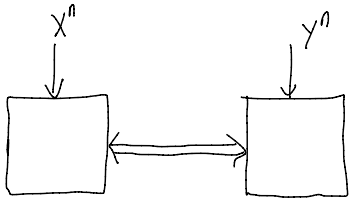
11/29/2016
Tuesday

Secret Key Agreement

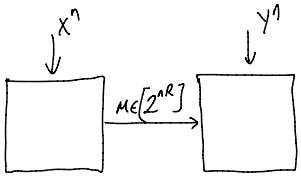


Unlimited Communication: $C_K = I(X;Y)$ ← Random Binning, Slepian-Wolf

Communication rate $H(X|Y)$

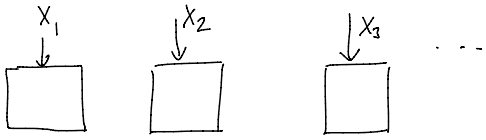
No Communication: $C_K = C_{GK}(X;Y)$
(Gacs-Körner 1975 ?)

Rate limited One-way communication:



We'll discuss today
Solved by
(Csiszar Narayan 2000)

Many Terminals:



All nodes must obtain key.

Unlimited communication: (Csiszar-Narayan, 2004)

$C_K = H(X_1, \dots, X_m) - R_{omni}$

$$R_{omni} = \min \left\{ R : \begin{array}{l} R = \sum_j R_j \\ \forall i \in \{1, \dots, m\} \text{ and } S \subseteq [m], \ \sum_{j \in S} R_j \geq H(X_S | X_i) \end{array} \right.$$

Equivalently, $C_K = \min_{\text{partitions } \pi} \frac{1}{|\pi| - 1} D(P_{X^m} \| P_{X_{\pi_1}} P_{X_{\pi_2}} \dots)$

Example: $m = 4$
$\pi = \{(X_1), (X_2, X_4), (X_3)\}$

(Equivalently (Chen Zhang 2010, CISS)

$\frac{1}{2} D(P_{X^4} \| P_{X_1} P_{X_2 X_3} P_{X_4}$

$$C_k = \min_{\text{partitions } \pi} \frac{1}{|\pi|-1} D(P_{X^m} \| P_{X_{\pi_1}} P_{X_{\pi_2}} \cdots)$$

$$= \min_{\text{partitions } \pi} \frac{1}{|\pi|-1} \sum_{i=2}^{|\pi|} I(X_{\pi^{i-1}}; X_{\pi_i})$$

means combine partitions up until $i-1$

Recall from Problem Set-1

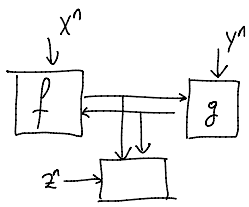
$$D(P_{X^m} \| P_{X_1} \cdots P_{X_m}) = \sum_{i=2}^{m} I(X^{i-1}; X_i)$$

What we don't know:

Rate limited (when we have unlimited rounds)

Recent work with Jingbo: One communication many terminals.

Include Eavesdropper observations



$X, Y, Z \sim P_{XYZ}$

Objective: $(M, Z^n) \perp\!\!\!\perp K$

All messages

Unlimited Communication $C_k = ?$

Upper bound

$C_k \leq I(X;Y|Z)$ → not always achievable

consider $X \perp\!\!\!\perp Y$

$X \sim Ber(1/2)$

$Y \sim Ber(1/2)$

$Z = X \oplus Y$

$I(X;Y|Z) = 1$ bit!

$C_k \leq I(X;Y)$

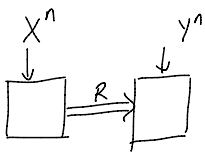
$C_k \leq \min_{(X,Y)-Z-\bar{Z}} I(X;Y|\bar{Z})$

One way communication (Ahlswede–Csiszar 1993)

One way Rate limited Communication (Csiszar–Narayan 2000)

same paper as is rate limited one way without eavesdropper

$Z = \emptyset$:



$$C_k = \max_{P_{U|X}:\ I(U;X) - I(U;Y) \leq R} I(U;Y)$$

$U - X - Y$

Unlimited rate ← slepian-wolf (lossless w/ side information)

limited rate ← Rate distortion w/ side information.

next (it is called Wyner-Ziv problem)