Information-Theoretic Secrecy Metrics

Perfect versus asymptotic secrecy

- Message $M \in [1, 2^n]$ observed through $Z^n$
  - joint distribution $p_{MZ^n}$
- Perfect secrecy: $M$ statistically independent of $Z^n$
  - distribution $p_{MZ^n} = p_{MPZ^n}$
- Asymptotic perfect secrecy: $M$ statistically independent of $Z^n$ in the limit of $n$ going to $\infty$
  \[
  \lim_{n \to \infty} S_i(p_{MZ^n}, p_{MPZ^n}) = 0
  \]

Motivation

Secrecy metrics and examples

- Kullback-Leibler divergence
  \[
  S_i(p_{MZ^n}, p_{MPZ^n}) = \mathbb{D}(p_{MZ^n} \parallel p_{MPZ^n})
  \]
  \[
  S_4(p_{MZ^n}, p_{MPZ^n}) = \frac{1}{n} \mathbb{D}(p_{MZ^n} \parallel p_{MPZ^n})
  \]
- Variational distance
  \[
  S_2(p_{MZ^n}, p_{MPZ^n}) = \mathcal{V}(p_{MZ^n}, p_{MPZ^n})
  \]
  \[
  S_3(p_{MZ^n}, p_{MPZ^n}) = \frac{1}{n} \mathcal{V}(p_{MZ^n}, p_{MPZ^n})
  \]
- Probability of outage
  \[
  S_1(p_{MZ^n}, p_{MPZ^n}) = \mathbb{P}(I(M; Z^n) > \epsilon)
  \]
  \[
  S_6(p_{MZ^n}, p_{MPZ^n}) = \mathbb{P}(\frac{1}{n} I(M; Z^n) > \epsilon)
  \]
Information-Theoretic Secrecy Metrics

Not all metrics are equal

Ordering of secrecy metrics

\[ S_1 \succ S_2 \succ S_3 \succ S_4 \succ S_5 \succ S_6 \]

[Block & 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
  \[ K \sim B(\frac{1}{2}) \]

- One-time pad guarantees that all messages induce the same distribution:
  \[ \forall m \in \{-1, +1\}, P_{Z|M=m} = \text{cst} \]

Coding Mechanisms

Transmission over noisy Gaussian channel

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

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

Coding Mechanisms

Secret-key distillation

- Extraction of secret bits from noisy observations
  \[ Z \in \{-1, +1\} \quad Z \sim B(\frac{1}{2}) \]
  \[ X = Z + N \quad N \sim \mathcal{N}(0, \sigma^2) \]

- One can show
  \[ \forall (p_K|Z=\pm1, P_K) = O(\sigma^{-3}) \]

- 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

- $M \in [1, 2^R]$ 
- Encoder 
- $X^n$ 
- $P_{ZY|X}$ 
- Decoder 
- $Y^n$ 
- $\hat{M}$ 
- $Z^n$

- Reliability $P_e(C_n) = \mathbb{P}(M \neq \hat{M}|C_n)$
- Secrecy $S_2(C_n) = \mathbb{V}(P_{MZ^n|C_n}, P_{MPZ^n|C_n})$
- $R$ is achievable if $\lim_{n \to \infty} P_e(C_n) = \lim_{n \to \infty} S_2(C_n) = 0$
- Secrecy capacity $C_s^{WT} = \sup \{R : R$ is achievable$\}$

Secrecy from Resolvability

- How do we ensure secrecy?
  \[ \mathbb{V}(P_{MZ^n|C_n}, P_{MPZ^n|C_n}) \leq 2 \sum_m \rho_M(m) \mathbb{V}(P_{Z^n|M=m, C_n}, q_{z^n}) \]
- $P_{Z^n|M=m, C_n}$ distribution induced by message $m$
- $q_{z^n}$ “target distribution”

Sufficient condition for secrecy

All messages should induce the same distribution
Channel Resolvability

$$X^n \text{ i.i.d. } p_X \xrightarrow{P} Z^n$$

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

**Achievable rates**

If $R > I(X; Z)$, then $R$ is achievable

[Han & Verdu 1993]

---

Coding Structure of Wiretap Codes

- Binning structure
  - message index bin
  - codeword selected at random

- Intuitively
  - Few enough codewords to ensure reliability: $R + R' < I(X; Y)$
  - Bins large enough to guarantee resolvability: $R' > I(X; Z)$

- $2^{nR'}$

$2^{n\mathbb{I}(Z|X)}$

$2^{n\mathbb{I}(Z)}$ relevant sequences

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

- [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 $R' = I(X; Z) - \epsilon_n$

- 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**

- Simulation $\mathbb{V}(p_{\varphi_n(X^n)}, p_U)$
- Independence $\mathbb{V}(p_{\varphi_n(X^n)Z^n}, p_{\varphi(X^n)Z^n})$
- $R$ is achievable if
  \[\lim_{n \to \infty} \mathbb{V}(p_{\varphi_n(X^n)}, p_U) = \lim_{n \to \infty} \mathbb{V}(p_{\varphi_n(X^n)Z^n}, p_{\varphi(X^n)Z^n}) = 0\]

---

Secret-Key Distillation Model

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

---

Channel intrinsic randomness

$R$ is achievable if and only if $R < H(X|Z)$

---

[Matthieu Bloch 2011]
Channel Intrinsic Randomness

- \(X^n\) and \(Z^n\) are the input and output sequences of the channel.
- \(2^{nI(X;Z)}\) is the maximum number of bins allowed.

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: \(R' > H(X|Y)\).
  - Bins small enough to guarantee intrinsic randomness: \(R < H(X|Z)\).

- \(R_k < H(X|Z) - H(X|Y)\)

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: \(R' = H(X|Z) + \epsilon_n\).

- 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).

Take Aways

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