Generalized Secrecy Capacity

Matthieu Bloch

Wireless Institute
University of Notre Dame

WIRELESS
INSTITUTE

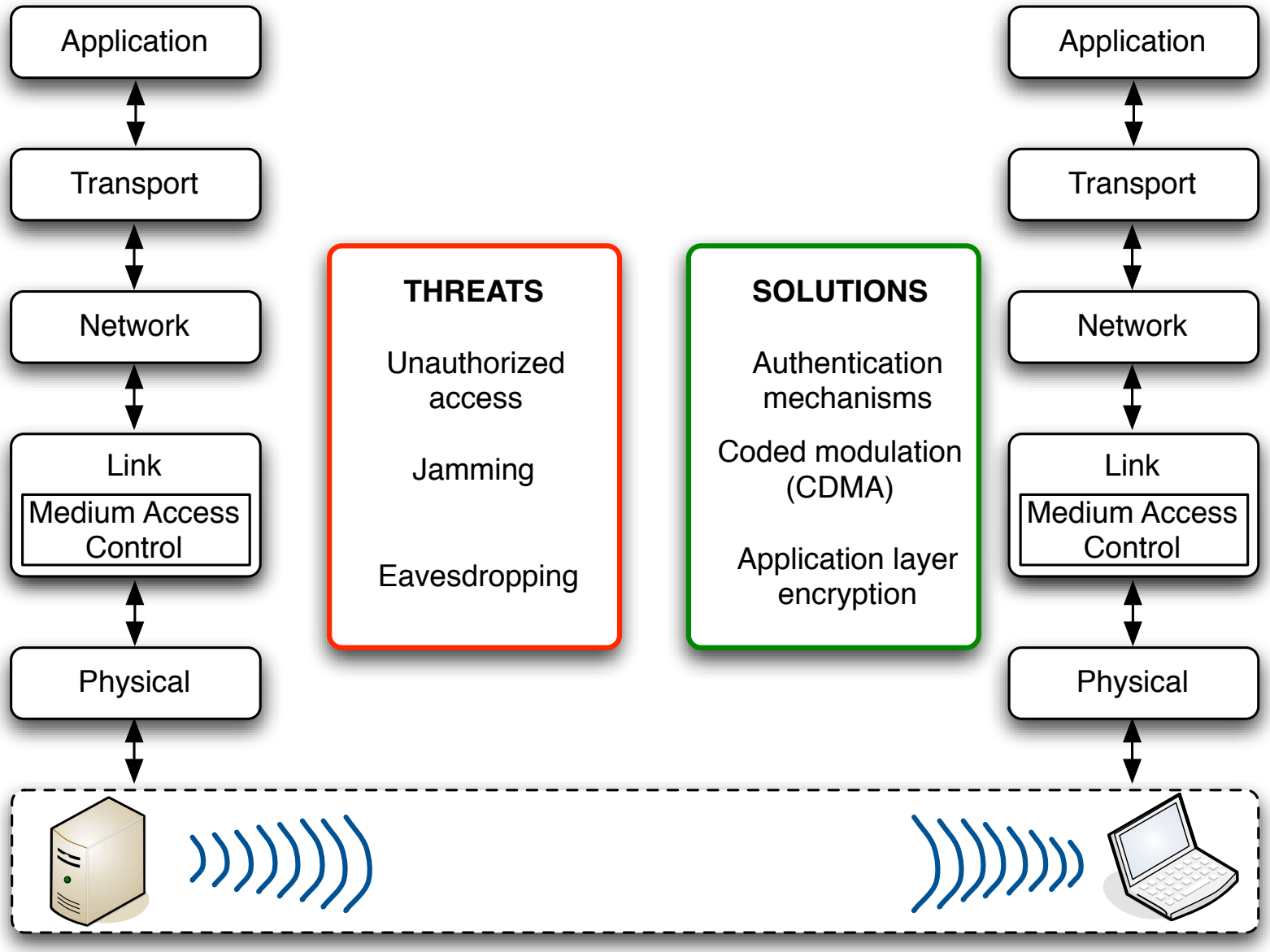
joint work with J. Nicholas Laneman

Agenda

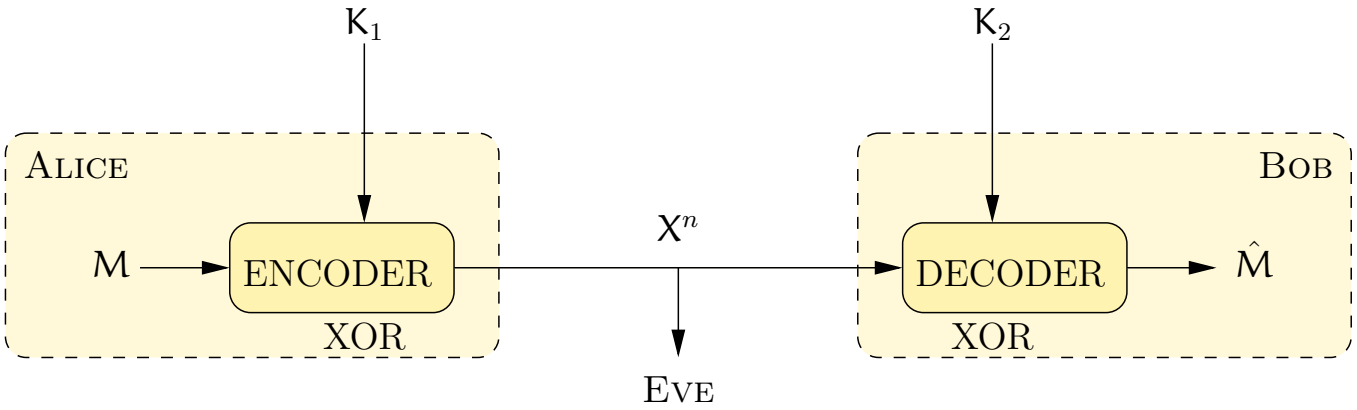
1. Physical-Layer Security
   - Computational security vs. information-Theoretic Security
   - Wiretap channel model
2. Secrecy Capacity of Arbitrary Wiretap Channels
   - Verdú-Han Information-Spectrum Approach
   - Security Criteria
   - Security and Resolvability
3. Applications
   - Discrete Memoryless Channels
   - Mixed Channels
   - Wiretap Channels with Channel State Information
4. Conclusion and Perspectives

Physical-Layer Security

Motivating example



Notions of security



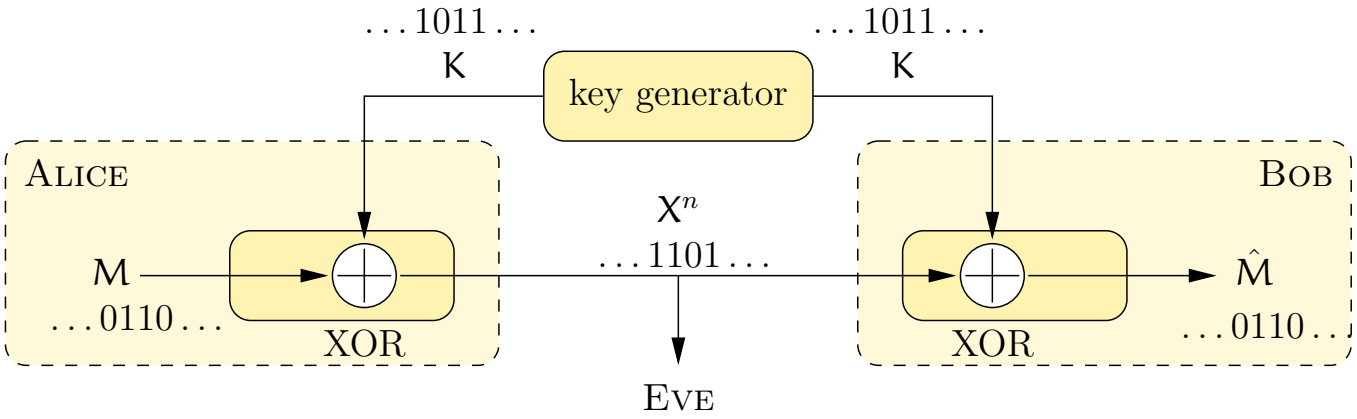
Computational security

- security based on mathematical conjectures
- assumptions on attacker's computational power
- effective in most situations

Perfect security

- strictest notion of security: $p(\mathrm{m}|\mathrm{x}^n) = p(\mathrm{m})$ $(\mathbb{I}(\mathrm{M};\mathrm{X}^n) = 0)$
- requires one-time pad and secret key such that $\mathbb{H}(\mathrm{K}) \geq \mathbb{H}(\mathrm{M})$

Notions of security



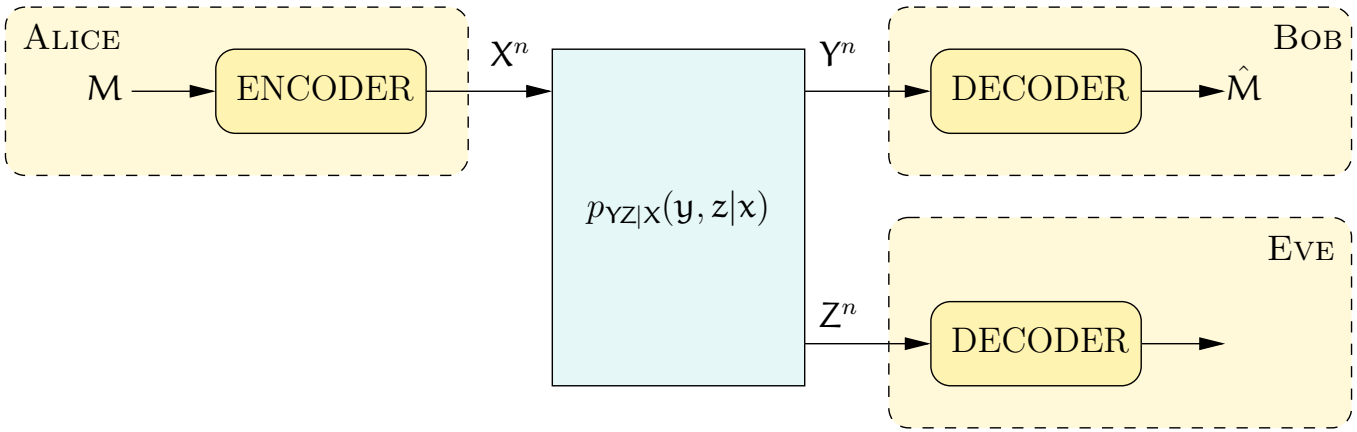
Computational security

- security based on mathematical conjectures
- assumptions on attacker's computational power
- effective in most situations

Perfect security

- strictest notion of security: $p(\mathrm{m}|\mathrm{x}^n) = p(\mathrm{m})$ $(\mathbb{I}(\mathrm{M};\mathrm{X}^n) = 0)$
- requires one-time pad and secret key such that $\mathbb{H}(\mathrm{K}) \geq \mathbb{H}(\mathrm{M})$

Communication over Wiretap Channel



- reliability constraint: $\mathbb{P}\left[M \neq \hat{M}\right] < \epsilon$
- secrecy constraint: $\frac{1}{n}\mathbb{H}(M|Z^n) \geq R - \epsilon$

Secrecy capacity of wiretap channel

- highest rate R_s such that constraints satisfied for all ϵ

$$C_s = \max_{V \to X \to YZ} \left[\mathbb{I}(V;Y) - \mathbb{I}(V;Z)\right]$$

- for noiseless channels $C_s = 0$

Caveats of Wiretap Channel Model

1. Knowledge of channel
   - wiretap channel model assumes perfect knowledge of channel
   - mainly results for memoryless case
2. Authentication
   - no protection against man-in-the-middle attacks
3. Passive attacker model
   - attacker cannot tamper with channel
4. Perfect random number generation
   - perfect randomness necessary for full secrecy
5. Definition of secrecy
   - common security criterion is weak
6. Scalability
   - model is hardly tractable in multi-user settings

Overcoming Caveats...

Understanding model is critical

Applicability of physical-layer security depends on assumptions.
$\Rightarrow$ Assumptions need to be credible

In this talk

1. Provide general framework for wiretap channel models
   - multi-user situations should be tractable
2. Strengthen existing results
   - use strongest secrecy criterion
3. Evaluate role of channel state information
   - how precise need channel state information be ?

Secrecy Capacity of Arbitrary Channels

Verdú-Han Information-Spectrum Approach

Information-Spectrum approach

- mutual information as a random variable

$$\mathrm{I}(\mathsf{X};\mathsf{Y}) := \log \frac{p_{\mathsf{XY}}(\mathsf{X},\mathsf{Y})}{p_{\mathsf{X}}(\mathsf{X})\, p_{\mathsf{Y}}(\mathsf{Y})} \qquad \mathbb{I}(\mathsf{X};\mathsf{Y}) = \mathbb{E}[\mathrm{I}(\mathsf{X};\mathsf{Y})]$$

- (rate)-information spectrum := density of $\frac{1}{n}\mathrm{I}(\mathsf{X};\mathsf{Y})$
- results expressed in terms of limsup and liminf in probability of random processes

A general formula for channel capacity

Arbitrary channel characterized by $\left\{p_{\mathsf{Y}^n|\mathsf{X}^n}(\mathsf{y}^n|\mathsf{x}^n)\right\}_{n=0}^{\infty}$

$$C = \max_{\{\mathsf{X}^n\}_{n=0}^{\infty}} \text{p-liminf}_{n\to\infty} \frac{1}{n}\mathrm{I}(\mathsf{X}^n;\mathsf{Y}^n)$$

Secrecy criteria

Message M is secure if M and Z^n are statistically independent.

- ideally: $\exists n_0 \geq 0$ such that $p_{\mathrm{M}\mathrm{Z}^{n_0}}(\mathrm{m}, \mathrm{z}^{n_0}) = p_{\mathrm{M}}(\mathrm{m})\, p_{\mathrm{Z}^{n_0}}(\mathrm{z}^{n_0})$
- realistically: $p_{\mathrm{M}\mathrm{Z}^{n}}(\mathrm{m}, \mathrm{z}^{n}) \approx p_{\mathrm{M}}(\mathrm{m})\, p_{\mathrm{Z}^{n}}(\mathrm{z}^{n})$ as $n \to \infty$

Secrecy criteria

$$\text{p-lim}_{n\to\infty}\, \mathbb{I}(\mathrm{M};\mathrm{Z}^n) = 0 \quad (1) \quad \text{strong secrecy}$$

$$\text{p-lim}_{n\to\infty}\, d(\mathrm{M},\mathrm{Z}^n) = 0 \quad (2) \quad \text{strong convergence in variational distance}$$

$$\text{p-lim}_{n\to\infty}\, |\mathrm{I}(\mathrm{M};\mathrm{Z}^n)| = 0 \quad (3) \quad \text{strong convergence of information spectrum}$$

$$\text{p-lim}_{n\to\infty}\, \frac{\mathbb{I}(\mathrm{M};\mathrm{Z}^n)}{n} = 0 \quad (4) \quad \text{weak secrecy}$$

$$\text{p-lim}_{n\to\infty}\, \frac{d(\mathrm{M},\mathrm{Z}^n)}{n} = 0 \quad (5) \quad \text{weak convergence in variational distance}$$

$$\text{p-lim}_{n\to\infty}\, \frac{|\mathrm{I}(\mathrm{M};\mathrm{Z}^n)|}{n} = 0 \quad (6) \quad \text{weak convergence of information spectrum}$$

Ordering of Secrecy Criteria

Ordering law

Criterion (i) is stronger than criterion (j) ($(i) \succeq (j)$) if and only if

$$(i)\,\text{satisfied} \;\Rightarrow\; (j)\,\text{satisfied}$$

Previous criteria can be ordered as

$$(1) \succeq (2) \succeq (3) \succeq (4) \succeq (5) \succeq (6)$$

Key issue

Which criteria are acceptable from a cryptographic perspective ?

Ordering of Secrecy Criteria

Example (Oviously flawed)

Let $\mathrm{u}^n = (\mathrm{u}_1, \ldots, \mathrm{u}_n)$ be a message. Let $\mathrm{k}^{n-k} = (\mathrm{k}_1, \ldots, \mathrm{k}_{n-k})$ be a uniformly distributed secret key. Encode as

$$\mathrm{x}^n = (\mathrm{u}_1 \oplus \mathrm{k}_1, \ldots, \mathrm{u}_{n-k} \oplus \mathrm{k}_{n-k}, \mathrm{u}_{n-k+1}, \ldots, \mathrm{u}_n)\,.$$

For this (dummy) scheme

$$\begin{aligned} \mathbb{I}(\mathrm{U}^n; \mathrm{X}^n) &= k \\ d\,(\mathrm{U}^n, \mathrm{X}^n) &> 0 \\ \frac{\mathbb{I}(\mathrm{U}^n; \mathrm{X}^n)}{n} \leq \frac{k}{n} &\leq \epsilon \quad \text{for } n \text{ large enough} \end{aligned}$$

Usual information-theoretic secrecy criterion is questionable !

Ordering of Secrecy Criteria

Example (Non-uniformity)

Let $\mathrm{u}^n = (\mathrm{u}_1, \ldots, \mathrm{u}_n)$ be a message. Let $\mathrm{k}^n = (\mathrm{k}_1, \ldots, \mathrm{k}_n)$ be a non-uniformly distributed secret key.

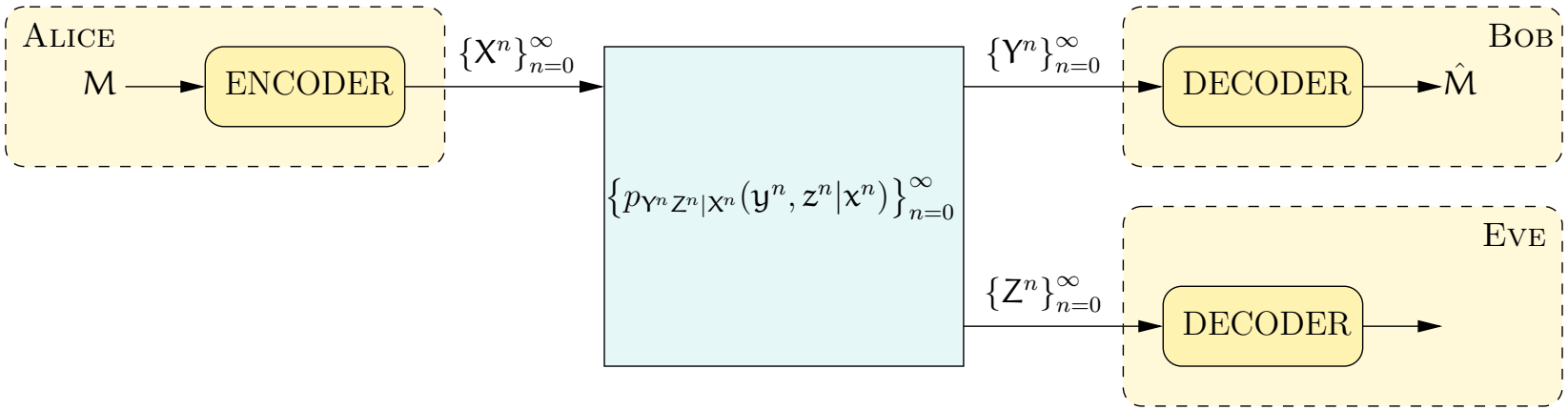
$$\mathbb{P}[\mathrm{K}^n = 0^n] = \frac{1}{n} \qquad \mathbb{P}[\mathrm{K}^n = \mathrm{k}^n] = \frac{1 - \frac{1}{n}}{2^n - 1}$$

Encode as $\mathrm{x}^n = (\mathrm{u}_1 \oplus \mathrm{k}_1, \ldots, \mathrm{u}_n \oplus \mathrm{k}_n)$
One can show

$$\mathbb{I}(\mathrm{U}^n; \mathrm{X}^n) \geq 1 - \epsilon$$
$$d\left(\mathrm{U}^n, \mathrm{X}^n\right) \to 0$$
$$\frac{\mathbb{I}(\mathrm{U}^n; \mathrm{X}^n)}{n} \to 0$$

Strong variational distance criterion is also questionable !

Arbitrary Wiretap Channels



Secrecy capacity

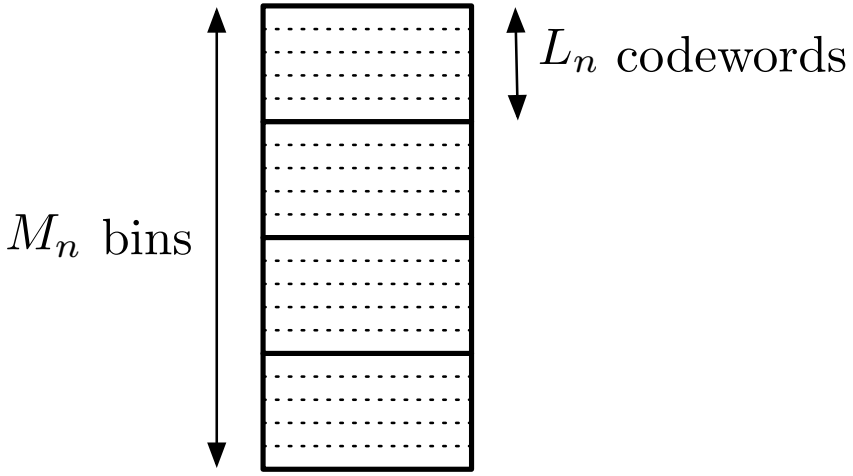
The secrecy capacity of an arbitraty wiretap channel under secrecy criteria (2)-(6) is

$$C_s = \max_{\{V^n, X^n\}_{n=1}^{\infty}} \left(\text{p-liminf}_{n\to\infty} \frac{1}{n} \mathrm{I}(V^n; Y^n) - \text{p-limsup}_{n\to\infty} \frac{1}{n} \mathrm{I}(V^n; Z^n) \right),$$

where $\{V^n, X^n\}_{n=1}^{\infty}$ is subject to $V^n \to X^n \to Z^n Y^n \quad \forall n \in \mathbb{N}^*$.

Secrecy and Resolvability

Key ingredients of wiretap coding: binning and stochastic encoding



$$d\left(p_{\mathsf{M}\mathsf{Z}^n}, p_{\mathsf{M}} p_{\mathsf{Z}^n}\right) \leq 2 \sum_{i=1}^{M_n} \frac{1}{M_n} d\left(p_{\mathsf{Z}^n|i}, \sum_{i=1}^{M_n} \frac{1}{M_n} p_{\mathsf{Z}^n|i}\right)$$

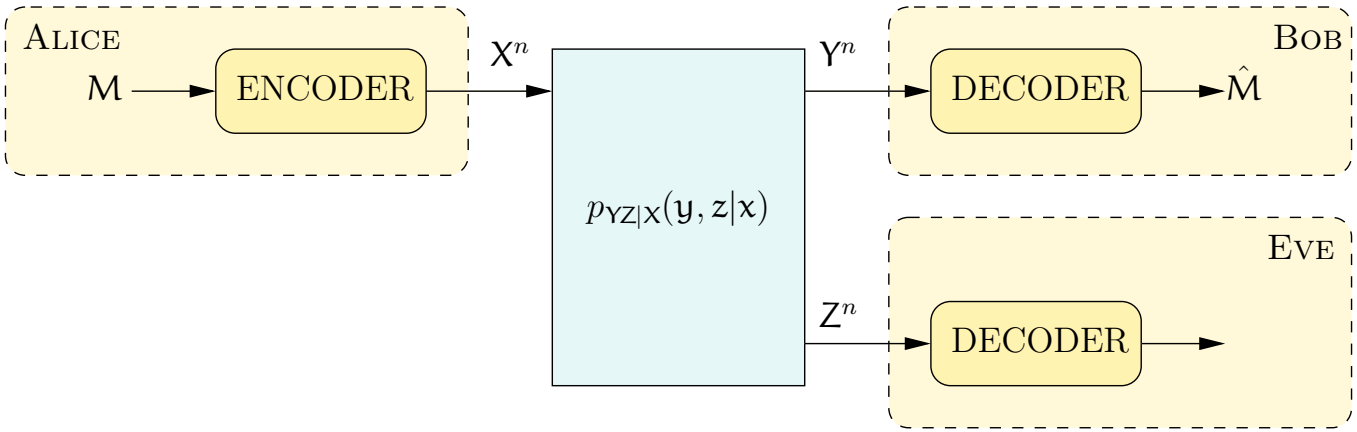
Each bin should induce same distribution at output of the channel.

- channel resolvability problem

$$\frac{1}{n} \log L_n \geq \text{p-limsup}_{n\to\infty} \frac{1}{n} \mathrm{I}(\mathsf{X}^n; \mathsf{Z}^n)$$

Applications

Discrete Memoryless Channels



Secrecy capacity follows from general formula

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

- achievability part is straightforward by law of large numbers
- converse does not follow easily

Mixed Wiretap Channel

Channel transition probabilities defined as

$$p_{\mathsf{Y}^n\mathsf{Z}^n|\mathsf{X}^n}(\mathsf{y}^n,\mathsf{z}^n|\mathsf{x}^n) = \alpha_1 p_{\mathsf{Y}_1^n\mathsf{Z}_1^n|\mathsf{X}^n}(\mathsf{y}^n,\mathsf{z}^n|\mathsf{x}^n) + \alpha_2 p_{\mathsf{Y}_2^n\mathsf{Z}_2^n|\mathsf{X}^n}(\mathsf{y}^n,\mathsf{z}^n|\mathsf{x}^n)\,.$$

Secrecy capacity of mixed channel

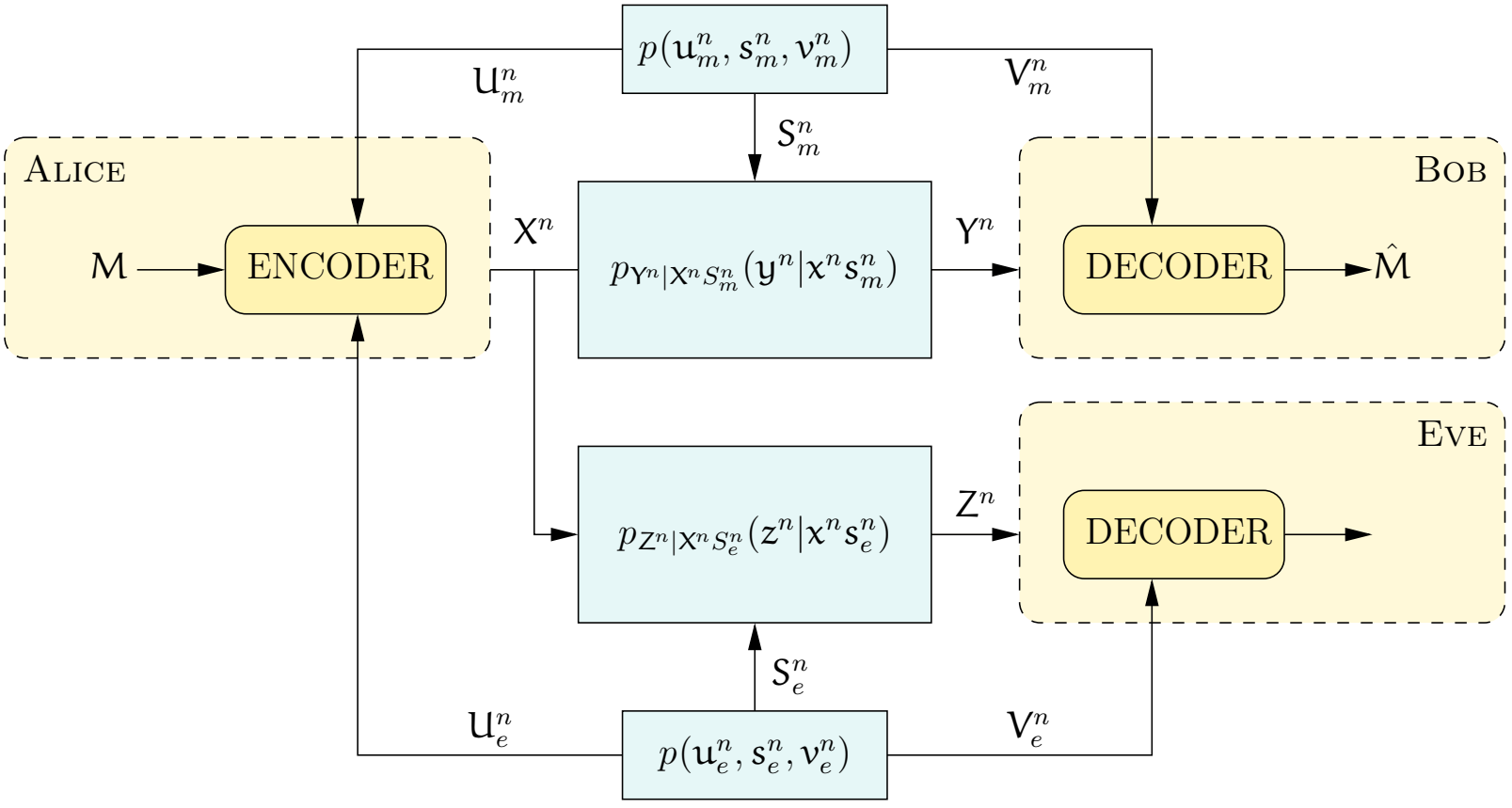
$$\max_{\{\mathsf{V}^n,\mathsf{X}^n\}_{n=1}^{\infty}} \left(\min_{i\in\{1,2\}} \text{p-liminf}_{n\to\infty} \frac{1}{n}\mathrm{I}(\mathsf{V}^n;\mathsf{Y}_i^n) - \max_{j\in\{1,2\}} \text{p-limsup}_{n\to\infty} \frac{1}{n}\mathrm{I}(\mathsf{V}^n;\mathsf{Z}_j^n) \right)$$

Secrecy capacity of memoryless mixed channels

$$C_s \geq \sup_{\mathsf{V}\to\mathsf{X}\to\mathsf{Y}_i\mathsf{Z}_j} \left(\min_{i\in\{1,2\}} \mathbb{I}(\mathsf{V};\mathsf{Y}_i) - \max_{j\in\{1,2\}} \mathbb{I}(\mathsf{V};\mathsf{Z}_j) \right)$$

Applications: parallel wiretap channels, broadcasting to many users, etc.

Wiretap Channels with Channel State Information



$$C_s = \max_{\{\mathsf{R}^n, \mathsf{T}^n\}_{n=1}^{\infty}} \left(\text{p-liminf}_{n\to\infty} \frac{1}{n} \mathrm{I}(\mathsf{R}^n; \mathsf{Y}^n | \mathsf{V}_m^n) \; - \text{p-limsup}_{n\to\infty} \frac{1}{n} \mathrm{I}(\mathsf{R}^n; \mathsf{Z}^n | \mathsf{V}_w^n) \right)$$

Gaussian Fading Wiretap Channel

Channel model

$$\begin{cases} Y_n = \sqrt{S_n} X_n + N_n^m & \text{with } N_n^m \sim \mathcal{N}(0,1) \\ Z_n = \sqrt{S'_n} X_n + N_n^e & \text{with } N_n^e \sim \mathcal{N}(0,1) \end{cases}$$

- $S_n \in \mathbb{R}^+$ and $S'_n \in \mathbb{R}^+$ are stationary ergodic processes
- Noisy CSIT: U_n and U'_n are noisy estimates of S_n and S'_n
- Perfect CSIR at both receivers: knowledge of received average SNR

$$V_n = S_n \mathbb{E}\left[|X_n|^2 | U_n\right] \qquad V'_n = S'_n \mathbb{E}\left[|X_n|^2 | U'_n\right]$$

- Average input power constraint $\mathbb{E}\left[X_n^2\right] \leq P$

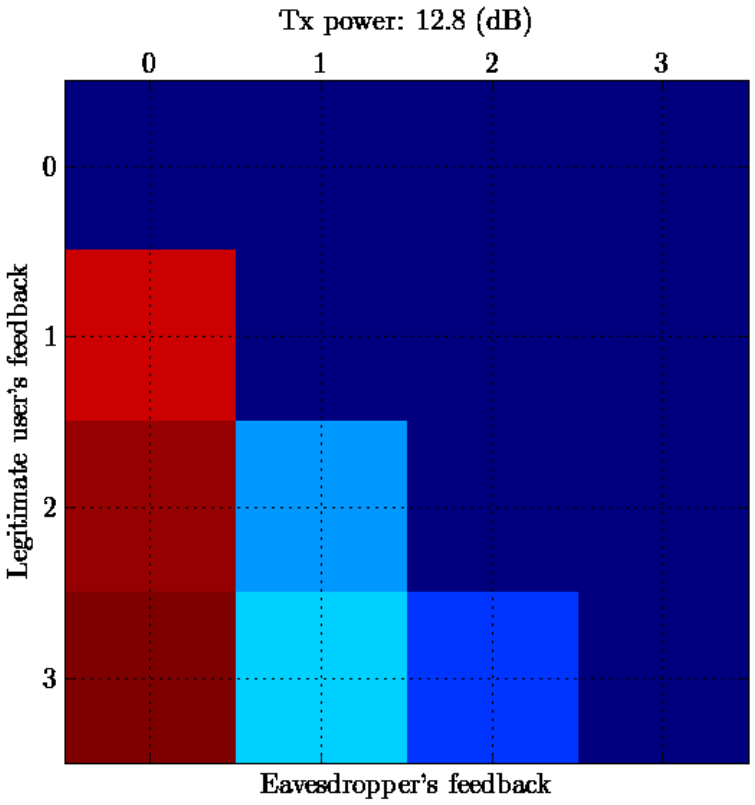
Lower bound on secrecy capacity

$$C_s \geq \max_{\gamma} \mathbb{E}_{S,S',U,U'} \left[\frac{1}{2} \log \left(\frac{1 + S\gamma(U,U')}{1 + S'\gamma(U,U')} \right) \right]$$

Gaussian Fading Wiretap Channel

Numerical example

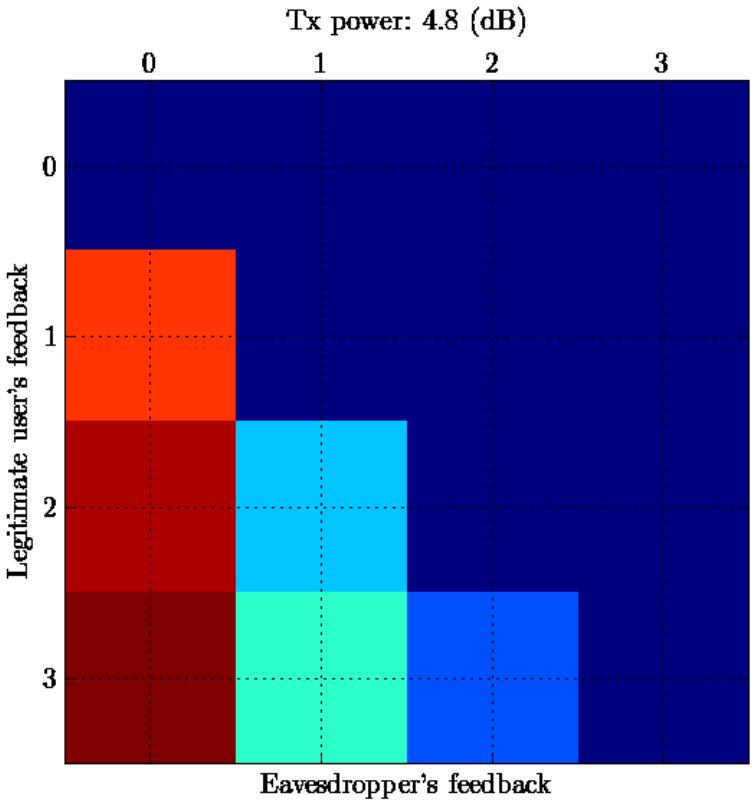
- Uniform fading on $[0, 2]$ for both channels
- U_n is b_m-bits uniform quantization feedback
- U'_n is b_w-bits quantization feedback



Gaussian Fading Wiretap Channel

Numerical example

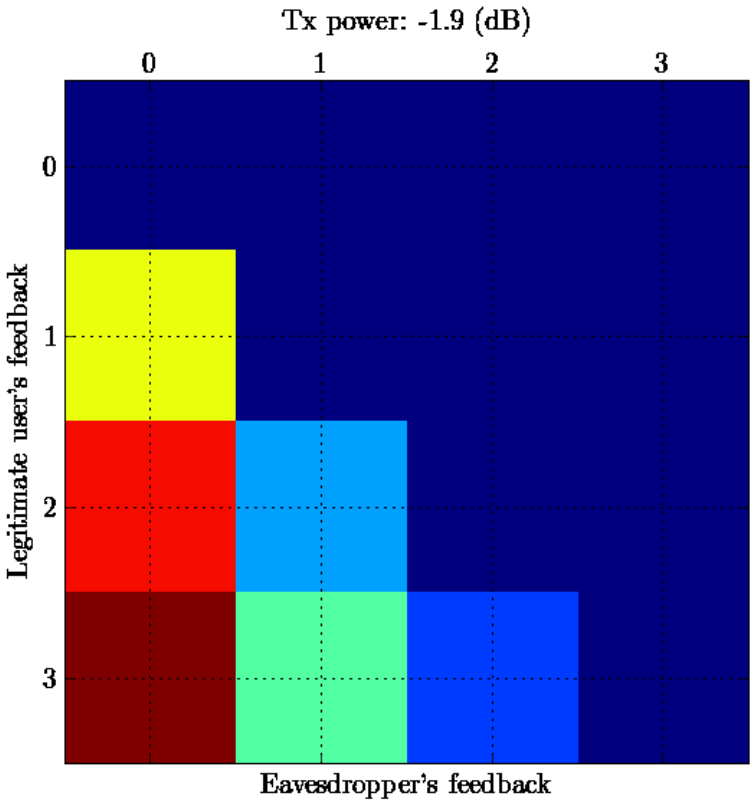
- Uniform fading on $[0, 2]$ for both channels
- U_n is b_m-bits uniform quantization feedback
- U'_n is b_w-bits quantization feedback



Gaussian Fading Wiretap Channel

Numerical example

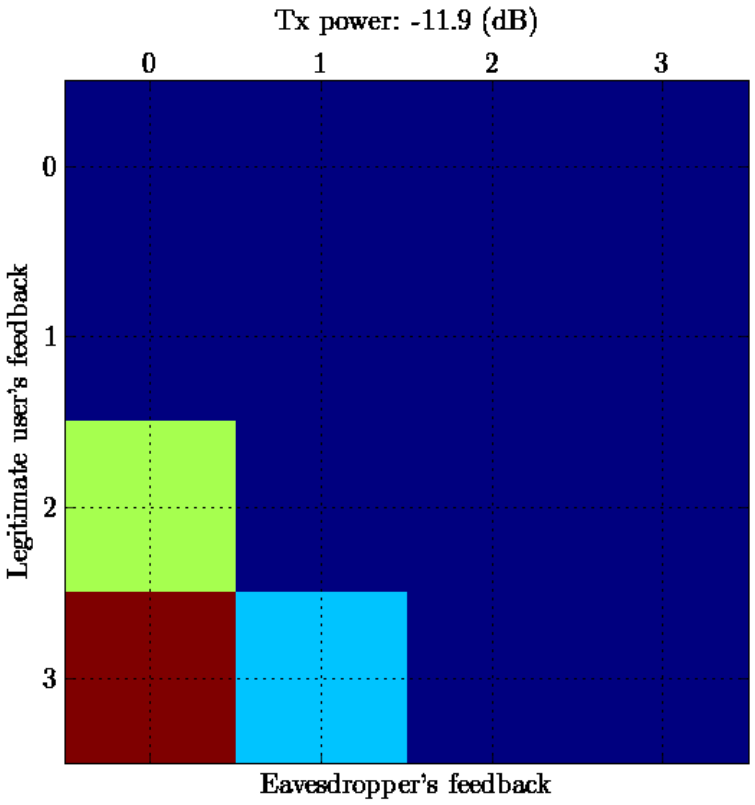
- Uniform fading on $[0, 2]$ for both channels
- U_n is b_m-bits uniform quantization feedback
- U'_n is b_w-bits quantization feedback



Gaussian Fading Wiretap Channel

Numerical example

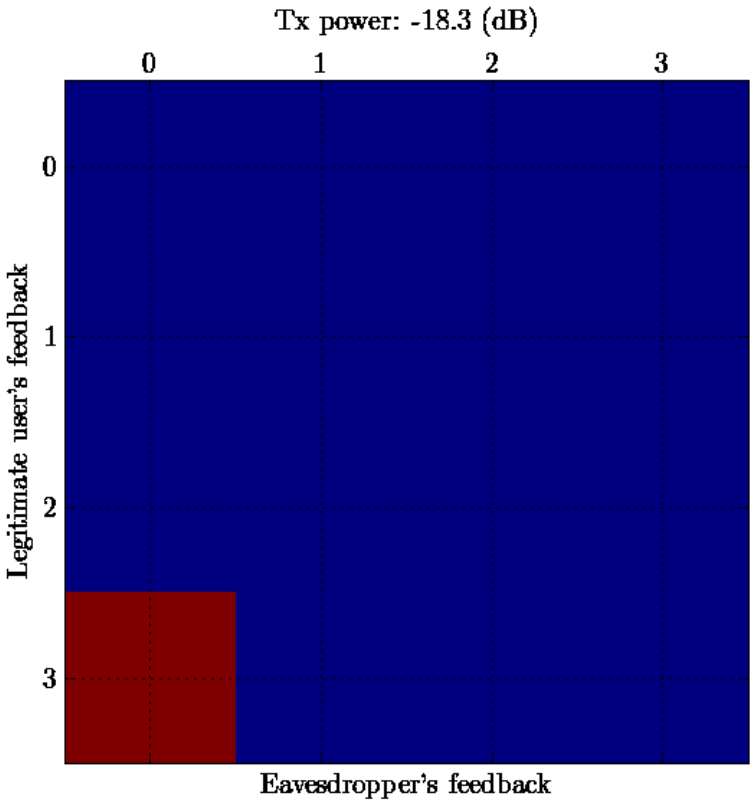
- Uniform fading on $[0, 2]$ for both channels
- U_n is b_m-bits uniform quantization feedback
- U'_n is b_w-bits quantization feedback



Gaussian Fading Wiretap Channel

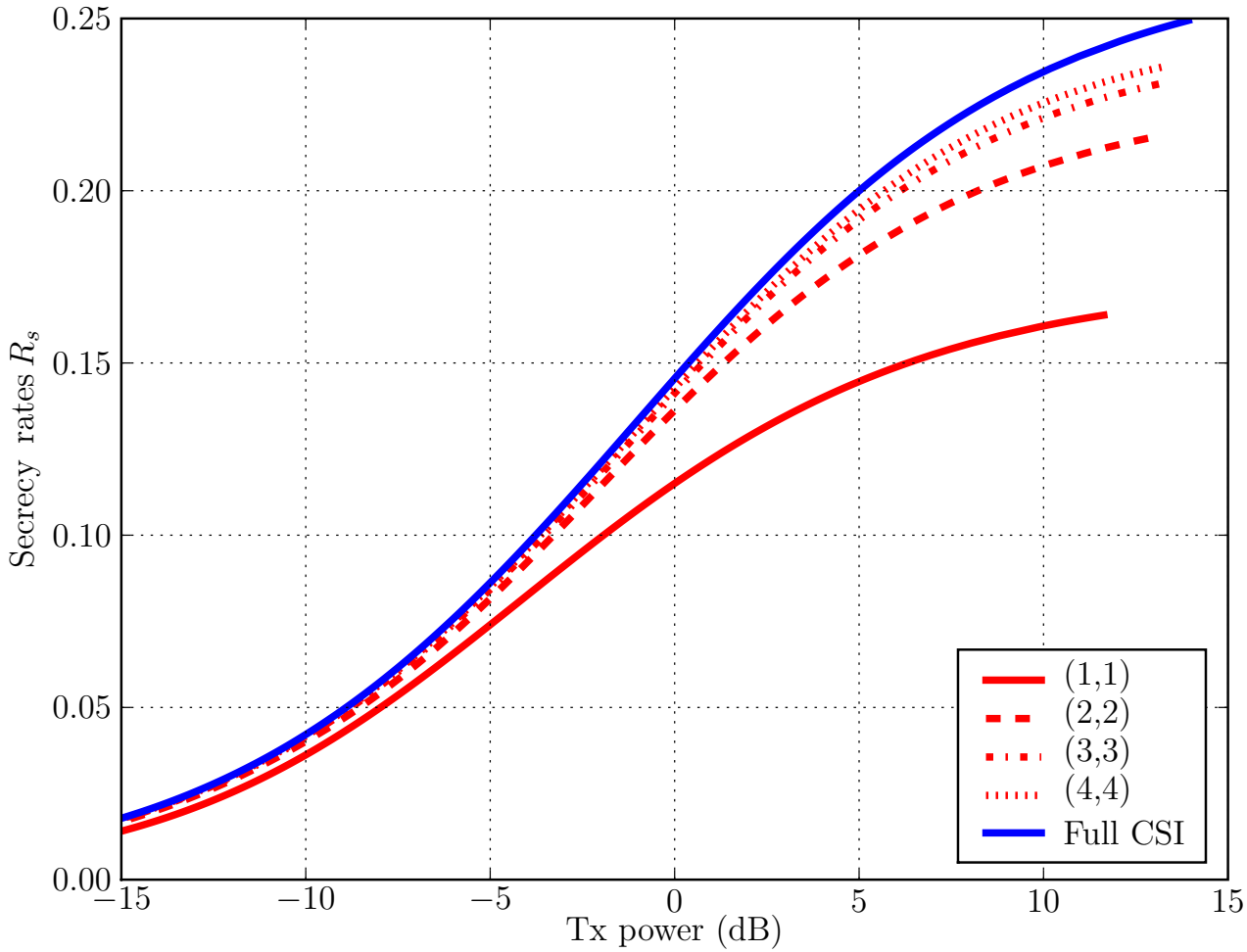
Numerical example

- Uniform fading on $[0, 2]$ for both channels
- U_n is b_m-bits uniform quantization feedback
- U'_n is b_w-bits quantization feedback



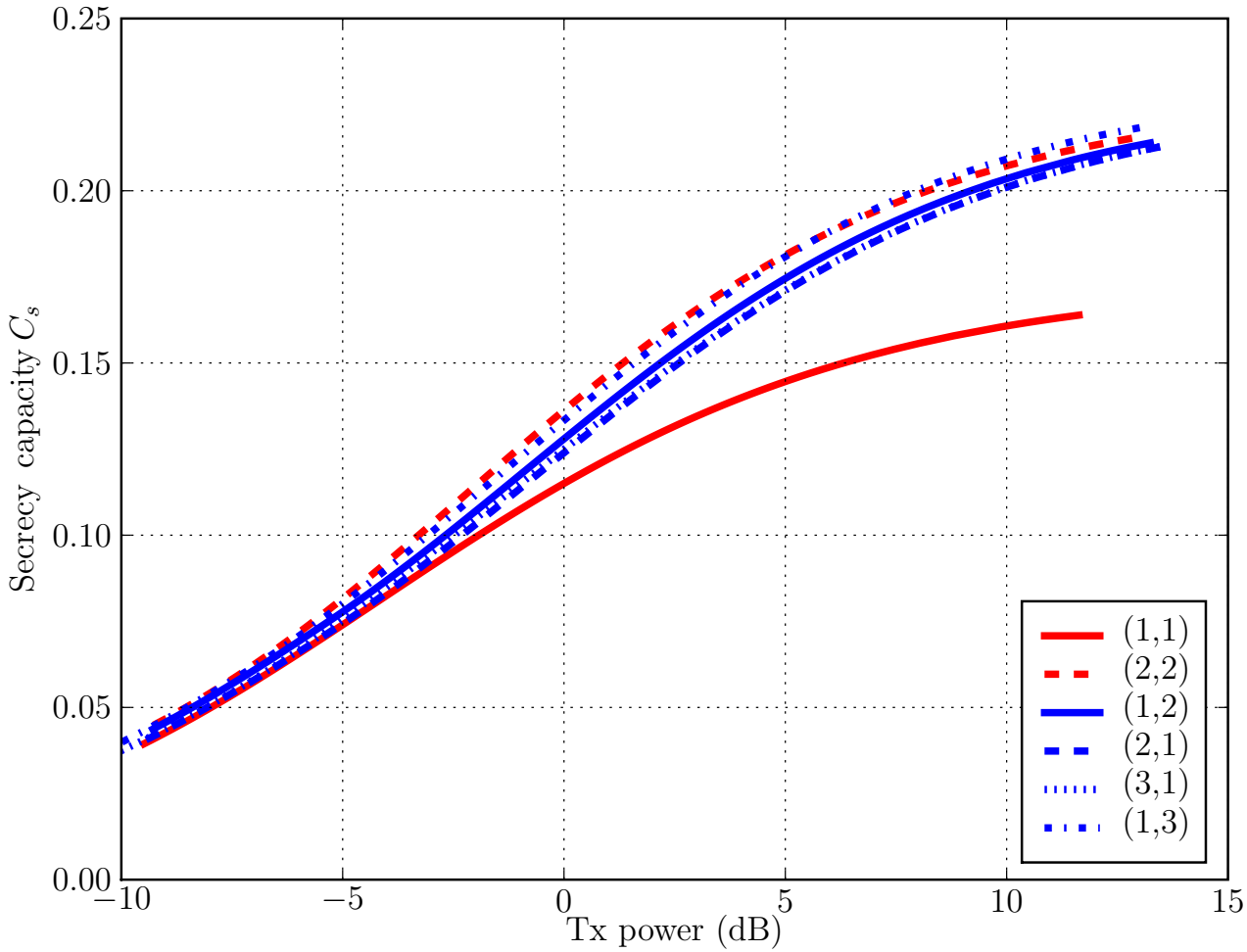
Gaussian Fading Wiretap Channel

Impact of number of feedback bits.



Gaussian Fading Wiretap Channel

Impact of number of feedback bits.



Agenda

1. Physical-Layer Security
   - Computational security vs. information-Theoretic Security
   - Wiretap channel model
2. Secrecy Capacity of Arbitrary Wiretap Channels
   - Verdú-Han Information-Spectrum Approach
   - Security Criteria
   - Security and Resolvability
3. Applications
   - Discrete Memoryless Channels
   - Mixed Channels
   - Wiretap Channels with Channel State Information
4. Conclusion and Perspectives

Conclusion

Information-spectrum approach is useful

- generalizes many wiretap channel models
- fundamentally different approach from Csiszár and Körner (channel resolvability)
- convenient way of computing achievable secure rates
- BUT usefulness somewhat limited for converse proofs

Channel state information impacts secrecy

- may not necessarily need much information
- may not require same precision for feedback

Perspectives

Feedback and security

- notion of feedback not captured in previous models
- feedback known to increase secrecy rates
- feedback may compensate absence of channel state information

Practical code constructions

- current results mostly of theoretical interest
- resolvability might provide an alternative approach

Fundamentals of Information-Theoretic Security

- A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1367, October 1975.
- I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.
- S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, July 1978.
- U. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, May 1993.
- U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in Advances in Cryptology - Eurocrypt 2000, Lecture Notes in Computer Science. B. Preneel, 2000, p. 351.
- S. Nitinawarat, "Secret key generation for correlated gaussian sources," in Proc. of 45th Allerton Conference on Communications, Control and Computing, Monticello, IL, USA, September 2007, pp. 1054–1058.

Information-Spectrum Approach

- T. Han and S. Verdú, "Approximation theory of output statistics," IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 752–772, 1993.
- S. Verdú and T. S. Han, "A general formula for channel capacity," IEEE Trans. Inf. Theory, vol. 40, no. 4, pp. 1147–1157, 1994.
- D. Kobayashi, H. Yamamoto, and T. Ogawa, "How to attain the ordinary channel capacity securely in wiretap channels," in Proc. IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005, pp. 13–18.
- H. Koga and N. Sato, "On an upper bound of the secrecy capacity for a general wiretap channel," in Proc. International Symposium on Information Theory ISIT 2005, Adelaide, Australia, September 2005, pp. 1641–1645.
- M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1562–1575, April 2006.
- M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in Proceedings of 46th Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 2008.

Multi-User Information-Theoretic Security

- I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.
- R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in Proc. of 44th Allerton Conference on Communication, Control and Computing, Urbana, IL, USA, September 2006, see also arXiv:cs/0702099.
- Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 976–1002, March 2008.
- E. Tekin and A. Yener, "The multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in Information Theory and Applications Workshop, San Diego, CA, USA, 2007.
- L. Lai and H. El-Gamal, "Cooperative secrecy: The relay-eavesdropper channel," in Proc. of IEEE International Symposium on Information Theory, Nice, France, July 2007, see also cs.IT/0612044.
- M. Yuksel and E. Erkip, "Secure communication with a relay helping the wire-tapper," in Proc. of IEEE Information Theory Workshop, Lake Tahoe, California, September 2007, pp. 595–600.
- Y. Oohama, "Coding for relay channels with confidential messages," in Proc. IEEE Information Theory Workshop, Cairns, Australia, September 2001, pp. 87–89.
- M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in Proceedings of the IEEE Information Theory Workshop, Porto, Portugal, May 2008, pp. 154–158.

Pratical Information-Theoretic Security

- C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized Privacy Amplification," IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, 1995.
- C. Cachin and U. M. Maurer, "Linking Information Reconciliation and Privacy Amplification," Journal of Cryptology, vol. 10, no. 2, pp. 97–110, March 1997.
- M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Transactions on Information Theory, special issue on Information Theoretic Security, vol. 54, no. 6, pp. 2515–2534, June 2008.
- L. H. Ozarow and A. D. Wyner, "Wire Tap Channel II," AT&T Bell Laboratories Technical Journal, vol. 63, no. 10, pp. 2135–2157, December 1984.
- A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channels," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
- R. Liu, Y. Liang, H. V. Poor, and P. Spasojević, "Secure nested codes for type II wiretap channels," in Proceedings of IEEE Information Theory Workshop, Lake Tahoe, California, USA, September 2007, pp. 337–342.