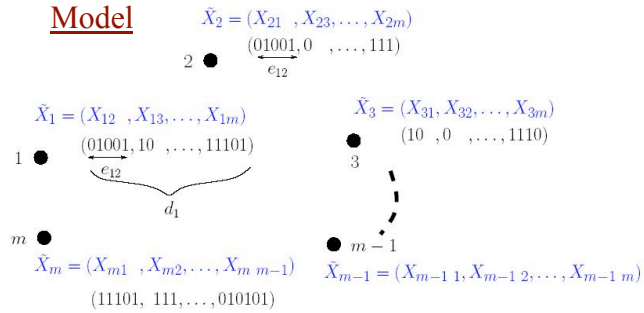


# Perfect Secrecy and Steiner Tree Packing

Sirin Nitinawarat, (Prakash Narayan and Alexander Barg, University of Maryland and ISR)

## Pairwise Independent Network (PIN)

### Model



- Let  $\mathcal{M} = \{1, \dots, m\}$ .
- $X_{ij} = X_{ji}$ ,  $1 \leq i < j \leq m$ , and  $X_{ij} \sim \text{unif.}\{0, 1\}^{\epsilon_{ij}}$ .
- $X_{ij}$ ,  $1 \leq i < j \leq m$  are mutually independent.
- $\tilde{X}_i = \{X_{ij}, j \in \mathcal{M} \setminus \{i\}\}$  with  $d_i = \sum_{j \neq i} \epsilon_{ij}$  bits.

## Perfect Secret Key Generation for a PIN Model

**Theorem 1:** The perfect SK capacity for a set of terminals  $A \subseteq \mathcal{M}$  is

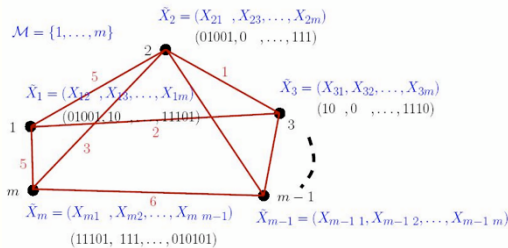
$$C(A) = \sum_{i,j} \epsilon_{ij} - OMN(A)$$

$$\text{where } OMN(A) = \min_{(R_1, \dots, R_m) \in \mathcal{R}(A)} \sum_{i=1}^m R_i,$$

$$\text{with } \mathcal{R}(A) = \left\{ (R_1, \dots, R_m) \in \mathbb{R}^m : R_i \geq 0, i = 1, \dots, m, \right. \\ \left. \text{for each } B \subset \mathcal{M}, B \not\supseteq A, \sum_{i \in B} R_i \geq (\sum_{i,j \in B} \epsilon_{ij}) \right\}.$$

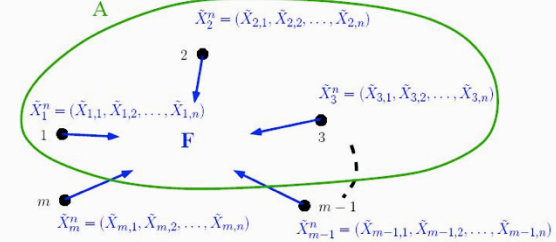
Furthermore, this perfect SK capacity can be achieved with linear noninteractive communication.

## PIN Model and Multigraph



There exists a one-to-one correspondence between a PIN model and a multigraph (undirected graph with no selfloop but with possibly multiple edges between any vertex pair). Specifically, a PIN model is equivalent to a multigraph with vertex set being  $\mathcal{M}$  and with  $e_{ij}$  edges connecting terminals  $i$  and  $j$ .

## Perfect Secret Key Generation for the PIN Model



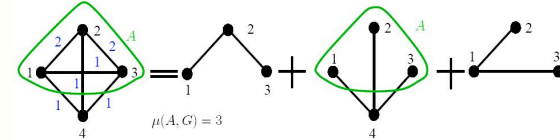
**Objective:** The terminals in a given  $A \subseteq \mathcal{M}$  wish to generate a *perfect secret key* with the cooperation of the remaining terminals.

**Perfect Secret Key (SK):** A random variable  $K^{(n)}$  with values in  $\mathcal{K}^{(n)}$  is a perfect SK for a set of terminals  $A$ , achievable with communication  $\mathbf{F}$  if

- $\Pr\{K^{(n)} = K_i, i \in A\} = 1$  ("common randomness")
- $I(K^{(n)} \wedge \mathbf{F}) = 0$  ("secrecy")
- $H(K^{(n)}) = \log |\mathcal{K}^{(n)}|$ , ("uniformity").

The *largest rate* of such a perfect SK for  $A$ , achievable with suitable communication, is the perfect SK capacity  $C(A) \triangleq \liminf_n \frac{1}{n} \log |\mathcal{K}^{(n)}|$ .

## Maximal Steiner Tree Packing and Perfect SK Generation



- For  $A \subseteq \mathcal{M}$ , a *Steiner tree* of  $G$  is a subgraph of  $G$  which is a tree whose vertex set contains  $A$ . For the special case of  $A = \mathcal{M}$ , a Steiner tree of  $G$  is also a spanning tree of  $G$ .
- A *Steiner tree packing* of  $G$  is any collection of edge-disjoint Steiner trees of  $G$ . Let  $\mu(A, G)$  denote the maximum size of such a packing.

**Proposition 2:** For every  $A \subseteq \mathcal{M} = \{1, \dots, m\}$ , it holds that

$$\sup_n \frac{1}{n} \mu(A, G^{(n)}) \leq C(A),$$

where  $C(A)$  is the perfect SK capacity of the PIN model associated with the multigraph  $G$ . Equality holds for the special case of  $A = \mathcal{M}$

Maximal Steiner Tree Packing of the multigraph associated with a PIN model leads to an efficient scheme for perfect SK generation using LDPC codes for the communication.

The scheme is achieving the perfect SK capacity when all the terminals seek the perfect SK !