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
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

- \( X^n_i = (X_{i1}, ..., X_{in}) \)
  - Data observed at time instance \( t \): \( X^M_t = (X_{1t}, ..., X_{mt}) \)
  - Probability distribution of \( X_1, ..., X_m \) is known.

- Observations are i.i.d. across time:
  - \( X^M_1, ..., X^M_n \) are i.i.d. rvs.

- Observations are finite-valued.
Assumptions on the protocol

- Each terminal has access to all the communication.
- Multiple rounds of interactive communication are allowed.
- Communication from terminal 1: $F_{11} = f_{11}(X^n_1)$
Assumptions on the protocol

- Each terminal has access to all the communication.
- Multiple rounds of interactive communication are allowed.
- Communication from terminal 2: $F_{21} = f_{21}(X^n_2, F_{11})$
Assumptions on the protocol

- Each terminal has access to all the communication.
- Multiple rounds of interactive communication are allowed.
- $r$ rounds of interactive communication: $F = F_1, \ldots, F_m$
Definition. $L$ is an $\varepsilon$-common randomness for $A$ from $F$ if

$$P (L = L_i(X^n_i, F), \ i \in A) \geq 1 - \varepsilon$$

Ahlswede-Csizsár '93 and '98.
**Definition.** An rv $K \in \mathcal{K}$ is an $\epsilon$-secret key for $\mathcal{A}$ from $\mathcal{F}$ if

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

---

Maurer '93  Ahlswede-Csiszár '93  Csiszár-Narayan '04.
Definition. An rv $K \in \mathcal{K}$ is an $\epsilon$-secret key for $A$ from $F$ if

1. **Recoverability**: $K$ is an $\epsilon$-CR for $A$ from $F$

2. **Security**: $K$ is concealed from an observer of $F$

$$P_{KF} \approx U_{\mathcal{K}} \times P_F$$

Maurer ’93 Ahlswede-Csiszár ’93 Csiszár-Narayan ’04.
Notions of Security

▶ Kullback-Leibler Divergence

\[ s_{in}(K, F) = D(P_{KF} \| U_K \times P_F) = \log |K| - H(K) + I(K \land F) \approx 0 \]

▶ Variational Distance

\[ s_{var}(K, F) = \| P_{KF} - U_K \times P_F \|_1 \approx 0 \]

▶ Weak

\[ s_{weak}(K, F) = \frac{1}{n} s_{in}(K, F) \approx 0 \]
Notions of Security

- **Kullback-Leibler Divergence**

\[ s_{in}(K, F) = D(P_{KF} \| U_K \times P_F) \]
\[ = \log |K| - H(K) + I(K \land F) \approx 0 \]

- **Variational Distance**

\[ s_{var}(K, F) = \| P_{KF} - U_K \times P_F \|_1 \approx 0 \]

- **Weak**

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

\[ 2 s_{var}(K, F)^2 \leq s_{in}(K, F) \leq s_{var}(K, F) \log \frac{|K|}{s_{var}(K, F)} \]
Definition. An rv $K \in \mathcal{K}$ is an $\epsilon$-secret key for $\mathcal{A}$ from $\mathbb{F}$ if

1. Recoverability: $K$ is an $\epsilon$-CR for $\mathcal{A}$ from $\mathbb{F}$

2. Security: $s(K, \mathbb{F}) \to 0$ as $n \to \infty$
**Definition.** An rv $K \in \mathcal{K}$ is an $\epsilon$-secret key for $A$ from $F$ if

1. **Recoverability:** $K$ is an $\epsilon$-CR for $A$ from $F$

2. **Security:** $s(K, F) \to 0$ as $n \to \infty$

Rate of $K \equiv \frac{1}{n} \log |\mathcal{K}|$
Definition. An rv $K \in \mathcal{K}$ is an $\epsilon$-secret key for $\mathcal{A}$ from $\mathcal{F}$ if

1. Recoverability: $K$ is an $\epsilon$-CR for $\mathcal{A}$ from $\mathcal{F}$

2. Security: $s(K, \mathcal{F}) \to 0$ as $n \to \infty$

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

- $\epsilon$-SK capacity $C(\epsilon) = \text{supremum over the rates of } \epsilon$-SKs
- SK capacity $C = \inf_{0<\epsilon<1} C(\epsilon)$
Theorem (Csiszár-Narayan ’04)

The SK capacity is given by

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

where

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

such that \( \sum_{i \in B} R_i \geq H(X_B \mid X_{B^c}) \), for all \( A \nsubseteq B \subseteq M \).
Secret Key Capacity

\[ R_{CO} \equiv \min \text{ rate of "communication for omniscience" for } A \]

**Theorem (Csiszár-Narayan '04)**

The SK capacity is given by

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

where

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

such that \( \sum_{i \in B} R_i \geq H(X_B \mid X_{B^c}) \), for all \( A \not\subseteq B \subseteq M \).
\[ R_{CO} \equiv \min \text{ rate of "communication for omniscience for } A \]

**Theorem (Csiszár-Narayan ’04)**

The SK capacity is given by

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

where

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

such that \( \sum_{i \in B} R_i \geq H(X_B \mid X_{B^c}), \) for all \( A \not\subseteq B \subseteq M. \)

(Maurer ’93, Ahlswede-Csiszár ’93)

For \( m = 2: \)

\[ C = I(X_1 \land X_2) \]
Secure Computation
Function computed at terminal $i$: $g_i(x_1, \ldots, x_m)$

- Denote the random value of $g_i(x_1, \ldots, x_m)$ by $G_i$
Function computed at terminal $i$: $g_i(x_1, \ldots, x_m)$

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

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

Value of private function $g_0$ must not be revealed

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

1. Recoverability: $P \left( G_i^n = \hat{G}_i^n(X_i^n, F), \ i \in \mathcal{M} \right) \to 1$
2. Security: $I(G_0^m \land F) \to 0$
Secure Function Computation

When are functions $g_0, g_1, \ldots, g_m$ securely computable?

Value of private function $g_0$ must not be revealed

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

1. **Recoverability:** $\Pr \left( G_i^m = \hat{G}_i^{(n)}(X_i^n, F), \ i \in M \right) \to 1$
2. **Security:** $I(G_0^m \land F) \to 0$
Secure Function Computation

When is a function \( g \) securely computable?

**Definition.** Function \( g \) is securely computable if

1. **Recoverability:** \( \mathbb{P} \left( G^n = \hat{G}_i^{(n)}(X_i^n, F), \; i \in M \right) \rightarrow 1 \)

2. **Security:** \( I(G^n \land F) \rightarrow 0 \)

Value of Private function \( g_0 = g \)
If $g$ is securely computable, then it constitutes an SK for $M$. Therefore,

\[ \text{rate of } G \leq \text{SK Capacity}, \]

i.e.,

\[ H(G) \leq C. \]
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 \( F \downarrow \sim G^n \).
- Noninteractive communication suffices.
- Randomization is not needed.
Example: Secure Computation using Secret Keys

\[ H(K) = 1 \]

\[ g(X_1, X_2) = B_1 \oplus B_2 \]
Example: Secure Computation using Secret Keys

\[ H(K) = 1 \]

Secret Key \( K \)

\[ g(X_1, X_2) = B_1 \oplus B_2 \]
Example: Secure Computation using Secret Keys

\[ g(X_1, X_2) = B_1 \oplus B_2 \]

\[ H(K) = 1 \]

\[ K \oplus B_1 \oplus B_2 \]
Example: Secure Computation using Secret Keys

Do fewer than $n$ bits suffice?

\[
g(X_1^n, X_2^n) = B_{11} \oplus B_{21}, \ldots, B_{1n} \oplus B_{2n}
\]
Example: Secure Computation using Secret Keys

Do fewer than \( n \) bits suffice?

\[
\begin{align*}
B_{11} & \quad \cdots \quad B_{1n} & K_1 & \quad \cdots \quad & K_n \\
K_1 & \quad \cdots \quad & K_n & \quad B_{21} & \quad \cdots \quad & B_{2n}
\end{align*}
\]

- If parity is securely computable:

\[
g(X_1^n, X_2^n) = B_{11} \oplus B_{21}, \ldots, B_{1n} \oplus B_{2n}
\]

\[1 = H(G) \leq C = H(K)\]
The functions $g_0, g_1, \ldots, g_m$ are secure computable if ($>)$ and only if ($\geq$)

$$H(X_M \mid G_0) \geq R^*.$$ 

$R^*$: minimum rate of $F$ such that

A data compression problem with no secrecy
Example: Functions of Binary Sources

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

<table>
<thead>
<tr>
<th>( g_0 )</th>
<th>( g_1 )</th>
<th>( g_2 )</th>
<th>( \tau )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( \phi )</td>
<td>1</td>
</tr>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1.X_2 )</td>
<td>2/3</td>
</tr>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>1/2</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>2\delta/3</td>
</tr>
</tbody>
</table>
Example: Functions of Binary Sources

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

<table>
<thead>
<tr>
<th>$g_0$</th>
<th>$g_1$</th>
<th>$g_2$</th>
<th>$\tau$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1 \oplus X_2$</td>
<td>$X_1 \oplus X_2$</td>
<td>$\phi$</td>
<td>1</td>
</tr>
<tr>
<td>$X_1 \oplus X_2$</td>
<td>$X_1 \oplus X_2$</td>
<td>$X_1 \cdot X_2$</td>
<td>2/3</td>
</tr>
<tr>
<td>$X_1 \oplus X_2$</td>
<td>$X_1 \oplus X_2$</td>
<td>$X_1 \oplus X_2$</td>
<td>1/2</td>
</tr>
<tr>
<td>$X_1 \oplus X_2, X_1 \cdot X_2$</td>
<td>$X_1 \oplus X_2, X_1 \cdot X_2$</td>
<td>$X_1 \cdot X_2$</td>
<td>$2\delta/3$</td>
</tr>
</tbody>
</table>
Example: Functions of Binary Sources

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

<table>
<thead>
<tr>
<th>( g_0 )</th>
<th>( g_1 )</th>
<th>( g_2 )</th>
<th>( \tau )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( \phi )</td>
<td>1</td>
</tr>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \cdot X_2 )</td>
<td>2/3</td>
</tr>
<tr>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>( X_1 \oplus X_2 )</td>
<td>1/2</td>
</tr>
<tr>
<td>( X_1 \oplus X_2, X_1 \cdot X_2 )</td>
<td>( X_1 \oplus X_2, X_1 \cdot X_2 )</td>
<td>( X_1 \cdot X_2 )</td>
<td>( 2\delta/3 )</td>
</tr>
</tbody>
</table>
Computing the Private Function

\[ H (X_M \mid G_0) \geq R^* \]

- Suppose \( g_i = g_0 \)

\( R^* \): minimum rate of \( F \) such that

\[ F \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]

\[ G^m_0 \]

\[ X^n_i \]
Computing the Private Function

\[ H(X_M | G_0) \geq R^* \]

- 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: \( \frac{1}{n} s_{in}(K, F) \to 0 \).

Secret key capacity \( C = I(X_1 \land X_2) \)

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

\[
H(X_1) = H(X_1|X_2) + I(X_1 \land X_2) \\
H(X_2) = H(X_2|X_1) + I(X_1 \land X_2)
\]
Digression: Secret Keys and Biometric Security

- Secure Server
  - $K(X_1)$

- Public Server
  - $F(X_1)$

Input: $X_1$
Digression: Secret Keys and Biometric Security

$$F(X_1)$$

$$K(X_1)$$

Secure Server

Public Server

$$X_1$$

$$X_2$$
Digression: Secret Keys and Biometric Security

Secure Server

\[ K(X_1) \]

[Diagram showing a secure server, a secure function \( K(X_1) \), and an output \( X_2 \).]

Public Server

\[ F(X_1) \]

[Diagram showing a public server, a public function \( F(X_1) \), and an output \( X_2 \).]
Digression: Secret Keys and Biometric Security

Secure Server

\[ K(X_1) \]

Public Server

\[ F(X_1) \]

\[ X_2 \]

Similar approach can be applied for **physically uncloneable functions**
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

\[ H(X_1) = H(X_1|X_2) + I(X_1 \land X_2) \]
\[ H(X_2) = H(X_2|X_1) + I(X_1 \land X_2) \]
What is the form of CR that yields an optimum rate SK?

- **Maurer-Ahlswede-Csiszár**
- **Csiszár-Narayan**

*Common randomness generated*

\[ X_1^n \text{ or } X_2^n \]

\[ (X_1^n, X_2^n) \]

*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*

\[
H(X_1) = H(X_1|X_2) + I(X_1 \land X_2)
\]

\[
H(X_2) = H(X_2|X_1) + I(X_1 \land X_2)
\]

\[
H(X_1, X_2) = H(X_1|X_2) + H(X_2|X_1) + I(X_1 \land X_2)
\]
Characterization of CR for Optimum Rate SK

**Theorem**

A CR $J$ recoverable from $F$ yields an optimum rate SK iff

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

Examples: $X_1^n$ or $X_2^n$ or $(X_1^n, X_2^n)$
Interactive Common Information

Let $J$ be a CR from communication $F$.

$$CI^r_i(X_1; X_2) \equiv \min. \text{ rate of } L = (J, F) \text{ such that}$$

$$\frac{1}{n} I(X^n_1 \land X^n_2 | L) \to 0$$

$$CI_i(X_1 \land X_2) := \lim_{r \to \infty} CI^r_i(X_1; X_2)$$
Interactive Common Information

Let $J$ be a CR from communication $F$.

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

$$\frac{1}{n}I(X_1^n \land X_2^n | L) \to 0 \quad (\ast)$$

$$CI_i(X_1 \land X_2) := \lim_{r \to \infty} CI_{ir}^r(X_1; X_2)$$

Wyner’s Common Information

$$CI(X_1 \land X_2) \equiv \text{min. rate of } L(X_1^n, X_2^n) \text{ s.t. (\ast) holds}$$
Minimum Communication for Optimum Rate SK

\( R_{SK}^r \): \text{min. rate of an } r \text{-round communication \textbf{F}} \text{ needed to generate an optimum rate SK}

**Theorem**

The minimum rate \( R_{SK}^r \) is given by

\[
R_{SK}^r = CI_i^r(X_1; X_2) - I(X_1 \land X_2).
\]

It follows upon taking the limit \( r \to \infty \) that

\[
R_{SK} = CI_i(X_1 \land X_2) - I(X_1 \land X_2)
\]

A single letter characterization of \( CI_i^r \) is available.
$R^r_{SK}$: min. rate of an $r$-round communication needed to generate an optimum rate SK

**Theorem**

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

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

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

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

Binary symmetric rvs: $CI^1_i = ... = CI^r_i = \min\{H(X_1), H(X_2)\}$
Minimum Communication for Optimum Rate SK

\( R_{SK}^r \): min. rate of an \( r \)-round communication needed to generate an optimum rate SK

**Theorem**

The minimum rate \( R_{SK}^r \) is given by

\[
R_{SK}^r = CI_i^r(X_1; X_2) - I(X_1 \land X_2).
\]

It follows upon taking the limit \( r \to \infty \) that

\[
R_{SK} = CI_i(X_1 \land X_2) - I(X_1 \land X_2)
\]

There is an example with \( CI_i^1 > CI_i^2 \) ⇒ Interaction does help!
Common Information Quantities

\[ CI_{GC} \leq I(X_1 \land X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\} \]
Common Information Quantities

\[ CI_{GC} \leq I(X_1 \land X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\} \]
Common Information Quantities

\[ CI_{GC} \leq I(X_1 \land X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\} \]
Common Information Quantities

\[ CI_{GC} \leq I(X_1 \land X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\} \]
Common Information Quantities

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

Interactive Common Information
Common Information Quantities

\[ CI_{GC} \leq I(X_1 \land X_2) \leq CI \leq CI_i \leq \min\{H(X_1), H(X_2)\} \]

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

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

Ahlswede-Csiszár ’93 and ’98.
Query Strategy

$V = v$

$q(u_1 \mid v) = 1$

Is $U = u_1$?

no

$q(u_t \mid v) = t$

Is $U = u_t$?

no

Query strategy for $U$ given $V$

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

$$q(\cdot|v) : \mathcal{U} \rightarrow \{1, \ldots, |\mathcal{U}|\},$$

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

“Is $U = u$?"

in the $q(u|v)^{th}$ 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

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

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

"Is $U = u$?"

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

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

$$|\{u : q(u|v) < \gamma\}| < \gamma$$
Definition. $E \geq 0$ is an $\epsilon$-achievable \textit{query exponent} if there exists $\epsilon$-CR $L_n$ for $\mathcal{A}$ from $\mathcal{F}_n$ such that

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

where the $\sup$ is over every query strategy for $L_n$ given $\mathcal{F}_n$. 
Definition. $E \geq 0$ is an $\epsilon$-achievable query exponent if there exists $\epsilon$-CR $L_n$ for $A$ from $F_n$ such that

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

where the $\sup$ is over every query strategy for $L_n$ given $F_n$.

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

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

$$E^* = E^*(\epsilon) = C.$$
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 $\epsilon$-SK capacity is given by

\[
C(\epsilon) = E^* = C.
\]
A Single-Shot Converse

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

**Theorem**

Let $\theta$ be such that

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

Then, there exists a query strategy $q_0$ for $L$ given $F$ such that

$$P \left( q_0(L \mid F) \lesssim \theta^{\frac{1}{k-1}} \right) \geq (1 - \sqrt{\epsilon})^2 > 0.$$
Rényi entropy of order $\alpha$ of a probability measure $\mu$ 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.

$$|\mathcal{U}_\delta| \lesssim \exp(H_\alpha(\mu)), \quad 0 \leq \alpha < 1.$$
Rényi entropy of order $\alpha$ of a probability measure $\mu$ on $\mathcal{U}$:

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

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

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

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

$$|\mathcal{U}_\delta| \gtrsim \exp(H_\alpha(\mu)), \quad \alpha > 1.$$
Rényi entropy of order $\alpha$ of a probability measure $\mu$ 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.

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

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

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

- Share all data to compute $g$: \textbf{Omniscience} $\equiv X^n_M$
- Can we attain omniscience using $F \perp \perp G^n$?

**Claim:** Omniscience can be attained using $F \perp \perp G^n$ 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, $F_1, \ldots, F_m$ result in omniscience if:
  \[ \sum_{i \in B} R_i \geq H(X_B | X_{B^c}) , \quad B \subsetneq \mathcal{M}. \]
- $R_{CO} = \min \sum_{i \in \mathcal{M}} R_i$. 

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.

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

**Balanced Coloring Lemma:** Probability that a random mapping $F : \mathcal{X} \to \{1, \ldots, 2^r\}$ 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 $\exp \left\{ r + \log(2N) - (\epsilon^2/3) 2^{(d-r)} \right\}$.

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 $F : \mathcal{X} \rightarrow \{1, \ldots, 2^r\}$ 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 $\exp \left\{ r + \log(2N) - (\epsilon^2/3) 2^{(d-r)} \right\}$.

**Generalized Privacy Amplification**

Ahlswede-Csiszár '93 and '98

Bennett-Brassard-Crépeau-Maurer '95
Consider random mappings $F_i = F_i (X_i^n)$ of rates $R_i$ such that
\[ \sum_{i \in B} R_i \geq H (X_B | X_{B^c}) , \quad B \subsetneq \mathcal{M}. \]
- $F$ results in omniscience at all the terminals.
- $F$ is approximately independent of $G^n$. 

Sufficiency of $H(G) < H (X_M) - R_{CO}$
Consider random mappings $F_i = F_i(X^n_i)$ of rates $R_i$ such that

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

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

Note: $I(F_1, \ldots, F_m \land G^n) \leq \sum_{i=1}^m I(F_i \land G^n, F_{\mathcal{M} \backslash i})$
Consider random mappings $F_i = F_i(X^n_i)$ of rates $R_i$ such that

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

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

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

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]