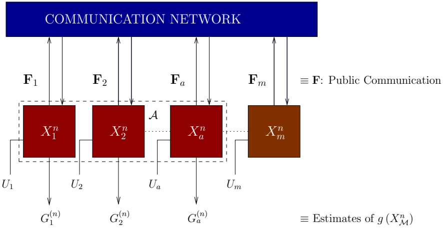
When is a Function Securely Computable?

H. Tyagi[1] P. Narayan[1] P. Gupta[2]

[1]Department of Electrical and Computer Engineering
and Institute of System Research
University of Maryland, College Park, USA.

[2]Bell Labs, Alcatel-Lucent.

Secure Computing of Functions



Secure computability of g by $\mathcal{A}$:

$$\texttt{Pr}\left(G_i^{(n)} = g\left(X_{\mathcal{M}}^n\right), i \in \mathcal{A}\right) \approx 1 : \quad \text{Recoverability}$$

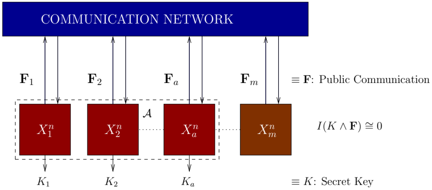
$$I\left(g\left(X_{\mathcal{M}}^n\right) \wedge \mathbf{F}\right) \approx 0 : \quad \text{Secrecy}$$

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

When is a given function g securely computable?

A Necessary Condition

Secret Key Generation



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

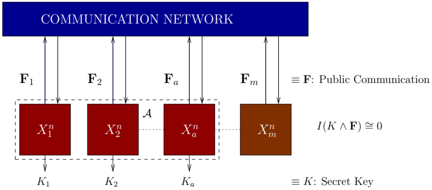
  [Csiszár-Narayan '04]

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

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

A Necessary Condition

Secret Key Generation



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

  [Csiszár-Narayan '04]

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

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

If g is securely computable by $\mathcal{A}$,

$$H(G) \leq C(\mathcal{A}).$$

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 $\mathbf{F} \underset{\sim}{\perp\!\!\!\perp} G^n$.

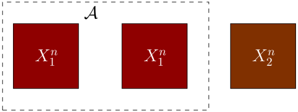
Is $H(G) < C(\mathcal{A})$ sufficient?

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 $\mathbf{F} \underset{\sim}{\perp\!\!\!\perp} G^n$.

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



$X_1 \perp\!\!\!\perp X_2$

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

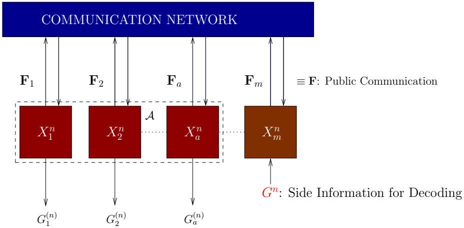
[Monty Python '69]

It's

A New Necessary Condition for Secure Computability

A New Necessary Condition

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



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

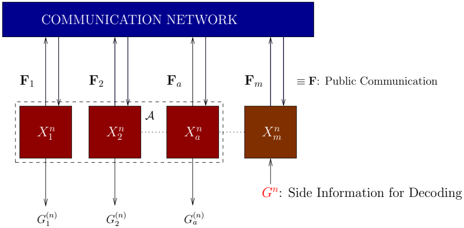
- Available *only for decoding* but *not for communicating*.

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.

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

$$C_{g,\mathcal{A}}(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{g,\mathcal{A}}(\mathcal{M}),$$

where

$R_{g,\mathcal{A}}(\mathcal{M}) =$ *min. sum rate of communication for omniscience at* $\mathcal{M}$

when G^n *is available as side information for decoding to terminals in* $\mathcal{A}^c$*.*

Characterization of Securely Computable Functions

Theorem

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

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

For securely computable function g:

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

Sketch of the Proof

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

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

Sketch of the Proof

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

2. Generate random mappings $F_i = F_i(X_i^n)$ of rate R_i:
   $\sum_i R_i \approx R_{g,\mathcal{A}}(\mathcal{M})$ with $(R_1, ..., R_m)$ 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. $H(G) < C_{g,\mathcal{A}}(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{g,\mathcal{A}}(\mathcal{M})$
   $\Leftrightarrow H\left(X_{\mathcal{M}} \mid G\right) > R_{g,\mathcal{A}}(\mathcal{M})$.

2. Generate random mappings $F_i = F_i(X_i^n)$ of rate R_i:
   $\sum_i R_i \approx R_{g,\mathcal{A}}(\mathcal{M})$ with $(R_1, ..., R_m)$ 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: $I(F_{\mathcal{M}} \wedge G^n) \leq \sum_{i}^{m} I\left(F_i \wedge G^n, F_{\mathcal{M}\setminus\{i\}}\right).$

Sketch of the Proof

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

2. Generate random mappings $F_i = F_i(X_i^n)$ of rate R_i:
   $\sum_i R_i \approx R_{g,\mathcal{A}}(\mathcal{M})$ with $(R_1, \ldots, R_m)$ 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: $I(F_{\mathcal{M}} \wedge G^n) \leq \sum_i^m I\left(F_i \wedge G^n, F_{\mathcal{M}\setminus\{i\}}\right)$.

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

- To prove:

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

- Shall show:

  For almost all $(\mathbf{y}, \mathbf{z})$:

  $$F_i \mid \{G^n = \mathbf{y}, F_{\mathcal{M}\setminus\{i\}} = \mathbf{z}\} \approx \text{uniform}.$$

- Family of distributions on X_i^n : $\left\{P_{X_i^n|\{G^n=\mathbf{y}, F_{\mathcal{M}\setminus\{i\}}=\mathbf{z}}\right\}$.

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

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

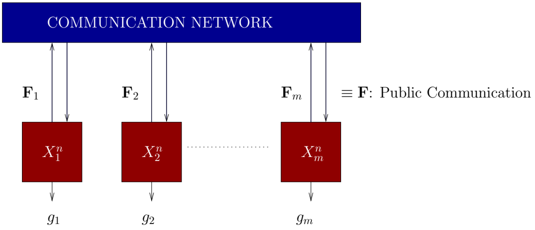
  Given a family of distributions with probabilities uniformly bounded above,

  $$\texttt{Pr}\,(\text{random coloring} \approx \text{uniform, w.r.t. all pmfs in the family}) \geq q,$$

  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



Secrecy Condition: $I\left(\mathbf{F} \wedge G_1^n, ..., G_m^n\right) \approx 0.$

$\boxed{\text{Which functions } g_1, ..., g_m \text{ are securely computable?}}$

Omniscience is not allowed in general

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