Secret Key Generation Using Compound Sources – Optimal Key-Rates and Communication Costs

Holger Boche and **Rafael Wyrembelski**

Technische Universität München
Lehrstuhl für Theoretische Informationstechnik

SCC 2013
Session Th3: Information Theory 2
January 24, 2013

Motivation

- Secret keys play an important role in cryptography
- Shared by transmitter and receiver, they can be used for encryption to keep eavesdroppers ignorant

➡ **Secret key generation** at distant locations is needed

- Major challenges for practical systems are
  - **Imperfect knowledge** – environment used for generation is known only imperfect
  - **Energy efficiency** – resources for generation should be as small as possible

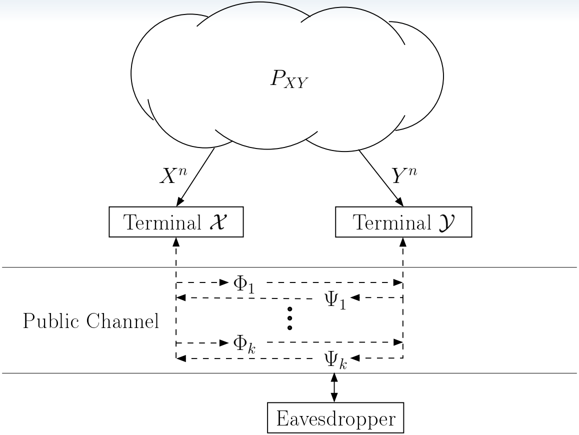
Motivation

- Secret keys play an important role in cryptography
- Shared by transmitter and receiver, they can be used for encryption to keep eavesdroppers ignorant

➠ **Secret key generation** at distant locations is needed

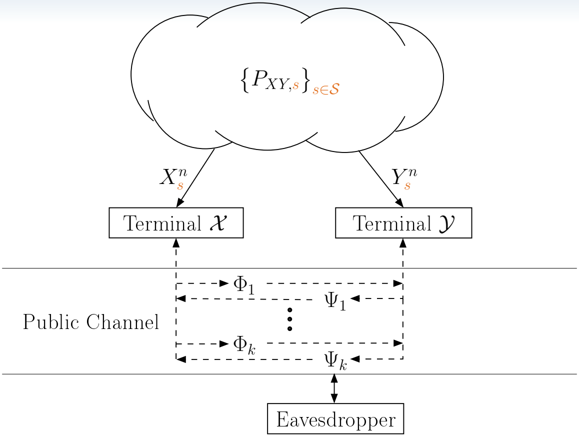
- Major challenges for practical systems are
  - **Imperfect knowledge** – environment used for generation is known only imperfect
  - **Energy efficiency** – resources for generation should be as small as possible

Secret Key Generation



- First proposed by Ahlswede/Cisiszár and Maurer:
  - Two terminals observe correlated components of a source
  - Noiseless channel for public discussion available

Compound Sources



- In this paper: uncertainty in source statistics
  - Set of all statistics $\mathcal{S}$ is known – realization $s \in \mathcal{S}$ is **unknown**
  - Secret key generation has to work for all $s \in \mathcal{S}$ simultaneously!

Secret Key Generation Protocol

1. *Initialization:* Both terminals generate $M_{\mathcal{X}}$ and $M_{\mathcal{Y}}$ to include randomized strategies

2. *First exchange:* Both terminals exchange messages

$$\Phi_1 = \Phi_1(M_{\mathcal{X}}, X_s^n) : \mathcal{M}_{\mathcal{X}} \times \mathcal{X}^n \to \mathcal{K}_{\mathcal{Y},1}^n$$
$$\Psi_1 = \Psi_1(M_{\mathcal{Y}}, Y_s^n) : \mathcal{M}_{\mathcal{Y}} \times \mathcal{Y}^n \to \mathcal{K}_{\mathcal{X},1}^n$$

3. *i-th exchange:* Both terminals exchange messages

$$\Phi_i = \Phi_i(M_{\mathcal{X}}, X_s^n, \Psi^{i-1}) : \mathcal{M}_{\mathcal{X}} \times \mathcal{X}^n \times \mathcal{K}_{\mathcal{X},1}^n \times ... \times \mathcal{K}_{\mathcal{X},i-1}^n \to \mathcal{K}_{\mathcal{Y}_i}^n$$
$$\Psi_i = \Psi_i(M_{\mathcal{Y}}, Y_s^n, \Phi^{i-1}) : \mathcal{M}_{\mathcal{Y}} \times \mathcal{Y}^n \times \mathcal{K}_{\mathcal{Y},1}^n \times ... \times \mathcal{K}_{\mathcal{Y},i-1}^n \to \mathcal{K}_{\mathcal{X}_i}^n$$

4. *After k exchanges:* Both terminals compute the secret key as

$$K = K(M_{\mathcal{X}}, X_s^n, \Psi^k) \quad \text{and} \quad L = L(M_{\mathcal{Y}}, Y_s^n, \Phi^k)$$

with $K, L \in \mathcal{K}^n$ the set of all possible keys

Secret Key Generation Protocol

Definition: Achievable Key Rate

A number $R_{key} \in \mathbb{R}_+$ is said to be an *achievable key rate* if for any $\epsilon > 0$ and sufficiently large n there is a secret key generation protocol such that K and L satisfy

$$\mathbb{P}\{K \neq L\} < \epsilon \tag{1a}$$

$$I(\Phi^k, \Psi^k; K) < \epsilon \tag{1b}$$

$$\frac{1}{n} H(K) > R_{key} - \epsilon \tag{1c}$$

$$\frac{1}{n} \log |\mathcal{K}^n| < \frac{1}{n} H(K) + \epsilon. \tag{1d}$$

The *key-capacity* C_{key} is the supremum of all achievable key rates.

(1a) Ensures both terminals generated the same key

(1b) **Strong secrecy** – eavesdropper gets nothing from public discussion

(1d) Secret key is nearly uniformly distributed (desirable for encryption)

Costs of Public Communication

Definition: Costs of Public Communication

For a key-capacity achieving protocol, the *costs of public communication* $R_{public}^{(k)}$ are given by

$$R_{public}^{(k)} = \limsup_{n\to\infty} \frac{1}{n} \sum_{i=1}^{k} \big(\log |\mathcal{K}_{\mathcal{X},i}^{n}| + \log |\mathcal{K}_{\mathcal{Y},i}^{n}| \big).$$

The minimum over all such protocols yields the *minimum costs of public communication* given by

$$C_{public}^{(k)} = \inf R_{public}^{(k)}.$$

Key-Capacity

- Ahlswede/Csiszár obtained for the non-compound case

Theorem: Key-Capacity

The *key-capacity* is given by

$$C_{key} = I(X;Y)$$

and can be achieved by a single forward (or backward) transmission only.

- They do not consider the problem of minimum costs explicitly
- By inspection, the communication costs of their protocol are

$$R_{public}^{forward} = H(X|Y)$$

R. Ahlswede and I. Csiszár, ''Common Randomness in Information Theory and Cryptography-Part I: Secret Sharing,'' *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993

Key-Capacity for Compound Sources

- Back to our problem with compound sources

Theorem: Key-Capacity for Compound Sources

i) The *key-capacity* for compound sources is

$$C_{key} = \min_{s \in \mathcal{S}} I(X_s; Y_s)$$

and can be achieved by a single forward (or backward) transmission only.

ii) For a single forward transmission and perfect secrecy, i.e., $I(\Phi; K) = 0$, the minimum costs of public communication are

$$C_{public}^{forward} = \max_{s \in \mathcal{S}} H(X_s | Y_s).$$

Comments on Key-Capacity

- In principle, proof technique of Ahlswede/Csiszár can easily be adapted to achieve key-capacity $C_{key} = \min_{s\in\mathcal{S}} I(X_s;Y_s)$

  ➠ Will result in **non-optimal** communication costs

$$R_{forward}^{public} = \max_{s\in\mathcal{S}} H(X_s) - \min_{s\in\mathcal{S}} I(X_s;Y_s)$$

➠ Necessitates more sophisticated protocol to achieve also the minimum costs $C_{public}^{forward} = \max_{s\in\mathcal{S}} H(X_s|Y_s)$

- Two phase protocol:
  - Based on own observed source outputs, terminals estimate own source statistic
  - Then use Ahlswede/Csiszár approach based on Slepian-Wolf coding to the reduced compound channel

Comments on Key-Capacity (2)

- Key-capacity

$$C_{key} = \min_{s\in\mathcal{S}} I(X_s;Y_s)$$

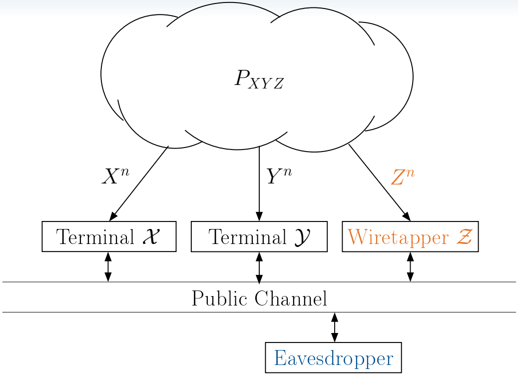
remains the same for different protocols (e.g. single forward / single backward)

➠ Mutual information is symmetric in X_s and Y_s!

- Costs of public communication depends on the protocol
  - Single forward transmission: $\max_{s\in\mathcal{S}} H(X_s|Y_s)$
  - Single backward transmission: $\max_{s\in\mathcal{S}} H(Y_s|X_s)$

➠ Entropy terms are **not** symmetric in X_s and Y_s!

Secret Key Generation with Wiretapper



- Introduce additional wiretapper which observes his own Z^n

➠ Two classes of attacks:
  - Overhearing the public discussion (eavesdropper)
  - Having additional access to the source (wiretapper)

First Results

- Two classes of secret keys:
  - $K^{(1)}$: secret from the eavesdropper
  - $K^{(2)}$: secret from the eavesdropper and wiretapper!
    - Require now $I(\Phi^k, \Psi^k, Z^n; K^{(2)}) < \epsilon$

Theorem: Sum Key-Capacity

For a single forward transmission, the *sum key-capacity* $C_{key,\Sigma}$ is given by

$$C_{key,\Sigma} = I(X;Y).$$

Main idea:

- Use wiretap code that achieve $R_{key}^{(2)} = I(X;Y) - I(X;Z)$
- Penalty term $I(X;Z)$ is used to "confuse" the wiretapper – but it is secure from the eavesdropper so that $R_{key}^{(1)} = I(X;Z)$

I. Bjelaković, H. Boche, and J. Sommerfeld, ‘‘Secrecy Results for Compound Wiretap Channels,’’ *Probl. Inf. Transmission*, 2012, accepted, available at http://arxiv.org/abs/1106.2013

First Results (2)

- Sum key-capacity looks similar to the key-capacity of the first result
- Wiretap codes make the analysis of communication costs difficult
  - ➠ Becomes tractable for Markov chain $X - Y - Z$

Corollary:

If $X - Y - Z$ forms a Markov chain, for a single forward transmission the *key-capacity region* for secret keys $(K^{(1)}, K^{(2)})$ is given by all rate pairs $(R_{key}^{(1)}, R_{key}^{(2)}) \in \mathbb{R}_+^2$ that satisfy

$$R_{key}^{(1)} \leq I(X;Z)$$
$$R_{key}^{(2)} \leq I(X;Y) - I(X;Z).$$

Furthermore, for perfect secrecy, the minimum costs of public communication are

$$C_{public}^{forward} = H(X|Y).$$

Conclusion

- Studied **secret key generation using compound sources**
  - Key-capacity
  - Costs of public communication

- Key-capacity is $C_{key} = \min_{s \in \mathcal{S}} I(X_s; Y_s)$
  - Can be achieved by different protocols (forward or backward)
  - Expression is symmetric in X_s and Y_s

- Costs of public communication are $C_{public}^{forward} = \max_{s \in \mathcal{S}} H(X_s | Y_s)$
  - Depends on the applied protocol
  - Straightforward extension of Ahlswede/Csiszár yields non-optimal costs!
  - ⇒ Requires a novel adaptive two-phase protocol!

Thank you for your attention!

Conclusion

- Studied **secret key generation using compound sources**
  - Key-capacity
  - Costs of public communication

- Key-capacity is $C_{key} = \min_{s \in \mathcal{S}} I(X_s; Y_s)$
  - Can be achieved by different protocols (forward or backward)
  - Expression is symmetric in X_s and Y_s

- Costs of public communication are $C_{public}^{forward} = \max_{s \in \mathcal{S}} H(X_s|Y_s)$
  - Depends on the applied protocol
  - Straightforward extension of Ahlswede/Csiszár yields non-optimal costs!
  - Requires a novel adaptive two-phase protocol!

Thank you for your attention!

Conclusion

- Studied **secret key generation using compound sources**
  - Key-capacity
  - Costs of public communication

- Key-capacity is $C_{key} = \min_{s \in \mathcal{S}} I(X_s; Y_s)$
  - Can be achieved by different protocols (forward or backward)
  - Expression is symmetric in X_s and Y_s

- Costs of public communication are $C_{public}^{forward} = \max_{s \in \mathcal{S}} H(X_s | Y_s)$
  - Depends on the applied protocol
  - Straightforward extension of Ahlswede/Csiszár yields non-optimal costs!

  ➠ Requires a novel adaptive two-phase protocol!

Thank you for your attention!

Conclusion

- Studied **secret key generation using compound sources**
  - Key-capacity
  - Costs of public communication

- Key-capacity is $C_{key} = \min_{s\in\mathcal{S}} I(X_s;Y_s)$
  - Can be achieved by different protocols (forward or backward)
  - Expression is symmetric in X_s and Y_s

- Costs of public communication are $C_{public}^{forward} = \max_{s\in\mathcal{S}} H(X_s|Y_s)$
  - Depends on the applied protocol
  - Straightforward extension of Ahlswede/Csiszár yields non-optimal costs!

  ➠ Requires a novel adaptive two-phase protocol!

Thank you for your attention!

References I

R. Ahlswede and I. Csiszár, ‘‘Common Randomness in Information Theory and Cryptography-Part I: Secret Sharing,’’ *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

I. Bjelaković, H. Boche, and J. Sommerfeld, ‘‘Secrecy Results for Compound Wiretap Channels,’’ *Probl. Inf. Transmission*, 2012, accepted, available at http://arxiv.org/abs/1106.2013.