# Common Randomness and Secret Key Capacities

Imre Csiszár    Prakash Narayan

## Common Randomness and Secret Key

**Common Randomness (CR):** Random variables (rvs) generated by different terminals, based on

- local measurements or observations
- transmissions or exchanges of information

such that

the rvs agree with probability $\cong 1$.

**Use:** For instance, in randomized encoding and decoding in certain communication situations.

## Common Randomness and Secret Key

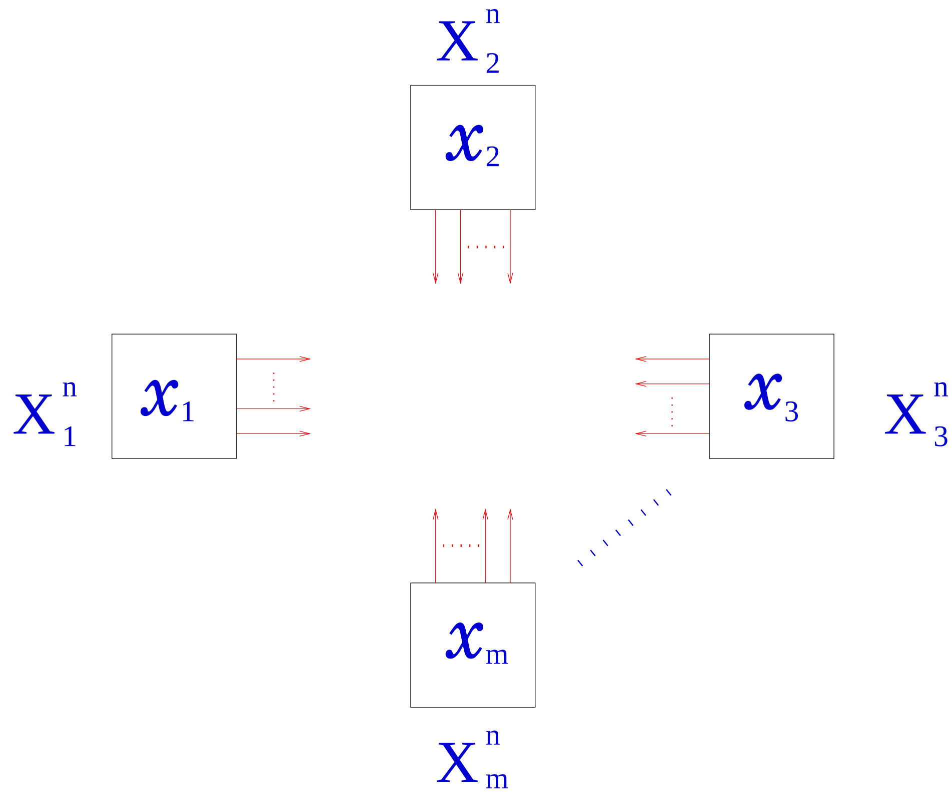
**Secret Key (SK):** The rvs are, in addition, effectively concealed from an eavesdropper with access to the public transmissions or from a wiretapper.

**Use:** For secure encrypted communication.

# An Overview

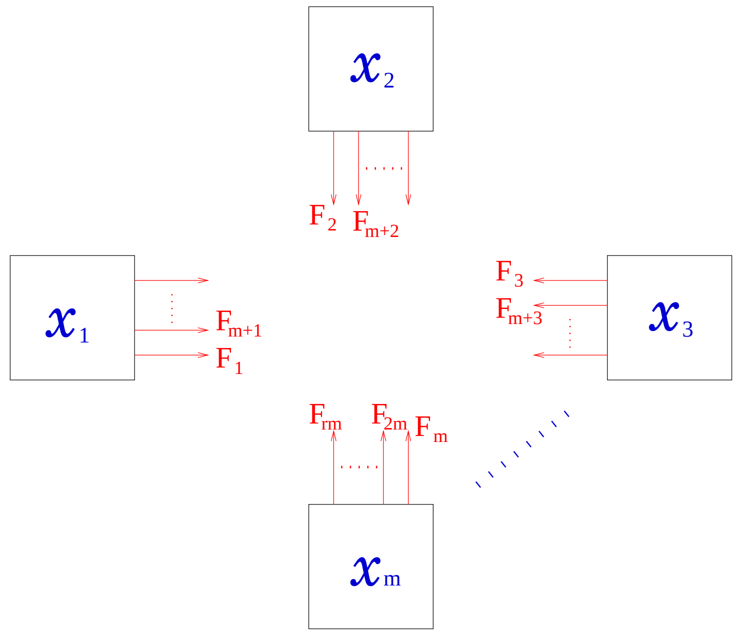
- We consider models with an arbitrary number of terminals.
- Each terminal observes a distinct component of a discrete memoryless multiple source.
- Unconstrained public communication (broadcast) is allowed between these terminals.
- An eavesdropper observes the communication between the terminals, but does not have access to any other information.
- Main contribution: Determination of $SK$-capacity (namely the largest achievable $SK$-rate).

# The Model



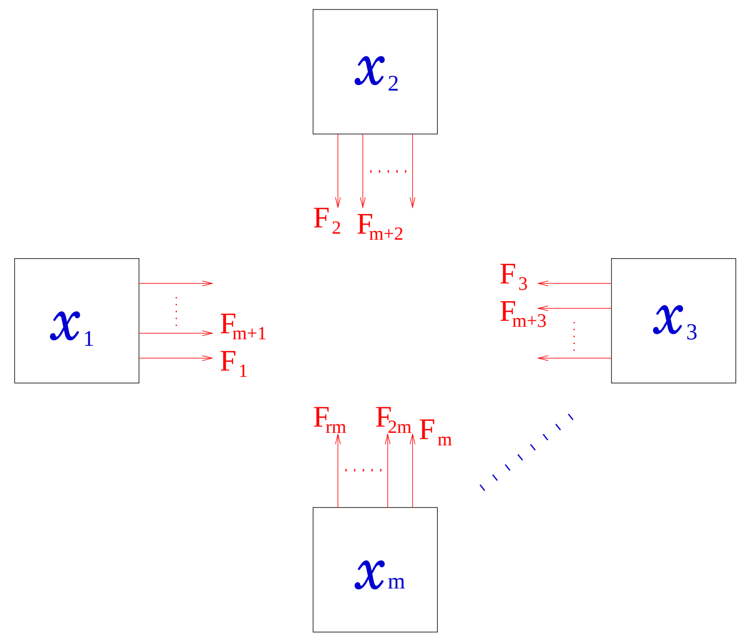

- $m \geq 2$ terminals.
- $X_1, \ldots, X_m$, $m \geq 2$, are rvs with finite alphabets $\mathcal{X}_1, \ldots, \mathcal{X}_m$.
- Consider a discrete memoryless multiple source with components $X_1^n = (X_{11}, \ldots, X_{1n}), \ldots, X_m^n = (X_{m1}, \ldots, X_{mn})$.
- Terminal $\mathcal{X}_i$ observes the component $X_i^n = (X_{i1}, \ldots, X_{in})$.

# The Model




- The terminals are allowed to communicate over a *noiseless public* channel, possibly interactively in several rounds.
- All transmissions are observed by all the terminals.
- No rate constraints on communication.
- Assume w.l.o.g that transmissions occur in consecutive time slots in $r$ rounds.
- Communication depicted by rvs $\mathbf{F} \triangleq F_1, \ldots F_{rm}$, where
  - ∗ $F_\nu$ = transmission in time slot $\nu$ by terminal $i \equiv (\nu - 1) \mod m + 1$.
  - ∗ $F_\nu$ is a function of $X_i^n$ and $(F_1, \ldots, F_{\nu-1})$.

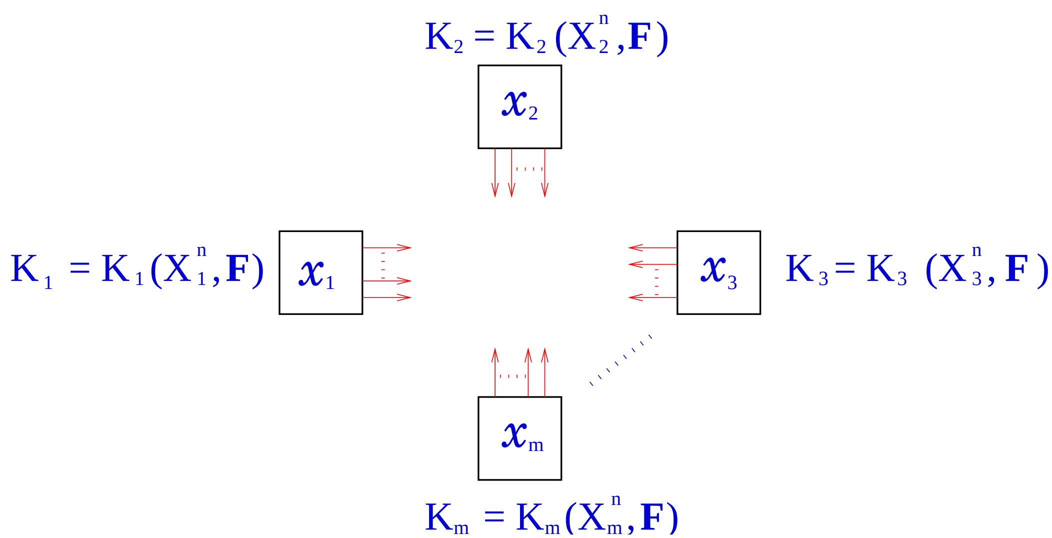
# The Model




- An eavesdropper observes the communication $\mathbf{F} = (F_1, \ldots, F_{rm})$ between the terminals, but does not have access to any other information.

- **Main contribution**: Determination of $SK$-capacity (namely the largest achievable $SK$-rate).

# Secret Key



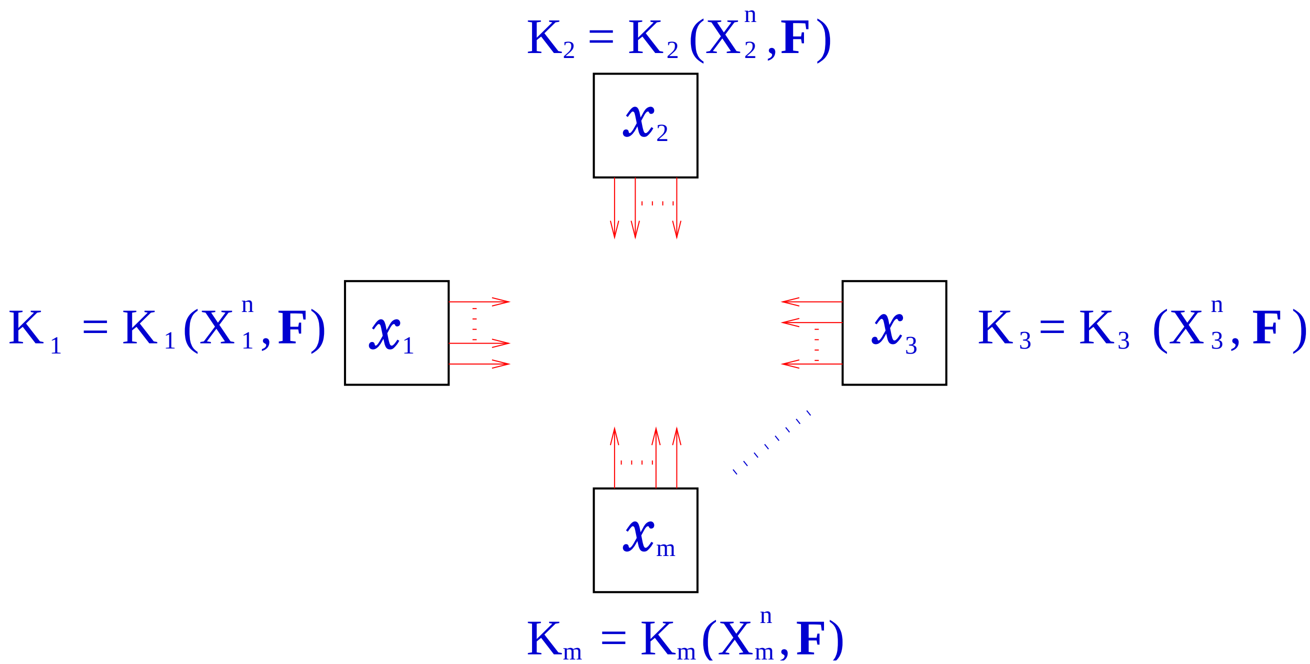

**Secret Key:** A function $K$ of $(X_1^n, \cdots, X_m^n)$ is an $\varepsilon$-$SK$, achievable with communication **F**, if

- $Pr\{K = K_1 = \cdots = K_m\} \geq 1 - \varepsilon$ ("$\varepsilon$-common randomness")
- $\frac{1}{n} I(K \wedge \mathbf{F}) \leq \varepsilon$ ("secrecy")
- $\frac{1}{n} H(K) \geq \frac{1}{n} \log |\mathcal{K}| - \varepsilon$ ("uniformity")

where $\mathcal{K}$ = set of all possible values of $K$.

Thus, a secret key is effectively concealed from an eavesdropper with access to **F**, and is nearly uniformly distributed.

**Secret Key Capacity**




- Achievable SK-rate: The (entropy) rate of such a SK, achievable with suitable communication (with the number of rounds possibly depending on $n$).
- SK-capacity $C_{SK}$ = largest achievable SK-rate.

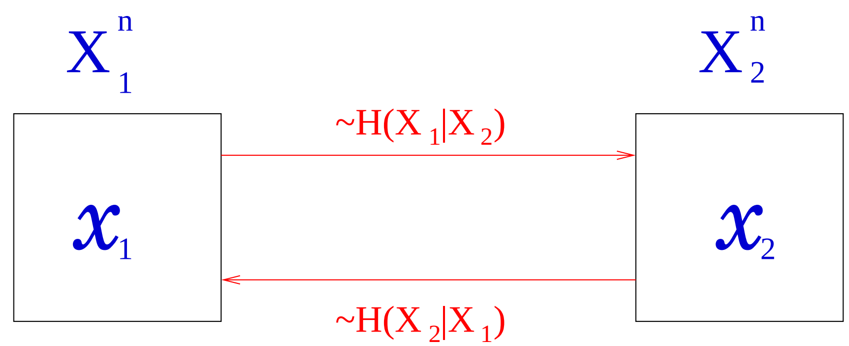
# Some Recent Related Work

- Maurer 1990, 1991, 1993, 1994, $\cdots$
- Ahlswede-Csiszár 1993, 1994, 1998, $\cdots$
- Bennett, Brassard, Crépeau, Maurer 1995.
- Csiszár 1996.
- Maurer - Wolf 1997, $\cdots$
- Venkatesan - Anantharam 1995, 1997, 1998, 2000, $\cdots$
- Csiszár - Narayan 2000.

$\vdots$

$\vdots$

## Special Case: Two Users




### Observation

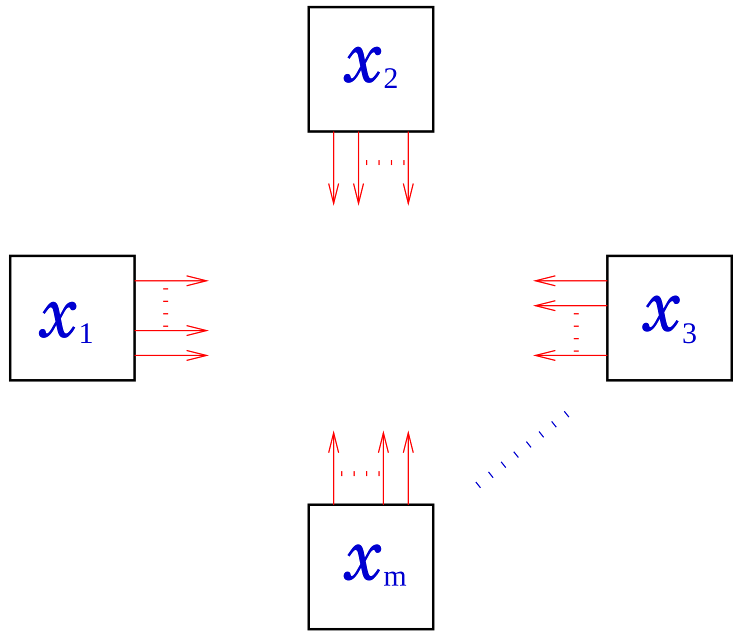
$$C_{SK} = I(X_1 \wedge X_2) \quad \text{[Maurer 1993, Ahlswede - Csiszár 1993]}$$

$$= H(X_1, X_2) - [H(X_1|X_2) + H(X_2|X_1)]$$

$$= \text{Total rate of shared } CR - \text{ Minimum rate}$$

of overall communication for “omniscience.”

**Example**




- $X_1, \cdots, X_{m-1}$ are $\{0,1\}$-valued, mutually independent, $(\frac{1}{2}, \frac{1}{2})$ rvs, and

$$X_{mt} = X_{1t} + \cdots + X_{(m-1)t} \; mod \; 2, \qquad t \geq 1.$$

- **Claim**: 1 bit of perfect $SK$ (i.e., with $\varepsilon = 0$) is achievable with observation length $n = m - 1$.

## Example

- *Scheme with "simple" communication:*

  - Let $n = m - 1$.

  - For $i = 1, \cdots, m-1$, $\mathcal{X}_i$ transmits $F_i = f_i(X_i^n)$ = block $X_i^n$ excluding $X_{ii}$.

  - $\mathcal{X}_m$ transmits $F_m = f_m(X_m^n) = (X_{m1} + X_{m2} \; mod \; 2, \; X_{m1} + X_{m3} \; mod \; 2, \; \cdots, X_{m1} + X_{mn} \; mod \; 2)$.

- $\mathcal{X}_1, \cdots, \mathcal{X}_m$ all recover $(X_1^n, \cdots, X_m^n)$. ("Omniscience")

- In particular, $X_{11}$ is independent of $\mathbf{F} = (F_1, \cdots, F_m)$.

- $X_{11}$ is an achievable perfect $SK$, so $C_{SK} \geq \frac{1}{m-1} H(X_{11}) = \frac{1}{m-1}$ bit.

## Example

### Observations

- Total rate of shared $CR = H(X_1, \cdots, X_m) = H(X_1 \cdots, X_{m-1}) = m - 1$ bits.
- Rate of overall communication which enables omniscience for every terminal $= \frac{1}{m-1} H(F_1, \cdots, F_m) = \frac{1}{m-1}[(m-1)(m-2) + (m-2)] = \frac{m(m-2)}{m-1}$ bits.
- Thus, $C_{SK} \geq$ Total rate of shared CR $-$ Rate of overall *communication for omniscience.*
- In fact, equality holds above for the **minimum** rate of overall *communication for omniscience.*

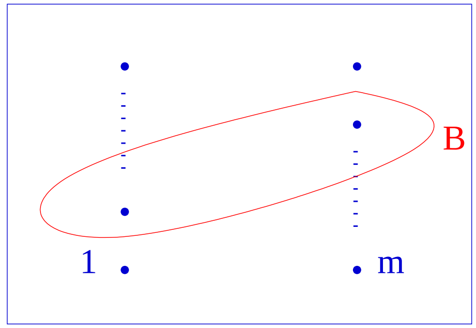
## An Overview of the Main Result

- SK-capacity:

$$C_{SK} \quad = \quad H(X_1, \ldots, X_m) - \text{ Smallest entropy rate of communication which enables omniscience for every terminal.}$$

- A single-letter characterization of this smallest entropy rate of communication for omniscience (CO-rate) and, hence, of $C_{SK}$.

## Main Lemma




If $K$ is $\varepsilon$-CR for the terminals $\mathcal{X}_1, \cdots, \mathcal{X}_m$, achievable with communication $\mathbf{F} = (F_1, \cdots, F_{rm})$, then

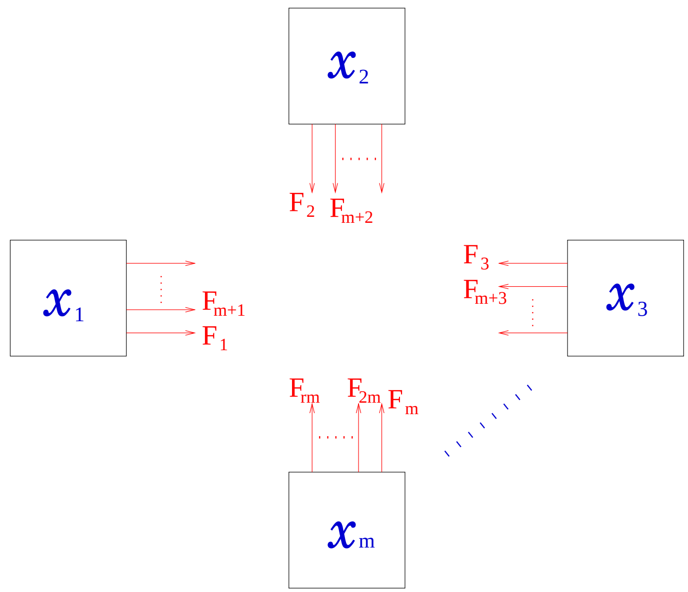
$$\frac{1}{n} H(K|\mathbf{F}) = H(X_1, \cdots, X_m) - \sum_{i=1}^{m} R_i + \frac{m(\varepsilon \log |\mathcal{K}| + 1)}{n}$$

for some numbers $(R_1, \cdots, R_m) \in \mathcal{R}_{SW}$ where

$$\mathcal{R}_{SW} = \left\{ (R_1', \cdots, R_m') : \sum_{i \in B} R_i' \geq H(X_B | X_{B^c}), \;\; B \subset \{1, \ldots, m\} \right\}.$$

*Remark*: The region $\mathcal{R}_{SW}$, if stated for *all* $B \subseteq \{1, \ldots, m\}$, gives the achievable rate region for the multiterminal version of the Slepian-Wolf source coding theorem.

**Theorem 1: Communication for Omniscience**




The smallest achievable CO-rate, $\lim_n \frac{1}{n} H(F_1^{(n)}, \ldots, F_{rm}^{(n)})$, which enables $(X_1^n, \ldots, X_m^n)$ to be $\varepsilon_n$-CR for all the terminals with communication $(F_1^{(n)}, \ldots, F_{rm}^{(n)})$ (with the number of rounds possibly depending on $n$), with $\varepsilon_n \longrightarrow 0$, is

$$H_{min} = \min_{(R_1, \ldots, R_m) \in \mathcal{R}_{SW}} \sum_{i=1}^{m} R_i.$$

**Proof**: Converse: *From Main Lemma.*

Achievability: *Straightforward extension of the multiterminal Slepian-Wolf source coding theorem.*

## Theorem 2: SK-Capacity $C_{SK}$

The SK-capacity $C_{SK}$ for a set of terminals $\{1, \ldots, m\}$ equals

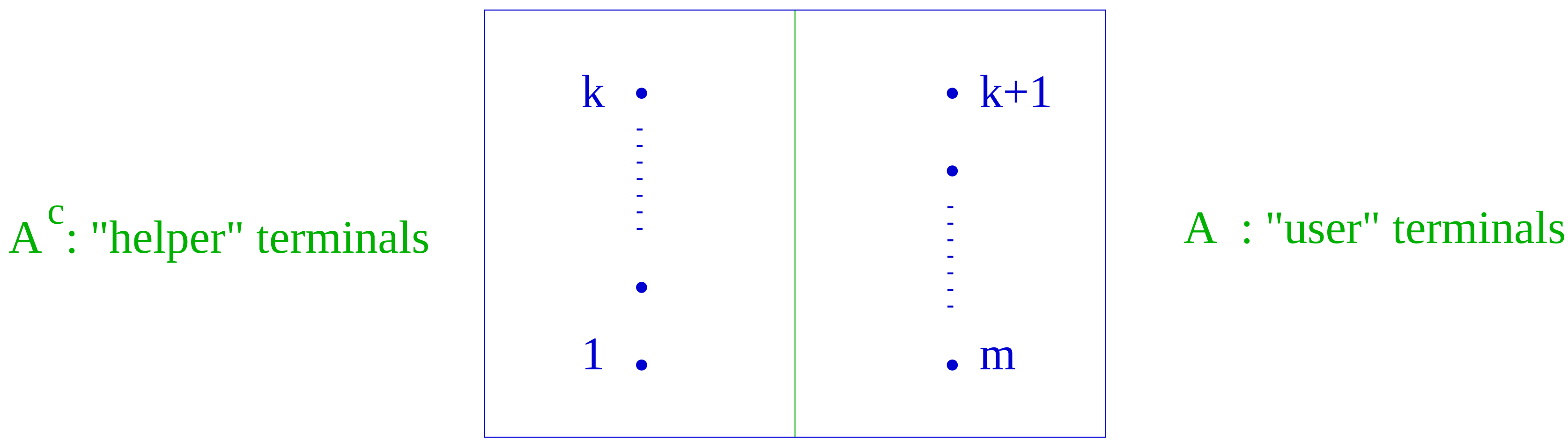
$$C_{SK} = H(X_1, \ldots, X_m) - H_{min}.$$

**Proof**: Converse: *From Main Lemma.*

Idea of achievability proof: *If $L$ represents $\varepsilon$-CR for the set of terminals, achievable with communication $\mathbf{F}$ for some block length $n$, then $\frac{1}{n}H(L|\mathbf{F})$ is an achievable SK-rate if $\varepsilon$ is small. With $L \cong (X_1^n, \ldots, X_m^n)$, we have*

$$\frac{1}{n}H(L|\mathbf{F}) \cong H(X_1, \ldots, X_m) - \frac{1}{n}H(\mathbf{F}).$$

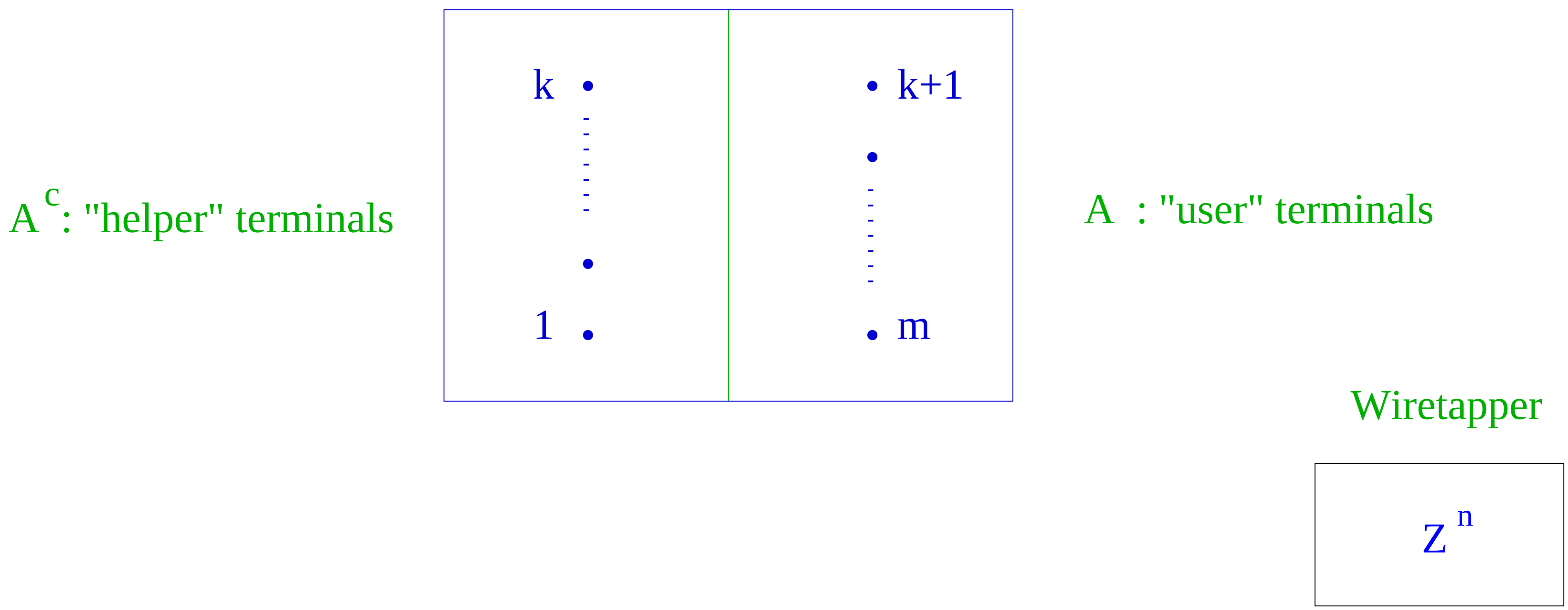
**Theorem 2a: SK-Capacity with Helpers**




The SK-capacity for the terminals in $A$, with the terminals in $A^c$ as helpers, is

$$C_{SK}(A) = H(X_1, \ldots X_m) - \text{Smallest CO-rate for user terminals in } A$$
$$= H(X_1, \ldots X_m) - H_{min}(A).$$

# Eavesdropper with Wiretapped Side Information



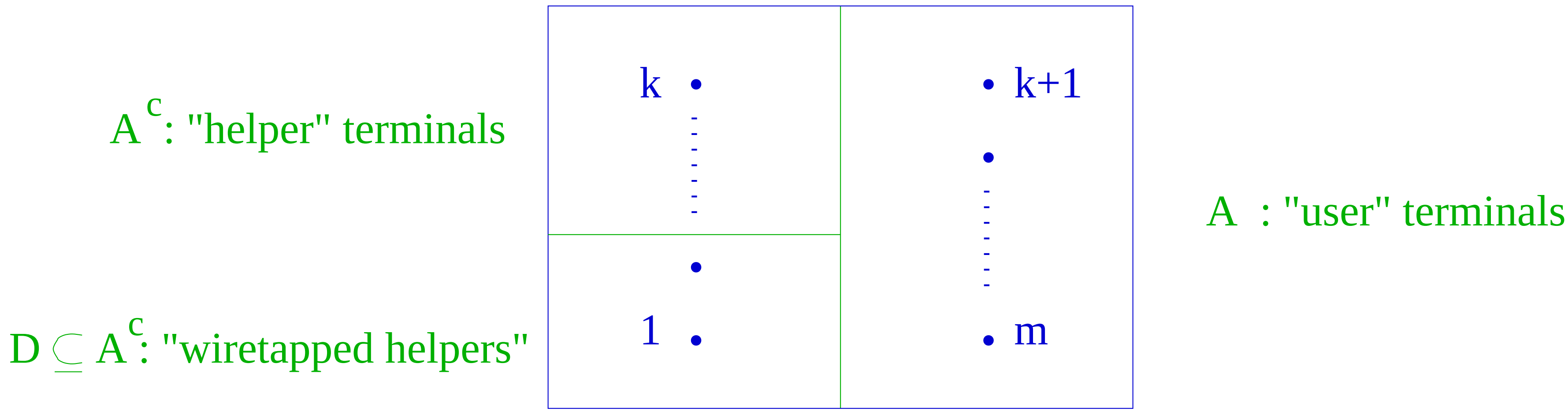

- The secrecy requirement now becomes

$$\frac{1}{n} I(K \wedge \mathbf{F}, Z^n) \leq \varepsilon.$$

- General problem remains unsolved.

- Special case solved: Eavesdropper wiretaps a subset of the “helper” terminals, i.e., $Z^n = \{X_i, i \in D\}$, $D \subseteq A^c$, which gives rise to the notion of $\cdots\cdots$

## Theorem 3: Private Key Capacity




The PK-capacity for the terminals in $A$, with privacy from the set of wiretapped helper terminals $D \subseteq A^c$, is

$$C_{PK}(A|D) = H(X_1, \ldots, X_m) - \text{“Revealed” entropy } H(\{X_i,\ i \in D\})$$

$$- \text{ Smallest CO-rate for user terminals in } A \text{ when they additionally know } \{X_i,\ i \in D\}$$

$$= H(X_1, \ldots, X_m) - H(X_D) - H_{min}(A|D).$$

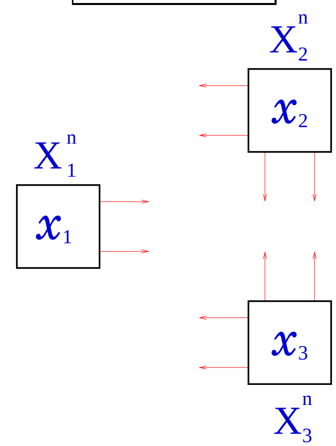
## Comments

- The proofs show that the $SK$- and $PK$-capacities are achievable with *simple* communication, i.e., a *single autonomous transmission* from each terminal is adequate:

$$\mathbf{F} = (F_1, \ldots, F_m) \text{ and } F_i = f_i(X_i^n), \quad i = 1, \ldots, m.$$

- Additional randomization at the terminals does not serve to enhance $SK$- or $PK$-capacities.

## Example




- $X_2^n, X_3^n$ are $\{0,1\}$-valued, *i.i.d.* $(\frac{1}{2}, \frac{1}{2})$ sequences, and $X_2^n$ is independent of $X_3^n$.

- $X_{1i} = X_{2i} + X_{3i} + N_i \mod 2$, $i = 1, \ldots, n$, with $N^n$ being a $\{0,1\}$-valued, *i.i.d.* $(1-p, p)$ sequence, and independent of $X_2^n, X_3^n$.

- All user terminals, no helper.

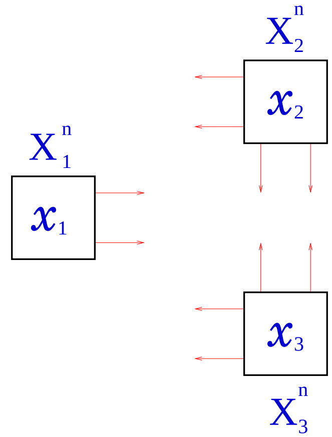
$$H(X_1, X_2, X_3) = 2 + h_b(p) \text{ bits.}$$

$$\mathcal{R}_{SW} = \{(R_1, R_2, R_3) : R_i \geq h_b(p), R_i + R_j \geq 1 + h_b(p), 1 \leq i \neq j \leq 3\}.$$

$$H_{min} = \min_{(R_1,R_2,R_3)\in\mathcal{R}_{SW}} \sum_{i=1}^{3} R_i = \cdots = \frac{3}{2}(1 + h_b(p)) \text{ bits.}$$

$$C_{SK} = H(X_1, X_2, X_3) - H_{min} = \frac{1}{2}(1 - h_b(p)) \text{ bit.}$$

**Example**




- $A = \{2,3\}$, $A^C = \{1\} =$ helper.

$$\mathcal{R}_{SW}(A) = \{(R_1, R_2, R_3) : R_i \geq h_b(p), R_1 + R_j \geq 1 + h_b(p), i = 1,2,3;\ j = 2,3\}.$$

$$H_{min}(A) = \min_{(R_1,R_2,R_3)\in\mathcal{R}_{SW}(A)} \sum_{i=1}^{3} R_i = 1 + 2h_b(p) \text{ bits.}$$

$$C_{SK}(A) = H(X_1, X_2, X_3) - H_{min}(A) = (1 - h_b(p)) \text{ bit.}$$

- $A = \{2,3\}$, $A^C =$ helper $= \{1\} =$ wiretapper $= D$.

$$\mathcal{R}_{SW}(A|D) = \{(R_1, R_2, R_3) : R_2 \geq h_b(p), R_3 \geq h_b(p)\}.$$

$$H_{min}(A|D) = \min_{(R_1,R_2,R_3)\in\mathcal{R}_{SW}(A|D)} \sum_{i=1}^{3} R_i = 2h_b(p) \text{ bits.}$$

$$C_{PK}(A|D) = H(X_1, X_2, X_3) - H(X_1) - H_{min}(A|D) = (1 - h_b(p)) \text{ bit.}$$

## Open Problems and Work in Progress

- Models with bona £de wiretappers who are not also helpers.
- Models with rate constraints imposed on the public communication.
- Computation of $SK$-capacity for large $m$.