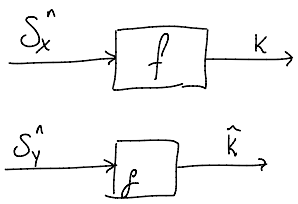
Secret Key Agreement:

11/22/2016
Tuesday



$(S_{X,i}, S_{Y,i}) \sim P_{S_X S_Y}$ (iid multisource)

$\forall \varepsilon > 0$, $\exists$ codebooks s.t.

$P[K \neq \hat{K}] < \varepsilon$

$\| P_K - U \|_{TV} < \varepsilon$

$U \uparrow$ unif $[2^{nR}]$

$R < I(S_X; S_Y)$?

Example: $S_X \sim \text{Bern}(1/2)$

$S_Y \sim \text{Bern}(1/2)$ no rate $R > 0$ is achievable.

$P[S_X = S_Y] = p \neq 0, 1$

Witzenhausen: Can't even agree on one bit.

↳ Rényi Correlation: (aka. Maximal correlation)

$$\rho^*(X,Y) = \max_{U-X-Y-V} \rho(U,V)$$ ← correlation coefficient.

$$= \max_{f,g} \rho(f(X), g(Y))$$

↳ Tensorizes: $\rho^*(P_{XY}^{\otimes n}) = \rho^*(P_{XY})$

$\rho^*(X^n, Y^n) = \rho^*(X,Y)$ (iid)

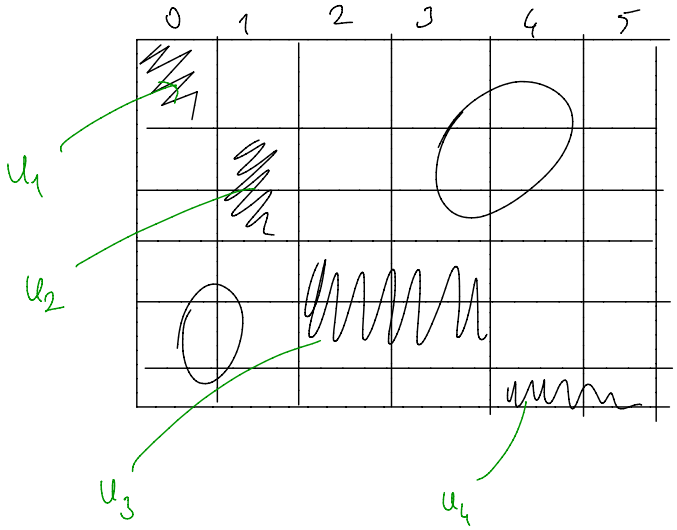
$$C_K = \max_{f,g:\ f(X)=g(Y)\ \text{w.p. } 1} H(f(X)) \triangleq C_{G\text{-}K}(X;Y)$$ ← Common Information, Gacs - Körner

$$= \max_{U-X-Y-U} H(U)$$

(Given X and Y, U must be deterministic: or given X, $U \perp\!\!\!\perp (Y,U)$ so $U=f(X)$; or given Y, $U \perp\!\!\!\perp (X,U)$ so $U=g(Y)$)

$$= \max_{\substack{U-X-Y \\ X-Y-U}} I(XY;U)$$

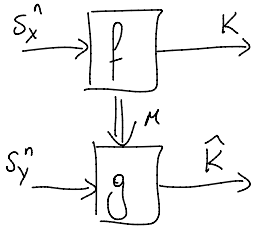
$U-X-Y$ and $X-Y-U$ is not the same as $U-X-Y-U$



← sparsity is required

look at the example in the prev. page, it has no sparsity!

→ We wont prove converse



Objective for key agreement

$M \perp\!\!\!\perp K$

$K = \hat{K}$ $\sim$Unif.

In this setting $C_K = I(X;Y)$ unlimited communication between f and g (so $M \in [\infty]$, rate $=\infty$)

Note: channel that we use to send M is not safe but it is authenticated so we know M comes from our ally but eaves dropper can listen M but $K \perp\!\!\!\perp M$ so our key wont be affected.

Recall Slepian-Wolf encoding; $R = H(X|Y)$ ← random binning

$\left(2^{\uparrow I(X;Y)} \text{ in each bin}\right)$ ← enumerate sequences use number as k

$S_X^n(1)$, $S_X^n(2)$, ... | $S_X^n(0)$, $S_X^n(6)$, ...