Communication Requirements for Generating Correlated Random Variables

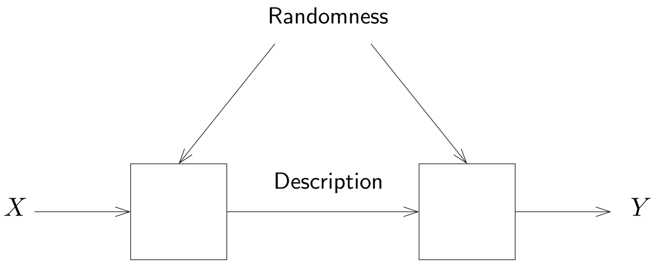
Paul Cuff

Stanford University

International Symposium on Information Theory
Toronto - July 9, 2008

Overview

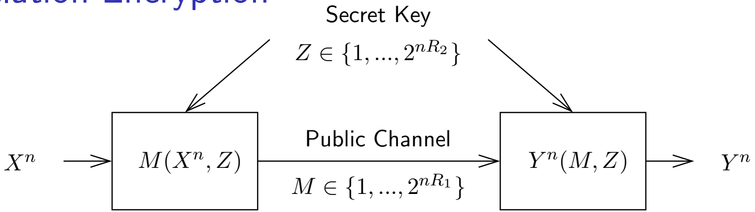
X is random and specified by nature.
How much must be told about X to generate Y correlated with X?
What is the effect of common randomness?



- Application:
  - Game theory — mixed strategies among participants on a team. [Anantharam, Borkar 07]

Talk Outline

Correlation Encryption

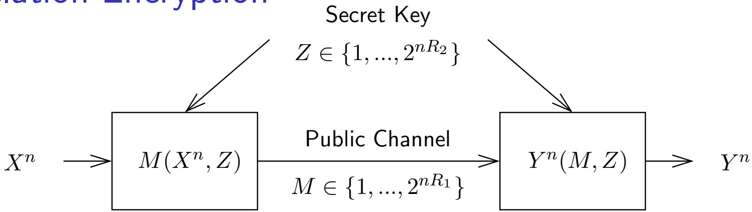


X is given by nature iid according to $p_0(x)$.

Goal:

1. Construct Y correlated with X according to $p_0(y|x)$.
2. Message doesn't give away anything about X and Y.

Correlation Encryption



Encoder: $p(m|x^n, z)$.
Decoder: $p(y^n|m, z)$.
Induced Distribution:

$$p(x^n, y^n, m, z) = p(x^n)p(z)p(m|x^n, z)p(y^n|m, z)$$

Achievable if there exists a sequence of encoders and decoders such that

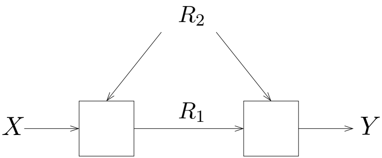
$$\lim_{n \to \infty} I(M; X^n, Y^n) = 0,$$

and

$$\lim_{n \to \infty} \left\| p(x^n, y^n) - \prod_{i=1}^{n} p_0(x_i) p_0(y_i|x_i) \right\|_{TV} = 0.$$

Correlation Encryption Rate Region

$$S_1 \triangleq Cl\{\text{ encryption achievable } (R_1, R_2)\}$$



Theorem: Encryption Rate Region

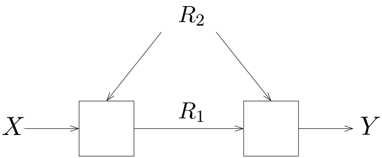
$S_1 = \{(R_1, R_2):$

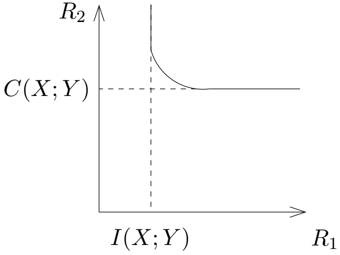
$$\begin{aligned} R_1 &\geq I(X;U), \\ R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Correlation Encryption Rate Region

$$S_1 \triangleq Cl\{ \text{ encryption achievable } (R_1, R_2)\}$$





Theorem: Encryption Rate Region

$S_1 = \{(R_1, R_2) :$

$$\begin{aligned} R_1 &\geq I(X;U), \\ R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Wyner's Common Information

[Wyner 75]:

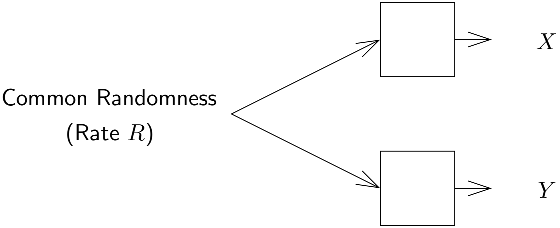
$$C(X;Y) \triangleq \min_{X-U-Y} I(X,Y;U).$$

Wyner's Common Information

[Wyner 75]:

$$C(X;Y) \triangleq \min_{X-U-Y} I(X,Y;U).$$

How much common randomness is needed to generate X and Y?

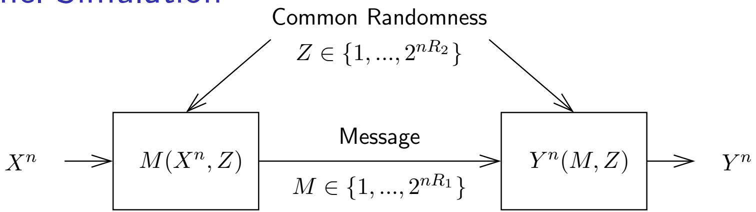


Result: $R > C(X;Y)$.

Talk Outline

1. Correlation Encryption
2. Channel Simulation
3. Proof
   - Achievability
   - Converse
4. Examples

Channel Simulation

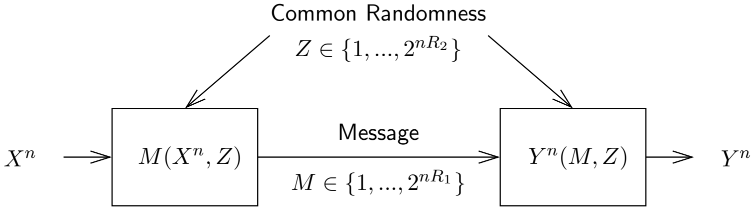


X is given by nature iid according to $p_0(x)$.

Goal:

1. Construct Y correlated with X according to $p_0(y|x)$.

Channel Simulation



Encoder: $p(m|x^n, z)$.
Decoder: $p(y^n|m, z)$.
Induced Distribution:

$$p(x^n, y^n, m, z) = p(x^n)p(z)p(m|x^n, z)p(y^n|m, z)$$

Achievable if there exists a sequence of encoders and decoders such that

$$\lim_{n\to\infty} \left|\left| p(x^n, y^n) - \prod_{i=1}^{n} p_0(x_i)p_0(y_i|x_i) \right|\right|_{TV} = 0.$$

Correlation Encryption — Channel Simulation

Difference between Correlation Encryption and Channel Simulation:

- One-time pad needed for Correlation Encryption

Theorem: Correlation Encryption relates to Channel Simulation

Define,

$$\begin{aligned} R_1' &= R_1, \\ R_2' &= R_1 + R_2. \end{aligned}$$

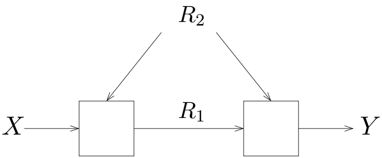
Then,

$$(R_1', R_2') \in S_1 \quad \Leftrightarrow \quad (R_1, R_2) \in S_2.$$

Reminder: S_1 is encryption rate region; S_2 is simulation rate region.

Channel Simulation Rate Region

$$S_2 \triangleq Cl\{\text{ simulation achievable } (R_1, R_2)\}$$



Theorem: Simulation Rate Region

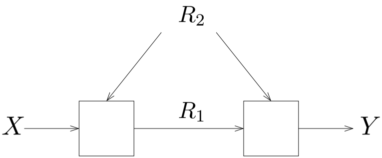
$S_2 = \{(R_1, R_2) :$

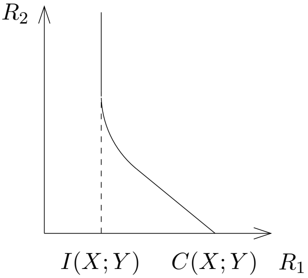
$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Channel Simulation Rate Region

$$S_2 \triangleq Cl\{\text{ simulation achievable } (R_1, R_2)\}$$





Theorem: Simulation Rate Region

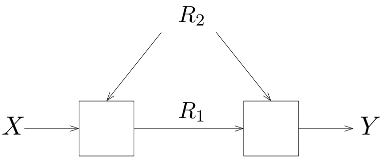
$S_2 = \{(R_1, R_2)$:

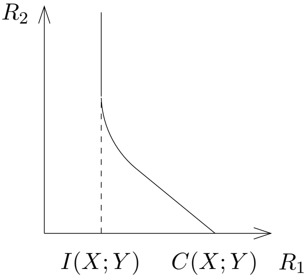
$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Channel Simulation Rate Region

$$S_2 \triangleq Cl\{\text{ simulation achievable } (R_1, R_2)\}$$





Theorem: Simulation Rate Region

$S_2 = \{(R_1, R_2)$:

$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Previous Results:

[Bennett et al. 02]: Reverse Shannon Th.:

$$(I(X;Y), \infty) \in S_2.$$

[Wyner 75]: $(C(X;Y), 0) \in S_2$.

Talk Outline

Achievability via Random Coding

Let (R_1, R_2) satisfy

$$\begin{aligned} R_1 &> I(X;U), \\ R_1 + R_2 &> I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ form a Markov chain.

Achievability via Random Coding

Let (R_1, R_2) satisfy

$$\begin{aligned} R_1 &> I(X;U), \\ R_1 + R_2 &> I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ form a Markov chain.

Construct Codebook randomly:

$\mathcal{C} = \{U^n(m)\}_{m=1}^{2^{n(R_1+R_2)}}$ where $U^n(m) \sim \prod_{i=1}^n p(u_i)$.

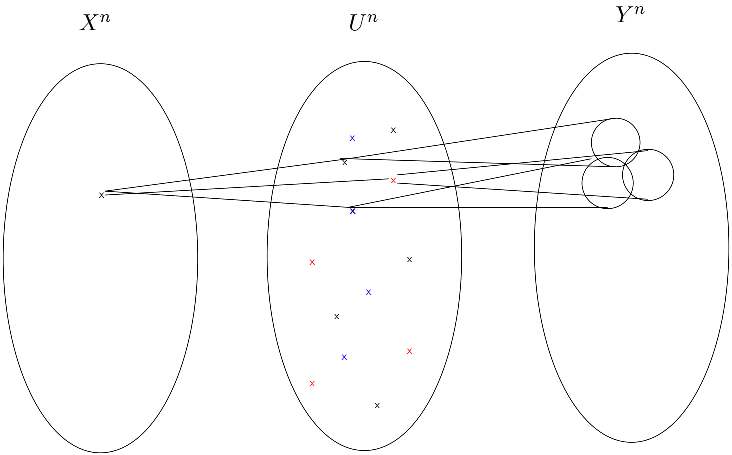
Binning: Bin the codewords into 2^{nR_2} bins.

Common randomness specifies the bin.

Encoder: Finds all jointly typical U^n in bin and randomly chooses one. Sends index.

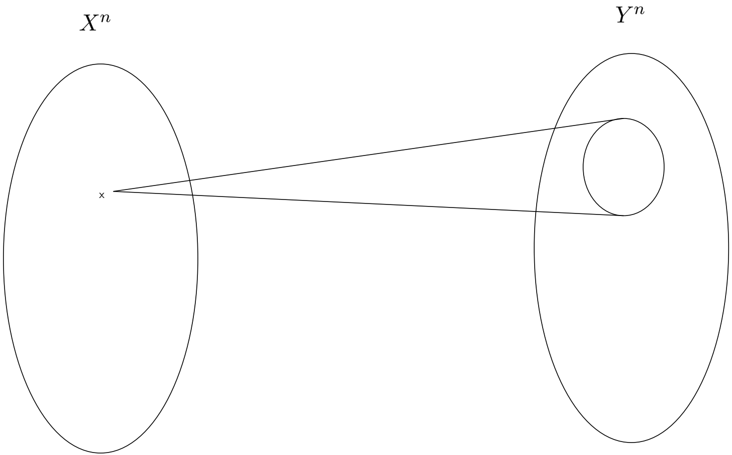
Decoder: Decodes $U^n(m)$ and generates Y^n according to $\prod_{i=1}^n p(y_i|u_i(m))$.

Achievability



Resolvability: [Wyner 75] [Han, Verdú 93]

Achievability



Resolvability: [Wyner 75] [Han, Verdú 93]

Talk Outline

Converse

Assume (R_1, R_2) is achievable.

Converse

Assume (R_1, R_2) is achievable.

Markovity by construction:

$$p(x^n, y^n, m, z) = p(x^n)p(z)p(m|x^n, z)p(y^n|m, z).$$

Therefore,

$$X^n - (M, Z) - Y^n,$$
$$X^n \perp Z.$$

Converse

Assume (R_1, R_2) is achievable.

$$X^n - (M, Z) - Y^n,$$
$$X^n \perp Z.$$

Converse

Assume (R_1, R_2) is achievable.

$$X^n - (M, Z) - Y^n,$$
$$X^n \perp Z.$$

$$\begin{aligned} n(R_1 + R_2) &\geq H(M, Z) \\ &\geq I(X^n, Y^n; M, Z) \end{aligned}$$

$$\begin{aligned} nR_1 &\geq H(M) \\ &\geq H(M|Z) \\ &\geq I(X^n; M|Z) \\ &= I(X^n; M, Z) \end{aligned}$$

Converse

Assume (R_1, R_2) is achievable.

$$X^n - (M, Z) - Y^n,$$
$$X^n \perp Z.$$

$$\begin{aligned} n(R_1 + R_2) &\geq H(M, Z) \\ &\geq I(X^n, Y^n; M, Z) \\ &\quad \text{(sequence of lemmas)} \\ &\quad \vdots \\ &\geq \approx \sum_{i=1}^{n} I(X_i, Y_i; M, Z) \\ &\approx nI(X_Q, Y_Q; M, Z, Q). \end{aligned}$$

where $Q \sim Unif(\{1, ..., n\})$.

$$\begin{aligned} nR_1 &\geq H(M) \\ &\geq H(M|Z) \\ &\geq I(X^n; M|Z) \\ &= I(X^n; M, Z) \\ &\quad \vdots \\ &\geq \approx \sum_{i=1}^{n} I(X_i; M, Z) \\ &\approx nI(X_Q; M, Z, Q). \end{aligned}$$

Converse

Assume (R_1, R_2) is achievable.

$$X^n - (M, Z) - Y^n,$$
$$X^n \perp Z.$$

$$\begin{aligned} R_1 &\geq \approx I(X_Q; M, Z, Q), \\ R_1 + R_2 &\geq \approx I(X_Q, Y_Q; M, Z, Q). \end{aligned}$$

where $Q \sim Unif(\{1, ..., n\})$.

Converse

Assume (R_1, R_2) is achievable.

$$X^n - (M, Z) - Y^n,$$
$$X^n \perp Z.$$

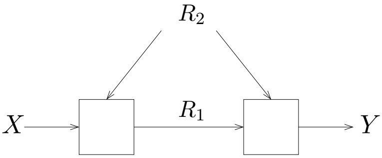
$$\begin{aligned} R_1 &\geq \approx I(X_Q; M, Z, Q), \\ R_1 + R_2 &\geq \approx I(X_Q, Y_Q; M, Z, Q). \end{aligned}$$

where $Q \sim Unif(\{1, ..., n\})$.

Label (M, Z, Q) as U.

Talk Outline

Simulation Rate Region Examples



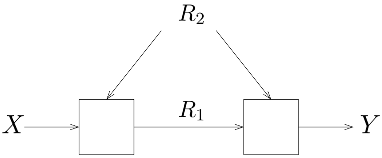
Simulation Rate Region

$S_2 = \{(R_1, R_2) :$

$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Simulation Rate Region Examples



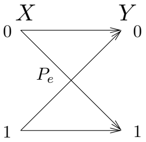
Simulation Rate Region

$S_2 = \{(R_1, R_2) :$

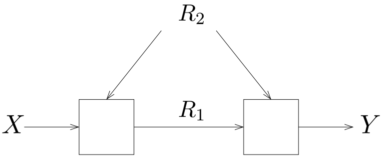
$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Binary Symmetric Channel ($X \sim Bern(\frac{1}{2})$):



Simulation Rate Region Examples



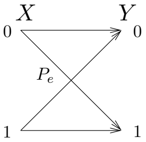
Simulation Rate Region

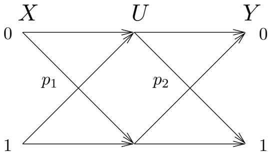
$S_2 = \{(R_1, R_2) :$

$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

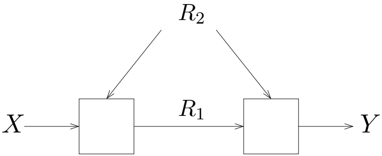
Binary Symmetric Channel ($X \sim Bern(\frac{1}{2})$):





$p_1(1 - p_2) + p_2(1 - p_1) = P_e$,
$p_1 \leq p_2 \leq P_e$.

Simulation Rate Region Examples



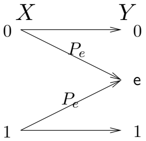
Simulation Rate Region

$S_2 = \{(R_1, R_2)$:

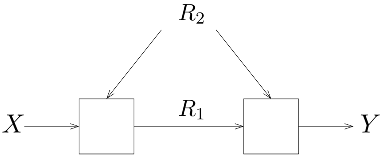
$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Binary Erasure Channel ($X \sim Bern(\frac{1}{2})$):



Simulation Rate Region Examples



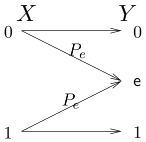
Simulation Rate Region

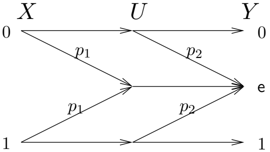
$S_2 = \{(R_1, R_2):$

$$\begin{aligned} R_1 &\geq I(X;U), \\ R_1 + R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

Binary Erasure Channel ($X \sim Bern(\frac{1}{2})$):





$(1 - p_1)(1 - p_2) = 1 - P_e,$
$0 \leq p_2 \leq \min\{P_e, 1/2\}.$

Example: Binary Erasure Channel

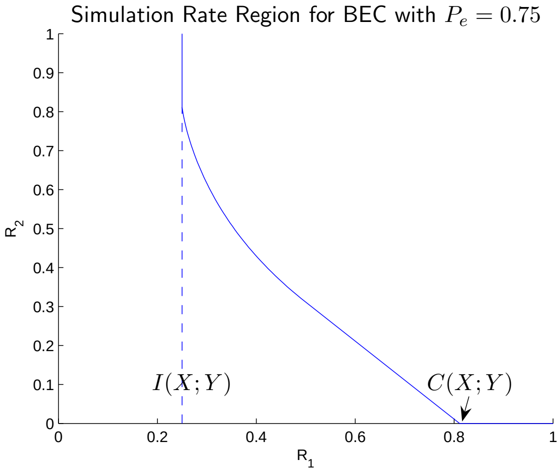
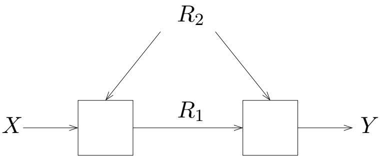


Figure: Boundary of the simulation rate region for a binary erasure channel with erasure probability $P_e = 0.75$ and a Bernoulli-half input.

Summary

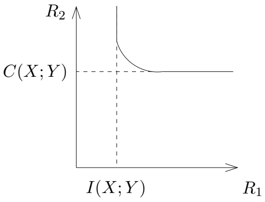


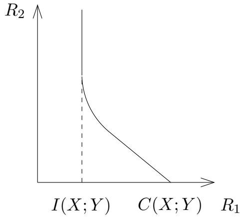
1. Correlation Encryption (Public Channel)

$$\begin{aligned} R_1 &\geq I(X;U), \\ R_2 &\geq I(X,Y;U), \end{aligned}$$

for some U such that $X - U - Y$ and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1$.

2. Fundamental quantities discovered as extreme points





Erasure Challenge

Person A

0 1 0 0 1 1 1 1

Erasure Challenge

Person A	Person B
0 1 0 0 1 1 1 1	0 e e e e 1 e e

Erasure Challenge

Person A	Person B
0 1 0 0 1 1 1 1	0 e e e e 1 e e

How much must Person A tell Person B?

Erasure Challenge

Person A								Person B							
0	1	0	0	1	1	1	1	0	e	e	e	e	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits

Erasure Challenge

Person A	Person B
0 1 0 0 1 1 1 1	0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits

Erasure Challenge

Person A	Person B
0 1 0 0 1 1 1 1	0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits

Erasure Challenge

Person A	Person B
0 1 | 0 0 | 1 1 | 1 1	0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A

0 1	0 0	1 1	1 1

Person B

0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A							
0	1	0	0	1	1	1	1

Person B							
0	1	e	e	1	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A			
0 1	0 0	1 1	1 1

Person B			
0 e	e e	e 1	e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A							
0	1	0	0	1	1	1	1

Person B							
0	e	e	e	e	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization
  $\log_2 \binom{4}{2} + 4$ bits

Erasure Challenge

Person A

0	1	0	0	1	1	1	1

Person B

0	e	e	e	e	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization
  $\log_2 \binom{4}{2} + 4$ bits $= \log_2 96 = 6.58$ bits