Information Theoretic Security: Fundamentals and Applications

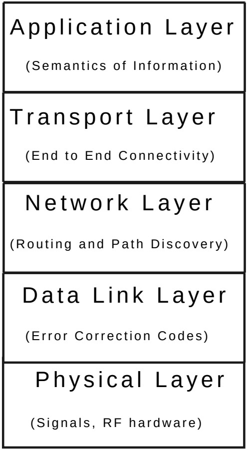
Ashish Khisti

University of Toronto

IPSI Seminar
Nov 25th 2013

Layered Architectures

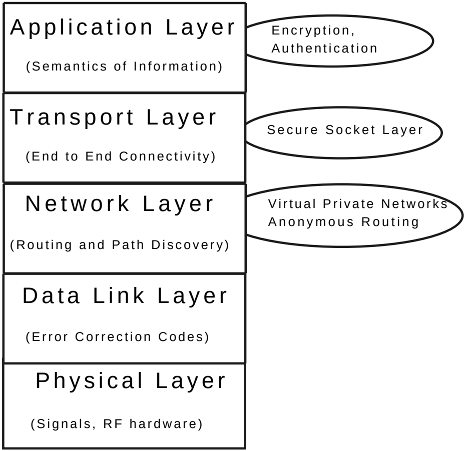
Layered architecture for communication systems.



Where is Security?

Layered Architectures

Layered architecture for communication systems.



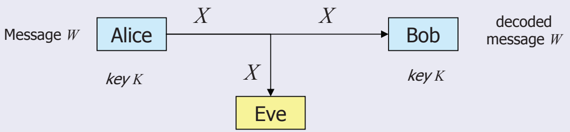
Where is Security?

Wireless Systems

Traditional Approach

A typical graduate level course in computer security introduces Shannon's notion of security.

Shannon's Notion



Perfect Secrecy: $p(w|x)=p(w)$

- Note that Key Size = Message length, hence impractical
- Focus: computational cryptography

Is this all about information theoretic security?

Outline

- Motivating Applications
  - Secure Biometrics
  - Smart-Meter Privacy
  - Wireless Systems
- Information Theoretic Models
  - Wiretap Channel Model
  - Secret-key agreement

Biometric Technologies

Laptop

ATM

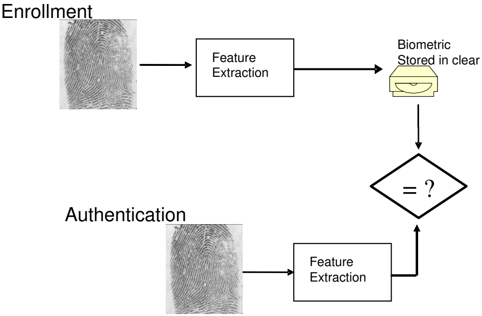
Passport

Biometric Technologies

Laptop

ATM

Passport

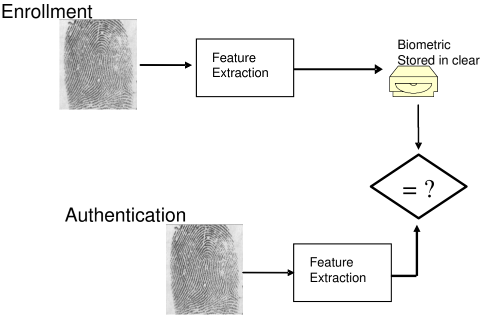


Biometric Technologies

Laptop

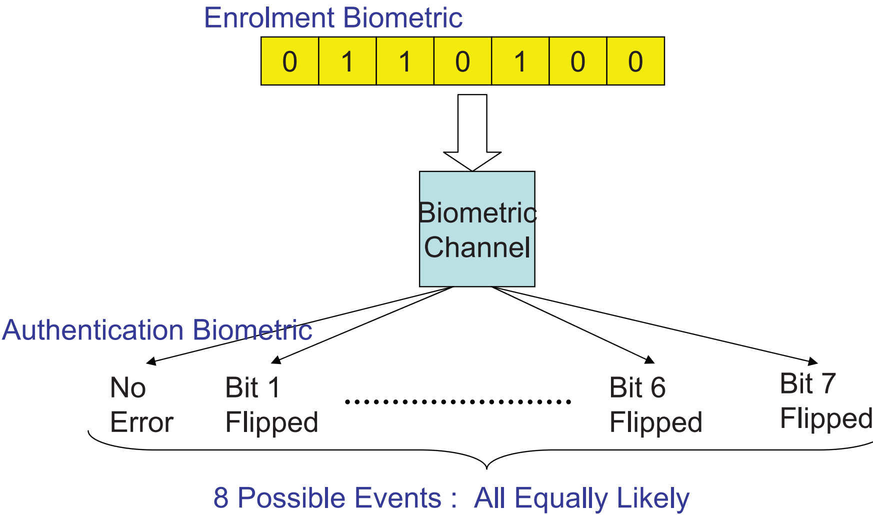
ATM

Passport



Issue: Biometrics are stored in the clear

Biometrics: Toy Example

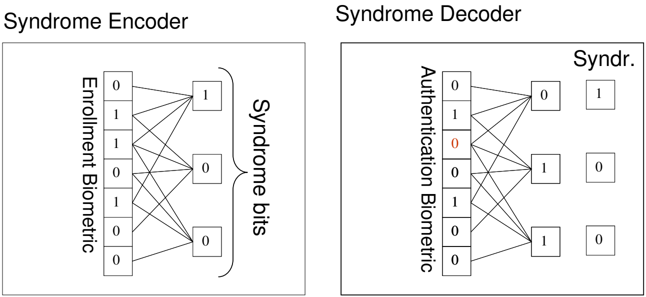


Biometrics: Toy Example

- **X**, **Y** : length seven binary sequence
- Channel Model: one bit flip (8 possibilities)
- 3 bits required.

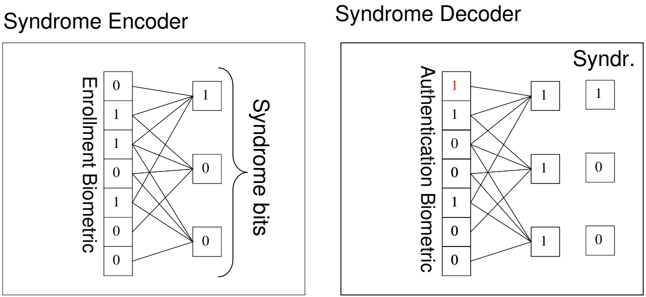
Biometrics: Toy Example

- **X**, **Y** : length seven binary sequence
- Channel Model: one bit flip (8 possibilities)
- 3 bits required.



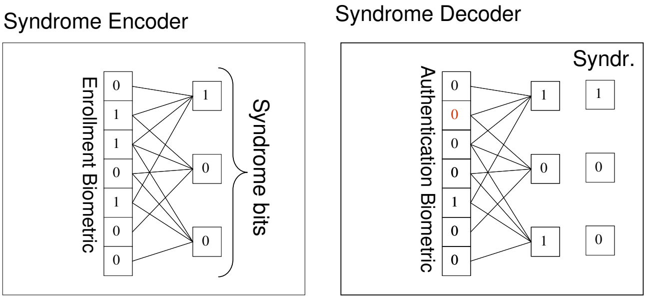
Biometrics: Toy Example

- **X**, **Y** : length seven binary sequence
- Channel Model: one bit flip (8 possibilities)
- 3 bits required.



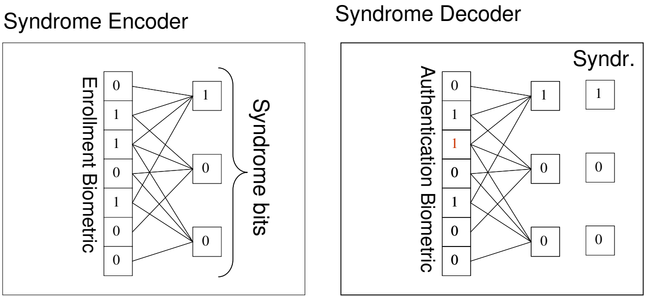
Biometrics: Toy Example

- **X**, **Y** : length seven binary sequence
- Channel Model: one bit flip (8 possibilities)
- 3 bits required.



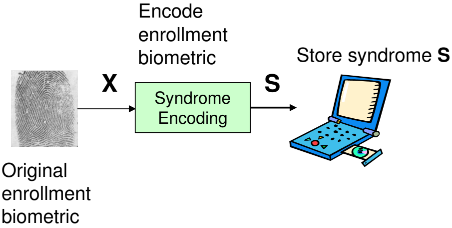
Biometrics: Toy Example

- **X**, **Y** : length seven binary sequence
- Channel Model: one bit flip (8 possibilities)
- 3 bits required.



Privacy Preserving Biometrics

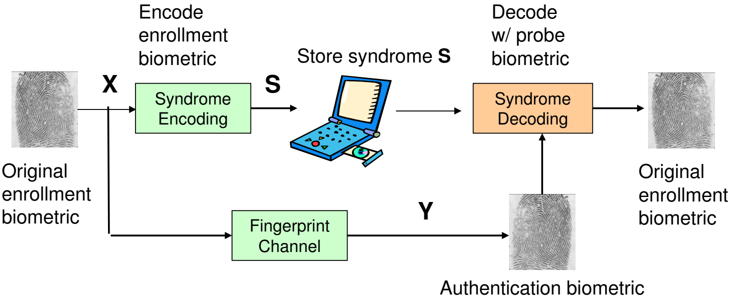
S. Draper, A. Khisti, et. al "Using distributed source coding to secure fingerprint biometrics" ICASSP, 2007



- Store syndromes

Privacy Preserving Biometrics

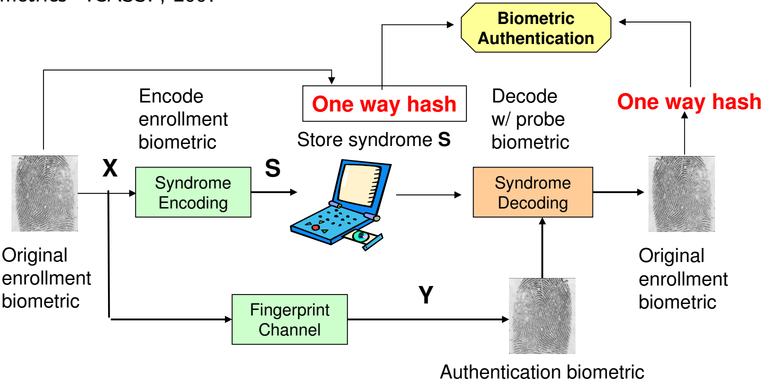
S. Draper, A. Khisti, et. al "Using distributed source coding to secure fingerprint biometrics" ICASSP, 2007



- Store syndromes
- Reproduce enrollment biometric

Privacy Preserving Biometrics

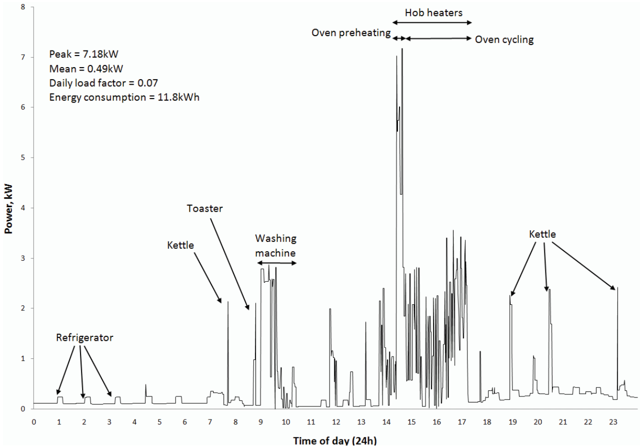
S. Draper, A. Khisti, et. al "Using distributed source coding to secure fingerprint biometrics" ICASSP, 2007



- Store syndromes
- Reproduce enrollment biometric
- Authenticate

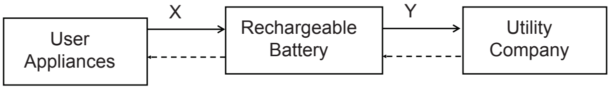
Smart-Meter Privacy

D. Varodayan and A Khisti, ICASSP 2011



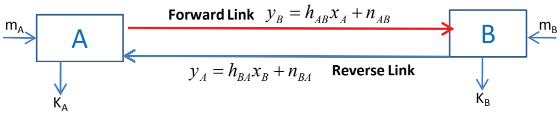
C. Efthymiou and G. Kalogridis, Smart grid privacy via anonymization of smart metering data, Smart Grid Commun. Conf., Gaithersburg, 2010.

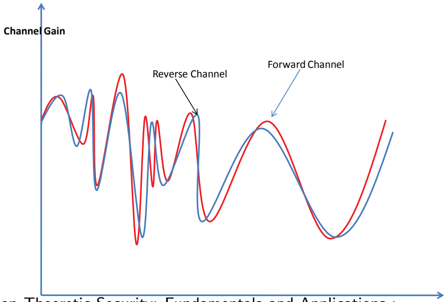
Smart-Meter Privacy
D. Varodayan and A Khisti, ICASSP 2011



- Privacy Leakage: $I(X^N; Y^N)$
- Battery: Limited Storage
- Model Battery as a Finite State Communication Channel
- "Design the Channel"

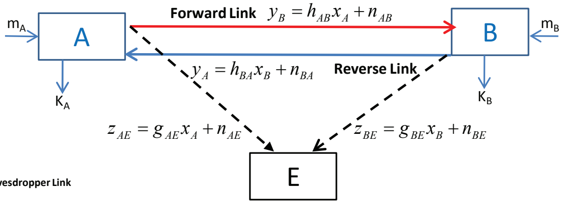
Secret-Key Generation in Wireless Fading Channels

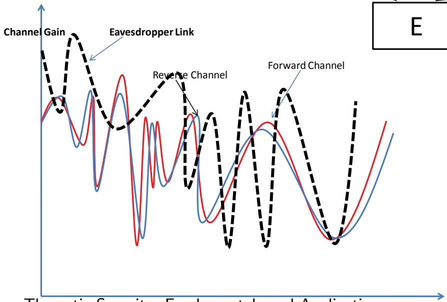




- Fading
- Reciprocity
- Spatial Decorrelation

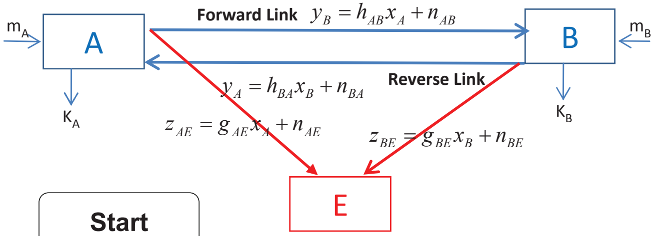
Secret-Key Generation in Wireless Fading Channels

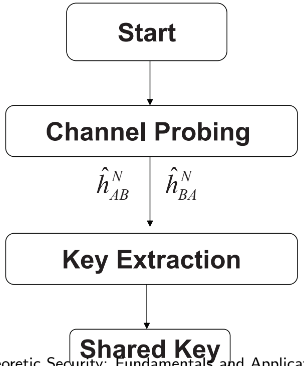




- Fading
- Reciprocity
- Spatial Decorrelation

Secret-Key Generation in Wireless Fading Channels
A. Khisti 2013



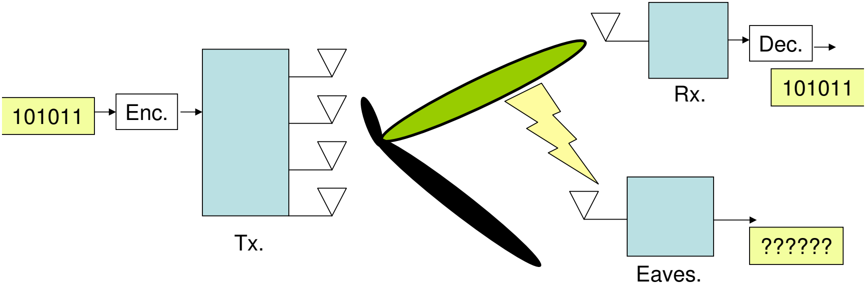


Two Phase Approach:

- **Phase I**: Channel Probing and Estimation: $(\hat{h}_{AB}^N, \hat{h}_{BA}^N)$
- **Phase 2**: Source Reconciliation and Key Extraction

Secret-Key Generation: Capacity Limits

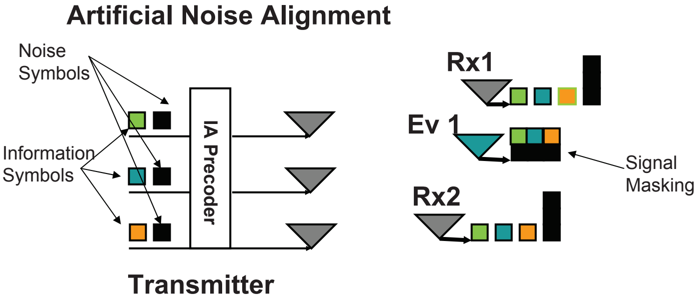
Secure MIMO Communication



- Signal of interest: direction of legitimate receiver.
- Synthetic noise: null-space of legitimate receiver.

Secure MIMO Multicast

A. Khisti, 2011



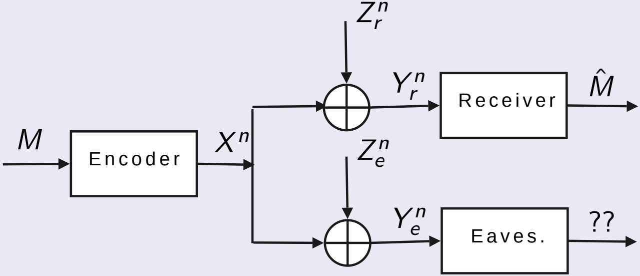
- Align Noise Symbols at Legitimate Receivers
- Mask Information Symbols at Eavesdroppers

Outline

- Motivating Applications
  - Secure Biometrics
  - Smart-Meter Privacy
  - Wireless Systems
- Information Theoretic Models
  - Wiretap Channel Model
  - Secret-key agreement

Wiretap Channel
Wyner'75

AWGN Wiretap Channel Model



- Reliability Constraint : $\Pr(M \neq \hat{M}) \xrightarrow{n} 0$
- Secrecy Constraint : $\frac{1}{n}H(M|Y_e^n) = \frac{1}{n}H(M) - o_n(1)$

Secrecy Capacity

Secrecy Criterion

$$\underbrace{\frac{1}{n}H(M|Y_e^n)}_{\substack{\text{Equivocation}\\\text{rate}}} = \underbrace{\frac{1}{n}H(M)}_{\substack{\text{Information}\\\text{rate}}} - o_n(1)$$

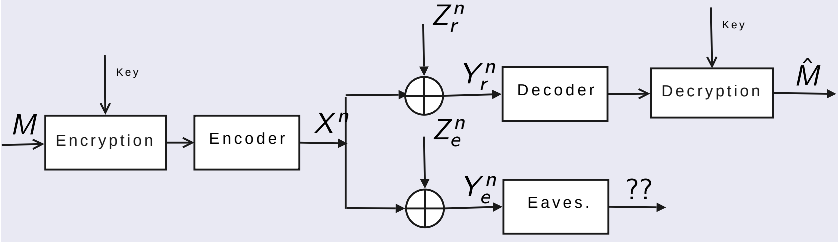
- Perfect Secrecy: $o_n(1) \equiv 0$, (Shannon '49)
- Weak Secrecy: $o_n(1) \xrightarrow{n} 0$, (Wyner '75)
- Strong Secrecy: $o_n(1) \in O\left(\frac{1}{n}\right)$, (Maurer and Wolf '00)
- Guessing approach : (Arikan & Merhav '02)

Focus: Wyner's notion

Joint Encryption and Encoding

Separation based approach vs. Wiretap codes

Traditional Approach : Separation ...



Traditional Approach

- Separation based
- Requires keys

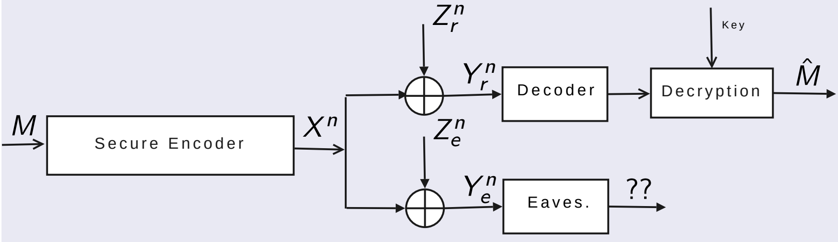
Wiretap Codes

- Joint encryption/encoding
- Channel based secrecy

Joint Encryption and Encoding

Separation based approach vs. Wiretap codes

Wiretap Codes: Joint Encryption and Encoding



Traditional Approach

- Separation based
- Requires keys

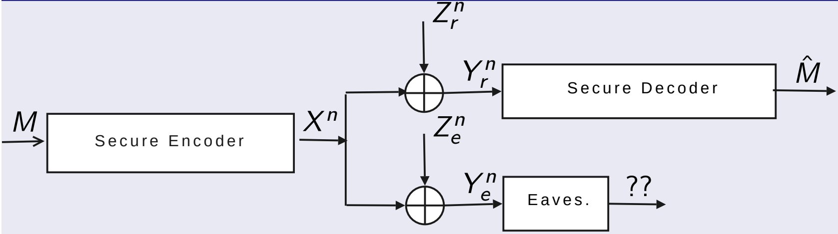
Wiretap Codes

- Joint encryption/encoding
- Channel based secrecy

Joint Encryption and Encoding

Separation based approach vs. Wiretap codes

Wiretap Codes: Joint Encryption and Encoding



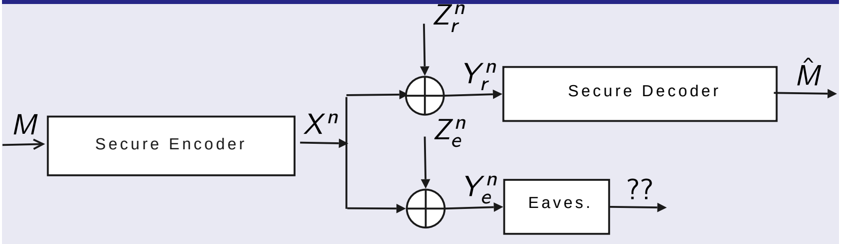
Traditional Approach

- Separation based
- Requires keys

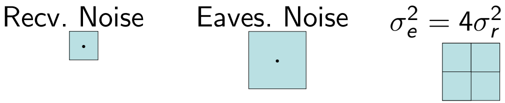
Wiretap Codes

- Joint encryption/encoding
- Channel based secrecy

Uniform Noise Wiretap Channel Model

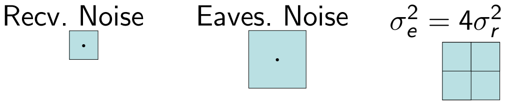


- QAM Modulation
- Uniform noise model
- $\sigma_e^2 = 4\sigma_r^2$



Wiretap Codes

- QAM Modulation
- Uniform noise model

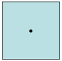


Wiretap Codes

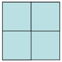
- QAM Modulation
- Uniform noise model

Recv. Noise

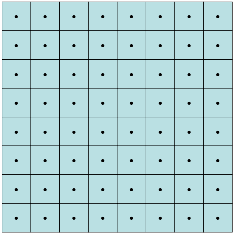
Eaves. Noise



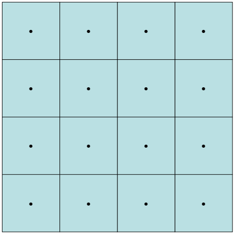
$\sigma_e^2 = 4\sigma_r^2$



Receiver's Constellation



Eavesdropper's Constellation



$C_r = \log_2 64 = 6$ b/s

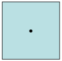
$C_e = \log_2 16 = 4$ b/s

Wiretap Codes

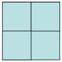
- QAM Modulation
- Uniform noise model

Recv. Noise

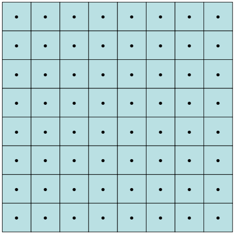
Eaves. Noise



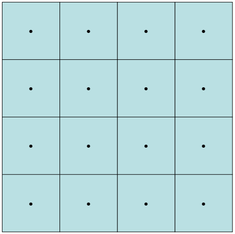
$\sigma_e^2 = 4\sigma_r^2$



Receiver's Constellation



Eavesdropper's Constellation



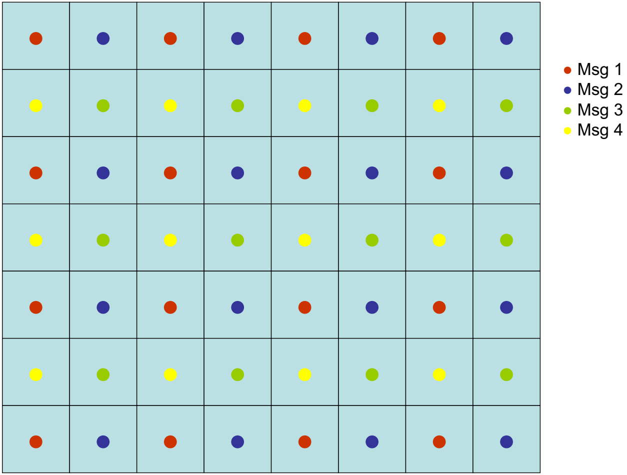
$C_r = \log_2 64 = 6$ b/s

$C_e = \log_2 16 = 4$ b/s

$\mathbf{C_s = C_r - C_e = 2}$ b/s

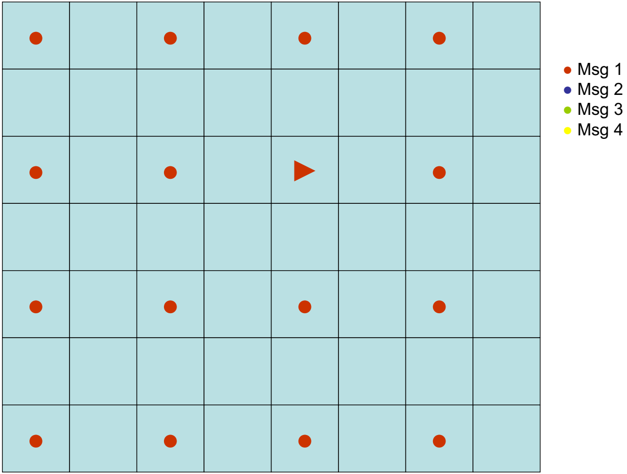
Wiretap Codes

Secure QAM Constellation



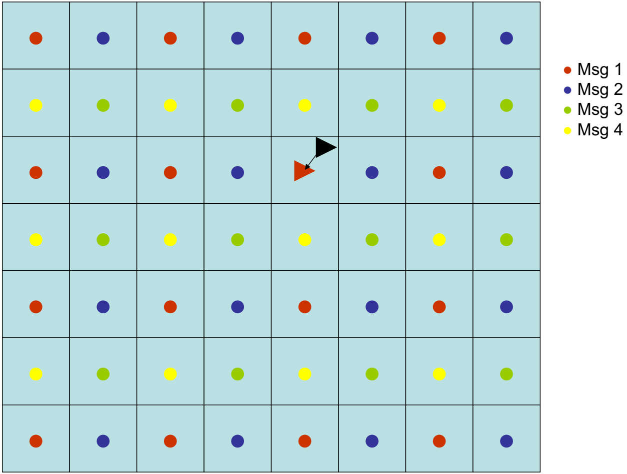
Wiretap Codes

Encoding: Randomly select one candidate



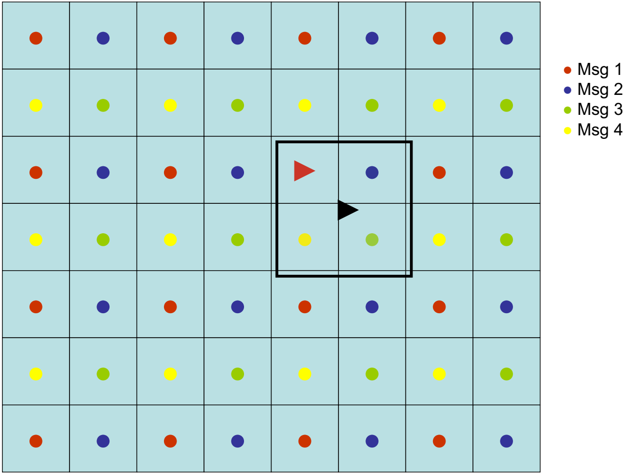
Wiretap Codes

Decoding at legitimate receiver



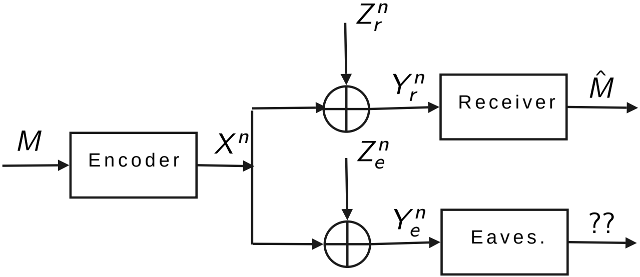
Wiretap Codes

Confusion at the eavesdropper



Gaussian Wiretap Channel

Leung-Yan-Cheong and Hellman'78



Secrecy Capacity

$$
\begin{aligned}
C_s &= \{\log(1 + SNR_r) - \log(1 + SNR_e)\}^+ \\
&= \{C(SNR_r) - C(SNR_e)\}^+
\end{aligned}
$$

- SNR_r: Legitimate receiver's signal to noise ratio
- SNR_e: Eavesdropper's signal to noise ratio

Other Classical Results

The secrecy capacity was also characterized for:

- Degraded Memoryless Wiretap Channel(Wyner'75)
  $X \to Y_r \to Y_e$

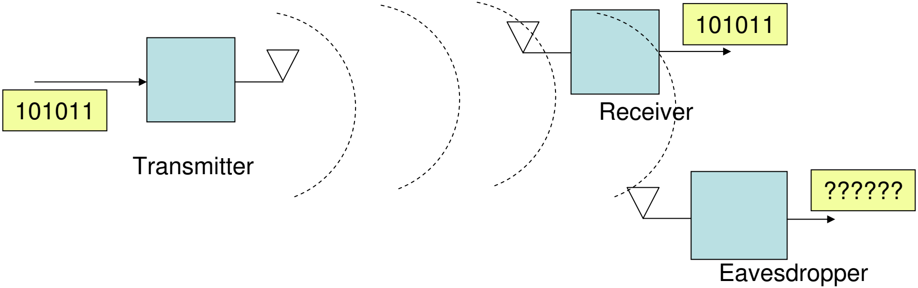
$$C = \max_{p_X} I(X; Y_r) - I(X; Y_e)$$

- Discrete Memoryless Wiretap Channel (Csiszar-Korner '78)

$$C = \max_{p_{U,X}} I(U; Y_r) - I(U; Y_e),$$

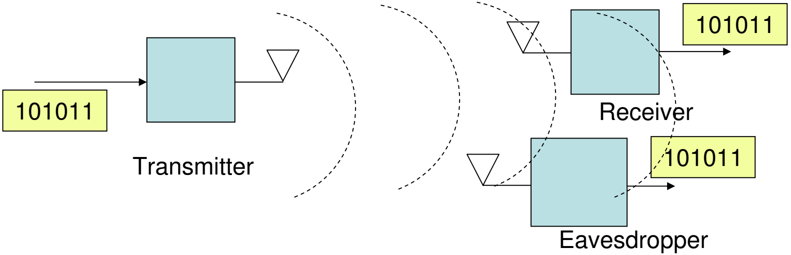
  $U \to X \to (Y_r, Y_e)$
  Cardinality bounds on the alphabet of U

Gaussian Wiretap Channel



Strong Requirement: Eavesdropper must not be closer to the transmitter

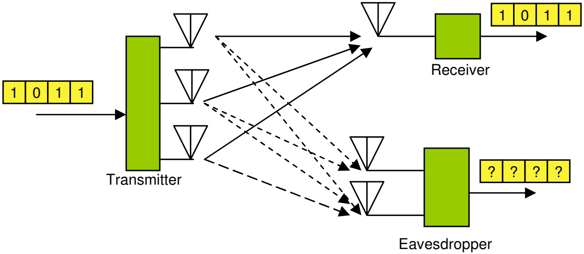
Gaussian Wiretap Channel



Strong Requirement: Eavesdropper must not be closer to the transmitter

Solution ... Multiple Antennas
Khisti-Wornell 2010

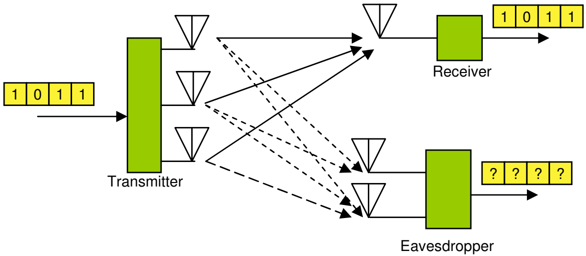
Multi-antenna wiretap channel



- Spatial Diversity: Multiple Antennas
- Temporal Diversity: Fading Channels

Solution ... Multiple Antennas
Khisti-Wornell 2010

Multi-antenna wiretap channel



Channel Model

$$Y_r = H_r X + Z_r$$
$$Y_e = H_e X + Z_e$$

- Channel matrices: $H_r \in \mathbb{C}^{N_r \times N_t}$, $H_e \in \mathbb{C}^{N_e \times N_t}$
- N_t: # Tx antennas
- AWGN noise: Z_r, Z_e

MIMOME: Secrecy Capacity

Khisti-Wornell 2010

Theorem

Secrecy capacity of the Multi-antenna wiretap channel is given by,

$$C_s = \max_{Q \succeq 0 : Tr(Q) \leq P} \log\det(I_r + H_r Q H_r^\dagger) - \log\det(I_e + H_e Q H_e^\dagger)$$

MIMOME: Secrecy Capacity

Khisti-Wornell 2010

Theorem

Secrecy capacity of the Multi-antenna wiretap channel is given by,

$$C_s = \max_{Q \succeq 0 : Tr(Q) \leq P} \log\det(I_r + H_r Q H_r^\dagger) - \log\det(I_e + H_e Q H_e^\dagger)$$

Scalar Gaussian Case (Leung-Yan-Cheong & Hellman '78),

$$C_s = \log(1 + SNR_r) - \log(1 + SNR_e)$$

- New information theoretic upper-bound
- Convex Optimization
- Matrix Analysis

Secrecy Capacity: Remarks

$$C_s = \max_{Q \succeq 0 : Tr(Q) \leq P} \log\det(I_r + H_r Q H_r^\dagger) - \log\det(I_e + H_e Q H_e^\dagger)$$

Secrecy Capacity: Remarks

$$C_s = \max_{Q \succeq 0 : Tr(Q) \leq P} \log\det(I_r + H_r Q H_r^\dagger) - \log\det(I_e + H_e Q H_e^\dagger)$$

1. Convex Reformulation

$$C_s = \min_{\Phi \in \mathcal{P}} \max_{Q \in \mathcal{Q}} R_+(\Phi, Q)$$

Secrecy Capacity: Remarks

$$C_s = \max_{Q \succeq 0 : Tr(Q) \leq P} \log\det(I_r + H_r Q H_r^\dagger) - \log\det(I_e + H_e Q H_e^\dagger)$$

1. Convex Reformulation

$$C_s = \min_{\Phi \in \mathcal{P}} \max_{Q \in \mathcal{Q}} R_+(\Phi, Q)$$

2. MISOME Case: rank-one covariance is optimal

$$C_s = \log^+ \lambda_{\max}(I + P h_r h_r^\dagger, I + P H_e^\dagger H_e)$$

Secrecy Capacity: Remarks

$$C_s = \max_{Q \succeq 0 : Tr(Q) \leq P} \log\det(I_r + H_r Q H_r^\dagger) - \log\det(I_e + H_e Q H_e^\dagger)$$

1. Convex Reformulation

$$C_s = \min_{\Phi \in \mathcal{P}} \max_{Q \in \mathcal{Q}} R_+(\Phi, Q)$$

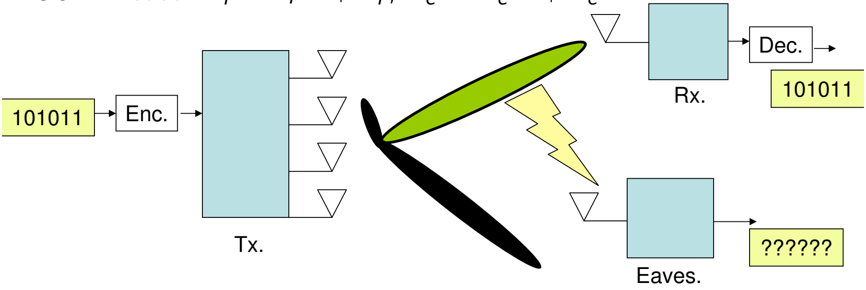
2. MISOME Case: rank-one covariance is optimal

$$C_s = \log^+ \lambda_{\max}(I + P h_r h_r^\dagger, I + P H_e^\dagger H_e)$$

3. High SNR case: GSVD transform
   Simultaneous diagonalization: (H_r, H_e)

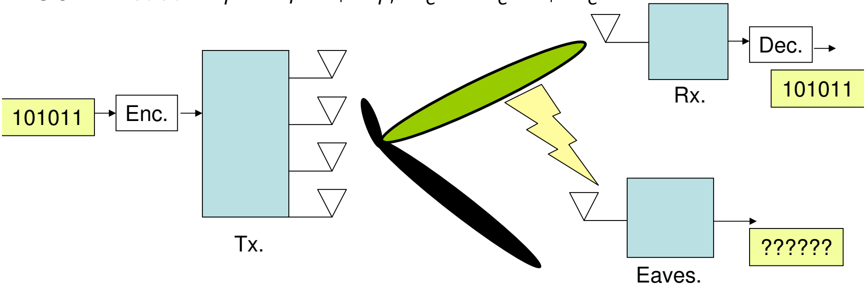
Masked Beamforming Scheme

MISOME Case: $Y_r = h_r^\dagger X + Z_r,\ Y_e = H_e X + Z_e$



Masked Beamforming Scheme

MISOME Case: $Y_r = h_r^\dagger X + Z_r, \; Y_e = H_e X + Z_e$

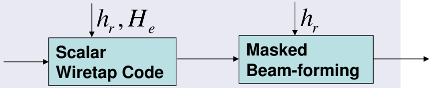


- Signal of interest: direction of legitimate receiver.
- Synthetic noise: null-space of legitimate receiver.

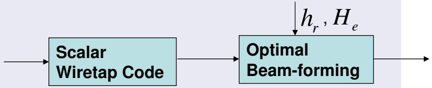
Masked Beamforming vs. Capacity Achieving Scheme

MISOME Case: $Y_r = h_r^\dagger X + Z_r,\ Y_e = H_e X + Z_e$

Masked beamforming scheme



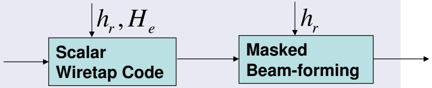
Capacity achieving scheme



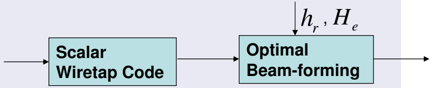
Masked Beamforming vs. Capacity Achieving Scheme

MISOME Case: $Y_r = h_r^\dagger X + Z_r, \; Y_e = H_e X + Z_e$

Masked beamforming scheme



Capacity achieving scheme



$$\lim_{P\to\infty} \left\{ C\left(h_r, H_e, \frac{P}{N_t}\right) - R_{\mathrm{MB}}(h_r, H_e, P) \right\} = 0$$

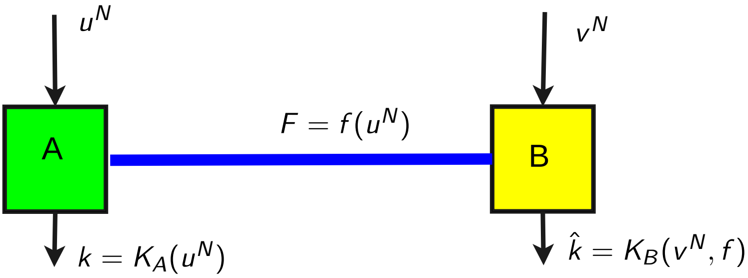
- Transmit Power: P
- Transmit antennas: N_t

Outline

- Motivating Applications
  - Secure Biometrics
  - Smart-Meter Privacy
  - Wireless Systems
- Information Theoretic Models
  - Wiretap Channel Model
  - Secret-key agreement

Secret Key Generation

Maurer '93, Ahlswede-Csiszar '93

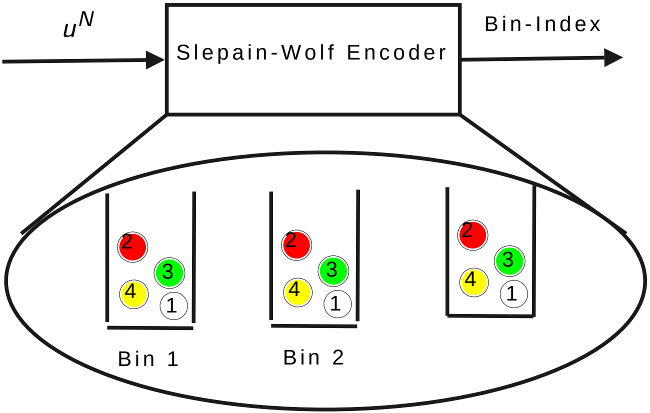


- Error Probability: $\Pr(k \neq \hat{k}) \leq \varepsilon_N$
- Equivocation: $\frac{1}{N} H(k|f) \geq \frac{1}{N} H(k) - \varepsilon_n$
- Rate $R = \frac{1}{N} H(k)$

$$C_{\text{key}} = I(u; v)$$

Achievability

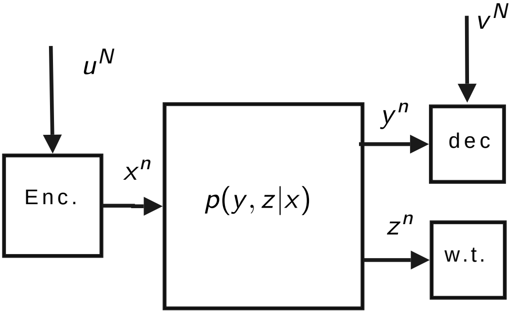
Random Binning Technique (Slepian-Wolf '73)



- No. of Bins: $\approx 2^{nH(v|u)}$
- No. of Sequences/Bin: $\approx 2^{nI(u;v)}$

Joint Source and Channel Coding

Khisti-Diggavi-Wornell '08

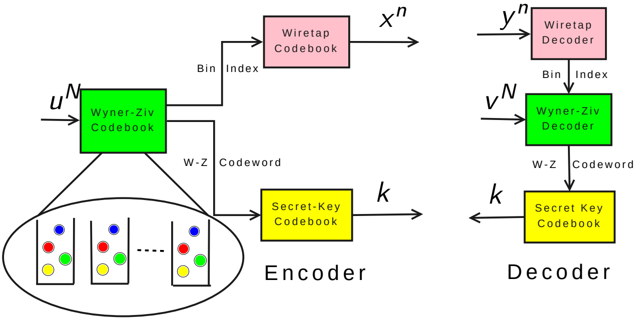


Two types of uncertainty

- Sources
- Channel

How to combine both these equivocation for secret-key-distillation?

Achievability



$$R_{\text{key}} = \max_{t,x} \underbrace{\beta I(t; v)}_{\text{src. equiv.}} + \underbrace{I(x; y) - I(x; z)}_{\text{channel equiv.}}$$

$$t \to u \to v, \quad \beta\{I(t; u) - I(t; v)\} \leq I(x; y)$$

Capacity Results

$$R_{\text{key}} = \max_{t,x} \beta I(t;v) + I(x;y|z)$$

$$t \to u \to v, \quad \beta\{I(t;u) - I(t;v)\} \leq I(x;y)$$

- Upper and lower bounds coincide, when channels are degraded or parallel reversely degraded broadcast.
- Capacity for Parallel Gaussian broadcast channels and Gaussian sources
- Extension to side information at the eavesdropper, when sources and channels are degraded.

Conclusions

- Motivating Applications
  - Secure Biometrics
  - Smart-Meter Privacy
  - Wireless Systems
- Information Theoretic Models
  - Wiretap Channel Model
  - Secret-key agreement