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

Program$_1$ ~ Program$_2$

Postcondition

Precondition

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

Probabilistic Program

Probabilistic Program

Postcondition

Relational Assertions

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

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

logical formula
over ????

R-Coupling

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

1) the marginal distributions of μ are μ_1 and μ_2, respectively,
2) the support of μ is contained in R. That is, if μ`(a,b)>0, then (a,b)`∈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 $\mathtt{R} \subseteq A\mathrm{x}B$, denoted $\mu_1\ \mathtt{R*}\ \mu_2$ 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:

$\{c_1\}_{m1} = \mu_1$ and $\{c_2\}_{m2} = \mu_2$ implies $Q^*(\mu_1, \mu_2)$.

Probabilistic Relational Hoare Logic

Skip

$$\frac{}{\vdash \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

Correctness of Skip Rule

$$\frac{}{\vdash \texttt{skip}\sim\texttt{skip}:\texttt{P}\Rightarrow\texttt{P}}$$

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

Correctness of Skip Rule

$$\frac{}{\vdash \mathtt{skip{\sim}skip:P{\Rightarrow}P}}$$

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

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

Correctness of Skip Rule

$$\frac{}{\vdash \mathtt{skip} \sim \mathtt{skip} : P \Rightarrow P}$$

Correctness of Skip Rule

$$\frac{}{\vdash \mathtt{skip} \sim \mathtt{skip} : P \Rightarrow P}$$

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

Correctness of Skip Rule

$$\frac{}{\vdash \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

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) $\pi_1(\mu)=\text{unit}(m)$ and $\pi_2(\mu)=\text{unit}(m')$
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 $R \subseteq A \times B$, if there is a mapping $h: A \to B$ such that:

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

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

Probabilistic Relational Hoare Logic

Random Assignment

$$\frac{\begin{array}{l} 1)\, h\ \ \text{bijective between}\ \mathtt{supp}(\mu 1)\ \text{and}\ \mathtt{supp}(\mu 2) \\ 2)\, \forall v \in \mathtt{supp}(\{d_1\})\, \mathtt{Pr}_{x\sim\{d1\}}[x=a]=\mathtt{Pr}_{x\sim\{d2\}}[x=h(a)] \\ 3)\, P=\forall v, v \in \mathtt{supp}(\{d_1\}) \Rightarrow Q[v/x_1<1>, h(v)/x_2<2>] \end{array}}{\vdash x_1 :=\$\ d_1 \sim x_2 :=\$\ d_2 : P \Rightarrow Q}$$

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

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

m_1 m_2

Back to our example

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

m_1

m_2

$m_1 \oplus k$

Back to our example

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

$$\begin{tikzcd}
m_1 \arrow[d] & m_2 \arrow[d] \\
m_1 \oplus k & m_2 \oplus (m_1 \oplus k \oplus m_2)
\end{tikzcd}$$

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?

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

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?

$$h(k)=(m\langle 1\rangle \oplus k \oplus m\langle 2\rangle)$$

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?

$$h(k)=(m\langle 1\rangle \oplus k \oplus m\langle 2\rangle)$$

What is the relation?

$$m\langle 1\rangle \oplus k\langle 1\rangle = m\langle 2\rangle \oplus k\langle 2\rangle$$

Back to our example

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 {d_1} and {d_2}
2) for every k$\in$supp({d_1}), m<1>$\oplus$k=m<2>$\oplus$(m<1>$\oplus$k$\oplus$m<2>)
3) $Pr_{x\sim\{d1\}}[x=v]= Pr_{x\sim\{d2\}}[x=v]$

Back to our example

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

Is this a good map?

$$h(k) = (m\langle 1\rangle \oplus k \oplus m\langle 2\rangle)$$

1) it is bijective between elements in the support of {d_1} and {d_2}
2) for every k∈supp({d_1}), m<1>⊕k=m<2>⊕(m<1>⊕k⊕m<2>)
3) $Pr_{x\sim\{d1\}}[x=v]= Pr_{x\sim\{d2\}}[x=v]$

It is a good map!

Back to our example

$$\dfrac{\begin{array}{l} h(k)=(m\langle 1\rangle \oplus k \oplus m\langle 2\rangle) \lhd (\{d_1\},\{d_2\}) \\ P=\forall k, k \in \{0,1\}^n \\ \Rightarrow\ m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle [v/k_1\langle 1\rangle, h(v)/k_2\langle 2\rangle] = \\ \quad m\langle 1\rangle \oplus k = m\langle 2\rangle \oplus (m\langle 1\rangle \oplus k \oplus m\langle 2\rangle) \end{array}}{\begin{array}{l} \vdash k_1 := \$Uniform(\{0,1\}^n) \sim k_2 := \$Uniform(\{0,1\}^n) : \\ \quad True \ \Rightarrow\ m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle \end{array}}$$

Back to our example

$$\frac{\begin{array}{l} h(k)=(m\langle 1\rangle \oplus k \oplus m\langle 2\rangle) \lhd (\{d_1\},\{d_2\}) \\ P=\forall k, k \in \{0,1\}^n \\ \Rightarrow\ m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle [v/k_1\langle 1\rangle, h(v)/k_2\langle 2\rangle] = \\ \quad m\langle 1\rangle \oplus k = m\langle 2\rangle \oplus (m\langle 1\rangle \oplus k \oplus m\langle 2\rangle) \end{array}}{\begin{array}{l} \vdash k_1 := \$Uniform(\{0,1\}^n) \sim k_2 := \$Uniform(\{0,1\}^n) : \\ \quad True\ \Rightarrow\ m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle \end{array}}$$

Using the assignment rule, we can conclude.

Consequences of Coupling

Given the following pRHL judgment

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

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 $\Pr_{x\sim\{c_1\}_m}[x \in R] \leq \Pr_{x\sim\{c_2\}_{m'}}[x \in S]$

Soundness

If we can derive $\vdash \texttt{c}_1 \sim \texttt{c}_2 : P \Rightarrow Q$ through the rules of the logic, then the quadruple $\texttt{c}_1 \sim \texttt{c}_2 : P \Rightarrow Q$ is valid.

Completeness?