A New Upper Bound On “Private Common Information”

Amin Aminzadeh Gohari

Presenting joint work with Venkat Anantharam

Private Common Information of correlated random variables

- Given correlated random variables (X, Y, Z), how can one quantify (in some operational sense) the common part of X and Y that is independent of Z?

Private Common Information of correlated random variables

- Given correlated random variables (X, Y, Z), how can one quantify (in some operational sense) the common part of X and Y that is independent of Z?

- Special cases:

  - If Z is independent of (X, Y) $\longrightarrow$ $I(X; Y)$

Private Common Information of correlated random variables

- Given correlated random variables (X, Y, Z), how can one quantify (in some operational sense) the common part of X and Y that is independent of Z?

- Special cases:

  - If Z is independent of $(X, Y) \longrightarrow I(X; Y)$
  - If $X = Y = K \longrightarrow H(K|Z)$.

Private Common Information of correlated random variables

- Given correlated random variables (X, Y, Z), how can one quantify (in some operational sense) the common part of X and Y that is independent of Z?

- Special cases:

  - If Z is independent of $(X, Y) \longrightarrow I(X; Y)$
  - If $X = Y = K \longrightarrow H(K|Z)$.

- What about $I(X; Y|Z)$?

Private Common Information of correlated random variables

- Given correlated random variables (X, Y, Z), how can one quantify (in some operational sense) the common part of X and Y that is independent of Z?
- What about $I(X; Y|Z)$?
  - But $I(X; Y|Z)$ can be positive when X and Y don't have anything in common.

Private Common Information of correlated random variables

- Given correlated random variables (X, Y, Z), how can one quantify (in some operational sense) the common part of X and Y that is independent of Z?

- What about $I(X;Y|Z)$?

  - But $I(X;Y|Z)$ can be positive when X and Y don't have anything in common.

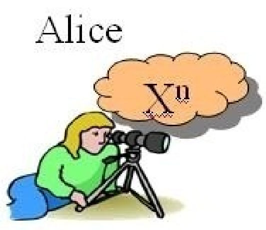
$$X \sim B(\frac{1}{2}), \;\; Y \sim B(\frac{1}{2}), \;\; X \perp Y, \;\; Z = X \oplus Y$$

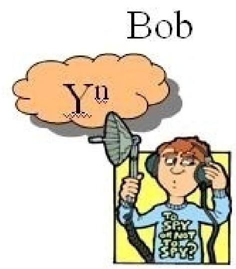
$$I(X;Y) = 0 \;\; < \;\; I(X;Y|Z) = 1$$

Outline

- Common Information
- One notion of "Common Private Information" of correlated random variables
  - Upper bounds
  - Our proof technique
- Conclusions

Notions of Common Information:
Gacs-Korner common information



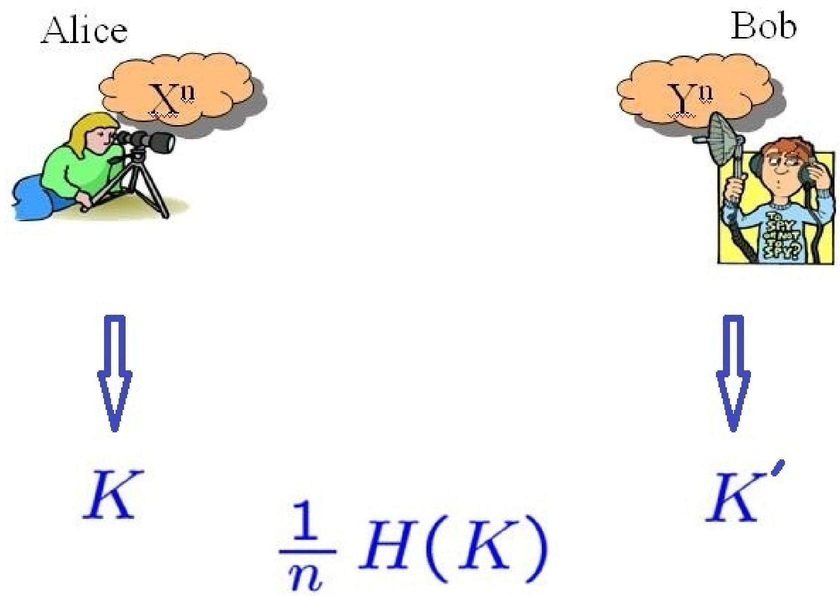


- Common randomness that can be extracted by knowing X and Y separately

Notions of Common Information:
Gacs-Korner common information

- Common randomness that can be extracted by knowing X and Y separately

Notions of Common Information:
Gacs-Korner common information



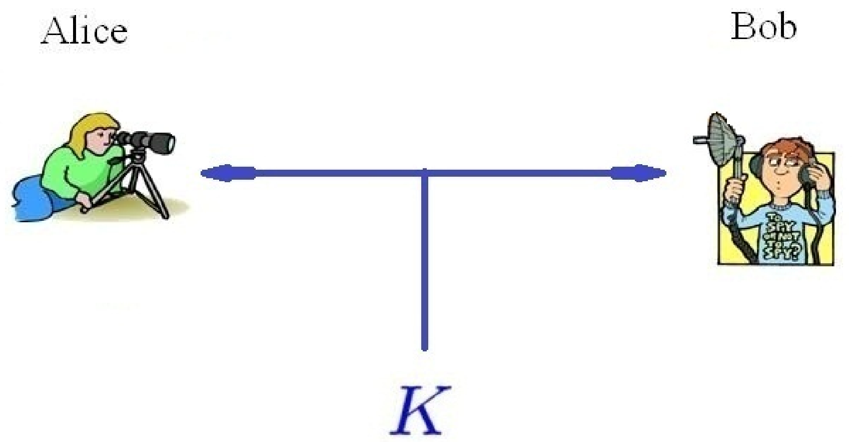
- Common randomness that can be extracted by knowing X and Y separately

  max $H(K)$ over K : $H(K|X) = H(K|Y) = 0$

Notions of Common Information: Wyner's common information

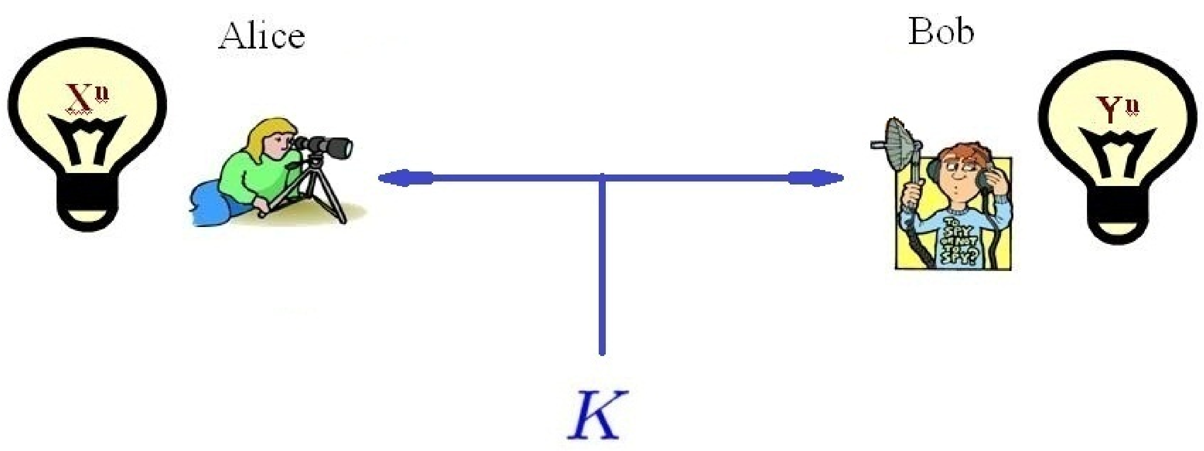
- Amount of common randomness that should be provided to generate X and Y separately

Notions of Common Information: Wyner's common information



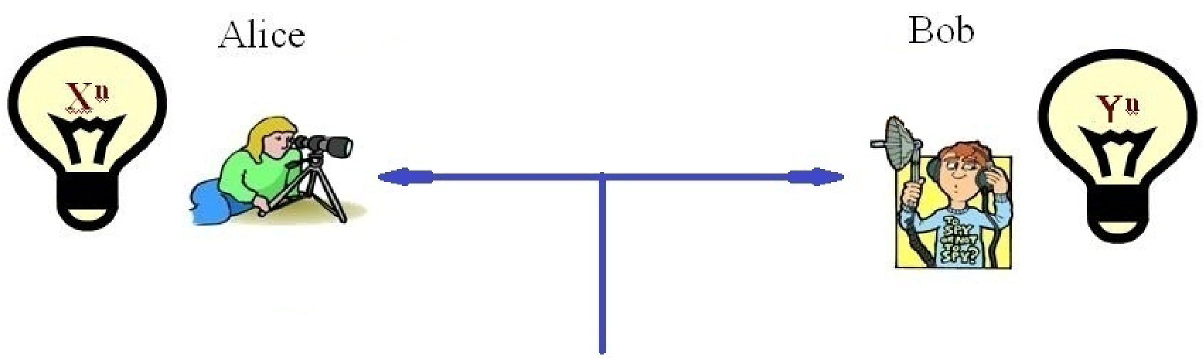
- Amount of common randomness that should be provided to generate X and Y separately

Notions of Common Information:
Wyner's common information



- Amount of common randomness that should be provided to generate X and Y separately

Notions of Common Information:
Wyner's common information



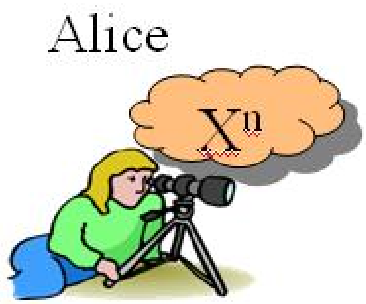
$$K$$

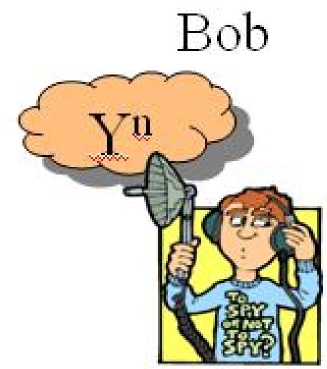
$$\frac{1}{n} H(K)$$

- Amount of common randomness that should be provided to generate X and Y separately

  min $I(K; XY)$ over $K : \; X - K - Y$

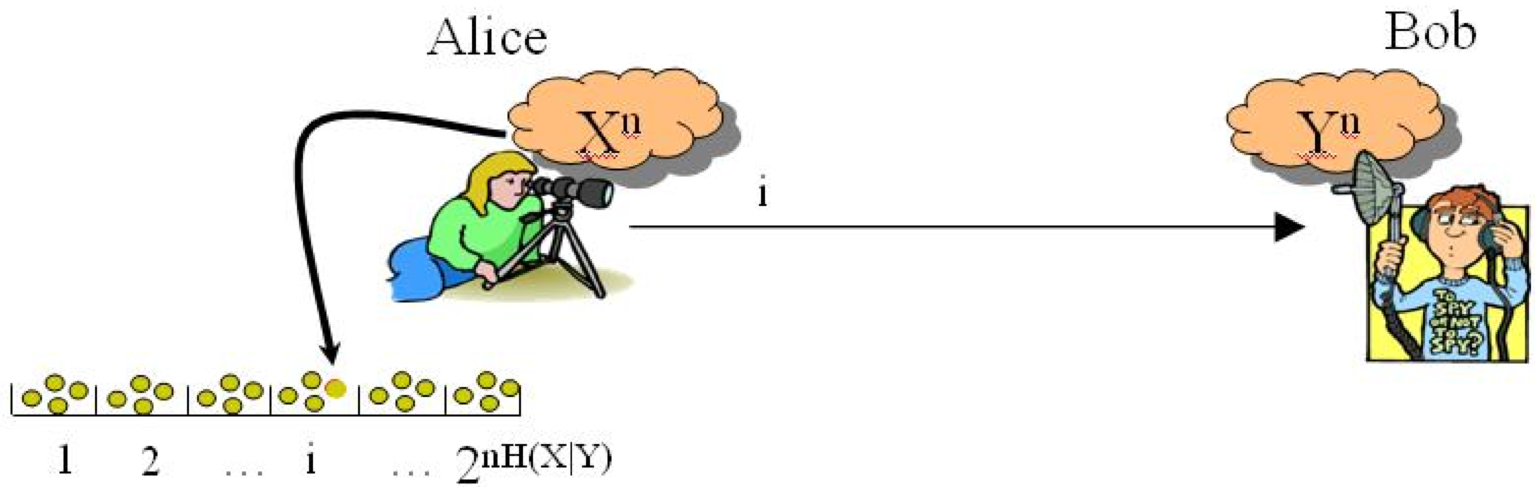
Notions of Common Information:
Shannon's mutual information





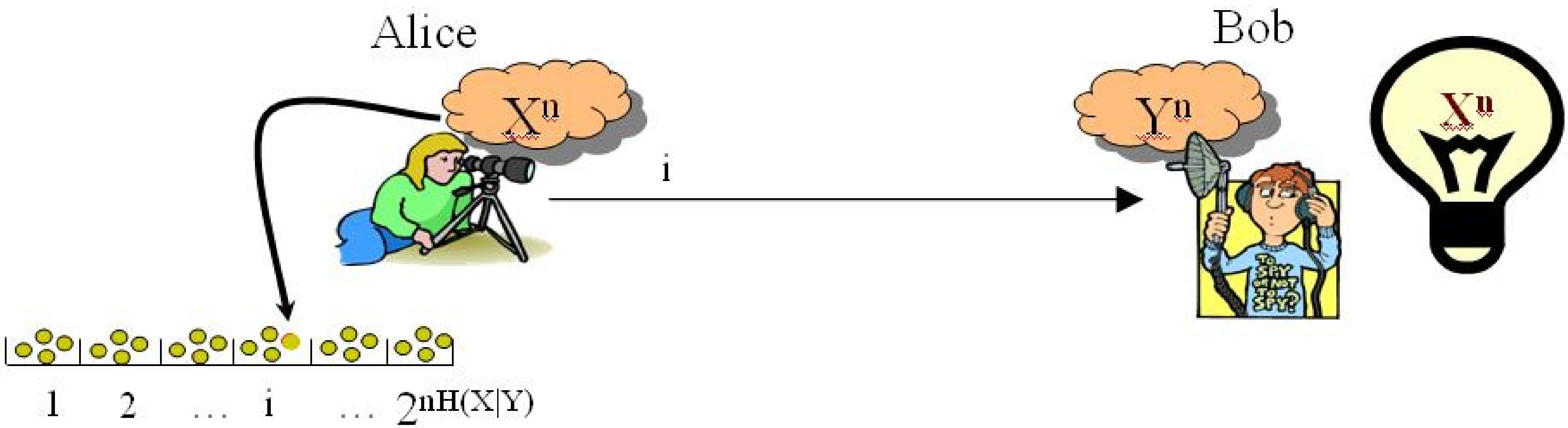
- Amount of common randomness that can be "extracted" following communication

Notions of Common Information: Shannon's mutual information



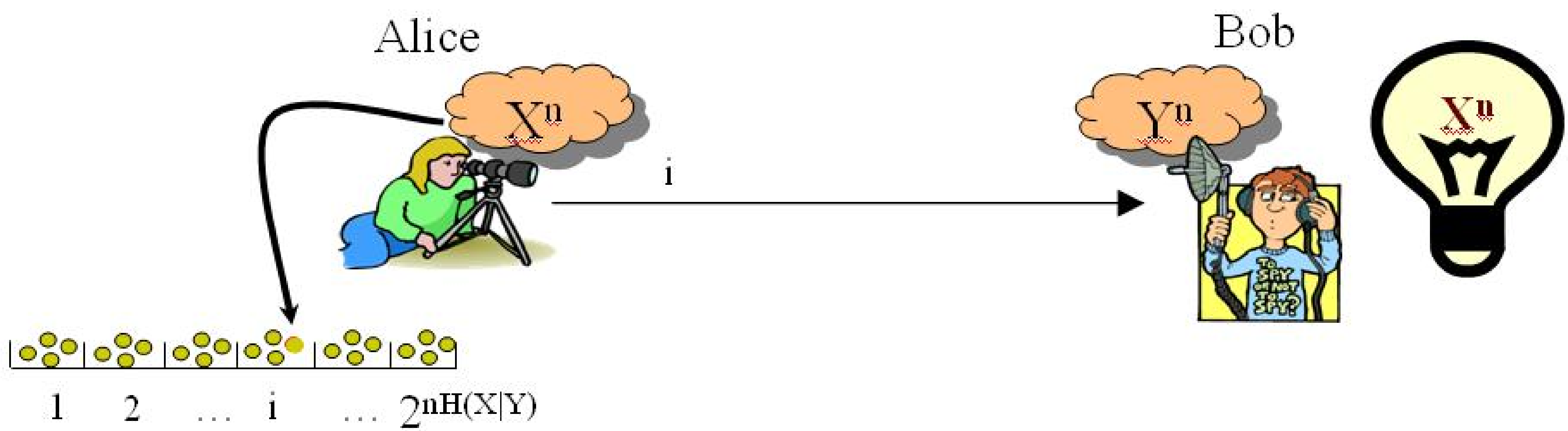
- Amount of common randomness that can be "extracted" following communication

Notions of Common Information: Shannon's mutual information



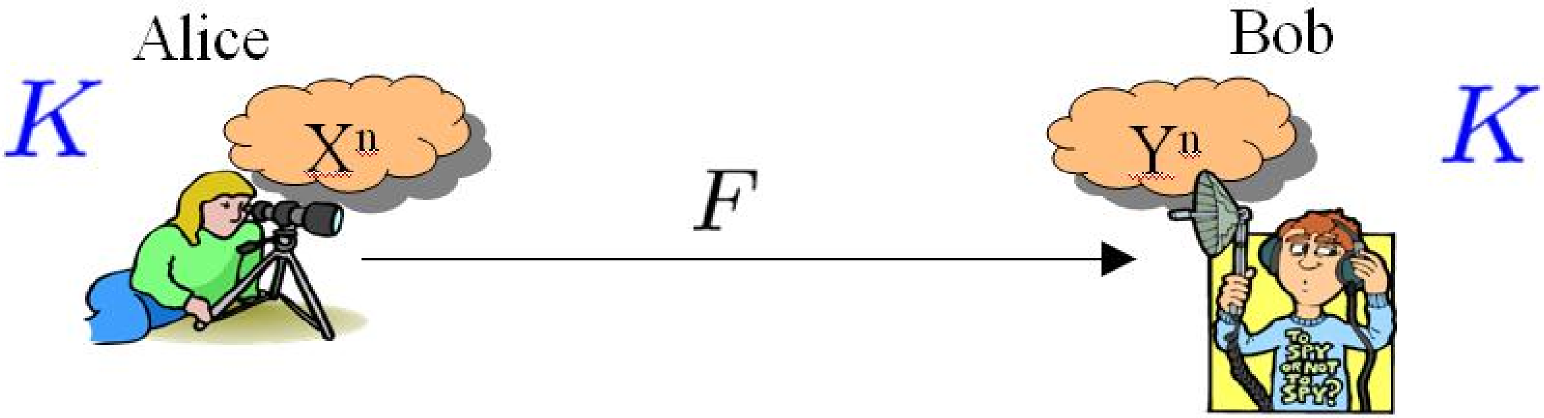
- Amount of common randomness that can be "extracted" following communication

Notions of Common Information:
Shannon's mutual information



Total Common Information		Common Information due to communication		Extracted Common Inf.
X^n		F		K
$H(X^n)$	=	$H(X^n \vert Y^n)$	+	$I(X^n;Y^n)$
		Bin Index		Index within the bin

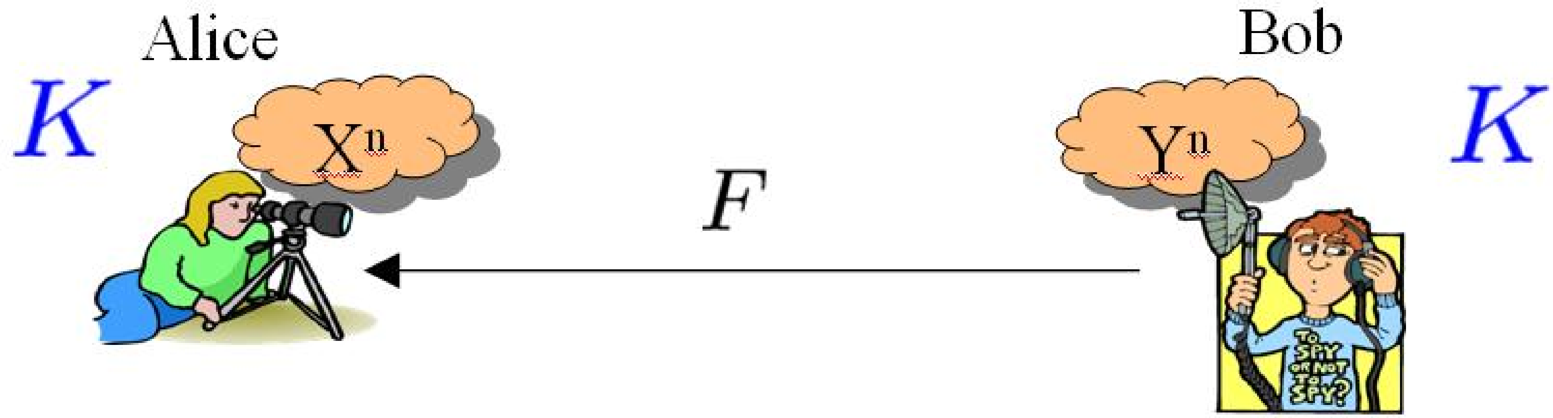
Notions of Common Information:
Shannon's mutual information



$$I(K; F) \cong 0$$

$$\frac{1}{n}H(K)$$

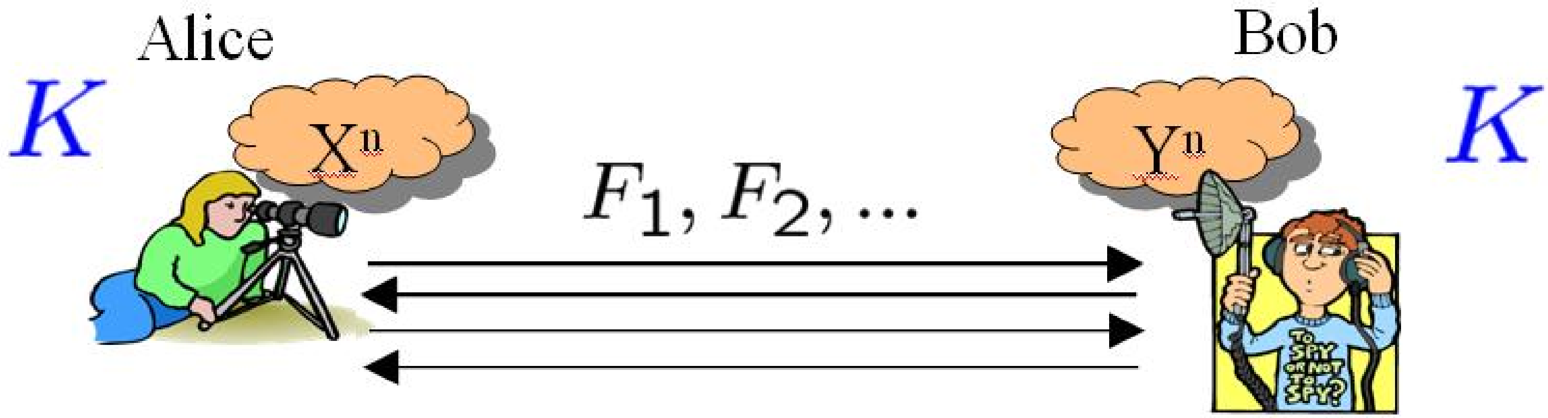
Notions of Common Information:
Shannon's mutual information



$$I(K;F) \cong 0$$

$$\frac{1}{n}H(K)$$

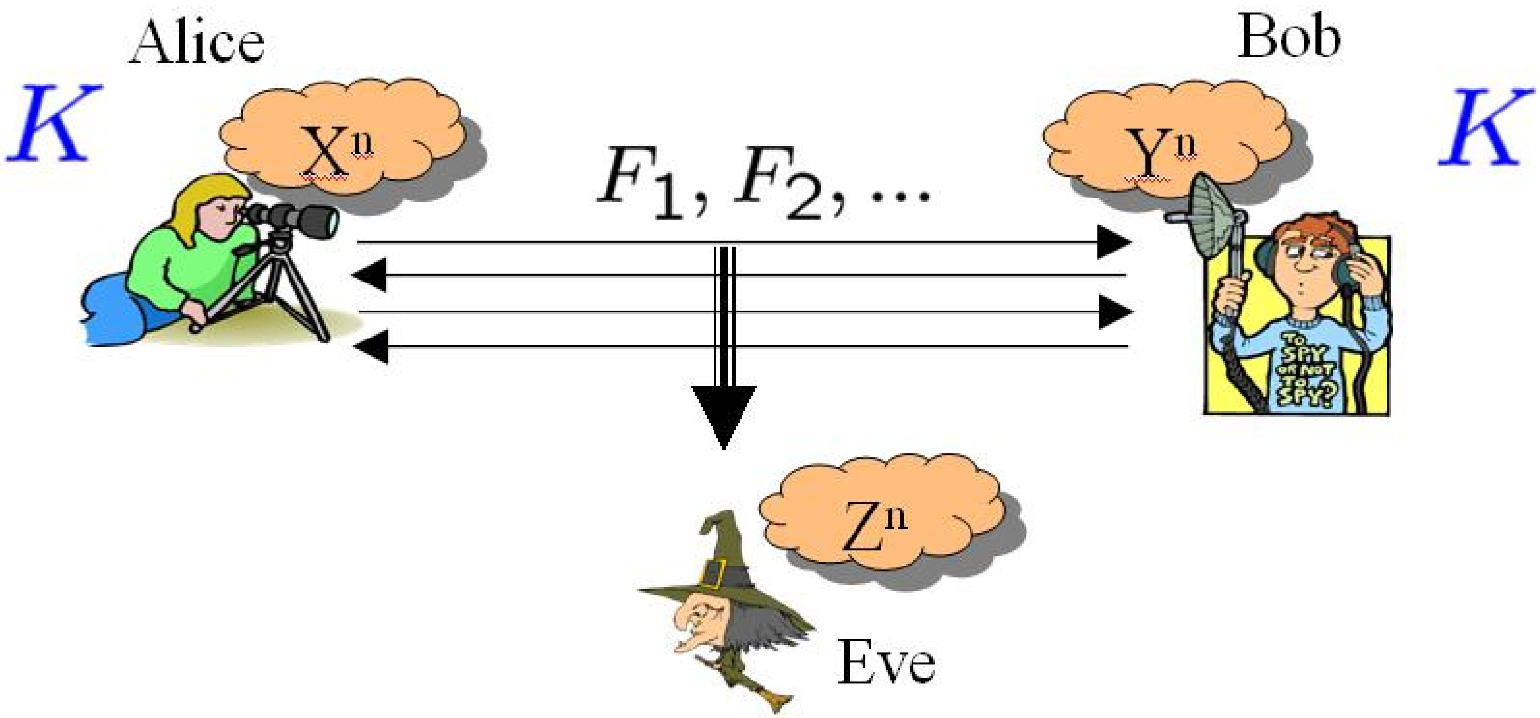
Notions of Common Information: Shannon's mutual information



$$I(K; \overrightarrow{F}) \cong 0$$

$$\frac{1}{n} H(K)$$

Extension to "Common Private Information"



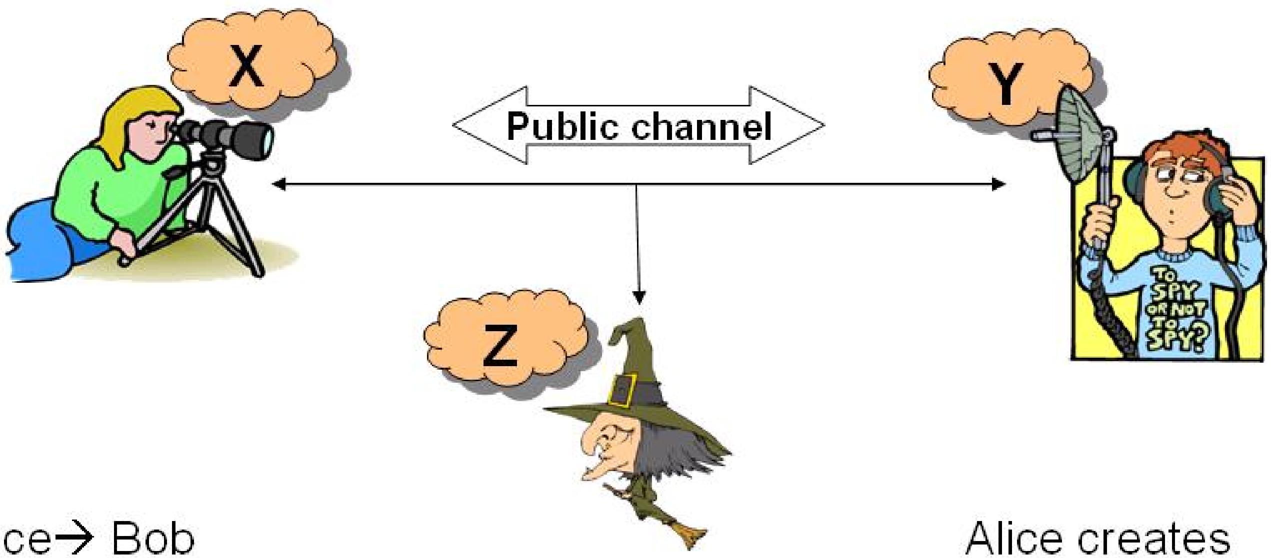
$$I(K; \overrightarrow{F} Z^n) \cong 0,$$

$$\frac{1}{n} H(K)$$

Outline

- Common Information
- One notion of "Common Private Information" of correlated random variables
  - Upper bounds
  - Our proof technique
- Conclusions

Definition of $S(X;Y\|Z)$



Alice → Bob

$F_1(X^{1:n})$

Bob → Alice

$F_2(Y^{1:n}, F_1)$

Alice → Bob

$F_3(X^{1:n}, F_1, F_2)$

....

Alice creates

$K_A(X^{1:n}, \mathbf{F})$

Bob creates

$K_B(Y^{1:n}, \mathbf{F})$

Requirements:

$P(K_A=K_B=K)>1-\varepsilon$

$\frac{1}{n} I(K ; Z^{1:n}, \mathbf{F}) \leq \varepsilon$

Secret key rate

$S(X;Y\|Z)$

Example I

$$X \sim B(\frac{1}{2}), \;\; Y \sim B(\frac{1}{2}), \;\; X \perp Y, \;\; Z = X \bigoplus Y$$

$$I(X;Y) = 0 \;\; < \;\; I(X;Y|Z) = 1$$

Example I

$$X \sim B(\frac{1}{2}),\ \ Y \sim B(\frac{1}{2}),\ \ X \perp Y,\ \ Z = X \bigoplus Y$$

$$I(X;Y) = 0 \ \ < \ \ I(X;Y|Z) = 1$$

- $S(X;Y\|Z) = 0$ because $X^n - \mathbf{F} - Y^n$ forms a Markov chain.

Example I

$$X \sim B(\frac{1}{2}),\ \ Y \sim B(\frac{1}{2}),\ \ X \perp Y,\ \ Z = X \oplus Y$$

$$I(X;Y) = 0 \ \ < \ \ I(X;Y|Z) = 1$$

- $S(X;Y\|Z) = 0$ because $X^n - \mathbf{F} - Y^n$ forms a Markov chain.
- In general $S(X;Y\|Z) \leq \min(I(X;Y), I(X;Y|Z))$.

Example I

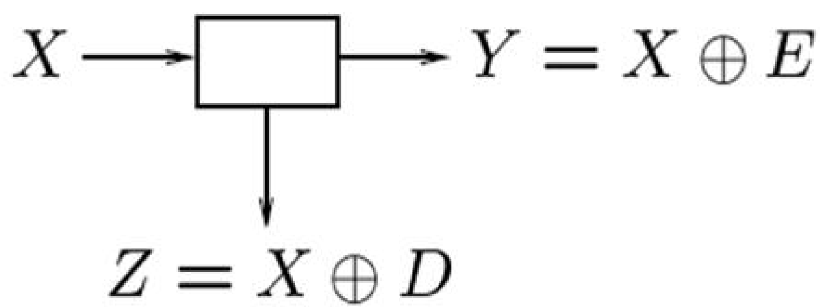
$$X \sim B(\frac{1}{2}),\ \ Y \sim B(\frac{1}{2}),\ \ X \perp Y,\ \ Z = X \oplus Y$$

$$I(X;Y) = 0 \ \ < \ \ I(X;Y|Z) = 1$$

- $S(X;Y\|Z) = 0$ because $X^n - \mathbf{F} - Y^n$ forms a Markov chain.
- In general $S(X;Y\|Z) \leq \min(I(X;Y), I(X;Y|Z))$.
- $I(X;Y)$ = Private Common part of X and Y+Non-private common part of X and Y.
- $I(X;Y|Z)$ = Private Common part of X and Y+Artificial correlation induced between X and Y through conditioning.

Example II

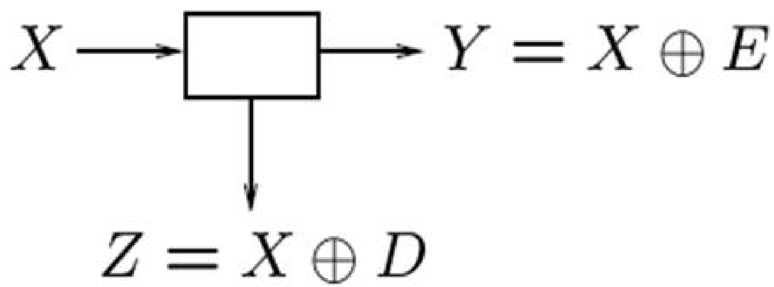
$$E \sim B(\epsilon), D \sim B(\delta), \epsilon < \delta < 0.5$$



Example II

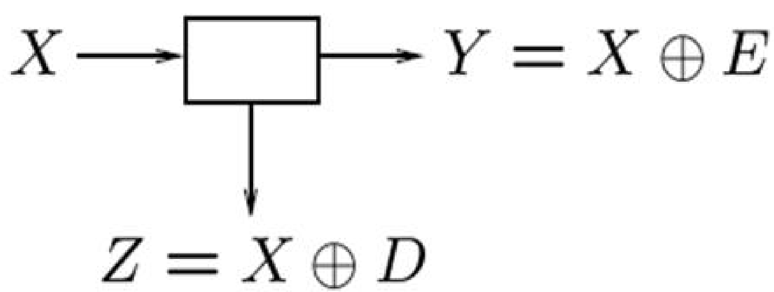
$$E \sim B(\epsilon), D \sim B(\delta), \epsilon < \delta < 0.5$$

$$I(X;Y) > I(X;Z)$$



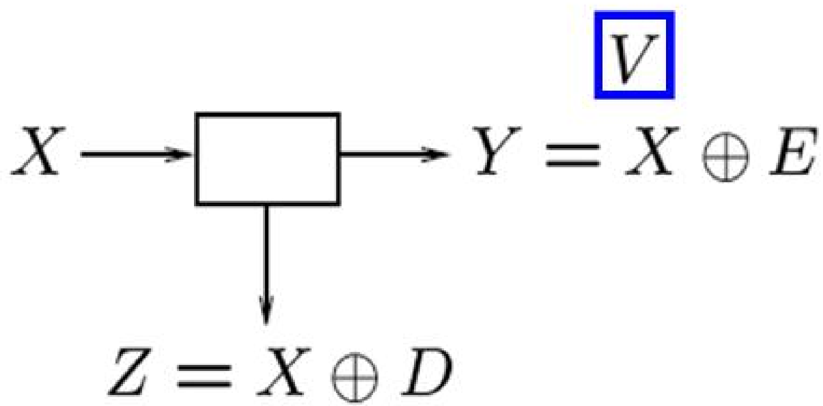
Example III

$$E \sim B(\epsilon), D \sim B(\delta), \delta < \epsilon < 0.5$$



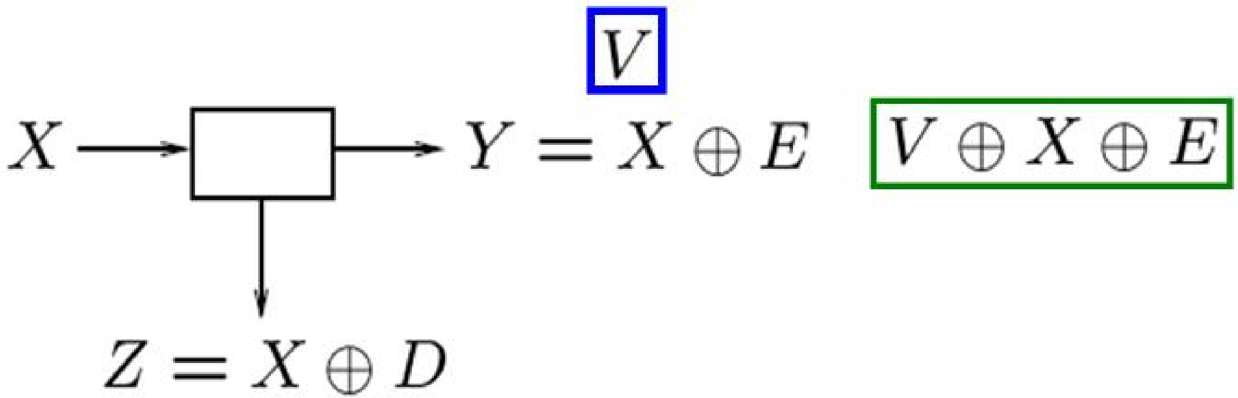
Example III

$$E \sim B(\epsilon), D \sim B(\delta), \delta < \epsilon < 0.5$$



Example III

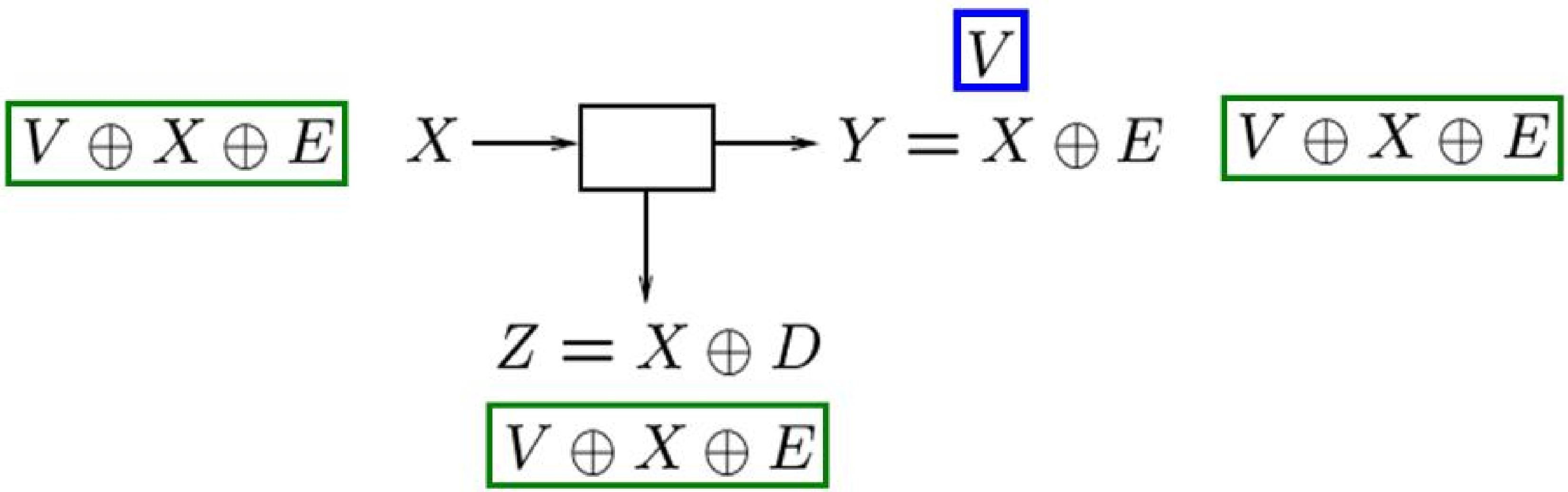
$$E \sim B(\epsilon), D \sim B(\delta), \delta < \epsilon < 0.5$$



Example III

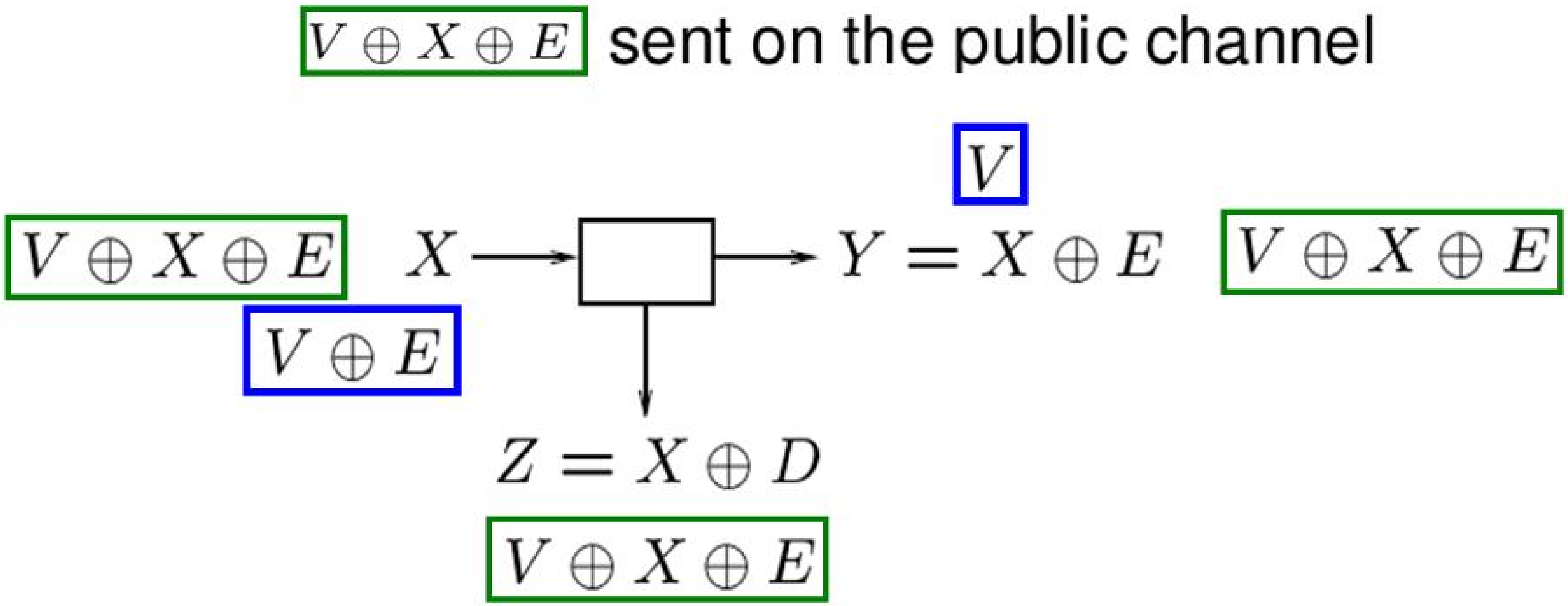
$$E \sim B(\epsilon), D \sim B(\delta), \delta < \epsilon < 0.5$$

$V \oplus X \oplus E$ sent on the public channel



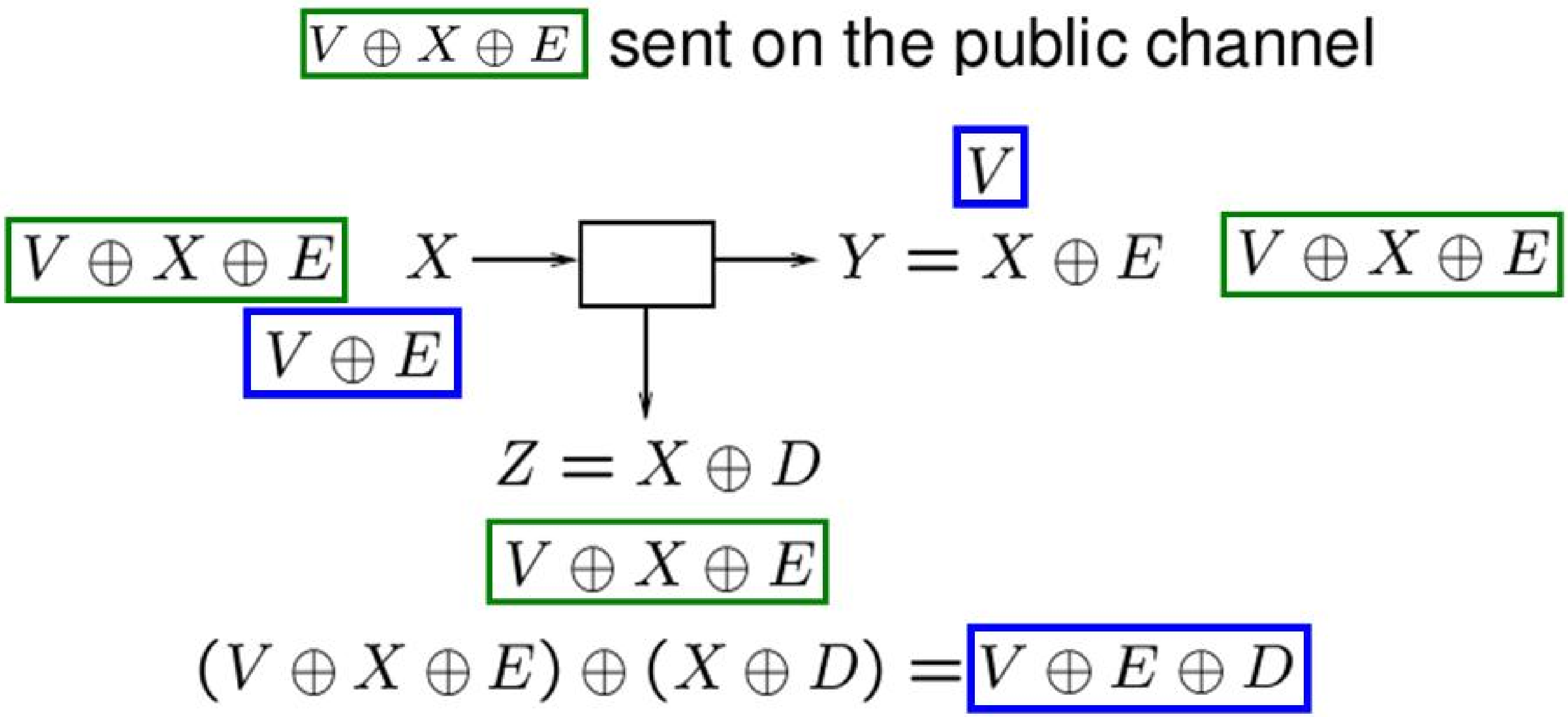
Example III

$$E \sim B(\epsilon), D \sim B(\delta), \delta < \epsilon < 0.5$$



Example III

$$E \sim B(\epsilon), D \sim B(\delta), \delta < \epsilon < 0.5$$



Outline

- Common Information
- One notion of "Common Private Information" of correlated random variables
  - Upper bounds
  - Our proof technique
- Conclusions

Upper bounds on $S(X;Y\|Z)$

Authors	Upper bounds on $S(X;Y\|Z)$
Maurer (1993)	$\min(I(X;Y), I(X;Y\|Z))$ Idea: classical arguments, e.g. $H(K_A) = nI(X;Y\|Z) - H(K_A\|K_B) - I(K_A;FZ^n)$ $H(K_A) = nI(X;Y) - H(K_A\|K_B) - I(K_A;F)$

Upper bounds on $S(X;Y\|Z)$

Authors	Upper bounds on $S(X;Y\|Z)$
Maurer (1993)	$\min(I(X;Y), I(X;Y\|Z))$
Maurer and Wolf (1999)	$I(X;Y\downarrow Z) := \inf_{XY-Z-J}(I(X;Y\|J))$ Idea: decreasing the information of Eve can not decrease the common private information

Upper bounds on $S(X;Y\|Z)$

Authors	Upper bounds on $S(X;Y\|Z)$
Maurer (1993)	$\min(I(X;Y), I(X;Y\|Z))$
Maurer and Wolf (1999)	$I(X;Y\downarrow Z) := \inf_{XY-Z-J}(I(X;Y\|J))$ Idea: decreasing the information of Eve can not decrease the common private information
Renner and Wolf (2003)	$\inf_U(H(U) + I(X;Y\downarrow ZU))$ Idea: providing Eve with a random variable U can not decrease the common private information by more than $H(U)$ bits.

Upper bounds on $S(X;Y\|Z)$

Authors	Upper bounds on $S(X;Y\|Z)$
Maurer (1993)	$\min(I(X;Y), I(X;Y\|Z))$
Maurer and Wolf (1999)	$I(X;Y\downarrow Z) := \inf_{XY-Z-J}(I(X;Y\|J))$ Idea: decreasing the information of Eve can not decrease the common private information
Renner and Wolf (2003)	$\inf_U(H(U)+I(X;Y\downarrow ZU))$ Idea: providing Eve with a random variable U can not decrease the common private information by more than $H(U)$ bits.
One of our results	$\inf_J I(XY;J\|Z)+I(X;Y\|J)$ Idea: Adding an imaginary receiver.

- $S(X;Y\|Z) \leq \inf_J S(X;Y;J^{(s)}\|Z) + S(X;Y\|J)$

Outline

- Common Information
- One notion of "Common Private Information" of correlated random variables
  - Upper bounds
  - Our proof technique
- Conclusions

The Goal

- Given $\psi(X;Y\|Z)$, we would like to show that

$$\psi(X;Y\|Z) \geq S(X;Y\|Z)$$

The Goal

- Given $\psi(X;Y\|Z)$, we would like to show that

$$\psi(X;Y\|Z) \geq S(X;Y\|Z)$$

- Find properties that $S(X;Y\|Z)$ has

The Goal

- Given $\psi(X;Y\|Z)$, we would like to show that

$$\psi(X;Y\|Z) \geq S(X;Y\|Z)$$

- Find properties that $S(X;Y\|Z)$ has
- Consider the set of all functions that have those properties

The Goal

- Given $\psi(X;Y\|Z)$, we would like to show that

$$\psi(X;Y\|Z) \geq S(X;Y\|Z)$$

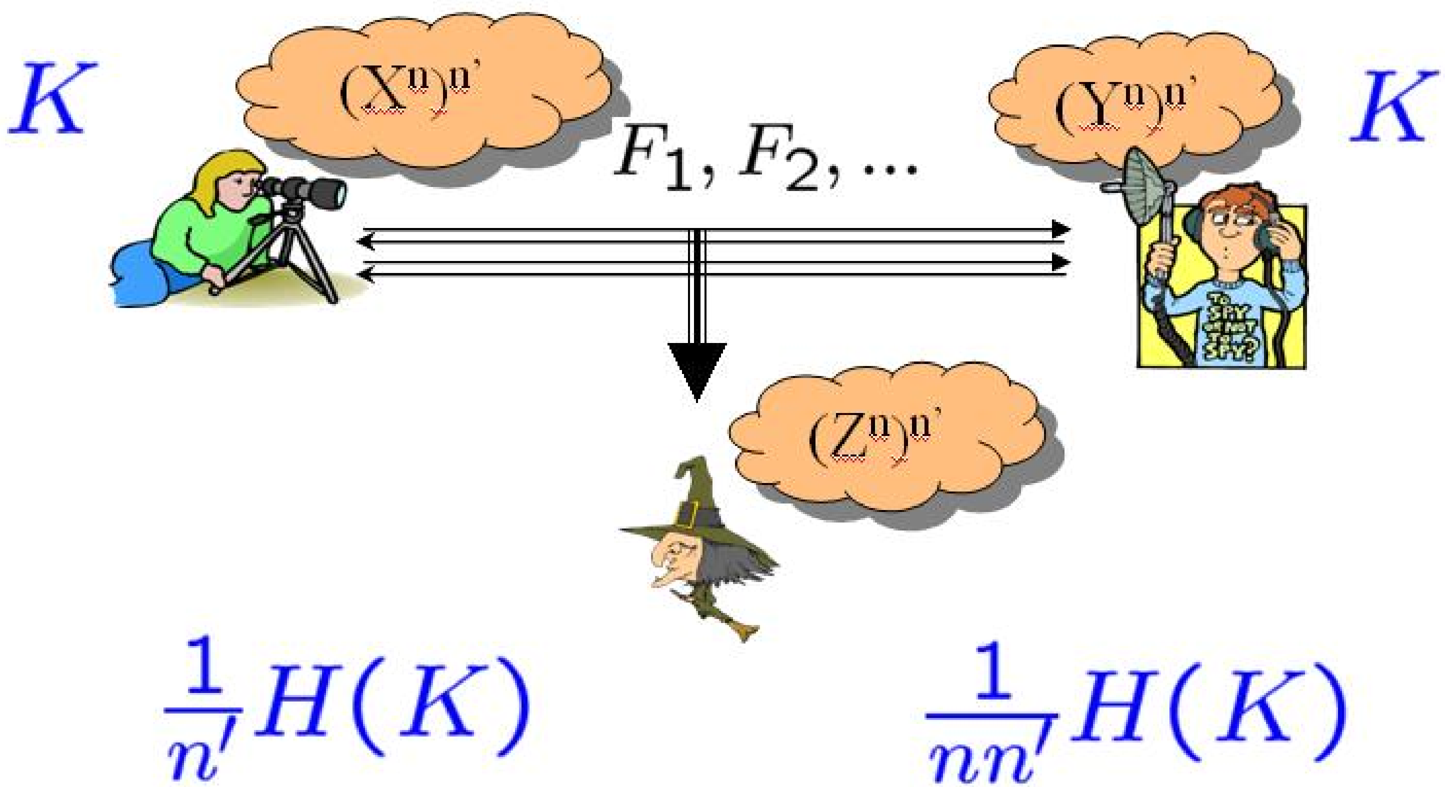
- Find properties that $S(X;Y\|Z)$ has
- Consider the set of all functions that have those properties
- Prove that each of them is an upper bound

Some properties of $S(X;Y\|Z)$

1) $n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n), \quad \forall n, p(x,y,z)$

Some properties of $S(X;Y\|Z)$

1) $n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n), \;\; \forall n, p(x,y,z)$



Some properties of $S(X;Y\|Z)$

1) $n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n), \;\; \forall n, p(x,y,z)$

2)$\forall F: H(F|X) = 0$ or $H(F|Y) = 0$,

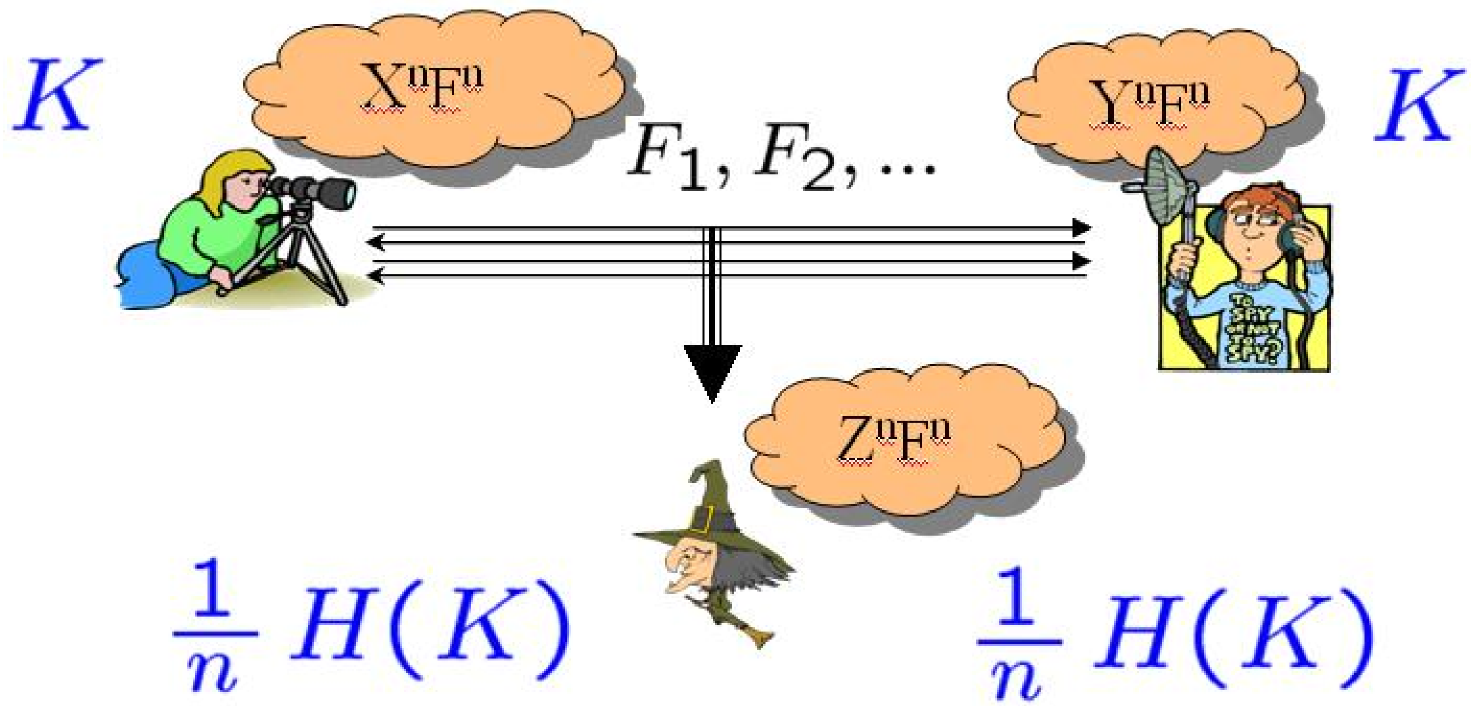
$\rightarrow S(X;Y\|Z) \geq S(XF;YF\|ZF)$

Some properties of $S(X;Y\|Z)$

1) $n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n), \;\; \forall n, p(x,y,z)$

2)$\forall F$: $H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow S(X;Y\|Z) \geq S(XF;YF\|ZF)$



Some properties of $S(X;Y\|Z)$

1) $n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n), \ \forall n, p(x,y,z)$

2)$\forall F: H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow S(X;Y\|Z) \geq S(XF;YF\|ZF)$

3)$\forall X', Y': H(X'|X) = 0, H(Y'|Y) = 0$,

$\rightarrow S(X;Y\|Z) \geq S(X';Y'\|Z)$

Some properties of $S(X;Y\|Z)$

1) $n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n), \quad \forall n, p(x,y,z)$

2)$\forall F : H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow S(X;Y\|Z) \geq S(XF;YF\|ZF)$

3)$\forall X', Y' : H(X'|X) = 0, H(Y'|Y) = 0$,

$\rightarrow S(X;Y\|Z) \geq S(X';Y'\|Z)$

4)$S(X;Y\|Z) \geq H(X|Z) - H(X|Y) = I(X;Y) - I(X;Z)$

S(Alices information; Bobs information$\|$ Eves information) is a non-increasing potential function

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

$n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n)$

Property used here: 1) $n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n)$

S(Alices information; Bobs information$\|$ Eves information) is a non-increasing potential function

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

$n \cdot S(X; Y\|Z) \geq S(X^n; Y^n\|Z^n)$

$\geq S(X^n F_1; Y^n F_1\|Z^n F_1)$

Property used here: 2)$\forall F$: $H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow S(X; Y\|Z) \geq S(XF; YF\|ZF)$

S(Alices information; Bobs information$\|$ Eves information) is a non-increasing potential function

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

$n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n)$

$\geq S(X^nF_1;Y^nF_1\|Z^nF_1)$

$\geq S(X^nF_1F_2;Y^nF_1F_2\|Z^nF_1F_2)$

Property used here: 2)$\forall F$: $H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow S(X;Y\|Z) \geq S(XF;YF\|ZF)$

S(Alices information; Bobs information$\|$ Eves information) is a non-increasing potential function

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

$n \cdot S(X; Y\|Z) \geq S(X^n; Y^n\|Z^n)$

$\geq S(X^nF_1; Y^nF_1\|Z^nF_1)$

$\geq S(X^nF_1F_2; Y^nF_1F_2\|Z^nF_1F_2) \geq ...$

$\geq S(X^n\overrightarrow{F}; Y^n\overrightarrow{F}\|Z^n\overrightarrow{F})$

Property used here: 2)$\forall F : H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow S(X; Y\|Z) \geq S(XF; YF\|ZF)$

S(Alices information; Bobs information$\|$ Eves information) is a non-increasing potential function

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

$n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n)$

$\geq S(X^nF_1;Y^nF_1\|Z^nF_1)$

$\geq S(X^nF_1F_2;Y^nF_1F_2\|Z^nF_1F_2) \geq ...$

$\geq S(X^n\overrightarrow{F};Y^n\overrightarrow{F}\|Z^n\overrightarrow{F})$

$\geq S(K_A;K_B\|Z^n\overrightarrow{F})$

Property used here: 3)$\forall X', Y' : H(X'|X) = 0, H(Y'|Y) = 0,$

$\rightarrow S(X;Y\|Z) \geq S(X';Y'\|Z)$

S(Alices information; Bobs information$\|$ Eves information) is a non-increasing potential function

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

$n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n)$

$\geq S(X^nF_1;Y^nF_1\|Z^nF_1)$

$\geq S(X^nF_1F_2;Y^nF_1F_2\|Z^nF_1F_2) \geq \ldots$

$\geq S(X^n\overrightarrow{F};Y^n\overrightarrow{F}\|Z^n\overrightarrow{F})$

$\geq S(K_A;K_B\|Z^n\overrightarrow{F})$

$\cong H(K_A|Z^n\overrightarrow{F}) - H(K_A|K_BZ^n\overrightarrow{F})$

Property used here: 4)$S(X;Y\|Z) \geq H(X|Z) - H(X|Y)$

S(Alices information; Bobs information$\|$ Eves information) is a non-increasing potential function

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

$n \cdot S(X;Y\|Z) \geq S(X^n;Y^n\|Z^n)$

$\geq S(X^nF_1;Y^nF_1\|Z^nF_1)$

$\geq S(X^nF_1F_2;Y^nF_1F_2\|Z^nF_1F_2) \geq ...$

$\geq S(X^n\overrightarrow{F};Y^n\overrightarrow{F}\|Z^n\overrightarrow{F})$

$\geq S(K_A;K_B\|Z^n\overrightarrow{F})$

$\cong H(K_A|Z^n\overrightarrow{F}) - H(K_A|K_BZ^n\overrightarrow{F}) \cong H(K_A)$

The set of all functions that satisfy the properties

1) $n \cdot \psi(X;Y\|Z) \geq \psi(X^n;Y^n\|Z^n), \quad \forall n, p(x,y,z)$

2)$\forall F$: $H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow \psi(X;Y\|Z) \geq \psi(XF;YF\|ZF)$

3)$\forall X', Y'$: $H(X'|X) = 0, H(Y'|Y) = 0$,

$\rightarrow \psi(X;Y\|Z) \geq \psi(X';Y'\|Z)$

4)$\psi(X;Y\|Z) \geq H(X|Z) - H(X|Y)$

Proving that any function that satisfies the properties is an upper bound

Take an arbitrary $p(x, y, z)$ and an arbitrary strategy of length n

Can write the same chain of inequalities:

$n \cdot \psi(X;Y\|Z) \geq \psi(X^n;Y^n\|Z^n)$

$\geq \psi(X^n F_1;Y^n F_1\|Z^n F_1)$

$\geq \psi(X^n F_1 F_2;Y^n F_1 F_2\|Z^n F_1 F_2) \geq \ldots$

$\geq \psi(X^n \overrightarrow{F};Y^n \overrightarrow{F}\|Z^n \overrightarrow{F})$

$\geq \psi(K_A;K_B\|Z^n \overrightarrow{F})$

$\cong H(K_A|Z^n \overrightarrow{F}) - H(K_A|K_B Z^n \overrightarrow{F}) \cong H(K_A)$

Conclusion: $\forall p(x, y, z), n$: $n \cdot \psi(X;Y\|Z) \geq H(K_A)$

Example: $I(X;Y|Z)$ is an upper bound

1) $n \cdot I(X;Y|Z) \geq I(X^n;Y^n|Z^n), \ \ \forall n, p(x,y,z)$ ✓

2)$\forall F$: $H(F|X) = 0$ or $H(F|Y) = 0$,

$\rightarrow \ I(X;Y|Z) \ \geq \ I(XF;YF|ZF)$ ✓ since if $H(F|X) = 0$:

$$I(X;Y|Z) = I(XF;Y|Z) = I(F;Y|Z) + I(XF;YF|ZF)$$

3)$\forall X', Y'$: $H(X'|X) = 0, H(Y'|Y) = 0$,

$\rightarrow I(X;Y|Z) \geq I(X';Y'|Z)$ ✓

4)$I(X;Y|Z) \geq H(X|Z) - H(X|Y)$ ✓

Strategy for finding a new upper bound

- Take an existing outer bound that verifies the properties
- Perturb the expression of the outer bound
- Check whether the properties are still satisfied:

Strategy for finding a new upper bound

- Take an existing outer bound that verifies the properties
- Perturb the expression of the outer bound
- Check whether the properties are still satisfied:
  - Yes!
    - Hopefully it is strictly better than the existing bound

Strategy for finding a new upper bound

- Take an existing outer bound that verifies the properties
- Perturb the expression of the outer bound
- Check whether the properties are still satisfied:
  - Yes!
    - Hopefully it is strictly better than the existing bound
  - No.
    - See which property is violated and why?
    - Trial and error: Try to change the perturbation in a way that it works

Our new upper bound (I)

$$S(X;Y\|Z) \leq \quad \inf_J S(XY;J\|Z) + S(X;Y\|J)$$

$$S(X;Y\|Z) \leq \inf_J S(XY;J^{(s)}\|Z) + S(X;Y\|J)$$

$$S(X;Y\|Z) \leq \inf_J S(X;Y;J^{(s)}\|Z) + S(X;Y\|J)$$

$$S(X;Y\|Z) \leq \inf_{J_1,J_2} S(X;Y;J_1^{(s)};J_2^{(s)}\|Z) + \max\left(S(X;Y\|J_1^{(s)}), S(X;Y\|J_2^{(s)})\right)$$

Our new upper bound (II)

For any increasing convex function $f : \mathbb{R}_+ \to \mathbb{R}_+$, $S(X;Y\|Z)$ is bounded from above by

$$\inf_J f^{-1}\{f(S(X;Y\|J)) + S_{f-one-way}(XY;J^{(s)}\|Z)$$

where

$$S_{f-one-way}(A;B^{(s)}\|C) =$$
$$\text{sup}_{U-V-A-BC}[f(H(U|ZV)) - f(H(U|YV))]$$

leads to an upper bound when $S(X;Y\|J)$ is bounded from above by $I(X;Y|J)$

Outline

- Common Information
- One notion of "Common Private Information" of correlated random variables
  - Upper bounds
  - Our proof technique
- Conclusions

Conclusions

- Derived a new upper bound on a notion of private common information
- Discussed a technique for proving outer bounds.
  - Applicable to other problems in information theory