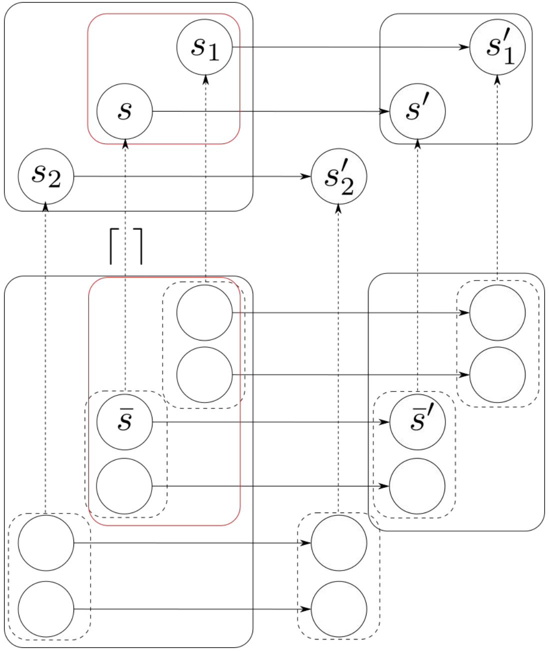
Confidentiality-Preserving Refinement

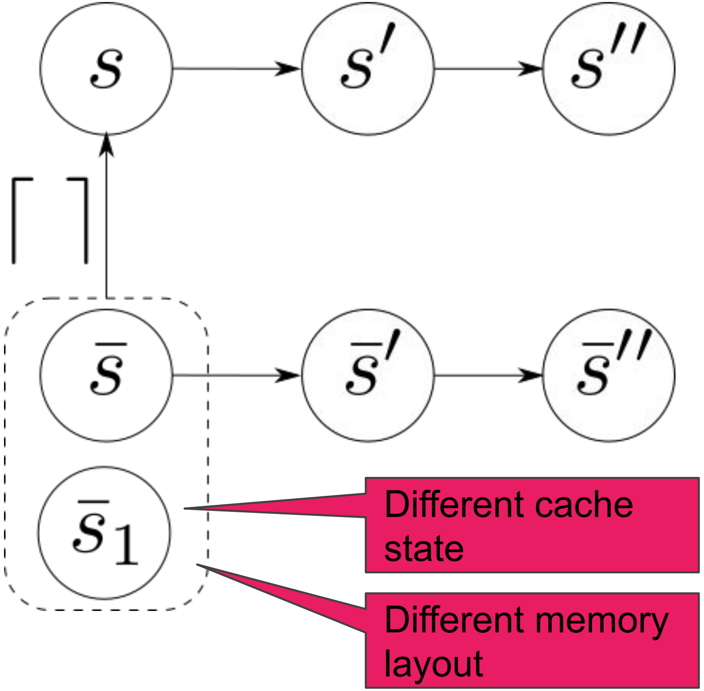
Roberto Guanciale
Christoph Baumann
Mads Dam
Hamed Nemati

Entropy 16/06/2019



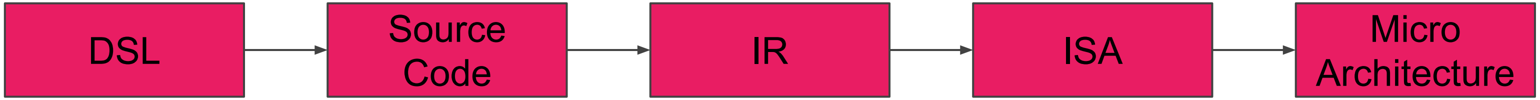
Refinement

- Change data representation
  - From C to assembly
  - From ideal function to SMC
- Add details
  - Caches
  - Timing
  - Addresses of variables
- Remove non-determinism
- Goal: prevent unintended leakage of secret data



Different cache state

Different memory layout



DSL → Source Code → IR → ISA → Micro Architecture

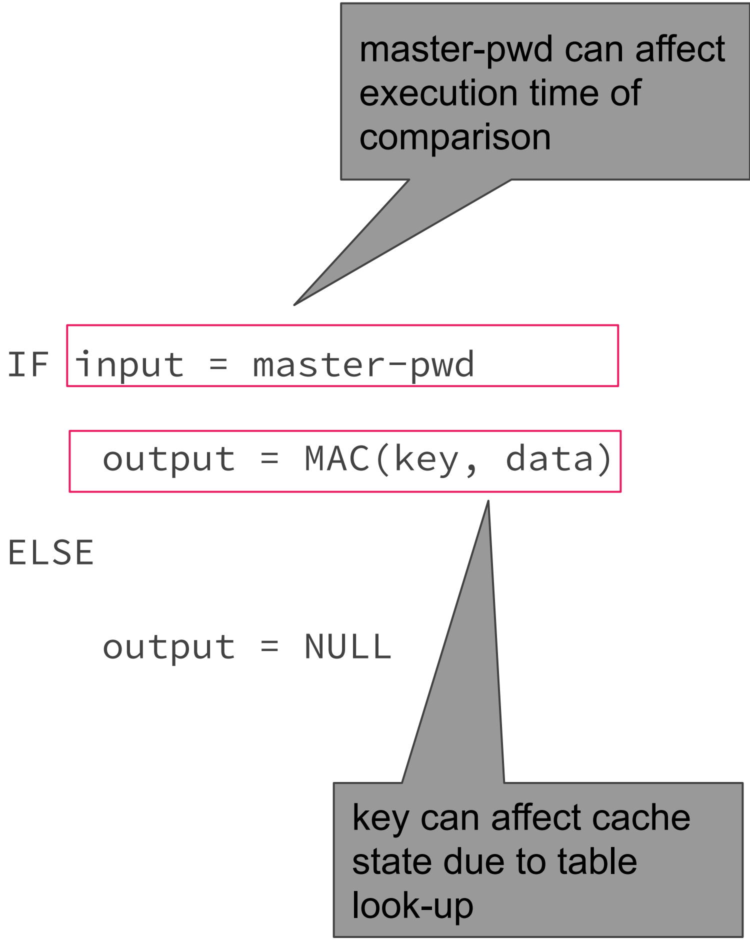
Challenges

- Simple accounts of refinement (e.g., trace inclusion) do not guarantee confidentiality properties
- Several ways to specify licit information flows
  - multi-level security, decentralised model
  - declassification
  - …
- Abstract model “specifies” the intentend information flows

```
IF input = master-pwd

    output = MAC(key, data)

ELSE

    output = NULL
```

Challenges

- Simple accounts of refinement (e.g., trace inclusion) do not guarantee confidentiality properties
- Several ways to specify licit information flows
  - multi-level security, decentralised model
  - declassification
  - …
- Abstract model “specifies” the intentend information flows



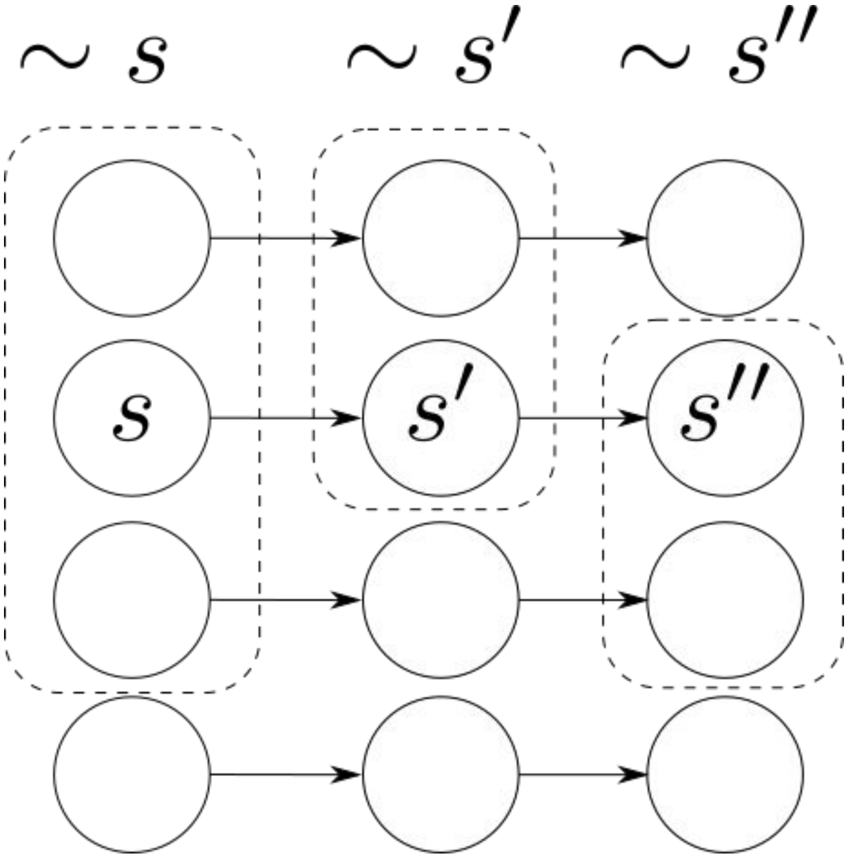
master-pwd can affect execution time of comparison

```
IF input = master-pwd

    output = MAC(key, data)

ELSE

    output = NULL
```

key can affect cache state due to table look-up

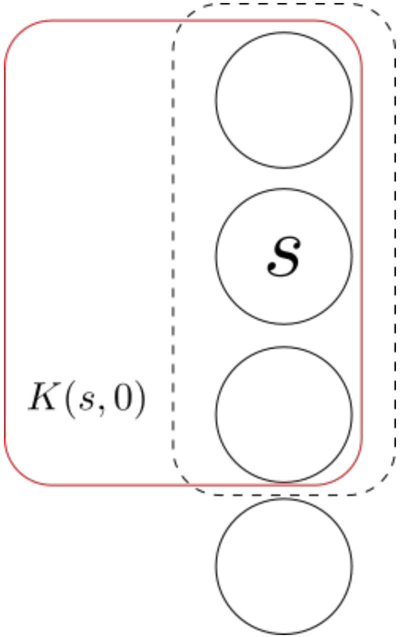
Observation equivalence

- Same attacker’s observations
  - I.e. input, data, output



Knowledge

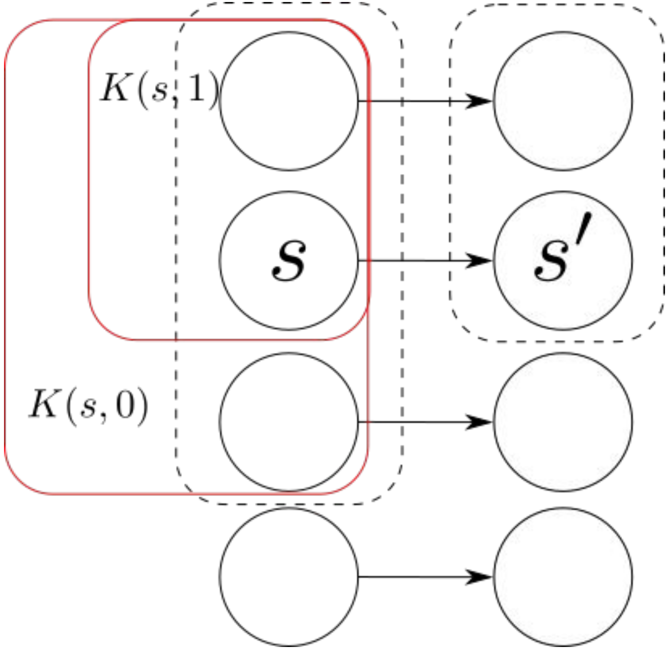
$$K(s,n) = \{s_1 \mid \forall n_1 \leq n . s \downarrow_{n_1} \sim s_1 \downarrow_{n_1}\}$$



Knowledge

$$K(s,n) = \{s_1 \mid \forall n_1 \leq n . s \downarrow_{n_1} \sim s_1 \downarrow_{n_1}\}$$

- `s.input=s.m-pwd iff s1.input=s1.m-pwd`

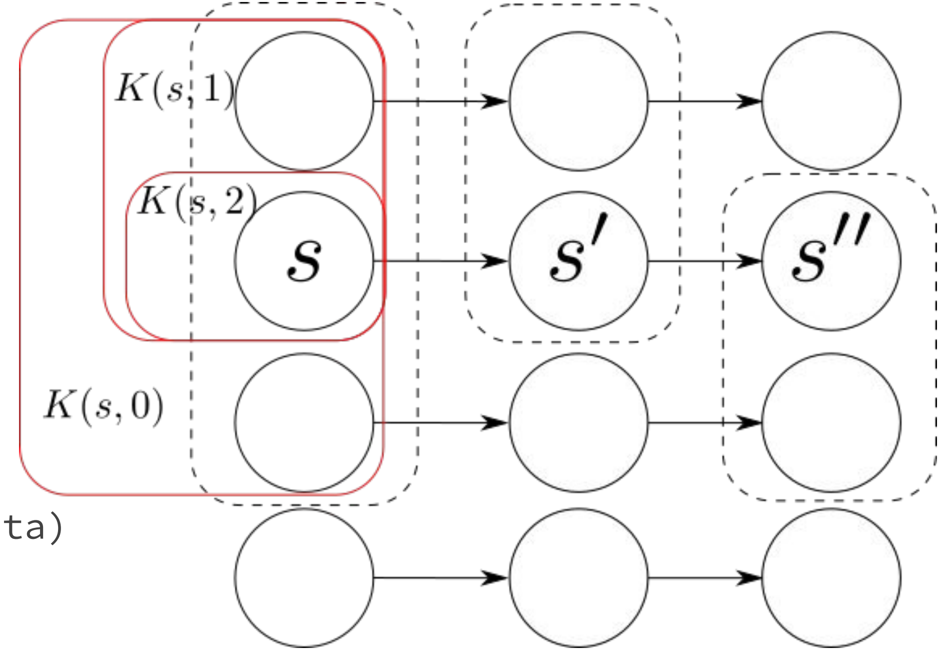


Knowledge $K(s,n) = \{s_1 \mid \forall n_1 \leq n. s \downarrow_{n_1} \sim s_1 \downarrow_{n_1}\}$

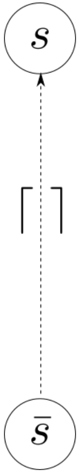
- s.input=s.m-pwd iff s1.input=s1.m-pwd

- if s.input=s.m-pwd then
  - S(s.key,s.data)=S(s1.key,s1.data)

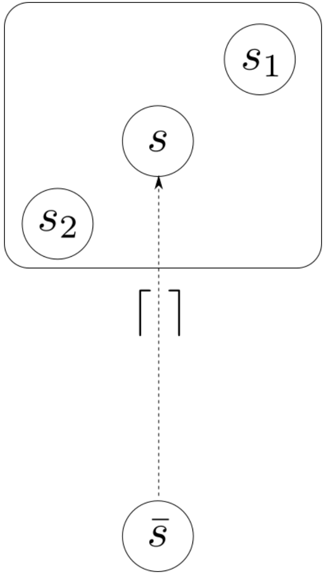
- Yardstick for information flows



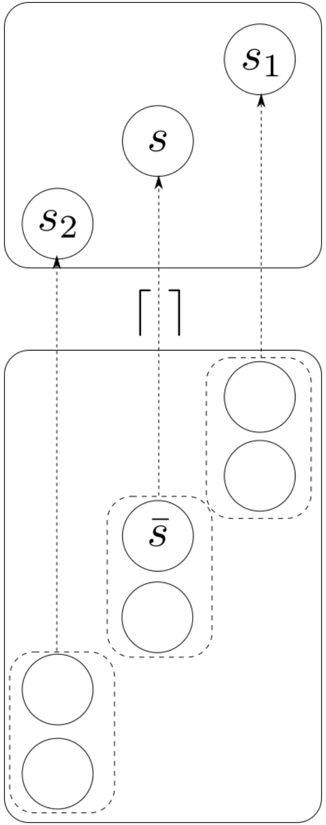
Confidentiality Preserving Refinement $\lceil K(\bar{s}, n) \rceil = K(\lceil \bar{s} \rceil, n)$



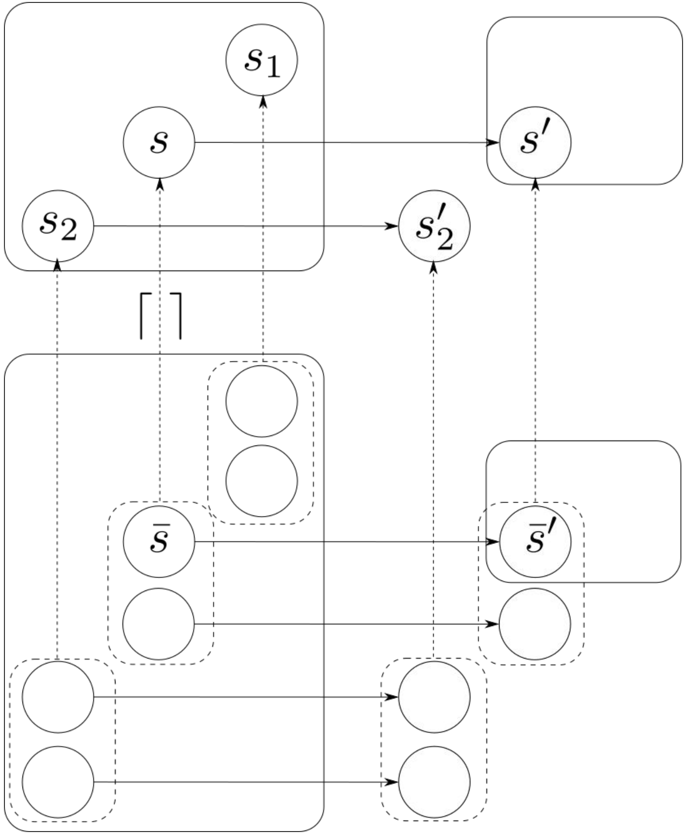
Confidentiality Preserving Refinement $\lceil K(\bar{s}, n) \rceil = K(\lceil \bar{s} \rceil, n)$



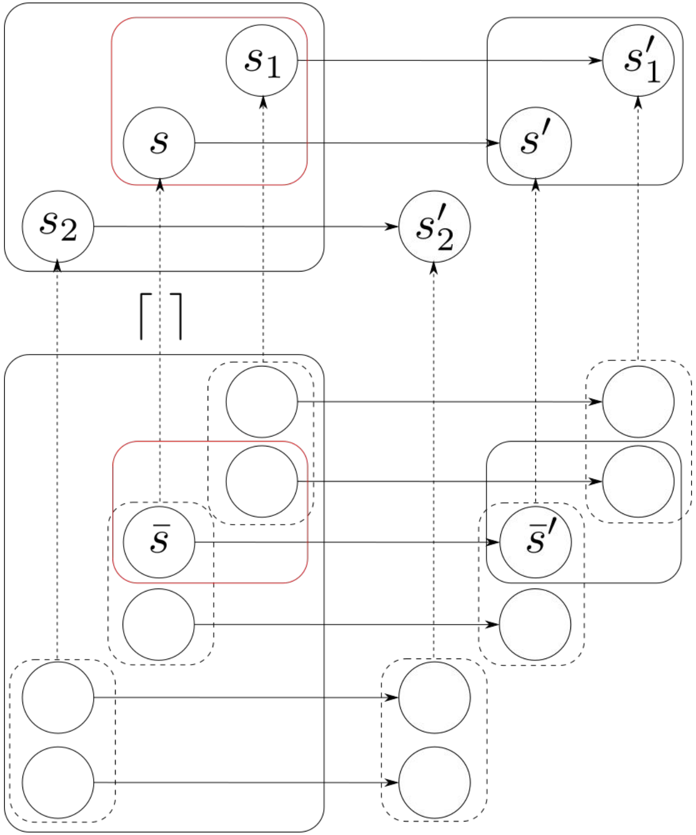
Confidentiality Preserving Refinement $\lceil K(\bar{s}, n) \rceil = K(\lceil \bar{s} \rceil, n)$



Confidentiality Preserving Refinement $\lceil K(\bar{s}, n) \rceil = K(\lceil \bar{s} \rceil, n)$

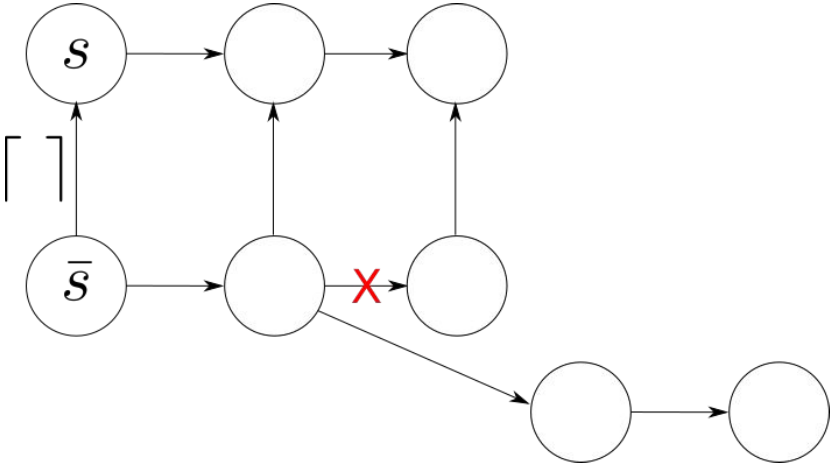


Confidentiality Preserving Refinement $\lceil K(\bar{s}, n) \rceil = K(\lceil \bar{s} \rceil, n)$

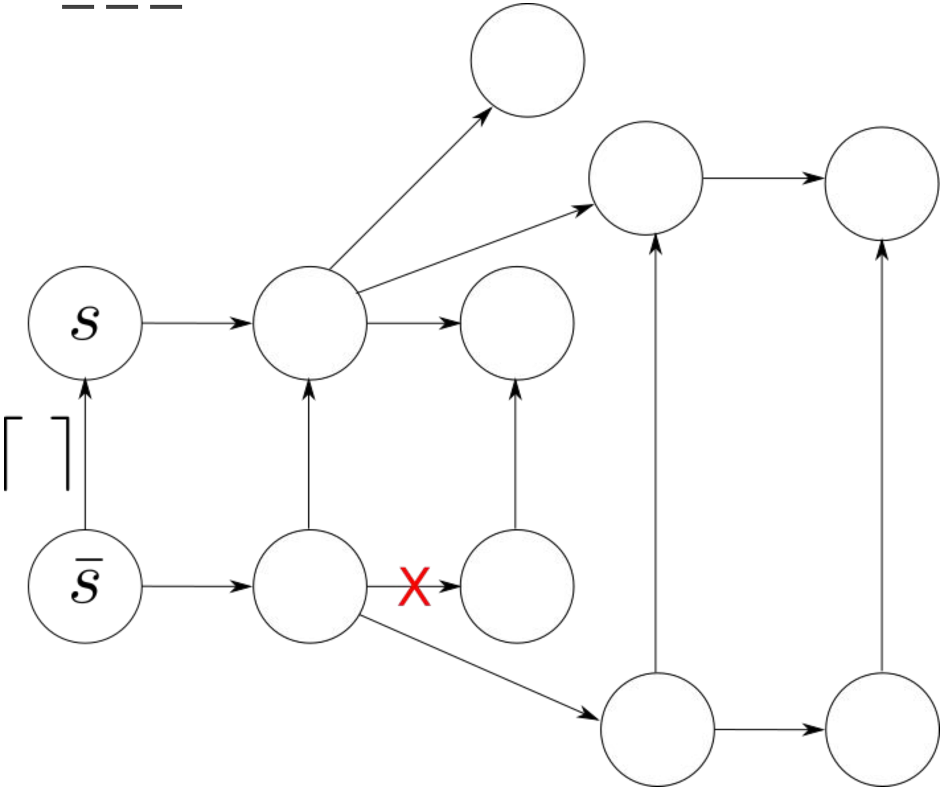


Behavioral morphing refinements

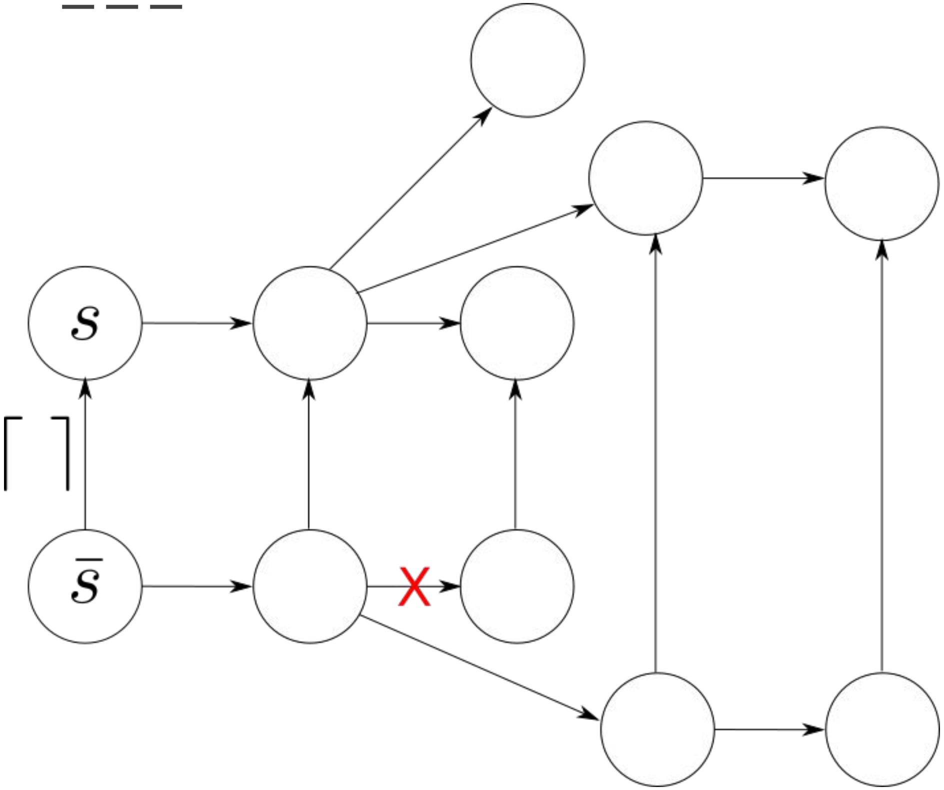
- Attacker behavior could diverge due to low-level features (row-hammer, mismatched cacheability, weak memory models)



Behavioral morphing refinements



Behavioral morphing refinements



```
IF ~~input = master-pwd~~ TRUE
    output = MAC(key, data)
ELSE
    output = NULL
```

Thank You