Secure Cascade Channel Synthesis

Sanket Satpathy and Paul Cuff
Princeton University

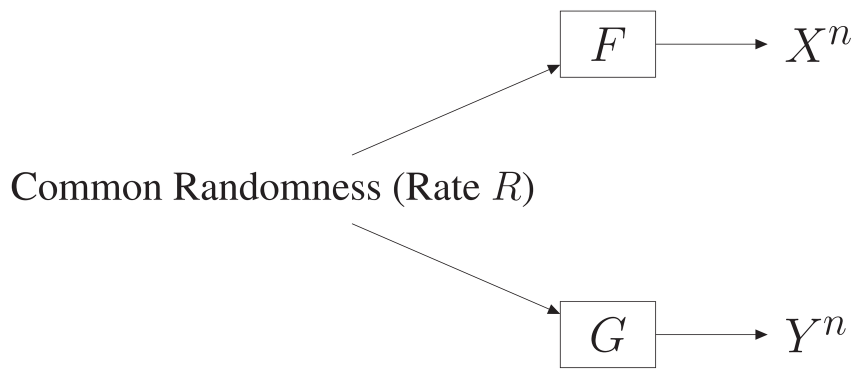
Center for Science of Information
NSF Science and Technology Center

Quantifying Correlation

- Shannon's Mutual Information:

$$I(X;Y) = H(X) - H(X|Y)$$

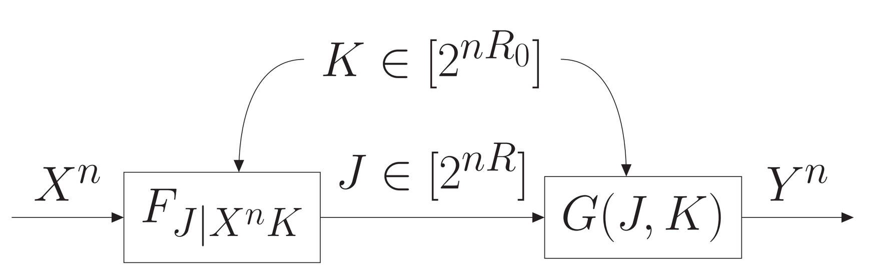
- Wyner's Common Information:
  How much common randomness needed to generate correlated (X^n, Y^n)?



Ans: $R > C(X;Y) = \min_{U: X-U-Y} I(U; X, Y)$

- Reverse Shannon Theorem [Bennett et al 02]:
  How much communication needed to synthesize $Y^n \sim \prod P_{Y|X}$ using a noiseless link and $X^n \sim \prod P_X$?
  Ans: Need communication rate $R > I(X;Y)$
  (Need shared randomness!)

An Operational Viewpoint: Strong Coordination [Cuff 08, Bennett et al. 09]



- Fix P_{XY} and consider $X^n \sim \prod P_X$ given by nature, independent of K
- Want $\lim_{n\to\infty} \left\| Q_{X^n,Y^n} - \prod P_X P_{Y|X} \right\|_1 = 0$
- What are optimal rates of communication and shared randomness?

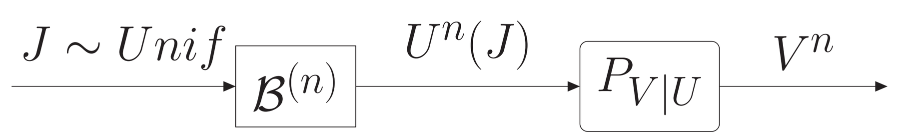
Ans: Need

$$R > I(U;X)$$
$$R + R_0 > I(U;X,Y),$$

with $X - U - Y$.

Cloud-Mixing Lemma 1

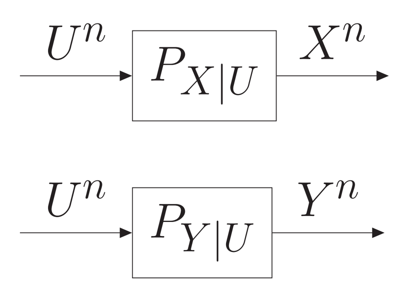
Fix P_{UV}. Want to synthesize $V^n \sim \prod P_V$ given a codebook $\mathcal{B}^{(n)}$ of 2^{nR} U^n sequences. How small can this codebook be?



Ans: $R > I(U;V)$ is sufficient[1].

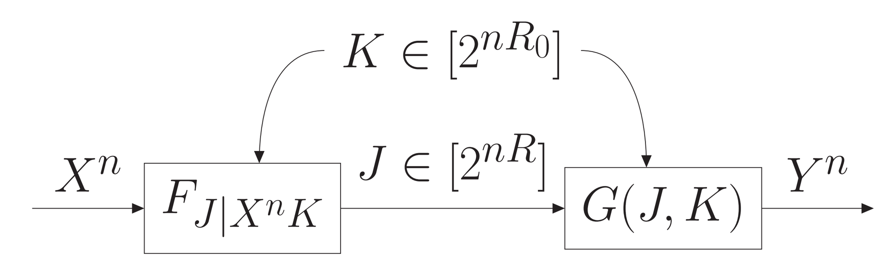
Strong Coordination: Achievability

Pick $U: X - U - Y$ and fold the problem.



- $R + R_0 > I(U;X,Y) \Rightarrow \lim_{n\to\infty} \left\| Q_{X^n,Y^n} - \prod P_X P_{Y|X} \right\|_1 = 0$
- Still need X^n to be i.i.d. and independent of K!
- $R > I(U;X) \Rightarrow \lim_{n\to\infty} \left\| Q_{X^n|K=k} - \prod P_X \right\|_1 = 0$

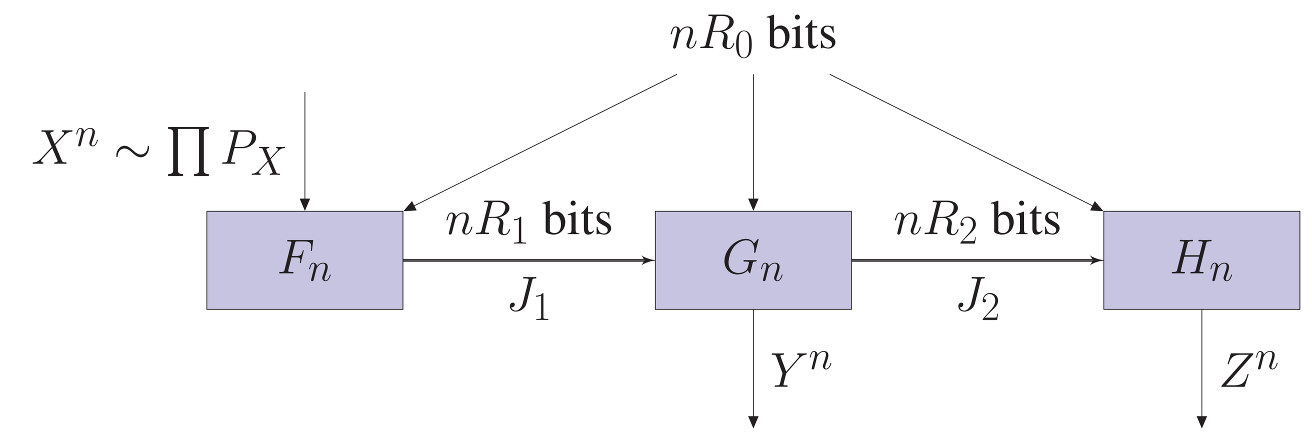
Strong Coordination with Eavesdropper [Cuff 08]



- Same as before, but want $J \perp (X^n, Y^n)$ as well
- Ans: With $X - U - Y$, need

$$R > I(U;X)$$
$$R_0 > I(U;X,Y).$$

Secure Cascade Channel Synthesis



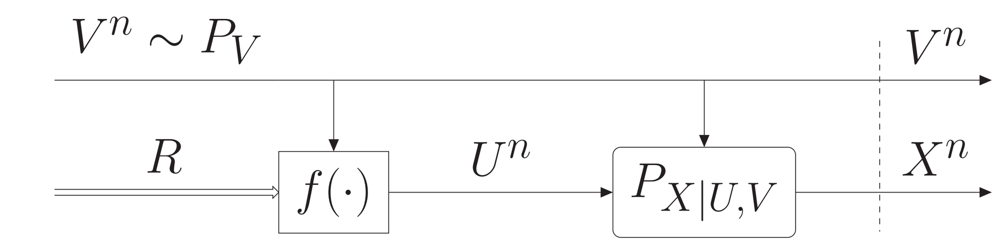
- Want $\lim_{n\to\infty} \left\| Q_{X^n,Y^n,Z^n} - \prod P_X P_{Y,Z|X} \right\|_1 = 0$
- Security constraint: $(J_1, J_2) \perp (X^n, Y^n, Z^n)$
- Ans: Need

$$R_2 > I(V;X)$$
$$R_1 > I(U,V;X)$$
$$R_0 > I(U,V;X,Y,Z),$$

with $X - (U,V) - Y$, $(X,Y,U) - V - Z$ and $H(V|U) = 0$.

Cloud-Mixing Lemma 2

Fix P_{UVX}. Want to synthesize $X^n \sim \prod P_{X|V}$ given $V^n \sim \prod P_V$ and a codebook $\mathcal{B}^{(n)}$ of 2^{nR} U^n sequences. How small can this codebook be?



Ans: $R > I(U;X|V)$ is sufficient[1].

Example: Task Assignment

Let $X \sim$unif$\{[m]\}$ for $m \geq 3$. Consider $P_{YZ|X}$ that produces a pair $Y \neq Z$ uniformly distributed over all distinct pairs in $[m] \setminus \{X\}$. The optimal rate region is

$$\text{ConvexHull}\left\{ \begin{array}{rl} (R_0, R_1, R_2) \in \mathbb{R}^3 & : \exists a \in [m-1] \setminus \{1\}, b \in [a-1] \text{ s.t.} \\ R_2 & \geq \log\left(\frac{m}{a}\right) \\ R_1 & \geq \log\left(\frac{m}{a-b}\right) \\ R_0 & \geq \log\left(\frac{m(m-1)(m-2)}{(a-b)b(m-a)}\right) \end{array} \right\}.$$

Open Problems/Applications

- Cascade Channel Synthesis (without Eavesdropper)[2]
- Strong Coordination with Private Channel [3]
- Strong Coordination through a Noisy Channel[4]
- Strong Coordination with Side Information at Decoder
- Rate-Distortion Theory for Secrecy Systems[5]

Acknowledgement

The authors would like to thank Curt Schieler for helpful discussions. This work is supported by the National Science Foundation (grant CCF-1116013) and the Air Force Office of Scientific Research (grant FA9550-12-1-0196).

References

- P. Cuff, "Distributed Channel Synthesis," *ArXiv e-prints*, Aug. 2012.
- M. R. Bloch and J. Kliewer, "Strong Coordination over a Line Network," *ArXiv e-prints*, May 2013.
- P. Cuff, "State Information in Bayesian Games," *ArXiv e-prints*, Nov. 2009.
- F. Haddadpour, M. H. Yassaee, M. R. Aref, and A. Gohari, "When is it possible to simulate a DMC channel from another?," *ArXiv e-prints*, May 2013.
- C. Schieler and P. Cuff, "Rate-Distortion Theory for Secrecy Systems," *ArXiv e-prints*, May 2013.