Protection of Sensitive Information

Catuscia Palamidessi
INRIA & Ecole Polytechnique of Paris
Leakage of information (13 March 2014)

Mark Zuckerberg 'confused and frustrated' by US spying

Facebook founder Mark Zuckerberg has said he has called President Barack Obama to "express frustration" over US digital surveillance.

The 28-year-old said in a blog post the US government "should be the champion for the internet, not a threat."

Related Stories

Target says it declined to act on early alert of cyber breach

BY JIM FINKLE AND SUSAN HEAVY

BOSTON/WASHINGTON Thu Mar 13, 2014 11:20am EDT

The European Parliament passed a strong new set of data protection measures on Wednesday, prompted in part by the disclosure by Edward J. Snowden, a former contractor at the United States National Security Agency, of America’s vast electronic spying program, David Jolly reports.
Protection of sensitive information

- Protecting the confidentiality of sensitive information is a fundamental issue in computer security.

- Access control and encryption are not sufficient! Systems could leak secret information through correlated observables.
  - The notion of “observable” depends on the adversary.
  - Often, secret-leaking observables are public, and therefore available to the adversary.
Leakage through correlated observables

Password checking

Election tabulation

Timings of decryptions
Plan of the course


2. Focus on Shannon leakage and min-entropy leakage.


5. Location Privacy and geo-indistinguishability
Quantitative Information Flow

Information Flow: Leakage of secret information via correlated observables

Ideally: No leak
- No interference [Goguen & Meseguer’82]

In practice: There is almost always some leak
- Intrinsic to the system (public observables, part of the design)
- Side channels

☞ need quantitative ways to measure the leak
Password checker

Password: $K_1 K_2 \ldots K_N$
Input by the user: $x_1 x_2 \ldots x_N$
Output: $out$ (Fail or OK)

Intrinsic leakage

By learning the result of the check the adversary learns something about the secret

```
out := OK
for i = 1, ..., N do
    if $x_i \neq K_i$ then
        out := FAIL
    end if
end for
```
Example 1

Password checker 2

Password: $K_1 K_2 \ldots K_N$
Input by the user: $x_1 x_2 \ldots x_N$
Output: $out$ (Fail or OK)

More efficient, but what about security?

```plaintext
\begin{verbatim}
out := OK
for i = 1, \ldots, N do
    if $x_i \neq K_i$ then
        out := FAIL
        exit()
    end if
end for
\end{verbatim}
```
Password checker 2

Password: $K_1 K_2 \ldots K_N$
Input by the user: $x_1 x_2 \ldots x_N$
Output: $out$ (Fail or OK)

Side channel attack

If the adversary can measure the execution time, then he can also learn the longest correct prefix of the password
Example 2

Example of Anonymity Protocol: DC Nets [Chaum’88]

- A set of nodes with some communication channels (edges).
- One of the nodes (source) wants to broadcast one bit $b$ of information.
- The source (broadcaster) must remain anonymous.
A set of nodes with some communication channels (edges).

One of the nodes (source) wants to broadcast one bit $b$ of information.

The source (broadcaster) must remain anonymous.

Example of Anonymity Protocol: DC Nets [Chaum’88]
Chaum’s solution

- Associate to each edge a fair binary coin
Chaum’s solution

- Associate to each edge a fair binary coin
- Toss the coins
Chaum’s solution

- Associate to each edge a fair binary coin
- Toss the coins
- Each node computes the binary sum of the incident edges. The source adds $b$. They all broadcast their results

$\ b = 1$
Chaum’s solution

• Associate to each edge a fair binary coin

• Toss the coins

• Each node computes the binary sum of the incident edges. The source adds $b$. They all broadcast their results

• Achievement of the goal:
  Compute the total binary sum: it coincides with $b$
Anonymity of DC Nets

**Observables:** An (external) attacker can only see the declarations of the nodes

**Question:** Does the protocol protects the anonymity of the source?
If the graph is connected and the coins are fair, then for an external observer, the protocol satisfies **strong anonymity**:

The *a posteriori* probability that a certain node is the source is equal to its *a priori* probability.

- A priori / a posteriori = before / after observing the declarations
Example 3: Crowds [Rubin and Reiter’98]

- Problem: A user (initiator) wants to send a message anonymously to another user (dest.)
- Crowds: A group of n users who agree to participate in the protocol.
- The initiator selects randomly another user (forwarder) and forwards the request to her
- A forwarder randomly decides whether to send the message to another forwarder or to dest.
- ... and so on
Example 3: Crowds [Rubin and Reiter’98]

- Problem: A user (initiator) wants to send a message anonymously to another user (dest.)
- Crowds: A group of n users who agree to participate in the protocol.
- The initiator selects randomly another user (forwarder) and forwards the request to her.
- A forwarder randomly decides whether to send the message to another forwarder or to dest.
- ... and so on

**Probable innocence:** under certain conditions, an attacker who intercepts the message from x cannot attribute more than 0.5 probability to x to be the initiator.
Common features

- **Secret information**
  - Password checker: The password
  - DC: the identity of the source
  - Crowds: the identity of the initiator

- **Public information (Observables)**
  - Password checker: The result (OK / Fail) and the execution time
  - DC: the declarations of the nodes
  - Crowds: the identity of the agent forwarding to a corrupted user

- **The system may be probabilistic**
  - Often the system uses randomization to obfuscate the relation between secrets and observables
  - DC: coin tossing
  - Crowds: random forwarding to another user
The basic model:

Systems = Information-Theoretic channels
Probabilistic systems are **noisy** channels: an output can correspond to different inputs, and an input can generate different outputs, according to a prob. distribution.

\[ p(o_j|s_i) \]: the conditional probability to observe \( o_j \) given the secret \( s_i \)
A channel is characterized by its matrix: the array of conditional probabilities

\[
p(o|s) = \frac{p(o \text{ and } s)}{p(s)}
\]

In a information-theoretic channel these conditional probabilities are independent from the input distribution

This means that we can model systems abstracting from the input distribution
Particular case: **Deterministic systems**
In these systems an input generates only one output
Still interesting: the problem is how to retrieve the input from the output

The entries of the channel matrix can be only 0 or 1
Example: DC nets (ring of 3 nodes, $b=1$)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, $b=1$)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, $b=1$)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, b=1)

<table>
<thead>
<tr>
<th></th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>n₀</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
</tr>
<tr>
<td>n₁</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
</tr>
<tr>
<td>n₂</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
</tr>
</tbody>
</table>

fair coins: \(\Pr(0) = \Pr(1) = \frac{1}{2}\)

strong anonymity

biased coins: \(\Pr(0) = \frac{2}{3}\), \(\Pr(1) = \frac{1}{3}\)

The source is more likely to declare 1 than 0
Quantitative Information Flow

• Intuitively, the leakage is the (probabilistic) information that the adversary gains about the secret through the observables.

• Each observable changes the prior probability distribution on the secret values into a posterior probability distribution according to the Bayes theorem.

• In the average, the posterior probability distribution gives a better hint about the actual secret value.
Observables: prior $\Rightarrow$ posterior
Observables: prior $\Rightarrow$ posterior

<table>
<thead>
<tr>
<th>p(n)</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
</tr>
</tbody>
</table>

$p(o|n)$
conditional prob
### Observables: prior $\Rightarrow$ posterior

<table>
<thead>
<tr>
<th>$p(n)$</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
</tr>
</tbody>
</table>

| $p(o|n)$ | 001 | 010 | 100 | 111 |
|--------|-----|-----|-----|-----|
| $n_0$ | $\frac{1}{6}$ | $\frac{1}{9}$ | $\frac{1}{9}$ | $\frac{1}{9}$ |
| $n_1$ | $\frac{1}{18}$ | $\frac{1}{12}$ | $\frac{1}{18}$ | $\frac{1}{18}$ |
| $n_2$ | $\frac{1}{18}$ | $\frac{1}{18}$ | $\frac{1}{12}$ | $\frac{1}{18}$ |

<table>
<thead>
<tr>
<th>$p(n,o)$</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n_0$</td>
<td>001</td>
<td>010</td>
<td>100</td>
<td>111</td>
</tr>
<tr>
<td>$n_1$</td>
<td>001</td>
<td>010</td>
<td>100</td>
<td>111</td>
</tr>
<tr>
<td>$n_2$</td>
<td>001</td>
<td>010</td>
<td>100</td>
<td>111</td>
</tr>
</tbody>
</table>

- $p(n)$: prior probability
- $p(o|n)$: conditional probability
- $p(n,o)$: joint probability
### Observables: prior $\Rightarrow$ posterior

<table>
<thead>
<tr>
<th>$p(n)$</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p(o)$</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{5}{18}$</td>
<td>$\frac{1}{4}$</td>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td></td>
</tr>
</tbody>
</table>

| $p(o|n)$ conditional prob | $p(n,o)$ joint prob |
|---------------------------|---------------------|
| $\frac{1}{6}$ | $\frac{1}{9}$ | $\frac{1}{9}$ | $\frac{1}{9}$ |
| $\frac{1}{18}$ | $\frac{1}{12}$ | $\frac{1}{18}$ | $\frac{1}{18}$ |
| $\frac{1}{18}$ | $\frac{1}{18}$ | $\frac{1}{12}$ | $\frac{1}{18}$ |
### Bayes Theorem

The Bayes theorem in this context is given by:

\[ p(n|o) = \frac{p(n, o)}{p(o)} \]

### Joint Probabilities, Conditional Probabilities, and Observed Probabilities

#### Post-Secret Probabilities

<table>
<thead>
<tr>
<th></th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
</tbody>
</table>

#### Observed Probabilities

<table>
<thead>
<tr>
<th></th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
</tbody>
</table>

### Conditional Probabilities

<table>
<thead>
<tr>
<th></th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
</tbody>
</table>

### Joint Probabilities

<table>
<thead>
<tr>
<th></th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
</tbody>
</table>

### Observed Probabilities

<table>
<thead>
<tr>
<th></th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
<tr>
<td>0.1</td>
<td>0.333</td>
<td>0.222</td>
<td>0.222</td>
<td>0.222</td>
</tr>
</tbody>
</table>
Let us construct the channel matrix

Note: The string $x_1x_2x_3$ typed by the user is a parameter, and $K_1K_2K_3$ is the channel input

The standard view is that the input represents the secret. Hence we should take $K_1K_2K_3$ as the channel input
Let us construct the channel matrix

Assume the user string is $x_1x_2x_3 = 110$

Input: $K_1 K_2 K_3 \in \{000, 001, \ldots, 111\}$
Output: $out \in \{\text{OK}, \text{FAIL}\}$

Different values of $x_1x_2x_3$ give different channel matrices, but they all have this kind of shape (seven inputs map to Fail, one maps to OK)
Password-checker 2

Assume the user string is $x_1x_2x_3 = 110$

Assume the adversary can measure the execution time

Let us construct the channel matrix

Input: $K_1K_2K_3 \in \{000, 001, \ldots, 111\}$

Output: $out \in \{\text{OK}, (\text{FAIL}, 1), (\text{FAIL}, 2), (\text{FAIL}, 3)\}$
Exercise 1

- Assuming that the possible passwords have uniform prior distribution, compute the matrix of the joint probabilities, and the posterior probabilities, for the two password-checker programs.
Example: DC nets. Ring of 2 nodes, and assume $b = 1$

Let us construct the channel matrix

Input: $n_0, n_1$

Output: the declarations of $n_1$ and $n_0$: $d_1d_0 \in \{01, 10\}$
Example: DC nets. Ring of 2 nodes, and assume $b = 1$

Let us construct the channel matrix

**Input:** $n_0, n_1$

**Output:** the declarations of $n_1$ and $n_0$: $d_1d_0 \in \{01, 10\}$

Fair coin: $p(0) = p(1) = \frac{1}{2}$

<table>
<thead>
<tr>
<th></th>
<th>01</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n_0$</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
</tr>
<tr>
<td>$n_1$</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
</tr>
</tbody>
</table>

Biased coin: $p(0) = \frac{2}{3}$ $p(1) = \frac{1}{3}$

<table>
<thead>
<tr>
<th></th>
<th>01</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n_0$</td>
<td>$\frac{2}{3}$</td>
<td>$\frac{1}{3}$</td>
</tr>
<tr>
<td>$n_1$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{3}$</td>
</tr>
</tbody>
</table>
Exercise 2

• Assuming that $n_0$ and $n_1$ have uniform prior distribution, compute the matrix of the joint probabilities, and the posterior probabilities, in the two cases of fair coins, and of biased coins

• Same exercise, but now assume that the prior distribution is $2/3$ for $n_0$ and $1/3$ for $n_1$
Information theory: useful concepts

- **Entropy** $H(X)$ of a random variable $X$
  - A measure of the degree of uncertainty of the events
  - It can be used to measure the vulnerability of the secret, i.e. how “easily” the adversary can discover the secret

- **Mutual information** $I(S;O)$
  - Degree of correlation between the input $S$ and the output $O$
  - Formally defined as difference between:
    - $H(S)$, the entropy of $S$ before knowing, and
    - $H(S|O)$, the entropy of $S$ after knowing $O$
  - It can be used to measure the leakage:
    \[
    \text{Leakage} = I(S;O) = H(S) - H(S|O)
    \]
  - $H(S)$ depends only on the prior; $H(S|O)$ can be computed using the prior and the channel matrix
Entropy and Operational Interpretation

In the realm of security, there is no unique notion of entropy. A suitable notion of entropy should have an **operational interpretation** in terms of the kind of **adversary** we want to **model**, namely:

- the kind of attack, and
- how we measure its success

A general **model of adversary** [Köpf and Basin, CCS’07]:

- Assume an oracle that answers yes/no to questions of a certain form.
- The adversary is defined by the form of the questions, and the measure of success of the attack.
- In general we consider the best strategy for the attacker, with respect to a given measure of success.
Entropy

Case 1:

- The questions are of the form: “is $S \in P$ ?”
- The measure of success is: the expected number of questions needed to find the value of $S$ in the attacker’s best strategy

Exercise: guessing a password in case of uniform distribution

Example: $S \in \{ a, b, c, d, e, f, g, h \}$

$$p(a) = p(b) = \frac{1}{4} \quad p(c) = p(d) = \frac{1}{8} \quad p(e) = p(f) = p(g) = p(h) = \frac{1}{16}$$

It is possible to prove that the best strategy for the adversary is to split each time the search space in two subspaces with probability masses as close as possible. This gives an almost perfectly balanced tree in terms of masses.
In the best strategy, the number of questions needed to determine the value of the secret $S$, when $S = s$, is: $- \log p(s)$ (log is in base 2)

This is in case we can construct a \textit{perfectly balanced tree}.
In most cases we can only construct an \textit{almost perfectly balanced tree}, so this formula is an approximation.

hence the \textbf{expected number} of question is:

$$H(S) = - \sum_{s} p(s) \log p(s)$$

This is exactly the formula for \textbf{Shannon entropy}.

\textbf{Conclusion:} For this model of adversary, the degree of protection of the secret, i.e., the degree of difficulty for the adversary to perform his attack, is measured by Shannon entropy.
Shannon entropy: information-theoretic int.

Information-theoretic interpretation:

$H(S)$ is the expected length of the optimal encoding of the values of $S$

For the strategy in previous example:  

- a: 01
- b: 10
- c: 000
- d: 111
- e: 0010
- f: 0011
- g: 1100
- h: 1101
Shannon entropy: properties

In general, the entropy is highest when the distribution is uniform.
If $|S| = n$, and the distribution is uniform, then $H(S) = \log n$

$S = \{a, b, c, d, e, f, g, h\}$ \hspace{1cm} p(a) = p(b) = \ldots = p(f) = \frac{1}{8}$

$H(S) = -8\frac{1}{8} \log \frac{1}{8} = \log 8 = 3$

$p(a) = p(b) = \frac{1}{4}$ \hspace{1cm} p(c) = p(d) = \frac{1}{8}$ \hspace{1cm} p(e) = p(f) = p(g) = p(h) = \frac{1}{16}$

$H(S) = -\sum_{s} p(s) \log p(s)$

$= -2\frac{1}{4} \log \frac{1}{4} - 2\frac{1}{8} \log \frac{1}{8} - 4\frac{1}{16} \log \frac{1}{16}$

$= 1 + \frac{3}{4} + 1$

$= \frac{11}{4}$
Shannon entropy: properties

The entropy is a concave function of the probability distribution

\[ S = \{a, b\} \]
\[ p(a) = x \quad p(b) = 1 - x \]
\[ H(S) \]

\[ S = \{a, b, c\} \]
\[ p(a) = x \quad p(b) = y \quad p(c) = 1 - (x + y) \]
\[ H(S) \]
An observable $o$ determines a new distribution on $S$:

$$p(s|o) = p(s) \frac{p(o|s)}{p(o)}$$

Bayes theorem

The entropy of the new distribution on $S$, given that $O = o$, is:

$$H(S|O = o) = -\sum_s p(s|o) \log p(s|o)$$

The conditional entropy is the expected value of the updated entropies:

$$H(S|O) = \sum_o p(o) H(S|O = o)$$

$$= -\sum_o p(o) \sum_s p(s|o) \log p(s|o)$$
Shannon mutual information

- In general \( H(S) \geq H(S|O) \)
  - the entropy may increase after one single observation, but in the average it cannot increase

- \( H(S) = H(S|O) \) if and only if \( S \) and \( O \) are independent
  - This is the case if and only if all rows of the channel matrix are the same
  - This case corresponds to strong anonymity in the sense of Chaum

- Shannon capacity \( C = \max I(S;O) \) over all priors (worst-case leakage)