Function Computation, Secrecy Generation and Common Randomness

Himanshu Tyagi

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

January 19, 2012
Correlated data are collected and stored at distributed terminals.

Examples include:

* Image from http://www.prismaelectronics.eu

Sensor Networks
Processing of Distributed Data

Correlated data are collected and stored at distributed terminals.

Examples include:

Data Centers

A public network is available for communication.
Correlated data are collected and stored at distributed terminals. A public network is available for communication.

- **Function computation:**
  A subset of terminals want to evaluate a function of the data. What is the minimum amount of communication required?

- **Secure function computation:**
  Computing a function of the data
  - using communication independent of the function value.

- **Secret key generation**
  Share bits using communication independent of the function value.
Assumption on the data

1. $X_i^n = (X_{i1}, \ldots, X_{in})$
   - Data observed at time instance $t$: $X_{Mt} = (X_{1t}, \ldots, X_{mt})$
   - Probability distribution of $X_1, \ldots, X_m$ is known.

2. Observations are i.i.d. across time:
   - $X_{M1}, \ldots, X_{Mn}$ are i.i.d. rvs.

3. Observations are finite-valued.
Interactive Communication Protocol

Assumptions on the protocol

- Each terminal has access to all the communication.
- Multiple rounds of interactive communication are allowed.
- Communication from terminal 1: $F_{11} = f_{11}(X_1^n)$
Interactive Communication Protocol

COMMUNICATION NETWORK

$F_{11}$  $F_{21}$

$X_1^n$  $X_2^n$  $X_m^n$

Assumptions on the protocol

- Each terminal has access to all the communication.
- Multiple rounds of interactive communication are allowed.
- Communication from terminal 2: $F_{21} = f_{21}(X_2^n, F_{11})$
Interactive Communication Protocol

Assumptions on the protocol

- Each terminal has access to all the communication.
- Multiple rounds of interactive communication are allowed.
- $r$ rounds of interactive communication: $F = F_1, \ldots, F_m$
Outline of the Talk

Function computation

Secure function computation

Common randomness for secret key generation

Computing without revealing the critical data
Outline of the Talk

Function computation

Secure function computation

Common randomness for secret key generation

Computing without revealing the critical data
Computing a Function of Distributed Data

Given: a single-letter function to be computed:

\[ g(X^n_M) = (g(X_{M1}), \ldots, g(X_{Mn})) \, . \]

Notation: \( G = g(X_M) \), \( G^n = (g(X_{M1}), \ldots, g(X_{Mn})) \)

Recoverability:

\[ \Pr \left( \hat{G}^{(n)}_i = G^n, i \in A \right) \geq 1 - \epsilon, \quad \text{for all } n \text{ large.} \]

What is the minimum rate of communication \( \frac{1}{n} \log \| F \| \) needed?
Computing a Function of Distributed Data

\[ F_1, F_2, F_a, F_m \equiv F: \text{Public Communication} \]

\[ \hat{G}_1^{(n)}, \hat{G}_2^{(n)}, \hat{G}_a^{(n)} \]

Recoverability:

\[ \Pr \left( \hat{G}_i^{(n)} = G^n, i \in A \right) \geq 1 - \epsilon, \quad \text{for all } n \text{ large.} \]

What is the minimum rate of communication \( \frac{1}{n} \log \|F\| \) needed?

A. C. Yao

Some complexity questions related to distributive computing

STOC '79
Computing a Function of Distributed Data

Recoverability:

\[ \Pr \left( \hat{G}^{(n)}_i = G^n, i \in A \right) \geq 1 - \epsilon, \quad \text{for all } n \text{ large.} \]

What is the minimum rate of communication \( \frac{1}{n} \log \|F\| \) needed?

J. Körner and K. Marton

How to encode the modulo-two sum of binary sources

IT, 25(2), March 1979, 219 - 221
Special Case: Körner-Marton

Function computed: \( g(X_1, X_2) = X_1 \oplus X_2 \)

**Theorem**

The rate region of communication for computing parity is given by

\[
\{(R_1, R_2) : R_1 \geq h(\delta), \quad R_2 \geq h(\delta)\}.
\]
Theorem

The minimum rate of communication required for function computation is given by

$$\min_{W \in X_1 \ominus X_2} I(W \land X_1 | X_2)$$

where $W | X_1 \sim$ independent sets of the function graph that contain $X_1$. 

Special Case: Orlitsky-Roche


The rate region of communication for function computation consists of \((R_1, R_2)\) s.t.

\[
\begin{align*}
(R_1, R_2) : R_1 &\geq I(U \land X_1|X_2), \quad R_2 \geq I(V \land X_2|X_1, U) \\
U \not\Rightarrow X_1 \not\Rightarrow X_2, \quad V \not\Rightarrow X_2, U \not\Rightarrow X_1 \quad \text{and} \quad H(G|U, V, X_1) = 0
\end{align*}
\]
Special Case: Orlitsky-Roche

Extensions:

- N. Ma and P. Ishwar, *Some results on distributed source coding for interactive function computation*, IT, 57(9), September 2011, pp. 6180-6195.


\[
\begin{align*}
\hat{G}_1(n) & \quad \hat{G}_2(n) \\
\hat{G}_1(n) & \quad \hat{G}_2(n)
\end{align*}
\]
Special Case: Orlitsky-Roche

Extensions:

- N. Ma and P. Ishwar, Some results on distributed source coding for interactive function computation, IT, 57(9), September 2011, pp. 6180-6195.

How many rounds of interaction are optimal?
Function Computation and Helper Problems

Theorem (No-helper problem)

The rate region consists of \( k \)-tuples \((R_1, ..., R_k)\) s.t.

\[
\sum_{i \in B} R_i \geq H \left( X_B | X_{\{1, ..., k\}/B} \right), \quad B \subseteq \{1, ..., k\}.
\]

Function Computation and Helper Problems


Theorem

*The rate region consists of* $k + l$-tuples $(R_1, ..., R_{k+l})$ *s.t.*

$$
\forall \ k + 1 \leq i \leq k + l : R_i \geq \frac{1}{n} H (f_i (X_i^n))
$$

$$
\forall \ B \subseteq \{1, ..., k\} : \sum_{i \in B} R_i \geq \frac{1}{n} H \left( X_B^n | X_{\{1, ..., k\}}^n / B, f_{\{1, ..., k\}} / B \right).
$$
Function Computation and Helper Problems

\[ X_1^n \rightarrow X_2^n \rightarrow \cdots \rightarrow X_k^n \rightarrow X_{k+1}^n \]

\( F_1, F_2, F_k, F_{k+1}, F_{k+l} \)

\( \hat{X}_1^{(n)}, \hat{X}_2^{(n)}, \ldots, \hat{X}_k^{(n)} \)

\( l \) helpers, \( k + l \) terminals


Single-letter characterization of the general helper problem remains open.

- **Entropy sets** corresponding to rvs $Y_1, ..., Y_p, Z_1, ..., Z_q$:

$$\text{cl} \left\{ \left( \frac{1}{n} H \left( Y_1^n | f_1, \ldots, f_q \right) , \ldots, \frac{1}{n} H \left( Y_p^n | f_1, \ldots, f_q \right) \right) : n \geq 1, f_i = f_i \left( Z_i^n \right) \right\}.$$

Here $Z_1, ..., Z_q$ correspond to the helper sources.
Single-letter characterization of the general helper problem remains open.

- **Entropy sets** corresponding to rvs $Y_1, \ldots, Y_p, Z_1, \ldots, Z_q$:

  $$\text{cl} \left\{ \left( \frac{1}{n} H\left( Y_1^n | f_1, \ldots, f_q \right), \ldots, \frac{1}{n} H\left( Y_p^n | f_1, \ldots, f_q \right) \right) : n \geq 1, f_i = f_i(Z_i^n) \right\}.$$ 

  Here $Z_1, \ldots, Z_q$ correspond to the helper sources.

---

Csizsár-Körner-Marton solved for $p = 3, q = 1$ with $Z_1 = Y_1$.

---

Most general achievable region for 1 helper problem:

Function Computation and Helper Problems

Function computation as a helper problem

- One of the encoders knows the function value ⇒ Helper problem
- In general, can we introduce a dummy terminal and set its rate to 0?
- How to handle interactive communication?

How does the Csiszár-Körner result extends to function computation?
Function computation

Secure function computation

Common randomness for secret key generation

Computing without revealing the critical data
Secure Computing of Functions

\[ F \perp G^n \]

COMMUNICATION NETWORK

\[ \hat{G}_i^{(n)} \]

\[ \hat{G}_2^{(n)} \]

\[ \hat{G}_m^{(n)} \]

\[ X_1^n \]

\[ X_2^n \]

\[ X_m^n \]

- \( G_i^{(n)} \) is the estimate of \( G^n \) at terminal \( i \).

Secure computability of \( g \):

**Recoverability**: \( \Pr \left( G_i^{(n)} = G^n, i \in \mathcal{M} \right) \geq 1 - \epsilon \)

**Secrecy**: \( I (G^n \land F') \leq \epsilon \)

When is a given function \( g \) securely computable?
Secure Computing of Functions

$G_i^{(n)}$ is the estimate of $G^n$ at terminal $i$.

Secure computability of $g$:

- **Recoverability**: $\Pr\left(G_i^{(n)} = G^n, i \in \mathcal{M}\right) \geq 1 - \epsilon$

- **Secrecy**: $I\left(G^n \land F\right) \leq \epsilon$

**Deterministic Model:**

Secure Computing of Functions

- $G_i^{(n)}$ is the estimate of $G^n$ at terminal $i$.

**Secure computability of $g$:**

- **Recoverability**: $\Pr \left( G_i^{(n)} = G^n, i \in M \right) \geq 1 - \epsilon$
- **Secrecy**: $I (G^n \land F') \leq \epsilon$

---

**When is a given function $g$ securely computable?**

A Sufficient Condition

- Share all data to compute $g$: Omniscience $\equiv X_M^n$
- Can we attain omniscience using $F \perp \sim G^n$?

Claim: Omniscience can be attained using $F \perp \sim G^n$ if:

$$H(G) < H(X_M) - R_{CO}$$
Random Mappings For Omniscience


- \( F_i = F_i (X_i^n) \): random mapping of rate \( R_i \).
- With large probability, \( F_1, ..., F_m \) result in omniscience if:
  \[
  \sum_{i \in B} R_i \geq H (X_B|X_{B^c}) , \quad B \subsetneq \mathcal{M}.
  \]
- \( R_{CO} = \min \sum_{i \in \mathcal{M}} R_i \).

- Given $\mathcal{X}$-valued rv $X$.
- $R(X) = -\log \sum_{x \in \mathcal{X}} P_X(x)^2$: Rényi entropy
- $F$ is chosen uniformly over the set of all mappings from $X$ to $\{0, 1\}^r$.

**Generalized Privacy Amplification:**

$$I(F(X) \land F) \leq \frac{2^r - R(X)}{\ln 2}.$$
Independence Properties of Random Mappings

C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer,
*Generalized privacy amplification*,

- Given $\mathcal{X}$-valued rv $X$.
- $R(X) = -\log \sum_{x \in \mathcal{X}} P_X(x)^2$: Rényi entropy
- $F$ is chosen uniformly over the set of all mappings from $X$ to $\{0, 1\}^r$.

**Generalized Privacy Amplification:**

$$I(F(X) \wedge F) \leq \frac{2^{r - R(X)}}{\ln 2}.$$ 

- $\Pr \left( \{y : R(X|Y = y) \geq c\} \right) \geq 1 - \delta$

$$I(F(X) \wedge F, Y) \leq \delta r + (1 - \delta) \left( \frac{2^{-(c-r)}}{\ln 2} \right).$$
Independence Properties of Random Mappings


\[ P \left( \left\{ x \in X : P(x) > \frac{1}{2d} \right\} \right) \leq \epsilon, \quad \forall P \in \mathcal{P}. \]

Balanced Coloring Lemma: Probability that a random mapping \( F : X \to \{1, \ldots, 2^r\} \) fails to satisfy for some \( P \in \mathcal{P} \)

\[ \sum_{i=1}^{2^r} \left| P(F(X) = i) - \frac{1}{2^r} \right| \leq 3\epsilon. \]

is less than

\[ \exp \left\{ r + \log(2N) - \left( \frac{\epsilon^2}{3} \right) 2^{(d-r)} \right\} \]

\[ X = X^n, \quad \mathcal{P} \equiv \text{family of distributions } P_{X^n|Y^n}(\cdot|y) \]
Sufficiency of $H(G) < H(X_M) - R_{CO}$


If $H(G) < H(X_M) - R_{CO}$:

Consider random mappings $F_i = F_i(X^n_i)$ of rates $R_i$ such that

$$\sum_{i \in B} R_i \geq H(X_B|X_{B^c}) , \quad B \subset M.$$  

- $F$ results in omniscience at all the terminals.
- $F$ is approximately independent of $G^n$.

We prove a multiterminal version of the balanced coloring lemma.
Sufficiency of $H(G) < H(X_M) - R_{CO}$


If $H(G) < H(X_M) - R_{CO}$:

Consider random mappings $F_i = F_i(X^n_i)$ of rates $R_i$ such that

$$\sum_{i \in B} R_i \geq H(X_B|X_{Bc}), \quad B \subsetneq M.$$  

- $F$ results in omniscience at all the terminals.
- $F$ is approximately independent of $G^n$.

C. Chan, Multiterminal secure source coding for a common secret source, Allerton 2011.

Proved a multiterminal version of privacy amplification.
Example: Secure Computation of Parity

\[ g(x_1, x_2) = x_1 \oplus x_2 \Rightarrow H(G) = h(\delta) \]

Sufficient condition for secure computing:

\[ H(G) < H(X_1, X_2) - R_{CO} \]
\[ \Leftrightarrow H(G') < I(X_1 \land X_2) = 1 - h(\delta). \]

\[ g \text{ is securely computable if} \]
\[ 2h(\delta) < 1 \]
Example: Secure Computation of Parity

- **Secure computability condition:** $h(\delta) < 1 - h(\delta)$
- **$P$:** parity check matrix of a linear SW code for $X_1$ given $X_2$
- $I(G^n \wedge X_1^n) = 0 \Rightarrow I(G^n \wedge F_1) = 0$.
- $K$: location of $X_1^n$ in the coset of the standard array (for $P$).
- Rate of $K = 1 - h(\delta)$.
- $I(K \wedge F_1) = 0$.
- $I(K \wedge F_1, G^n) = I(K \wedge F_1|G^n) = 0$
  - $P_{X^n}$ remains unchanged upon conditioning on $G^n$
- Use $K$ as one-time pad to send $\hat{G}^{(n)}$.

\[
\begin{array}{c}
X_1^n \\
X_2^n
\end{array}
\]
Example: Secure Computation of Parity

- Secure computability condition: \( h(\delta) < 1 - h(\delta) \)
- \( \mathbf{P} \): parity check matrix of a \textit{linear} SW code for \( X_1 \) given \( X_2 \)
- \( I(G_n \land X_1^n) = 0 \Rightarrow I(G_n \land F_1) = 0 \)
- \( K \): location of \( X_n^1 \) in the coset of the standard array (for \( P \)).
- Rate of \( K = 1 - h(\delta) \).
- \( I(K \land F_1) = 0 \).
- \( I(K \land F_1, G^n) = I(K \land F_1 | G^n) = 0 \)
- \( P_{X^n} \) remains unchanged upon conditioning on \( G^n \)
- Use \( K \) as one-time pad to send \( \hat{G}^{(n)} \).

\[
F_1 = PX_1^n
\]

A. D. Wyner

\textit{Recent Results in the Shannon Theory}

IT, 20, January 1974, pp. 2-10.
Example: Secure Computation of Parity

- Secure computability condition: $h(\delta) < 1 - h(\delta)$
- $P$: parity check matrix of a linear SW code for $X_1$ given $X_2$
- $I(G^n \land X_1^n) = 0 \Rightarrow I(G^n \land F_1) = 0$.
- $K$: location of $X_1^n$ in the coset of the standard array (for $P$).
- Rate of $K = 1 - h(\delta)$.
- $I(K \land F_1) = 0$.
- $I(K \land F_1, G^n) = I(K \land F_1 | G^n) = 0$
  - $P_{X^n}$ remains unchanged upon conditioning on $G^n$
- Use $K$ as one-time pad to send $\hat{G}^{(n)}$.

\[ F_1 = PX_1^n \]
Example: Secure Computation of Parity

- Secure computability condition: $h(\delta) < 1 - h(\delta)$
- $\mathbf{P}$: parity check matrix of a linear SW code for $X_1$ given $X_2$
- $I(G^n \land X_1^n) = 0 \Rightarrow I(G^n \land F_1) = 0$.
- $K$: location of $X_1^n$ in the coset of the standard array (for $\mathbf{P}$).
- Rate of $K = 1 - h(\delta)$.
- $I(K \land F_1) = 0$.

C. Ye and P. Narayan, *Secret key and private key constructions for simple multiterminal source models* IT, to appear in February 2012.

\[
F_1 = \mathbf{P}X_1^n
\]
Example: Secure Computation of Parity

- Secure computability condition: \( h(\delta) < 1 - h(\delta) \)
- \( P \): parity check matrix of a *linear* SW code for \( X_1 \) given \( X_2 \)
- \( I(G^n \land X_1^n) = 0 \Rightarrow I(G^n \land F_1) = 0. \)
- \( K \): location of \( X_1^n \) in the coset of the standard array (for \( P \)).
- Rate of \( K = 1 - h(\delta) \).
- \( I(K \land F_1) = 0. \)
- \( I(K \land F_1, G^n) = I(K \land F_1|G^n) = 0 \)
  - \( P_X^n \) remains unchanged upon conditioning on \( G^n \)
- Use \( K \) as one-time pad to send \( \hat{G}^{(n)} \).
Example: Secure Computation of Parity

- Secure computability condition: \( h(\delta) < 1 - h(\delta) \)
- \( P \): parity check matrix of a linear SW code for \( X_1 \) given \( X_2 \)
- \( I(G^n \land X_1^n) = 0 \Rightarrow I(G^n \land F_1) = 0. \)
- \( K \): location of \( X_1^n \) in the coset of the standard array (for \( P \)).
- Rate of \( K = 1 - h(\delta). \)
- \( I(K \land F_1) = 0. \)
- \( I(K \land F_1, G^n) = I(K \land F_1 | G^n) = 0 \)
  - \( P_{X^n} \) remains unchanged upon conditioning on \( G^n \)
- Use \( K \) as one-time pad to send \( \hat{G}^{(n)}. \)
$C = H(X) - R_C^0$

December 2004, pp. 3047 - 3061.

I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals, IT, 50(12),

C = H(X) − R_C^0$

Secret Key Generation

A Necessary Condition
A Necessary Condition

Secret Key Generation

\[ I(K \land F) \leq 0 \]

\[ \implies K: \text{Secret Key} \]

\[ \equiv F: \text{Public Communication} \]

\[ C = H(X_M) - R_{CO} \]

If \( g \) is securely computable,

\[ H(G) \leq C. \]
Theorem

If $g$ is securely computable: $H(G) \leq C$.

Conversely, $g$ is securely computable if: $H(G) < C$.

For a securely computable function $g$:

- Omniscience can be obtained using $F \perp \tilde{\sim} G^n$.
- Noninteractive communication suffices.
- Randomization is not needed.
Outline of the Talk

Function computation

Secure function computation

Common randomness for secret key generation

Computing without revealing the critical data
Common Randomness


\[ \Pr (L = L_1 = L_2) \geq 1 - \epsilon \]
Common Randomness


$L$ forms a CR if $L$ is $\epsilon$-recoverable from $F$:

$$\Pr (L = L_1 = L_2) \geq 1 - \epsilon$$

P. Gács and J. Körner, Common information is far less than mutual information, Problems of Control and Information Theory, 2(2), 1973, pp: 149-162.

- In general, CR rate is zero without public communication
Secret Key Generation

U. Maurer, *Secret key agreement by public discussion*, IT, 39(3), May 1993, pp. 733 - 742.


\[
\frac{1}{n} I(F \wedge K) \approx 0: \text{Weak Secrecy}
\]

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

Secret key capacity \( C = I(X \wedge Y) \)
What is the form of CR that yields an optimum rate SK?

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

- **Csiszár-Narayan**
  - *Common randomness* generated: $X^n, Y^n$ (*Omniscience*)
  - Rate of communication required $= H(X|Y) + H(Y|X)$
  - Decomposition:
    \[
    H(X, Y) = H(X|Y) + H(Y|X) + I(X \land Y)
    \]

Lemma (Characterization of CR for generating an optimum rate SK)

A CR $J$ recoverable from communication $F$ yields an optimum rate SK if and only if

$$\frac{1}{n} I(X^n \land Y^n | J, F) \approx 0.$$ 

- **Optimal rate of SK generated:** $\frac{1}{n} H(J|F)$

**Necessity:** If CR $J$ is generated to establish an SK $K$ and

$$\frac{1}{n} I(X^n \land Y^n | J, F) > 0,$$

$\Rightarrow$ there exists an SK $K'$ of positive rate and independent of $(J, F)$.

**Sufficiency:**

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

$$\leq \frac{1}{n} \left[ I(X^n \land Y^n | J, F') + H(J|F) \right]$$
Common Randomness for SK Capacity

Lemma (Characterization of CR for generating an optimum rate SK)

A CR $J$ recoverable from communication $F$ yields an optimum rate SK if and only if

$$\frac{1}{n} I (X^n \land Y^n | J, F) \approx 0.$$ 

What is the minimum rate of CR for optimum rate SK generation?

Interactive common information
Wyner's Common Information

In the context of source coding:

\[ CI(X \wedge Y) := \min_{R_0 + R_1 + R_2 \leq H(X,Y)} R_0 = \min_{X \oplus W \oplus Y} I(W \wedge X, Y). \]

Simple bound on CI: \( I(X \wedge Y) \leq CI(X \wedge Y) \leq \min\{H(X), H(Y)\}. \)
Wyner’s Common Information

In the context of source generation:

\[ D \left( P_{X^n,Y^n} || P_{\hat{X}^n,\hat{Y}^n} \right) \approx 0 \]

\[ CI(X \land Y) := \min R_0 \]
Interactive Common Information

- Wyner’s Common Information

\[ CI(X \land Y) \equiv \min \text{ rate of a function } L = L(X^n, Y^n) \text{ such that } \frac{1}{n} I(X^n \land Y^n|L) \approx 0. \]
Interactive Common Information

- **Wyner’s Common Information**

\[
CI(X \land Y) \equiv \min \text{ rate of a function } L = L(X^n, Y^n) \text{ such that } \\
\frac{1}{n} I(X^n \land Y^n | L) \approx 0.
\]

- **Interactive Common Information**

Terminals agree on CR $J$ using $r$ rounds of communication $F$. 

\[
CI^r_i(X; Y) \equiv \min \text{ rate of } (J, F) \text{ such that } \\
\frac{1}{n} I(X^n \land Y^n | J, F) \approx 0.
\]

\[
CI_i(X \land Y) := \lim_{r \to \infty} CI^r_i(X; Y)
\]

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

Common Information Quantities

For a pair of rvs $X, Y$

$$CI_{GC} \leq I(X \land Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X), H(Y)\}$$
Common Information Quantities

For a pair of rvs $X, Y$

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

$$C_{IGC} \leq I(X \land Y) \leq CI \leq CI_r \leq CI_r^{-1} \leq \min\{H(X), H(Y)\}$$
Common Information Quantities

For a pair of rvs $X, Y$

\[
CI_{GC} \leq I(X \land Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X), H(Y)\}
\]
Common Information Quantities

For a pair of rvs $X, Y$

\[
CI_{GC} \leq I(X \land Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X), H(Y)\}
\]

Interactive Common Information

- $CI_i$ is indeed a new quantity:

  For binary symmetric $X, Y$
  \[
  CI_i(X \land Y) = \min\{H(X), H(Y)\}
  
  CI(X \land Y) < \min\{H(X), H(Y)\}
  \]
Application: Minimum Communication for Optimum Rate SK

CR \((J, F)\) yields an optimum rate SK if and only if

\[
\frac{1}{n} I(X^n \land Y^n | J, F) \approx 0.
\]

\[\Rightarrow \text{It suffices to characterize minimum rate of the communication above.}\]

**Theorem**

*For \(r\)-round interactive communication \(F\) let*

\[CI^r_i = \text{min. rate of } (J, F) \text{ s.t. } X^n \perp \perp Y^n | (J, F),\]

\[R^r_{SK} = \text{min. rate of } F \text{ required for optimal rate SK generation},\]

\[R^r_{CI} = \text{min. rate of } F \text{ required for generating } \text{CR } J \text{ s.t. } X^n \perp \perp Y^n | (J, F),\]

*Then,*

\[R^r_{SK} = R^r_{CI} = CI^r_i(X; Y) - I(X \land Y).\]

*A single letter characterization of \(CI^r_i\) is available.*
Application: Minimum Communication for Optimum Rate SK

CR \((J, F)\) yields an optimum rate SK if and only if

\[
\frac{1}{n} I(X^n \land Y^n | J, F) \approx 0.
\]

⇒ It suffices to characterize minimum rate of the communication above.

**Theorem**

For \(r\)-round interactive communication \(F\) let

\[CI_i^r = \text{min. rate of } (J, F) \text{ s.t. } X^n \Downarrow \sim Y^n | (J, F),\]

\[R_{SK}^r = \text{min. rate of } F \text{ required for optimal rate SK generation},\]

\[R_{CI}^r = \text{min. rate of } F \text{ required for generating CR } J \text{ s.t. } X^n \Downarrow \sim Y^n | (J, F),\]

Then,

\[R_{SK}^r = R_{CI}^r = CI_i^r (X; Y) - I(X \land Y).\]

Taking limit \(r \rightarrow \infty:\)

\[R_{SK} = R_{CI} = CI_i(X \land Y) - I(X \land Y)\]
Outline of the Talk

Function computation

Secure function computation

Common randomness for secret key generation

Computing without revealing the critical data
Critical data: $g_0(X_M)$.

Secure computability of $g_M = (g_0, g_1, ..., g_m)$:

Recoverability: $\Pr \left( G_i^{(n)} = g_i(X_M^n), 1 \leq i \leq m \right) \approx 1$

Security: $I(g_0(X_M^n) \land F) \approx 0$

When is a given function $g_M$ securely computable?
Application to Binary Symmetric Sources

\[
\begin{align*}
\Pr(X_1 = 1) &= \frac{1}{2} \\
\Pr(X_1 \neq X_2) &= \delta
\end{align*}
\]

<table>
<thead>
<tr>
<th>( g_0 )</th>
<th>( g_1 )</th>
<th>( g_2 )</th>
<th>SC condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( h(\delta) &lt; \frac{1}{2} )</td>
</tr>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( \phi )</td>
<td>( h(\delta) &lt; 1 )</td>
</tr>
<tr>
<td>( X_1 \oplus X_2, X_1.X_2 )</td>
<td>( X_1 \oplus X_2, X_1.X_2 )</td>
<td>( X_1.X_2 )</td>
<td>( h(\delta) &lt; \frac{1}{3} )</td>
</tr>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1.X_2 )</td>
<td>( h(\delta) &lt; \frac{2}{3} )</td>
</tr>
</tbody>
</table>
In Closing ...

- Identify the form of CR established
- Restrictions on the CR established:
  - *Function computation:* $G^n$ is recoverable from $L$.
  - *Optimum rate SK generation:* CR renders $X^n$ and $Y^n$ conditionally independent.
- Restrictions on the communication:
  - *Secure function computation:* $G^n$ is independent of $F$.
  - *Secret key generation:* $K \equiv CR$ bits independent of $F$.

Can the study of CR generated lead to a better understanding of computation over networks?