Group Secret Key Agreement over State-Dependent Wireless Broadcast Channels

Mahdi Jafari Siavoshani
Sharif University of Technology, Iran

Shaunak Mishra, Suhas Diggavi, Christina Fragouli

Institute of Network Coding, CUHK, Hong Kong
August 2014

Group Secret Key Agreement over State-Dependent Wireless Broadcast Channels

Mahdi Jafari Siavoshani
Sharif University of Technology, Iran

Shaunak Mishra, Suhas Diggavi, Christina Fragouli

Institute of Network Coding, CUHK, Hong Kong
August 2014

over

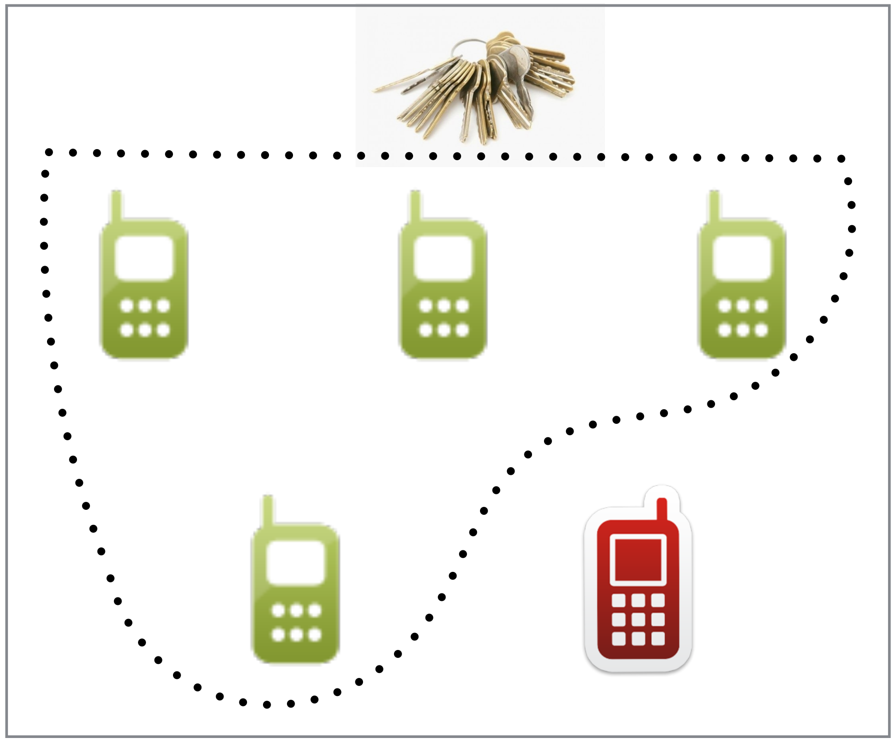
Mahdi Jafari Siavoshani
Sharif University of Technology, Iran

Shaunak Mishra, Suhas Diggavi, Christina Fragouli

Institute of Network Coding, CUHK, Hong Kong
August 2014

Motivation

- Consider m trusted terminals that communicate through a wireless channel
- Goal: Creating a common secret key K, which is concealed from a passive eavesdropper Eve



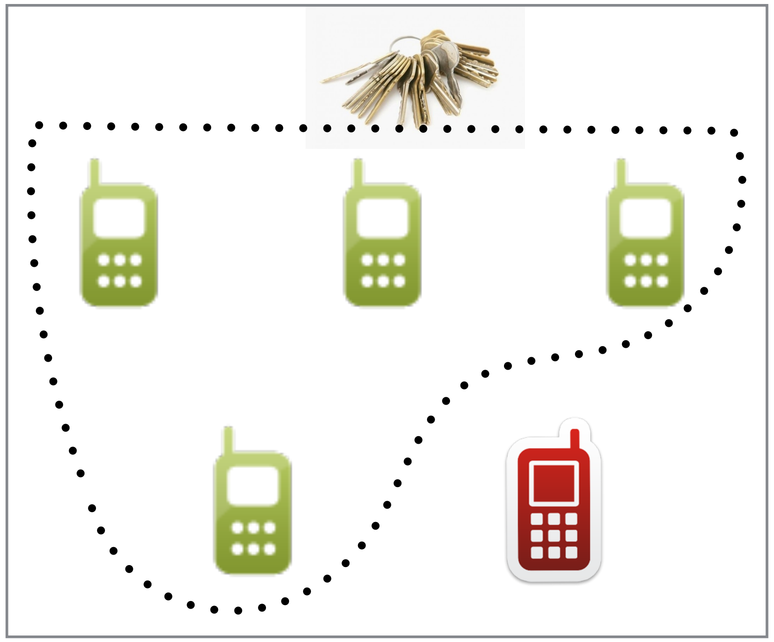
Motivation

- Current Approach: Using public-key cryptography; Based on:
    - Some unproven hardness problems

    - The computational power of Eve is limited

Motivation

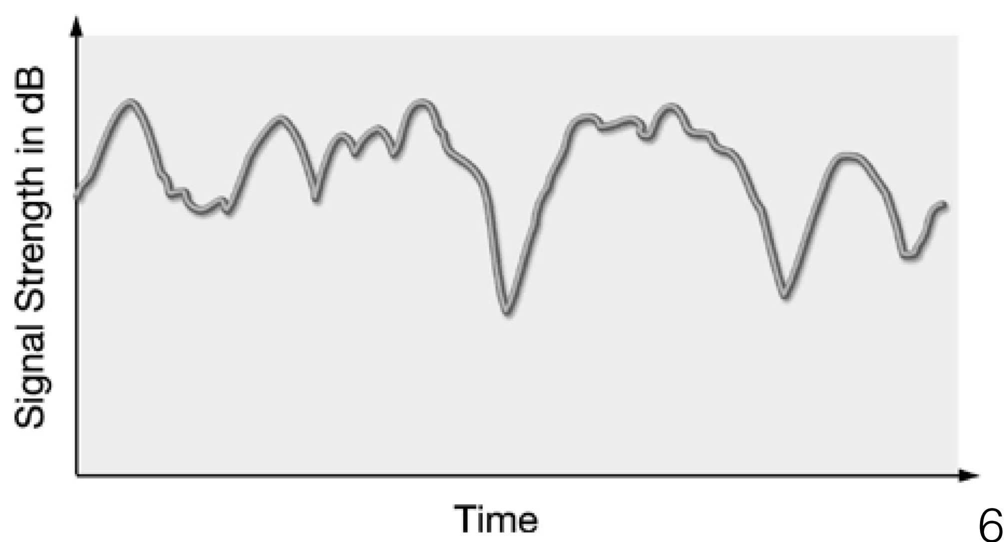
- Alternative Approach: Propose a scheme that guarantees information theoretical secrecy
  - Benefits:
    - It is the strongest notion of secrecy
    - No matter how computationally powerful Eve is, she cannot find any information about the secret key

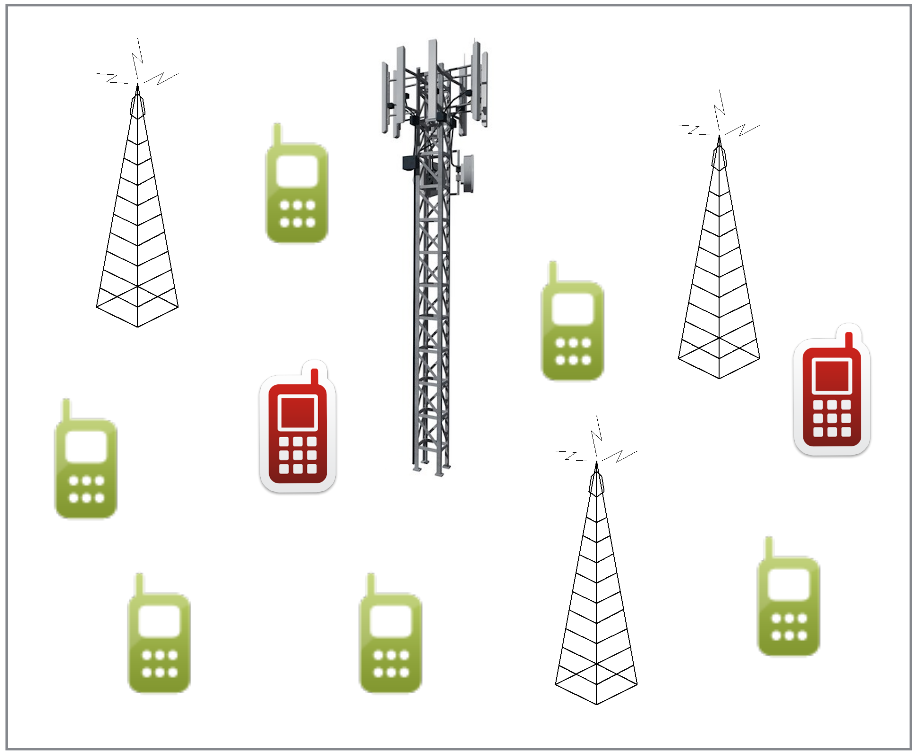


- Disclaimer! (use it at your own risk!) :-)
    - not claiming that this approach is a replacement for the current cryptographic systems

Motivation

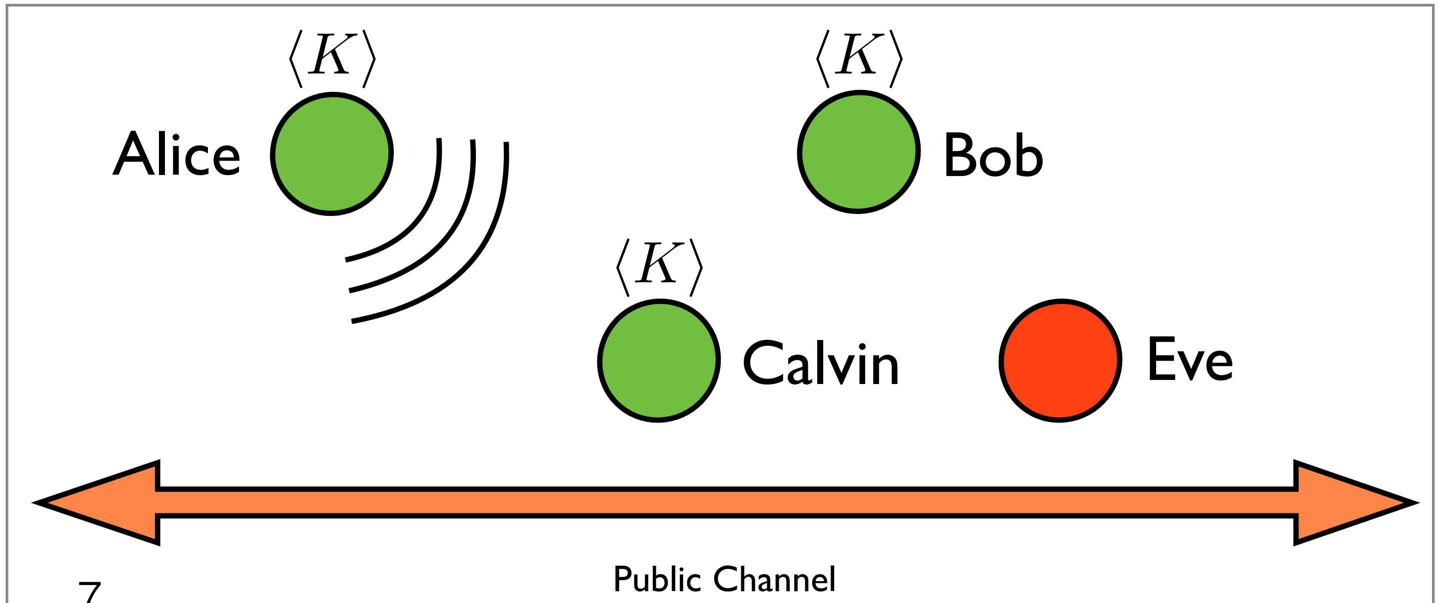
- Wireless Networks:
  - Disadvantage: Eavesdropping on wireless networks is much easier than wired network
  - Advantages: The channels from the source to different destinations are different and are changing over time
- Main idea: Use the non-uniformity nature (fluctuations) of the wireless medium





Problem Statement

- Goal: m trusted (authenticated) terminals aim to create a common secret key which will be secret from a passive eavesdropper Eve
  - There is a broadcast channel from one of the terminals (Alice) to the others including Eve
  - Trusted terminals have access to a costless public channel
  - Terminals can interact in many rounds
  - In general, the exact characterization of the secrecy rate is unknown!



Problem Statement

Wireless Channel Models

- Different Broadcast Models:

    1. We assume that the wireless broadcast channel acts as a broadcast packets erasure channel

    2. We approximately model different SNR levels by using a deterministic model

    3. We investigate a state-dependent Gaussian broadcast channel

- Assumption: The channels from Alice to the rest of terminal are independent, namely:

$$P_{X_1 \cdots X_m X_E|X_A}(x_1, \ldots, x_m, x_E|x_A) = P_{X_E|X_A}(x_E|x_A) \prod_{i=1}^{m} P_{X_i|X_A}(x_i|x_A)$$

Previous Results

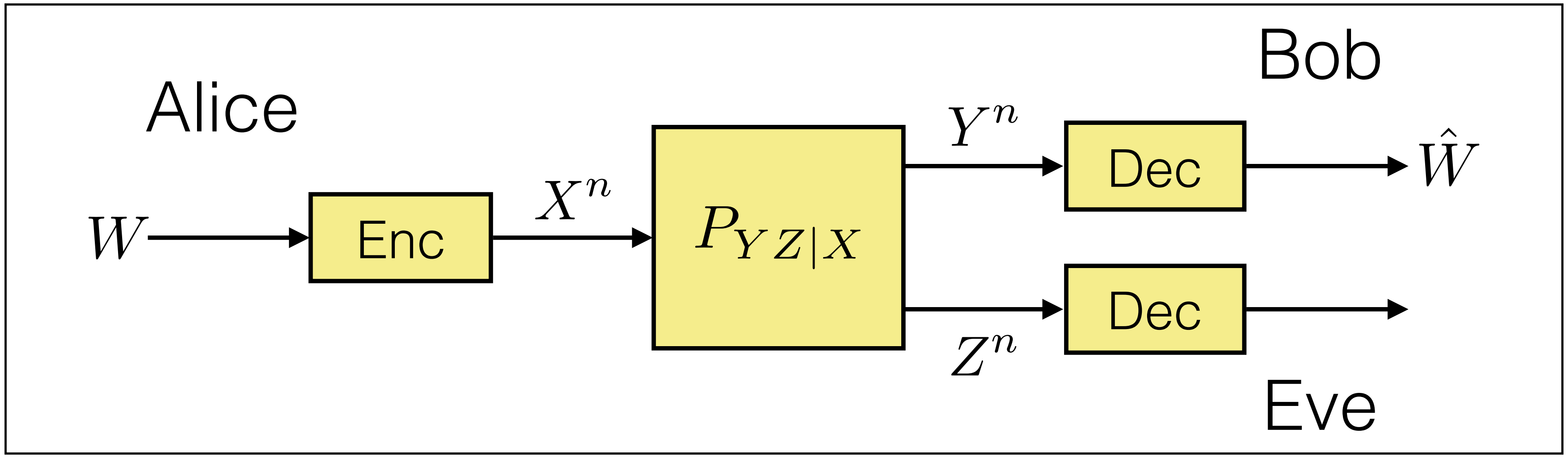
Previous Results

Wiretap Channel (Wyner 1975, Csiszar and Korner 1978)

- Goal: Alice wants to send a message to Bob over a broadcast channel where Eve overhears

$$\mathcal{P}[\hat{W} = W] > 1 - \epsilon \quad \text{and} \quad \frac{1}{n} I(W; Z^n) < \epsilon$$

- If Eve's channel is "less noisy" than Bob's => $C_s = 0$



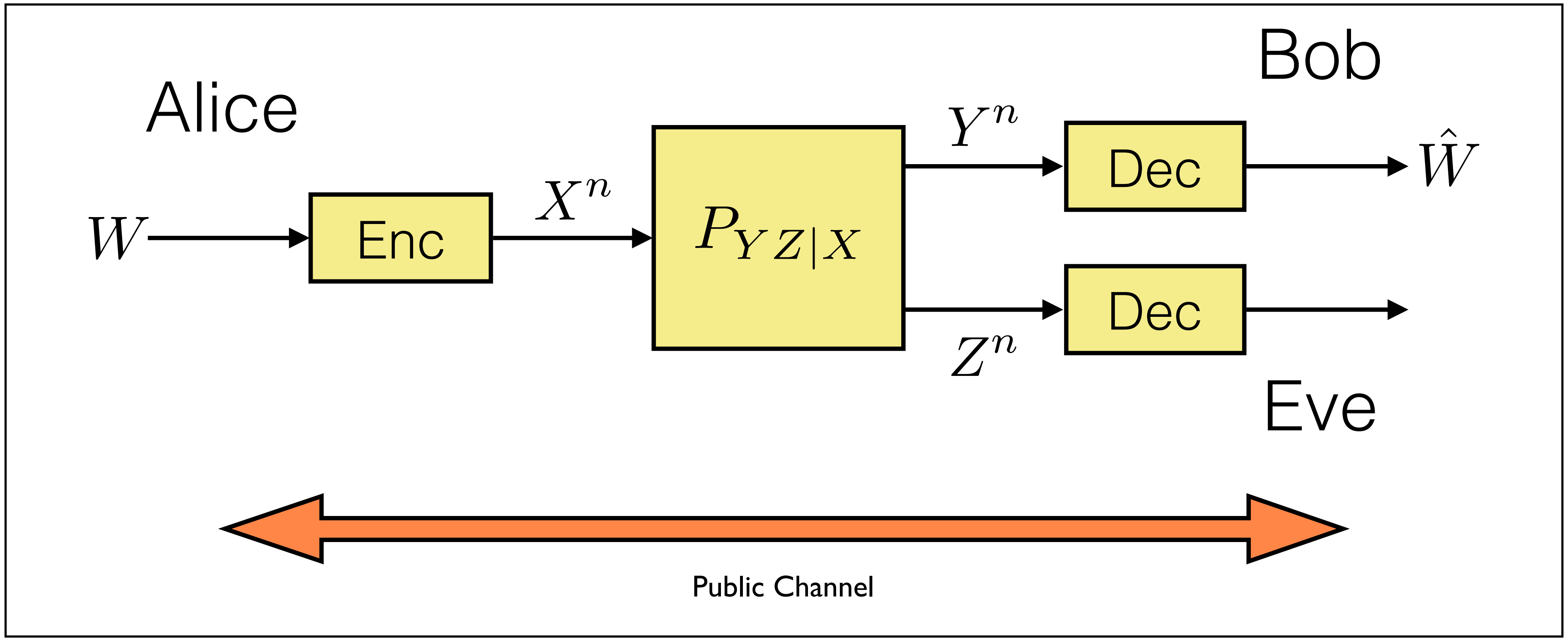
$$C_s = \max_{U - X - YZ} [I(U; Y) - I(U; Z)]$$

Previous Results

Feedback Can Help (Maurer 1993)

- The same setup as wiretap channel
- A rate-unlimited costless public channel is available
- Even if Eve's channel is "less noisy" than Bob's, we may have:

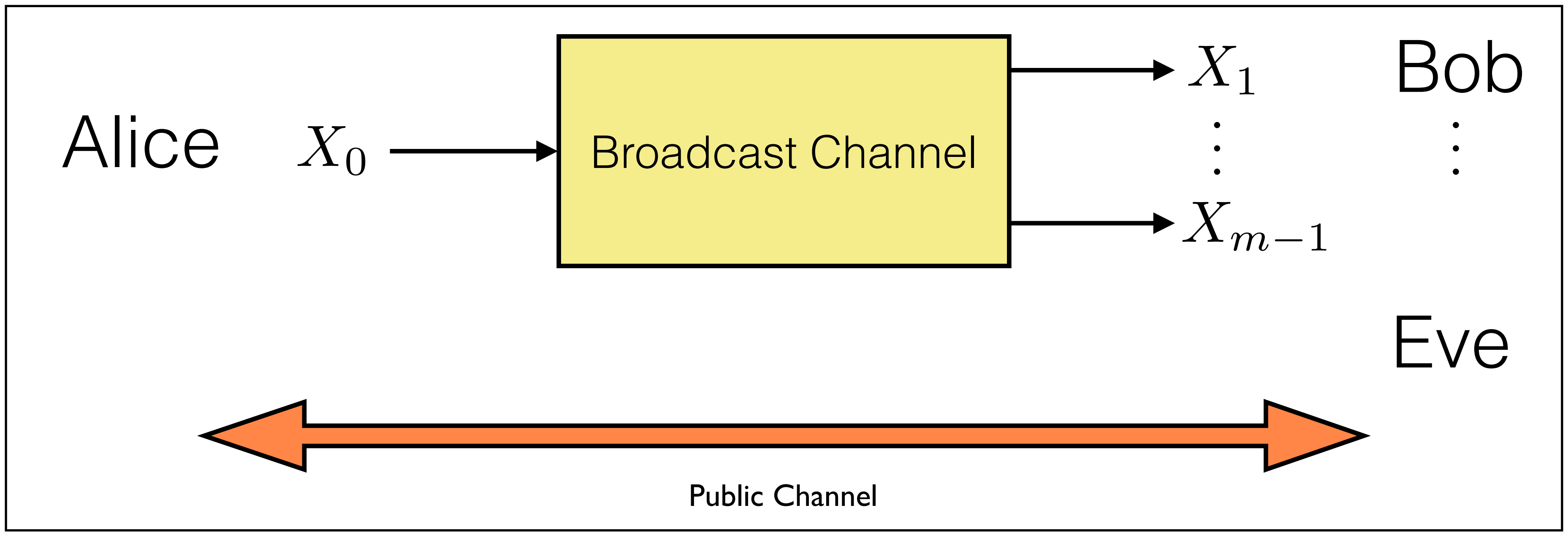
$$C_s > 0$$



Previous Results

Multi-terminal Secret Key Sharing Problem (Csiszar and Narayan 2008)

- Assumptions: A broadcast channel and a public channel is available; Terminal 0 broadcasts; Eve has only access to public channel; Terminals can interact in many rounds



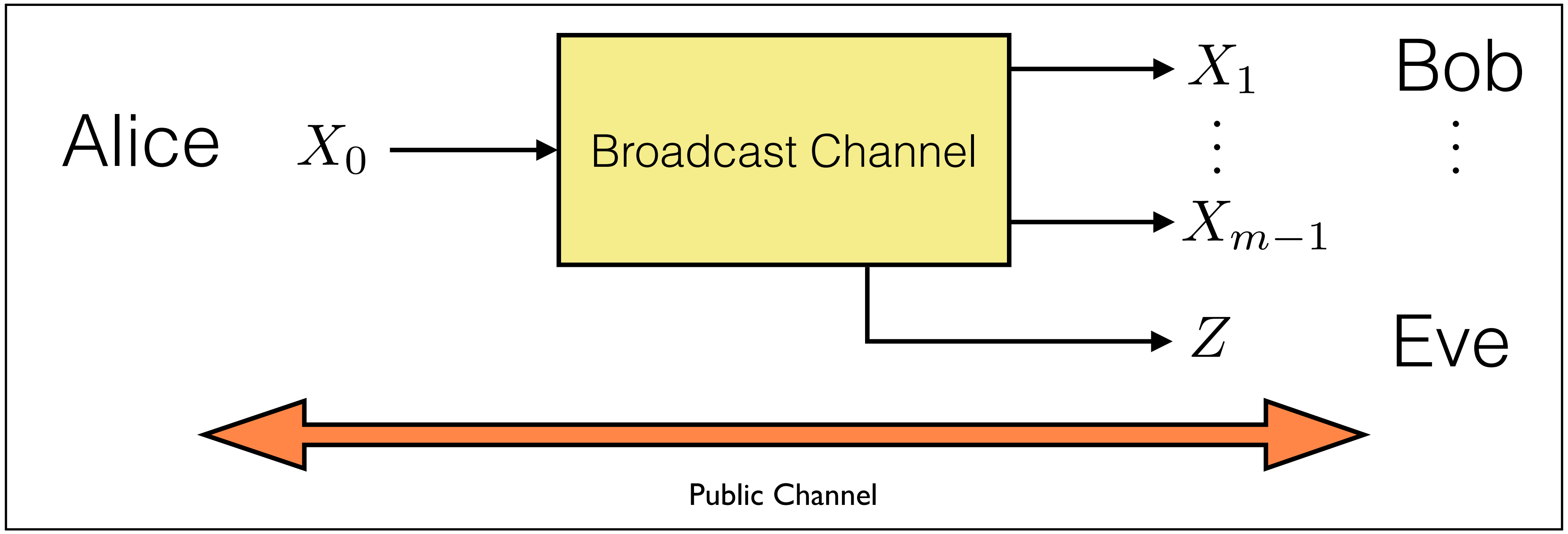
$$S(X_0; \cdots ; X_{m-1}) = \max_{P_{X_0}} \left[H(X_0, \ldots, X_{m-1}) - \underbrace{\max_{\lambda \in \Lambda} \sum_{B \subsetneq [0:m-1]} \lambda_B H(X_B | X_{B^c})}_{R_{CO}} \right]$$

- $R_{\rm CO}$ is the smallest rate of public discussion F such that $X^n_{[0:,m-1]}$ is recoverable from (X^n_i, F)

Previous Results

Multi-terminal Secret Key Sharing Problem with Side Information

- Assumptions: Similar to the previous problem;
  Eve has access to public channel+side information



- The problem is still open even for two terminals
- A corollary of the previous result (but no achievability proposed by Csiszar & Narayan):

$$S(X_0; \cdots ; X_{m-1} \| Z) \le \max_{P_{X_0}} \left[H(X_0, \ldots, X_{m-1}|Z) - \max_{\lambda \in \Lambda} \sum_{B \subsetneq [0:m-1]} \lambda_B H(X_B | X_{B^c}, Z) \right]$$

Previous Results

Extensions

- Multi-terminal Secret Key Sharing Problem with Side Information (Gohari and Anantharam 2010)
    - The same setup as before
    - Upper and lower bounds for the secret key generation (the achievability is hard to evaluate; infinite aux. rv.s)
- (Csiszar and Narayan 2013) and (Chan and Zheng 2014)
    - Extension to multi-input multi-output channel but without eavesdropper side information
    - Upper and lower bounds for the secret key generation

Upper Bound

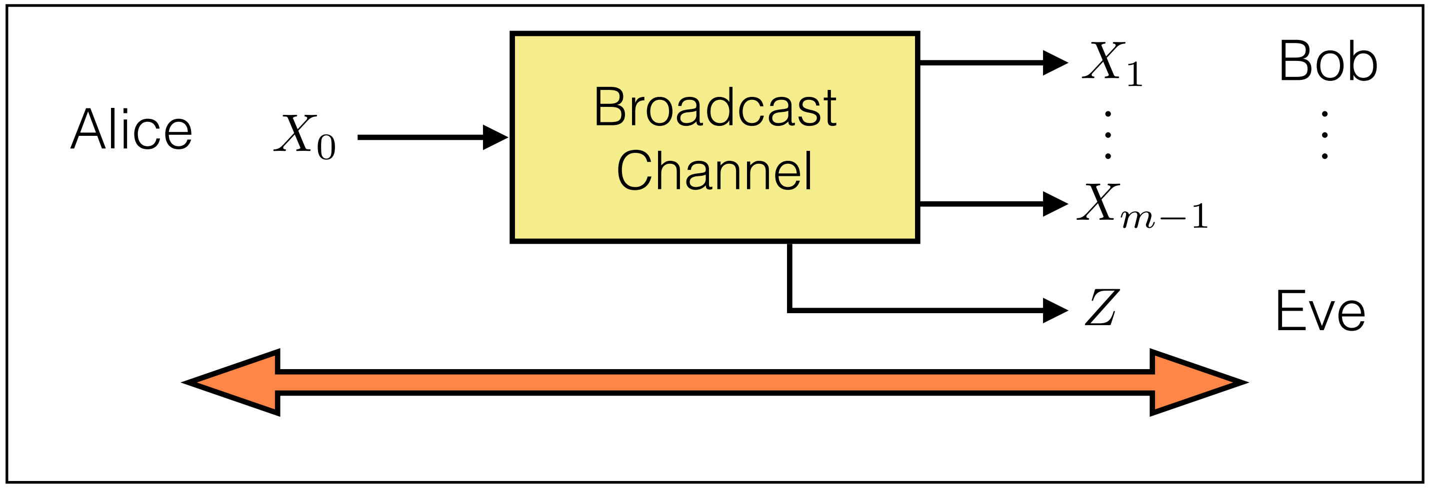
Multi-terminal Secret Key Sharing Problem with Side Information

- By [CsiszarNarayan08] and adding a dummy terminal, we have (but no achievability proposed by C&N):

$$S(X_0;\cdots;X_{m-1}\|Z) \le \max_{P_{X_0}} \left[H(X_0,\ldots,X_{m-1}|Z) - \max_{\lambda\in\Lambda} \sum_{B\subsetneq[0:m-1]} \lambda_B H(X_B|X_{B^c},Z) \right]$$

- If the channels are independent, we can further simplify:

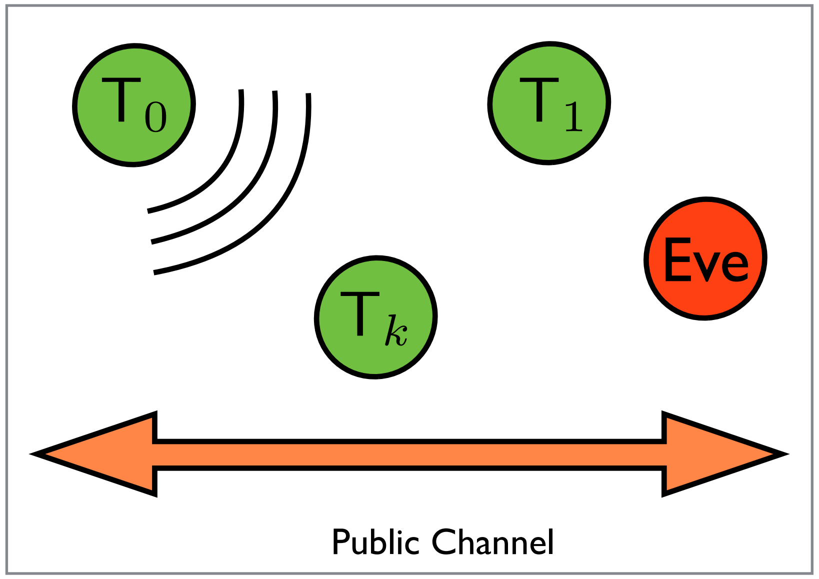
$$\begin{aligned} S(X_0;\ldots;X_{m-1}\|Z) &\le \max_{P_{X_0}} \min_{i\in[1:m-1]} I(X_0;X_i|Z) \\ &\le \min_{i\in[1:m-1]} \max_{P_{X_0}} I(X_0;X_i|Z) \end{aligned}$$



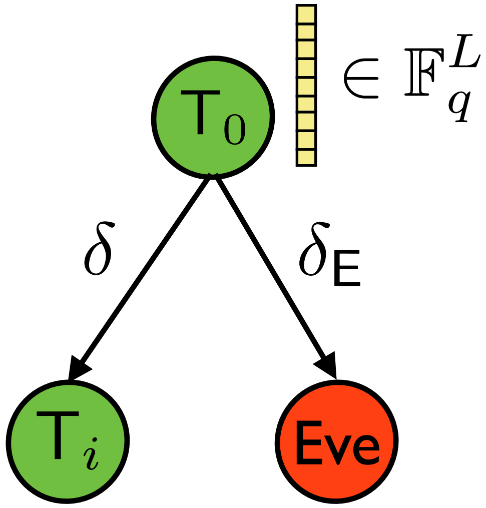
Erasure Broadcast Channel

Erasure Broadcast Channel

- The wireless channel is modelled by a packet erasure channel
- Each terminal either receives packets sent by Alice or not
- Channels are independent

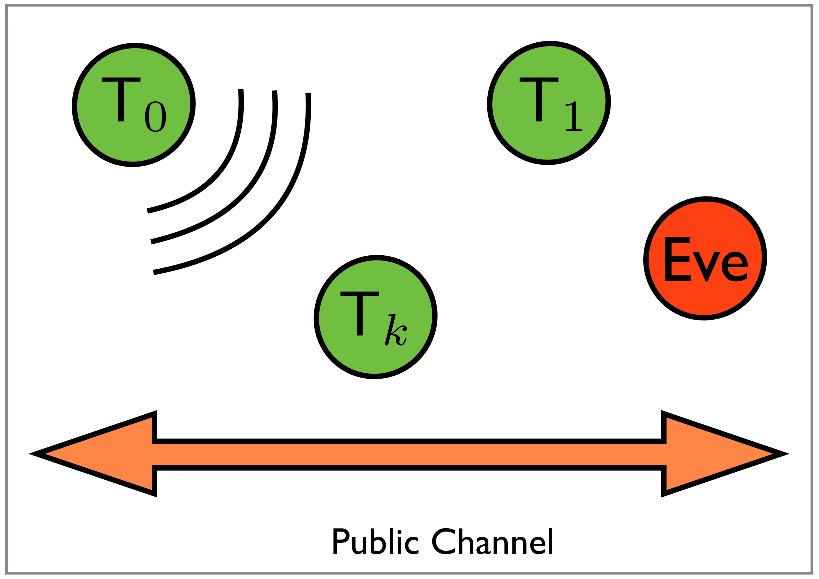


- The input and output symbols are packets of length L from $\mathbb{F}_q$



Erasure Broadcast Channel

- Question: What is the secret key sharing capacity in this setup?



- Theorem: The capacity of this problem is

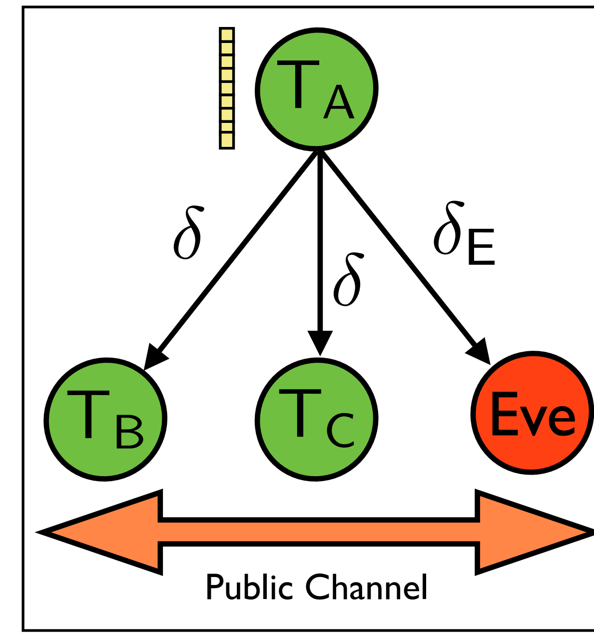
$$S(X_0; \ldots ; X_{m-1} \| Z) = (1-\delta)\delta_{\mathsf{E}} \times \underbrace{(L \log_2 q)}_{\text{packet length in bits}}$$

- The result does not depend on m!

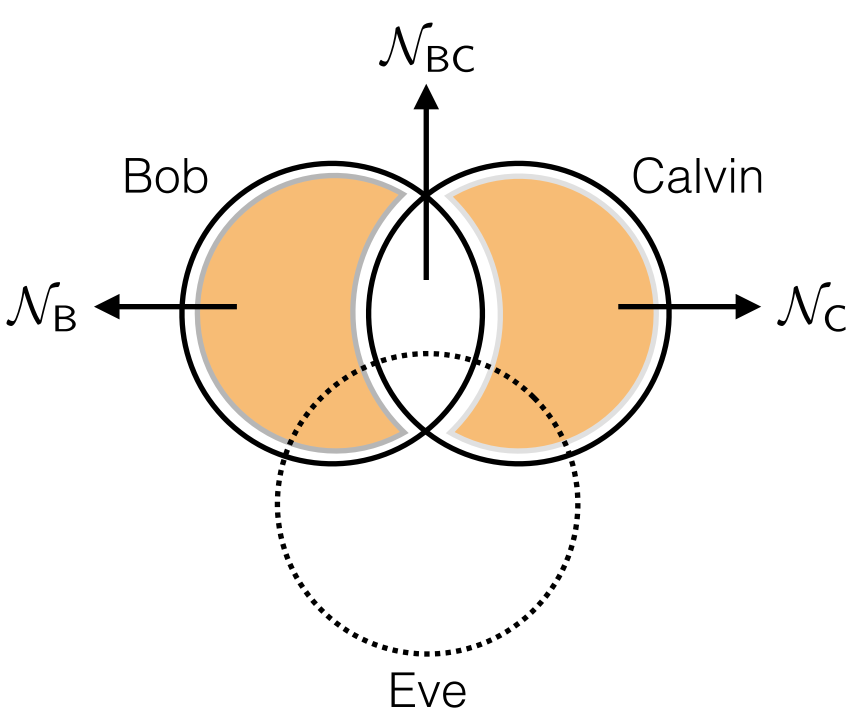
Sketch of the Achievability

Private Phase

- Alice sends n packets $\{x_1, \ldots, x_n\}$
- Bob and Calvin receives $(1-\delta)n$ packets each
- Eve observes $(1-\delta_E)(1-\delta)n$ packets from each of these sets



- => There exist some packets that Bob (Calvin) receives but Eve does not



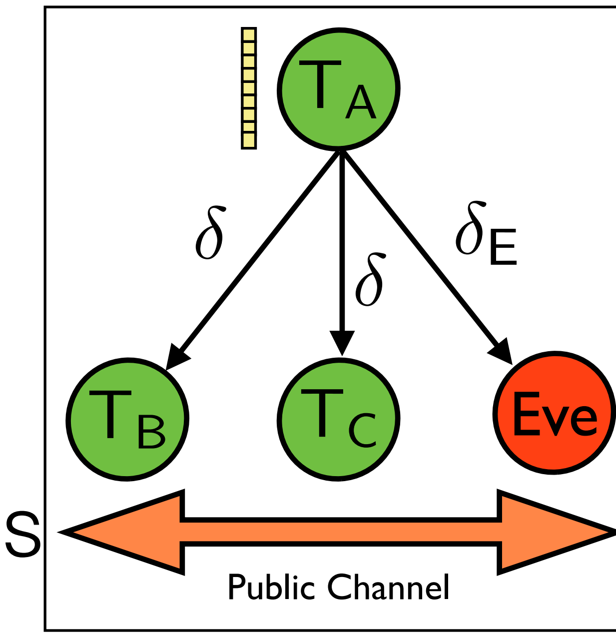
$$|\mathcal{N}_B| \approx |\mathcal{N}_C| \approx \delta(1-\delta)n$$
$$|\mathcal{N}_{BC}| \approx (1-\delta)^2 n$$

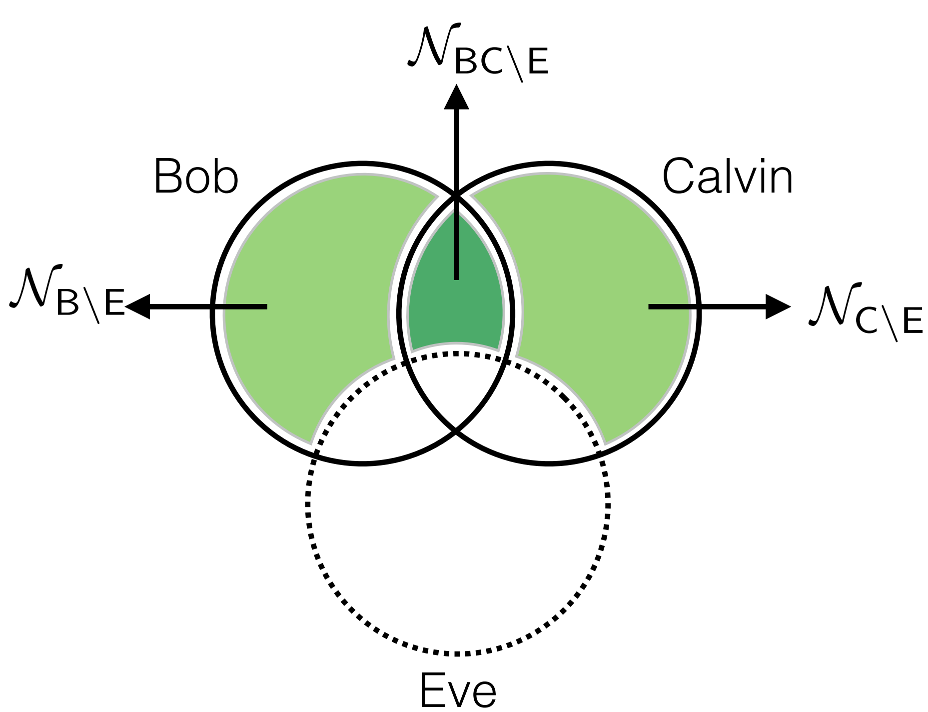
$$|\mathcal{N}_{B\setminus E}| \approx |\mathcal{N}_{C\setminus E}| \approx \delta(1-\delta)\delta_E n$$
$$|\mathcal{N}_{BC\setminus E}| \approx (1-\delta)^2 \delta_E n$$

Sketch of the Achievability

Public Discussion (Initial Phase)

- Bob and Calvin send back the indices of their packets publicly
- Alice reproduce $\mathcal{N}_{B}$, $\mathcal{N}_{C}$, and $\mathcal{N}_{BC}$
- If a genie tells Alice the indices of Eve's packets we are done => The green packets form a key
- Question: What we can do?





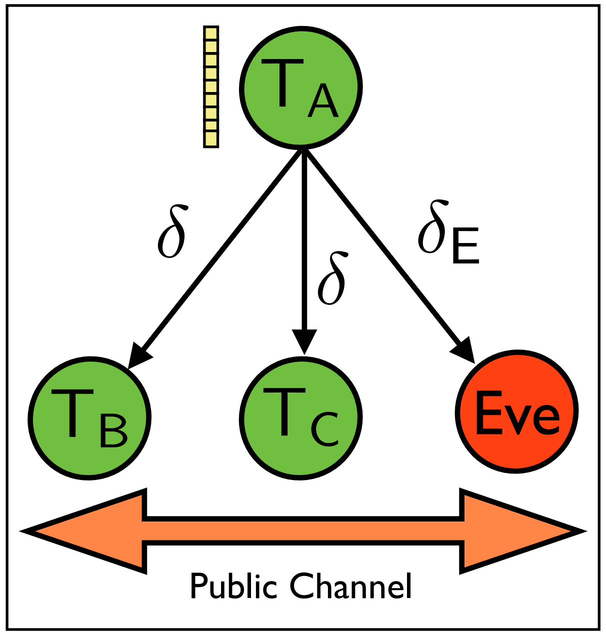
$$|\mathcal{N}_B| \approx |\mathcal{N}_C| \approx \delta(1-\delta)n$$
$$|\mathcal{N}_{BC}| \approx (1-\delta)^2 n$$

$$|\mathcal{N}_{B\setminus E}| \approx |\mathcal{N}_{C\setminus E}| \approx \delta(1-\delta)\delta_E n$$
$$|\mathcal{N}_{BC\setminus E}| \approx (1-\delta)^2 \delta_E n$$

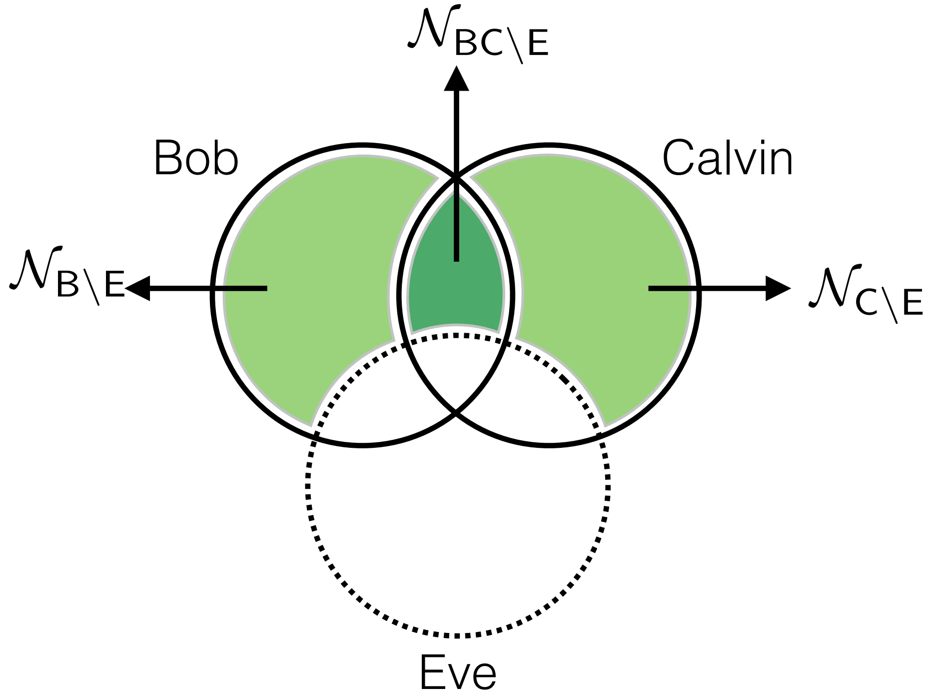
Sketch of the Achievability

Public Discussion (Initial Phase)

- Lemma: It is possible to create the same number as of green sets, linear combinations out of $\mathcal{N}_{\mathrm{B}}$, $\mathcal{N}_{\mathrm{C}}$ and over $\mathcal{N}_{\mathrm{BC}}$ so that these packets are secure from Eve.



- Alice sends the coefficients of these new green linear combinations publicly, Eve does not gain any information ==> A set of keys: $K_{\mathrm{B}},\ K_{\mathrm{C}},\ \text{and}\ K_{\mathrm{BC}}$



$$|\mathcal{N}_B| \approx |\mathcal{N}_C| \approx \delta(1-\delta)n$$
$$|\mathcal{N}_{BC}| \approx (1-\delta)^2 n$$

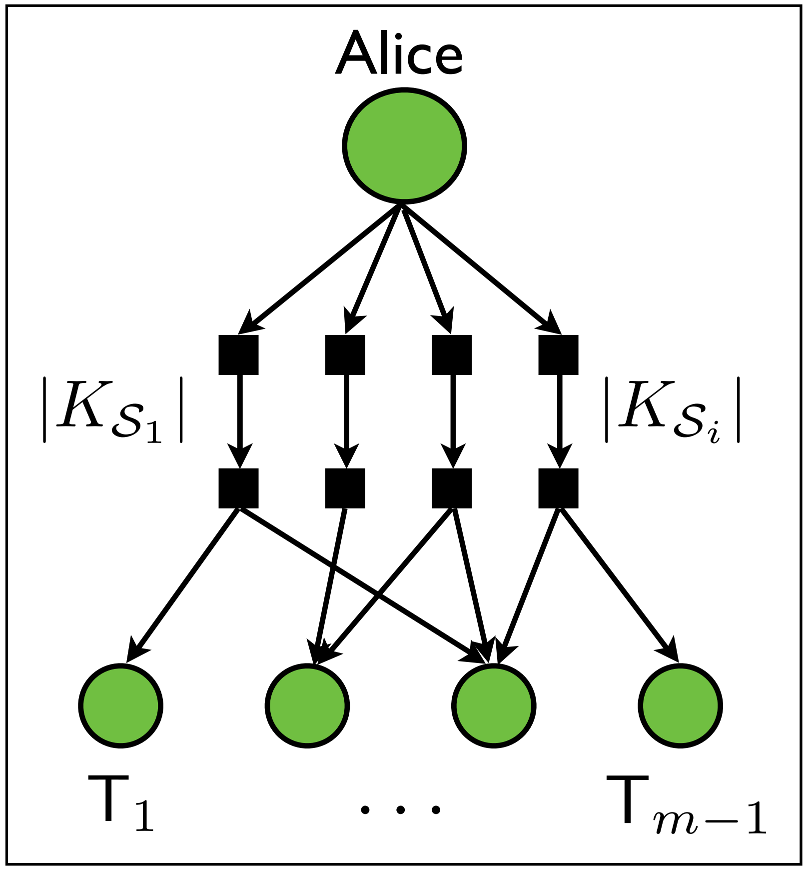
$$|\mathcal{N}_{B\setminus E}| \approx |\mathcal{N}_{C\setminus E}| \approx \delta(1-\delta)\delta_E n$$
$$|\mathcal{N}_{BC\setminus E}| \approx (1-\delta)^2 \delta_E n$$

Sketch of the Achievability

Public Discussion (Reconciliation Phase)

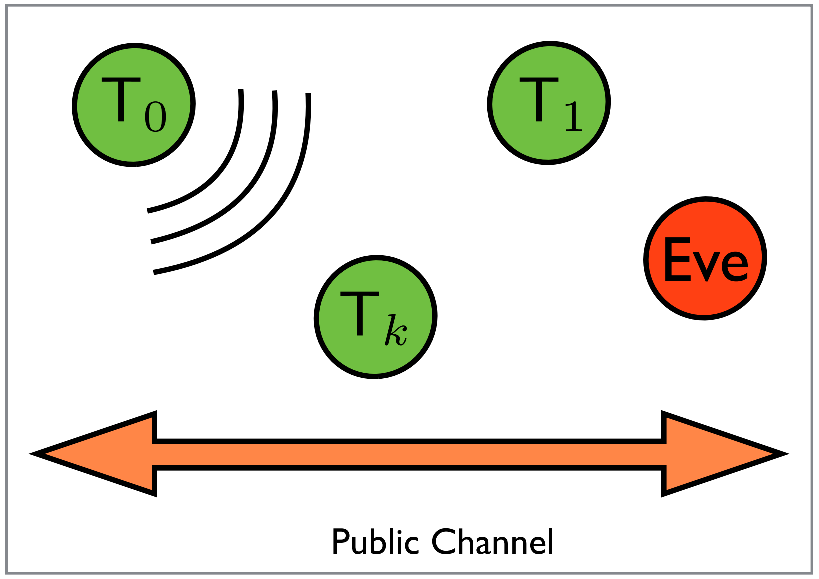
- K_{BC} can be part of the final key
- Using K_{B} and K_{C}, Alice can share a new key with Bob and Calvin over the public channel
- So in total, the final key size is: $|K_{\mathsf{B}}| + |K_{\mathsf{BC}}| = |\mathcal{N}_{B\setminus E}| + |\mathcal{N}_{BC\setminus E}| \approx (1-\delta)\delta_{\mathsf{E}} n$

- In general, Alice can use a network code to reconcile the key over the public channel



Erasure Broadcast Channel

Shortcomings of modelling a wireless channel with an erasure channel



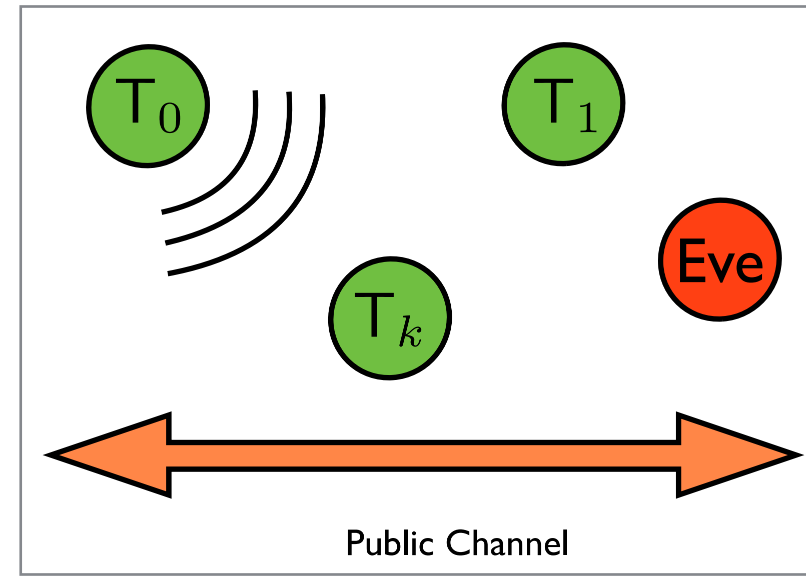
- A packet is declared as erased if some number of bits have been corrupted
  => Eve can exploit the remaining bits

- The actual channel is a continuous channel with varying SNR
  => Need a more sophisticated model to capture the different SNR levels

Deterministic Broadcast Channel

Deterministic Broadcast Channel

- The wireless channel is modelled by a deterministic channel*
- There are $s+1$ channel states modelling different SNR levels



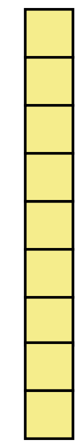
$$X_r[t] = \boldsymbol{F}_{\underbrace{S_r[t]}_{\text{Channel State}}} X_0[t]$$

- Channels are independent
- Assume CSI at receivers

[*] Avestimehr, Diggavi, and Tse, "Wireless Network Information Flow: A Deterministic Approach," IT11.

Deterministic Broadcast Channel

Received vector at r'th terminal $\leftarrow X_r[t] = \boldsymbol{F}_{S_r[t]} X_0[t] \rightarrow$

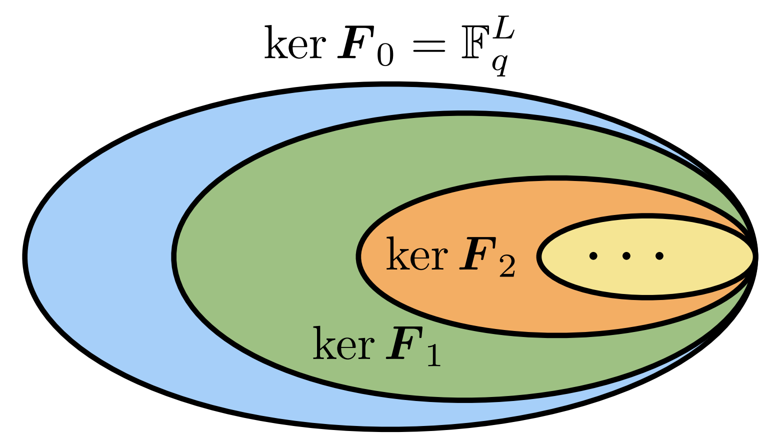


$\in \mathbb{F}_q^L$

Channel State $\in [0:s]$

$$\mathbf{0} = \ker \boldsymbol{F}_s \subset \ker \boldsymbol{F}_{s-1} \subset \cdots \subset \ker \boldsymbol{F}_0 = \mathbb{F}_q^L$$

$$\operatorname{rank}(\boldsymbol{F}_i - \boldsymbol{F}_{i-1}) = \operatorname{rank}(\boldsymbol{F}_i) - \operatorname{rank}(\boldsymbol{F}_{i-1})$$



$$\boldsymbol{F}_0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \boldsymbol{F}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \boldsymbol{F}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

pick the most significant symbol

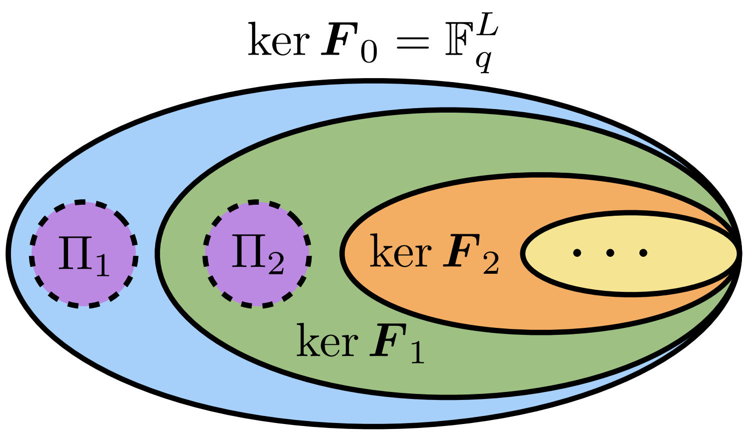
pick the least significant symbol

Sketch of the Achievability

Superposition Coding

- We can find subspaces $\Pi_1, \ldots, \Pi_s$ such that $\Pi_i \cap \Pi_j = \mathbf{0}$ and

$$
\begin{aligned}
\Pi_1 \oplus \ker \boldsymbol{F}_1 &= \mathbb{F}_q^L \\
\Pi_2 \oplus \Pi_1 \oplus \ker \boldsymbol{F}_2 &= \mathbb{F}_q^L \\
&\vdots \\
\Pi_s \oplus \cdots \oplus \Pi_1 \oplus \ker \boldsymbol{F}_s &= \mathbb{F}_q^L
\end{aligned}
$$



- Alice uses superposition coding:

$$X_0[t] = X_{0,1}[t] + \cdots + X_{0,s}[t] \qquad \text{where} \quad X_{0,i} \in \Pi_i$$

- Vector $X_{0,i}[t]$ is received by the r'th terminal only if $S_r \geq i$
  ==> we have s independent erasure channels!

- $X_{0,i}[t]$ is received with erasure probability $\theta_i \triangleq \sum_{j=0}^{i-1} \delta_i$

Sketch of the Achievability

Superposition Coding

- We can find subspaces $\Pi_1, \dots, \Pi_s$ such that $\Pi_i \cap \Pi_j = \mathbf{0}$ and

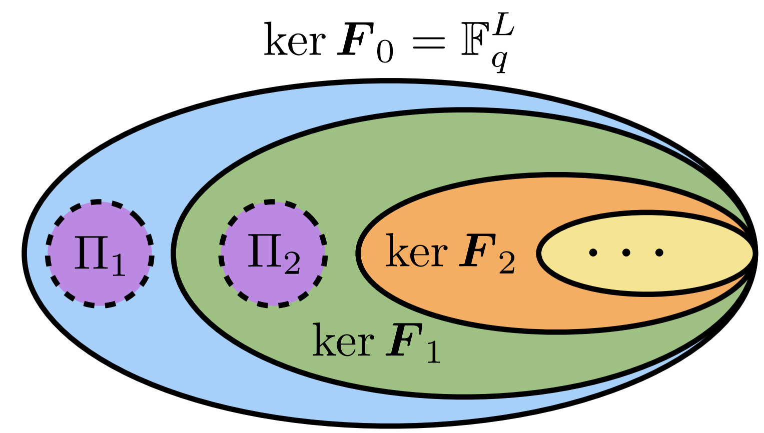
Form a basis

$$\Pi_1 \oplus \ker \boldsymbol{F}_1 = \mathbb{F}_q^L$$

$$\Pi_2 \oplus \Pi_1 \oplus \ker \boldsymbol{F}_2 = \mathbb{F}_q^L$$

$$\vdots$$

$$\Pi_s \oplus \cdots \oplus \Pi_1 \oplus \ker \boldsymbol{F}_s = \mathbb{F}_q^L$$



- Alice uses superposition coding:

$$X_0[t] = X_{0,1}[t] + \cdots + X_{0,s}[t] \qquad \text{where} \quad X_{0,i} \in \Pi_i$$

- Vector $X_{0,i}[t]$ is received by the r'th terminal only if $S_r \geq i$
  ==> we have s independent erasure channels!

- $X_{0,i}[t]$ is received with erasure probability $\theta_i \triangleq \sum_{j=0}^{i-1} \delta_i$

Deterministic Broadcast Channel

Final Result

- Theorem: The secret key generation capacity for the deterministic broadcast channel is:

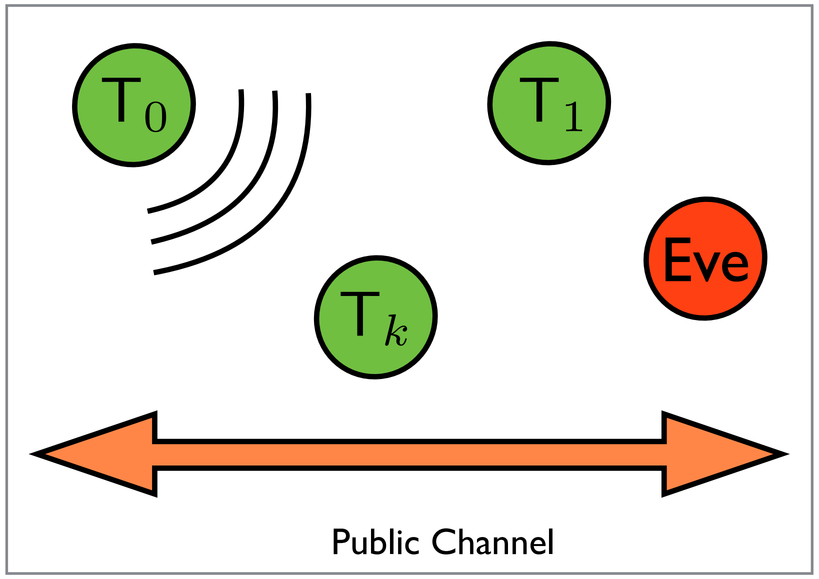
$$S(X_0;\ldots;X_m\|Z)=\sum_{j=1}^{s}\theta_j(1-\theta_j)\underbrace{\overbrace{[\operatorname{rank}\boldsymbol{F}_j-\operatorname{rank}\boldsymbol{F}_{j-1}]}^{\dim(\Pi_j)}\log_2 q}_{\#\text{ of messages in the }j\text{th layer (in bits)}}$$

Erasure probability of j'th layer

Gaussian Broadcast Channel

Gaussian Broadcast Model

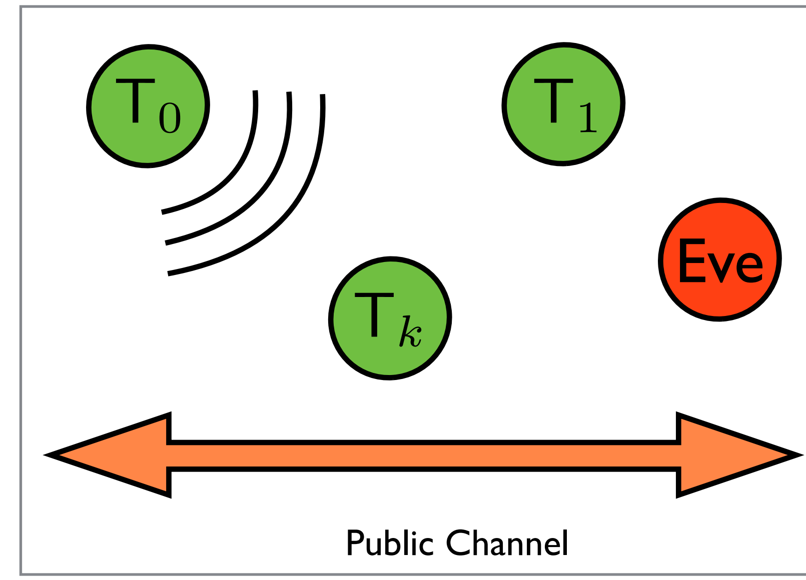
- There is a Gaussian broadcast channel from Alice to other terminals
- Channels are independent
- There are $s+1$ channel states having different SNR levels
- Assume CSI at receivers



$$X_r[t] = h_{S_r[t]} X_0[t] + Z_r[t]$$

Gaussian Broadcast Model

- There is a Gaussian broadcast channel from Alice to other terminals
- Channels are independent
- There are $s+1$ channel states having different SNR levels
- Assume CSI at receivers



$X_0[t] \in \mathbb{R}^L, \quad \frac{1}{L}\mathbb{E}\left[\|X_0\|^2\right] \le P$

$$X_r[t] = h_{S_r[t]} X_0[t] + Z_r[t]$$

$Z_r[t] \sim N(\mathbf{0}, \boldsymbol{I}_L)$

Channel gain $\in \mathbb{R}$

$h_0 \le \cdots \le h_s$

Channel State $\in [0:s]$

Upper Bound

Gaussian Broadcast Channel

- Theorem: (By combining [Csiszar-Narayan-08] and [Chan-Zheng-14] and independence of channels):
  The secret key generation capacity of the Gaussian broadcast channel using public discussion is upper bounded as follows:

$$C_s \leq \sup_{P_{X_0}:\ \frac{1}{L}\mathbb{E}[||X_0||^2] \leq P} \ \min_{j \in [1:m]} I(X_0; X_j | Z)$$

$$\leq \frac{1}{2} L \sum_{i=0}^{s} \sum_{j=0}^{s} \delta_i \delta_j \log \left(1 + \frac{h_i^2 P}{1 + h_j^2 P} \right)$$

Upper Bound

Gaussian Broadcast Channel

- Theorem: (By combining [Csiszar-Narayan-08] and [Chan-Zheng-14] and independence of channels):
  The secret key generation capacity of the Gaussian broadcast channel using public discussion is upper bounded as follows:

$$C_s \leq \sup_{P_{X_0}:\ \frac{1}{L}\mathbb{E}[||X_0||^2] \leq P} \ \min_{j \in [1:m]} I(X_0; X_j | Z)$$

$$\leq \frac{1}{2} L \sum_{i=0}^{s} \sum_{j=0}^{s} \delta_i \delta_j \log\left(1 + \frac{h_i^2 P}{1 + h_j^2 P}\right)$$

Input power budget

State probability

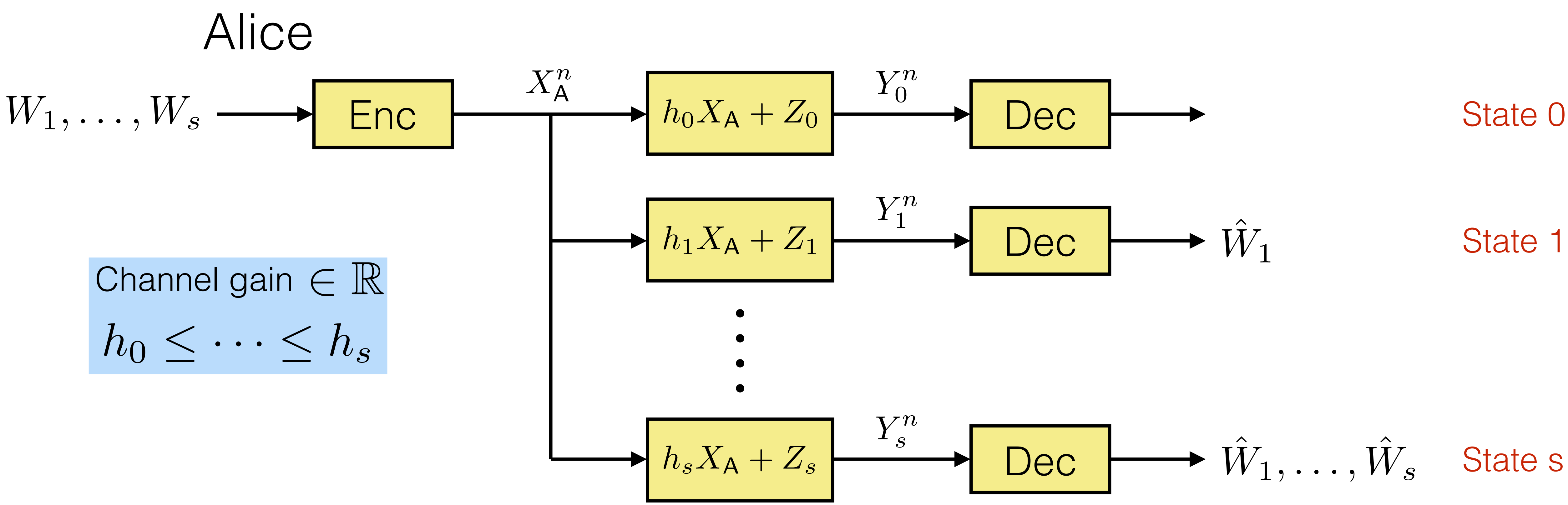
Channel gain $\in \mathbb{R}$

$h_0 \leq \cdots \leq h_s$

Sketch of the Achievability

- We want to mimic the orthogonality operation of the deterministic channel
- By using a properly designed layered wiretap code:
    - => we can introduce orthogonal layers (each layer acts as an erasure channel)
- On each layer, we apply the interactive scheme devised for the erasure channel

Nested Message Set, Degraded Wiretap Channel



- Code Design Goals:
  - Message W_i should be decodable by receivers $Y_i, \ldots, Y_s$
  - All receivers $Y_0, \ldots, Y_{i-1}$ should be ignorant about message W_i
  - Now, we have the orthogonality operation among messages W_i

Nested Message Set, Degraded Wiretap Channel

- Alice uses superposition coding: $X_{\mathsf{A}}[t] = X_{\mathsf{A},1}[t] + \cdots + X_{\mathsf{A},s}[t]$
- She maps W_i to $X_{\mathsf{A},i}$ as follows:
  - Construct codebook $\hat{\mathcal{C}}_i(2^{L\hat{R}_i}, L)$ by choosing independent symbols from $\mathcal{N}(0, P_i)$ where:

$$\hat{R}_i = \frac{1}{2}\log\left(1 + \frac{h_i^2 P_i}{1 + h_i^2 I_i}\right)$$

  - Each codebook $\hat{\mathcal{C}}_i$ is divided into 2^{LR_i} bins where:

$$R_i = \frac{1}{2}\left[\log\left(1 + \frac{h_i^2 P_i}{1 + h_i^2 I_i}\right) - \log\left(1 + \frac{h_{i-1}^2 P_i}{1 + h_{i-1}^2 I_i}\right)\right]$$

  - Message W_i is mapped to the bin index and $X_{\mathsf{A},i}$ is a random sequence from that bin

Nested Message Set, Degraded Wiretap Channel

- Alice uses superposition coding: $X_{\mathsf{A}}[t] = X_{\mathsf{A},1}[t] + \cdots + X_{\mathsf{A},s}[t] \longleftarrow W_s$

  W_1
- She maps W_i to $X_{\mathsf{A},i}$ as follows:
  - Construct codebook $\hat{\mathcal{C}}_i(2^{L\hat{R}_i}, L)$ by choosing independent symbols from $\mathcal{N}(0, P_i)$ where:

$$\hat{R}_i = \frac{1}{2}\log\left(1 + \frac{h_i^2 P_i}{1 + h_i^2 I_i}\right)$$

  - Each codebook $\hat{\mathcal{C}}_i$ is divided into 2^{LR_i} bins where:

$$R_i = \frac{1}{2}\left[\log\left(1 + \frac{h_i^2 P_i}{1 + h_i^2 I_i}\right) - \log\left(1 + \frac{h_{i-1}^2 P_i}{1 + h_{i-1}^2 I_i}\right)\right]$$

  - Message W_i is mapped to the bin index and $X_{\mathsf{A},i}$ is a random sequence from that bin

Nested Message Set, Degraded Wiretap Channel

- Alice uses superposition coding: $X_{\mathsf{A}}[t] = X_{\mathsf{A},1}[t] + \cdots + X_{\mathsf{A},s}[t] \leftarrow W_s$
- She maps W_i to $X_{\mathsf{A},i}$ as follows: ($W_1 \to X_{\mathsf{A},1}[t]$)
  - Construct codebook $\hat{\mathcal{C}}_i(2^{L\hat{R}_i}, L)$ by choosing independent symbols from $\mathcal{N}(0, P_i)$ where:

$$\hat{R}_i = \frac{1}{2}\log\left(1 + \frac{h_i^2 P_i}{1 + h_i^2 I_i}\right)$$

power of i'th layer (P_i)

$$I_i = \sum_{j=i+1}^{s} P_j$$

  - Each codebook $\hat{\mathcal{C}}_i$ is divided into 2^{LR_i} bins where:

$$R_i = \frac{1}{2}\left[\log\left(1 + \frac{h_i^2 P_i}{1 + h_i^2 I_i}\right) - \log\left(1 + \frac{h_{i-1}^2 P_i}{1 + h_{i-1}^2 I_i}\right)\right]$$

  - Message W_i is mapped to the bin index and $X_{\mathsf{A},i}$ is a random sequence from that bin

Sketch of the Achievability, cont.

- The r'th receiver with channel state $S_r = i$:
  - can successively decode messages up to layer i
  - is ignorant about messages of layers above i
- ==> Each W_i experiences an independent erasure channel with erasure probability:

$$\theta_i \triangleq \sum_{j=0}^{i-1} \delta_i$$

- For each layer, run the interactive scheme for erasure channels
- The achievable secret key generation rate, for each power allocation $\{P_i\}$ is:

$$R_s = \sum_{i=1}^{s} \theta_i (1 - \theta_i) R_i$$

Power Optimization Problem

Sketch of the Achievability

- The maximum achievable secrecy rate is given by:

$$R_s = \begin{cases} \max & \sum_{i=1}^{s} \theta_i(1-\theta_i)R_i \\ \text{subject to} & \sum_{i=1}^{s} P_i \leq P \\ & P_i \geq 0, \quad \forall i \in [1:s]. \end{cases}$$

- This is a not a convex optimization problem!
- Constraints are affine => KKT equations give necessary conditions
    - All of KKT solutions can be found by a backtracking algorithm
    - ==> The optimum solution can be found!
- The upper and lower bounds do not match!

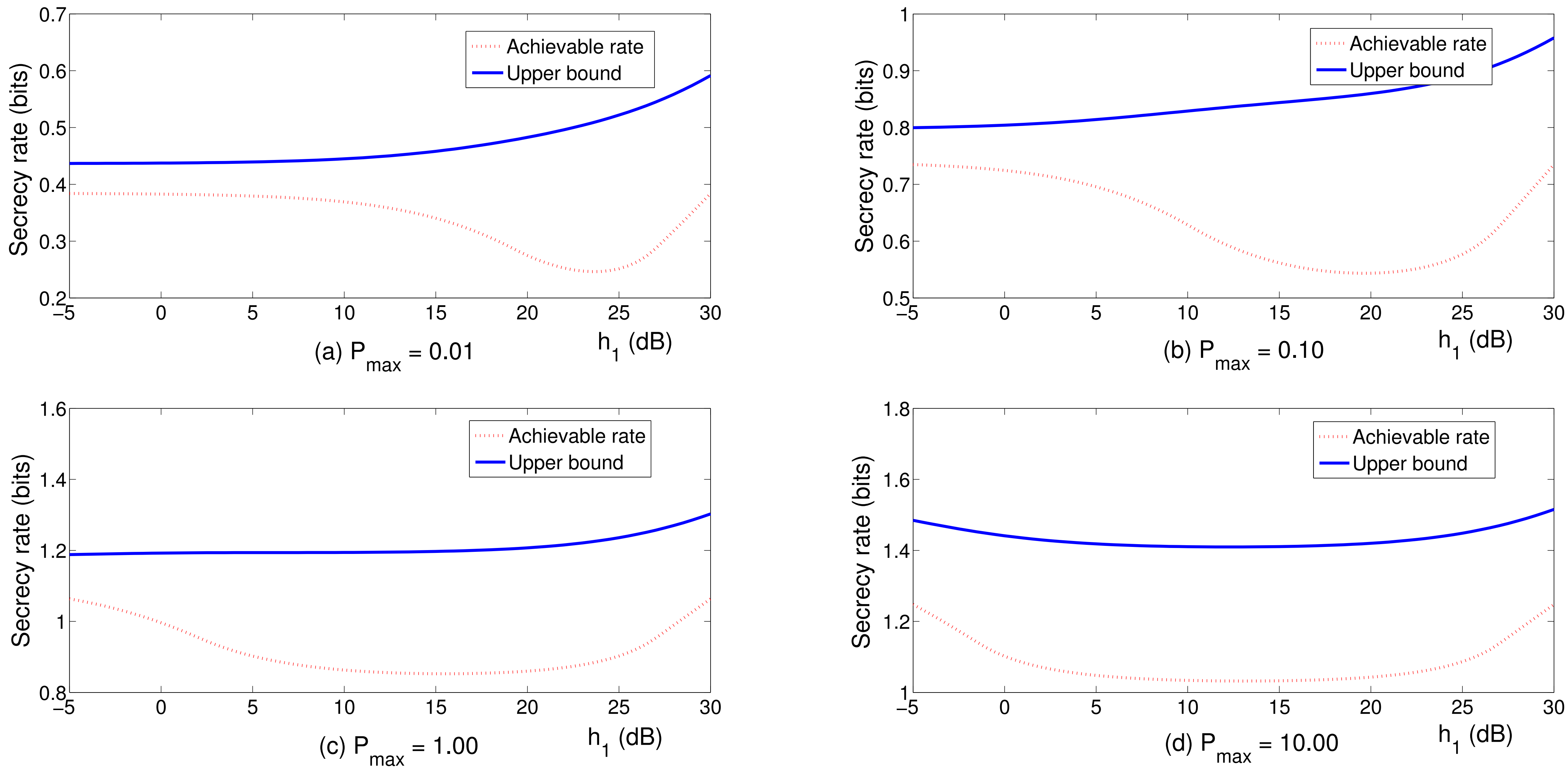
Results: Asymptotic Behaviour

- Assuming high-dynamic range, i.e., $h_i \gg h_{i-1}$ and high-SNR regime:
    - The upper and lower bounds match in a degrees of freedom sense ($h_i = Q^{\gamma_i}$):

$$
\begin{aligned}
\mathrm{DoF}_s &\triangleq \lim_{Q\to\infty} \frac{C_s}{\frac{1}{2}\log Q} \\
&= L\sum_{i=1}^{s}(\gamma_i - \gamma_{i-1})(1-\theta_i)\theta_i
\end{aligned}
$$

Results: Bounds Comparison

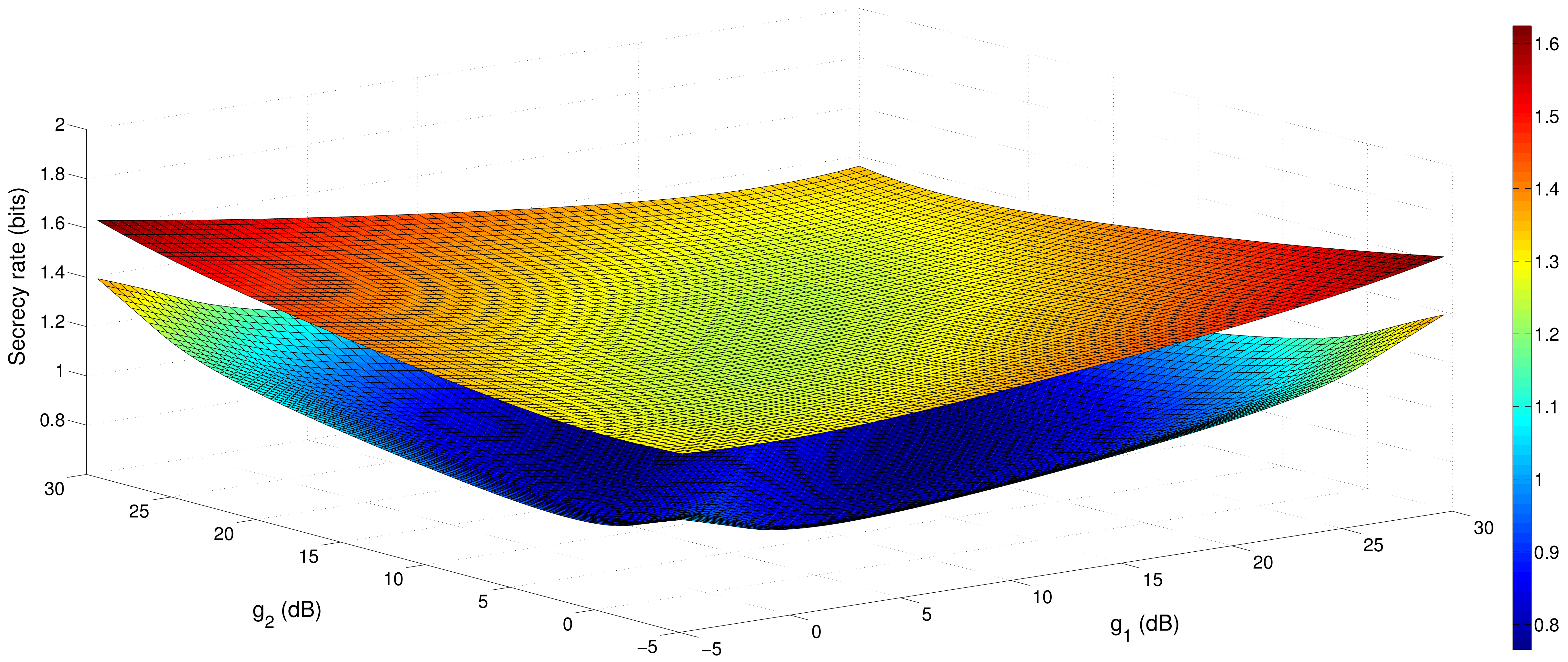
3 Equiprobable States



The achievable rate and the upper bound as a function of h1 with P: (a) P=0.01, (b) P=0.1, (c) P=1, and (d) P=10, in a setup with 3 equiprobable states (h0 = -5dB, -5dB < h1 < 30 dB, and h2 = 30dB).

Results: Bounds Comparison

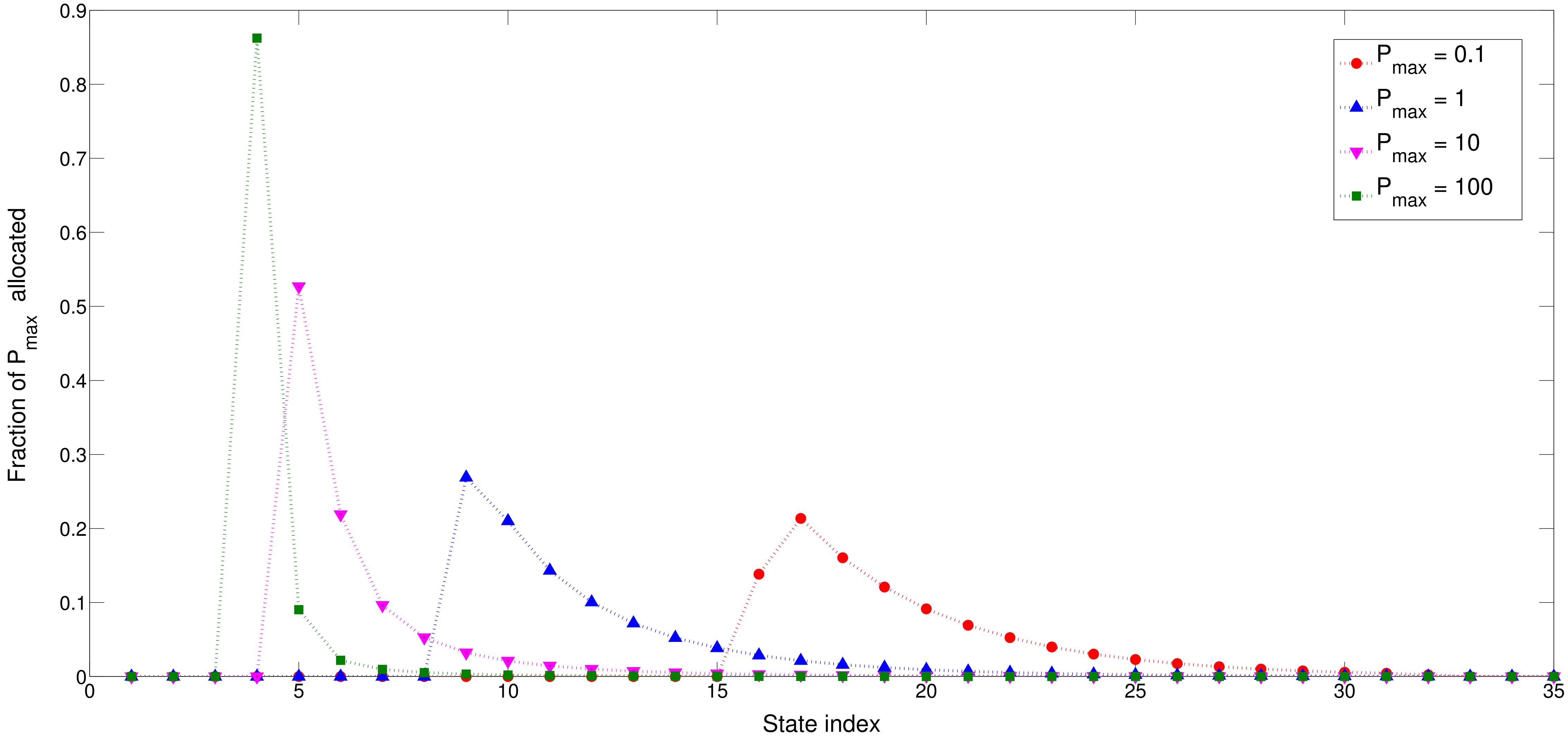
4 Equiprobable States



The achievable rate and the upper bound as a function of g1 and g2 with P=10 in a setup with 4 equiprobable states (h0 = -5dB, h1 = min[g1,g2], h2 = max[g1,g2], and h3 = 30dB).

Results: Power Allocation

36 Equiprobable States



Fraction of total power P allocated to each layer by the proposed scheme for P = 0.1, 1.0, 10, 100 in a setup consisting 36 equiprobable states (h0 = -5dB, h1 = -4dB, ..., h35 = 30dB).

Challenges

- For a usual cryptographic system:
  An attack can be done by an adversary who has very high computational power
- In the proposed setup:
  An attack can be done by an adversary who has multiple antennas at many different places
- In general, it is hard to estimate the Eve's channel statistics

Thank You!