Gaussian Secure Source Coding and Wyner's Common Information

Sanket Satpathy and Paul Cuff
(Princeton University)

This Work

- Optimize a rate region
- Show that a Gaussian auxiliary variable is optimal for Gaussian setting

This Work

- X, Y, U jointly Gaussian (given)
- V is auxiliary: $X - (U,V) - Y$

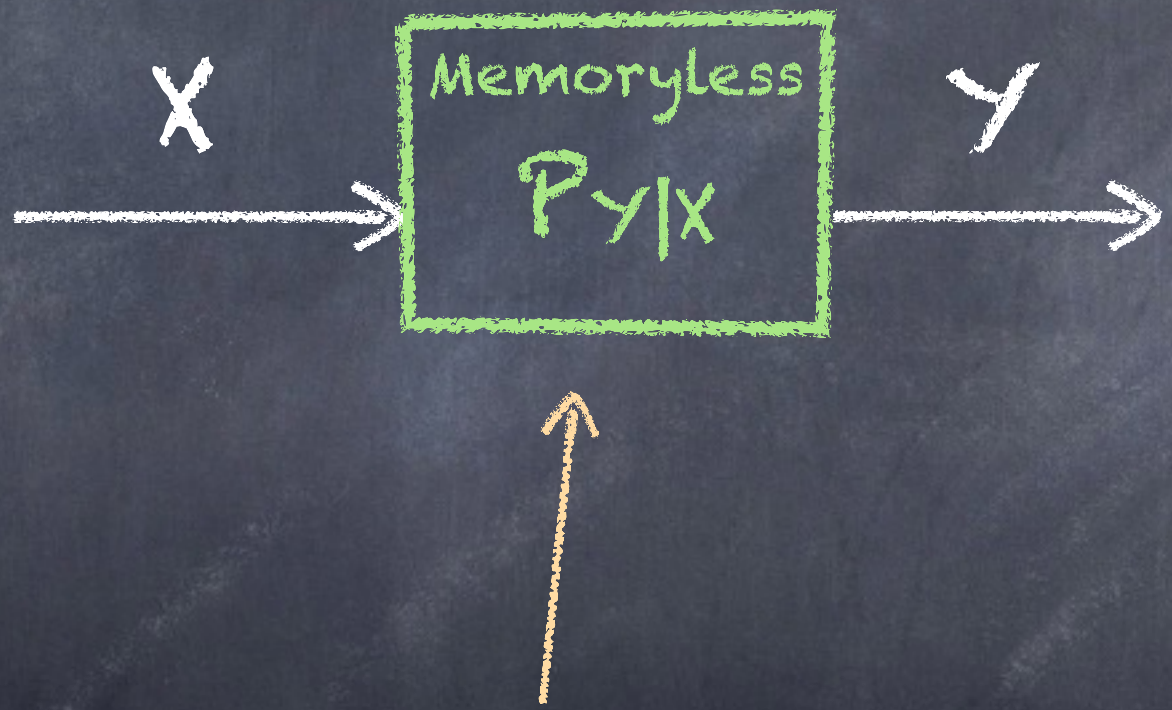
$$R \geq I(X;U,V)$$
$$R_0 \geq I(X,Y;V|U)$$

Context

- Synthetic Noise

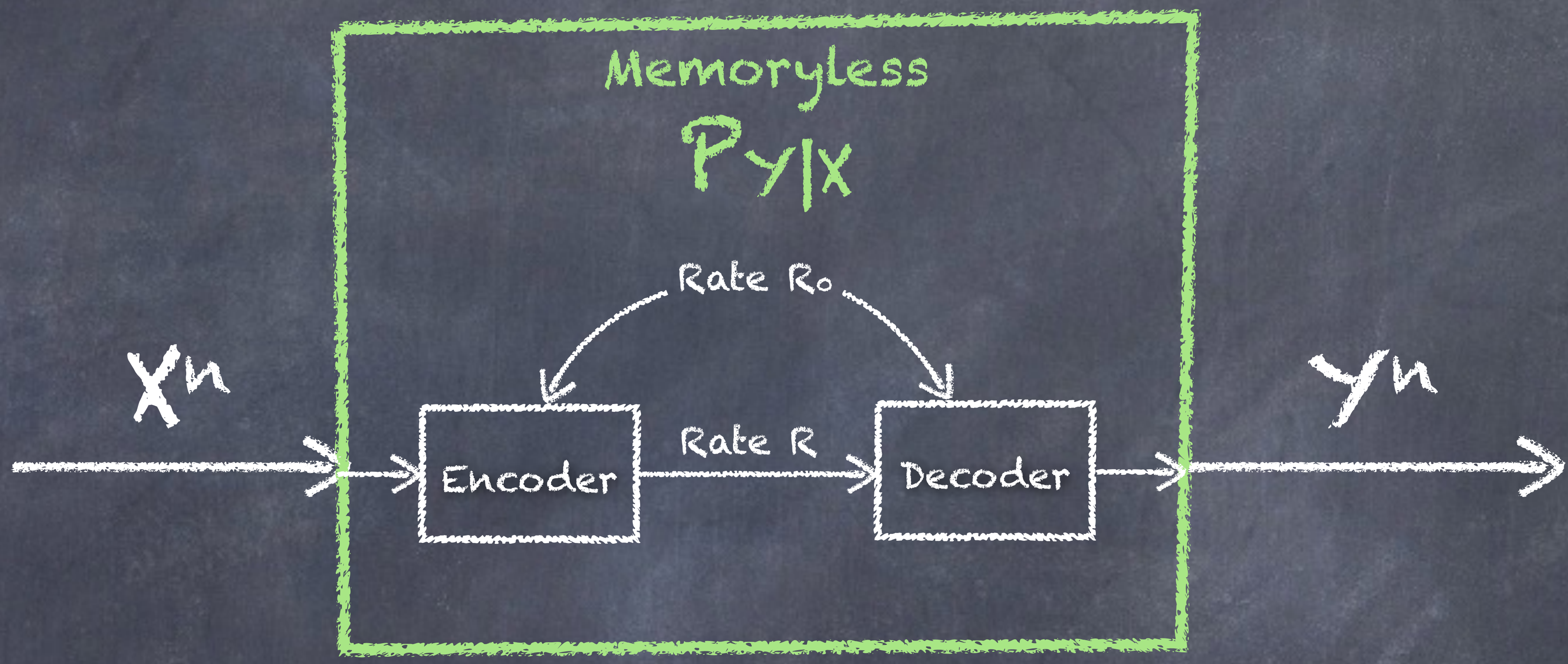
Context

- Synthetic Noise



What resources are required to produce this?

Synthetic Noise

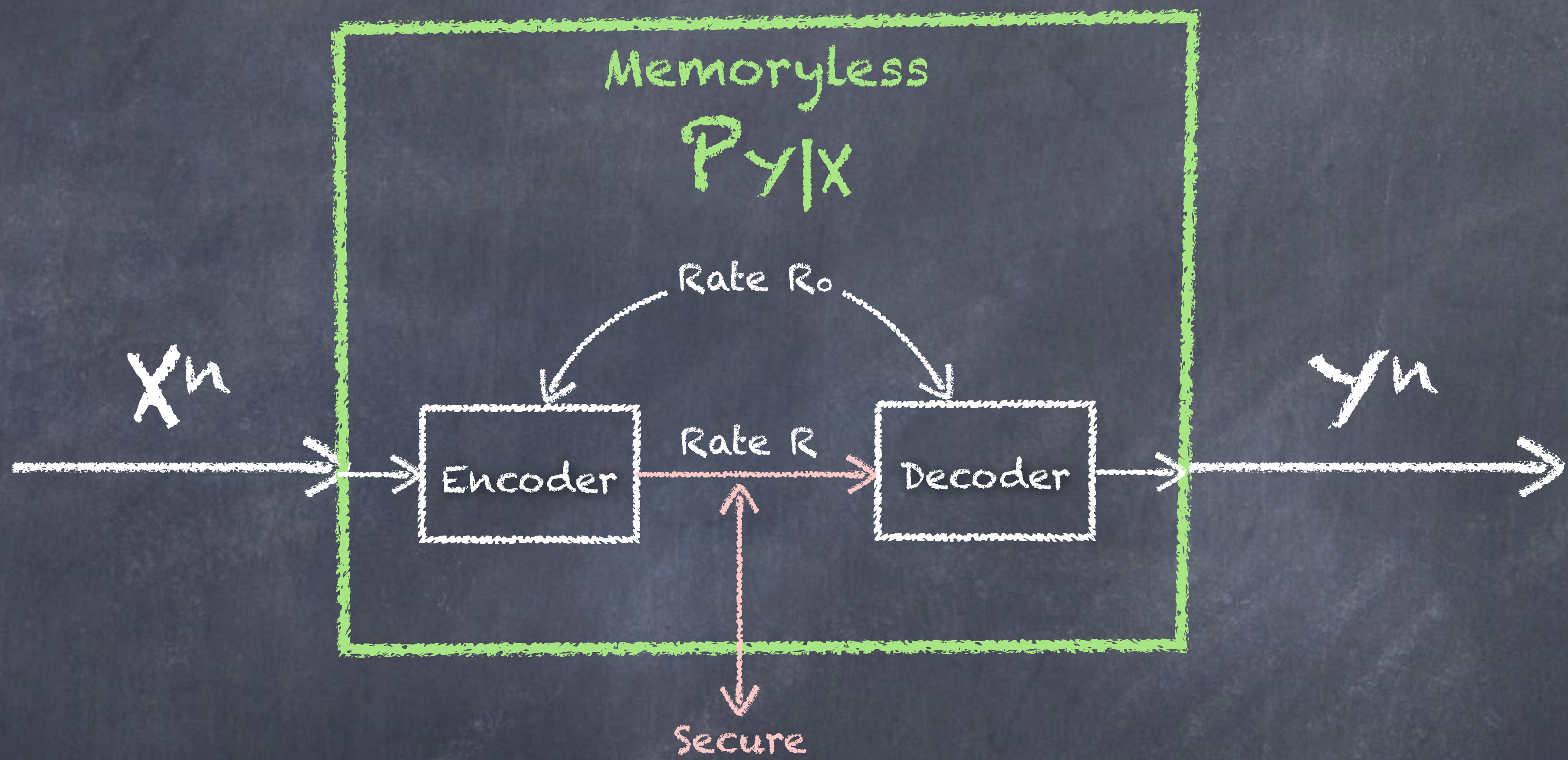


Resource Requirements: Choose V s.t. X–V–Y

$$R \geq I(X;V)$$
$$R + R_o \geq I(X,Y;V)$$

[Cuff, "Distributed Channel Synthesis," '13] [Bennett, et. al., "Reverse Shannon Theorem," '14]

Synthetic Noise

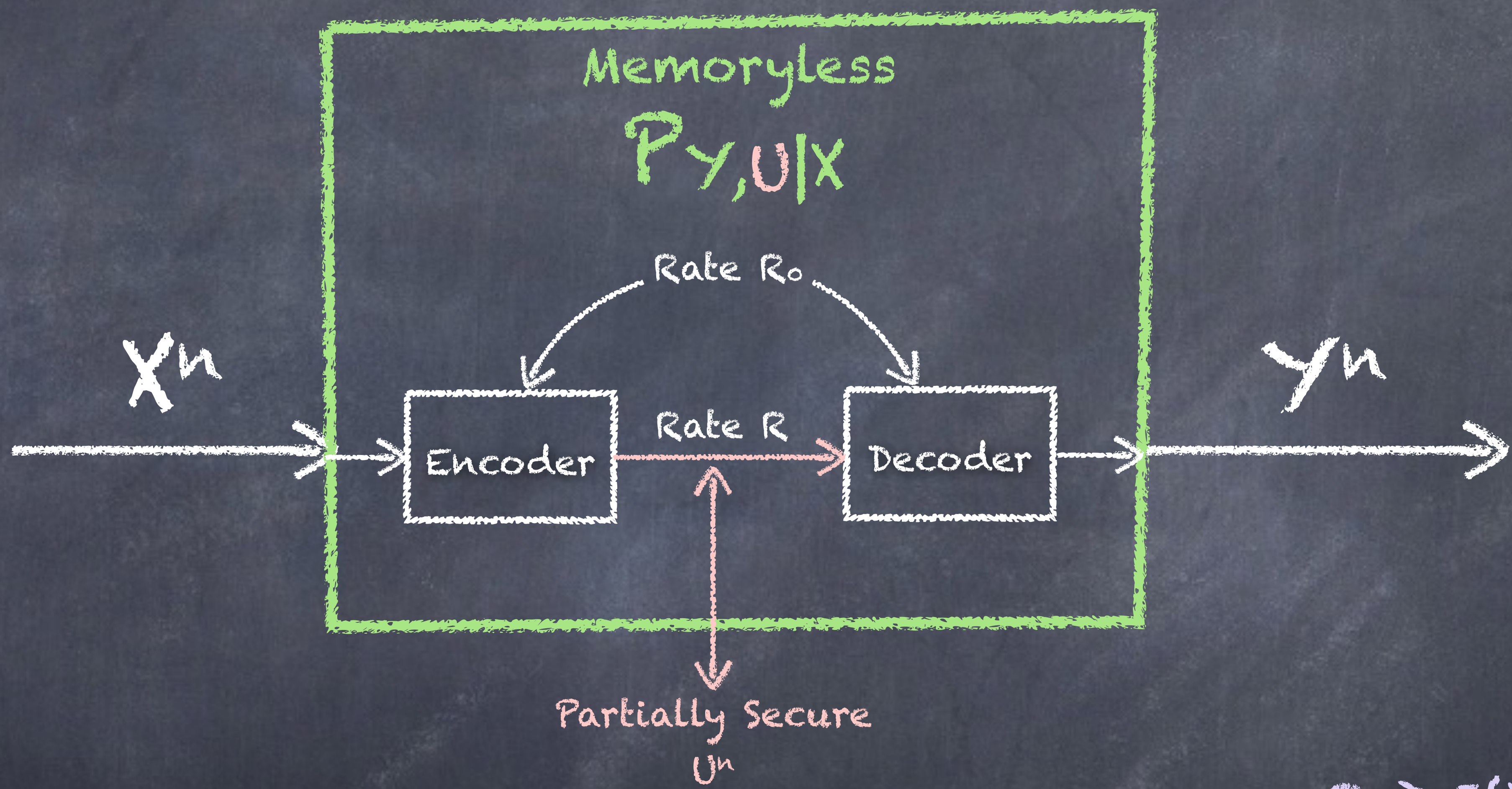


Resource Requirements: Choose V s.t. $X-V-Y$

$$R \geq I(X;V)$$
$$R + R_0 \geq I(X,Y;V)$$

[Cuff, "Distributed Channel Synthesis," '13]

Synthetic Noise

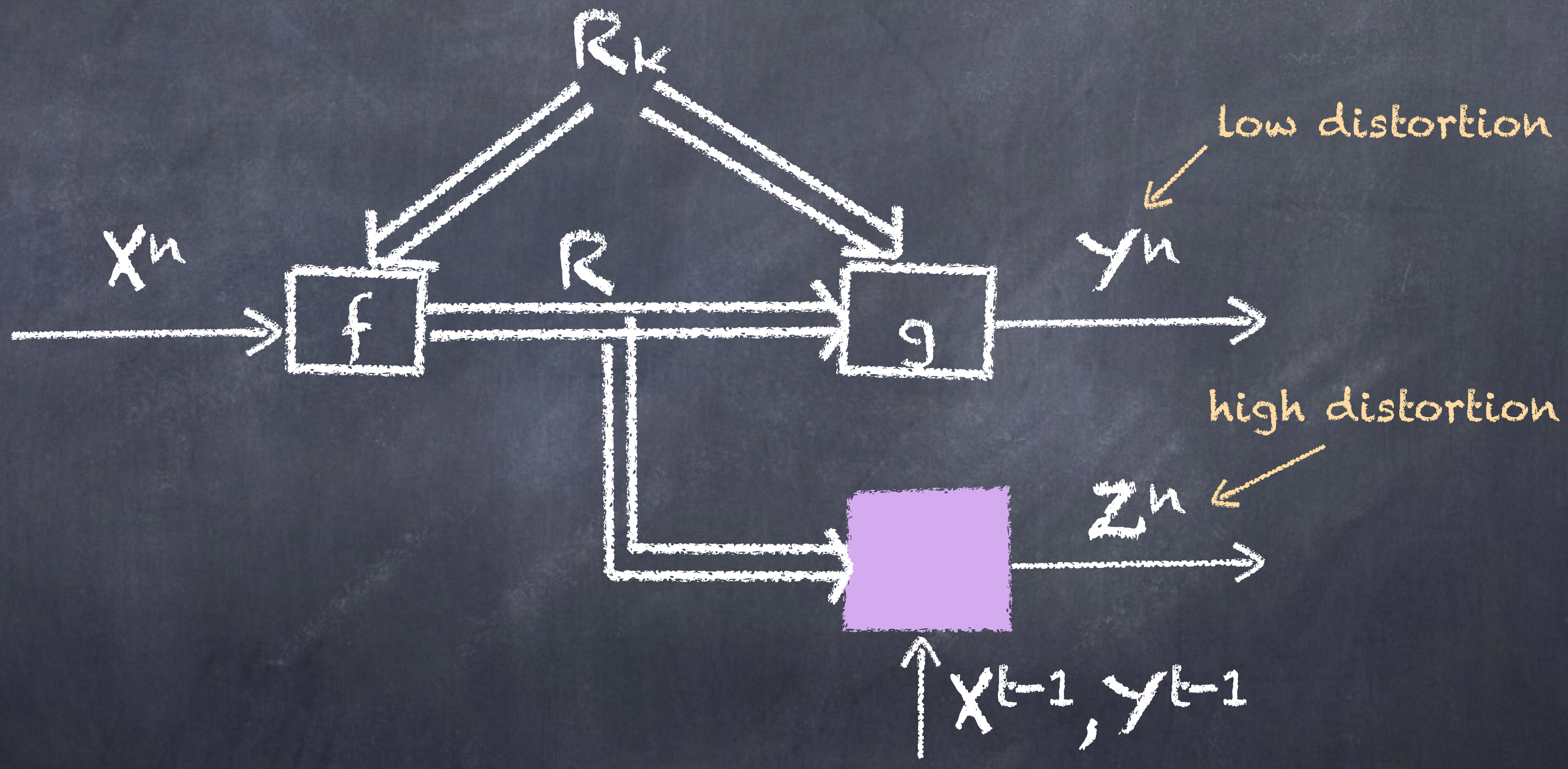


Resource Requirements: Choose V s.t. $X - (U,V) - Y$

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

[Schieler-Cuff, "Rate-Distortion Theory for Secrecy Systems," '14]

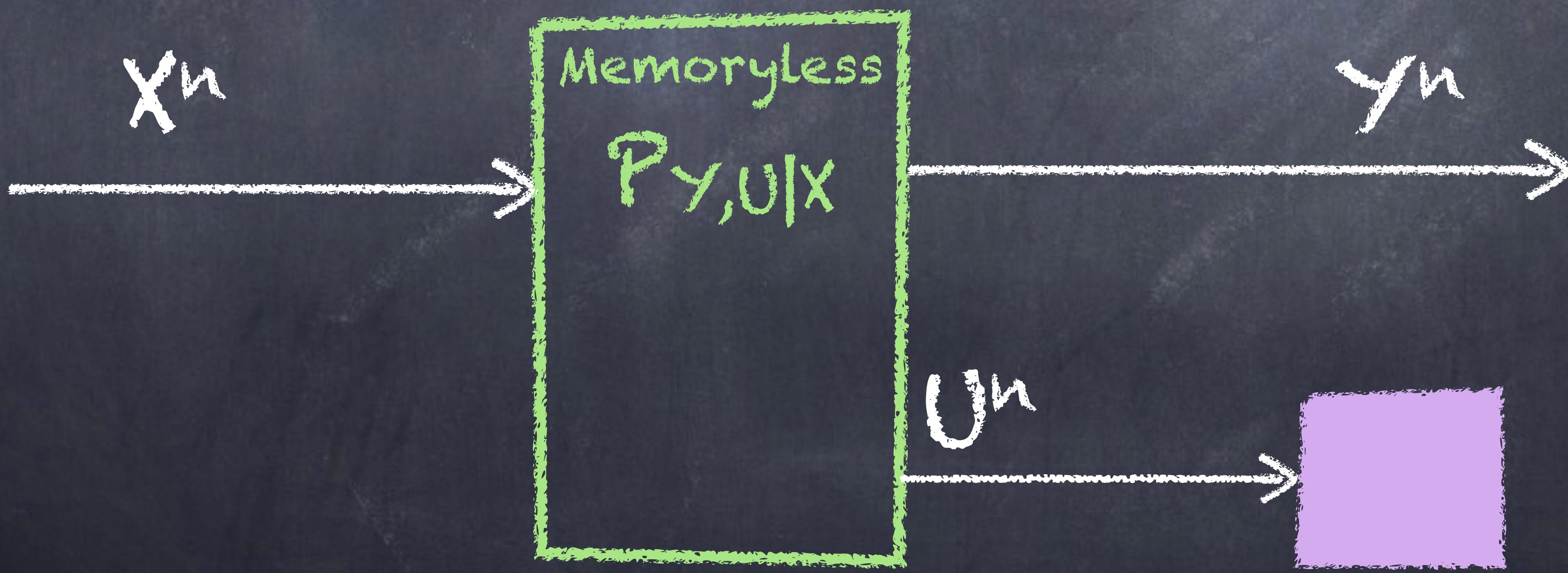
Secure Source Coding



[Schieler-Cuff, "Rate-Distortion Theory for Secrecy Systems," '14]

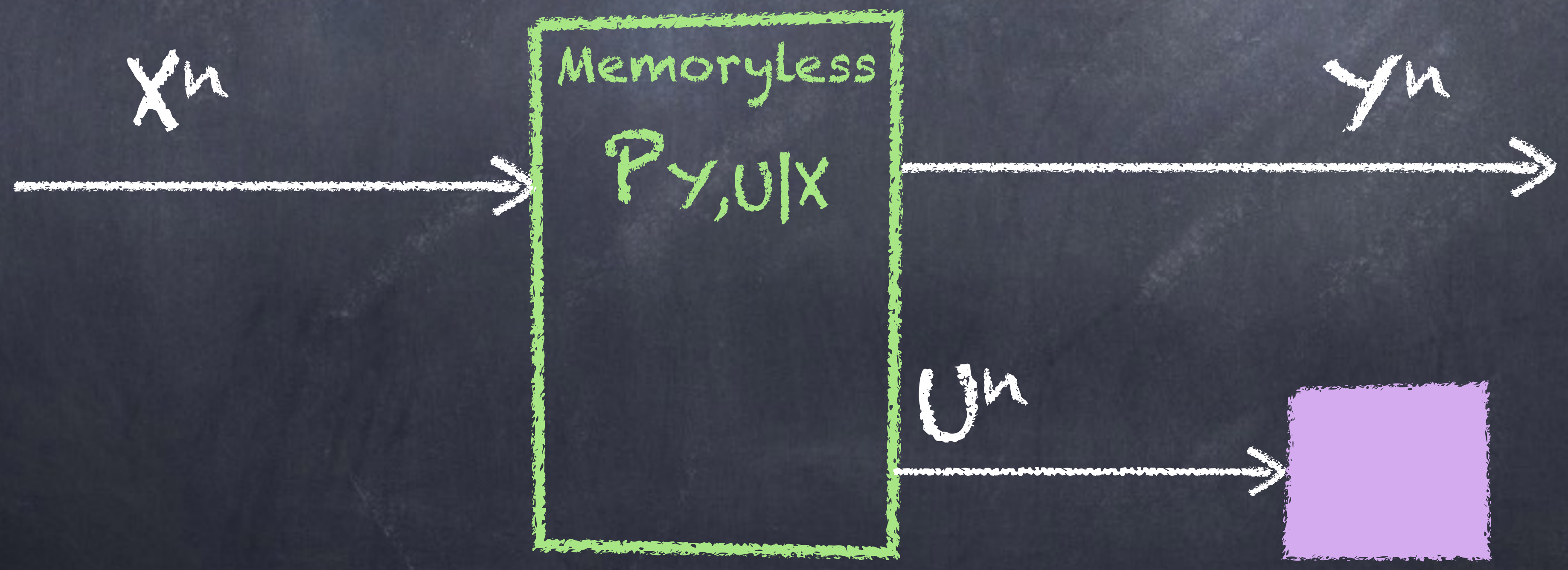
Synthetic Broadcast Channel

Optimal Communication for secure source coding

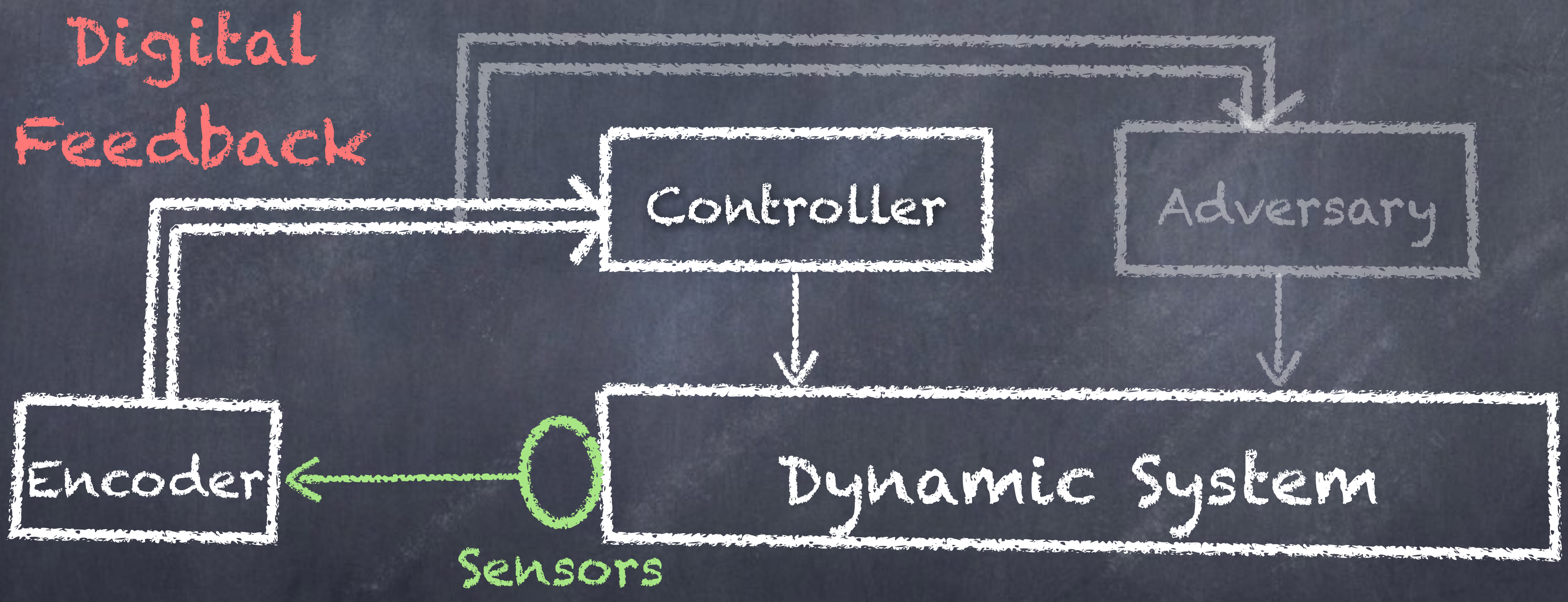


Properties

- U^n is statistically typical
- $X^n, Y^n | U^n$ is indistinguishable from memoryless channel

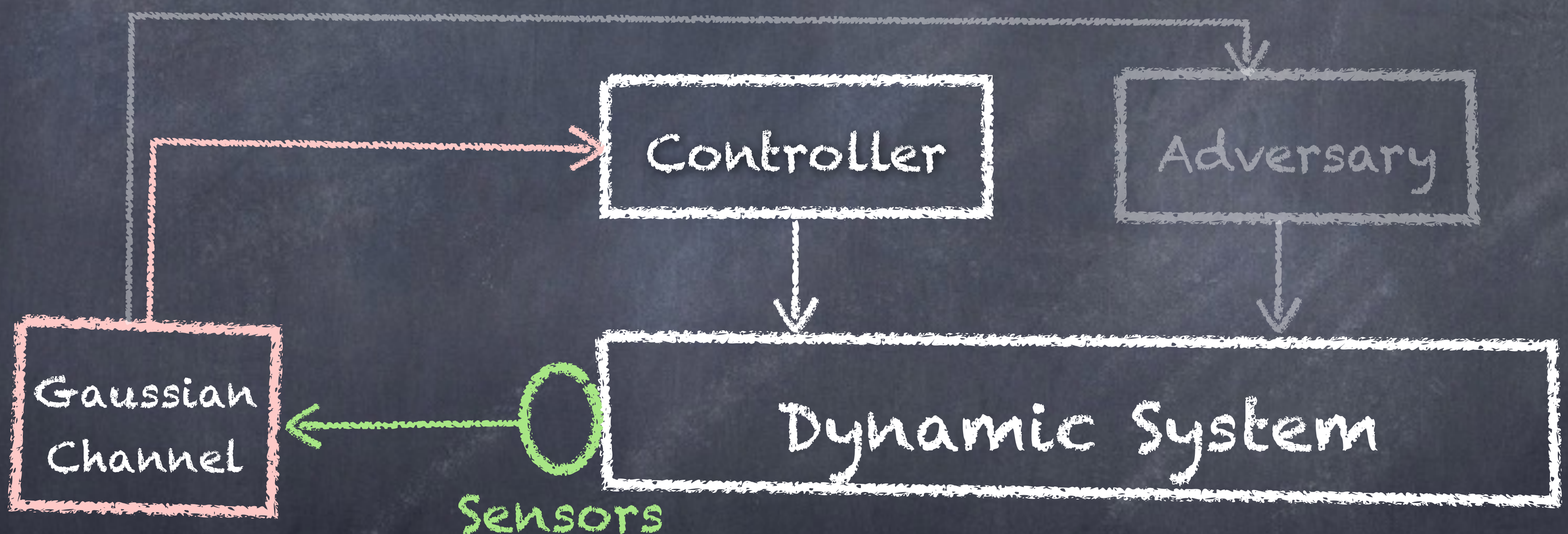


Gaussian Case - Control Application



[Tatikonda-Mitter-Sahai, "Data-Rate Theorem," '98]

Gaussian Case - Control Application



Rate-distortion theory (Gaussian channel): same fundamental limit

[Tatikonda-Mitter-Sahai, "Data-Rate Theorem," '98]

Optimization Problem

- X, Y, U jointly Gaussian (given)
- V is auxiliary: $X - (U,V) - Y$

$\Sigma_i \; 1/2 \log (1/(1-\rho_i^2))$

$$R \geq I(X;U,V) \quad = I(X;U) + I(X;V|U)$$
$$R_0 \geq I(X,Y;V|U)$$

$X, Y|U \sim$ Gaussian with covariance $\Sigma_{X,Y|U}$

Simpler Optimization

- X, Y jointly Gaussian ($\Sigma_{X,Y|U}$)
- V is auxiliary: $X - V - Y$

$$R \geq I(X;V)$$
$$R_0 \geq I(X,Y;V)$$

Without loss of generality:

$$\Sigma_X = I$$
$$\Sigma_Y = I$$
Σ_{XY} is diagonal

Process X and Y (invertibly):

Whiten: $\Sigma_X^{-1/2} X$

SVD of $P = \Sigma_X^{-1/2} \Sigma_{XY} \Sigma_Y^{-1/2}$

Collection of Independent Pairs

- X_k, Y_k jointly Gaussian scalars
  - mutually independent pairs
- V is auxiliary: $X^K - V - Y^K$

$$R \geq I(X^K; V)$$
$$R_0 \geq I(X^K, Y^K; V)$$

Use an independent V_k for each pair of scalars

Collection of Independent Pairs

- X_k, Y_k jointly Gaussian scalars
  - mutually independent pairs
- V is auxiliary: $X^K - V - Y^K$

$$R \geq I(X^K;V) \geq \sum I(X_k;V)$$
$$R_0 \geq I(X^K,Y^K;V) \geq \sum I(X_k,Y_k;V)$$

Use an independent V_k for each pair of scalars

Scalar Optimization

- X,Y jointly Gaussian scalars
- V is auxiliary: X–V–Y

$$R \geq I(X;V)$$
$$R_0 \geq I(X,Y;V)$$

Claim: Optimized by jointly Gaussian V

Wyner's Common Information

- X,Y jointly Gaussian scalars
- V is auxiliary: X–V–Y

$$R_0 \geq I(X,Y;V)$$

Claim: Optimized by jointly Gaussian V

[Xu-Liu-Chen, '13]

Vector Gaussian Common Information

$$C(X;Y) = I(X;Y) + \sum \log (1+\rho_i)$$

where ρ_i are singular values of $\Sigma_X^{-1/2} \Sigma_{XY} \Sigma_Y^{-1/2}$

Scalar Optimization

- X,Y jointly Gaussian scalars
- V is auxiliary: X–V–Y

$$R \geq I(X;V)$$
$$R_0 \geq I(X,Y;V)$$

Claim: Optimized by jointly Gaussian V

Sai's Proof

- Consider the weighted combination:
  - $\lambda I(X;V) + I(X,Y;V)$
    $= (\lambda+1)I(X;V) + I(Y;V) - I(X;Y)$
- Consider optimal estimation error
  - $D_x = 1 - E[E[X|V]^2]$
  - $D_y = 1 - E[E[Y|V]^2]$

Sai's Proof

- Consider the weighted combination:
  - $\lambda I(X;V) + I(X,Y;V)$
    $\geq (\lambda+1)R(D_x) + R(D_y) - I(X;Y)$
- Consider optimal estimation error
  - $D_x = 1 - E[E[X|V]^2]$
  - $D_y = 1 - E[E[Y|V]^2]$

Upper bound on distortion

- Claim: $\rho^2 \le (1-D_x)(1-D_y)$

- Proof (Cauchy-Schwarz):

$$\rho^2 = E[XY]^2 = E[E[XY|V]]^2$$
$$= E[E[X|V]E[Y|V]]^2 \longleftarrow \text{Markovity}$$
$$\le E[E[X|V]^2]\, E[E[Y|V]^2]$$
$$= (1-D_x)(1-D_y)$$

Two Bounds

- Rate-distortion function for quadratic Gaussian
- Cauchy-Schwartz
  - Orthogonality Principle

Two Bounds

- Rate-distortion function for quadratic Gaussian (maximum entropy)
- ~~Cauchy-Schwartz~~
  - Orthogonality Principle

Other Proof

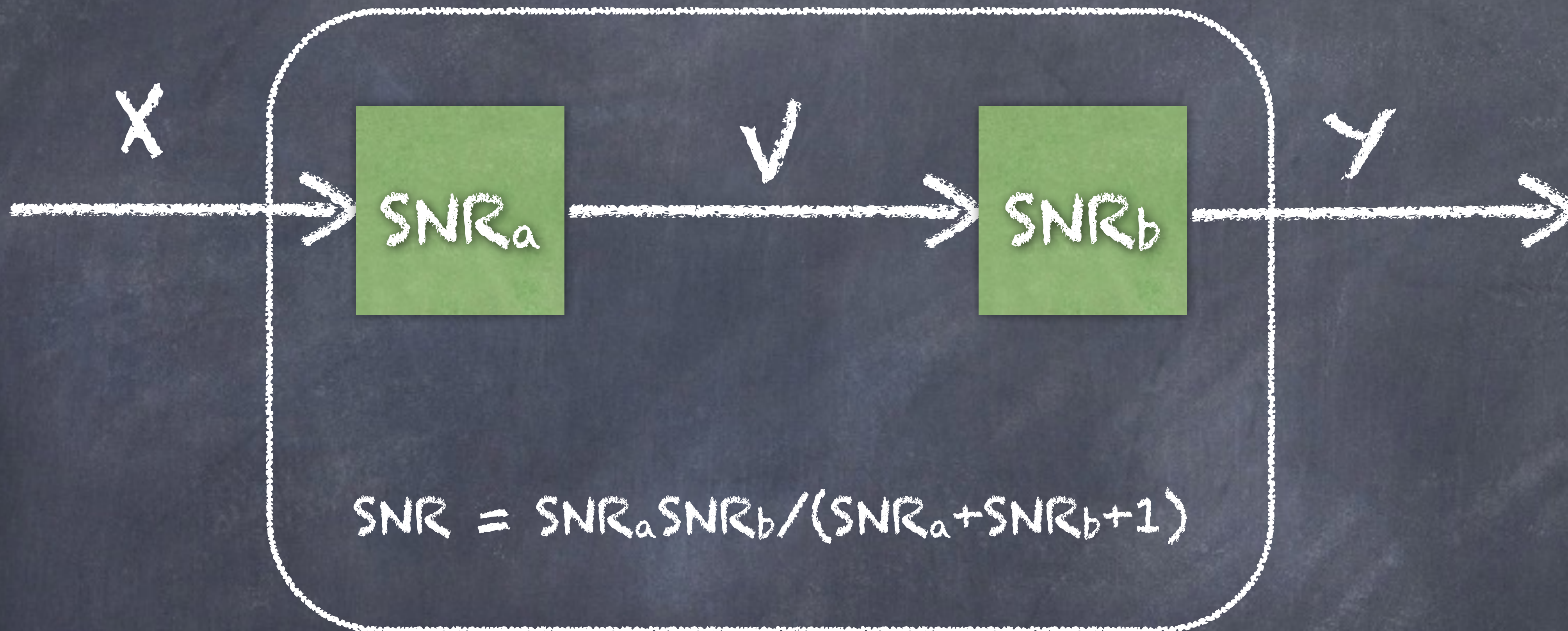
- Jun Chen:

Consider the four variables:
$X, E[X|V], E[Y|V], Y$

Construct Gaussian with same covariance:
X, V_a, V_b, Y

Properties Used:
- Maximum entropy
- Orthogonality Principle: $X-(V_a,V_b)-Y$

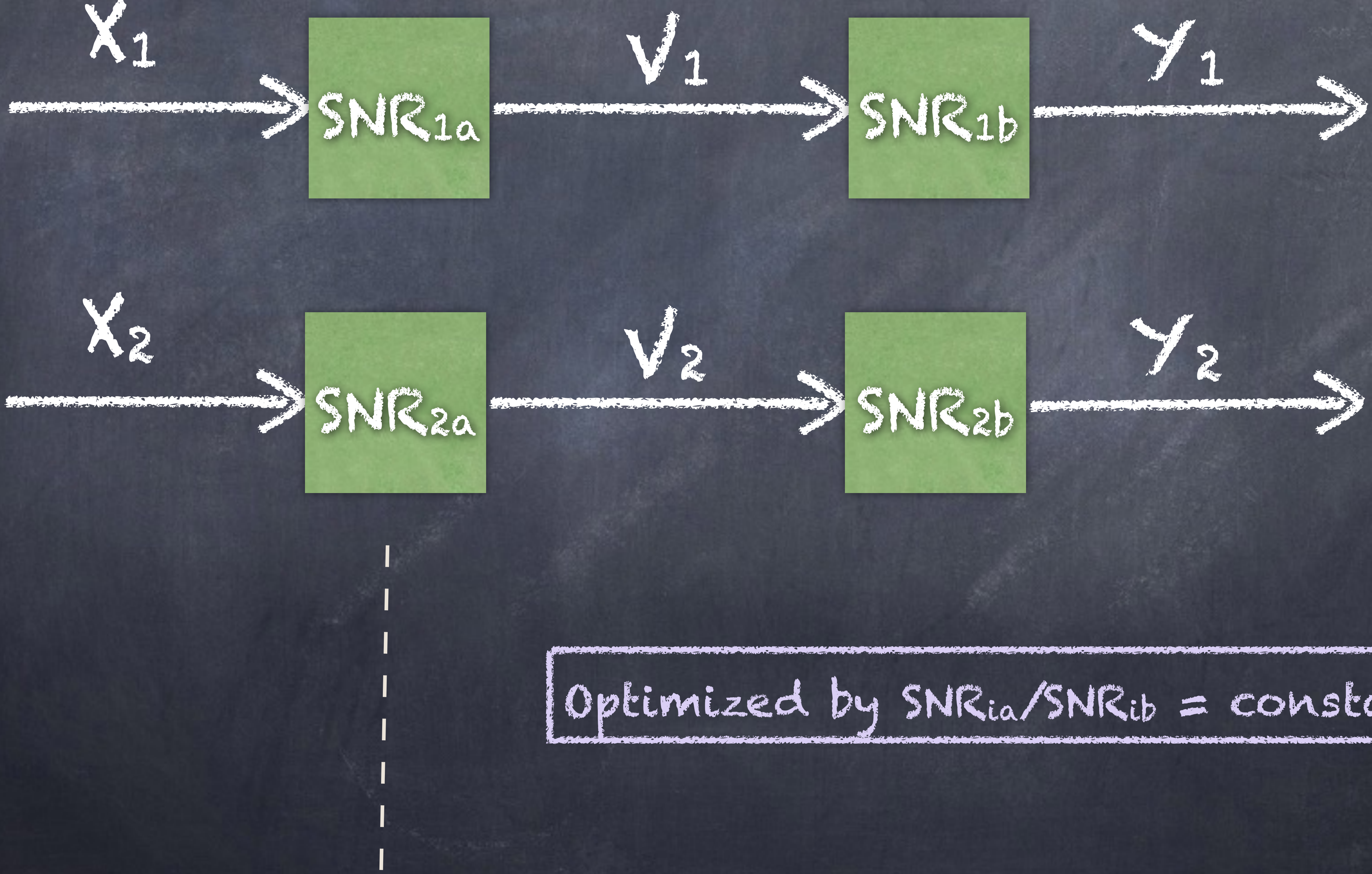
Tradeoff



$$I(X;V) = C(SNR_a)$$

$$I(X,Y;V) = C(SNR_a) + C(SNR/(SNR_a-SNR))$$

Vector Gaussian



Optimized by SNR_{ia}/SNR_{ib} = constant