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

Processing of Distributed Data

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.

Processing of Distributed Data

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:

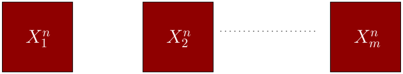
  Computing a function of the data

  - using communication independent of the function value.

- Secret key generation

  Share bits using communication independent of the function value.

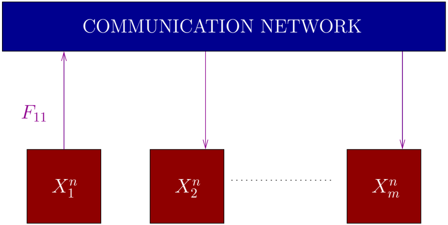
Multiterminal Source Model



Assumption on the data

1. $X_i^n = (X_{i1}, ..., X_{in})$
   - Data observed at time instance t: $X_{\mathcal{M}t} = (X_{1t}, ..., X_{mt})$
   - probability distribution of $X_1, ..., X_m$ is known.
2. Observations are i.i.d. across time:
   - $X_{\mathcal{M}1}, ..., X_{\mathcal{M}n}$ are i.i.d. rvs.
3. Observations are finite-valued.

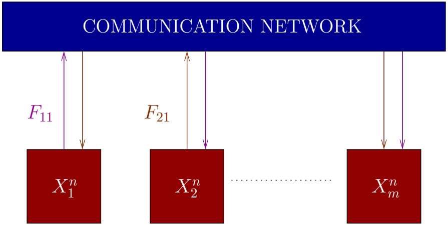
Interactive Communication Protocol



Assumptions on the protocol

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

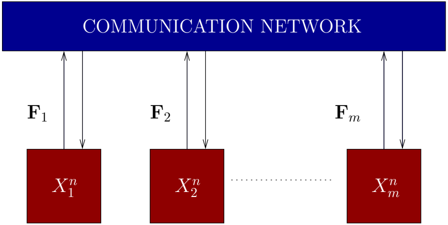
Interactive Communication Protocol



Assumptions on the protocol

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

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: $\mathbf{F} = \mathbf{F}_1, ..., \mathbf{F}_m$

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

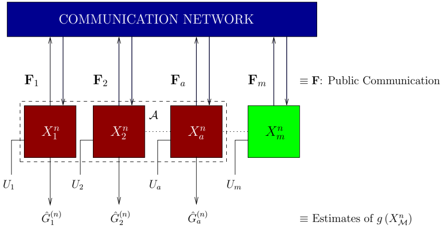
Function computation

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:

$$g\left(X_{\mathcal{M}}^n\right) = \left(g\left(X_{\mathcal{M}1}\right), ..., g\left(X_{\mathcal{M}n}\right)\right).$$

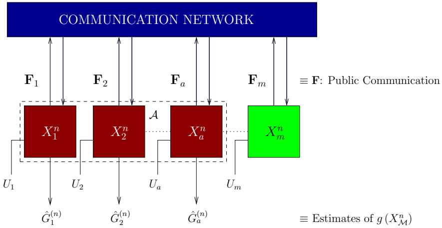
- Notation: $G = g\left(X_{\mathcal{M}}\right), \quad G^n = \left(g\left(X_{\mathcal{M}1}\right), ..., g\left(X_{\mathcal{M}n}\right)\right)$

Recoverability:

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

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

Computing a Function of Distributed Data



Recoverability:

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

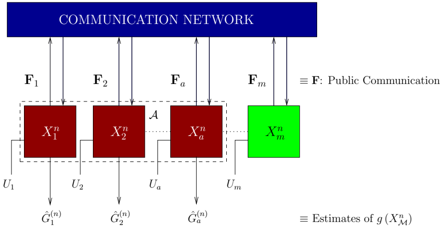
What is the minimum rate of communication $\frac{1}{n} \log \|\mathbf{F}\|$ needed?

A. C. Yao

Some complexity questions related to distributive computing

STOC '79

Computing a Function of Distributed Data



Recoverability:

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

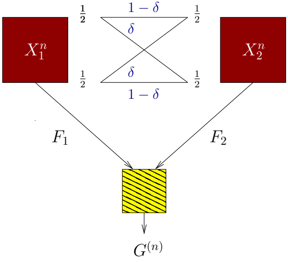
What is the minimum rate of communication $\frac{1}{n} \log \|\mathbf{F}\|$ needed?


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

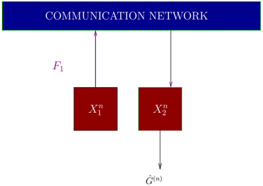
The rate region of communication for computing parity is given by

$$\{(R_1, R_2) : R_1 \geq h(\delta), \quad R_2 \geq h(\delta)\}.$$

Special Case: Orlitsky-Roche

Function Computation
Secure Computing
CR for SK Generation
General Secure Computing


A. Orlitsky and J. R. Roche, Coding for computing, IT, 47(3), March 2001, pp. 903-917.



Theorem

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

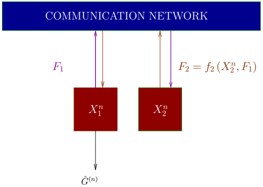
$$\min_{W -\!\circ\!- X_1 -\!\circ\!- X_2} I\left(W \wedge X_1 | X_2\right)$$

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

Special Case: Orlitsky-Roche

A. Orlitsky and J. R. Roche, Coding for computing, IT, 47(3), March 2001, pp. 903-917.



Theorem

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

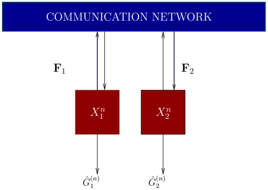
$$\Big\{ (R_1, R_2) : R_1 \geq I(U \wedge X_1 | X_2), \quad R_2 \geq I(V \wedge X_2 | X_1, U)$$

$$U -\!\!\circ\!\!- X_1 -\!\!\circ\!\!- X_2, \quad V -\!\!\circ\!\!- X_2, U -\!\!\circ\!\!- X_1 \quad \text{and} \quad H(G | U, V, X_1) = 0 \Big\}.$$

Special Case: Orlitsky-Roche

Extensions:

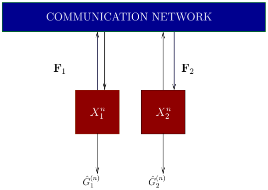
- N. Ma and P. Ishwar, Some results on distributed source coding for interactive function computation, IT, 57(9), September 2011, pp. 6180-6195.
- N. Ma and P. Ishwar, Infinite-message distributed source coding for interactive function computation, arXiv:0908.3512v2.



Special Case: Orlitsky-Roche

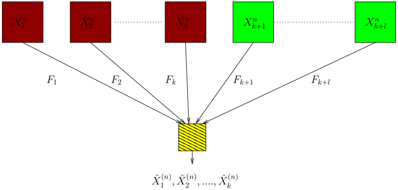
Extensions:

- N. Ma and P. Ishwar, Some results on distributed source coding for interactive function computation, IT, 57(9), September 2011, pp. 6180-6195.
- N. Ma and P. Ishwar, Infinite-message distributed source coding for interactive function computation, arXiv:0908.3512v2.



How many rounds of interaction are optimal?

Function Computation and Helper Problems



l helpers, $k+l$ terminals

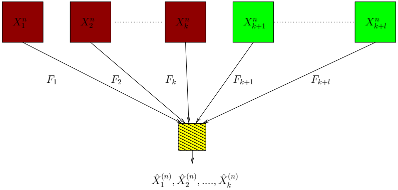

I. Csiszár and J. Körner, Towards a general theory of source networks, IT, 26(2), March 1980, pp. 155-165.

Theorem (No-helper problem)

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

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

Function Computation and Helper Problems



l helpers, $k+l$ terminals


I. Csiszár and J. Körner, Towards a general theory of source networks, IT, 26(2), March 1980, pp. 155-165.

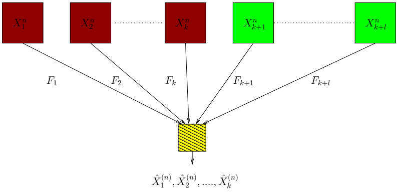
Theorem

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

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

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

Function Computation and Helper Problems



l helpers, $k + l$ terminals

T. S. Han and K. Kobayashi, A unified achievable rate region for a general class of multiterminal source coding systems, IT, 26(3), May 1980, pp. 277-288.

Function Computation and Helper Problems


I. Csiszár and J. Körner, Towards a general theory of source networks, IT, 26(2), March 1980, pp. 155-165.

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

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

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

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

Function Computation and Helper Problems

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

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

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

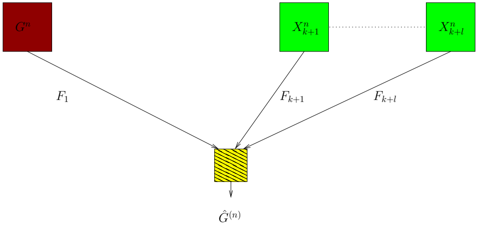
Here $Z_1, \ldots, Z_q$ correspond to the helper sources.

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

Most general achievable region for 1 helper problem:

J. Körner, "OPEC or a basic problem in source networks," IT, 30(1), January 1984, pp. 68 - 77.

Function Computation and Helper Problems



Function computation as a helper problem

- One of the encoders knows the function value $\Rightarrow$ 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?

Outline of the Talk

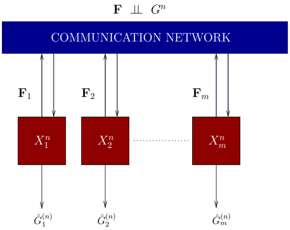
Function computation

Secure function computation

Common randomness for secret key generation

Computing without revealing the critical data

Secure Computing of Functions



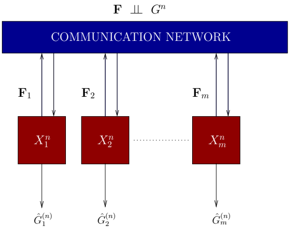
- $\hat{G}_i^{(n)}$ is the estimate of G^n at terminal i.

Secure computability of g:

$$\textit{Recoverability}: \quad \Pr\left(G_i^{(n)} = G^n, i \in \mathcal{M}\right) \geq 1 - \epsilon$$
$$\textit{Secrecy}: \quad I\left(G^n \wedge \mathbf{F}\right) \leq \epsilon$$

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:

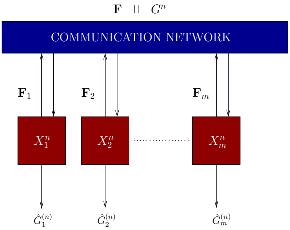
$$\textit{Recoverability}: \quad \Pr\left(G_i^{(n)} = G^n, i \in \mathcal{M}\right) \geq 1 - \epsilon$$

$$\textit{Secrecy}: \quad I\left(G^n \wedge \mathbf{F}\right) \leq \epsilon$$

Deterministic Model:

A. Orlitsky and A. El Gamal, Communication with secrecy constraints, STOC '84.

Secure Computing of Functions



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

Secure computability of g:

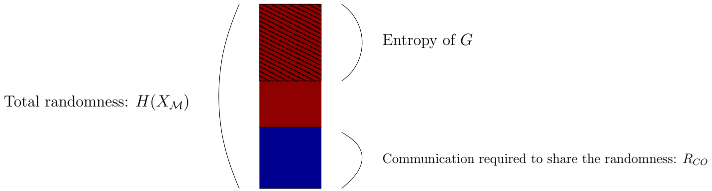
$$\begin{aligned} &Recoverability: && \Pr\left(G_i^{(n)} = G^n, i \in \mathcal{M}\right) \geq 1 - \epsilon \\ &Secrecy: && I\left(G^n \wedge \mathbf{F}\right) \leq \epsilon \end{aligned}$$

When is a given function g securely computable?

H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?," IT, 57(10), October 2011, pp. 6337-6350.

A Sufficient Condition

- Share all data to compute g: Omniscience $\equiv X^n_{\mathcal{M}}$
- Can we attain omniscience using $\mathbf{F} \underset{\sim}{\perp\!\!\!\perp} G^n$?



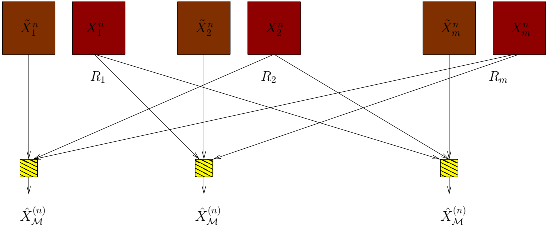
Claim: Omniscience can be attained using $\mathbf{F} \underset{\sim}{\perp\!\!\!\perp} G^n$ if:

$$H(G) < H\left(X_{\mathcal{M}}\right) - R_{CO}$$

.

Random Mappings For Omniscience


I. Csiszár and P. Narayan, Secrecy capacities for multiple terminals , IT, 50(12), December 2004, pp. 3047 - 3061.

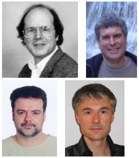


- $F_i = F_i\left(X_i^n\right)$: random mapping of rate R_i.
- With large probability, $F_1, \ldots, F_m$ result in omniscience if:

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

- $R_{CO} = \min \sum_{i \in \mathcal{M}} R_i$.

Independence Properties of Random Mappings



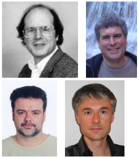
C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer,
Generalized privacy amplification,
IT, 41(6), November 1995, pp. 1915-1923.

- 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:

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

Independence Properties of Random Mappings



C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer,
Generalized privacy amplification,
IT, 41(6), November 1995, pp. 1915-1923.

- 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:

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

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

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

Independence Properties of Random Mappings

R. Ahlswede and I. Csiszár, Common randomness in information theory and cryptography. ii. CR capacity, IT, 44(1), January 1998, pp. 225 - 240.

- $\mathcal{P}$ be a family of N pmfs on $\mathcal{X}$ s.t.

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

Balanced Coloring Lemma: Probability that a random mapping $F : \mathcal{X} \to \{1, ..., 2^r\}$ 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

$$\exp\left\{r + \log(2N) - \left(\epsilon^2/3\right) 2^{(d-r)}\right\}$$

- $X = X^n, \quad \mathcal{P} \equiv$ family of distributions $P_{X^n|Y^n}(\cdot|\mathbf{y})$

Sufficiency of $H(G) < H(X_{\mathcal{M}}) - R_{CO}$

H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?," IT, 57(10), October 2011, pp. 6337-6350.

If $H(G) < H(X_{\mathcal{M}}) - R_{CO}$:

Consider random mappings $F_i = F_i(X_i^n)$ of rates R_i such that

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

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

We prove a multiterminal version of the balanced coloring lemma.

Sufficiency of $H(G) < H(X_{\mathcal{M}}) - R_{CO}$

H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?," IT, 57(10), October 2011, pp. 6337-6350.

If $H(G) < H(X_{\mathcal{M}}) - R_{CO}$:

Consider random mappings $F_i = F_i(X_i^n)$ of rates R_i such that

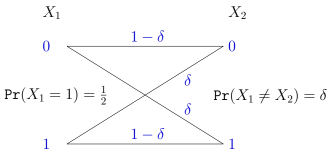
$$\sum_{i \in B} R_i \geq H(X_B | X_{B^c}), \quad B \subsetneq \mathcal{M}.$$

- $\mathbf{F}$ results in omniscience at all the terminals.
- $\mathbf{F}$ 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 conditon for secure computing:

$$H(G) < H\left(X_1, X_2\right) - R_{CO}$$
$$\Leftrightarrow H(G) < I\left(X_1 \wedge X_2\right) = 1 - h(\delta).$$

- g is securely computable if

$$2h(\delta) < 1$$

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
- $I(G^n \wedge X_1^n) = 0 \Rightarrow I(G^n \wedge F_1) = 0.$
- K: location of X_1^n in the coset of the standard array (for $\mathbf{P}$).
- Rate of $K = 1 - h(\delta)$.
- $I(K \wedge F_1) = 0.$
- $I\left(K \wedge F_1, G^n\right) = I\left(K \wedge F_1 | G^n\right) = 0$
  - P_{X^n} remains unchanged upon conditioning on G^n
- Use K as one-time pad to send $\hat{G}^{(n)}$.

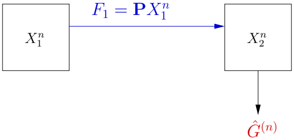
Example: Secure Computation of Parity

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

A. D. Wyner

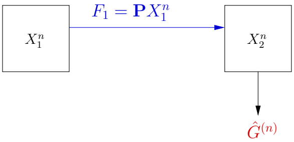
Recent Results in the Shannon Theory

IT, 20, January 1974, pp. 2-10.



Example: Secure Computation of Parity

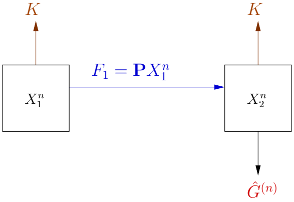
- Secure computability condition: $h(\delta) < 1 - h(\delta)$
- $\mathbf{P}$: parity check matrix of a *linear* SW code for X_1 given X_2
- $I(G^n \wedge X_1^n) = 0 \Rightarrow I(G^n \wedge F_1) = 0.$
- K: location of X_1^n in the coset of the standard array (for $\mathbf{P}$).
- Rate of $K = 1 - h(\delta)$.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

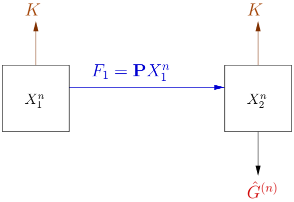
- Secure computability condition: $h(\delta) < 1 - h(\delta)$
- $\mathbf{P}$: parity check matrix of a *linear* SW code for X_1 given X_2
- $I(G^n \wedge X_1^n) = 0 \Rightarrow I(G^n \wedge F_1) = 0.$
- K: location of X_1^n in the coset of the standard array (for $\mathbf{P}$).
- Rate of $K = 1 - h(\delta)$.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


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



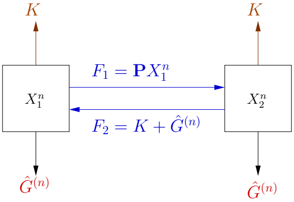
Example: Secure Computation of Parity

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



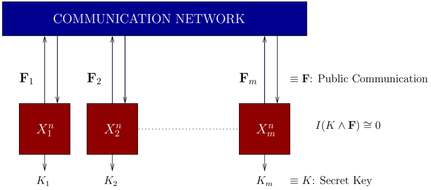
Example: Secure Computation of Parity

- Secure computability condition: $h(\delta) < 1 - h(\delta)$
- $\mathbf{P}$: 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 $\mathbf{P}$).
- Rate of $K = 1 - h(\delta)$.
- $I(K \wedge F_1) = 0.$
- $I\left(K \wedge F_1, G^n\right) = I\left(K \wedge F_1 | G^n\right) = 0$
  - P_{X^n} remains unchanged upon conditioning on G^n
- Use K as one-time pad to send $\hat{G}^{(n)}$.



A Necessary Condition

Secret Key Generation

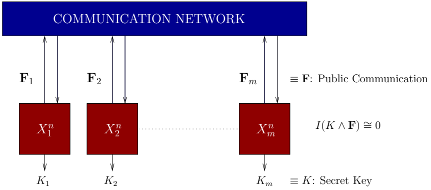


- I. Csiszár and P. Narayan, Secrecy capacities for multiple terminals, IT, 50(12), December 2004, pp. 3047 - 3061.

$$C = H\left(X_{\mathcal{M}}\right) - R_{CO}$$

A Necessary Condition

Secret Key Generation



- I. Csiszár and P. Narayan, Secrecy capacities for multiple terminals, IT, 50(12), December 2004, pp. 3047 - 3061.

$$C = H\left(X_{\mathcal{M}}\right) - R_{CO}$$

If g is securely computable,

$$H(G) \leq C.$$

Characterization of Securely Computable Functions

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 $\mathbf{F} \underset{\sim}{\perp\!\!\!\perp} G^n$.*
- *Noninteractive communication suffices.*
- *Randomization is not needed.*

Outline of the Talk

Function computation

Secure function computation

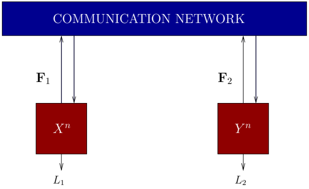
Common randomness for secret key generation

Computing without revealing the critical data

Common Randomness

Function Computation
Secure Computing
CR for SK Generation
General Secure Computing

R. Ahlswede and I. Csiszár, Common randomness in information theory and cryptography. ii. CR capacity, IT, 44(1), January 1998, pp. 225 - 240.

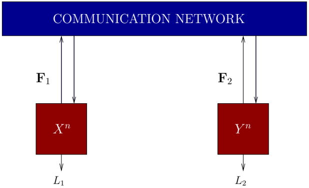


L forms a CR if L is ϵ-*recoverable* from $\mathbf{F}$:

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

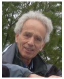
Common Randomness

R. Ahlswede and I. Csiszár, Common randomness in information theory and cryptography. ii. CR capacity, IT, 44(1), January 1998, pp. 225 - 240.



L forms a CR if L is ϵ-*recoverable* from $\mathbf{F}$:

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

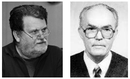


P. Gács and J. Körner, Common information is far less than mutual information, Problems of Control and Informaton Theory, 2(2), 1973, pp: 149-162.

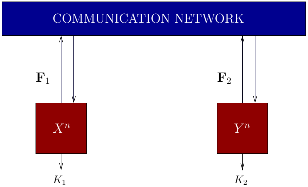
- In general, CR rate is zero without public communication

Secret Key Generation

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



R. Ahlswede and I. Csiszár, Common randomness in information theory and cryptography. i. secret sharing, IT, 39(4) , July 1993, pp. 1121 - 1132.



$\frac{1}{n} I(\mathbf{F} \wedge K) \approx 0$: Weak Secrecy

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

Secret key capacity $C = I(X \wedge Y)$

Common Randomness for SK Capacity

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

Himanshu Tyagi, Minimal public communication for maximum rate secret key generation, ISIT 2011.

Common Randomness for SK Capacity

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

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

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

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

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

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

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

Sufficiency:

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

Common Randomness for SK Capacity

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

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

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

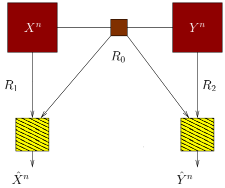
What is the minimum rate of CR for optimum rate SK generation?

Interactive common information

Function Computation
Secure Computing
CR for SK Generation
General Secure Computing

Interactive Common Information

- Wyner's Common Information
  In the context of source coding:



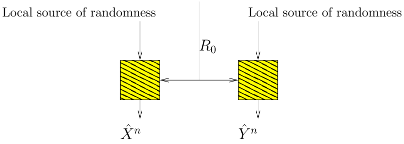
$$CI(X \wedge Y) := \min_{R_0+R_1+R_2 \leq H(X,Y)} R_0 = \min_{X -\!\circ\!- W -\!\circ\!- Y} I(W \wedge X, Y).$$

Simple bound on CI: $I(X \wedge Y) \leq CI(X \wedge Y) \leq \min\{H(X), H(Y)\}$.

Interactive Common Information

- Wyner's Common Information

  In the context of source generation:



$$D\left(\mathrm{P}_{X^n,Y^n} || \mathrm{P}_{\hat{X}^n,\hat{Y}^n}\right) \approx 0$$

$$CI(X \wedge Y) := \min R_0$$

Interactive Common Information

- Wyner's Common Information

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

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

Interactive Common Information

- Wyner's Common Information

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

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

- Interactive Common Information

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

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

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

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

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

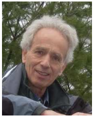
Common Information Quantities

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

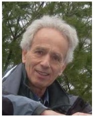
For a pair of rvs X, Y

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

Common Information Quantities

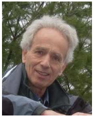
For a pair of rvs X, Y



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

Common Information Quantities

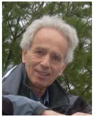
For a pair of rvs X, Y



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

Common Information Quantities

For a pair of rvs X, Y

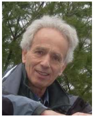


$$CI_{GC} \leq I(X \wedge Y) \leq CI \leq CI_i \leq CI_i^r \leq CI_i^{r-1} \leq \min\{H(X), H(Y)\}$$

Interactive Common Information

Common Information Quantities

For a pair of rvs X, Y



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

Interactive Common Information

- CI_i is indeed a new quantity:

  For binary symmetric X, Y

$$CI_i(X \wedge Y) = \min\{H(X), H(Y)\}$$
$$CI(X \wedge Y) < \min\{H(X), H(Y)\}$$

Application: Minimum Communication for Optimum Rate SK

CR $(J, \mathbf{F})$ yields an optimum rate SK if and only if

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

$\Rightarrow$ It suffices to characterize minimum rate of the communication above.

Theorem

For r-round interactive communication $\mathbf{F}$ let

$CI_i^r =$ *min. rate of* $(J, \mathbf{F})$ *s.t.* $X^n \underset{\sim}{\perp\!\!\!\perp} Y^n | (J, \mathbf{F})$,

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

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

Then,

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

A single letter characterization of CI_i^r is available.

Application: Minimum Communication for Optimum Rate SK

CR $(J, \mathbf{F})$ yields an optimum rate SK if and only if

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

$\Rightarrow$ It suffices to characterize minimum rate of the communication above.

Theorem

For r-round interactive communication $\mathbf{F}$ let

CI_i^r = *min. rate of* $(J, \mathbf{F})$ *s.t.* $X^n \underset{\sim}{\perp\!\!\!\perp} Y^n | (J, \mathbf{F})$,

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

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

Then,

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

Taking limit $r \to \infty$:

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

Outline of the Talk

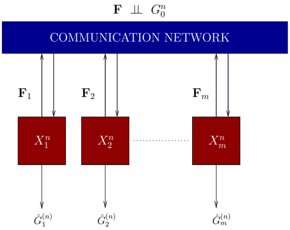
Function computation

Secure function computation

Common randomness for secret key generation

Computing without revealing the critical data

Computing Without Revealing Critical Data



- Critical data: $g_0\left(X_{\mathcal{M}}\right)$.
- *Secure computability* of $g_{\mathcal{M}} = (g_0, g_1, ..., g_m)$:

$$\text{Recoverability :} \quad \Pr\left(G_i^{(n)} = g_i\left(X_{\mathcal{M}}^n\right), 1 \leq i \leq m\right) \approx 1$$

$$\text{Security :} \quad I\left(g_0\left(X_{\mathcal{M}}^n\right) \wedge \mathbf{F}\right) \approx 0$$

When is a given function $g_{\mathcal{M}}$ securely computable?

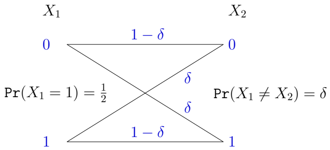
Function Computation

Secure Computing

CR for SK Generation

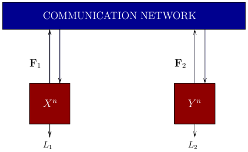
General Secure Computing

Application to Binary Symmetric Sources



g_0	g_1	g_2	SC condition
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1 \oplus X_2$	$h(\delta) < 1/2$
$X_1 \oplus X_2$	$X_1 \oplus X_2$	ϕ	$h(\delta) < 1$
$X_1 \oplus X_2, \ X_1.X_2$	$X_1 \oplus X_2, \ X_1.X_2$	$X_1.X_2$	$h(\delta) < 1/3$
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1.X_2$	$h(\delta) < 2/3$

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 $\mathbf{F}$.
  - *Secret key generation:* $K \equiv$ CR bits independent of $\mathbf{F}$.

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