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

```
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 Noninterference

In symbols, c is probabilistically noninterferent if and only if for every $m_1 \sim_{low} m_2$:

$\{c\}_{m1} = \mu_1$ and $\{c\}_{m2} = \mu_2$ implies $\mu_1 \sim_{low} \mu_2$

Revisiting the example

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

Revisiting the example

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

m_1 m_2

Revisiting the example

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

m_1 m_2

$m_1 \oplus k$

Revisiting the example

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

m_1 m_2

$m_1 \oplus k$

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

Revisiting the example

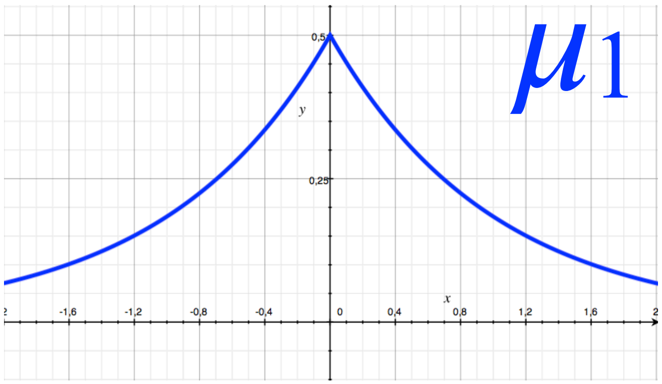
```
OneTimePad(m : private msg) : public msg
   key :=$ Uniform({0,1}ⁿ);
   cipher := m xor key;
   return cipher
```

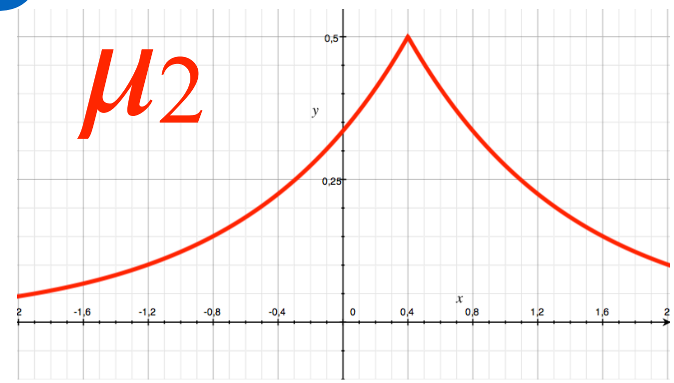
$m_1 \longrightarrow m_1 \oplus k$

$m_2 \longrightarrow m_2 \oplus (m_1 \oplus k \oplus m_2)$

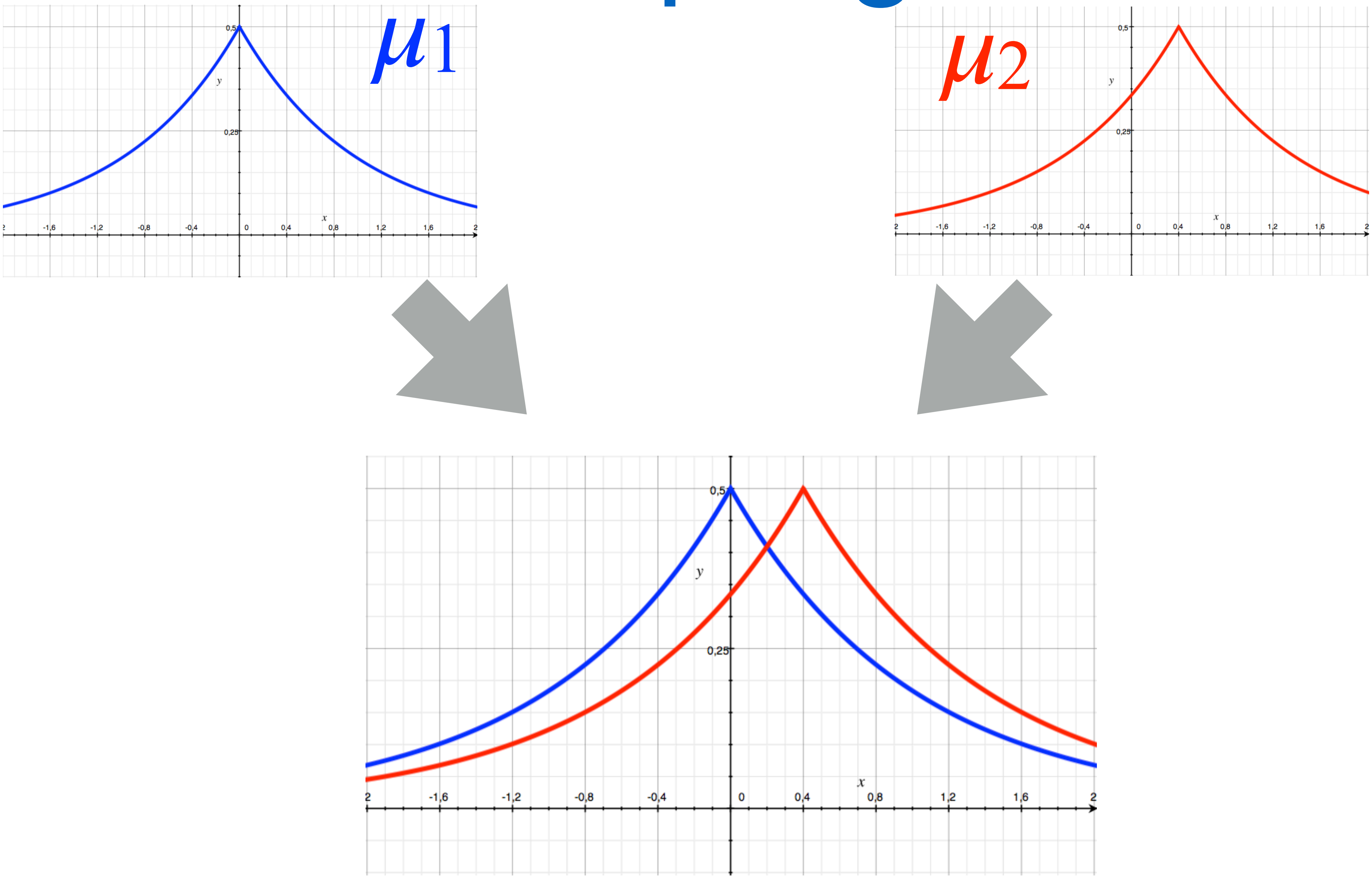
Suppose we can now chose the key for m_2. What could we choose?

Coupling


μ_1
0,5
0,25
y
x
-1,6
-1,2
-0,8
-0,4
0
0,4
0,8
1,2
1,6
2


μ_2
0,5
0,25
y
x
-1,6
-1,2
-0,8
-0,4
0
0,4
0,8
1,2
1,6
2

Coupling



Example of Our Coupling

00	0.25
01	0.25
10	0.25
11	0.25

$$k_1 = m_1 \oplus k_2 \oplus m_2$$

$$k_1 = 10 \oplus k_2 \oplus 00$$

00	0.25
01	0.25
10	0.25
11	0.25

Example of Our Coupling

00	0.25
01	0.25
10	0.25
11	0.25

$$k_1 = m_1 \oplus k_2 \oplus m_2$$

$$k_1 = 10 \oplus k_2 \oplus 00$$

00	0.25
01	0.25
10	0.25
11	0.25

	00	01	10	11
00			0.25	
01				0.25
10	0.25			
11		0.25		

Coupling formally

Given two distributions $\mu_1 \in D(A)$, and $\mu_2 \in D(B)$, a coupling between them is a joint distribution $\mu \in D(A \times B)$ whose marginal distributions are μ_1 and μ_2, respectively.

$$\pi_1(\mu)(a) = \sum_b \mu(a, b) \qquad \pi_2(\mu)(b) = \sum_a \mu(a, b)$$

Probabilistic Relational Hoare Quadruples

Precondition

Program$_1$ ~ Program$_2$

Postcondition

Precondition

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

Probabilistic Program

Probabilistic Program

Postcondition

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 $Q(\mu_1, \mu_2)$.

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 $Q(\mu_1, \mu_2)$.

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 ????

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)`$\in$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 $\mathtt{R} \subseteq A x B$, denoted $\mu_1 \; \mathtt{R*} \; \mu_2$ if and only if there exist an $\mathtt{R}$-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

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

Probabilistic Relational Hoare Logic

Assignment

$$\frac{}{\vdash x_1 := e_1 \sim x_2 := e_2 : P[e_1\langle 1\rangle / x_1\langle 1\rangle, e_2\langle 2\rangle / x_2\langle 2\rangle] \Rightarrow P}$$

Probabilistic Relational Hoare Logic

Composition

$$\frac{\vdash c_1 \sim c_2 : P \Rightarrow R \qquad \vdash c_1' \sim c_2' : R \Rightarrow S}{\vdash c_1; c_1' \sim c_2; c_2' : P \Rightarrow S}$$

Probabilistic Relational Hoare Logic

Consequence

$$\frac{P \Rightarrow S \qquad \vdash c_1 \sim c_2 : S \Rightarrow R \qquad R \Rightarrow Q}{\vdash c_1 \sim c_2 : P \Rightarrow Q}$$

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.

Probabilistic Relational Hoare Logic

If-then-else

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

$$\vdash c_1 \sim c_2 : e_1\langle 1\rangle \wedge P \Rightarrow Q$$

$$\vdash c_1' \sim c_2' : \neg e_1\langle 1\rangle \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{c}\texttt{if } e_1 \texttt{ then } c_1 \texttt{ else } c_1' \\ \sim \\ \texttt{if } e_2 \texttt{ then } c_2 \texttt{ else } c_2'\end{array} : P \Rightarrow Q$$

Probabilistic Relational Hoare Logic

While

$$\frac{\begin{array}{c} P \Rightarrow (e_1\langle 1\rangle \Leftrightarrow e_2\langle 2\rangle) \\ \vdash c_1 \sim c_2 : e_1\langle 1\rangle \wedge P \Rightarrow P \end{array}}{\vdash \begin{array}{c} \texttt{while } e_1 \texttt{ do } c_1 \\ \sim \\ \texttt{while } e_2 \texttt{ do } c_2 \end{array} : P \Rightarrow P \wedge \neg e_1\langle 1\rangle}$$

Probabilistic Relational Hoare Logic

If-then-else - left

$$\vdash c_1 \sim c_2 : e\langle 1\rangle \land P \Rightarrow Q$$

$$\vdash c_1' \sim c_2 : \neg e\langle 1\rangle \land P \Rightarrow Q$$

$$\vdash \begin{array}{c} \texttt{if } e \texttt{ then } c_1 \texttt{ else } c_1' \\ \sim \\ c_2 \end{array} : P \Rightarrow Q$$

Probabilistic Relational Hoare Logic

If-then-else - right

$$\vdash c_1 \sim c_2 : e\langle 2\rangle \wedge P \Rightarrow Q$$

$$\vdash c_1 \sim c_2' : \neg e\langle 2\rangle \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{c} c_1 \\ \sim \\ \texttt{if } e \texttt{ then } c_2 \texttt{ else } c_2' \end{array} : P \Rightarrow Q$$

Probabilistic Relational Hoare Logic

Assignment - left

$$\frac{}{\vdash \texttt{x:=e} \sim \texttt{skip}: \texttt{P[e<1>/x<1>]} \Rightarrow \texttt{P}}$$

How about the random assignment?

Probabilistic Relational Hoare Logic
Random Assignment

$$\vdash \mathtt{x_1 := \$ \ d_1 \sim x_2 := \$ \ d_2 : \ ??}$$

We would like to have:

$$\frac{\texttt{P}(\texttt{m}_1,\texttt{m}_2) \Rightarrow \texttt{let a=\{d}_1\texttt{\}}_{\texttt{m1}}\texttt{ in unit(m}_1\texttt{[x}_1\leftarrow\texttt{a])}\ \texttt{Q*}\ \texttt{let a=\{d}_2\texttt{\}}_{\texttt{m2}}\texttt{ in unit(m}_2\texttt{[x}_2\leftarrow\texttt{a])}}{\vdash \texttt{x}_1 \texttt{ :=\$ d}_1 \sim \texttt{x}_2 \texttt{ :=\$ d}_2 \texttt{ : P} \Rightarrow \texttt{Q}}$$

What is the problem with this rule?

Restricted Probabilistic Expressions

We consider a restricted set of expressions denoting probability distributions.

$$\texttt{d::= f(}d_1, \ldots, d_k\texttt{)}$$

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.

$$\texttt{d::= f(d}_1\texttt{,…,d}_k\texttt{)}$$

Where `f` is a distribution declaration

Some expression examples similar to the previous

`uniform({0,1}`^{128}`)`   `bernoulli(.5)`   `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 $R \subseteq AxB$, if there is a mapping $h: A \rightarrow B$ such that:

1) h is a bijective map between elements in supp(μ_1) and supp(μ_2),
2) for every $a \in supp(\mu_1)$, $(a,h(a)) \in R$
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.
We write $h \triangleleft (\mu_1,\mu_2)$ in this case.

Probabilistic Relational Hoare Logic
Random Assignment

$$\frac{\begin{array}{l} h \lhd (\{d_1\},\{d_2\}) \\ P = \forall v, v \in supp(\{d_1\}) \\ \Rightarrow Q[v/x_1\langle 1\rangle, h(v)/x_2\langle 2\rangle] \end{array}}{\vdash x_1 :=\$\ d_1 \sim x_2 :=\$\ d_2 : P \Rightarrow Q}$$

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
```

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

$$m_1 \downarrow$$

$m_1 \oplus k$

Back to our example

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

$m_1 \longrightarrow m_1 \oplus k$

$m_2 \longrightarrow m_2 \oplus (m_1 \oplus k \oplus m_2)$

Back to our example

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

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

Is this a good map?

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

Back to our example

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

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

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
```

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

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?

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

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) $Pr_{x\sim\{d1\}}[x=v] = Pr_{x\sim\{d2\}}[x=v]$

It is a good map!

Back to our example

$h(k) = (m\langle 1\rangle \oplus k \oplus m\langle 2\rangle) \lhd (\{d_1\}, \{d_2\})$

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

$\Rightarrow\ m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle [v/k_1\langle 1\rangle, h(v)/k_2\langle 2\rangle] =$

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

$$\frac{}{\vdash k_1 := \$Uniform(\{0,1\}^n) \sim k_2 := \$Uniform(\{0,1\}^n) : \text{True} \Rightarrow m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle}$$

Back to our example

$$h(k)=(m\langle 1\rangle \oplus k \oplus m\langle 2\rangle) \lhd (\{d_1\},\{d_2\})$$

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

$$\Rightarrow\ m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle [v/k_1\langle 1\rangle, h(v)/k_2\langle 2\rangle] =$$

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

$$\vdash k_1 := \$Uniform(\{0,1\}^n) \sim k_2 := \$Uniform(\{0,1\}^n) :$$

$$True\ \Rightarrow\ m\langle 1\rangle \oplus k_1\langle 1\rangle = m\langle 2\rangle \oplus k_2\langle 2\rangle$$

Using the assignment rule, we can conclude.

Soundness

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

Completeness?