Mechanisms of Physical-Layer Security

Securenets 2011 ▪ May 20th, 2011

Matthieu Bloch
Georgia Institute of Technology
School of Electrical and Computer Engineering

Motivation

Secrecy metrics and examples

Information-Theoretic Secrecy Metrics

Perfect versus asymptotic secrecy

- Message $M \in [\![1, 2^{nR}]\!]$ observed through Z^n
  - joint distribution p_{MZ^n}
- Perfect secrecy: M statistically independent of Z^n
  - distribution $p_{MZ^n} = p_M p_{Z^n}$
- Asymptotic perfect secrecy: M statistically independent of Z^n in the limit of n going to ∞

$$\lim_{n\to\infty} S_i(p_{MZ^n}, p_M p_{Z^n}) = 0$$

Information-Theoretic Secrecy Metrics

Choice of metrics

- Kullback-Leibler divergence

$$S_1(p_{MZ^n}, p_M p_{Z^n}) = \mathbb{D}(p_{MZ^n} \| p_M p_{Z^n})$$
$$S_4(p_{MZ^n}, p_M p_{Z^n}) = \frac{1}{n}\mathbb{D}(p_{MZ^n} \| p_M p_{Z^n})$$

- Variational distance

$$S_2(p_{MZ^n}, p_M p_{Z^n}) = \mathbb{V}(p_{MZ^n}, p_M p_{Z^n})$$
$$S_5(p_{MZ^n}, p_M p_{Z^n}) = \frac{1}{n}\mathbb{V}(p_{MZ^n}, p_M p_{Z^n})$$

- Probability of outage

$$S_3(p_{MZ^n}, p_M p_{Z^n}) = \mathbb{P}(\mathrm{I}(M; Z^n) > \epsilon)$$
$$S_6(p_{MZ^n}, p_M p_{Z^n}) = \mathbb{P}(\tfrac{1}{n}\mathrm{I}(M; Z^n) > \epsilon)$$

Information-Theoretic Secrecy Metrics

Not all metrics are equal

Ordering of secrecy metrics

$$S_1 \succcurlyeq S_2 \succcurlyeq S_3 \succcurlyeq S_4 \succcurlyeq S_5 \succcurlyeq S_6$$

[Bloch & Laneman, 2008]

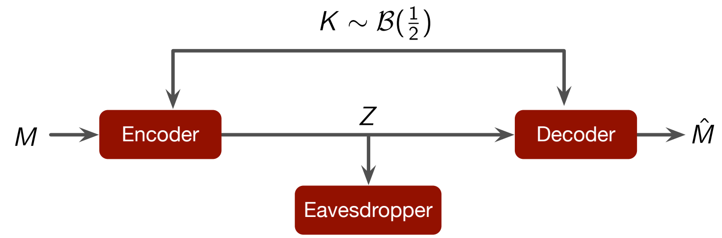
Expectations

Coding mechanisms should ensure secrecy for all metrics
Fundamental limits should not depend on specific metric

Coding Mechanisms

Secure communication

- Shannon's cipher system



- One-time pad guarantees that all messages induce the same distribution :

$$\forall m \in \{-1, +1\},\ p_{Z|M=m} = \text{cst}$$

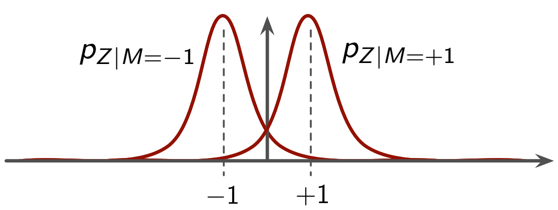
[Shannon 1949; Forney 2003]

Coding Mechanisms

Secure communication

- Transmission over noisy Gaussian channel

$$M \in \{-1, +1\} \quad Z = M + N \text{ with } N \sim \mathcal{N}(0, \sigma^2)$$



- Channel noise induces similar distributions
- Can we code using the same principle ?

Coding Mechanisms

Secret-key distillation

- Extraction of secret bits from noisy observations

$$Z \in \{-1; +1\} \quad Z \sim \mathcal{B}(\tfrac{1}{2})$$

$$X = Z + N \text{ with } N \sim \mathcal{N}(0, \sigma^2)$$

  - One can show $\mathbb{V}\left(p_{K|Z=\pm 1}, p_K\right) = \mathcal{O}(\sigma^{-3})$

- Possible to extract secrecy from noisy source
- Can we code using the same principle ?

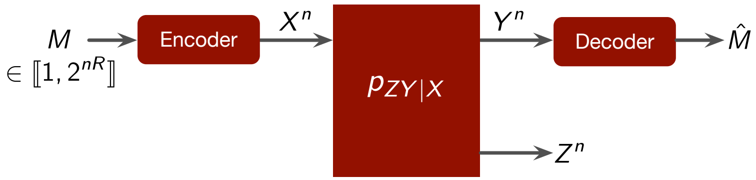
Goals of Talk

- Discuss coding mechanisms for secure communication over noisy channels
- Discuss coding mechanisms for secret-key distillation from noisy sources
- Get insight into the design of practical coding schemes

Channel Resolvability

Coding for secure communication

Wiretap Channel Model



- Reliability $P_e(\mathcal{C}_n) = \mathbb{P}\left(M \neq \hat{M} | \mathcal{C}_n\right)$
- Secrecy $S_2(\mathcal{C}_n) = \mathbb{V}\left(p_{MZ^n|\mathcal{C}_n}, p_M p_{Z^n|\mathcal{C}_n}\right)$
- R is achievable if $\lim_{n\to\infty} P_e(\mathcal{C}_n) = \lim_{n\to\infty} S_2(\mathcal{C}_n) = 0$
- Secrecy capacity $C_s^{WT} = \sup\{R\colon R \text{ is achievable}\}$

[Wyner 1975; Csiszár & Körner 1978]

Secrecy from Resolvability

- How do we ensure secrecy ?

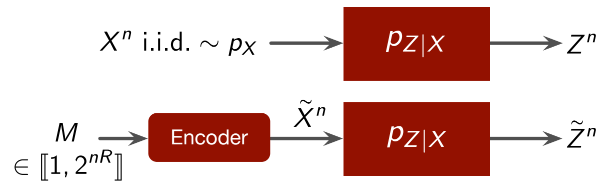
$$\mathbb{V}\left(p_{MZ^n|\mathcal{C}_n}, p_M p_{Z^n|\mathcal{C}_n}\right) \leqslant 2 \sum_m p_M(m) \mathbb{V}\left(p_{Z^n|M=m,\mathcal{C}_n}, q_{Z^n}\right)$$

- $p_{Z^n|M=m,\mathcal{C}_n}$ distribution induced by message m
- q_{Z^n} “target distribution”

Sufficient condition for secrecy

All messages should induce the same distribution

Channel Resolvability



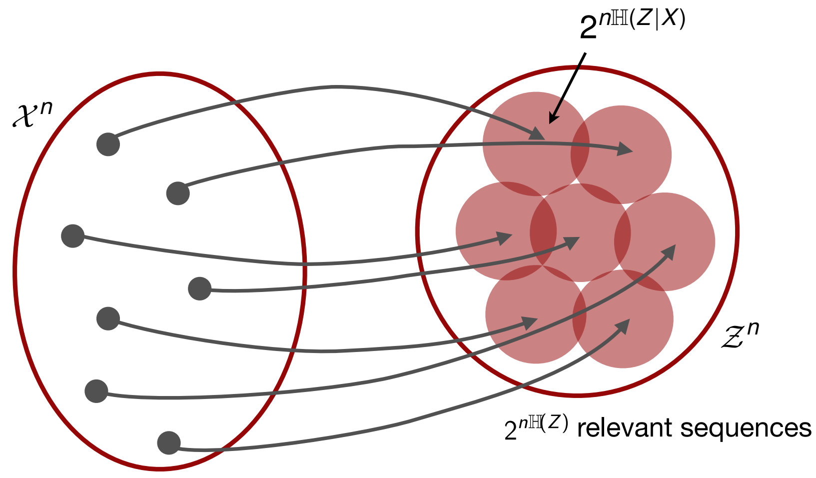
- Simulation $\mathbb{V}\left(p_{Z^n}, p_{\tilde{Z}^n}\right)$
- R is achievable if $\lim_{n\to\infty} \mathbb{V}\left(p_{Z^n}, p_{\tilde{Z}^n}\right) = 0$

Achievable rates

If $R > \mathbb{I}(X;Z)$, then R is achievable

[Han & Verdu 1993]

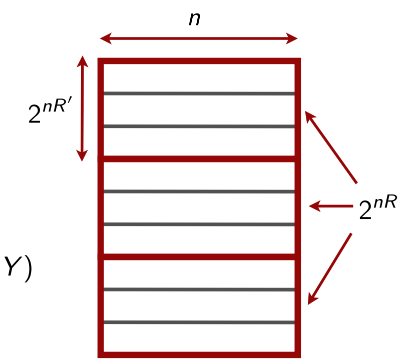
Channel Resolvability



minimum number of balls required: $2^{n\mathbb{I}(X;Z)}$

Coding Structure of Wiretap Codes

- Binning structure
  - message index bin
  - codeword selected at random
- Intuitively
  - Few enough codewords to ensure reliability: $R + R' < \mathbb{I}(X;Y)$
  - Bins large enough to guarantee resolvability: $R' > \mathbb{I}(X;Z)$



$R < \mathbb{I}(X;Y) - \mathbb{I}(X;Z)$

[Hayashi 2006, Bloch & Laneman 2008]

Capacity Versus Resolvability

- "Capacity-based" wiretap codes
  - Code structure based on capacity
  - Few enough codewords to ensure reliability
  - Bins are capacity achieving codes $R' = \mathbb{I}(X;Z) - \epsilon_n$

Resolvability is more powerful than capacity

- Random capacity-based codes cannot achieve strong secrecy capacity
- Random resolvability-based codes achieve strong secrecy capacity

[Bloch 2011; Luzzi & Bloch 2011]

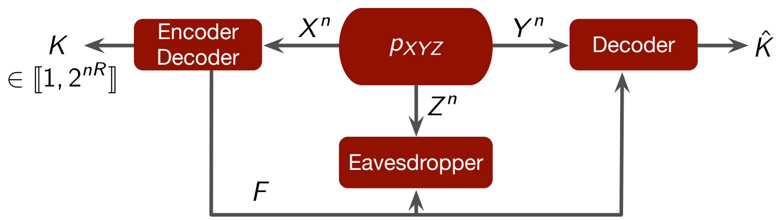
Take Aways

- Resolvability as coding mechanism for secure communication
- Coding operates with strong secrecy metrics
- Many applications
- Insight into strongly secure codes ?

Channel Intrinsic Randomness

Coding for secret-key distillation

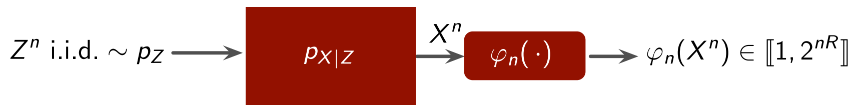
Secret-Key Distillation Model



- Uniformity $U(\mathcal{S}_n) = \mathbb{V}(p_K, p_U)$
- Reliability $P_e(\mathcal{S}_n) = \mathbb{P}\left(K \neq \hat{K}|\mathcal{S}_n\right)$
- Secrecy $S_2(\mathcal{S}_n) = \mathbb{V}\left(p_{KZ^nF|\mathcal{S}_n}, p_K p_{Z^nF|\mathcal{S}_n}\right)$
- R is achievable if $\lim_{n\to\infty} P_e(\mathcal{S}_n) = \lim_{n\to\infty} S_2(\mathcal{S}_n) = \lim_{n\to\infty} U(\mathcal{S}_n) = 0$

[Maurer 1993; Ahlswede & Csiszár 1978]

Channel Intrinsic Randomness



- Simulation $\mathbb{V}\left(p_{\varphi_n(X^n)}, p_U\right)$
- Independence $\mathbb{V}\left(p_{\varphi_n(X^n)Z^n}, p_{\varphi(X^n)}p_{Z^n}\right)$
- R is achievable if

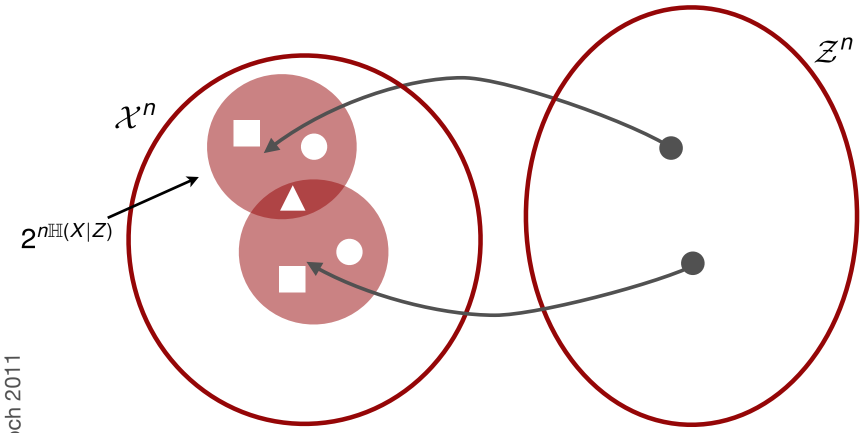
$$\lim_{n\to\infty} \mathbb{V}\left(p_{\varphi_n(X^n)}, p_U\right) = \lim_{n\to\infty} \mathbb{V}\left(p_{\varphi_n(X^n)Z^n}, p_{\varphi(X^n)}p_{Z^n}\right) = 0$$

Channel intrinsic randomness

R is achievable if and only if $R < \mathbb{H}(X|Z)$

[Csiszar, 1996, Bloch 2010]

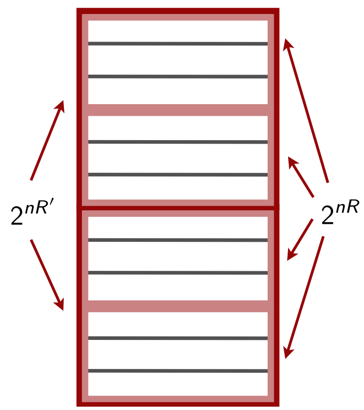
Channel Intrinsic Randomness



maximum number of bins allowed: $2^{n\mathbb{H}(X|Z)}$

Coding Structure of Key-Distillation Scheme

- Binning structure
  - observed sequences fall into bins
  - use bin index for public information and key
- Intuitively
  - enough bins to ensure reliability:
    $R' > \mathbb{H}(X|Y)$
  - bins small enough to guarantee intrinsic randomness:
    $R < \mathbb{H}(X|Z)$



$R_k < \mathbb{H}(X|Z) - \mathbb{H}(X|Y)$

Capacity Versus Intrinsic Randomness

- "Capacity-based" key-distillation strategies
  - Code structure based on capacity
  - Enough bins to ensure reliability
  - Bins are capacity achieving for source coding with side information $R' = \mathbb{H}(X|Z) + \epsilon_n$

Intrinsic randomness is more powerful than capacity

- No capacity-based key-distillation can achieve strong secrecy capacity
- Intrinsic randomness-based strategies can achieve strong secrecy (privacy amplification)

[Watanabe *et al.* 2009, Bennett *et al.* 1995]

Take Aways

- Intrinsic randomness as coding mechanism for secret-key distillation
- Fundamentally different from secure communications
- How existing key-distillation techniques operate (privacy amplification)

Conclusion

Wrapping Up

- Channel Intrinsic Randomness as coding mechanism for secret-key distillation from noisy sources
- Channel Resolvability as coding mechanism for secure communication over noisy channels
- Powerful and (conceptually) simple information-theoretic tools
  - Applications to general settings
  - Guidelines for code design

Follow Up

- References

  - Bloch & Laneman, "Secrecy from resolvability," on arXiv soon
  - Pierrot & Bloch, "Strongly secure communication over the two-way wiretap channel," *IEEE Trans. Info. Forensics and Security,* 2011, arXiv:1010.0177
  - Bloch, "Achieving secrecy: capacity vs. resolvability," *ISIT 2011*
  - Luzzi & Bloch, "Capacity-based random codes cannot achieve strong secrecy over symmetric wiretap channels," *Securenets 2011*
  - Bloch, "Channel intrinsic randomness," *ISIT 2010*