From Shannon's Cipher System to Secret Key Agreement

Parthajit Mohapatra

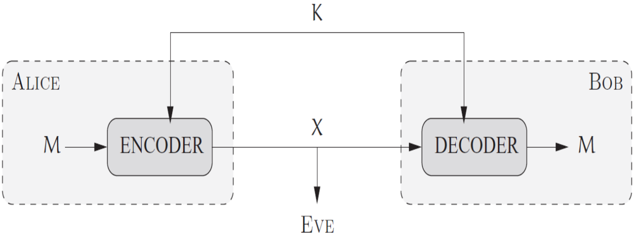
ECE Department, Indian Institute of Science, Bangalore

19th Aug. 2014

Outline

- Shannon's cipher system
- Wiretap channel
- Secret-key agreement
    - Source model
        - Sequential key distillation strategy
    - Channel model

Shannon's cipher system



- Secret key (K)
  - Known to Alice and Bob, but not known to Eve
  - K is independent of M

Encoding and decoding

- Encoder

$$e : \mathcal{M} \times \mathcal{K} \to \mathcal{X}$$

- Decoder

$$d : \mathcal{X} \times \mathcal{K} \to \mathcal{M}$$

- (e, d): coding scheme
- Eve's knowledge
  - No knowledge about key
  - Assume to know e and d

Secrecy measure

- Equivocation: $H(M|X)$

Perfect secrecy

A coding scheme is said to achieve perfect secrecy if

$$H(M|X) = H(M) \Leftrightarrow I(M;X) = 0$$

- Codewords X are statistically independent of the message M

Proposition

If a coding scheme for Shannon's cipher system achieves perfect secrecy, then

$$H(K) \geq H(M)$$

- Necessary to use at least one secret-key bit for each message bit

Secure communication over noisy channel

- Shannon's result
  - Key length should be as large as the message
  - Perfect secrecy is a stringent measure
- What happens when Eve listens through a different channel as compared to Bob
- Different secrecy measure is used

Weak and strong secrecy

- Exact statistical independence between message M and Eve's observations Z^n $\rightarrow$ asymptotic statistical independence

$$\lim_{n\to\infty} d(P_{MZ^n}, P_M P_{Z^n}) = 0$$

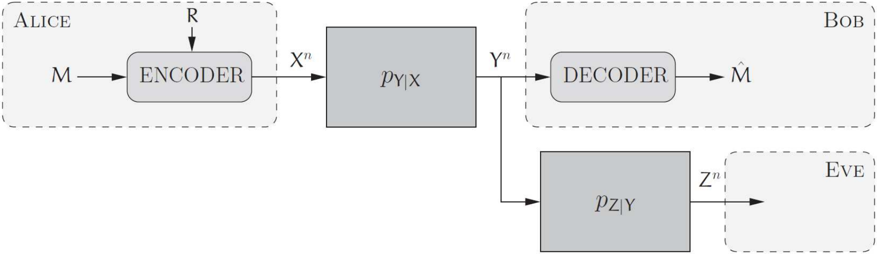
- $d(.,.)$: Kullback-Leibler divergence

$$\lim_{n\to\infty} I(M, Z^n) = 0 \qquad \text{(Strong secrecy condition)}$$

- Weak secrecy condition

$$\lim_{n\to\infty} \frac{1}{n} I(M, Z^n) = 0$$

Wiretap channel



- Secrecy capacity was originally introduced by Wyner

Theorem

The secrecy capacity of a DWTC $(\mathcal{X}, p_{Z|Y}p_{Y|X}, \mathcal{Y}, \mathcal{Z})$ is

$$C_s^{\text{DWTC}} = \max_{p_X}[I(X;Y) - I(X;Z)]$$

- If $Y = Z$, then $C_s^{\text{DWTC}} = 0$
- $C_s^{\text{DWTC}} \geq C_m - C_e$
- Stochastic encoding is crucial to enable secure communication[1]

[1] There is no point in considering stochastic decoder

Role of noise in security

- Wiretap channel
  - Communications are inherently rate limited
  - One-way
- When secrecy capacity is zero
  - Lack of any physical advantage over the eavesdropper

or

  - Restrictions imposed on the communication schemes

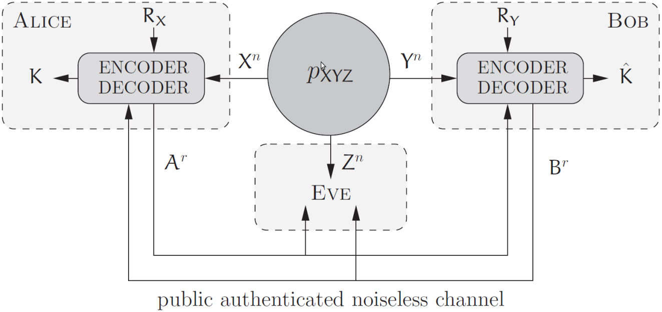
Goal

How much secrecy one can extract from thee noise itself in the form of a secret key?

Role of noise in security

- Secret key agreement
  - The legitimate parties (Alice and Bob) and eavesdropper (Eve) observes realization of correlated RVs
  - Legitimate parties attempt to agree on a secret key to the eavesdropper
- Standard models
  - Source model
  - Channel model

Source model



- Can exchange message over noiseless, two-way and authenticated channel
- Two-way channel is public
- Uncontrollable external source

Key-distillation strategy

- A $(2^{nR}, n)$ key-distillation strategy $\mathcal{S}_n$ for a source model with DMS $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$ consists of[2]
  - Key alphabet $\mathcal{K} = [1, 2^{nR}]$
  - Alphabet $\mathcal{A}$ used by Alice to communicate over the channel
  - Source of local randomness for Alice $(\mathcal{R}_{\mathcal{X}}, p_{R_X})$
  - r: number of rounds of communications
  - r encoding functions $f_i : \mathcal{X}^n \times \mathcal{B}^{i-1} \times \mathcal{R}_{\mathcal{X}} \to \mathcal{A}$ for $i \in [1, r]$
  - Key-distillation function $\kappa_a : \mathcal{X}^n \times \mathcal{B}^r \times \mathcal{R}_{\mathcal{X}} \to \mathcal{K}$

[2] Only defined for Alice

Performance measures

- Average probability of error

$$P_e(S_n) = P(K \neq \hat{K}|S_n)$$

- Information leakage to the eavesdropper

$$L(S_n) = I(K; Z^n A^r B^r|S_n)$$

- Uniformity of the key

$$U(S_n) = \log\lceil 2^{nR}\rceil - H(K|S_n)$$

Secret-key capacity

- A weak secret-key rate R is achievable if there exists a sequence of $(2^{nR}, n)$ key-distillation strategies $\{S_n\}_{n\geq 1}$ s.t.
  - $\lim_{n\to\infty} P_e(S_n) = 0$ (Reliability)
  - $\lim_{n\to\infty} \frac{1}{n} L(S_n) = 0$ (Weak secrecy)
  - $\lim_{n\to\infty} \frac{1}{n} U(S_n) = 0$ (Weak uniformity)

Theorem

The weak secret-key capacity of a source model $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$ satisfies

$$I(X;Y) - \min\{I(X;Z), I(Y;Z)\} \leq C_s^{SM} \leq \min\{I(X;Y), I(X;Y|Z)\}$$

Comments on secret-key capacity

- The lower bound is in general loose
- Can be obtained using
  - Using wiretap code or
  - Slepian-wolf codes
- Above techniques does not give any insight for practical schemes
- Is it possible to handle reliability and secrecy requirements independently

Sequential key distillation

- Randomness sharing: Alice, Bob and Eve observe n realizations of a DMS $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$
- Advantage distillation: Alice and Bob exchange messages observe the public channel to distill obsn. for which they have an advantage over Eve
- Information reconciliation: Alice and Bob communicate with each other to agree on a common bit sequence
- Privacy amplification: Alice and Bob publicly agree on a deterministic function and used it to generate a secret key from the common sequence

Advantage distillation

- Suppose Eve has an advantage over both Alice and Bob

$$I(X;Y) < I(X;Z) \text{ and } I(X;Y) < I(Y;Z)$$

- Reverse Eve's advantage by exchanging messages over the public channel

- Crates a new DMS $(\mathcal{X}'\mathcal{Y}'\mathcal{Z}', p_{X'Y'Z'})$ with components X', Y' and $Z' = Z^n A^r B^r$ such that

$$I(X';Y') \geq I(X';Z') \text{ or } I(X';Y') \geq I(Y';Z')$$

- Performance measure: advantage distillation rate

$$R(D_n) = \frac{1}{n}\max[I(X';Y') - I(X';Z'), I(X';Y') - I(Y';Z')]$$

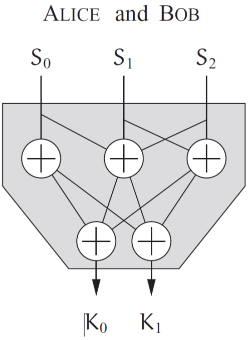
Information reconciliation

- Allow Alice and Bob to agree on a common sequence S
- Common message S could be function of
  - Alice and Bob's observations
  - Messages exchanged over the public channel
  - Can randomize their operations using sources of local randomness
- Reliability performance of a reconciliation protocol

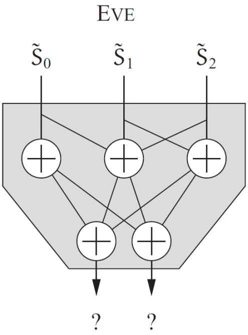
$$P_e = P(S \neq \hat{S} | R_n)$$

Privacy amplification

- Alice and Bob distill a secret key from S



function
f

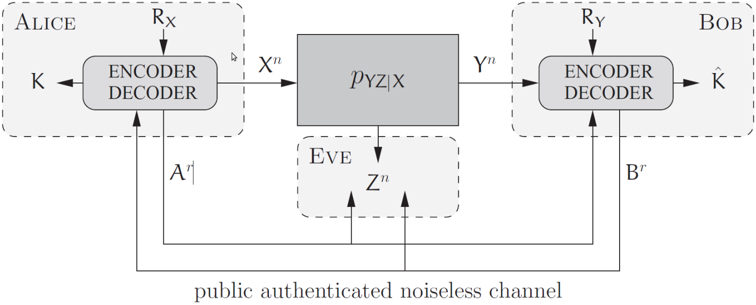


Privacy amplification contd.

- Types of functions
  - Hash function
    - Can produce significantly different outputs even when their inputs are quite similar
  - Extractors
    - Can output more uniform randomness then is used at the input

Channel model

- In the source model, Alice, Bob and Eve cannot control the external source
- What happens if the source is partially controlled by one of the parties
- If Eve controls, the problem is not fully understood
- Analysis is somewhat less difficult, when one of the legitimate parties controls the source
  - This model is called channel model for secret-key agreement



Theorem

The secret-key capacity C_s^{CM} of a channel model satisfies

$$\max\left[\max_{p_X}\{I(X;Y)-I(X;Z)\},\max_{p_X}\{I(X;Y)-I(Y;Z)\}\right]$$
$$\leq C_s^{\mathrm{CM}} \leq \max_{p_X}\min\{I(X;Y),I(X;Y|Z)\}$$