CS 591: Formal Methods in Security and Privacy
Probabilistic Relational Hoare Logic

Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu
From the previous classes
An example

\textbf{OneTimePad}(m : private msg) : public msg
key := $ \text{Uniform}(\{0,1\}^n)$;
cipher := m xor key;
return cipher

Learning a ciphertext does not change any a priori knowledge about the likelihood of messages.
Probabilistic Noninterference

In symbols, $c$ is probabilistically noninterferent if and only if for every $m_1 \sim_{\text{low}} m_2 : \{c\}_{m_1} = \mu_1$ and $\{c\}_{m_2} = \mu_2$ implies $\mu_1 \sim_{\text{low}} \mu_2$.
Revisiting the example

```
OneTimePad(m : private msg) : public msg
key := Uniform({0,1}^n);
cipher := m xor key;
return cipher
```
Revisiting the example

\textbf{OneTimePad}(m : \text{private msg}) : \text{public msg}
key := \$ \text{Uniform}\left(\{0,1\}^n\right);
cipher := m \text{ xor key};
return cipher

\text{m}_1 \quad \text{m}_2
OneTimePad(m : private msg) : public msg
key ::= Uniform({0,1}^n);
cipher := m xor key;
return cipher

\[ m_1 \oplus k \]

\[ m_1 \]

\[ m_2 \]
Revisiting the example

\[ \textbf{OneTimePad}(m : \text{private msg}) : \text{public msg} \]

\[
\begin{align*}
\text{key} & := \$ \text{Uniform}\{(0,1)^n\}; \\
\text{cipher} & := m \oplus \text{key}; \\
\text{return} & \text{cipher}
\end{align*}
\]

Suppose we can now choose the key for \( m_2 \). What could we choose?
Revisiting the example

OneTimePad (m : private msg) : public msg
key := Uniform({0,1}^n);
cipher := m xor key;
return cipher

Suppose we can now chose the key for m_2. What could we choose?
Coupling

$\mu_1$

$\mu_2$
Coupling

$\mu_1$

$\mu_2$
Example of Our Coupling

\[ k_1 = m_1 \oplus k_2 \oplus m_2 \]

\[ k_1 = 10 \oplus k_2 \oplus 00 \]
Example of Our Coupling

\[ k_1 = m_1 \oplus k_2 \oplus m_2 \]

\[ k_1 = 10 \oplus k_2 \oplus 00 \]
Coupling formally
Given two distributions \( \mu_1 \in \mathcal{D}(A) \), and \( \mu_2 \in \mathcal{D}(B) \), a coupling between them is a joint distribution \( \mu \in \mathcal{D}(A \times B) \) whose marginal distributions are \( \mu_1 \) and \( \mu_2 \), respectively.

\[
\pi_1(\mu)(a) = \sum_b \mu(a, b) \\
\pi_2(\mu)(b) = \sum_a \mu(a, b)
\]
Probabilistic Relational Hoare Quadruples

Program_1 \sim Program_2

\begin{align*}
\text{Precondition} & : \quad c_1 \sim c_2 \\
\text{Postcondition} & : \quad P \Rightarrow Q
\end{align*}
Validity of Probabilistic Hoare quadruple

We say that the quadruple $c_1 \leadsto c_2 : P \Rightarrow Q$ is valid if and only if for every pair of memories $m_1, m_2$ such that $P(m_1, m_2)$ we have:

$\{c_1\}_{m_1} = \mu_1$ and $\{c_2\}_{m_2} = \mu_2$ implies $Q(\mu_1, \mu_2)$. 
Validity of Probabilistic Hoare quadruple

We say that the quadruple \( c_1 \sim c_2 : P \Rightarrow Q \) is valid if and only if for every pair of memories \( m_1, m_2 \) such that \( P(m_1, m_2) \) we have:

\[ \{c_1\}_{m_1} = \mu_1 \quad \text{and} \quad \{c_2\}_{m_2} = \mu_2 \]

implies \( Q(\mu_1, \mu_2) \).

Is this correct?!!
Today: Probabilistic Relational HL
Relational Assertions

$c_1 \sim c_2 : P \Rightarrow Q$

logical formula over pair of memories
(i.e. relation over memories)

logical formula over ????
\textbf{R-Coupling}

Given two distributions $\mu_1 \in \mathcal{D}(A)$, and $\mu_2 \in \mathcal{D}(B)$, an \textit{R-coupling} between them, for $R \subseteq A \times B$, is a joint distribution $\mu \in \mathcal{D}(A \times B)$ such that:

1) the marginal distributions of $\mu$ are $\mu_1$ and $\mu_2$, respectively,

2) the support of $\mu$ is contained in $R$. That is, if $\mu(a,b) > 0$, then $(a,b) \in R$. 
We say that two subdistributions $\mu_1 \in D(A)$ and $\mu_2 \in D(B)$ are in the relational lifting of the relation $R \subseteq A \times B$, denoted $\mu_1 \ R^* \mu_2$ if and only if there exist an $R$-coupling between them.
Validity of Probabilistic Hoare quadruple

We say that the quadruple $c_1 \sim c_2 : P \Rightarrow Q$ is valid if and only if for every pair of memories $m_1, m_2$ such that $P(m_1, m_2)$ we have:

$\{c_1\}_{m_1} = \mu_1$ and $\{c_2\}_{m_2} = \mu_2$ implies $Q^*(\mu_1, \mu_2)$. 
Probabilistic Relational Hoare Logic
Skip

\[ \vdash \text{skip} \sim \text{skip} : P \Rightarrow P \]
Probabilistic Relational Hoare Logic
Assignment

\[ \vdash x_1 := e_1 \sim x_2 := e_2 : \]

\[ P [ e_1<1>/x_1<1>, e_2<2>/x_2<2> ] \Rightarrow P \]
Probabilistic Relational Hoare Logic Composition

\[ \vdash C_1 \sim C_2 : P \Rightarrow R \quad \vdash C_1' \sim C_2' : R \Rightarrow S \]

\[ \vdash C_1 ; C_1' \sim C_2 ; C_2' : P \Rightarrow S \]
We can **weaken** $P$, i.e. replace it by something that is implied by $P$. In this case $S$.

We can **strengthen** $Q$, i.e. replace it by something that implies $Q$. In this case $R$. 

$$
\begin{align*}
P &\Rightarrow S \\
\vdash c_1 \sim c_2 : S &\Rightarrow R \\
R &\Rightarrow Q \hline
\vdash c_1 \sim c_2 : P &\Rightarrow Q
\end{align*}
$$
Probabilistic Relational Hoare Logic
If-then-else

\[ P \Rightarrow (e_1 < 1> \iff e_2 < 2>) \]
\[ \vdash c_1 \sim c_2 : e_1 < 1> \land P \Rightarrow Q \]
\[ \vdash c_1' \sim c_2' : \neg e_1 < 1> \land P \Rightarrow Q \]

\[ \frac{\vdash \sim : P \Rightarrow Q}{\text{if } e_1 \text{ then } c_1 \text{ else } c_1'} \]
\[ \vdash \text{if } e_2 \text{ then } c_2 \text{ else } c_2' \]
Probabilistic Relational Hoare Logic

While

\[ P \Rightarrow (e_1 \langle 1 \rangle \ Leftrightarrow e_2 \langle 2 \rangle) \]

\[ \vdash c_1 \sim c_2 : e_1 \langle 1 \rangle \land P \Rightarrow P \]

while e_1 do c_1

\[ \vdash \sim : P \Rightarrow P \land \neg e_1 \langle 1 \rangle \]

while e_2 do c_2
Probabilistic Relational Hoare Logic

If-then-else - left

\[ \vdash c_1 \sim c_2 : e < 1 > \land P \Rightarrow Q \]

\[ \vdash c_1' \sim c_2 : \neg e < 1 > \land P \Rightarrow Q \]

\[ \vdash \sim c_2 : P \Rightarrow Q \]

if e then c₁ else c₁'
Probabilistic Relational Hoare Logic

If-then-else - right

\[ \vdash c_1 \sim c_2 : e<2> \land P \Rightarrow Q \]

\[ \vdash c_1 \sim c_2' : \neg e<2> \land P \Rightarrow Q \]

\[ \vdash c_1 \sim \neg c_2' : \neg e<2> \land P \Rightarrow Q \]

\[ \vdash \text{if } e \text{ then } c_2 \text{ else } c_2' : P \Rightarrow Q \]
Probabilistic Relational Hoare Logic
Assignment - left

\[ \vdash x := e \sim \text{skip}: \]
\[ P[e<1>/x<1>] \Rightarrow P \]
How about the random assignment?
\( \vdash x_1 := \$ d_1 \sim x_2 := \$ d_2 : ?? \)
We would like to have:

\[ P(m_1, m_2) \]

\[ \Rightarrow \]

\[ \text{let } a = \{d_1\}_{m_1} \text{ in unit}(m_1[x_1 \leftarrow a]) \]

\[ Q^* \]

\[ \text{let } a = \{d_2\}_{m_2} \text{ in unit}(m_2[x_2 \leftarrow a]) \]

\[ \vdash x_1 := \$ \ d_1 \sim x_2 := \$ \ d_2 : \ P \Rightarrow Q \]

What is the problem with this rule?
Restricted Probabilistic Expressions

We consider a restricted set of expressions denoting probability distributions.

\[ d ::= f(d_1, ..., d_k) \]

Where \( f \) is a distribution declaration

Some expression examples similar to the previous

- uniform(\{0,1\}^{128})
- bernoulli(.5)
- laplace(0,1)
Restricted Probabilistic Expressions

We consider a restricted set of expressions denoting probability distributions.

\[ d ::= f (d_1, ..., d_k) \]

Where \( f \) is a distribution declaration.

Some expression examples similar to the previous

\[ \text{uniform} (\{0,1\}^{128}) \quad \text{bernoulli} (.5) \quad \text{laplace} (0,1) \]

Notice that we don’t need a memory anymore to interpret them.
A sufficient condition for $R$-Coupling

Given two distributions $\mu_1 \in D(A)$, and $\mu_2 \in D(B)$, and a relation $R \subseteq A \times B$, if there is a mapping $h : A \rightarrow B$ such that:

1) $h$ is a bijective map between elements in $\text{supp}(\mu_1)$ and $\text{supp}(\mu_2)$,
2) for every $a \in \text{supp}(\mu_1)$, $(a, h(a)) \in R$
3) $\Pr_{x \sim \mu_1}[x = a] = \Pr_{x \sim \mu_2}[x = h(a)]$

Then, there is an $R$-coupling between $\mu_1$ and $\mu_2$. We write $h \triangleleft (\mu_1, \mu_2)$ in this case.
h ≜ (\{d_1\}, \{d_2\})

P = \forall v, v \in supp(\{d_1\})

\Rightarrow Q[v/x_1<1>, h(v)/x_2<2>]

\vdash x_1 := d_1 \sim x_2 := d_2 : P \Rightarrow Q
Back to our example

\begin{verbatim}
OneTimePad(m : private msg) : public msg
    key := Uniform({0,1}^n);
    cipher := m xor key;
    return cipher
\end{verbatim}
Back to our example

OneTimePad(m : private msg) : public msg

key := Uniform({0,1}^n);
cipher := m xor key;
return cipher
Back to our example

\begin{verbatim}
OneTimePad(m : private msg) : public msg
  key := \$ Uniform(\{0,1\}^n);
  cipher := m \text{ xor } key;
  return cipher
\end{verbatim}

\begin{center}
\begin{tabular}{c|c}
  m_1 & m_2 \\
\end{tabular}
\end{center}
Back to our example

\textbf{OneTimePad}(m : private msg) : public msg
key := Uniform(\{0,1\}^n);
cipher := m \oplus key;
return cipher

\[ m_1 \oplus k \]

\[ m_1 \]

\[ m_2 \]
Back to our example

OneTimePad(m : private msg) : public msg
key := Uniform(\{0,1\}^n);
cipher := m \oplus key;
return cipher

\[
\begin{align*}
m_1 & \rightarrow m_1 \oplus k \\
m_2 & \rightarrow m_2 \oplus (m_1 \oplus k \oplus m_2)
\end{align*}
\]
Back to our example

\textbf{OneTimePad} (m : private msg) : public msg
key := Uniform(\{0,1\}^n);
cipher := m \oplus key;
return cipher

\[d_1 = \text{Uniform}(\{0,1\}^n)\quad d_2 = \text{Uniform}(\{0,1\}^n)\]

Is this a good map?

\[h (k) = (m<1> \oplus k \oplus m<2>)\]
Back to our example

\textbf{OneTimePad}(m : \text{private msg}) : \text{public msg}

key := $\text{Uniform}\{0, 1\}^n$;
cipher := m \text{xor} key;
return cipher

\[d_1=\text{Uniform}\{0, 1\}^n\] \hspace{1cm} \[d_2=\text{Uniform}\{0, 1\}^n\]

Is this a good map?

\[h(k) = (m<1> \oplus k \oplus m<2>)\]

What is the relation?
Back to our example

```
OneTimePad(m : private msg) : public msg
    key := Uniform({0,1}^n);
    cipher := m xor key;
    return cipher
```

d_1 = Uniform({0,1}^n)
d_2 = Uniform({0,1}^n)

Is this a good map?

\[ h(k) = (m^{<1>} \oplus k \oplus m^{<2>}) \]

What is the relation?

\[ m^{<1>} \oplus k^{<1>} = m^{<2>} \oplus k^{<2>} \]
Back to our example

\[ d_1 = \text{Uniform}([0,1]^n) \quad \text{and} \quad d_2 = \text{Uniform}([0,1]^n) \]

Is this a good map?

\[ h(k) = (m^{<1>} \oplus k \oplus m^{<2>}) \]

1) it is bijective between elements in the support of \(\{d_1\}\) and \(\{d_2\}\)
2) for every \(k \in \text{supp}(\{d_1\})\), \(m^{<1>} \oplus k = m^{<2>} \oplus (m^{<1>} \oplus k \oplus m^{<2>})\)
3) \(P_{x \sim \{d_1\}}[x = v] = P_{x \sim \{d_2\}}[x = v]\)
Back to our example

\[ d_1 = \text{Uniform}(\{0, 1\}^n) \quad \quad \quad d_2 = \text{Uniform}(\{0, 1\}^n) \]

Is this a good map?

\[ h(k) = (m^{<1>} \oplus k \oplus m^{<2>}) \]

1) it is bijective between elements in the support of \{d_1\} and \{d_2\}
2) for every \( k \in \text{supp}(\{d_1\}) \), \( m^{<1>} \oplus k = m^{<2>} \oplus (m^{<1>} \oplus k \oplus m^{<2>}) \)
3) \( \Pr_{x \sim \{d_1\}}[x = v] = \Pr_{x \sim \{d_2\}}[x = v] \)

It is a good map!
Back to our example

\[ h(k) = (m<1> \oplus k \oplus m<2>) \triangleleft (\{d_1\}, \{d_2\}) \]

\[ P = \forall k, k \in \{0, 1\}^n \]

\[ \Rightarrow m<1> \oplus k_1<1> = m<2> \oplus k_2<2> \]

\[ [\text{v} / k_1<1>, h(\text{v}) / k_2<2>] = m<1> \oplus k = m<2> \oplus (m<1> \oplus k \oplus m<2>) \]

\[ \vdash k_1 : = \text{Uniform}\{0, 1\}^n \sim k_2 : = \text{Uniform}\{0, 1\}^n : \]

\[ \text{True} \Rightarrow m<1> \oplus k_1<1> = m<2> \oplus k_2<2> \]
Back to our example

\[ h(k) = (m^{<1>} \oplus k^{<1>} \oplus m^{<2>}) \triangleleft (\{d_1\}, \{d_2\}) \]

\[ P = \forall k, k \in \{0, 1\}^n \]

\[ \Rightarrow m^{<1>} \oplus k^{<1>} = m^{<2>} \oplus k^{<2>} \]

\[ [v / k^{<1>}, h(v) / k^{<2>}] = m^{<1>} \oplus k = m^{<2>} \oplus (m^{<1>} \oplus k \oplus m^{<2>}) \]

\[ \neg k_1 := \text{Uniform} \left( \{0,1\}^n \right) \sim k_2 := \text{Uniform} \left( \{0,1\}^n \right) : \]

\[ \text{True} \Rightarrow m^{<1>} \oplus k_1^{<1>} = m^{<2>} \oplus k_2^{<2>} \]

Using the assignment rule, we can conclude.
Soundness

If we can derive \( \vdash c_1 \sim c_2 : P \Rightarrow Q \) through the rules of the logic, then the quadruple \( c_1 \sim c_2 : P \Rightarrow Q \) is valid.
Completeness?