When is a Function Securely Computable?

H. Tyagi\textsuperscript{1}  P. Narayan\textsuperscript{1}  P. Gupta\textsuperscript{2}

\textsuperscript{1}Department of Electrical and Computer Engineering and Institute of System Research University of Maryland, College Park, USA.

\textsuperscript{2}Bell Labs, Alcatel-Lucent.
Secure Computing of Functions

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

\[ U_1, U_2, U_a, U_m \]

\[ G_i^{(n)} = g(X_{\mathcal{M}}^n), \ i \in \mathcal{A} \]
\[ I(g(X_{\mathcal{M}}^n) \land F) \approx 0 : \text{Secrecy} \]
\[ \Pr \left( G_i^{(n)} = g(X_{\mathcal{M}}^n), \ i \in \mathcal{A} \right) \approx 1 : \text{Recoverability} \]

- Single-letter function: \( g(X_{\mathcal{M}}^n) = (g(X_{\mathcal{M}1}), \ldots, g(X_{\mathcal{M}n})) \).
- Notation: \( G = g(X_{\mathcal{M}}), \quad G^n = g(X_{\mathcal{M}}^n) \).

When is a given function \( g \) securely computable?
A Necessary Condition

Secret Key Generation

- Secret Key Capacity $C(A) \equiv$ Largest achievable rate of $K$.

[Csiszár-Narayan ‘04]

$$C(A) = H(X_M) - R(A),$$

$R(A) = \text{Min. sum rate of communication for omniscience at } A.$
A Necessary Condition

Secret Key Generation

**COMMUNICATION NETWORK**

\[ F_1, F_2, F_a, F_m \]

- **F**: Public Communication
- **K**: Secret Key

\[ I(K \wedge F) \geq 0 \]

- **A**

► **Secret Key Capacity** \( C(A) \equiv \text{Largest achievable rate of } K \).

[Csiszár-Narayan ‘04]

\[
C(A) = H(X_{\mathcal{M}}) - R(A),
\]

\[
R(A) = \text{Min. sum rate of communication for omniscience at } A.
\]

If \( g \) is securely computable by \( A \),

\[
H(G) \leq C(A).
\]
Is $H(G) < C(A)$ sufficient?

All terminals wish to compute: $A = M$ [TNG ‘10]

If $H(G) < C(M)$ ⇒ a protocol for SC of $g$ by $M$ exists.

- Noninteractive communication suffices.
- Randomization is not needed.
- Idea: Omniscience can be obtained using communication $\mathbf{F} \parallel \sim G^m$. 
Is $H(G) < C(\mathcal{A})$ sufficient?

All terminals wish to compute: $\mathcal{A} = \mathcal{M}$ [TNG ‘10]

If $H(G) < C(\mathcal{M}) \Rightarrow$ a protocol for SC of $g$ by $\mathcal{M}$ exists.

- Noninteractive communication suffices.
- Randomization is not needed.
- Idea: Omniscience can be obtained using communication $\mathcal{F} \Downarrow G^n$.

Counterexample for $\mathcal{A} \subsetneq \mathcal{M}$

$g(x_1, x_1, x_2) = x_2$.

- Let $H(X_2) < H(X_1) = C(\mathcal{A}) \Rightarrow H(G) < C(\mathcal{A})$ is satisfied.

However, $g$ is clearly not securely computable.
And Now For Something Completely Different

[Monty Python ’69]

It’s

A New Necessary Condition for Secure Computability
A New Necessary Condition

If $G^n$ is securely computable by $A$:

Provide $G^n$ as side information to terminals in $A^c$.

- Available only for decoding but not for communicating.

$G^n$ forms a secret key for all terminals, termed an aided secret key.

- Let $C'_{g,A}(M)$ be that largest achievable rate of such a key.
A New Necessary Condition

If \( G^n \) is securely computable by \( \mathcal{A} \):

Provide \( G^n \) as side information to terminals in \( \mathcal{A}^c \).

- Available only for decoding but not for communicating.

\( G^n \) forms a secret key for all terminals, termed an aided secret key.

- Let \( C_{g,\mathcal{A}}(\mathcal{M}) \) be that largest achievable rate of such a key.

For a \( g \) securely computable by \( \mathcal{A} \),

\[
H(G) \leq C_{g,\mathcal{A}}(\mathcal{M})
\]
Aided Secret Key Capacity

Theorem

The aided secret key capacity is

\[ C_{g,A}(M) = H(X_M) - R_{g,A}(M), \]

where

\[ R_{g,A}(M) = \min \text{ sum rate of communication for omniscience at } M \]

when \( G^m \) is available as side information for decoding to terminals in \( \mathcal{A}^c \).
Characterization of Securely Computable Functions

Theorem

\textbf{If \( g \) is securely computable by \( A \): \( H(G) \leq C_{g,A}(\mathcal{M}) \).}

\textbf{Conversely, \( g \) is securely computable by \( A \) if: \( H(G) < C_{g,A}(\mathcal{M}) \).}

For securely computable function \( g \):

- Omniscience can be obtained at \( A \) using \( F \perp \parallel G^n \).
- Noninteractive communication suffices.
- Randomization is not needed.
Consider random binning of *appropriate rate* at each terminal:

- To allow omniscience at $\mathcal{M}$, with $G^n$ given to the terminals in $\mathcal{A}^c$ for decoding.
- To keep bin indices independent of $G^n$. 

Sketch of the Proof
Sketch of the Proof

1. \( H(G) < C_{g,A}(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{g,A}(\mathcal{M}) \)
\[ \iff H(X_{\mathcal{M}} | G) > R_{g,A}(\mathcal{M}). \]
Sketch of the Proof

1. \( H(G) < C_{g,A}(\mathcal{M}) = H(X_\mathcal{M}) - R_{g,A}(\mathcal{M}) \)
\( \Leftrightarrow H(X_\mathcal{M} | G) > R_{g,A}(\mathcal{M}). \)

2. Generate random mappings \( F_i = F_i(X_i^n) \) of rate \( R_i \):
\[ \sum_i R_i \approx R_{g,A}(\mathcal{M}) \text{ with } (R_1, ... , R_m) \text{ s.t.} \]
   - it enables omniscience at \( \mathcal{M} \) with side information \( G^n \)
     given to the terminals in \( \mathcal{A}^c \) only for decoding.
Sketch of the Proof

1. \[ H(G) < C_{g,A}(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{g,A}(\mathcal{M}) \]
   \[ \iff H(X_{\mathcal{M}} | G) > R_{g,A}(\mathcal{M}). \]

2. Generate random mappings \( F_i = F_i(X^n_i) \) of rate \( R_i \):
   \[ \sum_i R_i \approx R_{g,A}(\mathcal{M}) \text{ with } (R_1, \ldots, R_m) \text{ s.t.} \]
   - it enables omniscience at \( \mathcal{M} \) with side information \( G^n \) given to the terminals in \( \mathcal{A}^c \) only for decoding.

3. Observe: \[ I(F_{\mathcal{M}} \land G^n) \leq \sum_{i} I(F_i \land G^n, F_{\mathcal{M}\{i\}}). \]
Sketch of the Proof

1. \( H(G) < C_{g,A}(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{g,A}(\mathcal{M}) \)
   \[
   \iff H(X_{\mathcal{M}} | G) > R_{g,A}(\mathcal{M}).
   \]

2. Generate random mappings \( F_i = F_i(X_i^n) \) of rate \( R_i \):
   \[
   \sum_i R_i \approx R_{g,A}(\mathcal{M}) \text{ with } (R_1, \ldots, R_m) \text{ s.t.}
   \]
   - it enables omniscience at \( \mathcal{M} \) with side information \( G^n \)
     given to the terminals in \( A^c \) only for decoding.

3. Observe: \( I(F_{\mathcal{M}} \wedge G^n) \leq \sum_{i=1}^m I(F_i \wedge G^n, F_{\mathcal{M}\{i\}}) \).

4. To prove:
   With high probability \( I(F_i \wedge G^n, F_{\mathcal{M}\{i\}}) \approx 0 \), for each \( i \).
Independence Properties of Random Mappings
The Balanced Coloring Lemma

- To prove:
  With high probability $I \left( F_i \land G^n, F_{\mathcal{M}\setminus\{i\}} \right) \cong 0$, for each $i$.

- Shall show:
  For almost all $(y, z)$:
  
  $$F_i \mid \{G^n = y, F_{\mathcal{M}\setminus\{i\}} = z\} \approx \text{uniform}.$$ 

- Family of distributions on $X^n_i$:
  $$\hat{P}_{X^n_i} \{G^n = y, F_{\mathcal{M}\setminus\{i\}} = z\}.$$

- Seek conditions for random mappings to be uniformly distributed
  - w.r.t. a given family of distributions.
Independence Properties of Random Mappings

The Balanced Coloring Lemma

- Balanced Coloring Lemma:
  [R. Ahlswede-I. Csiszár, '98], [I. Csiszár-P.N., '04]

  Given a family of distributions with probabilities uniformly bounded above,
  \[
  \Pr(\text{random coloring } \approx \text{uniform, w.r.t. all pmfs in the family}) \geq q,
  \]
  where \( q \) depends on the size of the family, the uniform bound and the rate of coloring.

- For the case at hand: a slightly generalized version is applied.
  - \( q = q(n) \) grows to 1 super-exponentially in \( n \).
Secure Computability of Multiple Functions

COMMUNICATION NETWORK

\[ F_1 \quad F_2 \quad \cdots \quad F_m \equiv F: \text{Public Communication} \]

\[ X^n_1 \quad X^n_2 \quad \cdots \quad X^n_m \]

Secrecy Condition: \( I(F \wedge G^n_1, \ldots, G^n_m) \approx 0. \)

Which functions \( g_1, \ldots, g_m \) are securely computable?

Omniscience is not allowed in general

- For \( m = 2 \):
  \[ X_1 \perp \perp X_2 \quad g_i(x_1, x_2) = x_i. \]