Dynamic Leakage

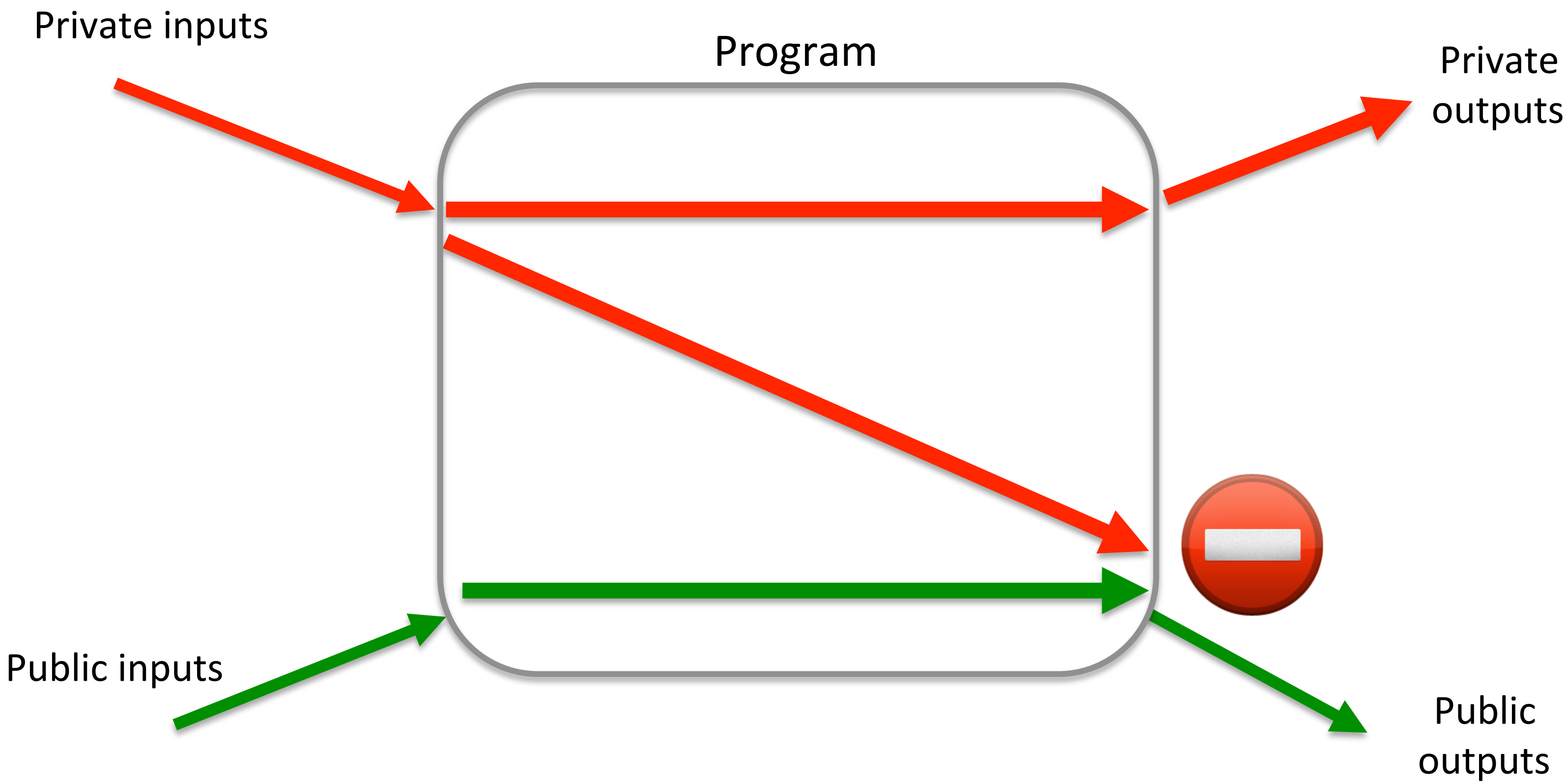
A Need for a New Quantitative Information Flow Measure

Nataliia Bielova

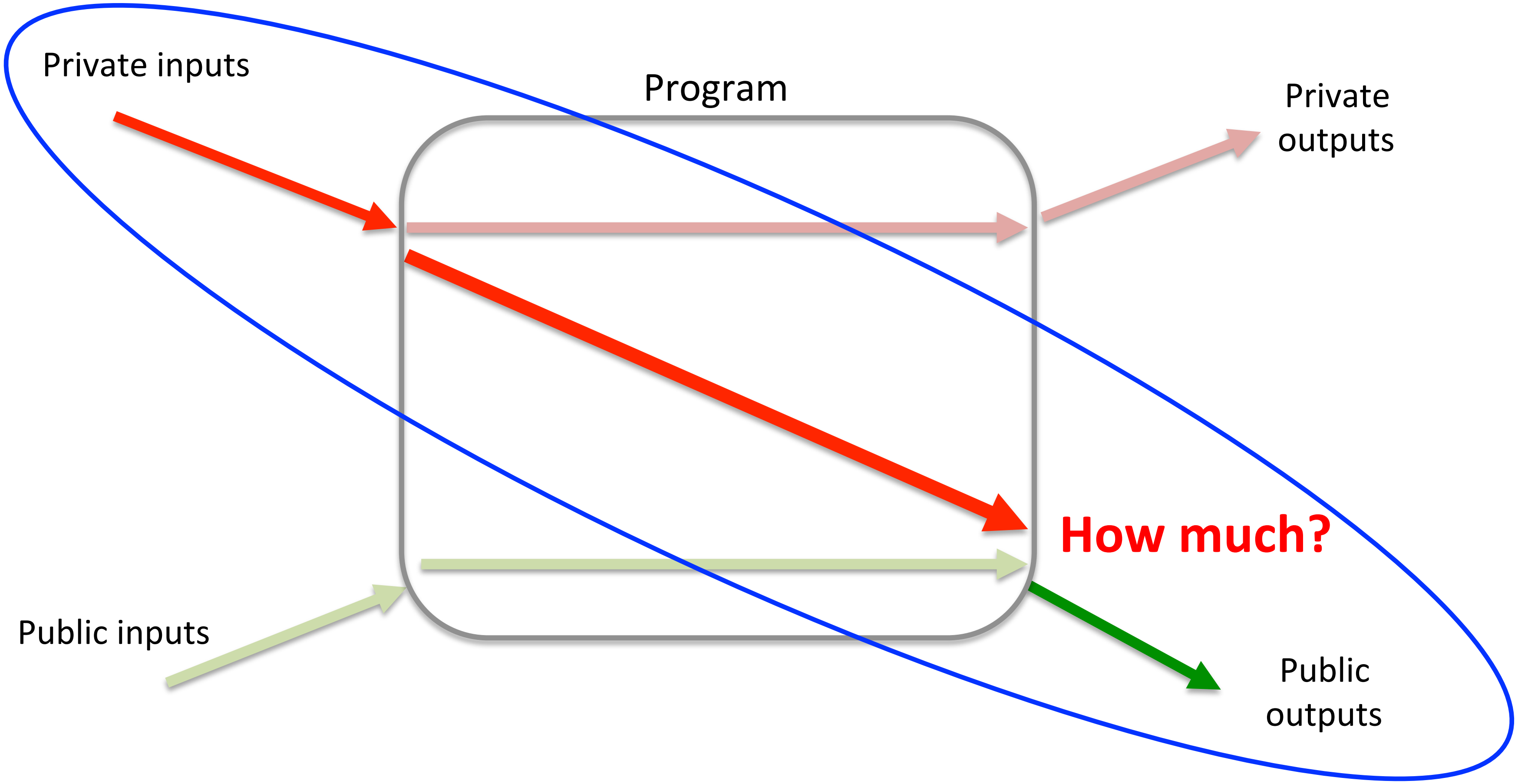
24 October 2016

PLAS'16

Noninterference

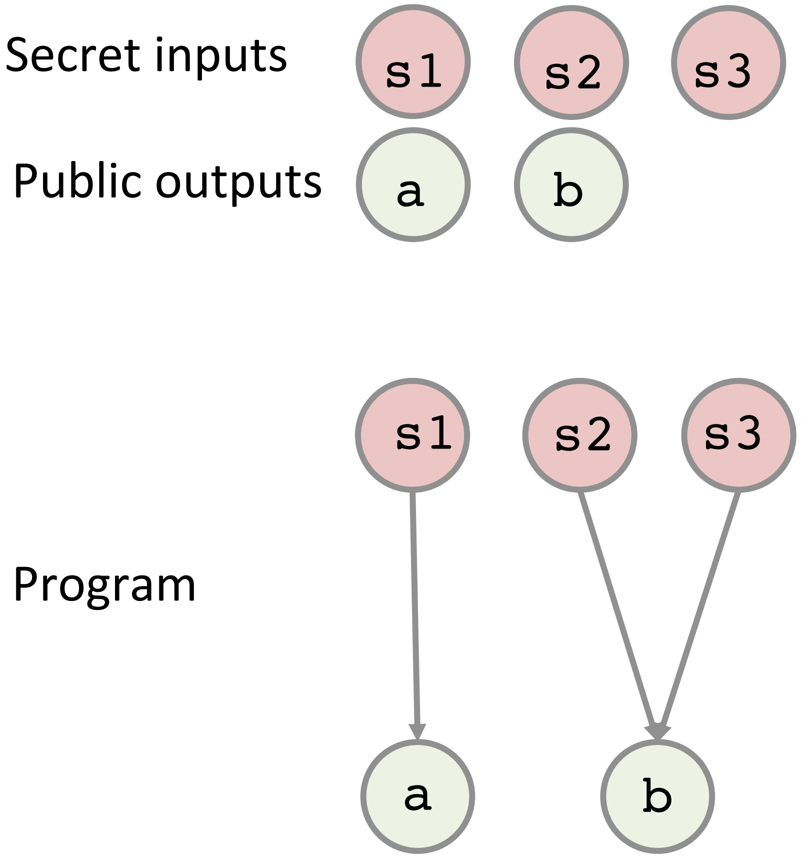


Quantitative Information Flow



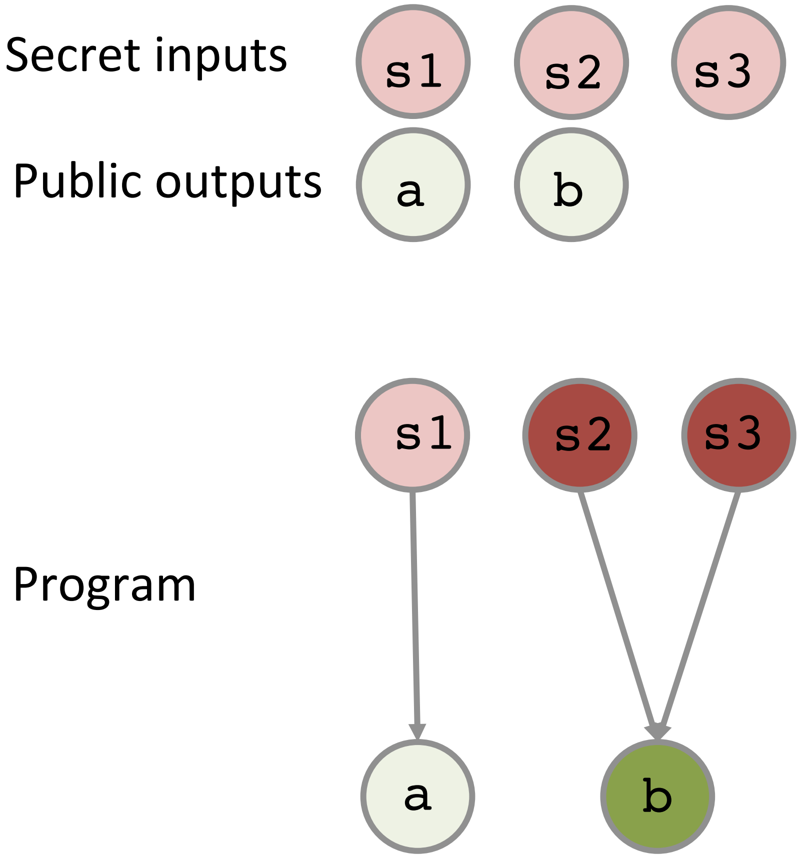
How much does the attacker learn when she observes **a concrete public output**?

```
if S = s1 then O = a else O = b
```



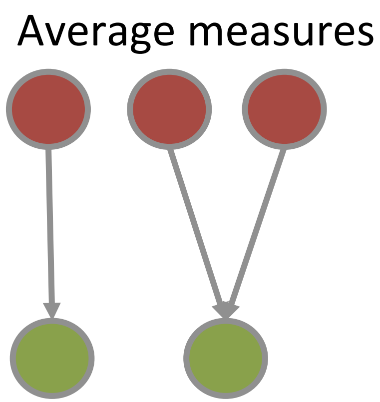
How much does the attacker learn when she observes **output b**?

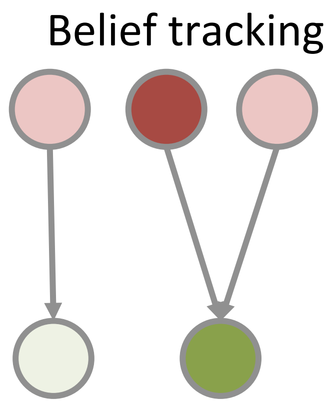
```
if S = s1 then O = a else O = b
```



How much does the attacker learn when she observes **output b**?

Existing measures of info leakage



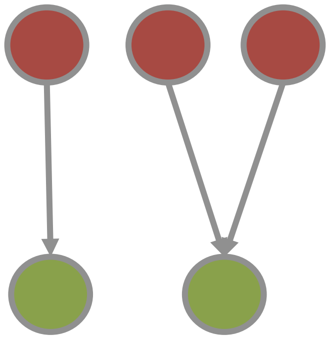


- Shannon Entropy
- Min Entropy
- Guessing Entropy
- g-leakage
- Channel capacity

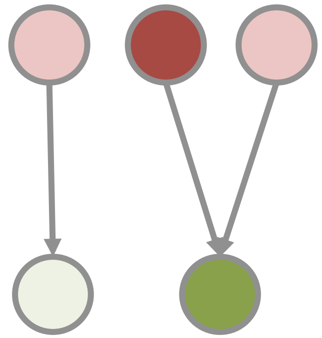
- Belief Tracking

A need for a new measure

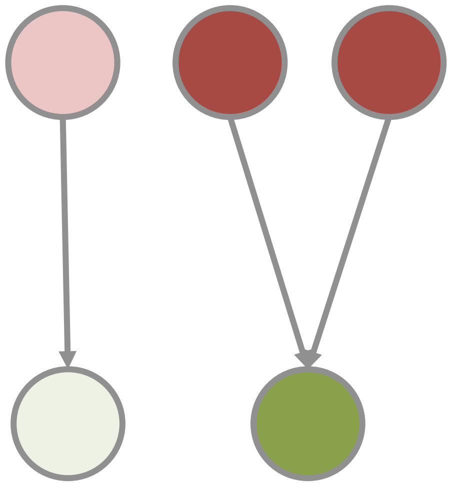
Average measures



Belief tracking



Dynamic Leakage?



```
if S = s1 then O = a else O = b
```

a priori

	π
s1	0.875
s2	0.0625
s3	0.0625

a posteriori after a

	$p_{S\|a}$
s1	1
s2	0
s3	0

a posteriori after b

	$p_{S\|b}$
s1	0
s2	0.5
s3	0.5

Average measure: Shannon Entropy

	π
s1	0.875
s2	0.0625
s3	0.0625

Uncertainty about the secret

$$\mathcal{H}(\pi) = -\sum_{s \in \mathcal{S}} \pi(s) \cdot \log \pi(s)$$

Leakage:

$$\mathcal{L} = \mathcal{H}(\pi) - \mathcal{H}(p_{S|O})$$

average for all possible outputs

$$\mathcal{H}(p_{S|O}) = -\sum_{o \in \mathcal{O}} p(o) \cdot \log \mathcal{H}(p_{S|o})$$

entropy for one output

Average measure: Shannon Entropy

	π
s1	0.875
s2	0.0625
s3	0.0625

	$p_{S\|a}$
s1	1
s2	0
s3	0

	$p_{S\|b}$
s1	0
s2	0.5
s3	0.5

$\mathcal{H}(\pi) = 0.67$

$\mathcal{H}(p_{S|a}) = 0$

$\mathcal{H}(p_{S|b}) = 1$

$\mathcal{H}(p_{S|O}) = 0.13$

$$\mathcal{L} = 0.67 - 0.13 = \mathbf{0.54}$$

average information leakage
for all possible outputs

Dynamic Leakage for Shannon Entropy

$$\mathcal{L}^{\text{dynamic}} = \mathcal{H}(\pi) - \mathcal{H}(p_{S|b})$$

a posteriori for concrete output b

Dynamic Leakage for Shannon Entropy

	π
s1	0.875
s2	0.0625
s3	0.0625

	$p_{S\|b}$
s1	0
s2	0.5
s3	0.5

$\mathcal{H}(\pi) = 0.67$

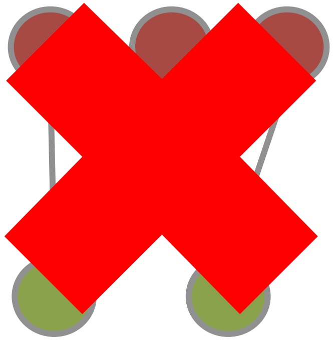
$\mathcal{H}(p_{S|b}) = 1$

$$\mathcal{L}^{\text{dynamic}} = 0.67 - 1 = \mathbf{-0.33}$$

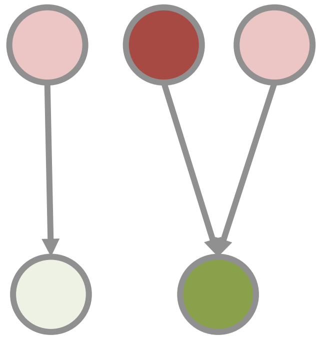
no leakage!

A need for a new measure

Average measures



Belief tracking



Belief tracking

	π
s1	0.875
s2	0.0625
s3	0.0625

	$p_{S\|b}$
s1	0
s2	0.5
s3	0.5

concrete secret

	p’
s1	0
s2	1
s3	0

$\mathcal{D}(p_{S|b} \rightarrow p')$

$\mathcal{D}(\pi \rightarrow p')$

$$\mathcal{L}^{belief} = \mathcal{D}(\pi \rightarrow p') - \mathcal{D}(p_{S|b} \rightarrow p')$$

concrete secret input

a posteriori for one output

Belief tracking

	π
s1	0.875
s2	0.0625
s3	0.0625

	$p_{S\|b}$
s1	0
s2	0.5
s3	0.5

concrete secret

	p’
s1	0
s2	1
s3	0

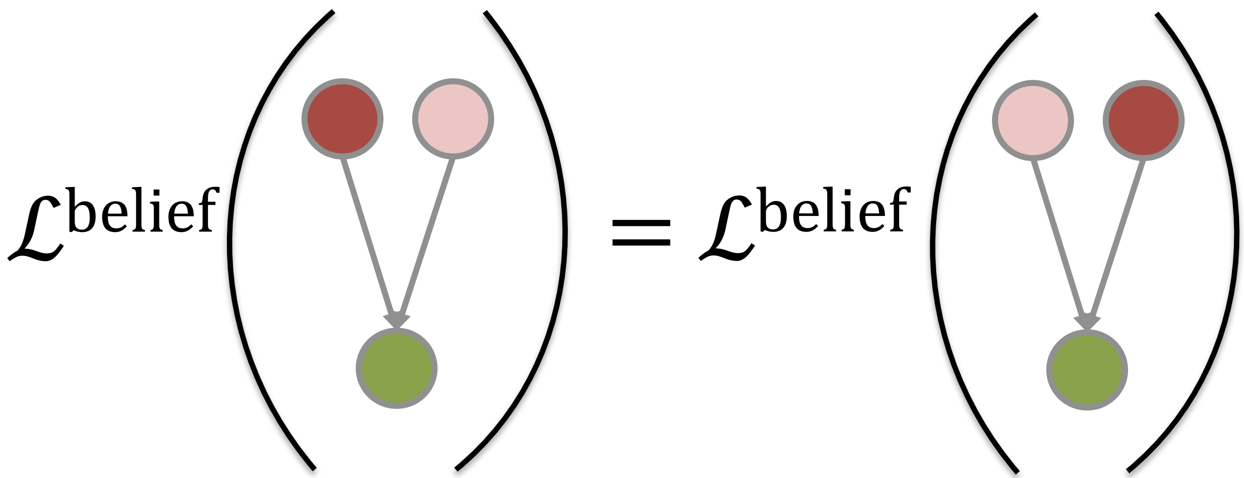
$$\mathcal{D}(p_{S|b} \rightarrow p') = 1$$

$$\mathcal{D}(\pi \rightarrow p') = 4$$

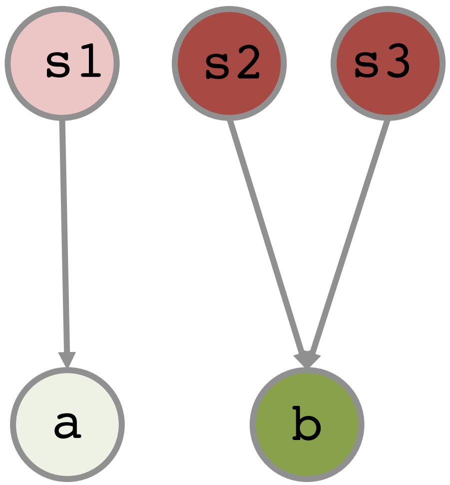
$$\mathcal{L}^{\text{belief}} = 4 - 1 = 3$$

Belief tracking is suitable for deterministic programs

Theorem 1. $\mathcal{L}^{\text{belief}} = -\log p(o)$



Belief tracking is suitable for deterministic programs

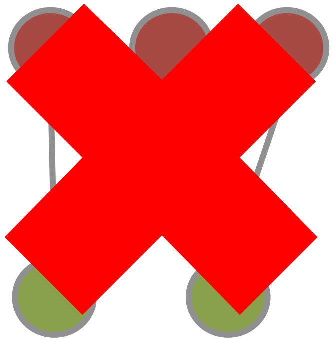


$$\mathcal{L}^{\text{belief}} = -\log p(b)$$
$$= -\log (\pi(s2) + \pi(s3))$$

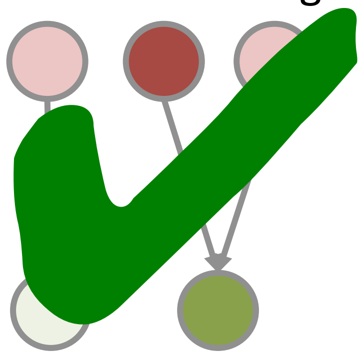
Initial probabilities of secrets that can produce output b

A need for a new measure

Average measures



Belief tracking



is suitable for deterministic programs

Belief tracking for probabilistic programs?

	π
s1	0.25
s2	0.75

	$p_{S\|b}$
s1	0.75
s2	0.25

concrete secret s1

	p’
s1	1
s2	0

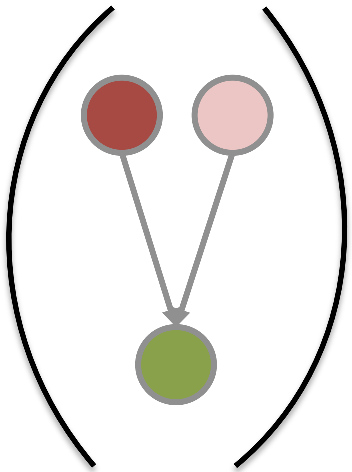
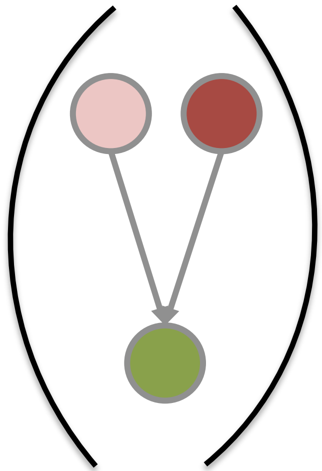
$\mathcal{L}^{\text{belief}} = 1.58$

concrete secret s2

	p’
s1	0
s2	1

$\mathcal{L}^{\text{belief}} = -1.58$

Belief tracking for probabilistic programs?

$\mathcal{L}^{\text{belief}}$  $\neq \mathcal{L}^{\text{belief}}$ 

Conclusions

✖ Average measures become negative

✔ Belief tracking is suitable for deterministic programs

? Which measure is suitable for probabilistic programs?

- Operational scenario?
- Reasonable evaluation criteria?