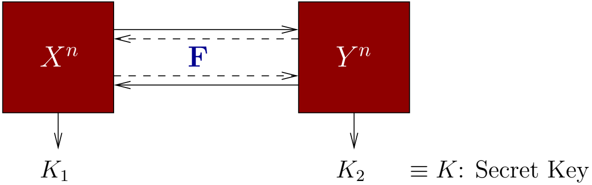
Minimal Public Communication for Maximum Rate Secret Key Generation

Himanshu Tyagi

Department of Electrical and Computer Engineering
and Institute of System Research
University of Maryland, College Park, USA.

Secret Key Generation



Secret key (SK) K with interactive communication $\mathbf{F}$ satisfies:

$$\Pr(K_1 = K_2 = K) \approx 1 : \quad \text{Recoverability}$$

$$\frac{1}{n} I\left(K \wedge \mathbf{F}\right) \approx 0 : \quad \text{Secrecy}$$

Rate of the secret key $= \frac{1}{n} H(K)$.

Secret key capacity $C =$ maximum achievable rate of a secret key.

[Maurer '93, Ahlswede-Csiszár '93]

$$C = I(X \wedge Y).$$

Communication for SK Capacity

What is the min. rate of $\mathbf{F}$ required for achieving SK capacity?

- Maurer-Ahlswede-Csiszár
  - *Common randomness* (CR) generated: X^n or Y^n.
  - Rate of communication required $= \min\{H(X|Y); H(Y|X)\}$.
  - Decomposition:
    $H(X) = H(X \mid Y) + I(X \wedge Y)$,
    $H(Y) = H(Y \mid X) + I(X \wedge Y)$.
- Csiszár-Narayan
  - *Common randomness* generated: X^n, Y^n.
  - Rate of communication required $= H(X|Y) + H(Y|X)$.
  - Decomposition:
    $H(X,Y) = H(X \mid Y) + H(Y \mid X) + I(X \wedge Y)$.

Communication for SK Capacity

What is the min. rate of $\mathbf{F}$ required for achieving SK capacity?

- Maurer-Ahlswede-Csiszár
  - *Common randomness* (CR) generated: X^n or Y^n.
  - Rate of communication required $= \min\{H(X|Y); H(Y|X)\}$.
  - Decomposition:
    $H(X) = H(X \mid Y) + I(X \wedge Y)$,
    $H(Y) = H(Y \mid X) + I(X \wedge Y)$.
- Csiszár-Narayan
  - *Common randomness* generated: X^n, Y^n.
  - Rate of communication required $= H(X|Y) + H(Y|X)$.
  - Decomposition:
    $H(X,Y) = H(X \mid Y) + H(Y \mid X) + I(X \wedge Y)$.

Q1: Forms of CR for agreeing on optimum rate SK ?

Communication for SK Capacity

What is the min. rate of $\mathbf{F}$ required for achieving SK capacity?

- Maurer-Ahlswede-Csiszár
  - *Common randomness* (CR) generated: X^n or Y^n.
  - Rate of communication required $= \min\{H(X|Y); H(Y|X)\}$.
  - Decomposition:
    $H(X) = H(X \mid Y) + I(X \wedge Y)$,
    $H(Y) = H(Y \mid X) + I(X \wedge Y)$.
- Csiszár-Narayan
  - *Common randomness* generated: X^n, Y^n.
  - Rate of communication required $= H(X|Y) + H(Y|X)$.
  - Decomposition:
    $H(X, Y) = H(X \mid Y) + H(Y \mid X) + I(X \wedge Y)$.

Q1: Forms of CR for agreeing on optimum rate SK ?

Q2: Does minimum communication rate correspond to "minimum" CR?

Interactive Form of Wyner's Common Information

- Wyner's Common Infomation

  $CI(X \wedge Y) \equiv$ min. rate of a function $L = L\left(X^n, Y^n\right)$ such that

  $$\frac{1}{n} I(X^n \wedge Y^n \mid L) \approx 0.$$

  Defined in the context of source generation and source coding.

Interactive Form of Wyner's Common Information

- Wyner's Common Infomation

  $CI(X \wedge Y) \equiv$ min. rate of a function $L = L(X^n, Y^n)$ such that

  $$\frac{1}{n} I(X^n \wedge Y^n \mid L) \approx 0.$$

  Defined in the context of source generation and source coding.

- Interactive Common Information

  Terminals agree on CR J using r-rounds $\mathbf{F}$.

  $CI_i^r(X \wedge Y) \equiv$ min. rate of $(J, \mathbf{F})$ such that

  $$\frac{1}{n} I(X^n \wedge Y^n \mid J, \mathbf{F}) \approx 0.$$

  $CI_i(X \wedge Y) = \lim_{r \to \infty} CI_i^r(X \wedge Y).$

Note: $CI(X \wedge Y) \leq CI_i(X \wedge Y) \leq \min\{H(X); H(Y)\}.$

Minimum Communication for Optimum SK

For minimum rate of communication R_{SK} for optimum rate SK:

We characterize the CR associated with optimum rate SK.

- A CR J recoverable from communication $\mathbf{F} \Rightarrow$ SK of rate $\frac{1}{n}H(J|\mathbf{F})$.
- An optimum rate SK corresponds to a CR J recoverable from $\mathbf{F}$ s.t.

$$\frac{1}{n}I(X^n \wedge Y^n \mid J, \mathbf{F}) \approx 0.$$

  - *For instance:* $J = X^n$, Y^n or (X^n, Y^n).
  - R_{CI} be the min. rate of communication for such CR.

- Shall show: CR of the above form always yields optimum rate SK.

Minimum Communication for Optimum SK

For minimum rate of communication R_{SK} for optimum rate SK:

We characterize the CR associated with optimum rate SK.

- A CR J recoverable from communication $\mathbf{F} \Rightarrow$ SK of rate $\frac{1}{n}H(J|\mathbf{F})$.
- An optimum rate SK corresponds to a CR J recoverable from $\mathbf{F}$ s.t.

$$\frac{1}{n}I(X^n \wedge Y^n \mid J, \mathbf{F}) \approx 0.$$

  - *For instance:* $J = X^n$, Y^n or (X^n, Y^n).
  - R_{CI} be the min. rate of communication for such CR.

- Shall show: CR of the above form always yields optimum rate SK.

Theorem

$$R_{SK} = R_{CI} = CI_i(X \wedge Y) - I(X \wedge Y).$$

Minimum Communication for Optimum SK

Theorem

$$R_{SK} = R_{CI} = CI_i(X \wedge Y) - I(X \wedge Y).$$

- **Lemma:** For each $r \geq 1$:
  - $R_{SK}^r \geq R_{CI}^r \geq R_{SK}^{r+1}$.
  - Decomposition:
    $R_{CI}^r \geq CI_i^r(X \wedge Y) - I(X \wedge Y) \geq R_{CI}^{r+1}$.
- Theorem follows by taking the limit $r \to \infty$ in the Lemma.

Idea of the Proof

- Proof is based on the observation:

$$I(X \wedge Y) \approx \frac{1}{n}\left[I\left(X^n \wedge Y^n \mid J, \mathbf{F}\right) + H(J, \mathbf{F}) - H(\mathbf{F} \mid X^n) - H(\mathbf{F} \mid Y^n)\right].$$

Characterization of the form of CR in optimum SK generation:

$$\frac{1}{n} I\left(X^n \wedge Y^n \mid J, \mathbf{F}\right) \approx 0$$

if and only if

$$I(X \wedge Y) \approx \frac{1}{n}\left[H(J, \mathbf{F}) - \left[H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)\right]\right].$$

Idea of the Proof

- Proof is based on the observation:

$$I(X \wedge Y) \approx \frac{1}{n}\left[I\left(X^n \wedge Y^n \mid J, \mathbf{F}\right) + H(J, \mathbf{F}) - H(\mathbf{F} \mid X^n) - H(\mathbf{F} \mid Y^n)\right].$$

Characterization of the form of CR in optimum SK generation:

$$\frac{1}{n} I\left(X^n \wedge Y^n \mid J, \mathbf{F}\right) \approx 0$$

if and only if

$$I(X \wedge Y) \approx \frac{1}{n}\left[H(J, \mathbf{F}) - \left[H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)\right]\right].$$

SK rate associated with CR J recoverable from $\mathbf{F}$

Minimum Communication for Optimum SK

Theorem

R_{SK} = min. rate of $\mathbf{F}$ required for optimal rate SK generation.

R_{CI} = min. rate $\mathbf{F}$ required for generating CR J s.t. $X^n \underset{\sim}{\perp\!\!\!\perp} Y^n | (J, \mathbf{F})$.

Then,

$$R_{SK} = R_{CI} = CI_i(X \wedge Y) - I(X \wedge Y).$$

$$CI_i(X \wedge Y) = \lim_{r \to \infty} CI_i^r(X \wedge Y).$$

Characterization of CI_i

- Given rvs X, Y and $r \geq 1$, we have

$$CI_i^r(X \wedge Y) = \min_{U_1,V_1,\ldots,U_r,V_r} I(X,Y \wedge U_1,V_1,...,U_r,V_r),$$

$$U_1 -\circ- X -\circ- Y, \qquad V_1 -\circ- Y, U_1 -\circ- X,$$

$$U_2 -\circ- X, V_1 -\circ- Y, \qquad V_2 -\circ- Y, U_1, V_1 -\circ- X$$

$$\vdots \qquad \vdots$$

$$U_r -\circ- X, U^{r-1}, V^{r-1} -\circ- Y, \qquad V_r -\circ- Y, U^r, V^{r-1} -\circ- X.$$

$$X -\circ- U^r, V^r -\circ- Y$$

- Single-letter expression for CI_i is not (yet) available.

Noninteractive Communication for SK Capacity

Communication from X^n to Y^n:

$$R_{SK}^{one} = \min_{\substack{U -\circ- X -\circ- Y \\ X -\circ- U -\circ- Y}} I(X, Y \wedge U) - I(X \wedge Y)$$

U satisfies: $U -\circ- X -\circ- Y, \quad X -\circ- U -\circ- Y.$

- [Problem 16.26, Csiszár-Körner]

$$\min_{\substack{U -\circ- X -\circ- Y \\ X -\circ- U -\circ- Y}} I(X, Y \wedge U) = \min_{\substack{g(X) s.t. \\ X -\circ- g(X) -\circ- Y}} H(g(X))$$

.

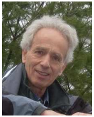
Common Information Quantities

For a pair of rvs X, Y

$$CI_{GC} \leq I(X \wedge Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X); H(Y)\}$$

Common Information Quantities

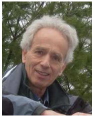
For a pair of rvs X, Y



$$CI_{GC} \leq I(X \wedge Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X); H(Y)\}$$

Common Information Quantities

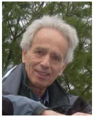
For a pair of rvs X, Y



$$CI_{GC} \le I(X \wedge Y) \le CI \le CI_i \le CI_i^r \le CI_i^{r-1} \le \min\{H(X); H(Y)\}$$

Common Information Quantities

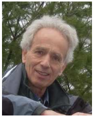
For a pair of rvs X, Y



$$CI_{GC} \leq I(X \wedge Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X); H(Y)\}$$

Common Information Quantities

For a pair of rvs X, Y

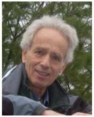


$$CI_{GC} \leq I(X \wedge Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X); H(Y)\}$$

Interactive Common Information

Common Information Quantities

For a pair of rvs X, Y



$$CI_{GC} \leq I(X \wedge Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X); H(Y)\}$$

Interactive Common Information

- CI_i is indeed a new quantity

  For binary rvs X and Y: $CI_i(X \wedge Y) = \min\{H(X); H(Y)\}$.

  For binary symmetric X and Y: $CI(X \wedge Y) < \min\{H(X); H(Y)\}$.