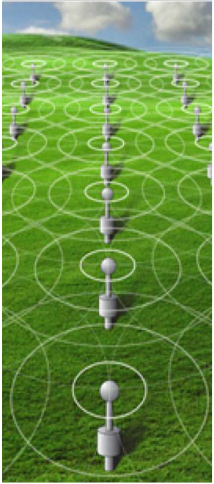
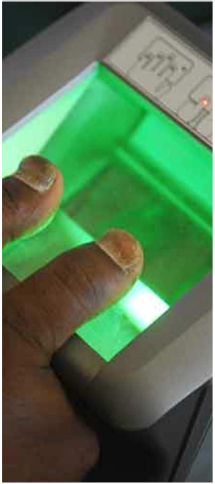
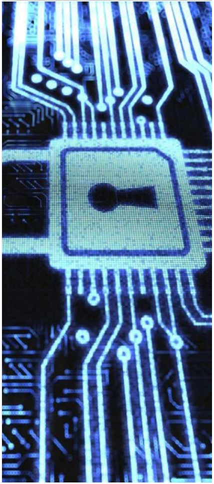
Common Randomness Principles of Secrecy

Himanshu Tyagi

Department of Electrical and Computer Engineering
and Institute of Systems Research

Correlated Data, Distributed in Space and Time

Sensor Networks	Cloud Computing	Biometric Security	Hardware Security
			

Secure Processing of Distributed Data

Three classes of problems are studied:

1. Secure Function Computation with Trusted Parties
2. Communication Requirements for Secret Key Generation
3. Querying Eavesdropper

Secure Processing of Distributed Data

Three classes of problems are studied:

1. Secure Function Computation with Trusted Parties
2. Communication Requirements for Secret Key Generation
3. Querying Eavesdropper

Our Approach

- Identify the underlying *common randomness*
- Decompose common randomness into independent components

Outline

1. Basic Concepts
2. Secure Computation
3. Minimal Communication for Optimum Rate Secret Keys
4. Querying Common Randomness
5. Principles of Secrecy Generation

Basic Concepts

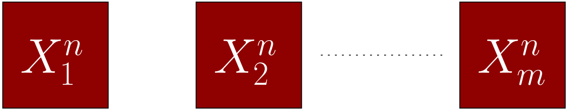
Multiterminal Source Model

Interactive Communication Protocol

Common Randomness

Secret Key

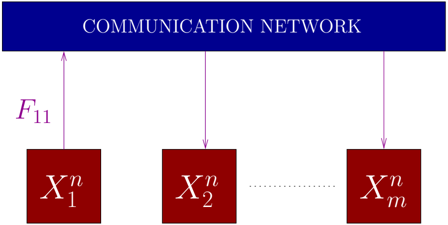
Multiterminal Source Model



Assumption on the data

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

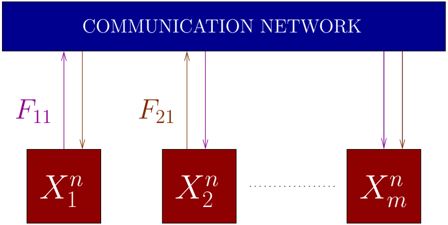
Interactive Communication Protocol



Assumptions on the protocol

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

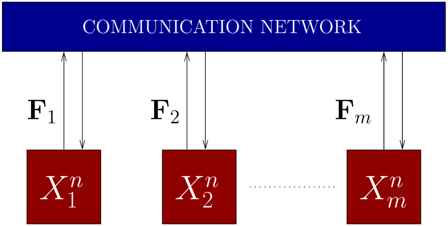
Interactive Communication Protocol



Assumptions on the protocol

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

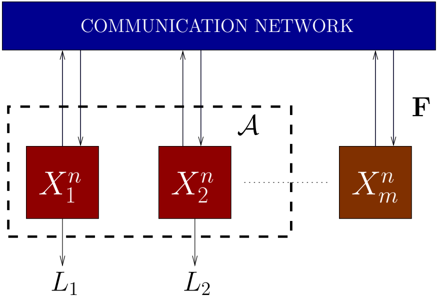
Interactive Communication Protocol



Assumptions on the protocol

- Each terminal has access to all the communication.
- Multiple rounds of interactive communication are allowed.
- r rounds of interactive communication: $\mathbf{F} = \mathbf{F}_1, ..., \mathbf{F}_m$

Common Randomness

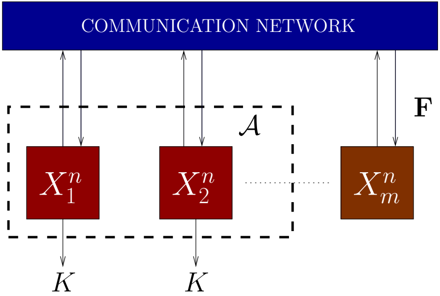


Definition. L is an ϵ-common randomness for $\mathcal{A}$ from $\mathbf{F}$ if

$$\mathrm{P}\left(L = L_i(X_i^n, \mathbf{F}),\ i \in \mathcal{A}\right) \geq 1 - \epsilon$$

Ahlswede-Csiszár '93 and '98.

Secret Key

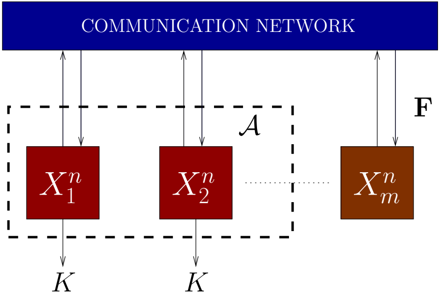


Definition. An rv $K \in \mathcal{K}$ is an ϵ-secret key for $\mathcal{A}$ from $\mathbf{F}$ if

1. *Recoverability:* K is an ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$
2. *Security:* K is concealed from an observer of $\mathbf{F}$

Maurer '93 Ahlswede-Csiszár '93 Csiszár-Narayan '04.

Secret Key



Definition. An rv $K \in \mathcal{K}$ is an ϵ-secret key for $\mathcal{A}$ from $\mathbf{F}$ if

1. *Recoverability:* K is an ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$
2. *Security:* K is concealed from an observer of $\mathbf{F}$

$$\mathrm{P}_{K\mathbf{F}} \approx U_{\mathcal{K}} \times \mathrm{P}_{\mathbf{F}}$$

Maurer '93 Ahlswede-Csiszár '93 Csiszár-Narayan '04.

Notions of Security

- Kullback-Leibler Divergence

$$\begin{aligned} s_{in}(K, \mathbf{F}) &= D\left(\mathrm{P}_{K\mathbf{F}} \| U_{\mathcal{K}} \times \mathrm{P}_{\mathbf{F}}\right) \\ &= \log|\mathcal{K}| - H(K) + I(K \wedge \mathbf{F}) \approx 0 \end{aligned}$$

- Variational Distance

$$s_{var}(K, \mathbf{F}) = \left\| \mathrm{P}_{K\mathbf{F}} - U_{\mathcal{K}} \times \mathrm{P}_{\mathbf{F}} \right\|_1 \approx 0$$

- Weak

$$s_{weak}(K, \mathbf{F}) = \frac{1}{n} s_{in}(K, \mathbf{F}) \approx 0$$

Notions of Security

- Kullback-Leibler Divergence

$$\begin{aligned} s_{in}(K, \mathbf{F}) &= D\left(\mathrm{P}_{K\mathbf{F}} \| U_{\mathcal{K}} \times \mathrm{P}_{\mathbf{F}}\right) \\ &= \log|\mathcal{K}| - H(K) + I(K \wedge \mathbf{F}) \approx 0 \end{aligned}$$

- Variational Distance

$$s_{var}(K, \mathbf{F}) = \|\mathrm{P}_{K\mathbf{F}} - U_{\mathcal{K}} \times \mathrm{P}_{\mathbf{F}}\|_1 \approx 0$$

- Weak

$$s_{weak}(K, \mathbf{F}) = \frac{1}{n} s_{in}(K, \mathbf{F}) \approx 0$$

$$2\, s_{var}(K, \mathbf{F})^2 \leq s_{in}(K, \mathbf{F}) \leq s_{var}(K, \mathbf{F}) \log \frac{|\mathcal{K}|}{s_{var}(K, \mathbf{F})}$$

Secret Key Capacity

Definition. An rv $K \in \mathcal{K}$ is an ϵ-secret key for $\mathcal{A}$ from $\mathbf{F}$ if

1. *Recoverability:* K is an ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$
2. *Security:* $s(K, \mathbf{F}) \to 0$ as $n \to \infty$

Secret Key Capacity

Definition. An rv $K \in \mathcal{K}$ is an ϵ-secret key for $\mathcal{A}$ from $\mathbf{F}$ if

1. *Recoverability:* K is an ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$
2. *Security:* $s(K, \mathbf{F}) \to 0$ as $n \to \infty$

Rate of $K \equiv \frac{1}{n} \log |\mathcal{K}|$

Secret Key Capacity

Definition. An rv $K \in \mathcal{K}$ is an ϵ-secret key for $\mathcal{A}$ from $\mathbf{F}$ if

1. *Recoverability:* K is an ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$
2. *Security:* $s(K, \mathbf{F}) \to 0$ as $n \to \infty$

Rate of $K \equiv \frac{1}{n} \log |\mathcal{K}|$

- ϵ-SK capacity $C(\epsilon) =$ supremum over the rates of ϵ-SKs
- SK capacity $C = \inf_{0<\epsilon<1} C(\epsilon)$

Secret Key Capacity

Theorem (Csiszár-Narayan '04)

The SK capacity is given by

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

where

$$R_{CO} = \min \sum_{i=1}^{m} R_i,$$

such that $\sum_{i \in B} R_i \geq H\left(X_B \mid X_{B^c}\right)$, *for all* $\mathcal{A} \nsubseteq B \subseteq \mathcal{M}$.

Secret Key Capacity

$R_{CO} \equiv$ min. rate of "communication for omniscience" for $\mathcal{A}$

Theorem (Csiszár-Narayan '04)

The SK capacity is given by

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

where

$$R_{CO} = \min \sum_{i=1}^{m} R_i,$$

such that $\sum_{i \in B} R_i \geq H\left(X_B \mid X_{B^c}\right)$, *for all* $\mathcal{A} \nsubseteq B \subseteq \mathcal{M}$.

Secret Key Capacity

$R_{CO} \equiv$ min. rate of "communication for omniscience" for $\mathcal{A}$

Theorem (Csiszár-Narayan '04)

The SK capacity is given by

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

where

$$R_{CO} = \min \sum_{i=1}^{m} R_i,$$

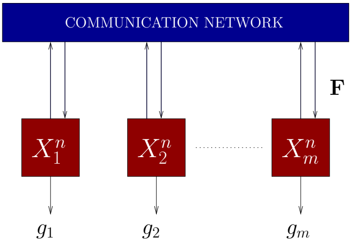
such that $\sum_{i \in B} R_i \geq H\left(X_B \mid X_{B^c}\right)$, *for all* $\mathcal{A} \nsubseteq B \subseteq \mathcal{M}$.

(Maurer '93, Ahlswede-Csiszár '93)

For $m = 2$: $\boxed{C = I(X_1 \wedge X_2)}$

Secure Computation

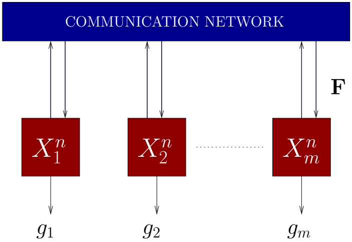
Computing Functions of Distributed Data



Function computed at terminal i: $g_i(x_1, ..., x_m)$

- Denote the random value of $g_i(x_1, ..., x_m)$ by G_i

Computing Functions of Distributed Data

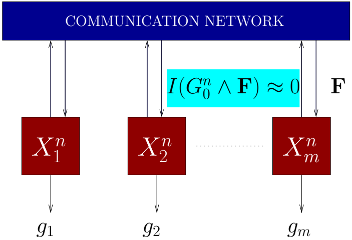


Function computed at terminal i: $g_i(x_1, ..., x_m)$

- Denote the random value of $g_i(x_1, ..., x_m)$ by G_i

$$\mathrm{P}\left(G_i^n = \hat{G}_i^{(n)}(X_i^n, \mathbf{F}),\ \text{for all } 1 \leq i \leq m\right) \geq 1 - \epsilon$$

Secure Function Computation



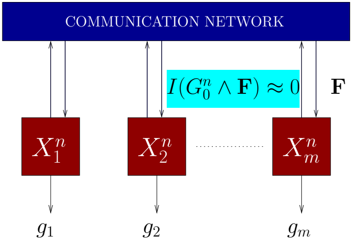
Value of *private function* g_0 must not be revealed

Definition. Functions $g_0, g_1, ..., g_m$ are securely computable if

1. *Recoverability:* $\mathrm{P}\left(G_i^n = \hat{G}_i^{(n)}(X_i^n, \mathbf{F}),\ i \in \mathcal{M}\right) \to 1$
2. *Security:* $I(G_0^n \wedge \mathbf{F}) \to 0$

Secure Function Computation

When are functions $g_0, g_1, ..., g_m$ securely computable?



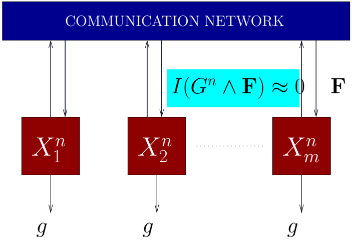
Value of *private function* g_0 must not be revealed

Definition. Functions $g_0, g_1, ..., g_m$ are securely computable if

1. *Recoverability:* $\mathrm{P}\left(G_i^n = \hat{G}_i^{(n)}(X_i^n, \mathbf{F}),\ i \in \mathcal{M}\right) \to 1$
2. *Security:* $I(G_0^n \wedge \mathbf{F}) \to 0$

Secure Function Computation

When is a function g securely computable?



Value of Private function $g_0 = g$

Definition. Function g is securely computable if

1. *Recoverability:* $\mathrm{P}\left(G^n = \hat{G}_i^{(n)}(X_i^n, \mathbf{F}),\ i \in \mathcal{M}\right) \to 1$
2. *Security:* $I(G^n \wedge \mathbf{F}) \to 0$

A Necessary Condition

If g is securely computable, then it constitutes an SK for $\mathcal{M}$.

Therefore,

$$\text{rate of } G \leq \text{SK Capacity},$$

i.e.,

$$\boxed{H(G) \leq C.}$$

When is g securely computable?

Theorem

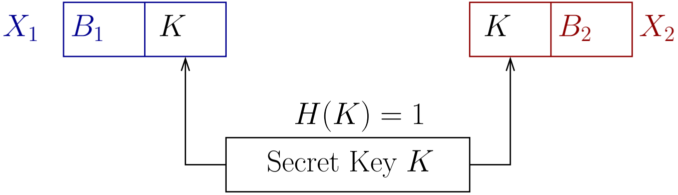
If g is securely computable, then $H(G) \leq C$.

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

For a securely computable function g:

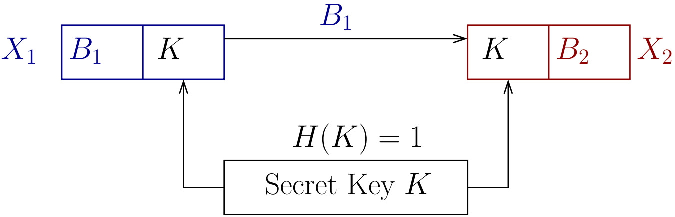
- *Omniscience can be obtained using $\mathbf{F} \underset{\sim}{\perp\!\!\!\perp} G^n$.*
- *Noninteractive communication suffices.*
- *Randomization is not needed.*

Example: Secure Computation using Secret Keys



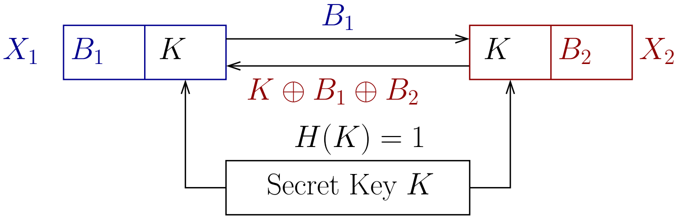
$$g(X_1, X_2) = B_1 \oplus B_2$$

Example: Secure Computation using Secret Keys



$$g(X_1, X_2) = B_1 \oplus B_2$$

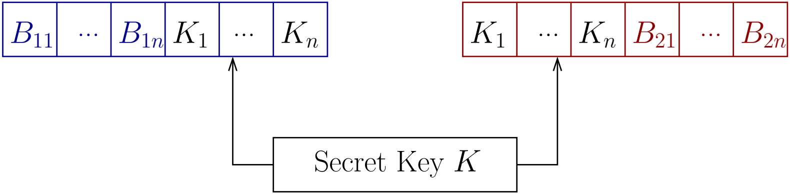
Example: Secure Computation using Secret Keys



$$g(X_1, X_2) = B_1 \oplus B_2$$

Example: Secure Computation using Secret Keys

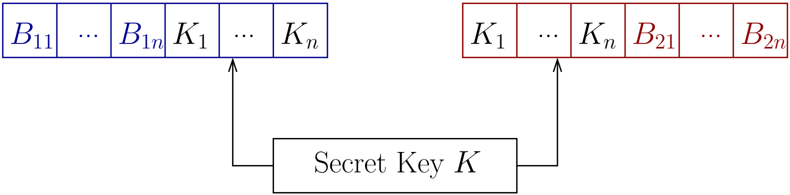
Do fewer than n bits suffice?



$$g(X_1^n, X_2^n) = B_{11} \oplus B_{21}, ..., B_{1n} \oplus B_{2n}$$

Example: Secure Computation using Secret Keys

Do fewer than n bits suffice?



$$g(X_1^n, X_2^n) = B_{11} \oplus B_{21}, ..., B_{1n} \oplus B_{2n}$$

- If parity is securely computable:

$$1 = H(G) \leq C = H(K)$$

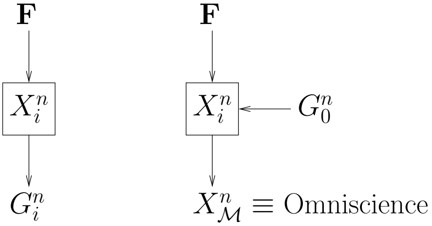
Characterization of Secure Computability

Theorem

The functions $g_0, g_1, ..., g_m$ are secure computable if ($>$) and only if ($\geq$)

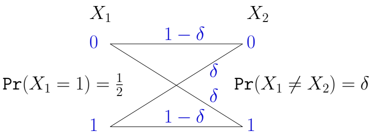
$$H\left(X_{\mathcal{M}} \mid G_0\right) \geq R^*.$$

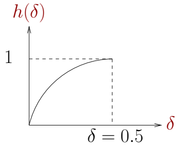
R^*: minimum rate of $\mathbf{F}$ such that



A data compression problem with no secrecy

Example: Functions of Binary Sources

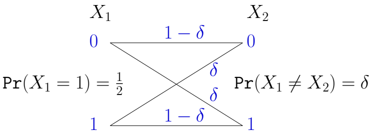


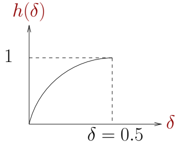


Functions are securely computable iff(!) $h(\delta) \leq \tau$

g_0	g_1	g_2	τ
$X_1 \oplus X_2$	$X_1 \oplus X_2$	ϕ	1
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1.X_2$	$2/3$
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1 \oplus X_2$	$1/2$
$X_1 \oplus X_2,\ X_1.X_2$	$X_1 \oplus X_2,\ X_1.X_2$	$X_1.X_2$	$2\delta/3$

Example: Functions of Binary Sources

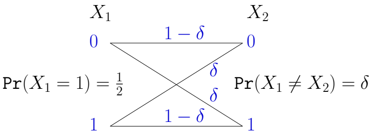


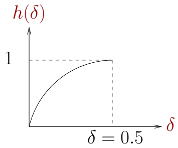


Functions are securely computable iff(!) $h(\delta) \leq \tau$

g_0	g_1	g_2	τ
$X_1 \oplus X_2$	$X_1 \oplus X_2$	ϕ	1
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1.X_2$	$2/3$
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1 \oplus X_2$	$1/2$
$X_1 \oplus X_2,\ X_1.X_2$	$X_1 \oplus X_2,\ X_1.X_2$	$X_1.X_2$	$2\delta/3$

Example: Functions of Binary Sources





Functions are securely computable iff(!) $h(\delta) \leq \tau$

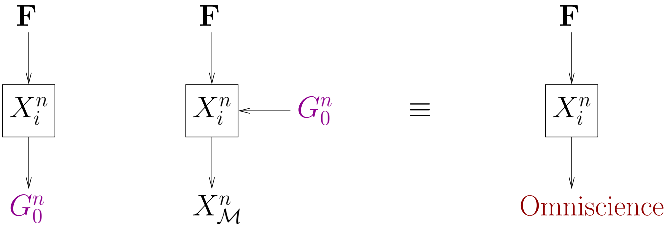
g_0	g_1	g_2	τ
$X_1 \oplus X_2$	$X_1 \oplus X_2$	ϕ	1
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1.X_2$	$2/3$
$X_1 \oplus X_2$	$X_1 \oplus X_2$	$X_1 \oplus X_2$	$1/2$
$X_1 \oplus X_2,\ X_1.X_2$	$X_1 \oplus X_2,\ X_1.X_2$	$X_1.X_2$	$2\delta/3$

Computing the Private Function

$$\boxed{H\left(X_{\mathcal{M}} \mid G_0\right) \geq R^*}$$

- Suppose $g_i = g_0$

R^*: minimum rate of $\mathbf{F}$ such that

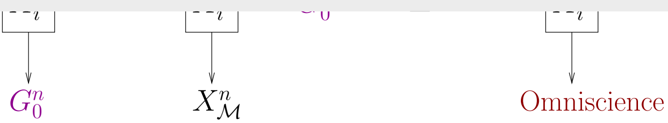


Computing the Private Function

$$H\left(X_{\mathcal{M}} \mid G_0\right) \geq R^*$$

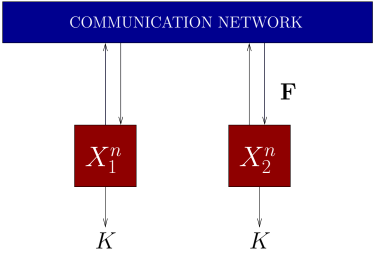
- Suppose $g_i = g_0$

If g_0 is securely computable at a terminal then
the entire data can be recovered securely at that terminal



Minimal Communication for an Optimum Rate Secret Key

Secret Key Generation for Two Terminals



Weak secrecy criterion: $\frac{1}{n} s_{in}(K, \mathbf{F}) \to 0$.

Secret key capacity $C = I(X_1 \wedge X_2)$

Maurer '93 Ahlswede-Csiszár '93

Common Randomness for SK Capacity

What is the form of CR that yields an optimum rate SK?

- Maurer-Ahlswede-Csiszár

Common randomness generated

$$X_1^n \text{ or } X_2^n$$

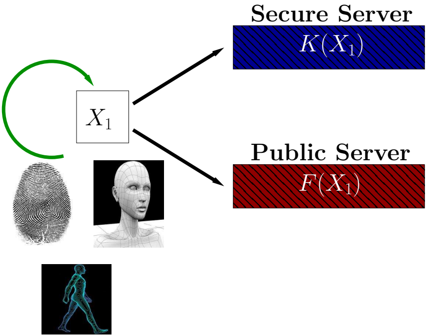
Rate of communication required

$$\min\{H(X_1|X_2), H(X_2|X_1)\}$$

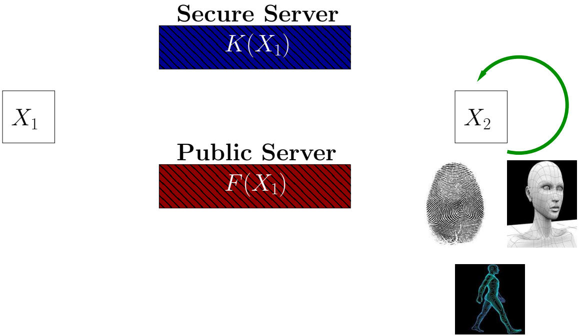
Decomposition

$$H(X_1) = H(X_1|X_2) + I(X_1 \wedge X_2)$$
$$H(X_2) = H(X_2|X_1) + I(X_1 \wedge X_2)$$

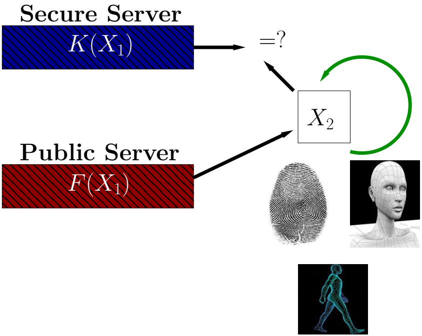
Digression: Secret Keys and Biometric Security



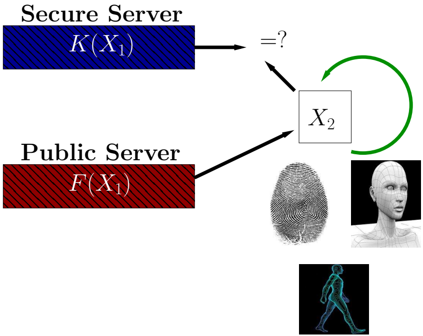
Digression: Secret Keys and Biometric Security



Digression: Secret Keys and Biometric Security



Digression: Secret Keys and Biometric Security



Similar approach can be applied for physically uncloneable functions

Common Randomness for SK Capacity

What is the form of CR that yields an optimum rate SK?

- Maurer-Ahlswede-Csiszár

Common randomness generated

$$X_1^n \text{ or } X_2^n$$

Rate of communication required

$$\min\{H(X_1|X_2), H(X_2|X_1)\}$$

Decomposition

$$H(X_1) = H(X_1|X_2) + I(X_1 \wedge X_2)$$
$$H(X_2) = H(X_2|X_1) + I(X_1 \wedge X_2)$$

Common Randomness for SK Capacity

What is the form of CR that yields an optimum rate SK?

- Maurer-Ahlswede-Csiszár | Csiszár-Narayan

Common randomness generated

X_1^n or X_2^n | (X_1^n, X_2^n)

Rate of communication required

$\min\{H(X_1|X_2), H(X_2|X_1)\}$ | $H(X_1|X_2) + H(X_2|X_1)$

Decomposition

$$H(X_1) = H(X_1|X_2) + I(X_1 \wedge X_2)$$
$$H(X_2) = H(X_2|X_1) + I(X_1 \wedge X_2)$$

$$H(X_1, X_2) = H(X_1|X_2) + H(X_2|X_1) + I(X_1 \wedge X_2)$$

Characterization of CR for Optimum Rate SK

Theorem

A CR J recoverable from $\mathbf{F}$ yields an optimum rate SK iff

$$\frac{1}{n} I\left(X_1^n \wedge X_2^n | J, \mathbf{F}\right) \to 0.$$

Examples: X_1^n or X_2^n or (X_1^n, X_2^n)

Interactive Common Information

- Interactive Common Information

Let J be a CR from communication $\mathbf{F}$.

$CI_i^r(X_1; X_2) \equiv$ min. rate of $L = (J, \mathbf{F})$ such that

$$\frac{1}{n} I(X_1^n \wedge X_2^n | L) \to 0 \qquad (*)$$

$$\boxed{CI_i(X_1 \wedge X_2) := \lim_{r \to \infty} CI_i^r(X_1; X_2)}$$

Interactive Common Information

- Interactive Common Information

  Let J be a CR from communication $\mathbf{F}$.

  $CI_i^r(X_1; X_2) \equiv$ min. rate of $L = (J, \mathbf{F})$ such that

  $$\frac{1}{n} I(X_1^n \wedge X_2^n | L) \to 0 \qquad (*)$$

  $$\boxed{CI_i(X_1 \wedge X_2) := \lim_{r \to \infty} CI_i^r(X_1; X_2)}$$

- Wyner's Common Information

  $CI(X_1 \wedge X_2) \equiv$ min. rate of $L\,(X_1^n, X_2^n)$ s.t. $(*)$ holds

Minimum Communication for Optimum Rate SK

R^r_{SK}: min. rate of an r-round communication $\mathbf{F}$ needed to generate an optimum rate SK

Theorem

The minimum rate R^r_{SK} is given by

$$R^r_{SK} = CI^r_i(X_1; X_2) - I(X_1 \wedge X_2).$$

It follows upon taking the limit $r \to \infty$ that

$$R_{SK} = CI_i(X_1 \wedge X_2) - I(X_1 \wedge X_2)$$

A single letter characterization of CI^r_i is available.

Minimum Communication for Optimum Rate SK

R^r_{SK}: min. rate of an r-round communication $\mathbf{F}$ needed to generate an optimum rate SK

Theorem

The minimum rate R^r_{SK} is given by

$$R^r_{SK} = CI^r_i(X_1; X_2) - I(X_1 \wedge X_2).$$

It follows upon taking the limit $r \to \infty$ that

$$R_{SK} = CI_i(X_1 \wedge X_2) - I(X_1 \wedge X_2)$$

Binary symmetric rvs: $CI^1_i = ... = CI^r_i = \min\{H(X_1), H(X_2)\}$

Minimum Communication for Optimum Rate SK

R^r_{SK}: min. rate of an r-round communication $\mathbf{F}$ needed to generate an optimum rate SK

Theorem

The minimum rate R^r_{SK} is given by

$$R^r_{SK} = CI^r_i(X_1; X_2) - I(X_1 \wedge X_2).$$

It follows upon taking the limit $r \to \infty$ that

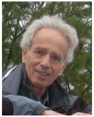
$$R_{SK} = CI_i(X_1 \wedge X_2) - I(X_1 \wedge X_2)$$

There is an example with $CI^1_i > CI^2_i \Rightarrow$ Interaction does help!

Common Information Quantities

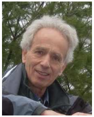
$$CI_{GC} \leq I(X_1 \wedge X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\}$$

Common Information Quantities

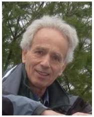
$$CI_{GC} \leq I(X_1 \wedge X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\}$$

Common Information Quantities



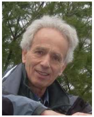
$$CI_{GC} \leq I(X_1 \wedge X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\}$$

Common Information Quantities



$$\boxed{CI_{GC}} \leq \boxed{I(X_1 \wedge X_2)} \leq \boxed{CI} \leq \boxed{CI_i} \leq \min\{H(X_1), H(X_2)\}$$

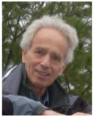
Common Information Quantities



$$CI_{GC} \le I(X_1 \wedge X_2) \le CI \le CI_i \le \min\{H(X_1), H(X_2)\}$$

Interactive Common Information

Common Information Quantities



$$CI_{GC} \le I(X_1 \wedge X_2) \le CI \le CI_i \le \min\{H(X_1), H(X_2)\}$$

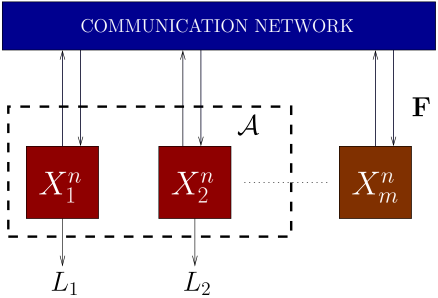
Interactive Common Information

- CI_i is indeed a new quantity

  Binary symmetric rvs: $CI < \min\{H(X_1), H(X_2)\} = CI_i$.

Querying Common Randomness

Common Randomness

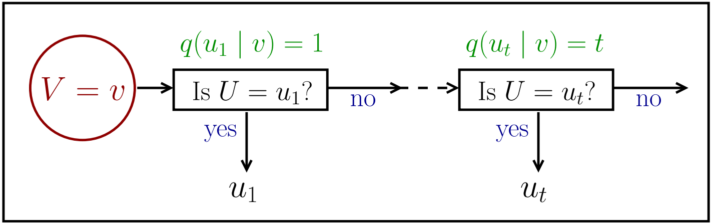


Definition. L is an ϵ-common randomness for $\mathcal{A}$ from $\mathbf{F}$ if

$$\mathrm{P}\left(L = L_i(X_i^n, \mathbf{F}),\ i \in \mathcal{A}\right) \geq 1 - \epsilon$$

Ahlswede-Csiszár '93 and '98.

Query Strategy



Query strategy for U given V

Massey '94, Arikan '96, Arikan-Merhav '99, Hanawal-Sundaresan '11

Query Strategy

Given rvs U, V with values in the sets $\mathcal{U}, \mathcal{V}$.

Definition. A *query strategy* q for U given $V = v$ is a bijection

$$q(\cdot|v) : \mathcal{U} \to \{1, ..., |\mathcal{U}|\},$$

where the querier, upon observing $V = v$, asks the question

“Is $U = u$?"

in the $q(u|v)^{\text{th}}$ query.

$q(U|V)$: random query number for U upon observing V

Query Strategy

Given rvs U, V with values in the sets $\mathcal{U}, \mathcal{V}$.

Definition. A *query strategy* q for U given $V = v$ is a bijection

$$q(\cdot|v) : \mathcal{U} \to \{1, ..., |\mathcal{U}|\},$$

where the querier, upon observing $V = v$, asks the question

"Is $U = u$?"

in the $q(u|v)^{\text{th}}$ query.

$q(U|V)$: random query number for U upon observing V

$$\boxed{|\{u : q(u \mid v) < \gamma\}| < \gamma}$$

Optimum Query Exponent

Definition. $E \geq 0$ is an ϵ-achievable *query exponent* if there exists ϵ-CR L_n for $\mathcal{A}$ from $\mathbf{F}_n$ such that

$$\sup_q \mathrm{P}\left(q(L_n \mid \mathbf{F}_n) < 2^{nE}\right) \to 0 \quad \text{as} \quad n \to \infty,$$

where the $\sup$ is over every query strategy for L_n given $\mathbf{F}_n$.

Optimum Query Exponent

Definition. $E \geq 0$ is an ϵ-achievable *query exponent* if there exists ϵ-CR L_n for $\mathcal{A}$ from $\mathbf{F}_n$ such that

$$\sup_q \mathrm{P}\left(q(L_n \mid \mathbf{F}_n) < 2^{nE}\right) \to 0 \quad \text{as} \quad n \to \infty,$$

where the $\sup$ is over every query strategy for L_n given $\mathbf{F}_n$.

$$E^*(\epsilon) \triangleq \sup\{E : E \text{ is an } \epsilon\text{-achievable query exponent}\}$$

$$E^* \triangleq \inf_{0<\epsilon<1} E^*(\epsilon) : \text{ optimum query exponent}$$

Characterization of Optimum Query Exponent

Theorem

For $0 < \epsilon < 1$, the optimum query exponent E^* equals

$$E^* = E^*(\epsilon) = C.$$

Characterization of Optimum Query Exponent

Theorem

For $0 < \epsilon < 1$, the optimum query exponent E^* equals

$$E^* = E^*(\epsilon) = C.$$

Proof.

Achievability: $E^*(\epsilon) \geq C(\epsilon)$ - Easy

Converse: $E^*(\epsilon) \leq C$ - Main contribution

Characterization of Optimum Query Exponent

Theorem

For $0 < \epsilon < 1$, the optimum query exponent E^* equals

$$E^* = E^*(\epsilon) = C.$$

Proof.

Achievability: $E^*(\epsilon) \geq C(\epsilon)$ - Easy

Converse: $E^*(\epsilon) \leq C$ - Main contribution

Theorem (Strong converse for SK capacity)

For $0 < \epsilon < 1$, the ϵ-SK capacity is given by

$$C(\epsilon) = E^* = C.$$

A Single-Shot Converse

For rvs $Y_1, ..., Y_k$, let L be an ϵ-CR for $\{1, ..., k\}$ from $\mathbf{F}$.

Theorem

Let θ be such that

$$\mathrm{P}\left(\left\{(y_1, ..., y_k) : \frac{\mathrm{P}_{Y_1,...,Y_k}(y_1, ..., y_k)}{\prod_{i=1}^{k} \mathrm{P}_{Y_i}(y_i)} \le \theta\right\}\right) \approx 1.$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \lesssim \theta^{\frac{1}{k-1}}\right) \ge (1-\sqrt{\epsilon})^2 > 0.$$

Small Cardinality Sets with Large Probabilities

Rényi entropy of order α of a probability measure μ on $\mathcal{U}$:

$$H_\alpha(\mu) \triangleq \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha, \quad 0 \le \alpha \neq 1$$

Lemma. There exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu\left(\mathcal{U}_\delta\right) \ge 1 - \delta$ s.t.

$$|\mathcal{U}_\delta| \lesssim \exp\left(H_\alpha(\mu)\right), \qquad 0 \le \alpha < 1.$$

Small Cardinality Sets with Large Probabilities

Rényi entropy of order α of a probability measure μ on $\mathcal{U}$:

$$H_\alpha(\mu) \triangleq \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha, \quad 0 \leq \alpha \neq 1$$

Lemma. There exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu\left(\mathcal{U}_\delta\right) \geq 1-\delta$ s.t.

$$|\mathcal{U}_\delta| \lesssim \exp\left(H_\alpha(\mu)\right), \qquad 0 \leq \alpha < 1.$$

Conversely, for any set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu\left(\mathcal{U}_\delta\right) \geq 1-\delta$,

$$|\mathcal{U}_\delta| \gtrsim \exp\left(H_\alpha(\mu)\right), \qquad \alpha > 1.$$

Small Cardinality Sets with Large Probabilities

Rényi entropy of order α of a probability measure μ on $\mathcal{U}$:

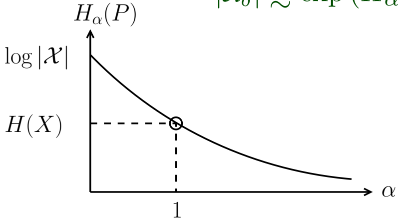
$$H_\alpha(\mu) \triangleq \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha, \quad 0 \leq \alpha \neq 1$$

Lemma. There exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu(\mathcal{U}_\delta) \geq 1 - \delta$ s.t.

$$|\mathcal{U}_\delta| \lesssim \exp\left(H_\alpha(\mu)\right), \qquad 0 \leq \alpha < 1.$$

Conversely, for any set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu(\mathcal{U}_\delta) \geq 1 - \delta$,

$$|\mathcal{U}_\delta| \gtrsim \exp\left(H_\alpha(\mu)\right), \qquad \alpha > 1.$$



In Closing ...

Our Approach

- Identify the underlying *common randomness*
- Decompose common randomness into independent components

Our Approach

- Identify the underlying *common randomness*
- Decompose common randomness into independent components

Secure Computing

Common Randomness

Omniscience with side information g_0 for decoding

Decomposition

The private function, the communication and the residual randomness

Our Approach

- Identify the underlying *common randomness*
- Decompose common randomness into independent components

Two Terminal Secret Key Generation

Common Randomness

Renders the observations conditionally independent

Decomposition

The secret key and the communication

Our Approach

- Identify the underlying *common randomness*
- Decompose common randomness into independent components

Querying Eavesdropper

Requiring the number of queries to be as large as possible
– is tantamount to decomposition into independent parts

Principles of Secrecy Generation

Computing the private function g_0 at a terminal is as difficult as securely recovering the entire data at that terminal.

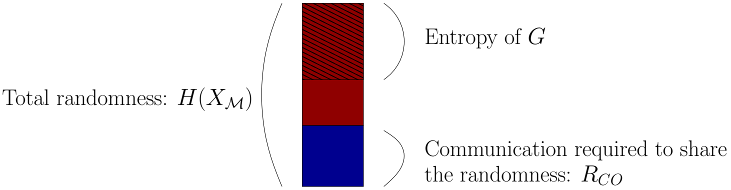
A CR yields an optimum rate SK iff it renders the observations of the two terminals (almost) conditionally independent.

Almost independence secrecy criterion is equivalent to imposing a lower bound on the complexity of a querier of the secret.

Supplementary Slides

Sufficiency

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

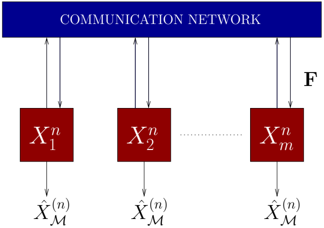


Claim: Omniscience can be attained using $\mathbf{F} \underset{\sim}{\perp\!\!\!\perp} G^n$ if:

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

.

Random Mappings For Omniscience



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

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

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

Csiszár-Körner '80 Han-Kobayashi '80 Csiszár-Narayan '04

Independence Properties of Random Mappings

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

Ahlswede-Csiszár '93 and '98

Independence Properties of Random Mappings

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

Generalized Privacy Amplification

Ahlswede-Csiszár '93 and '98 Bennett-Brassard-Crépeau-Maurer '95

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

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

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

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

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

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

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

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

Note: $I(F_1, ..., F_m \wedge G^n) \leq \sum_{i=1}^{m} I(F_i \wedge G^n, F_{\mathcal{M} \setminus i})$

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

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

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

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

Note: $I(F_1, ..., F_m \wedge G^n) \leq \sum_{i=1}^{m} I(F_i \wedge G^n, F_{\mathcal{M}\setminus i})$

Show $I(F_i \wedge G^n, F_{\mathcal{M}\setminus i}) \approx 0$ with probability close to 1

- using an extension of the BC Lemma [Lemma 2.7]