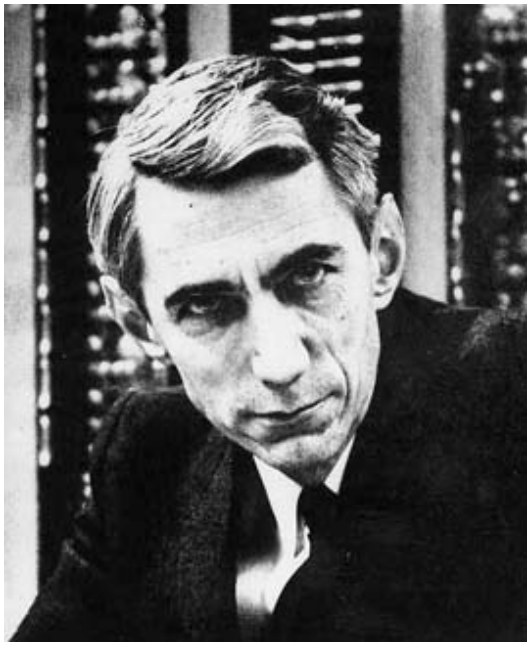
Information-theoretic Security

Venkat Anantharam

EECS Department
University of California Berkeley

(Joint work with Amin Aminzadeh Gohari)

Claude Elwood Shannon (1916 -2001)



- *A Mathematical Theory of Communication*, Bell System Technical Journal, 1948, called “The Magna Charta of the Communication Age” in an appreciation in the U.S. Congress on his death in 2001.

Entropy

- $$X \sim (p_1, p_2, \ldots, p_M)$$

$$H(X) = -p_1 \log p_1 - p_2 \log p_2 - \ldots - p_M \log p_M$$

- Similarly:

$$H(X_1, \ldots, X_n)$$

Information sources

- For *syntactic purposes* each information source has an entropy rate
-

> La musique souvent me prend comme une mer!
> Vers ma pâle étoile,
> Sous un plafond de brume ou dans un vaste éther,
> Je mets à la voile;
> ⋮

-

$$H(\text{ Baudelaire }) = ??$$

Multiple sources

- These reveal information about each other.
- $$H(Y \mid X, Z, W)$$

  or

  $$H(X, Y \mid A, W) - H(X \mid A, W)$$

  etc.
- The mutual information is *symmetric*

$$I(X \wedge Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$$

Typical sequences

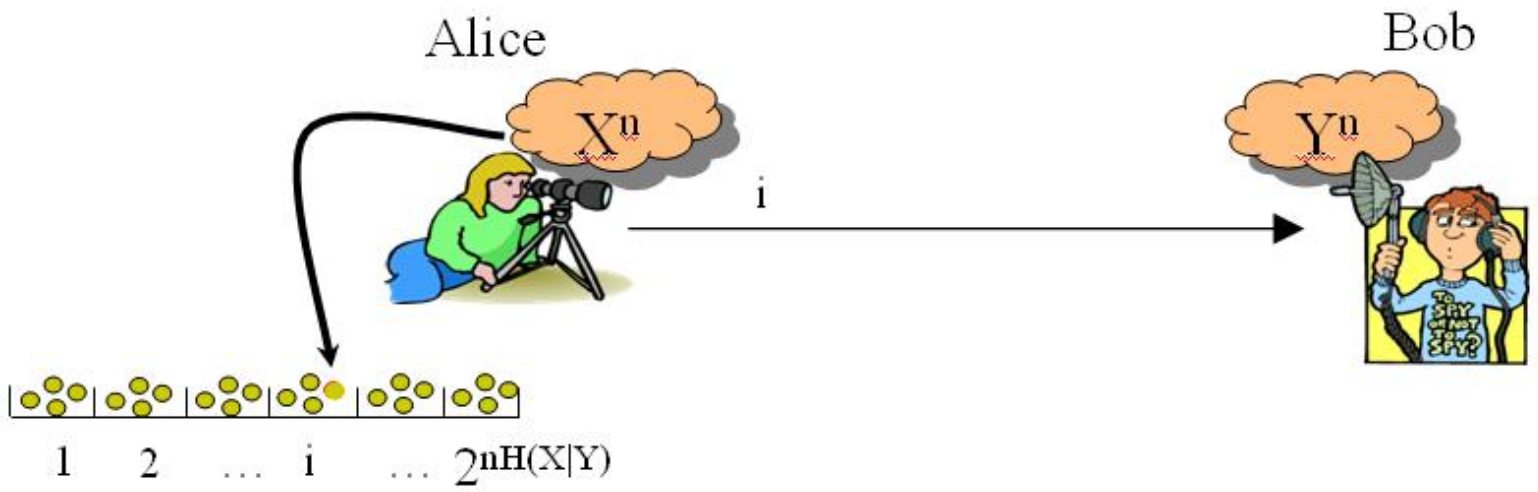
- $(X_1, Y_1), (X_2, Y_2), \ldots, (X_n, Y_n)$, i. i. d. $\sim p_{XY}(x, y)$.
- $t_{x^n} \in \mathcal{P}(\mathcal{X})$ defined by $t_{x^n}(x) = \frac{1}{n} N(x \mid x^n)$.
- $T_X^n := \{x^n \ : \ \mid t_{x^n}(x) - p_X(x) \mid \leq \frac{K}{\sqrt{n}}, \quad t_{x^n}(x) = 0 \ \text{ if } \ p_X(x) = 0\}$.
- Then $\mid T_X^n \mid = 2^{nH(X)+o(1)}$
- Also, $p_{X^n}(x^n) = 2^{-nH(X)+o(1)}$ if $x^n \in T_X^n$.

Conditionally typical sequences

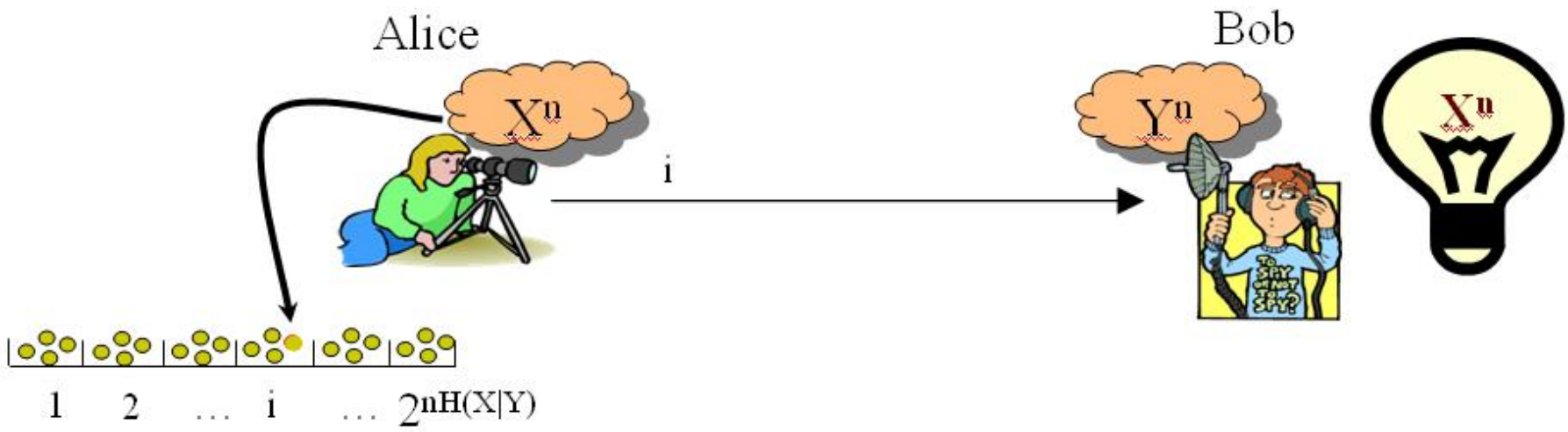
- $(X_1, Y_1), (X_2, Y_2), \ldots, (X_n, Y_n)$, i. i. d. $\sim p_{XY}(x, y)$.
- For $x^n \in T_X^n$
  $T_{Y|x^n}^n := \{y^n \ : \ \mid t_{x^n y^n}(x, y) - p_{XY}(x, y) \mid \leq \frac{K}{\sqrt{n}},$
  $t_{x^n y^n}(x, y) = 0 \quad \text{if } p_{XY}(x, y) = 0\}$
- Then $\mid T_{Y|x^n}^n \mid = 2^{nH(Y|X)+o(1)}$
- Also, $p_{Y^n|X^n}(y^n \mid x^n) = 2^{-nH(Y|X)+o(1)}$ if $y^n \in T_{Y|x^n}^n$.

For two random variables (X, Y): a sense in which $I(X;Y)$ represents the common part of X and Y

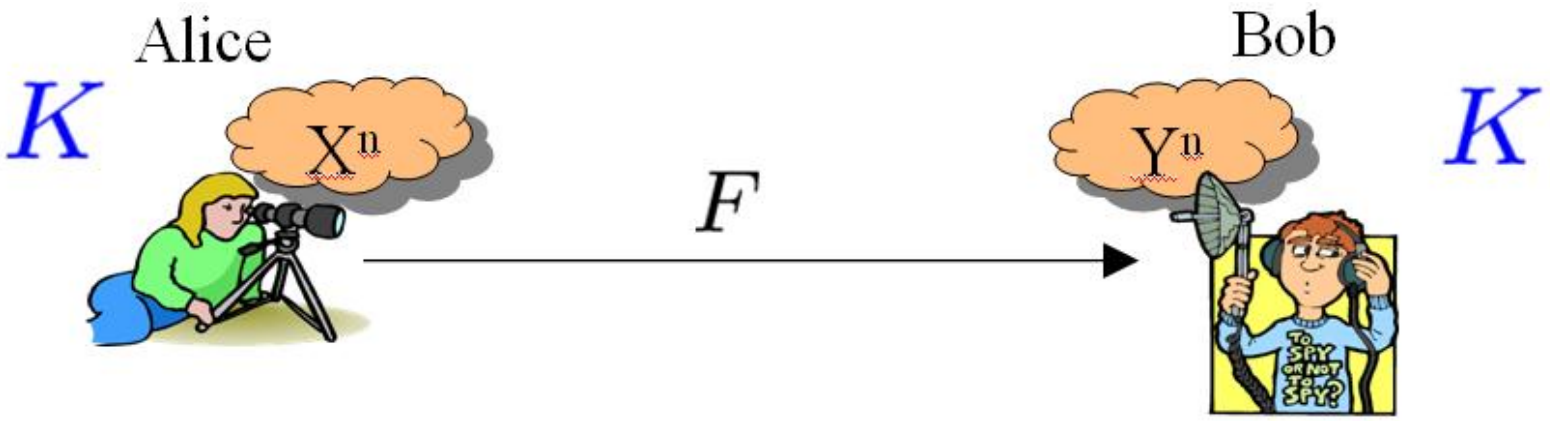
For two random variables (X, Y): a sense in which $I(X;Y)$ represents the common part of X and Y



For two random variables (X, Y): a sense in which $I(X;Y)$ represents the common part of X and Y



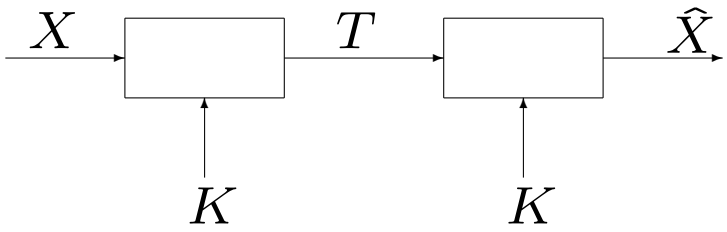
For two random variables (X, Y): a sense in which $I(X;Y)$ represents the common part of X and Y



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

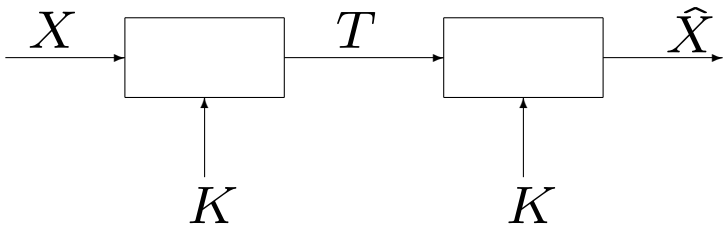
$$\frac{1}{n}H(K)$$

Secure communication based on a secret key



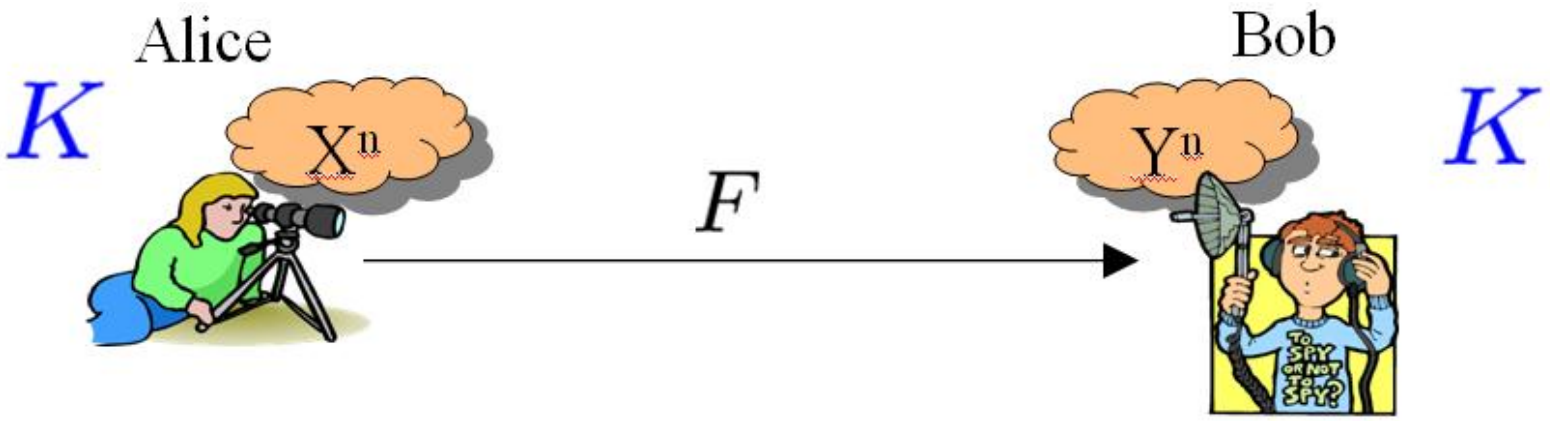
- X is the message, K is the key, $X \amalg K$.
- T is a deterministic function of X and K.
- $\widehat{X}$ is a deterministic function of T and K and should equal X.
- For secrecy we must have $X \amalg T$.
- Shannon's "One-time pad" result: We must have $H(K) \geq H(X)$.
- *Communication Theory of Secrecy*, Bell System Technical Journal, 1949.

The “one-time pad” result



- $H(X \mid T, K) = 0$.
- Hence $H(X, K \mid T) = H(K \mid T) \leq H(K)$.
- Hence $H(K \mid X, T) + H(X \mid T) \leq H(K)$.
- But $H(X \mid T) = H(X)$.
- Hence $H(X) \leq H(K)$.

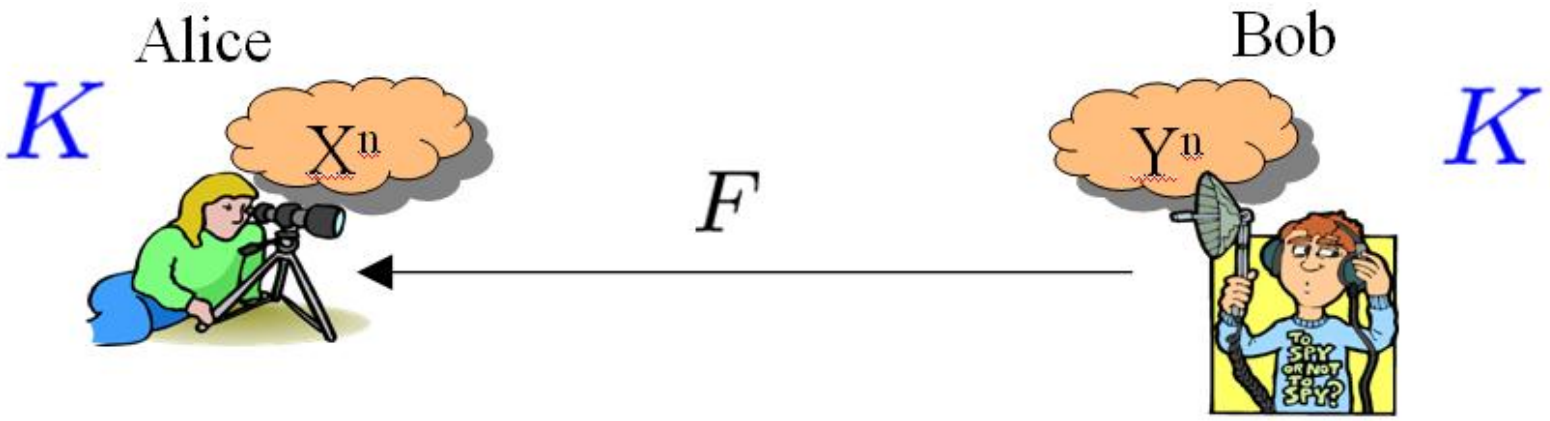
For two random variables (X, Y): a sense in which $I(X;Y)$ represents the common part of X and Y



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

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

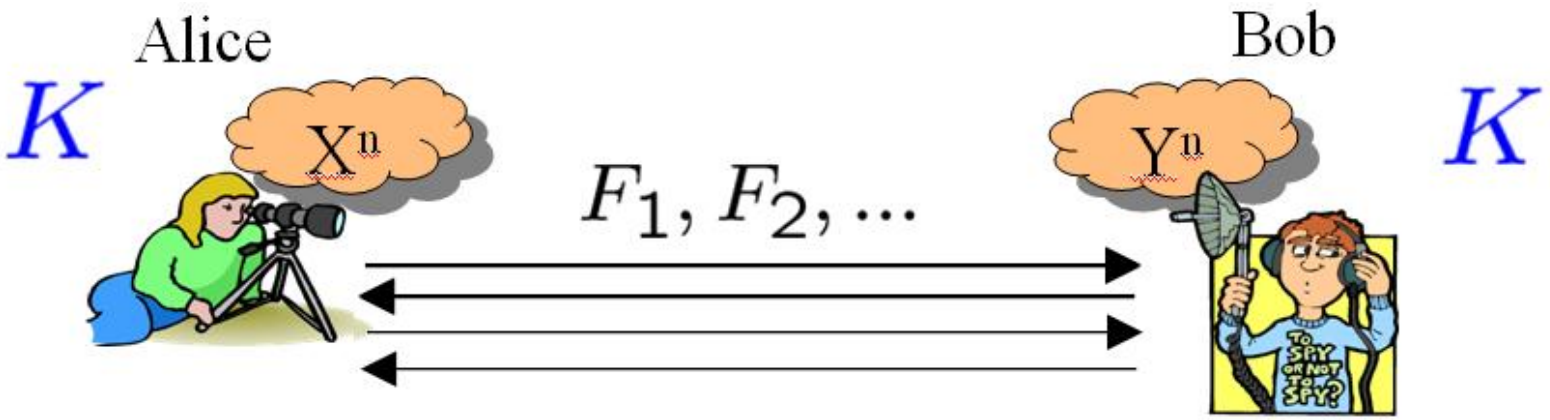
For two random variables (X, Y): a sense in which $I(X;Y)$ represents the common part of X and Y



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

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

For two random variables (X, Y): a sense in which $I(X;Y)$ represents the common part of X and Y

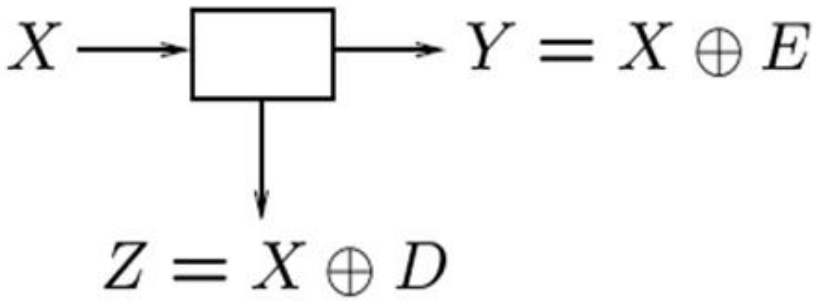


$$I(K; \overrightarrow{F}) \cong 0$$

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

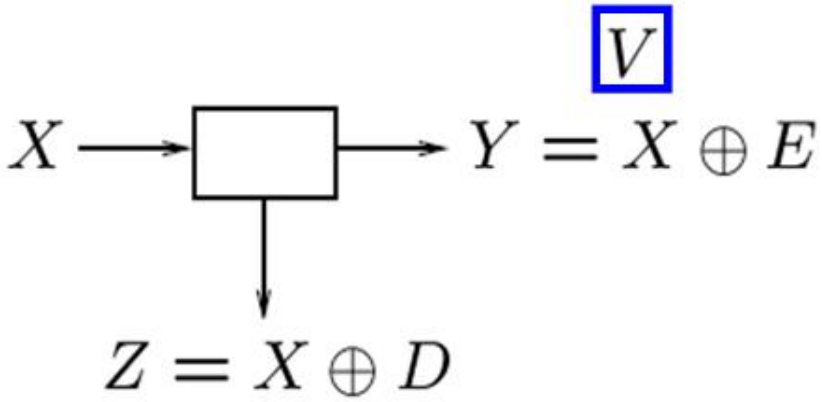
Power of public discussion

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



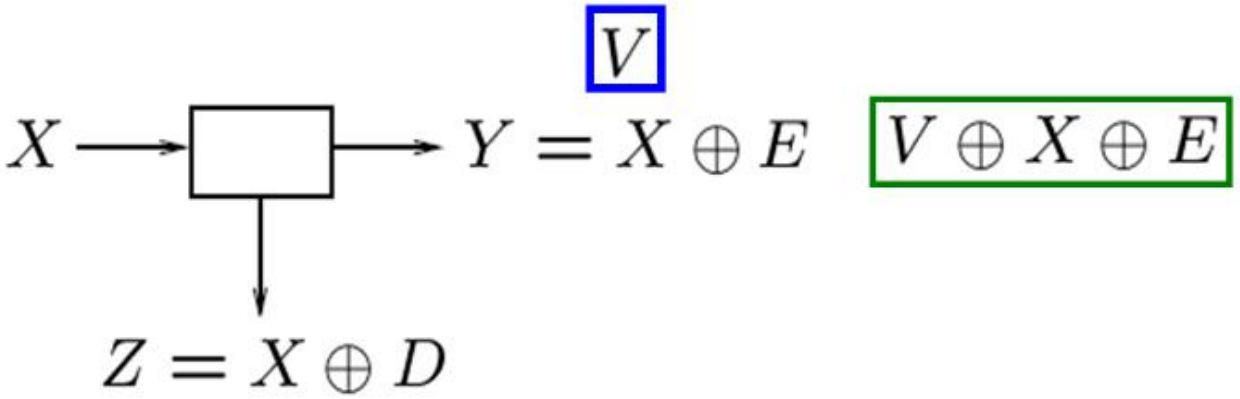
Power of public discussion

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



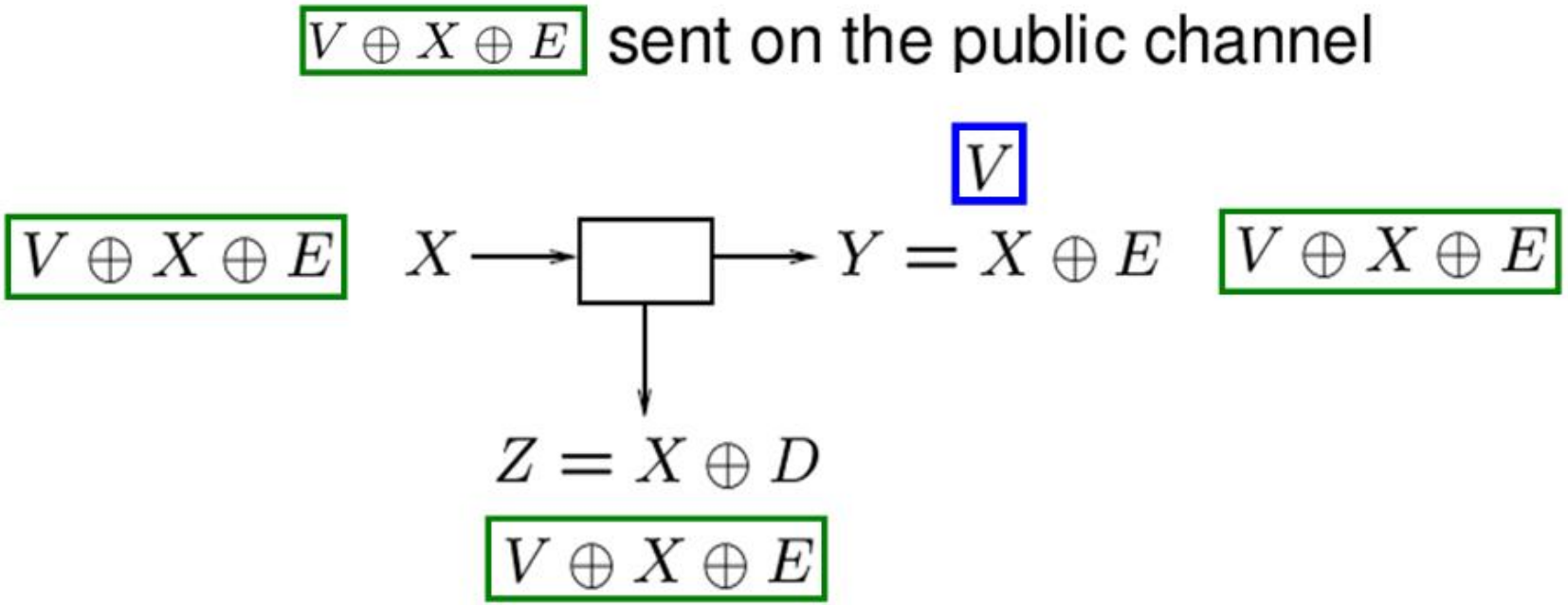
Power of public discussion

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



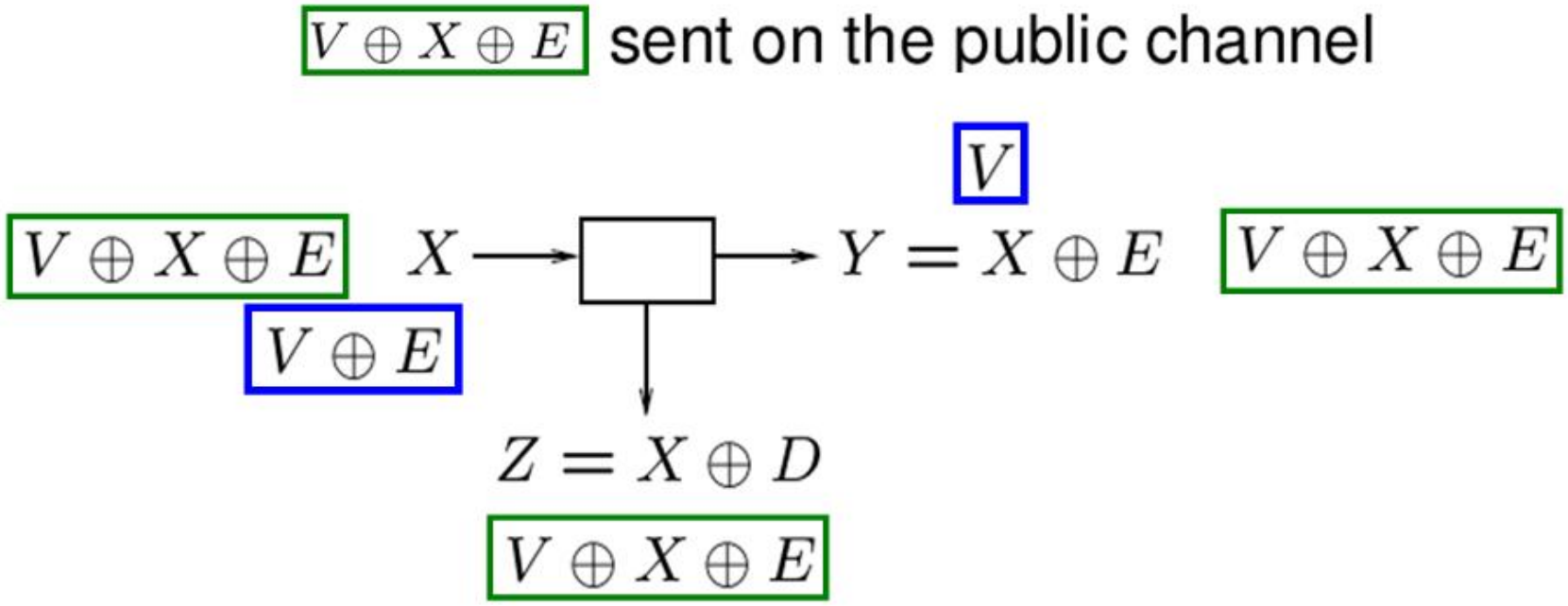
Power of public discussion

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



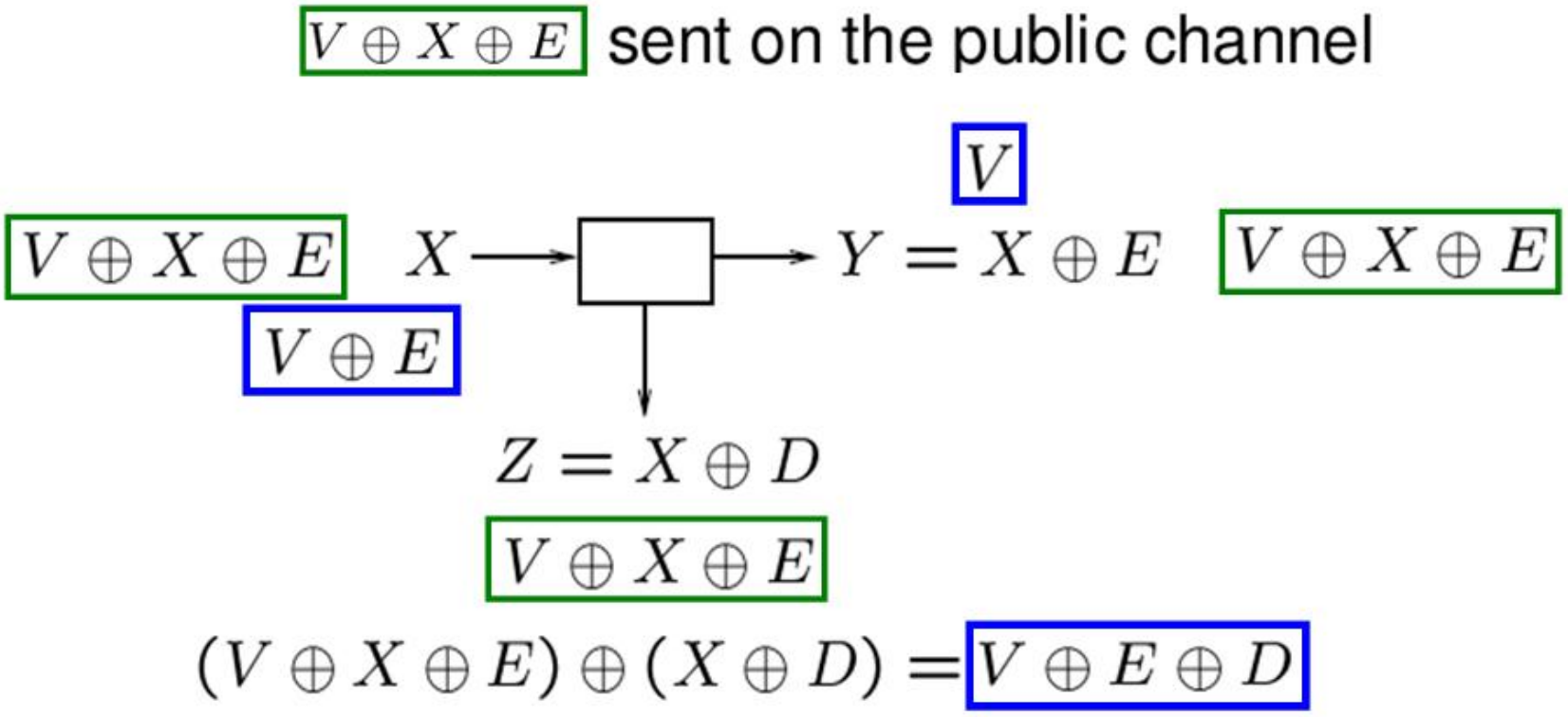
Power of public discussion

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

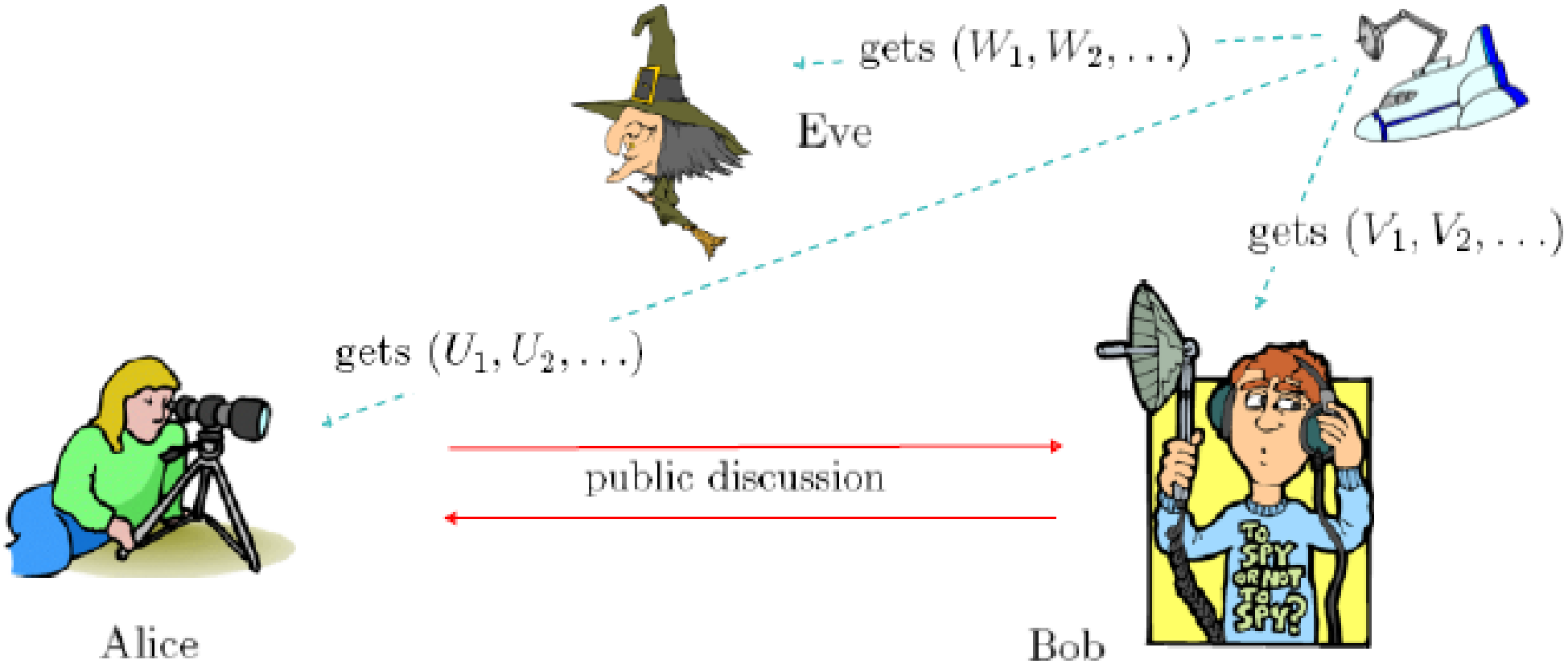


Power of public discussion

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



Is information theoretic security dead?



Secret key agreement by public discussion from common information U. M. Maurer IEEE-IT 1993

Common Information of a pair of random variables private from an eavesdropper

- Given random variables (X, Y, Z), how can one quantify the common part of r.v.s X and Y that is independent of Z?
  - Application in a private communication system: secret key generation

Common Information of a pair of random variables private from an eavesdropper

- Given random variables (X, Y, Z), how can one quantify the common part of r.v.s X and Y that is independent of Z?
- Special cases:
  - If Z is independent of $(X, Y) \longrightarrow I(X; Y)$

Common Information of a pair of random variables private from an eavesdropper

- Given random variables (X, Y, Z), how can one quantify the common part of r.v.s X and Y that is independent of Z?
- Special cases:
  - If Z is independent of $(X, Y) \longrightarrow I(X; Y)$
  - If $X = Y = K \longrightarrow H(K|Z)$.

Common Information of a pair of random variables private from an eavesdropper

- Given random variables (X, Y, Z), how can one quantify the common part of r.v.s 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 $I(X;Y|Z)$?

Common Information of a pair of random variables private from an eavesdropper

- Given random variables (X, Y, Z), how can one quantify the common part of r.v.s X and Y that is independent of Z?
- What about $I(X;Y|Z)$?
  - But $I(X;Y|Z)$ can be greater than $I(X;Y)$!

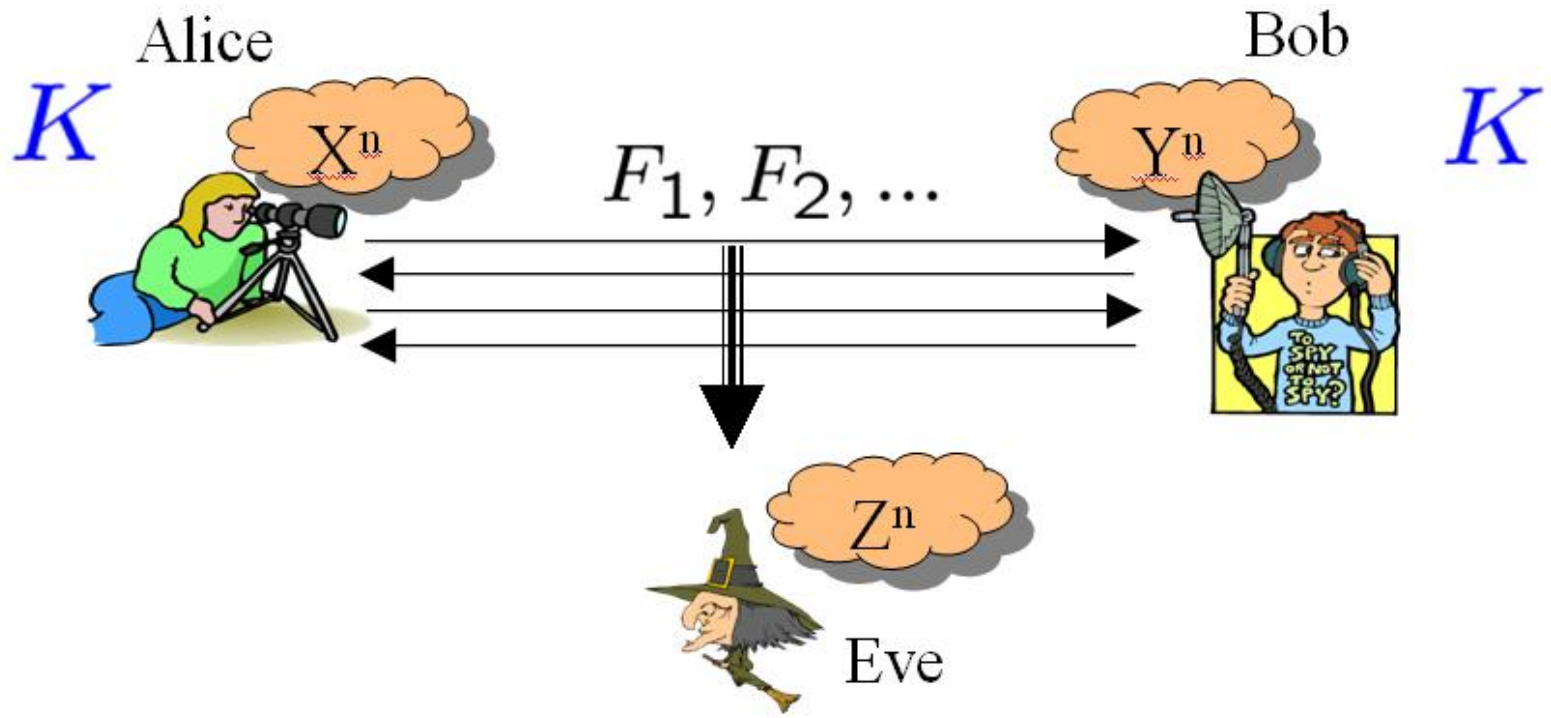
$$X \sim B(\frac{1}{2}),\ \ Y \sim B(\frac{1}{2}),\ \ X \perp Y,\ \ Z = X \oplus Y$$

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

Common Information of a pair of random variables private from an eavesdropper

- Given random variables (X, Y, Z), how can one quantify the common part of r.v.s X and Y that is independent of Z?
- What about $I(X;Y|Z)$?
- $S(X;Y||Z)$ defined later in the talk works.

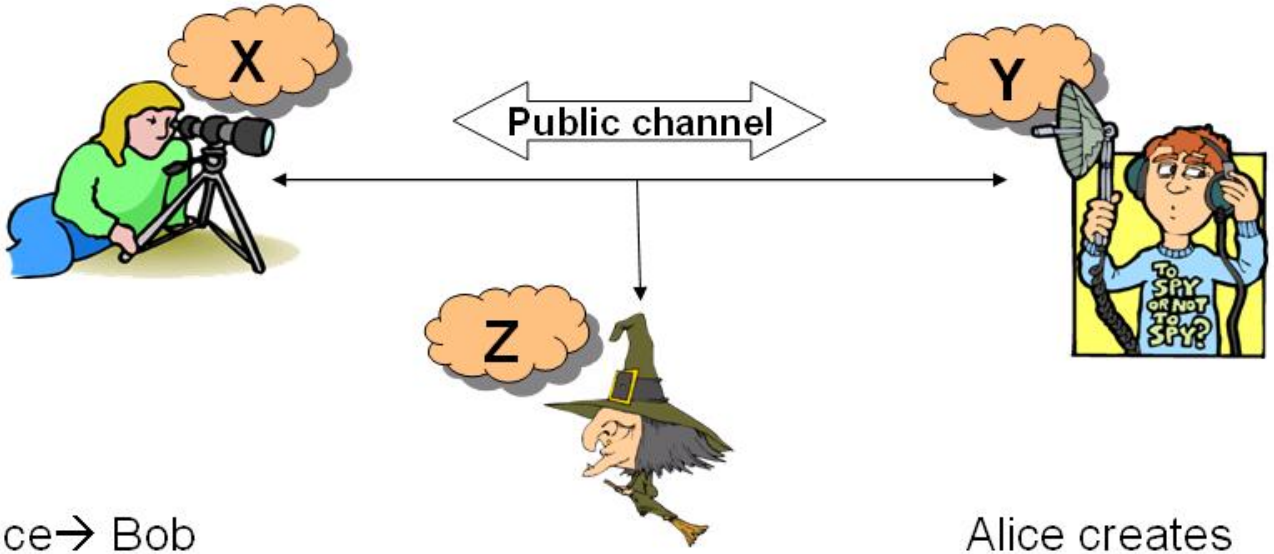
The general case requiring secrecy



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

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

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:
$P(K_A=K_B=K)>1-\varepsilon$
$\frac{1}{n} I(K ; Z^{1:n}, \mathbf{F}) \le \varepsilon$

Secret key rate
$S(X;Y\|Z)$

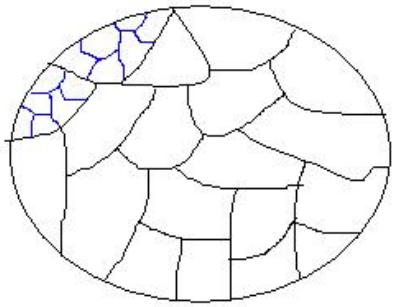
Historical development

- Known as the Source model, the model was developed in the context of "Information theoretic security"
- Evolutionary ancestors of the model

Model	Type of advantage
Shannon's one time pad	Common secret key
↓	↓
Wyner's Wire-Tap Channel	Eve's channel degraded
↓	↓
Csiszár & J. Körner's Broadcast channel	Directions at which Eve's channel is worst
↓	↓
Maurer's model	Public discussion
↓	↓
Maurer, Alhswede, Csiszár's models: Source Model and Channel model	Public discussion and/or Quality of observations

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

Authors	Lower bounds on $S(X;Y\|Z)$
Maurer (1993)	$\max\{I(X;Y)-I(X;Z), I(Y;X)-I(Y;Z)\}$
Ahlswede and Csisz'ar (1993)	$\max\left(\sup_{V-U-X-YZ} I(U;Y\|V)-I(U;Z\|V), \sup_{V-U-Y-XZ} I(U;X\|V)-I(U;Z\|V)\right)$
	Proof idea for $I(X;Y)-I(X;Z)$: The X^n space is first partitioned into $2^{n\cdot H(Y\|X)}$ bins of size $2^{n\cdot I(X;Y)}$, i.e. the Slepian-Wolf binning strategy; each bin is then further partitioned into $2^{n[I(X;Y)-I(X;Z)]}$ bins of size $2^{n\cdot I(X;Z)}$.



Known 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. $H(K_A) = nI(X;Y\|Z) + H(K_A\|K_B) + I(K_A;FZ^n)$ $H(K_A) = nI(X;Y) + H(K_A\|K_B) + I(K_A;F)$
Maurer and Wolf (1999)	$I(X;Y \downarrow Z) := \inf_{XY-Z-T}(I(X;Y\|T))$ Idea: decreasing the information of Eve cannot 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 cannot decrease the common private information by more than $H(U)$ bits.

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

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

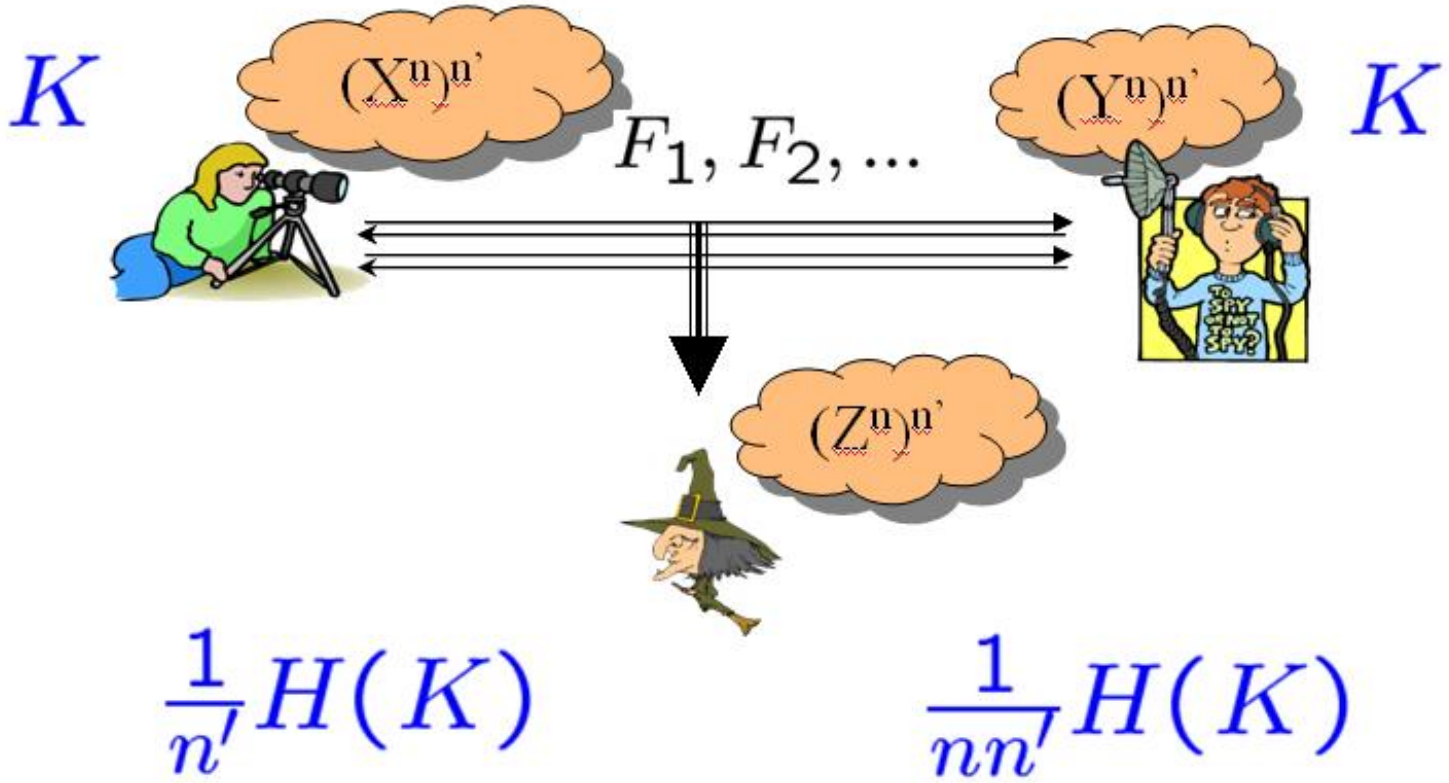
- Find properties that $S(X;Y\|Z)$ has
- Consider the set of all functions that have those properties
- Prove that each of them is an upper bound

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



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

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

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

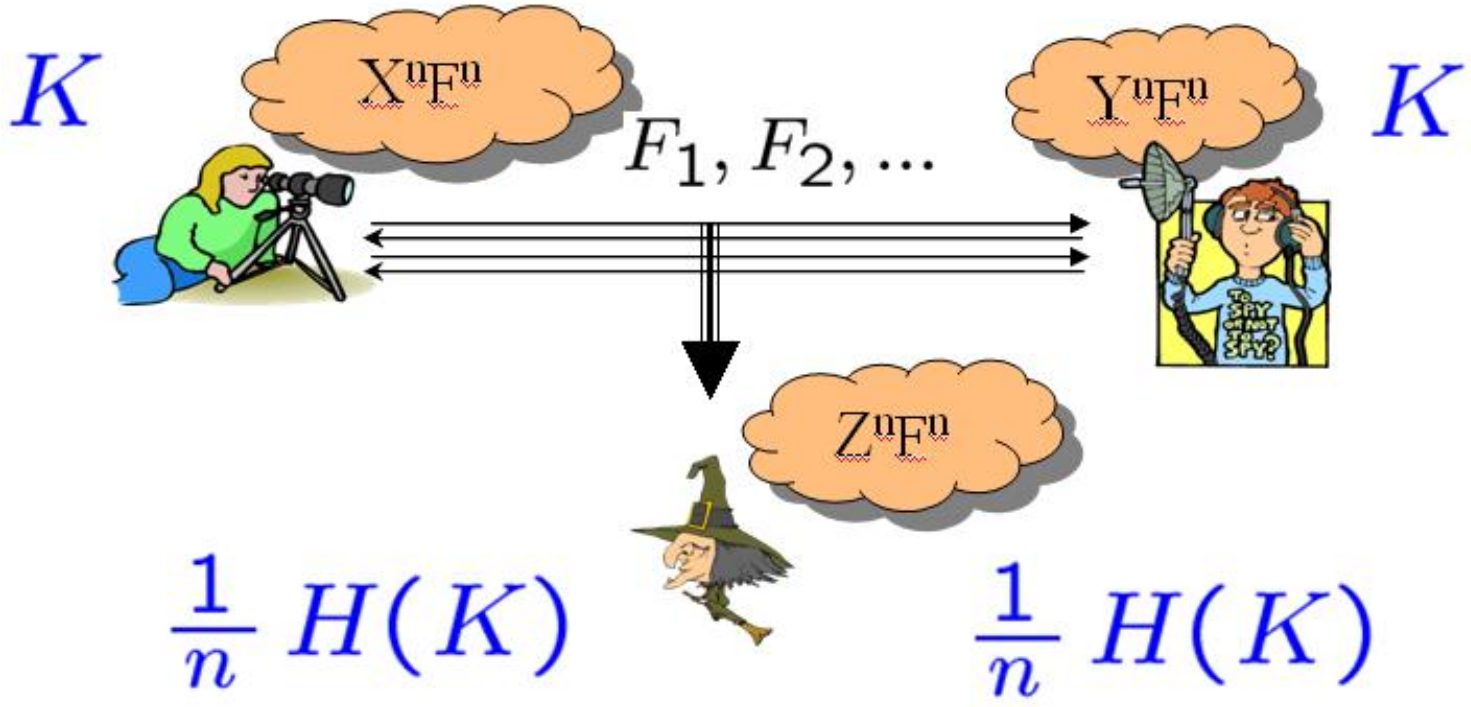
$\rightarrow S(X;Y\|Z) \geq S(XF;YF\|ZF)$

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

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

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

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



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

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(Alice's information; Bob's information|| Eve's 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(Alice's information; Bob's information|| Eve's 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(Alice's information; Bob's information|| Eve's information) is a non-increasing potential function

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

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

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

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

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(Alice's information; Bob's information|| Eve's information) is a non-increasing potential function

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

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

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

$$\geq S(X^n F_1 F_2; Y^n F_1 F_2 \| Z^n F_1 F_2) \geq ...$$

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

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(Alice's information; Bob's information|| Eve's information) is a non-increasing potential function

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

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

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

$$\geq S(X^n F_1 F_2; Y^n F_1 F_2 \| Z^n F_1 F_2) \geq ...$$

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

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

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(Alice's information; Bob's information|| Eve's information) is a non-increasing potential function

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

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

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

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

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

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

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

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

S(Alice's information; Bob's information|| Eve's information) is a non-increasing potential function

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

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

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

$$\geq S(X^n F_1 F_2; Y^n F_1 F_2 \| Z^n F_1 F_2) \geq ...$$

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

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

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

Properties required of the functions of interest

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

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

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

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:

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

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

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

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

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

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

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

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

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

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

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

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

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

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
  - 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

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

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

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

Comparison with Renner and Wolf upper bound (I)

$\inf_J \Big(I(XY;J|Z) + I(X;Y|J)\Big)$ is a computable expression that is greater than or equal to our new upper bound.

- $\inf_J \Big(I(XY;J|Z) + I(X;Y|J)\Big) \leq \inf_U (H(U) + I(X;Y \downarrow ZU))$:

$\inf_U (H(U) + I(X;Y \downarrow ZU)) = \inf_U \Big(H(U) + \min_{J-ZU-XY} I(X;Y|J)\Big)$

Assume minimum occurs at J_U:

$$\inf_U (H(U) + I(X;Y \downarrow ZU)) = \inf_U \Big(H(U) + I(X;Y|J_U)\Big) \geq$$
$$\inf_U \Big(I(XY;ZU|Z) + I(X;Y|J_U)\Big) \geq \inf_U \Big(I(XY;J_U|Z) + I(X;Y|J_U)\Big) \geq$$
$$\inf_J \Big(I(XY;J|Z) + I(X;Y|J)\Big)$$

Comparison with Renner and Wolf upper bound (II)

- There is an example for which the inequality is strict

$$\inf_J \Big(I(XY;J|Z) + I(X;Y|J) \Big) < \inf_U (H(U) + I(X;Y \downarrow ZU))$$

Idea: perturbing the Renner-Wolf example:

	X				
Y		0	1	2	3
	0	$\frac{1}{8}$	$\frac{1}{8}$	0	0
	1	$\frac{1}{8}$	$\frac{1}{8}$	0	0
	2	0	0	$\frac{1}{4}$	0
	3	0	0	0	$\frac{1}{4}$

$$Z = \begin{cases} X + Y \pmod 2 & \text{if } X, Y \in \{0,1\} \\ X \pmod 2 & \text{if } X \in \{2,3\} \end{cases} \qquad U = \lfloor \frac{X}{2} \rfloor$$

Comparison with Renner and Wolf upper bound (III)

We perturb the mentioned example. Since the RW bound does not behave as smoothly as the new bound behaves, the new bound outperforms the RW bound.

We find a binary random variable V of small entropy satisfying $V - U - XYZ$ such that the new bound is strictly better than the double intrinsic information bound for the triple $\widetilde{X} = X,\ \widetilde{Y} = Y,\ \widetilde{Z} = (Z, V)$. Proof idea:

- Assuming that the RW bound and ours are the same at $(\widetilde{X},\ \widetilde{Y},\ \widetilde{Z})$, we prove that: For any sequence of U_i's such that $H(U_i) + I(X; Y \downarrow ZU_i) \to \inf_U [H(U) + I(X; Y \downarrow ZU)]$ as $i \to \infty$, we must have $H(U_i) \to 0$.
- Since the intrinsic information is a continuous function, $H(U_i) + I(X; Y \downarrow ZU_i)$ must converge to $I(X; Y \downarrow Z)$ which is equal to $\frac{3}{2}$. Hence the RW bound would be around $\frac{3}{2}$ at $(\widetilde{X},\ \widetilde{Y},\ \widetilde{Z})$.
- Since our bound is continuous, and is around 1 at (X, Y, Z), it has to be close to 1 at $(\widetilde{X},\ \widetilde{Y},\ \widetilde{Z})$. Contradiction!

New Lower Bound

Given

$$U_1 - X - YZ; t_1 := I(U_1; Y) - I(U_1; Z)$$

$$U_2 - YU_1 - XZU_1; t_2 := I(U_2; Y|U_1) - I(U_2; Z|U_1)$$

$$U_3 - XU_1U_2 - YZU_1U_2; t_3 := I(U_3; Y|U_1U_2) - I(U_3; Z|U_1U_2)$$

$$\ldots$$

$$S(X; Y\|Z) \geq \Sigma_{i=p}^{q} t_i$$

Comparison with Ahlswede and Csiszárs lower bound

- A generalization of Ahlswede and Csiszárs lower bound (new feature: interactive communication): $U_1 = V, U_2 = 0, U_3 = U, p = q = 3$

Comparison with Ahlswede and Csiszárs lower bound

• A generalization of Ahlswede and Csiszárs lower bound (new feature: interactive communication): $U_1 = V, U_2 = 0, U_3 = U, p = q = 3$

• There is an example for which the new bound is strictly better: it is tight for the example provided in Ahlswede and Csisz'ar to show that their bound is not tight: Choice of $X = (X_1, X_2), Y = (Y_1, Y_2), Z = (Z_1, Z_2)$

$$X_1 - Y_1 - Z_1, \quad Y_2 - X_2 - Z_2, \quad I(X_1 Y_1 Z_1; X_2 Y_2 Z_2) = 0$$

Proof idea

For simplicity assume $p = 1$, $q = 2$:

$$U_1^n - X^n - Y^n Z^n$$
$$U_2^n - Y^n U_1^n - X^n Z^n$$

- U_1^n is created by X^n and transmitted to Y^n using Slepian-Wolf bin index F_1
- U_2^n is created by $Y^n U_1^n$ transmitted to X^n using Slepian-Wolf bin index F_2
- Generated key:

$H(U_1^n U_2^n | F_1 F_2 Z^n) = H(U_1^n | F_1 F_2 Z^n) + H(U_2^n | U_1^n F_1 F_2 Z^n) =$
$H(U_1^n | F_1 F_2 Z^n) + H(U_2^n | U_1^n F_2 Z^n)$

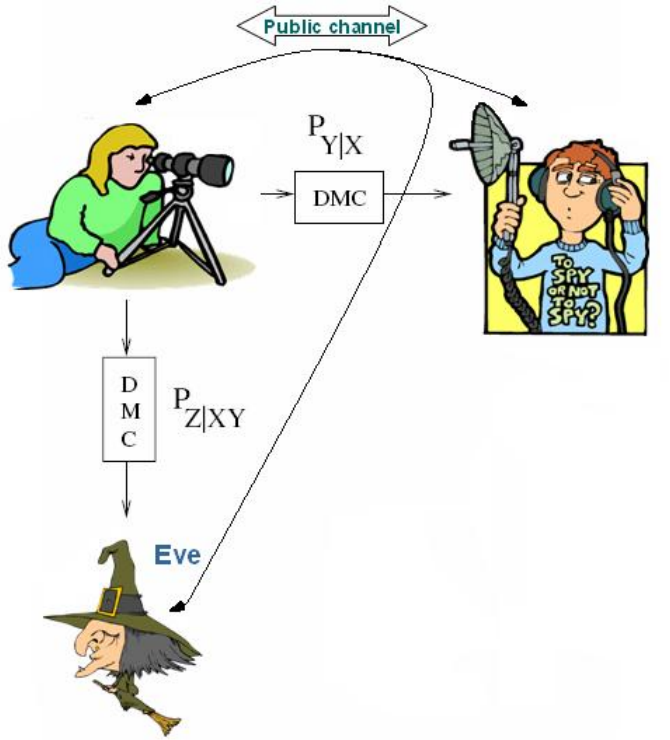
If $t_2 > 0$, $F_2 \perp (Z^n U_1^n) \Rightarrow H(U_1^n | F_1 F_2 Z^n) = H(U_1^n | F_1 Z^n) = [t_1]_+$
$H(U_2^n | U_1^n F_2 Z^n) = t_2 \Longrightarrow \frac{1}{n} H(U_1^n U_2^n | F_1 F_2 Z^n) \geq t_1 + t_2$

If $t_2 \leq 0$, $H(U_1^n | F_1 F_2 Z^n) \geq H(U_1^n | F_1 Z^n) - n|t_2| \Longrightarrow \frac{1}{n} H(U_1^n U_2^n | F_1 F_2 Z^n) \geq$
$t_1 + t_2$

Channel Model: Definition of $C_{CH}(p(yz|x))$

Alice puts X_1, Bob and Eve receive Y_1, Z_1; a round of public discussion; Alice puts X_2, Bob and Eve receive Y_2, Z_2; a round of public discussion... Alice creates $K_A(X^n, \overrightarrow{F})$, Bob creates $K_B(Y^n, \overrightarrow{F})$.

$$P(K_A = K_B = K) > 1 - \epsilon, \frac{1}{n} I(K; Z^n \overrightarrow{F}) < \epsilon$$



Known results on $C_{CH}(p(yz|x))$

Authors	Lower bounds on $C_{CH}(p(yz\|x))$
Maurer (1993)	$\sup_{p(x)}(\max\{I(X;Y)-I(X;Z), I(Y;X)-I(Y;Z)\})$ Idea: $C_{CH}(p(yz\|x)) \geq \sup_{p(x)} S(X;Y\|Z)$ Remark: Can use the lower bound of Ahlswede and Csisz'ar to get a better lower bound
Authors	Upper bounds on $C_{CH}(p(yz\|x))$
Maurer (1993)	$\min(\sup_{p(x)} I(X;Y\|Z), \sup_{p(x)} I(X;Y))$ Idea: Idea: classical converse arguments.

Known results on $C_{CH}(p(yz|x))$

Authors	Lower bounds on $C_{CH}(p(yz\|x))$
Maurer (1993)	$\sup_{p(x)}(\max\{I(X;Y)-I(X;Z), I(Y;X)-I(Y;Z)\})$ Idea: $C_{CH}(p(yz\|x)) \geq \sup_{p(x)} S(X;Y\|Z)$ Remark: Can use the lower bound of Ahlswede and Csisz'ar to get a better lower bound
Authors	Upper bounds on $C_{CH}(p(yz\|x))$
Maurer (1993)	$\min(\sup_{p(x)} I(X;Y\|Z), \sup_{p(x)} I(X;Y))$ Idea: Idea: classical converse arguments.

We prove new lower and upper bounds

Application of the potential function method to Channel Model

New upper bound (can be shown to be strictly better than the best known upper bound):

$$\sup_{p(x)} \inf_{J} [I(X;Y|J) + I(XY;J|Z)]$$

Idea:Find properties that imply an expression is an upper bound

Verify that the given expression satisfies these properties.

Would like to prove that

$$\Psi(q(xy|z)) = \sup_{q(x)} \psi(q(x)q(y,z|x))$$

is an outer bound.

Sufficient conditions for a function to be an upper bound for the Channel Model

1) Whenever $H(X'|X) = 0$ and $XYZ - X - X' - X'Y'Z'$ and $p(y', z'|x') = q(y', z'|x')$ are true, we have:

$\psi(XX'; YY'\|ZZ') \geq \psi(X; Y\|Z) + \Psi(q(xy|z))$

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