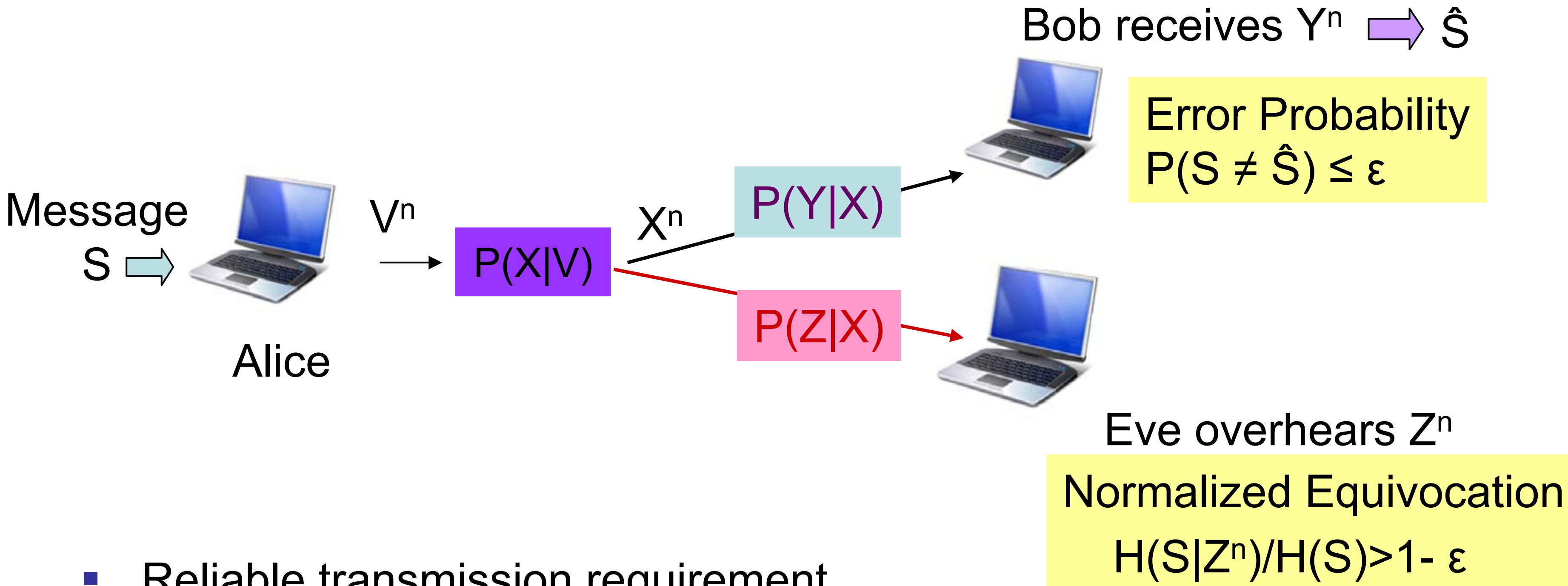
- Open medium: eavesdropping & jamming
- Traditional approach: cryptography
  - Initially shared key among communication parties
  - Central authority to distribute the key
  - Computational security
- Unique properties of wireless can be exploited to achieve secret communication among the users directly
- Information theoretic secret communication for the wireless PHY layer

Scenario



- Wireless broadcast channel
- Passive eavesdropper
- Can Alice talk to Bob secretly? If yes, at what secret rate?

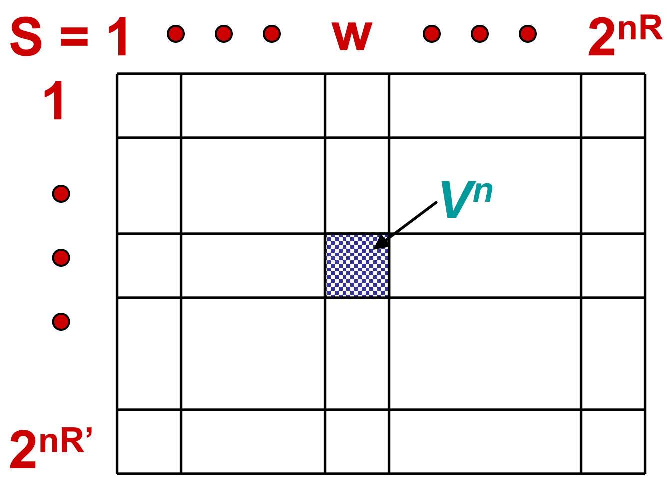
Information Secure Secret Communication



- Reliable transmission requirement
- Perfect secrecy requirement
- **Secrecy capacity**: maximum reliable rate with perfect secrecy
  - Rates may be very small, but sufficient to establish a key for subsequent communication

Coding Procedure

- Stochastic encoding, joint typical decoding (Csiszar&Korner 78)



$X^n = f(V^n)$

To ensure correct decoding at Bob

(Bob finds only one typical sequence in the whole table.)

$$R + R' < I(V;Y)$$

To ensure full equivocation at Eve

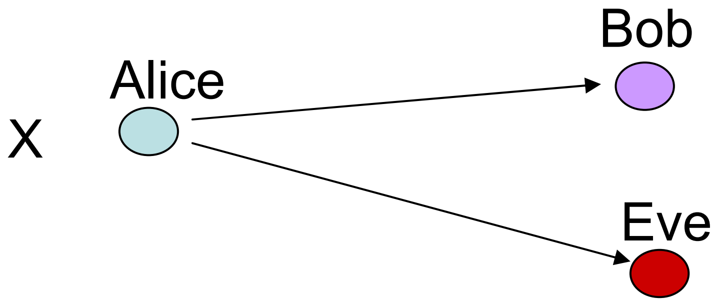
(Eve finds at least one typical sequence in every column.)

$$R' > I(V;Z)$$

$$\Rightarrow \quad R < I(V;Y) - I(V;Z)$$

Motivation

Scalar AWGN Broadcast Channel



$$Y = \sqrt{b}\,X + W_1$$

$$Z = \sqrt{g}\,X + W_2$$

$W_1, W_2 \sim N(0,1)$

$$C_{AWGN} = \max_{P(x)} I(X;Y) - I(X;Z) = \frac{1}{2}\left(\log(1+bP) - \log(1+gP)\right)^{+}$$

[Leung-Yan-Cheong & Hellman 78], [Van Dijk 97]

$\lim_{P\to\infty} C_{AWGN} = \{\frac{1}{2}\log(b/g)\}^{+}$

Bob must have a better channel than Eve for nonzero secret rates

Recent Work on Information Theoretic Secrecy

- Channel models:
  - Parallel channels: Li06
  - Fading: Barros06, Liang06, Gopala07, Li07, Tang07, Tang09
  - MIMO: Khisti07, Shafiee07, Li07, Parada05, Hero03, Negi03, Liu09
  - Feedback: Lai07, Tang07, Ekrem08
- Transmitter CSI assumptions
  - Non-causal CSI: Mitrpant06, Chen07
  - Unknown eavesdropper CSI: Lai07, Li07, Negi05
  - No CSI: Tang07
- Multiple users
  - Relay/helper: Lai06, Tang08
  - Multi-access channel: Ekrem08,Tang07, Liang07, Tekin07, Liu06
  - Broadcast: Khisti07, Liu07, Liu09
  - Interference channel: Liu08, Yates08, Li08

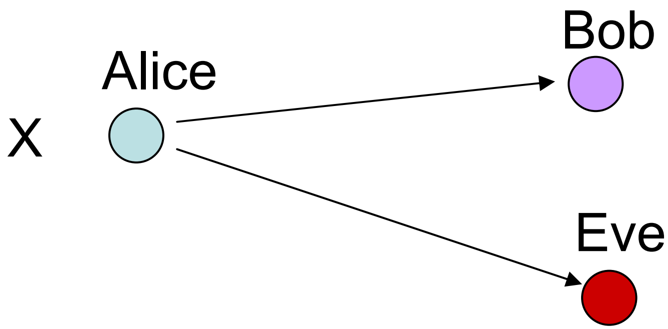
Opportunistic Secret Communication

- Although Eve may have (on average) a better channel …
- Diversity creates opportunities for secret communication
  - OFDM: Frequency Diversity
  - Multiple Antennas: Spatial Diversity
  - **Fading: Temporal Diversity**
- **Nonzero Secrete rates even if Alice & Bob can't observe the opportunities**

The rest of this talk

- Secrecy rate of fast Rayleigh fading channels
  - Alice & Bob don't know Eve's channel
  - Gaussian codes with additive noise and burst strategy can achieve positive secrecy rate even when Eve has an on-average better channel
- Practical signaling (QAM)
  - More power is not always better
  - QAM can perform better than Gaussian for fast Rayleigh fading channels

Gaussian Broadcast Fading Channel



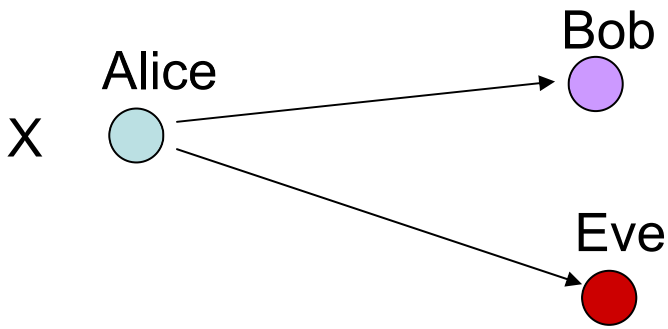
$$Y = \sqrt{B}X + W_1$$

$$Z = \sqrt{G}X + W_2$$

$W_1, W_2 \sim N(0,1)$

- A→B channel gain B is known to Bob, Alice & Eve
- A→E channel gain G is known to Eve
  - but not to Alice or Bob
  - TX can't exploit CSI of A→E channel

Gaussian Broadcast Fast Fading Channel



$$Y = \sqrt{B}X + W_1$$

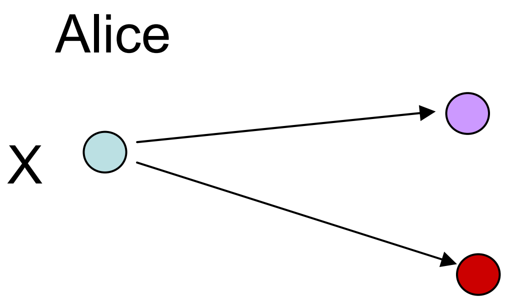
$$W_1, W_2 \sim N(0,1)$$

$$Z = \sqrt{G}X + W_2$$

- The model we are interested in:
  - Channels are fast Rayleigh fading
  - A codeword experiences the ergodic variation of the channel

- Special Case:
  - A→B channel is AWGN with fixed SNR b
  - A→E channel is fast fading with channel gain only known to Eve

Gaussian Broadcast Channel with Fading Eavesdropper



Bob $Y = \sqrt{b}X + W_1$

Eve $Z = \sqrt{G}X + W_2$

AWGN

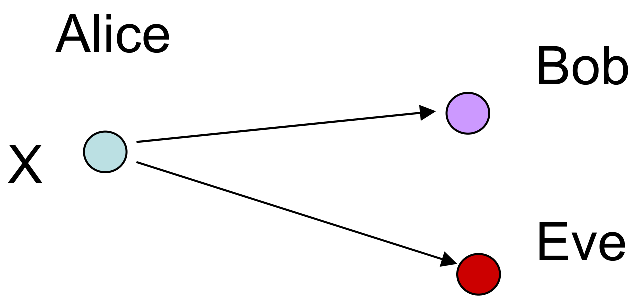
iid fading

- Ergodic Secrecy Capacity (Csiszar-Korner)

$$C_s = \max_{V \to X \to YGZ} I(V;Y) - I(V;Z \mid G)$$

How to choose V and V → X channel?

Gaussian Broadcast Channel (with Fading Eve) Direct Gaussian Input V=X



$$Y = \sqrt{b}X + W_1$$

AWGN SNR = b

$$Z = \sqrt{G}X + W_2$$

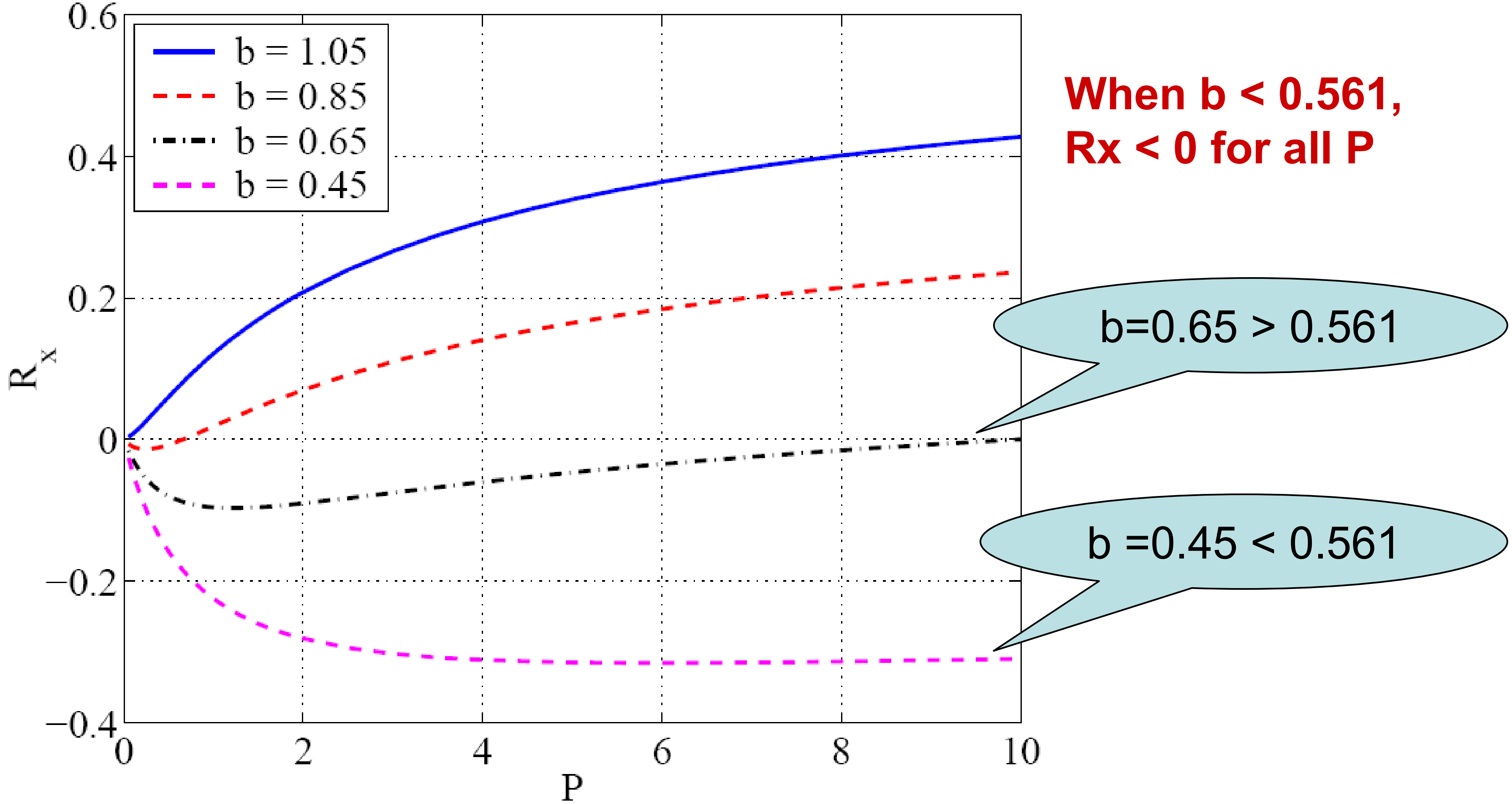
Rayleigh SNR = 1

- b < 1: $\mathrm{SNR}_{\mathrm{Bob}} < \mathrm{SNR}_{\mathrm{Eve}}$
- b > 1: $\mathrm{SNR}_{\mathrm{Bob}} > \mathrm{SNR}_{\mathrm{Eve}}$

$$\begin{aligned} R_x(P,b) &= I(X;Y) - I(X;Z \mid G) \\ &= \log(1+bP) - E[\log(1+GP)] \\ &= \log(1+bP) - e^{1/P} E_1(1/P) \end{aligned}$$

$$E_1(x) = \int_x^{\infty} \frac{e^{-t}}{t} dt$$

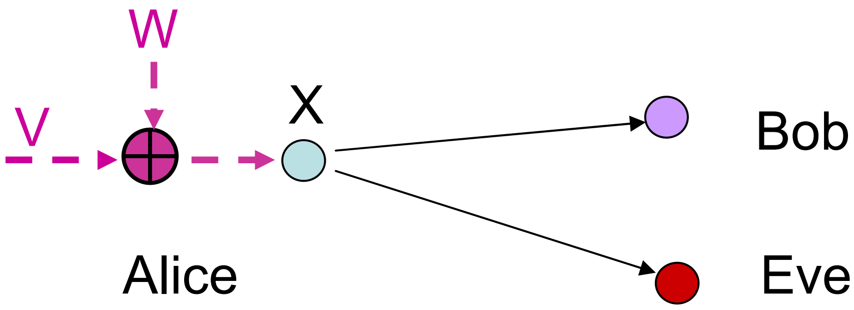
Achievable Positive Secrecy Rates $R_X(P)$ (Rayleigh Fading Eve)



When b < 0.561, Rx < 0 for all P

Artificial Noise Injection: X=V+W

- Preprocessing Channel
  - Artificial AWGN: $X = V + W_i$



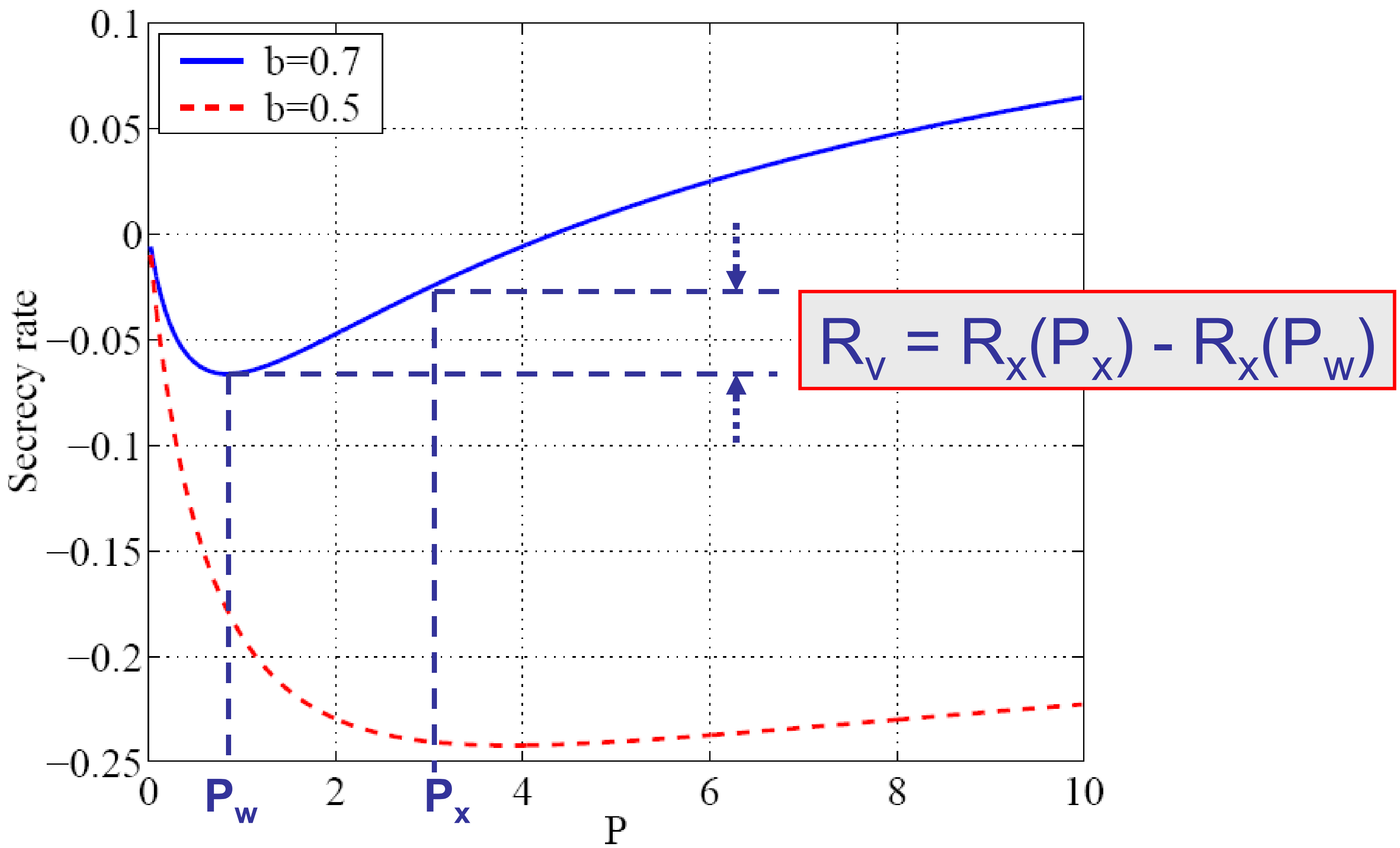
$$Y_i = \sqrt{b}V_i + \sqrt{b}W_i + W_{1,i},$$

$$Z_i = \sqrt{G_i}V_i + \sqrt{G_i}W_i + W_{2,i}$$

$$\begin{aligned}\mathcal{R}_v &= I(V;Y) - I(V;Z|G)\\ &= R_x(P_w + P_v) - R_x(P_w)\\ &= R_x(P_x) - R_x(P_w).\end{aligned}$$

$$\boxed{P_W < P_X \leq P}$$

Artificial Noise Injection



WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

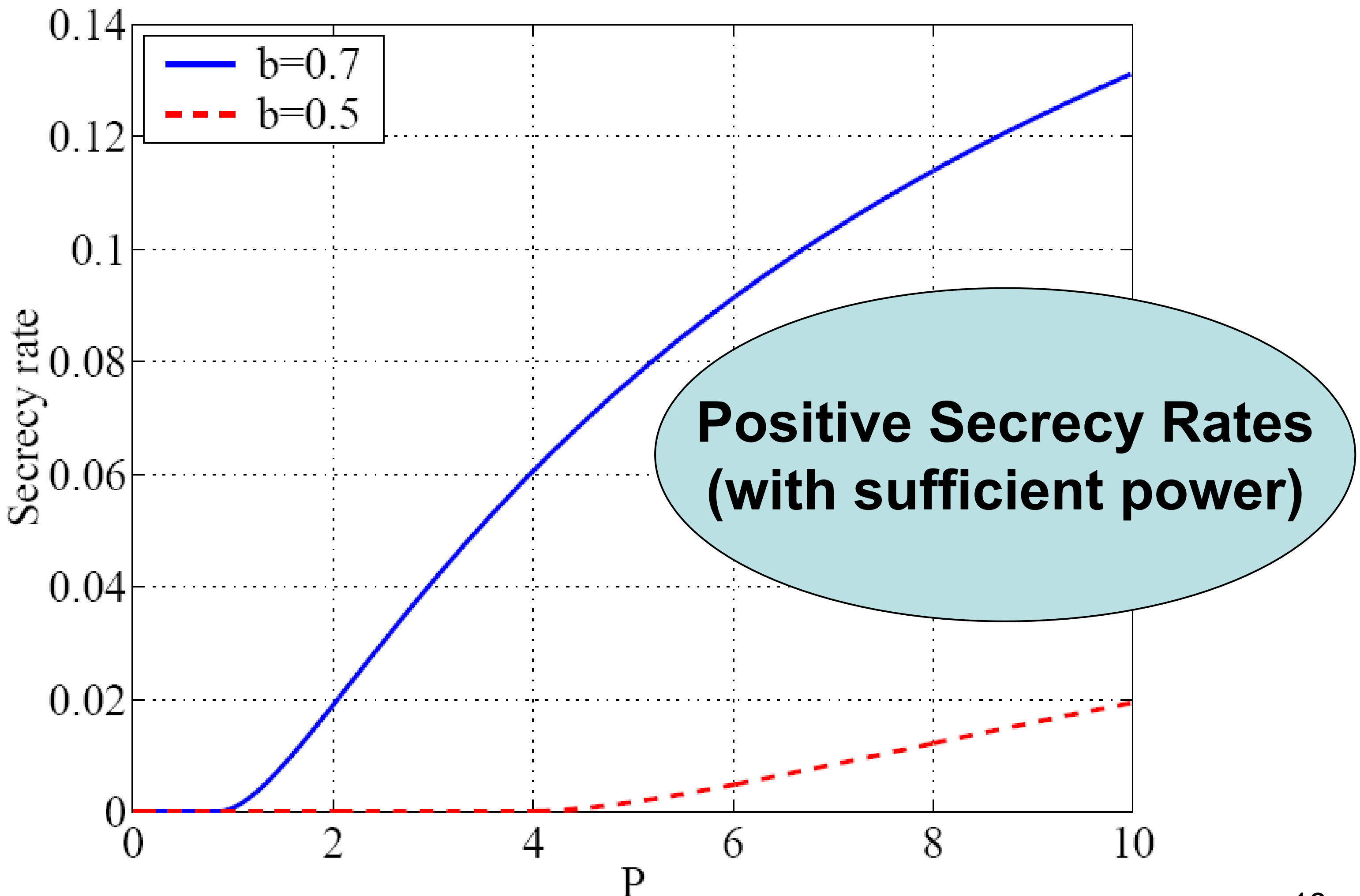
Artificial Noise Injection

- There always exists P_W such that $R_X(P_W) < 0$
- The optimal P_W^* minimizes $R_X(P)$
- $R_X(P)$ increases for $P > P_W^*$
- So for large enough P, positive secrecy rate is always achievable
  - A rule of thumb: $P > \exp(\gamma + 1/b)$ guarantees $R_X(P) - R_X(P_W^*) > 0$

    ($\gamma = 0.57721566$ □ □ □ is the Euler-Mascheroni constant)

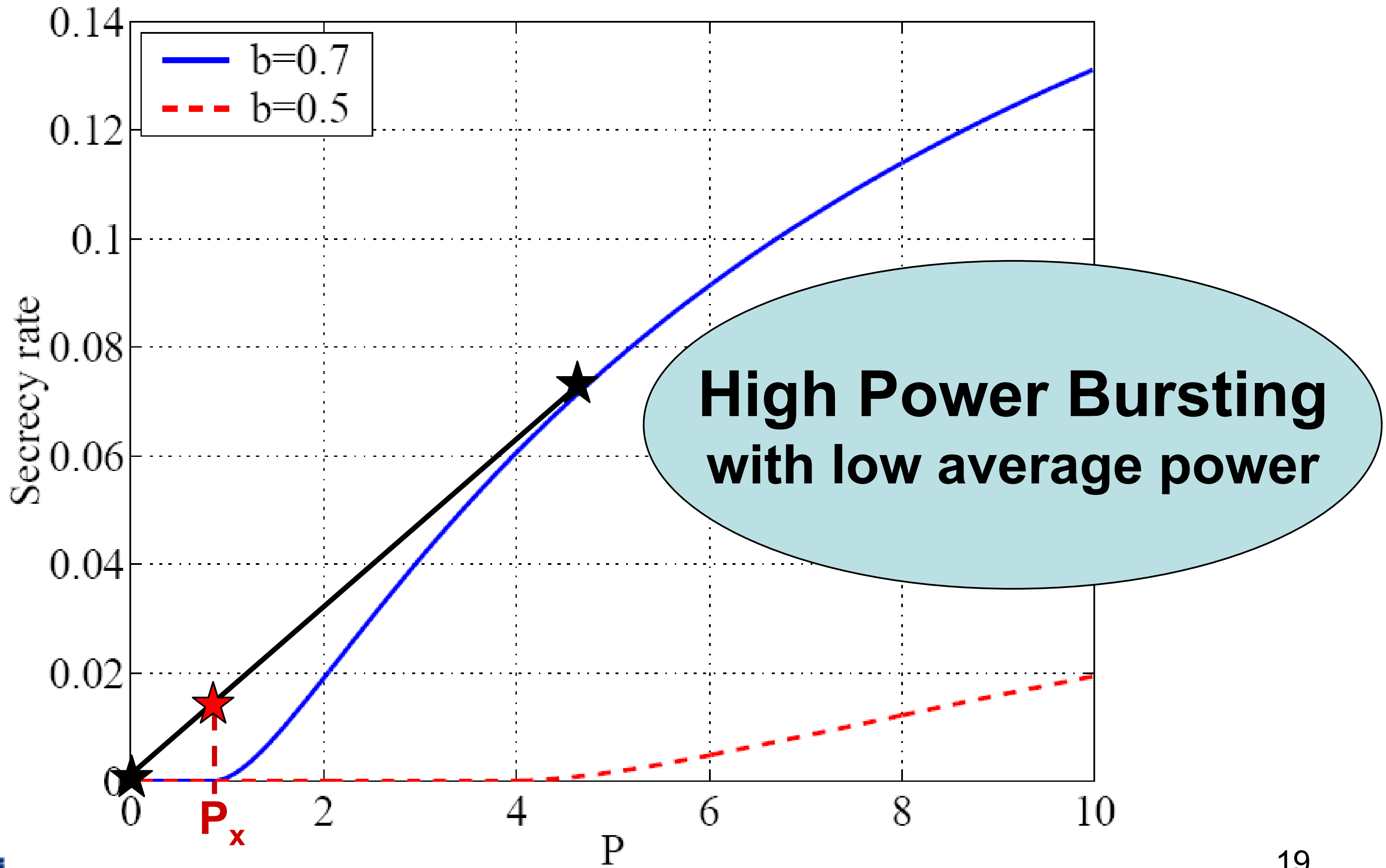
- **Intuition:**
  - **Artificial noise limits Eve's SNR**
    - **even if Eve's channel is very good**

Achievable Secrecy Rates (Fading Eve + Artificial Noise Injection)

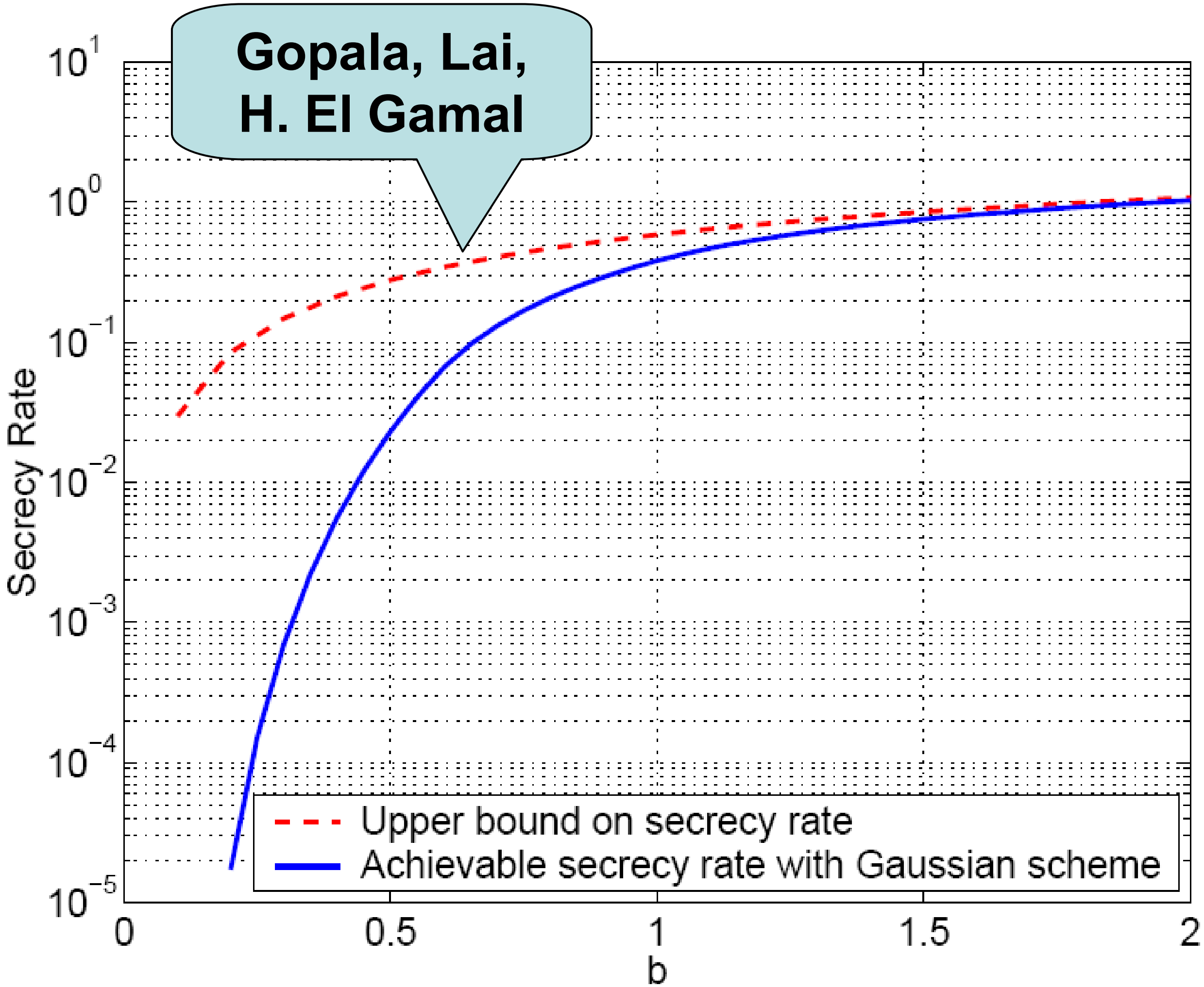


WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Achievable Secrecy Rates
(Fading Eve + Artificial Noise Injection + Bursting)



Achievable Secrecy Rate (P=10)



Summary

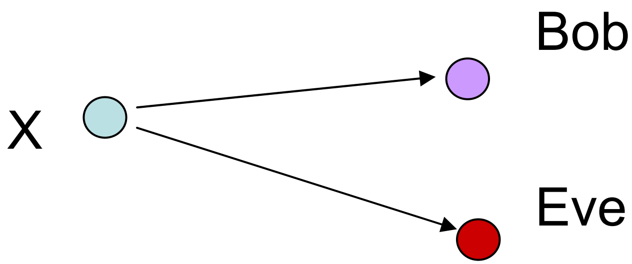
- Achievable secrecy rates
  - constant main channel
  - fast Rayleigh fading eavesdropper’s channel
  - Methods:
    - Artificial noise
    - Bursting

- Although Bob’s channel can be much worse than Eve’s average channel, positive secrecy rate is always achievable
- Insight: Artificial Noise restricts Eve’s ability to overhear when her SNR is very high

Practical Discrete Signaling (QAM)

- Gaussian random codes cannot be implemented in practical systems
- Study the effect of discrete signaling on secret communication rate
  - For conventional communication, larger power and larger constellation are always better
  - How about for secret communication?
- Evaluate the achievable secret communication rate with Quadrature Amplitude Modulation (QAM)

Achievable Rate for AWGN

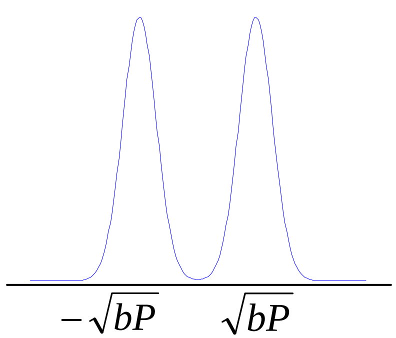


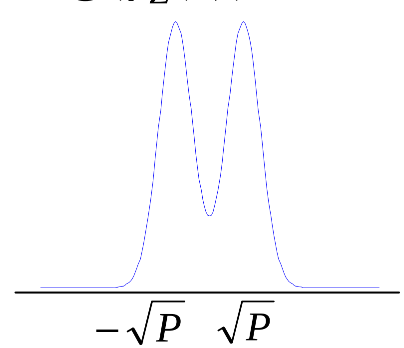
$$Y = \sqrt{b}X + W_1$$

$$Z = X + W_2$$

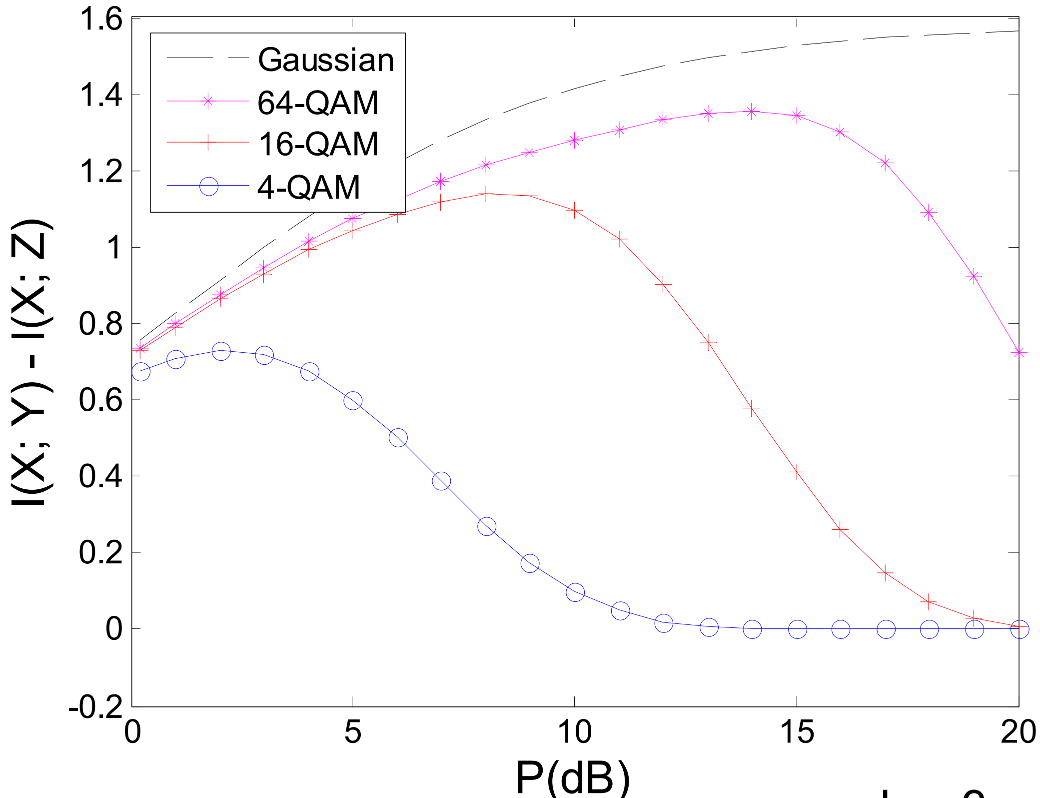
- Achievable rate

$$R = I(X;Y) - I(X;Z)$$
$$= H(Y) - H(Z)$$
$$= -\int_{-\infty}^{\infty} f(y)\log(f_Y(y))\,dy + \int_{-\infty}^{\infty} f(z)\log(f_Z(z))\,dz$$





Achievable Rate for AWGN Channels

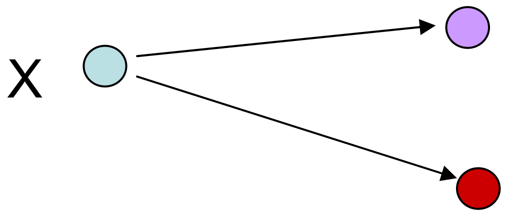


b = 3

- Optimal P* for each QAM constellation

WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Achievable Rate for Fast Fading Channels



Bob $Y = \sqrt{b}X + W_1$

Eve $Z = \sqrt{G}X + W_2$

AWGN

iid fading

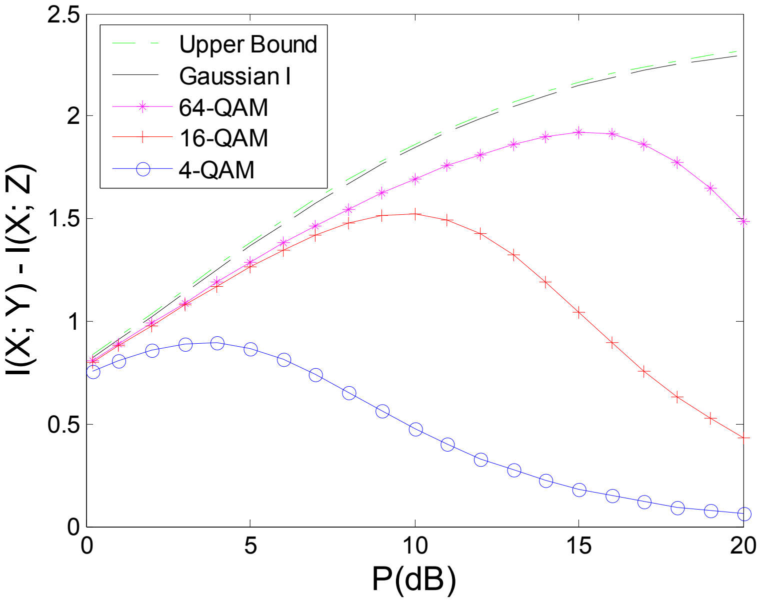
- Achievable rate

$$
\begin{aligned}
R &= I(X;Y) - I(X;GZ) \\
&= H(Y) - H(Z \mid G) \\
&= -\int_{-\infty}^{\infty} f(y)\log(f_Y(y))\,dy + \int_{0}^{\infty} f_G(g)\int_{-\infty}^{\infty} f_Z(z)\log(f_Z(z))\,dz\,dg
\end{aligned}
$$

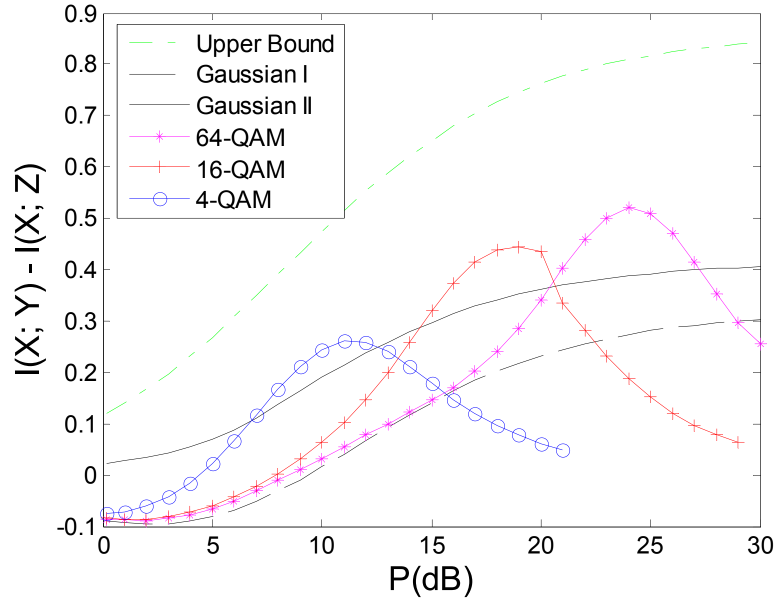
WINLAB WIRELESS INFORMATION NETWORK LABORATORY

Achievable Rate for Fast Fading Channels

b = 3



b = 0.7



QAM outperforms Gaussian schemes when Bob’s channel is on average worse than Eve’s channel

– QAM limits the information leakage when Eve’s channel is better

WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Conclusion

- Information theoretic secret communication can be facilitated by the wireless fading
  - Even if Alice and Bob can’t track Eve’s channel

- Practical signaling is discrete
  - More power is not always better
  - QAM can perform better than Gaussian for fast Rayleigh fading channels