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

Marco Gaboardi gaboardi@bu.edu

Alley Stoughton stough@bu.edu

An example

```
OneTimePad(m : private msg) : public msg
  key :=$ 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 Relational Hoare

Quadruples

Precondition

Precondition

Program₁ ~ Program₂

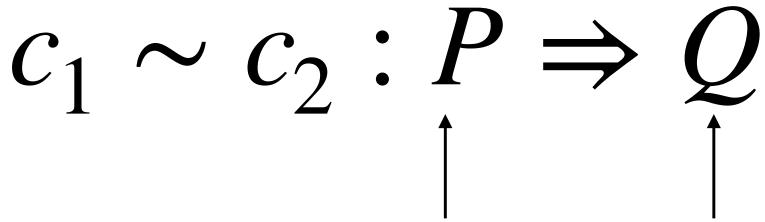
Postcondition

$$c_1 \sim c_2 : P \Rightarrow Q$$

Probabilistic Probabilistic Program Program

Postcondition

Relational Assertions



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

R-Coupling

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

- the marginal distributions of μ are μ₁ and μ₂, respectively,
- 2) the support of μ is contained in R. That is, if $\mu(a,b)>0$, then $(a,b)\in R$.

Relational lifting of a predicate

We say that two subdistributions $\mu_1 \in D(A)$ and $\mu_2 \in D(B)$ are in the relational lifting of the relation $R \subseteq AxB$, 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

⊢skip~skip:P⇒P

To show this rule correct we need to show the validity of the quadruple skip~skip: P⇒P.

To show this rule correct we need to show the validity of the quadruple skip~skip: P⇒P.

```
For every m_1, m_2 such that P(m,m') we have \{skip\}_m=unit(m) \text{ and } \{skip\}_{m'}=unit(m') \} we need P*(m,m').
```

Hskip~skip:P⇒P

⊢skip~skip:P⇒P

μ	m_1	m_2	 m'	
m_1	0	0	 0	0
m_2	0	0	 0	0
m	0	0	 1	0

μ	m_1	m_2	 m'	
m_1	0	0	 0	0
m_2	0	0	 0	0
m	0	0	 1	0

We need to show:

- 1) $\pi_1(\mu)$ =unit(m) and $\pi_2(\mu)$ =unit(m')
- 2) $(m,m') \in P$

A sufficient condition for R-Coupling

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

- h is a bijective map between elements in supp(µ₁) and supp(µ₂),
- 2) for every a∈supp(µ₁), (a,h(a))∈R
- 3) $Pr_{x\sim\mu1}[x=a]=Pr_{x\sim\mu2}[x=h(a)]$

Then, there is an R-coupling between μ_1 and μ_2 .

Probabilistic Relational Hoare Logic Random Assignment

1) h bijective between supp (μ 1) and supp (μ 2) 2) $\forall v \in \text{supp} (\{d_1\}) \Pr_{x \sim \{d1\}} [x=a] = \Pr_{x \sim \{d2\}} [x=h(a)]$ 3) $P = \forall v$, $v \in \text{supp} (\{d_1\}) \Rightarrow Q[v/x_1 < 1>, h(v)/x_2 < 2>]$

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

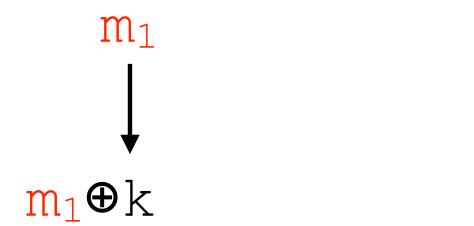
```
OneTimePad(m : private msg) : public msg
  key :=$ Uniform({0,1}n);
  cipher := m xor key;
  return cipher
```

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

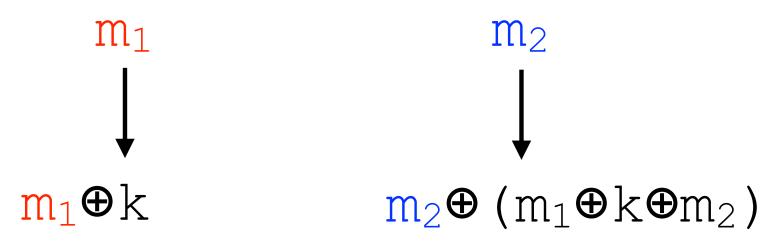
 m_1 m_2

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

 m_2



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



```
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) =
$$(m<1>\oplus k\oplus m<2>)$$

```
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?

```
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?

$$m<1>\oplus k<1>=m<2>\oplus k<2>$$

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

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

Is this a good map?

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

- 1) it is bijective between elements in the support of {d₁} and {d₂}
- 2) for every $k \in \text{supp}(\{d_1\})$, $m < 1 > \oplus k = m < 2 > \oplus (m < 1 > \oplus k \oplus m < 2 >)$
- 3) $Pr_{x\sim\{d1\}}[x=v]=Pr_{x\sim\{d2\}}[x=v]$

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

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

Is this a good map?

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

- 1) it is bijective between elements in the support of {d₁} and {d₂}
- 2) for every $k \in \text{supp}(\{d_1\})$, $m < 1 > \oplus k = m < 2 > \oplus (m < 1 > \oplus k \oplus m < 2 >)$
- 3) $Pr_{x\sim\{d1\}}[x=v]=Pr_{x\sim\{d2\}}[x=v]$

It is a good map!

```
h (k) = (m<1>⊕k⊕m<2>) \triangleleft ({d<sub>1</sub>}, {d<sub>2</sub>})

P=\forallk, k\in {0,1}<sup>n</sup>

⇒ m<1>⊕k<sub>1</sub><1>=m<2>⊕k<sub>2</sub><2>[v/k<sub>1</sub><1>, h (v)/k<sub>2</sub><2>] =

m<1>⊕k=m<2>⊕ (m<1>⊕k⊕m<2>)
```

```
\vdash k_1 := \$Uniform(\{0,1\}^n) \sim k_2 := \$Uniform(\{0,1\}^n) :
True \Rightarrow m < 1 > \oplus k_1 < 1 > = m < 2 > \oplus k_2 < 2 >
```

```
h (k) = (m<1>⊕k⊕m<2>) \triangleleft ({d<sub>1</sub>}, {d<sub>2</sub>})

P=\forallk, k\in {0,1}<sup>n</sup>

⇒ m<1>⊕k<sub>1</sub><1>=m<2>⊕k<sub>2</sub><2>[v/k<sub>1</sub><1>, h (v)/k<sub>2</sub><2>] =

m<1>⊕k=m<2>⊕ (m<1>⊕k⊕m<2>)
```

```
\vdash k_1 := \$Uniform(\{0,1\}^n) \sim k_2 := \$Uniform(\{0,1\}^n) :
True ⇒ m<1> ⊕ k_1<1> = m<2> ⊕ k_2<2>
```

Using the assignment rule, we can conclude.

Consequences of Coupling

Given the following pRHL judgment

$$\vdash c_1 \sim c_2 : \mathsf{True} \Rightarrow Q$$

We have that:

if
$$Q \Rightarrow (R\langle 1 \rangle \iff S\langle 2 \rangle)$$
, then $\Pr_{x \sim \{c_1\}_m}[x \in R] = \Pr_{x \sim \{c_2\}_{m'}}[x \in S]$

if
$$Q \Rightarrow (R\langle 1 \rangle \Rightarrow S\langle 2 \rangle)$$
, then $\Pr_{x \sim \{c_1\}_m} [x \in R] \le \Pr_{x \sim \{c_2\}_{m'}} [x \in S]$

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?