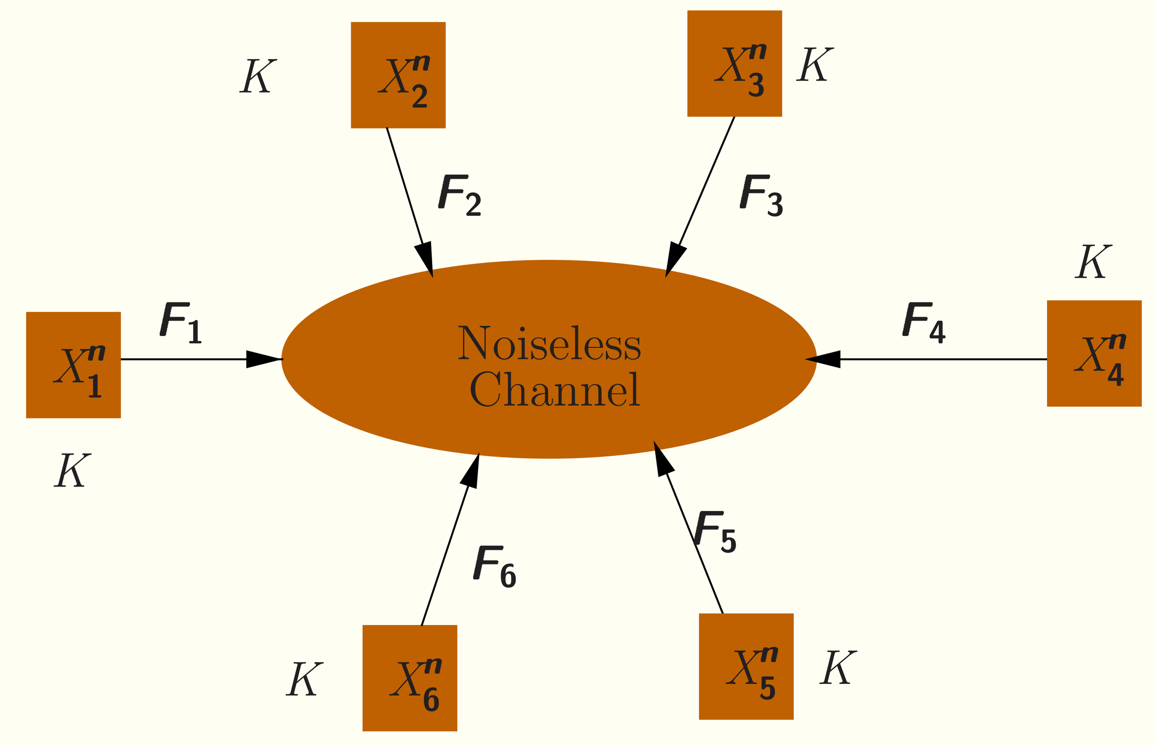
On the Communication Complexity for SK Generation in the Multiterminal Source Model

Manuj Mukherjee, Navin Kashyap
Indian Institute of Science, Bangalore, India

The Multiterminal Source Model



- A set of terminals $\mathcal{M} = \{1, 2, \dots, m\}$, with each terminal possessing a component of a Discrete Memoryless Multiple Source, X_i^n, $\forall 1 \le i \le m$.
- The terminals are allowed to communicate 'interactively'.
- $\mathbf{F} = \{F_1, F_2, \cdots, F_r\}$ is the interactive communication taking values in $\mathcal{F}$. Here F_j sent by some terminal i is a function of X_i^n and all the previous communication.
- *Rate* of the interactive communication is $\frac{1}{n}\log|\mathcal{F}|$.
- The terminals compute a secret key (SK) $\mathbf{K} = \mathbf{K}(X_{\mathcal{M}}^n)$ with the aid of $\mathbf{F}$.
- The secret key $\mathbf{K}$ satisfies the following property: for any $\epsilon > 0$ and for all sufficiently large n,
  - $\exists$ some function $g_i^{(n)}(X_i^n, \mathbf{F})$ such that $\mathcal{P}(\mathbf{K} \neq g_i^{(n)}(X_i^n, \mathbf{F})) \le \epsilon, \forall 1 \le i \le m$. (*Recoverability*)
  - $I(\mathbf{K}; \mathbf{F}) \le \epsilon$. (*Strong secrecy*)
  - $\log|\mathcal{K}| - H(\mathbf{K}) \le \epsilon$, where $\mathcal{K}$ is the range of $\mathbf{K}$. (*Uniformity*)
- If $\frac{1}{n}H(\mathbf{K}) \to \mathbf{R}$ as $n \to \infty$, then $\mathbf{R}$ is called an achievable secret key rate.
- SK capacity $\mathbf{I}(X_{\mathcal{M}}) = \sup \mathbf{R}$.

Achieving SK Capacity

- Use a Slepian-Wolf code to recover $X_{\mathcal{M}}^n$ at all terminals.
- Such a code is called a communication for omniscience.
- The *achievable rate region*:

$$\mathcal{R}_{\text{CO}} = \{(R_1, R_2, ..., R_m) : R_i \ge 0, \forall 1 \le i \le m, \sum_{j \in B} R_j \ge H(X_B|X_{B^c}), \forall B \subset \mathcal{M}, B \neq \phi\}$$

- Use a balanced coloring function on $X_{\mathcal{M}}^n$ to get $\mathbf{K}$.

Evaluating SK Capacity

- $\mathbf{I}(X_{\mathcal{M}}) = H(X_{\mathcal{M}}) - R_{\text{CO}}$, where $R_{\text{CO}} = \min_{(R_1, R_2, ..., R_m) \in \mathcal{R}_{\text{CO}}} \sum_{i=1}^m R_i$ is the minimum rate of communication for omniscience. [Csiszár & Narayan, '04]
- $\mathbf{I}(X_{\mathcal{M}}) = \min_{\mathcal{P}} \boldsymbol{\Delta}(\mathcal{P})$, where $\boldsymbol{\Delta}(\mathcal{P}) = \frac{1}{\ell - 1}[H(X_{A_1}) + H(X_{A_2}) + \cdots + H(X_{A_\ell}) - H(X_{\mathcal{M}})]$ for any partition $\mathcal{P} = \{A_1, A_2, \dots, A_\ell\}$ of $\mathcal{M}$ with $\ell \ge 2$. We denote by $\mathcal{P}^*$ the finest optimal partition and call it the fundamental partition. [Chan & Zheng, '10]

Communication Complexity

- R_{SK} = Communication complexity, is the minimum rate of communication required to achieve SK capacity.
- $R_{\text{SK}} \le R_{\text{CO}}$. [Csiszár & Narayan, 2004]
- If $R_{\text{SK}} = R_{\text{CO}}$, we call the source R_{SK}-maximal. These are thus the worst-case sources in terms of communication rates.

Lower Bound on Communication Complexity

- **Result**: $R_{\text{SK}} \ge \text{CI}(X_{\mathcal{M}}) - \mathbf{I}(X_{\mathcal{M}})$. [Mukherjee & Kashyap, '16]
  - $\text{CI}(X_{\mathcal{M}})$ is the minimum rate of interactive common information.
  - Fact: $H(X_{\mathcal{M}}) \ge \text{CI}(X_{\mathcal{M}}) \ge \mathbf{I}(X_{\mathcal{M}})$ and hence the lower bound is non-negative.

What is Interactive Common Information?

- $\mathbf{J} = \mathbf{J}(X_{\mathcal{M}}^n)$ is a common randomness if $\mathbf{J}$ is recoverable at all terminals using some interactive communication $\mathbf{F}$.
- $(\mathbf{J}, \mathbf{F})$ is an interactive common information (CI) if $(\mathbf{J}, \mathbf{F})$ is a Wyner common information for $X_{\mathcal{M}}^n$.
- $\text{CI}(X_{\mathcal{M}}) = \min_{(\mathbf{J},\mathbf{F}) \text{ is CI}} \lim_{n \to \infty} \frac{1}{n} H(\mathbf{J}, \mathbf{F})$.

What is Wyner Common Information?

- $\mathbf{L} = \mathbf{L}(X_{\mathcal{M}}^n)$ is a Wyner common information for $X_{\mathcal{M}}^n$ if $\lim_{n \to \infty} \frac{1}{n} \mathbf{I}(X_{\mathcal{M}}^n|\mathbf{L}) = 0$ where

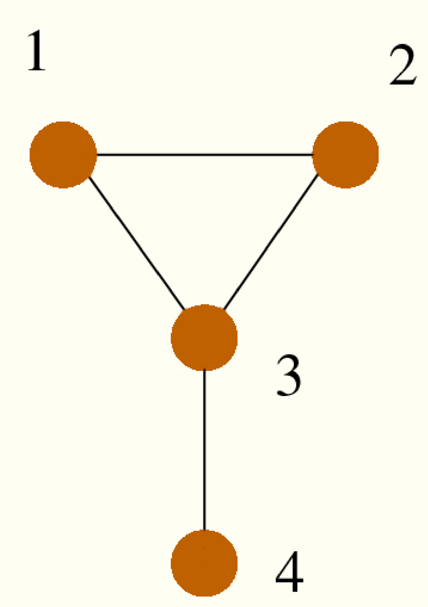
$$\mathbf{I}(X_{\mathcal{M}}^n|\mathbf{L}) \triangleq \frac{1}{|\mathcal{P}^*| - 1}\left[\sum_{A \in \mathcal{P}^*} H(X_A^n|\mathbf{L}) - H(X_{\mathcal{M}}^n|\mathbf{L})\right].$$

- Remark: $\mathbf{I}(X_{\mathcal{M}}^n|\mathbf{L}) = 0$ implies conditional independence of $(X_A^n)_{A \in \mathcal{P}^*}$ given $\mathbf{L}$.

Evaluating $\text{CI}(X_{\mathcal{M}})$: The Hypergraphical Source

- Consider a hypergraph $\mathcal{H} = (\mathcal{V}, \mathcal{E})$.
- $\mathcal{V} = \mathcal{M}$.
- Associate with each hyperedge $e \in \mathcal{E}$ an i.i.d. sequence of n Bernoulli $(1/2)$ random variables ξ_e^n.
- Random variables associated with distinct hyperedges in $\mathcal{E}$ are independent.
- Define a multiterminal source as follows: $X_i^n = (\xi_e^n : e \in \mathcal{E}$ such that $i \in e)$.
- The multiterminal source $X_{\mathcal{M}}^n$ is known as the hypergraphical source.
- **Result**: For a hypergraphical source $\text{CI}(X_{\mathcal{M}}) = |\mathcal{E}_{\mathcal{P}^*}|$, where $\mathcal{E}_{\mathcal{P}^*}$ is the set of hyperedges intersecting with at least two parts of $\mathcal{P}^*$.

The Lower Bound is Loose



- Consider the following binary hypergraphical model.
  - $m = 4$ and $\mathcal{E} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{3, 4\}\}$.
  - $\mathcal{P}^* = \{\{1, 2, 3\}, \{4\}\}$ and $\mathbf{I}(X_{\mathcal{M}}) = 1$.
- Therefore, $\text{CI}(X_{\mathcal{M}}) = 1$ and hence, $\text{CI}(X_{\mathcal{M}}) - \mathbf{I}(X_{\mathcal{M}}) = 0$.
- However, $R_{\text{SK}} > 0$ as (X_1, X_2) is independent of X_4.

Results on R_{SK}-maximality

- **Result**: A multiterminal source $X_{\mathcal{M}}$ with fundamental partition $\mathcal{P}^*$ is R_{SK}-maximal if for all $A \in \mathcal{P}^*$ we have $H(X_A|X_{A^c}) = 0$.
- **Result**: A hypergraphical source $\mathcal{H} = (\mathcal{M}, \mathcal{E})$ is R_{SK}-maximal iff $\mathcal{E} = \mathcal{E}_{\mathcal{P}^*}$.

Examples of R_{SK}-maximal Sources

- Hypergraphical source defined on the complete t-uniform hypergraph $K_{m,t}$: $\mathcal{V} = \mathcal{M}$. $\mathcal{E}$ is the set of all t-subsets of $\mathcal{M}$.
- Hypergraphical source defined on Harary graphs: These are k-*regular*, k-*edge-connected* graphs (i.e., all hyperedges are of size 2).
- Hypergraphical source defined on Steiner Triple Systems: $\mathcal{V} = \mathcal{M}$. $\mathcal{E}$ consists of 3-subsets of $\mathcal{M}$ such that every $\{i, j\}$, $i, j \in \mathcal{M}, i \neq j$, is a subset of exactly one $e \in \mathcal{E}$.