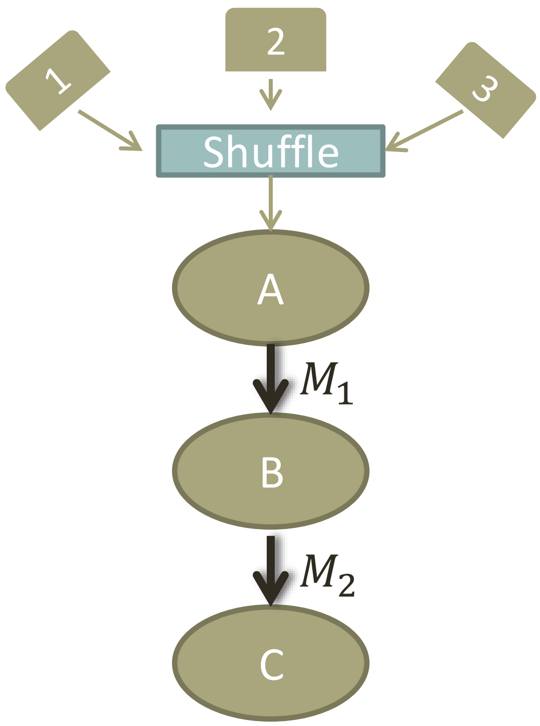
Secrecy in Cascade Networks

Paul Cuff

Three Cards Example

Cascade Network



Objective

- Players B and C produce numbers such that all three differ (literature)
  - $R_1 \geq \log 3$
  - $R_2 \geq \log 3 - 1$ bit
- **Secrecy:** Keep A's card secret from an eavesdropper (this work)
  - Tradeoff between secret key rate and error probability for the eavesdropper

Source Coding

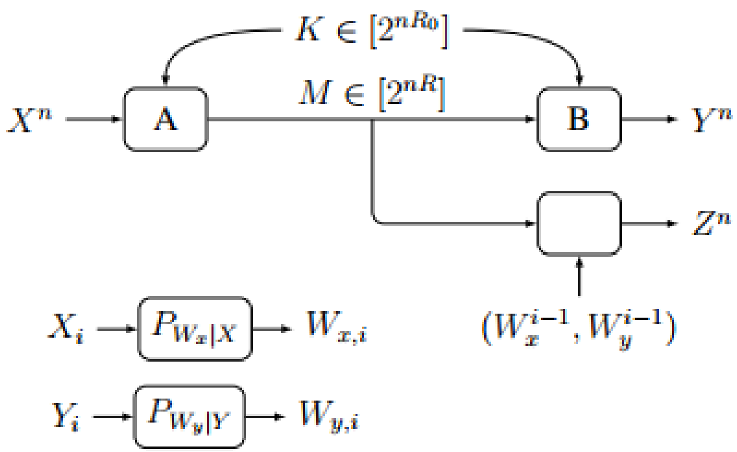
- Not physical layer security
  - Assume secure digital resources are provided

- Problem specifics:
  - Source distribution (memoryless)
  - Encoding rate
  - Secret key rate
  - Distortion metric (time averaged)

Rate-Distortion Theory for Secrecy Systems

- [Schieler, Cuff], under review
- Main features:
  - Asymptotic fundamental limits
  - Performance guarantee (distortion/payoff)
    - Instead of “information leakage rate”
  - Extra side information at the receiver
    - Full causal disclosure yields most robust secrecy

Basic Setting – Previous Work



Performance :

$$\liminf_{n\to\infty} \min_{\{P_{Z_i|M,W^{i-1}}\}_{i=1}^n} \mathbb{E}\, \frac{1}{n} \sum_{i=1}^{n} \pi(X_i, Y_i, Z_i) \geq \Pi.$$

Asymptotic Result:

$$\bigcup_{W_x - X - (U,V) - Y - W_y} \left\{ \begin{array}{rl} (R, R_0, \Pi) : & R \geq I(X; U, V) \\ & R_0 \geq I(W_x W_y; V|U) \\ & \Pi \leq \min_{z(u)} \mathbb{E}\, \pi(X, Y, z(U)) \end{array} \right\},$$

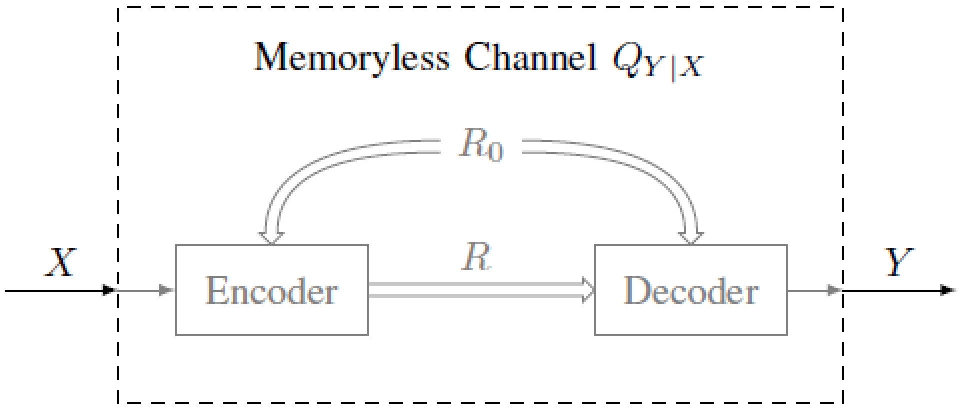
Information Leakage Rate

- Traditional metric for partial secrecy in source coding
  - Information leakage rate: $\frac{1}{n} I(X^n; M)$
  - Vast literature on minimizing information leakage rate
  - Note:
    - Weak perfect secrecy requires this to be negligible.
    - Strong secrecy requires $I(X^n; M)$ to be negligible.

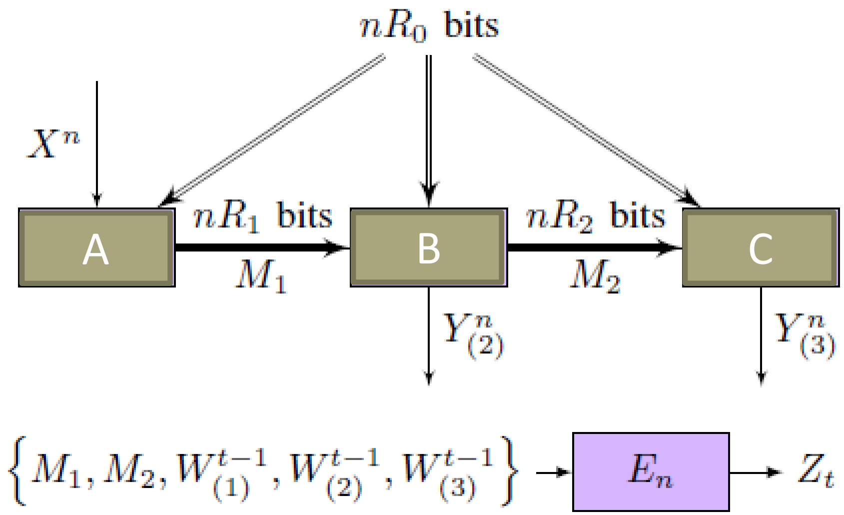
- Information leakage rate is recovered from rate-distortion theory for secrecy systems using log-loss function.

The Role of Channel Synthesis

- Key ingredients for optimal source coding for secrecy.
  - Superposition code
    - First layer dictates information the eavesdropper obtains
    - Second layer used for channel synthesis.



Cascade Network



- Why the cascade network?
  - Source coding without secrecy is tractable.
  - [Satpathy, Cuff 13]: channel synthesis in cascade networks
  - It seems we have all the ingredients.

Results of This Work

- Inner and outer bounds
- Evaluation of bounds for two examples where bounds are tight

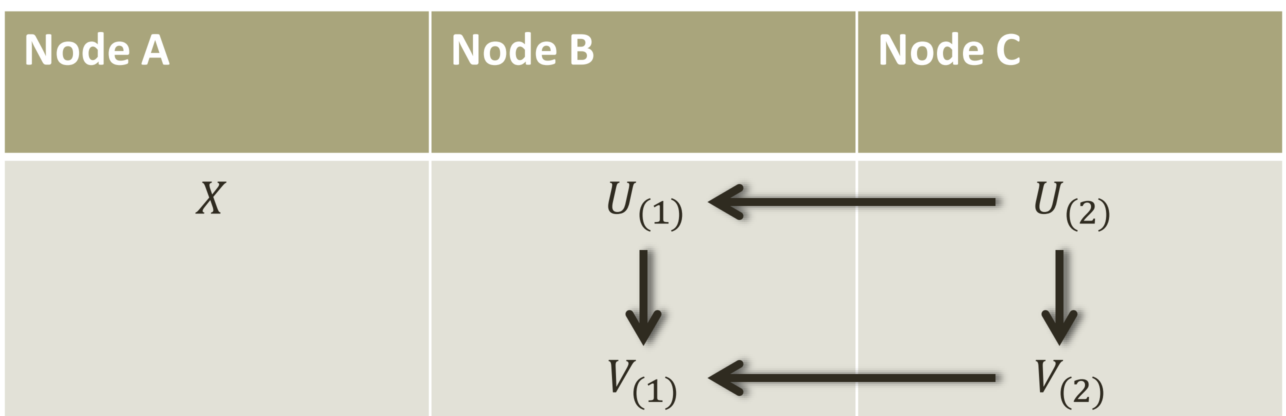
What are the complications (bounds not tight)?

- Two competing superposition code designs
  - Effective secrecy
    - channel synthesis built on top of non-secure layer
  - Efficient source coding in the cascade network:
    - Message to closer node is built on layer with message to further node

- How do we prioritize superposition layers in the cascade network?
  - Channel synthesis layer to further node vs. non-secure layer to closer node

Diagram of the Dilemma

- $U_{(i)}$ represents information that is not secured.
- $V_{(i)}$ is used for channel synthesis.



Inner Bound

$$\begin{aligned} R_1 &\geq I(X;V_{(1)}), \\ R_2 &\geq I(X;V_{(2)}), \\ R_0 &> I(W;V_{(1)}|U_{(1)}), \\ \Pi &< \min_{z(\cdot)} \mathbb{E}\, \pi(X,Y_{(2)},Y_{(3)},z(U_{(1)})), \end{aligned}$$

$$U_{(1)} - U_{(2)} - V_{(2)}$$

$$\begin{aligned} X - V_{(1)} &- Y_{(2)}, \\ (X,V_{(1)},Y_{(2)}) - V_{(2)} &- Y_{(3)}, \end{aligned}$$

$$\begin{aligned} H(V_{(2)},U_{(1)}|V_{(1)}) &= 0, \\ H(U_{(2)}|U_{(1)}) &= 0, \\ H(U_{(2)}|V_{(2)}) &= 0, \end{aligned}$$

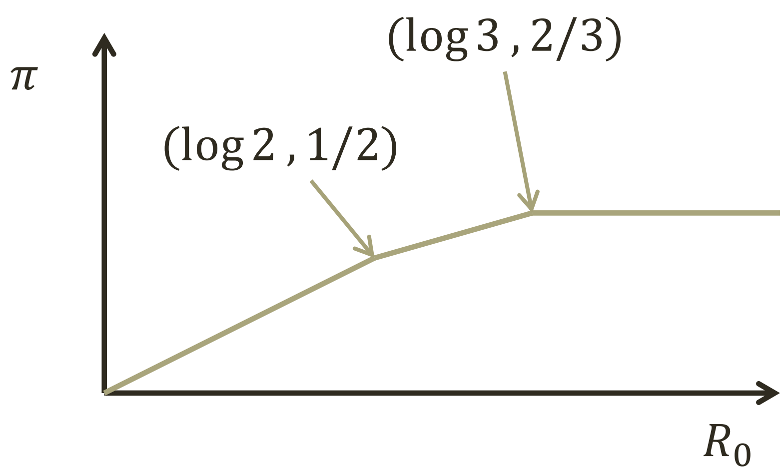
- Likelihood Encoder used for encoding
- Secret key used to index a codebook in the channel synthesis layer

Likelihood Encoder

- Talk on Thursday on this subject
- Encoder (given a codebook and joint distribution) chooses messages stochastically, with probability proportional to the likelihood of the observation X^n given each codeword.
- Analysis is simple. If rates are high enough, induced distribution behaves as a uniform distribution over the codebook connected to the channel.

Three Card Example

- $R_1 \geq \log 3$
- $R_2 \geq \log 3 - 1$ bit



Information Leakage Rate

$$\mathcal{S} \subset \{X, Y_{(2)}, Y_{(3)}\}$$

- Information leakage: $\frac{1}{n} I(S^n; M_1, M_2)$
- Reconstruction constraints:

$$\begin{aligned} \mathbb{E}\,\frac{1}{n}\sum_{t=1}^{n} d_1(X_t, Y_{(2),t}) &\leq D_1, \\ \mathbb{E}\,\frac{1}{n}\sum_{t=1}^{n} d_2(X_t, Y_{(3),t}) &\leq D_2. \end{aligned}$$

- Minimum leakage rate:
  - $\min_{P} I(S; V_{(1)}) - R_0$

$$\mathcal{P} = \left\{ \begin{array}{rcl} P_{X,Y_{(2)},Y_{(3)},V_1,V_2} & : & \\ X & \sim & P_X, \\ X - & V_1 & - Y_{(2)}, \\ (X, V_1, Y_{(2)}) - & V_2 & - Y_{(3)}, \\ H(V_2|V_1) & = & 0, \\ \mathbb{E}\, d_1(X, Y_{(2)}) & \leq & D_1, \\ \mathbb{E}\, d_2(X, Y_{(3)}) & \leq & D_2, \\ I(X; V_1) & \leq & R_1, \\ I(X; V_2) & \leq & R_2. \end{array} \right\}.$$