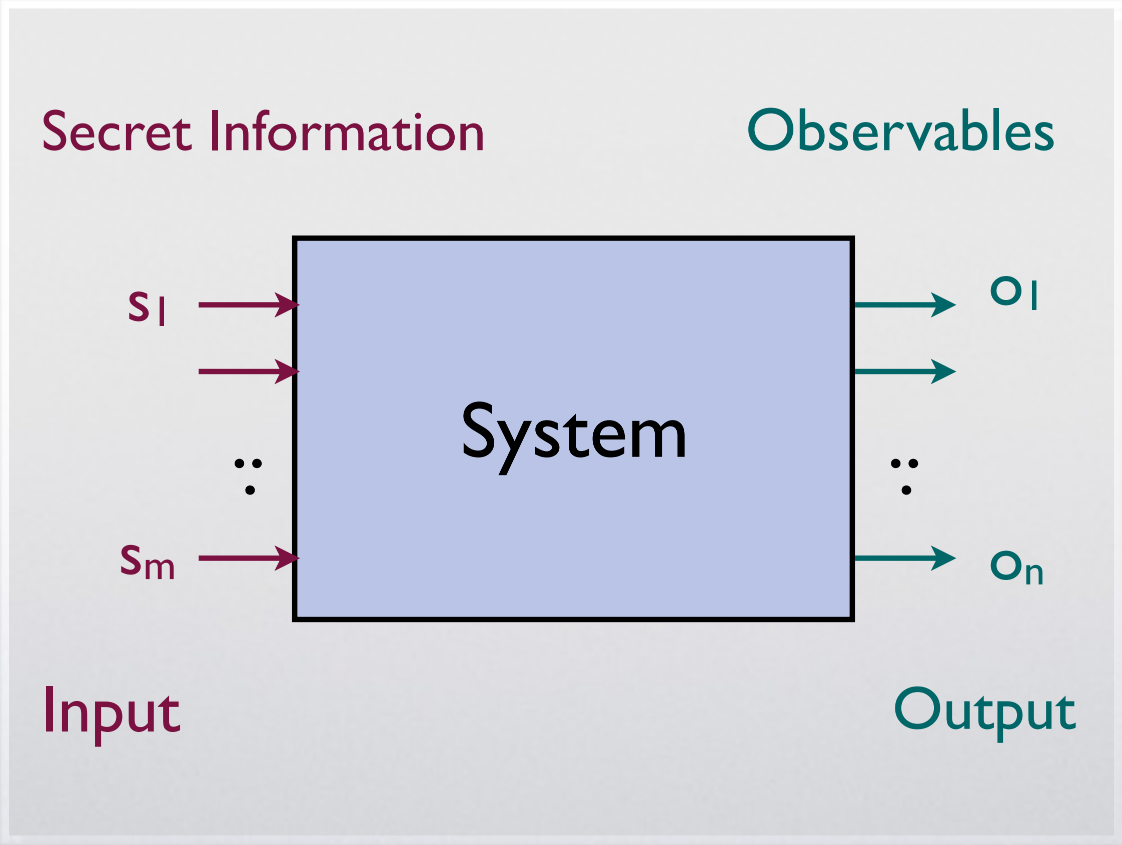
Quantitative Information Flow

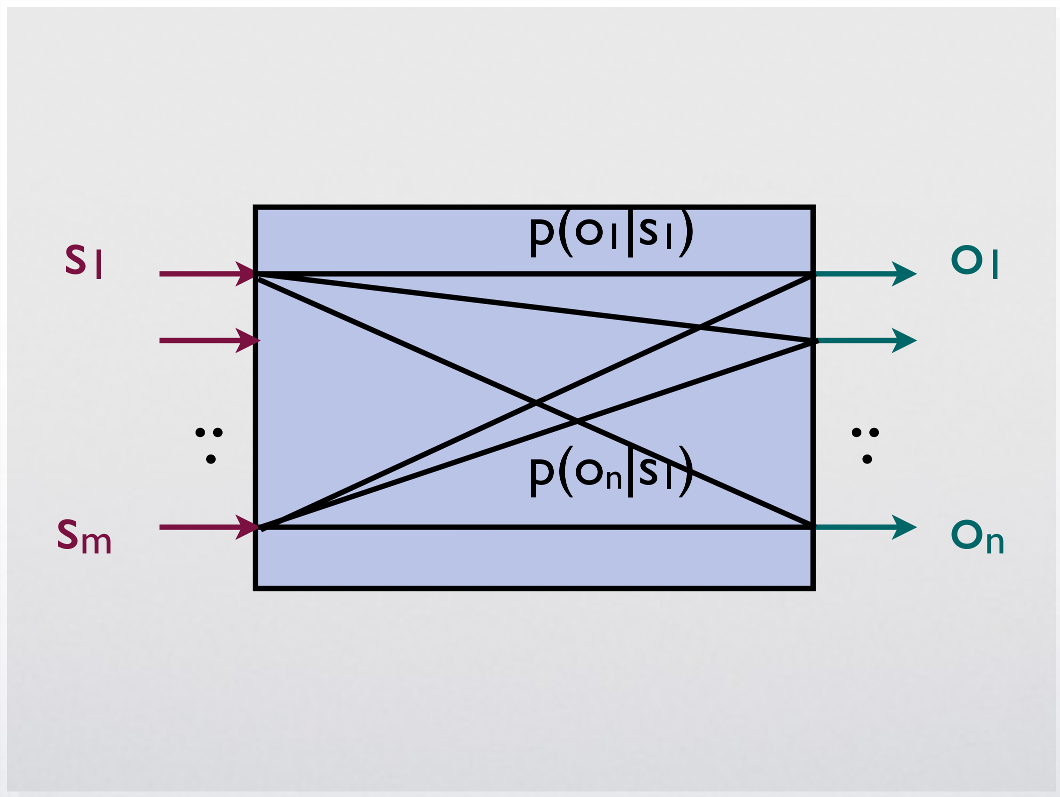
Lecture 7

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

	o_1	$\dots$	o_n
s_1	$p(o_1 \mid s_1)$	$\dots$	$p(o_n \mid s_1)$
$\vdots$	$\vdots$		
s_m	$p(o_1 \mid s_m)$		$p(o_n \mid s_m)$

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

A channel is characterized by its matrix: the array of conditional probabilities

In a information-theoretic channel these conditional probabilities are independent from the input distribution; they depend only in the way the channel operates on the inputs.

In our case, the conditional probabilities depend only on the way the system works. We assume that this is known to the adversary.

Password-checker 1

$out := \mathsf{OK}$
for $i = 1, \ldots, N$ **do**
  if $x_i \neq K_i$ **then**
    $out := \mathsf{FAIL}$

  end if
end for

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

Password-checker 1

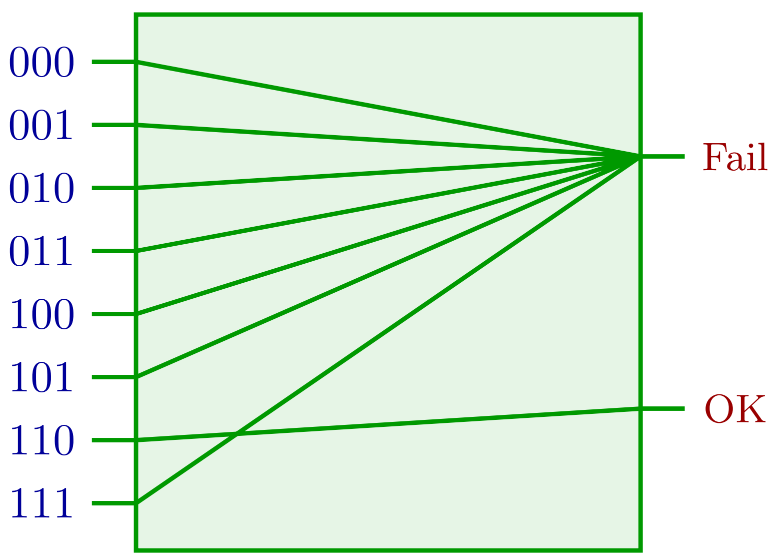
```
out := OK
for i = 1, ..., N do
    if x_i ≠ K_i then
        out := FAIL

    end if
end for
```

Assume the user string is $x_1 x_2 x_3 = 110$

Let us construct the channel matrix

Input: $K_1 K_2 K_3 \in \{000, 001, \ldots, 111\}$

Output: $out \in \{\mathsf{OK}, \mathsf{FAIL}\}$



	Fail	OK
000	1	0
001	1	0
010	1	0
011	1	0
100	1	0
101	1	0
110	0	1
111	1	0

Different values of $x_1 x_2 x_3$ give different channel matrices, but they all have this kind of shape (seven inputs map to Fail, one maps to OK)

Password-checker 2

```
out := OK
for i = 1, ..., N do
  if x_i ≠ K_i then
    { out := FAIL
      exit() }
  end if
end for
```

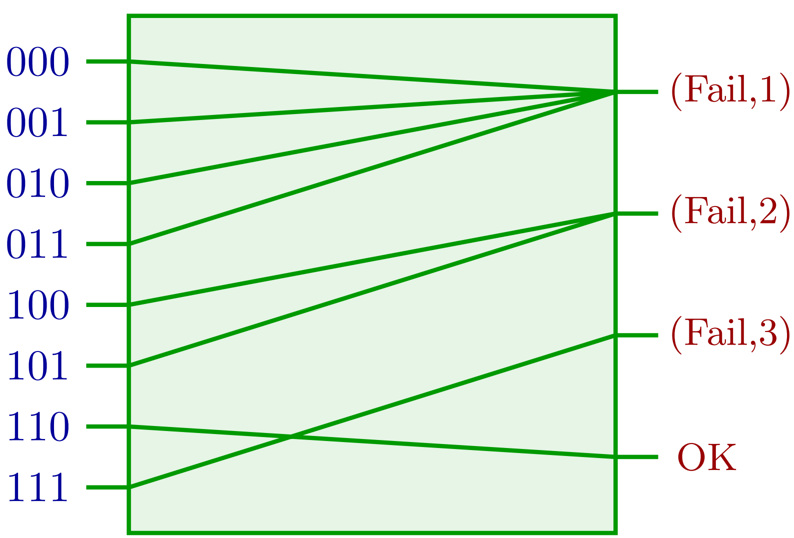
Assume the user string is $x_1 x_2 x_3 = 110$

Assume the adversary can measure the execution time

Let us construct the channel matrix

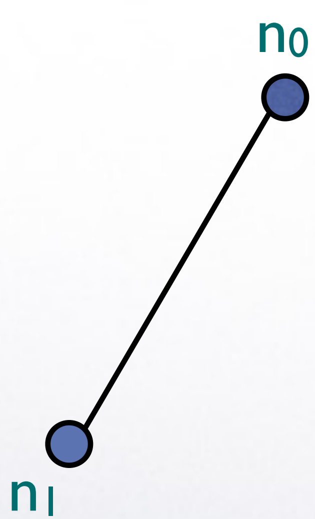
Input: $K_1 K_2 K_3 \in \{000, 001, \ldots, 111\}$

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



	(Fail, 1)	(Fail, 2)	(Fail, 3)	OK
000	1	0	0	0
001	1	0	0	0
010	1	0	0	0
011	1	0	0	0
100	0	1	0	0
101	0	1	0	0
110	0	0	0	1
111	0	0	1	0

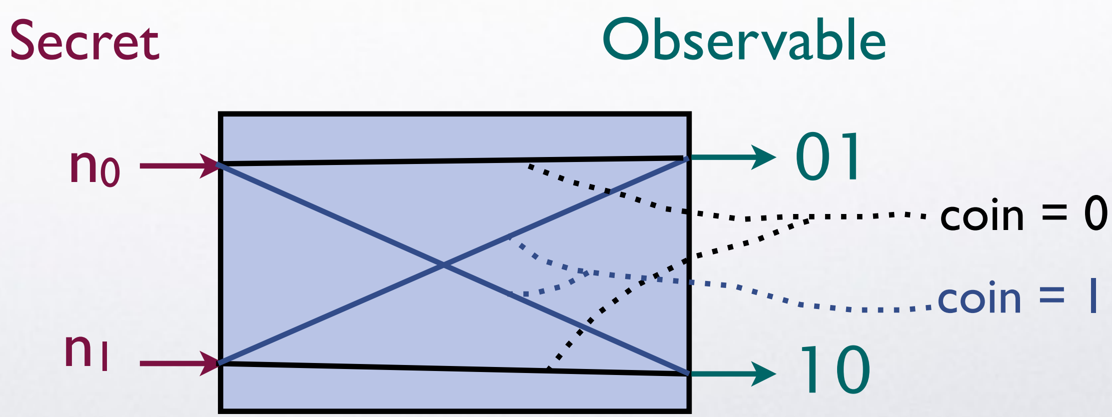
Example: DC nets. Ring of 2 nodes, and assume b = 1



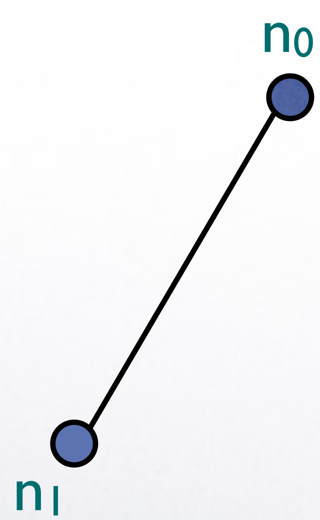
Let us construct the channel matrix

Input: n_0 , n_1

Output: the declarations of n_1 and n_0: $d_1 d_0 \in \{01, 10\}$



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: $d_1 d_0 \in \{01, 10\}$

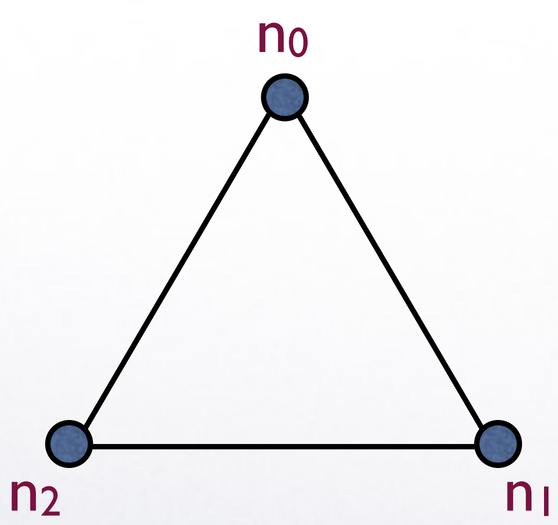
Fair coin: $p(0) = p(1) = ½$

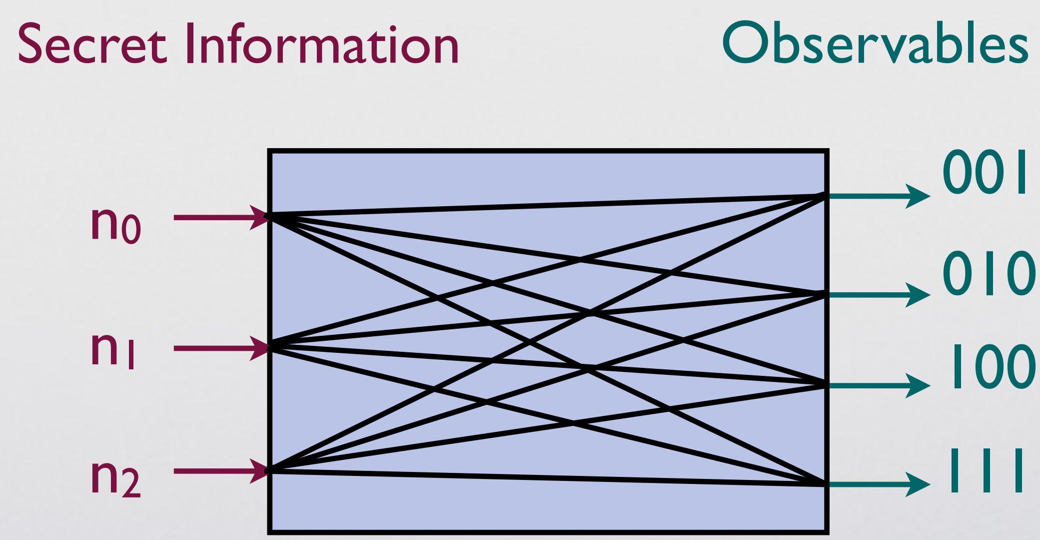
	01	10
n_0	½	½
n_1	½	½

Biased coin: $p(0) = ⅔$ $p(1) = ⅓$

	01	10
n_0	⅔	⅓
n_1	⅓	⅔

Example: DC nets (ring of 3 nodes, b=1)





Example: DC nets (ring of 3 nodes, b=1)

	001	010	100	111
n_0	¼	¼	¼	¼
n_1	¼	¼	¼	¼
n_2	¼	¼	¼	¼

	001	010	100	111
n_0	⅓	2/9	2/9	2/9
n_1	2/9	⅓	2/9	2/9
n_2	2/9	2/9	⅓	2/9

fair coins: $\Pr(0) = \Pr(1) = ½$

strong anonymity

biased coins: $\Pr(0) = ⅔$, $\Pr(1) = ⅓$

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 ⇒ posterior

$p(n)$		001	010	100	111
½	n_0	⅓	$^2/_9$	$^2/_9$	$^2/_9$
¼	n_1	$^2/_9$	⅓	$^2/_9$	$^2/_9$
¼	n_2	$^2/_9$	$^2/_9$	⅓	$^2/_9$

prior secret prob

$p(o|n)$
conditional prob

Observables: prior ⇒ posterior

$p(n)$		001	010	100	111
$1/2$	n_0	$1/3$	$2/9$	$2/9$	$2/9$
$1/4$	n_1	$2/9$	$1/3$	$2/9$	$2/9$
$1/4$	n_2	$2/9$	$2/9$	$1/3$	$2/9$

prior secret prob

$p(o|n)$
conditional prob

	001	010	100	111
n_0	$1/6$	$1/9$	$1/9$	$1/9$
n_1	1/18	1/12	1/18	1/18
n_2	1/18	1/18	1/12	1/18

$p(n,o)$
joint prob

Observables: prior ⇒ posterior

p(n)		001	010	100	111
$\frac{1}{2}$	n_0	$\frac{1}{3}$	$\frac{2}{9}$	$\frac{2}{9}$	$\frac{2}{9}$
$\frac{1}{4}$	n_1	$\frac{2}{9}$	$\frac{1}{3}$	$\frac{2}{9}$	$\frac{2}{9}$
$\frac{1}{4}$	n_2	$\frac{2}{9}$	$\frac{2}{9}$	$\frac{1}{3}$	$\frac{2}{9}$

prior secret prob

p(o|n)
conditional prob

	001	010	100	111
p(o)	$\frac{5}{18}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{2}{9}$
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	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{18}$

obs prob

p(n,o)
joint prob

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

Bayes theorem

p(o)	5/18	1/4	1/4	2/9

obs prob

p(n|001)		001	010	100	111
3/5	n_0	1/3	2/9	2/9	2/9
1/5	n_1	2/9	1/3	2/9	2/9
1/5	n_2	2/9	2/9	1/3	2/9

post secret prob

p(o|n)
conditional prob

	001	010	100	111
n_0	1/6	1/9	1/9	1/9
n_1	1/18	1/12	1/18	1/18
n_2	1/18	1/18	1/12	1/18

p(n,o)
joint prob

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

Exercise 2

- **DC net with 2 nodes:** 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

Towards a quantitative notion of leakage

A general principle:

Leakage	=	difference between
		the a priori vulnerability
		and
		the a posteriori vulnerability

- vulnerability = vulnerability of the secret,
- a priori / a posteriori = before / after the observation

Intuitively the vulnerability depends on the distribution: the more uncertainty there is about the exact value of the secret, the less vulnerable the secret is.

Note that the observation updates the input probability:

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

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

Notions of Entropy

- In Information Theory, there are several notions of entropy:
  - Shannon's entropy (which is the most famous),
  - the Rényi's entropies,
  - guessing entropy
  - …
- Which one should we choose ?