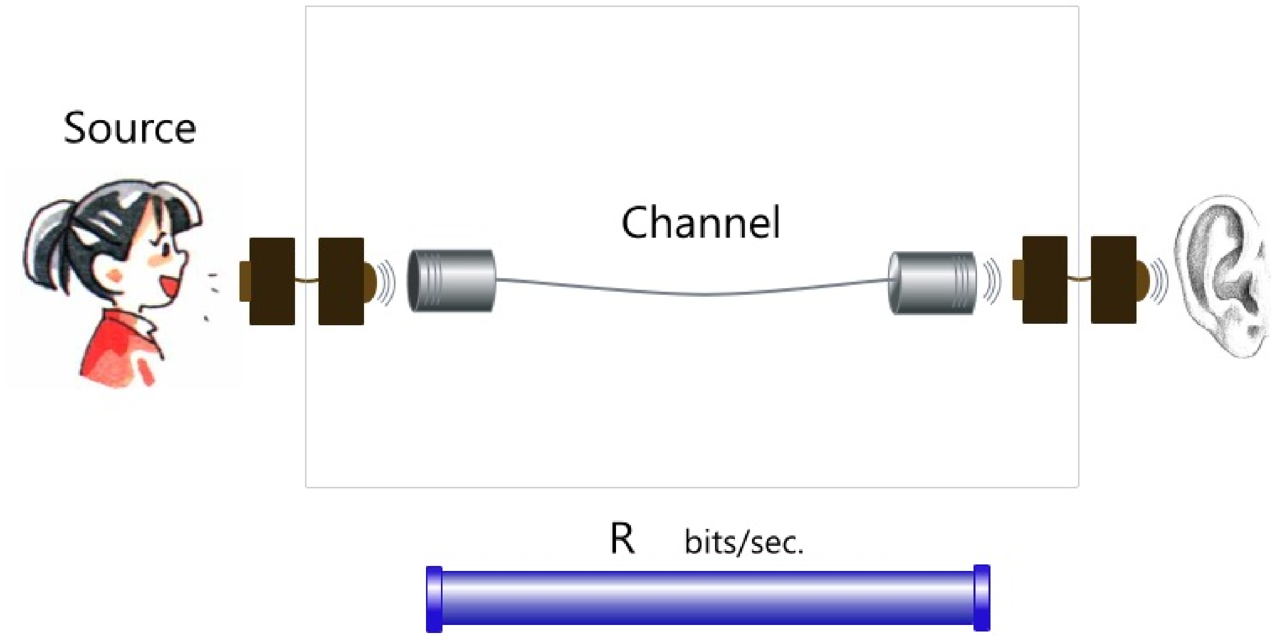
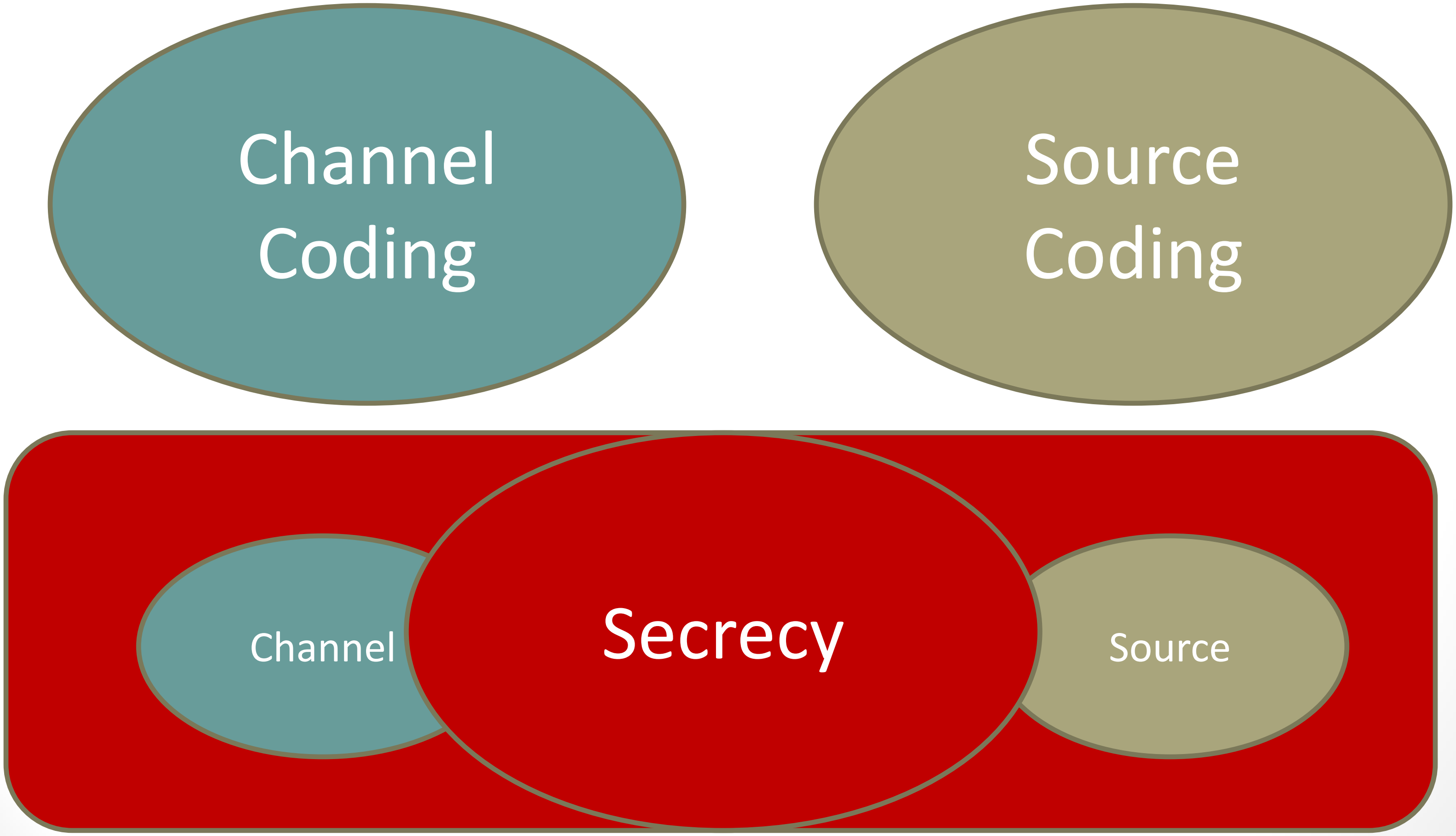
PRINCETON UNIVERSITY

Rate-distortion Theory for Comm. in Games

Paul Cuff, C. Schieler, E. Song, S. Satpathy
Electrical Engineering
Princeton University

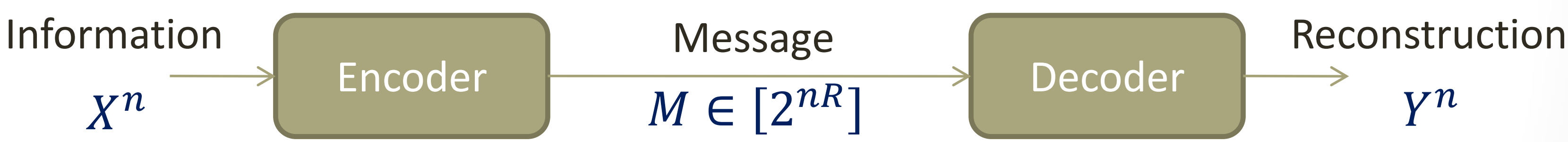

Source
Channel
R bits/sec.

Information Theory



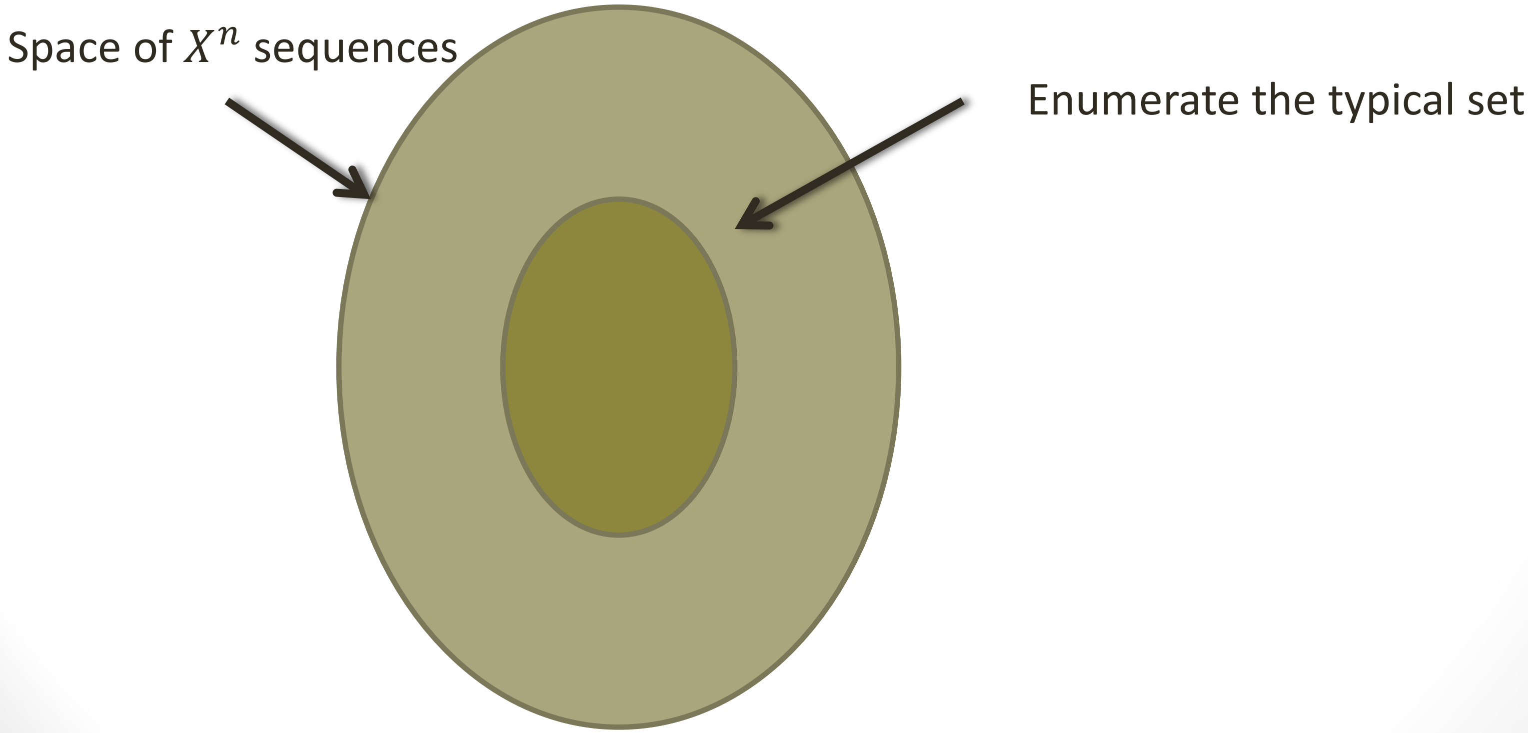
Source Coding

- Describe an information signal (source) with a message.



Entropy

- If X^n is i.i.d. according to P_X
- $R > H(X)$ is necessary and sufficient for lossless reconstruction



Lossy Source Coding

- What if the decoder must reconstruct with less than complete information?

- Error probability will be close to one

- Distortion as a performance metric

$$\frac{1}{n}\sum_{i=1}^{n} d(X_i, Y_i)$$

Puzzle

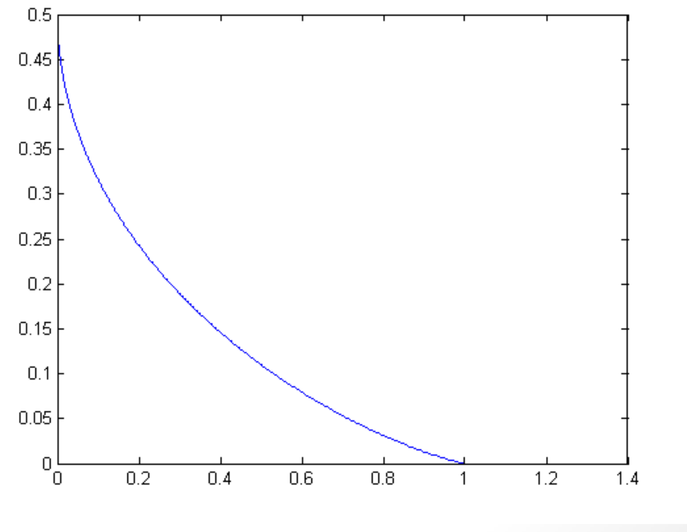
- Describe an n-bit random sequence
- Allow 1 bit of distortion
- Send only 1 bit

Rate Distortion Theorem

- [Shannon]
- Choose p(y|x):

$$R > I(X;Y)$$
$$D > E\, d(X,Y)$$

$$D \geq 1 + p\log p + (1-p)\log(1-p)$$



Game Setting

- X is the state (stochastic)
- Y and Z are the actions of the players
- $\pi(X, Y, Z)$ is the game payoff

- Information structure:
  - How does information about X effect the game?
  - Correlated equilibriums, etc.

- Optimal Information:
  - What is the most useful information about X?

Simplifying Assumptions

- X, Y, and Z discrete
- Zero-sum game
- State information has cardinality constraint and is designed to help Player Y.

Communication Details

- Repeated Game:
  - Full information of past known to both players
  - Block communication allowed

- Communication specifics
  - Constraint on average bit rate per iteration of game
    - i.e. Cardinality of information constrained to 2^{nR}
    - Communication viewed by both parties
  - Secret key known only to encoder and Player Y
    - Also at a restricted rate R_0

Question to Answer

- What is the max-min average payoff for Player Y?
  - Maximize over encodings and strategies
  - Minimize over Player Z's strategy.

$$\underbrace{\max_{\substack{n \\ Encodings \\ Strategies}} \min_{\{Z_t = z_t(M, X^{t-1}, Y^{t-1})\}} \mathbf{E} \frac{1}{n} \sum_{t=1}^{n} \pi(X_t, Y_t, Z_t)}_{\Pi}$$

Payoff-Rate Function

- Maximum achievable average payoff

Theorem:

$$\Pi(R, R_0) = \max \left\{ \Pi \ : \ \begin{array}{rcl} & & \exists\, p(u,v|x)p(y|u,v)\ s.t. \\ R & \geq & I(X;U,V), \\ R_0 & \geq & I(W;V|U), \\ \Pi & = & \min_{z(u)} \mathbf{E}\, \pi(X,Y,z(U)). \end{array} \right\}$$

- Markov relationship:

$$X - (U,V) - Y$$

Block Encoding vs. Instantaneous

Instantaneous Encoding

- $|\mathcal{V}| \leq 2^{R_0}$
- $|\mathcal{U}| \leq 2^{R}$
- $V \perp X$
- $X - (U,V) - Y$

Block Encoding Asymptotics

- $I(V;X,Y|U) \leq R_0$
- $I(U;X|V) + I(V;X) \leq R$
- $X - (U,V) - Y$

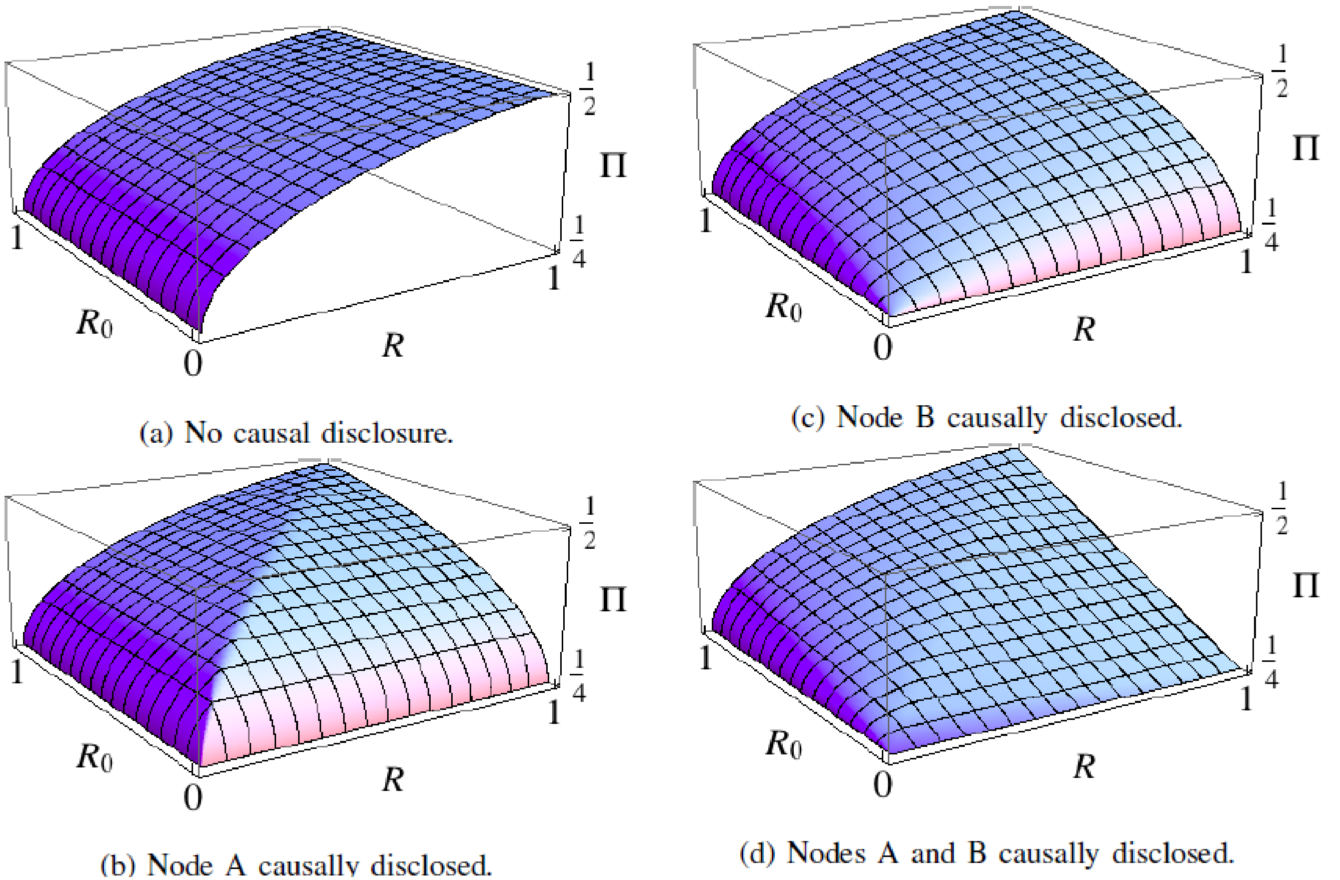
Generalizations

- Those we can solve:
  - Player Z sees only partial information of past
  - Player Y sees only partial information of past
  - Payoff is a vector
  - X, Y, and Z are not discrete
  - Player Z sees information about X and Y ahead of time

- Those we can't:
  - Communication (M) is not seen by Player Y
  - Past information delayed to Player Y

Binary Jamming Example

State distribution is Bernoulli(1/2).
Payoff: One point if Y=X but Z≠X.



(a) No causal disclosure.

(b) Node A causally disclosed.

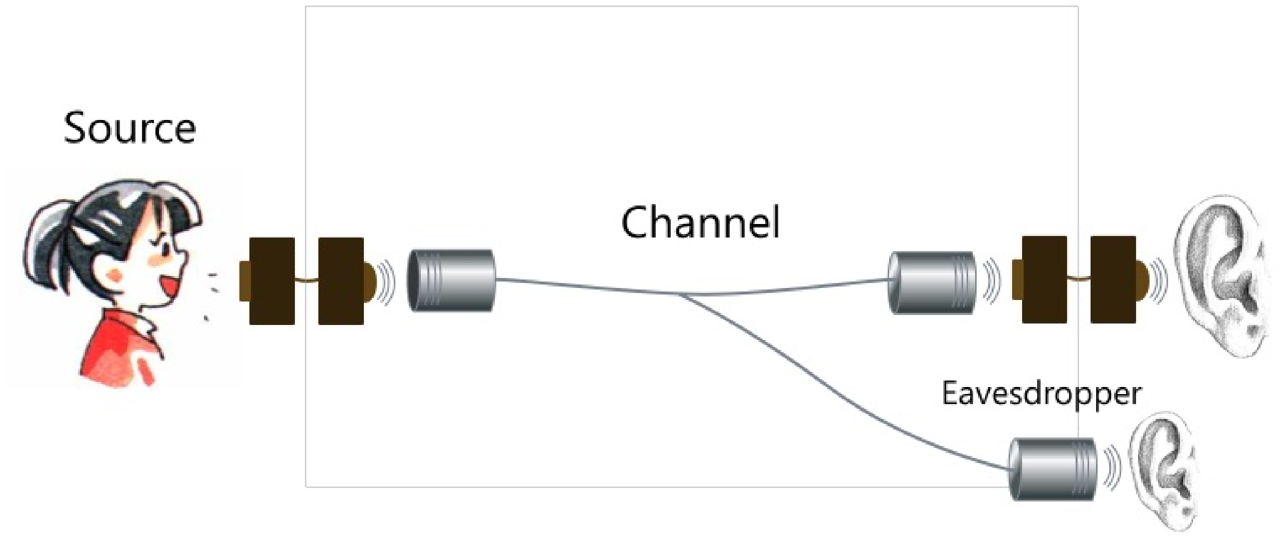
(c) Node B causally disclosed.

(d) Nodes A and B causally disclosed.

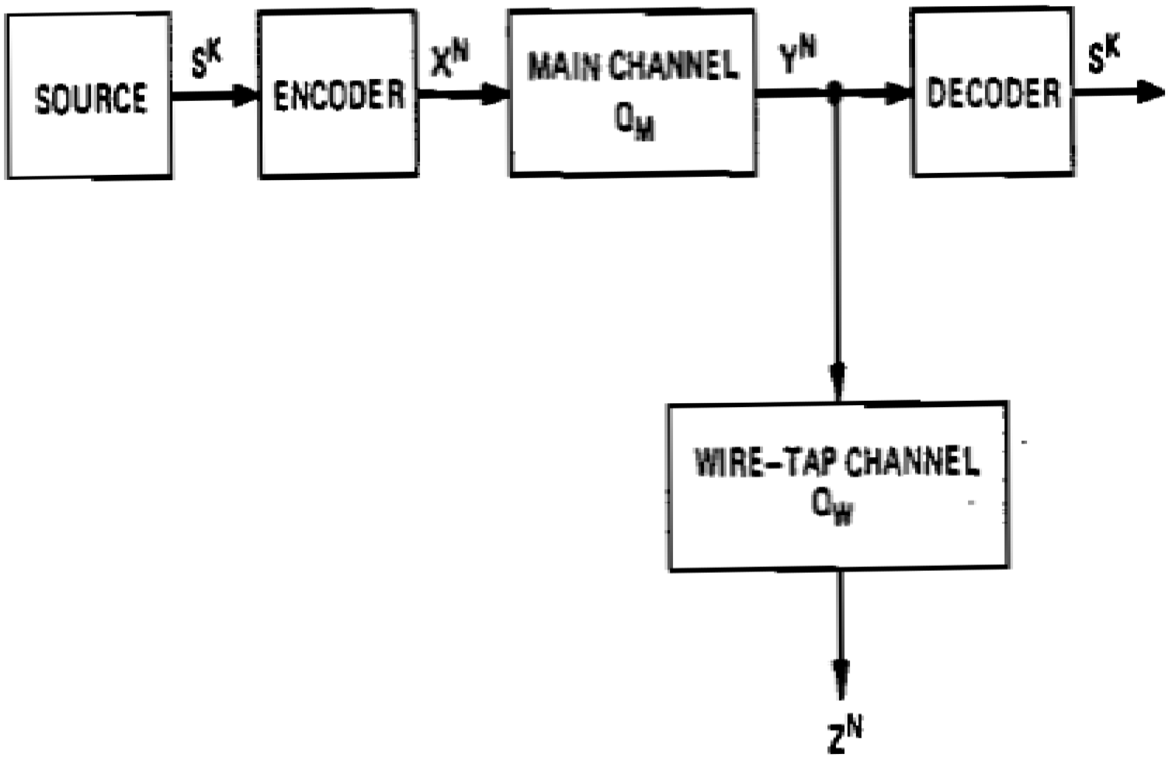
Information Theory Innovations

- Use digital resources to create an arbitrary "analog" channel
  - Broadcast channel: $P_{Y,U|X}$
  - Requires stochastic decoder
- New encoder design for simple analysis
  - Likelihood encoder

Information Theoretic Security



Wiretap Channel
[Wyner 75]



Wiretap Channel
[Wyner 75]

We take the equivocation

$$\Delta \triangleq \frac{1}{K} H(\mathbf{S}^K | \mathbf{Z}^N)$$

as a measure of the degree to which the wire-tapper is confused.

Wiretap Channel
[Wyner 75]

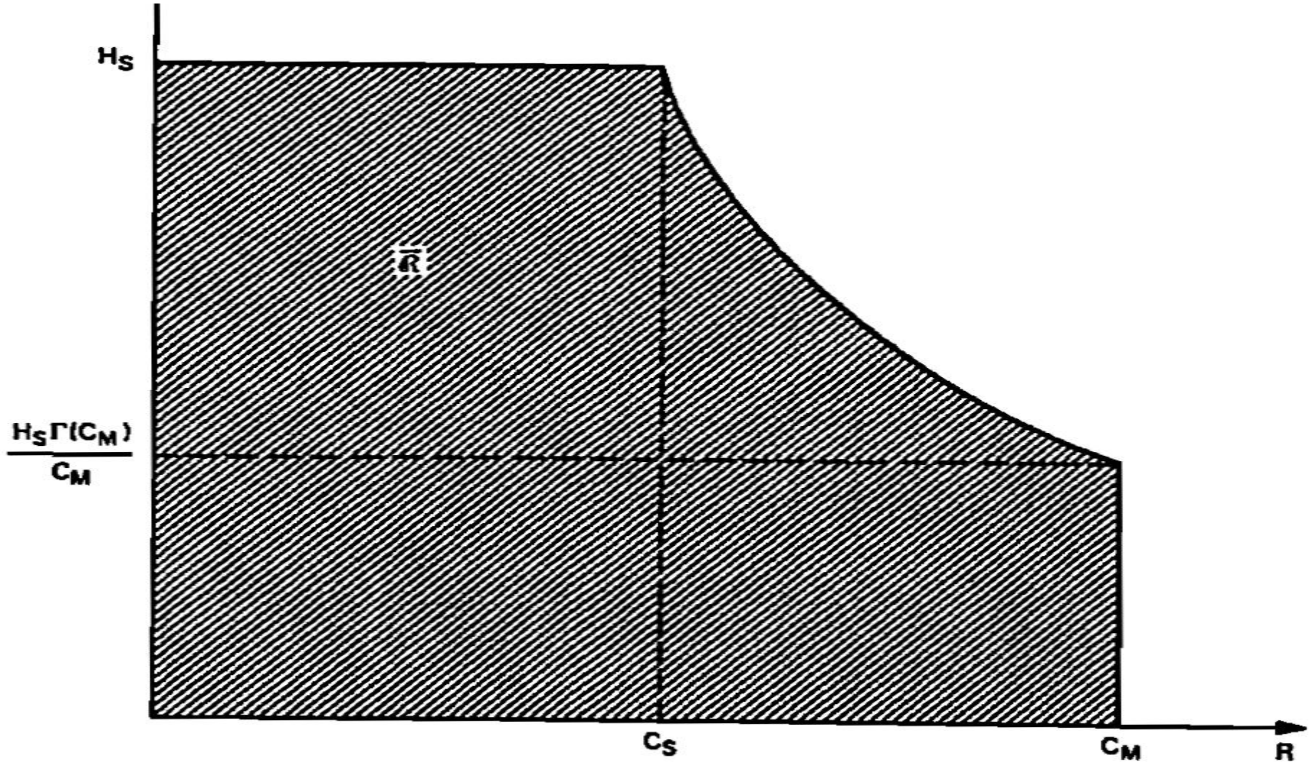


Fig. 3—Region $\bar{\mathcal{R}}$.

Theorem 2: The set $\mathcal{R}$, *as defined above, is equal to* $\bar{\mathcal{R}}$, *where*

$$\bar{\mathcal{R}} \triangleq \{(R, d): \quad 0 \leqq R \leqq C_M, \quad 0 \leqq d \leqq H_S, \quad Rd \leqq H_S\Gamma(R)\}.$$

Confidential Messages

[Csiszar, Korner 78]

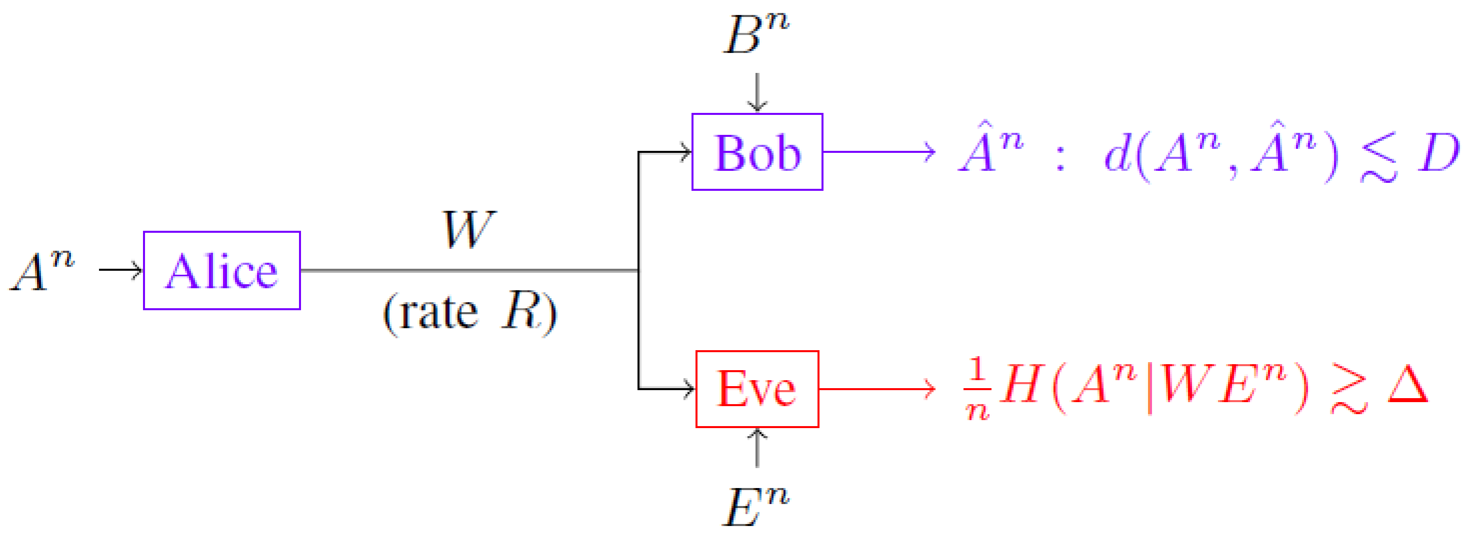
Following Wyner [8], we shall measure confidentiality by equivocation.

Confidential Messages

[Csiszar, Korner 78]

Following Wyner [8], we shall measure confidentiality by equivocation. Our main result is a single-letter characterization of the set of triples (R_1, R_e, R_0) such that, in addition to a common message at rate R_0, a private message can be sent reliably at rate R_1 to receiver 1 with equivocation at least R_e per channel use at receiver 2.

Villard-Piantanida 2010



Our Approach to Security

- Communication for games is a more meaningful measurement of “secure” communication.

- Don’t ask encoder to maximize equivocation.
- Ask encoder to maximize score in a game.
  - Equivalent to forcing an eavesdropper to have high distortion when reconstructing the signal.

- Natural extension of rate-distortion theory to secrecy systems.
  - Problem involves:
    - Source distribution
    - Rates
    - A payoff function

The Best Part

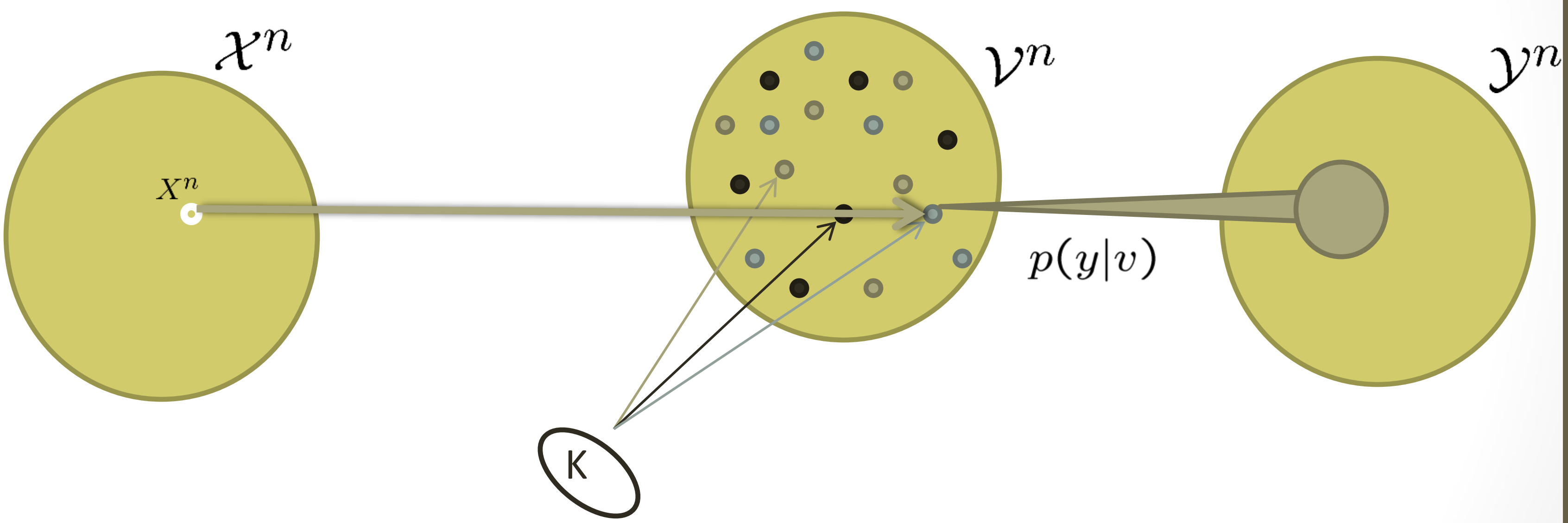
- Rate-distortion theory for secrecy (i.e. comm. for games) yields maximum equivocation as a special case.
  - "Log-loss function"

$$\pi_1(x, y, z) = \log \frac{1}{z(x)}$$

Summary

- Formula to characterize asymptotic performance of block communication of state in zero-sum games
  - Synthetic analog channel
  - Likelihood encoder
- Results yield more general analysis of security communication than current tradition of using equivocation (i.e. “information leakage rate”).

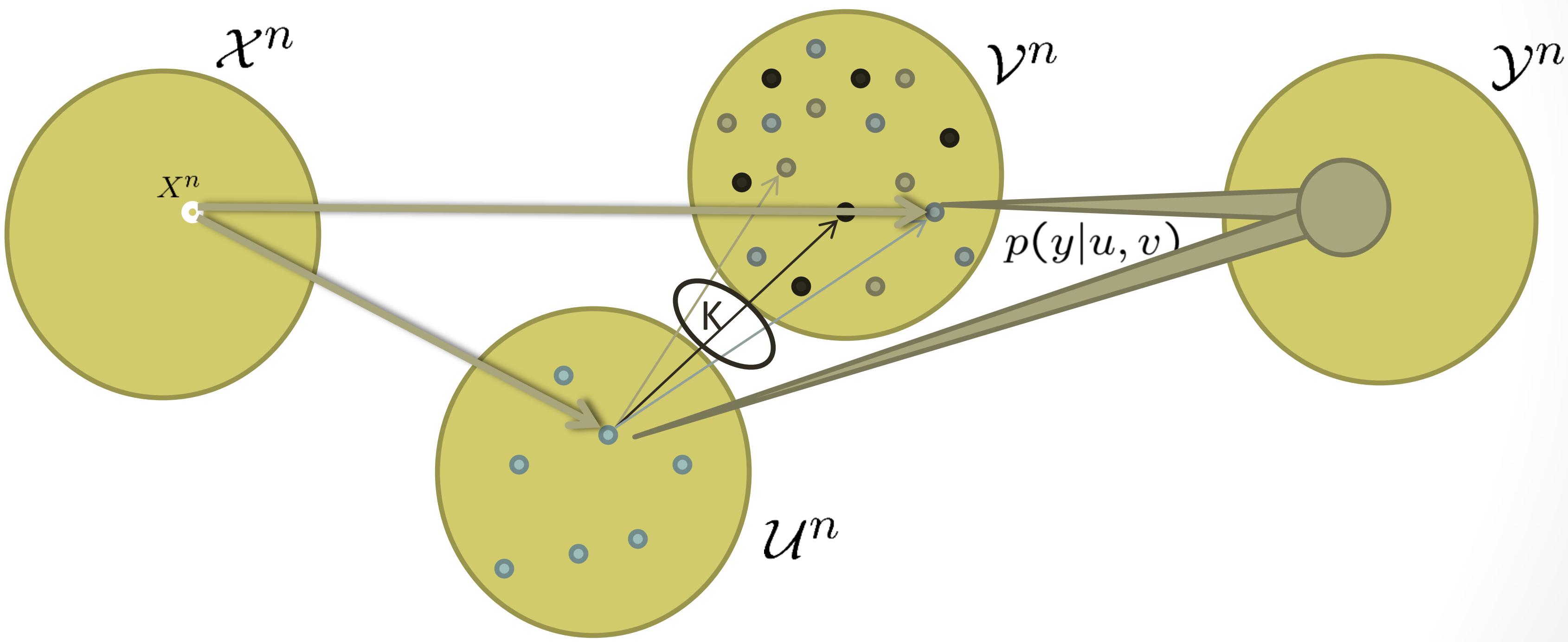
Structure of Strong Coord.



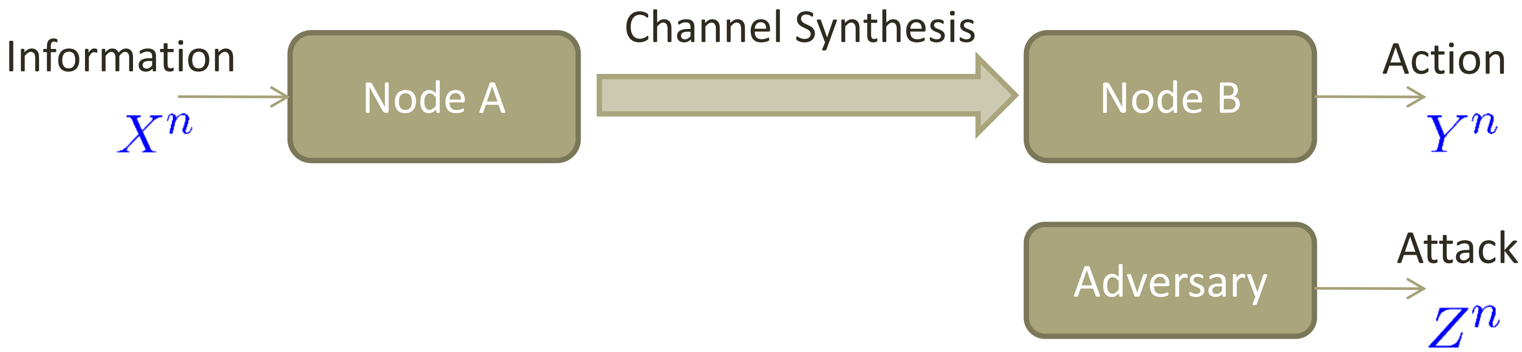
Comm. rate: $R > I(X;U)$

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

Structure of Secrecy Code

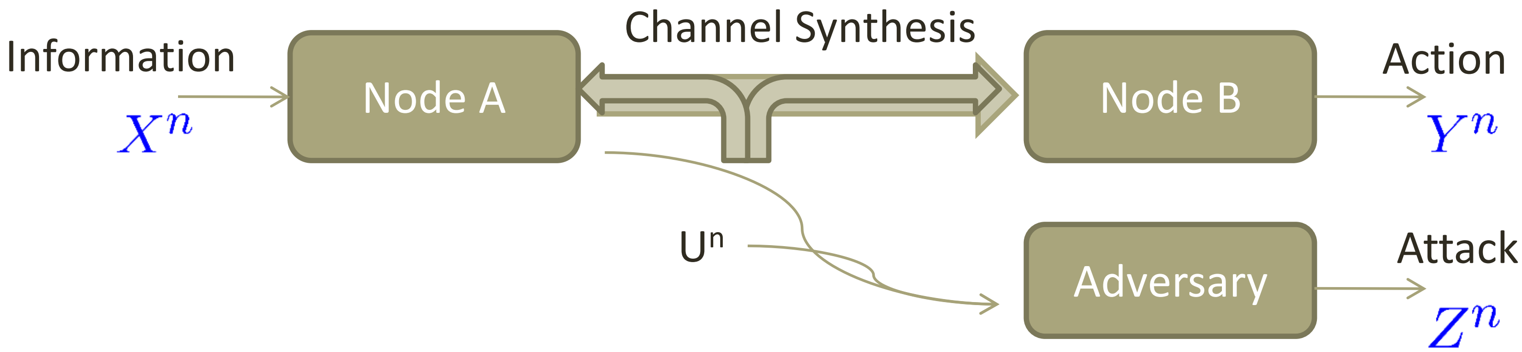


Strong Coord. for Secrecy



Not optimal use of resources!

Strong Coord. for Secrecy

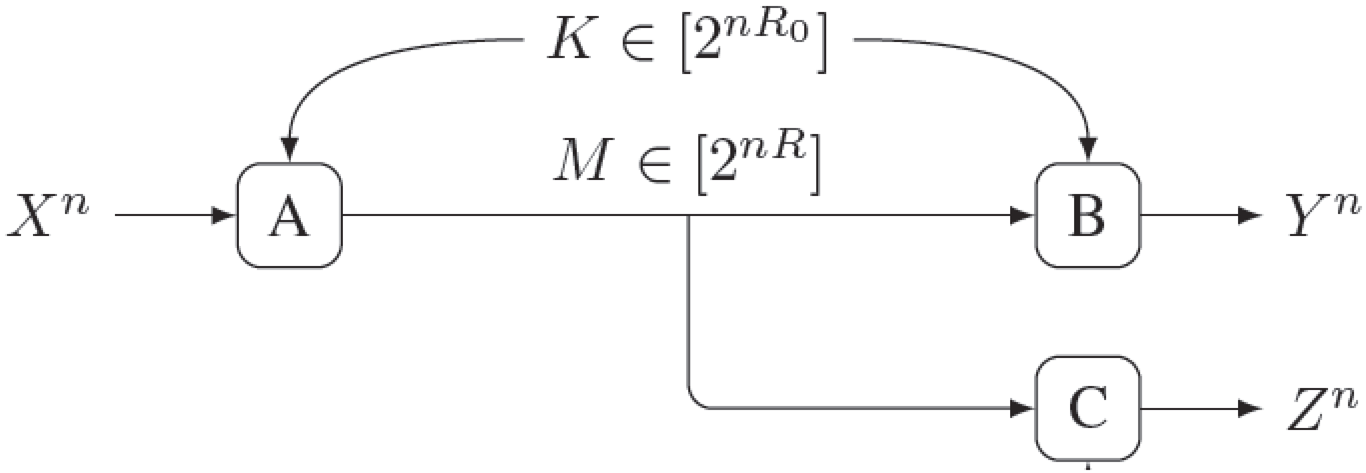


Reveal auxiliary U^n "in the clear"

Best Reconstruction Yields Entropy

$$\min_{Z=z(U)} \mathbf{E} \log \frac{1}{Z(X)} = H(X|U)$$

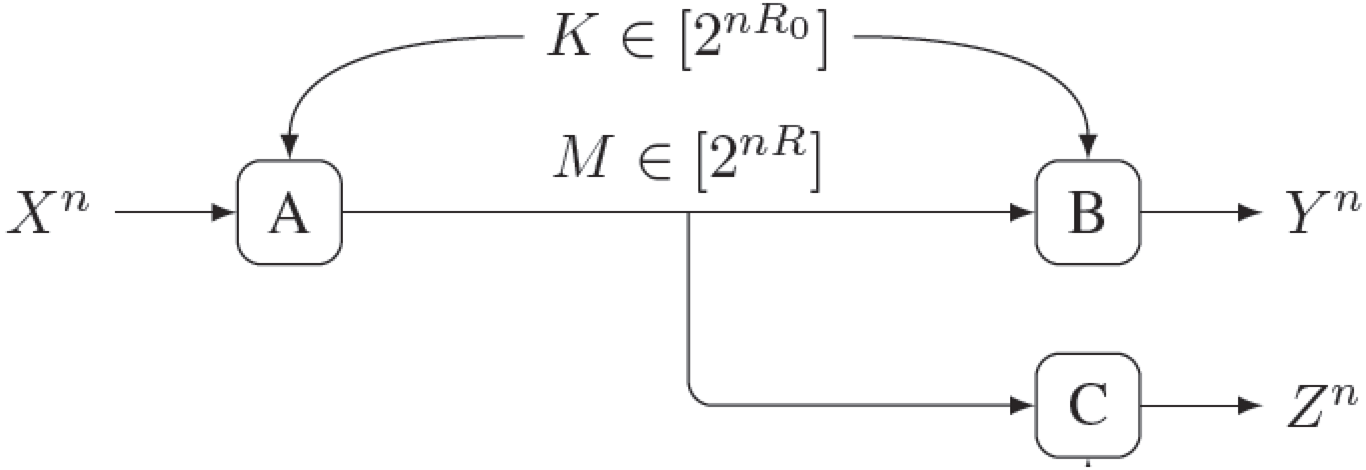
Log-loss π_1 (disclose X causally)



$$\max_{A,B} \; \max_{\{Z_i = z_i(M, Z^{i-1})\}} \; \frac{1}{n} \sum_{i=1}^{n} \pi(X_i, Y_i, Z_i)$$

$$\min \frac{1}{n} H(X^n | M) \quad \frac{1}{n} \sum_{i=1}^{n} H(X_i | M, X^{i-1})$$

Result 1 from Secrecy R-D Theory



$$\max_{A,B} \frac{1}{n} H(X^n|M)$$

$$= \min\{H(X|Y) + R_0,\ H(X)\}$$