Concurrent infoflow security-preserving compilation

Short talk: DeepSpec Summer School ’18

Robert Sison | PhD supervisors: Toby Murray, Kai Engelhardt

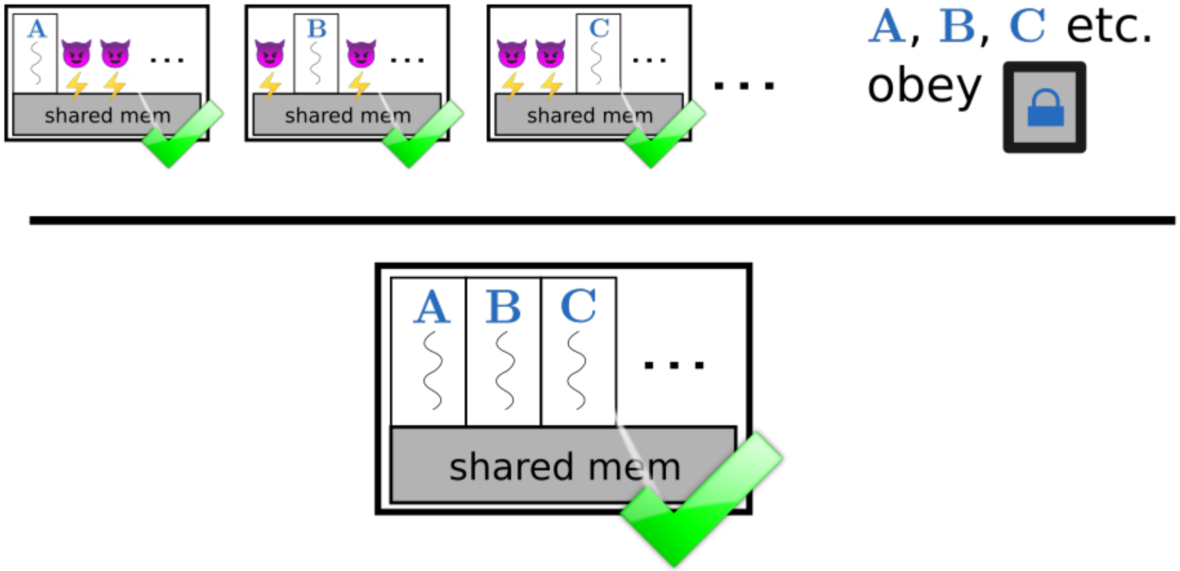
July 2018

THE UNIVERSITY OF
NEW SOUTH WALES

Motivation

Infoflow security

(Noninterference, for shared-variable concurrent programs)

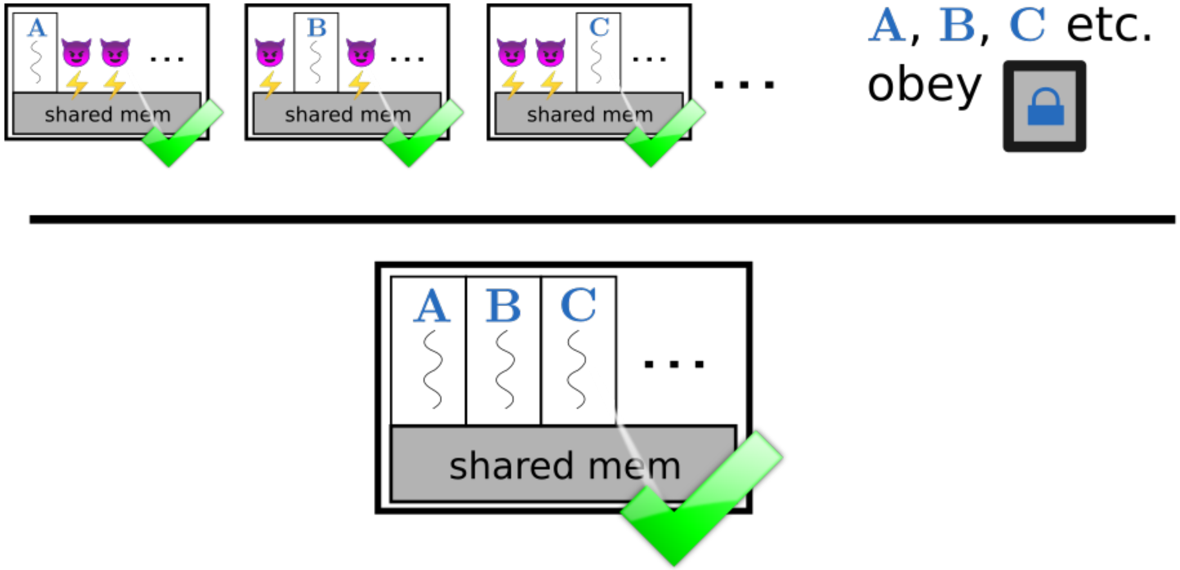


A, B, C etc. obey 🔒

Motivation

Infoflow security

(Noninterference, for shared-variable concurrent programs)

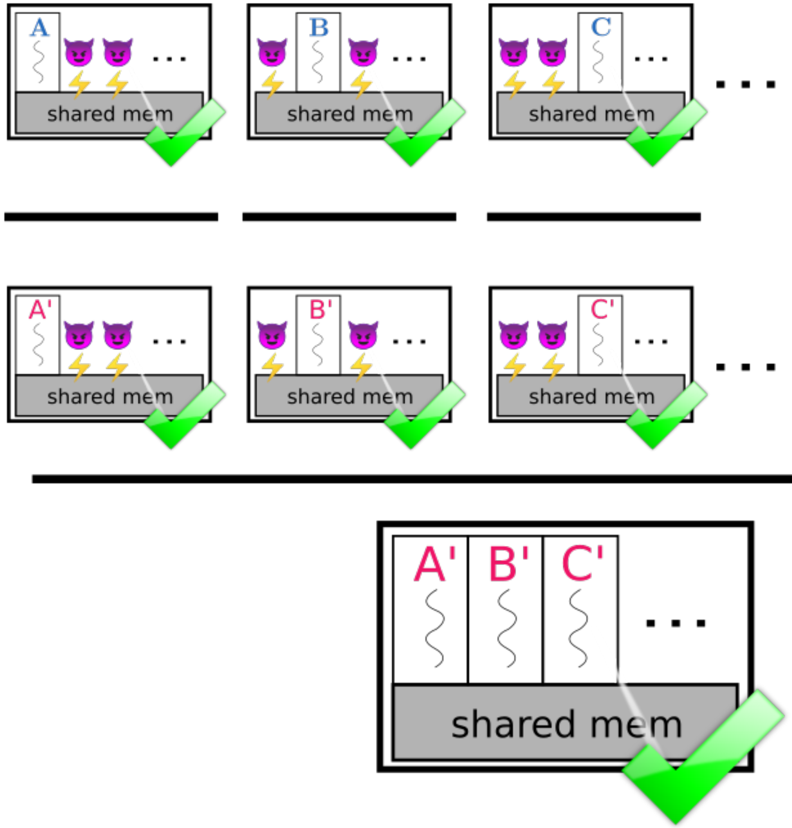


A, B, C etc. obey 🔒

Motivation

Infoflow security-preserving compilation

(Noninterference, for shared-variable concurrent programs)



A, B, C etc. obey 🔒

Source

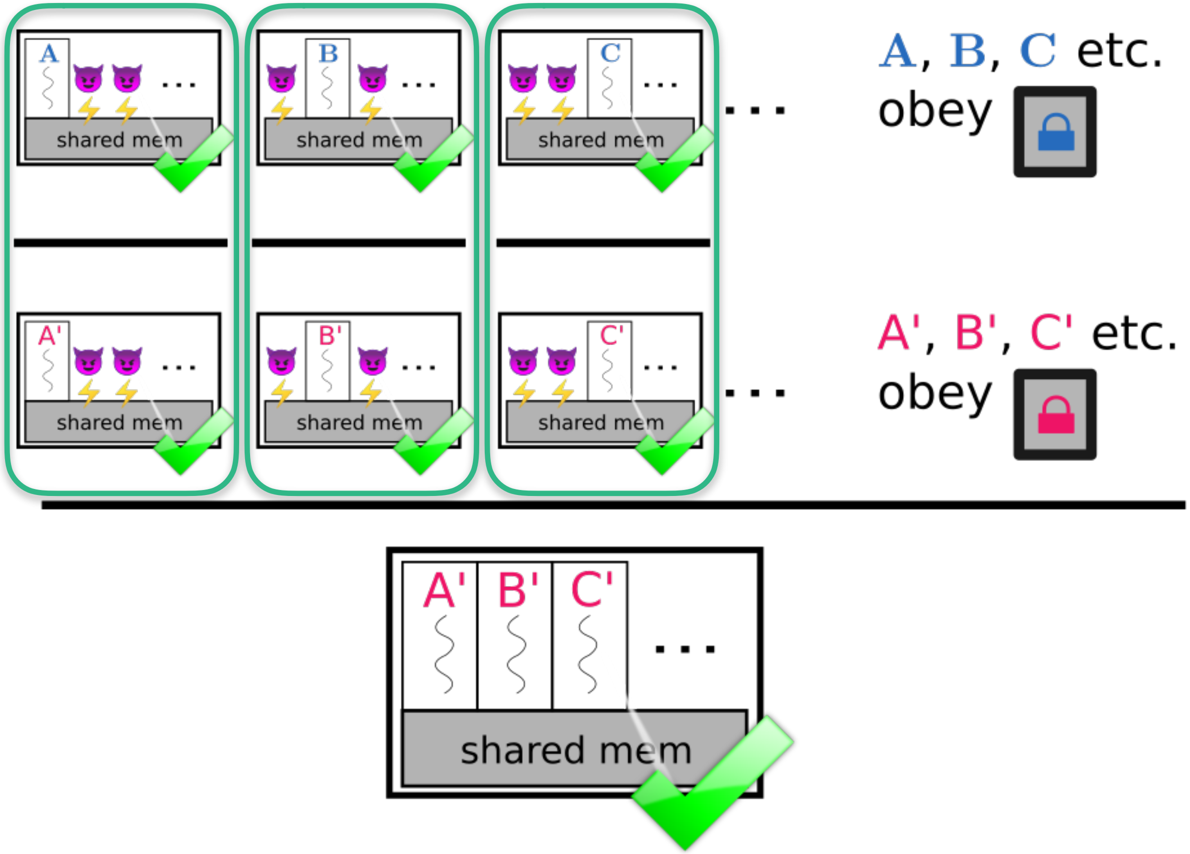
A', B', C' etc. obey 🔒

Target

Motivation

Infoflow security-preserving compilation

(Noninterference, for shared-variable concurrent programs)



A, B, C etc. obey 🔒

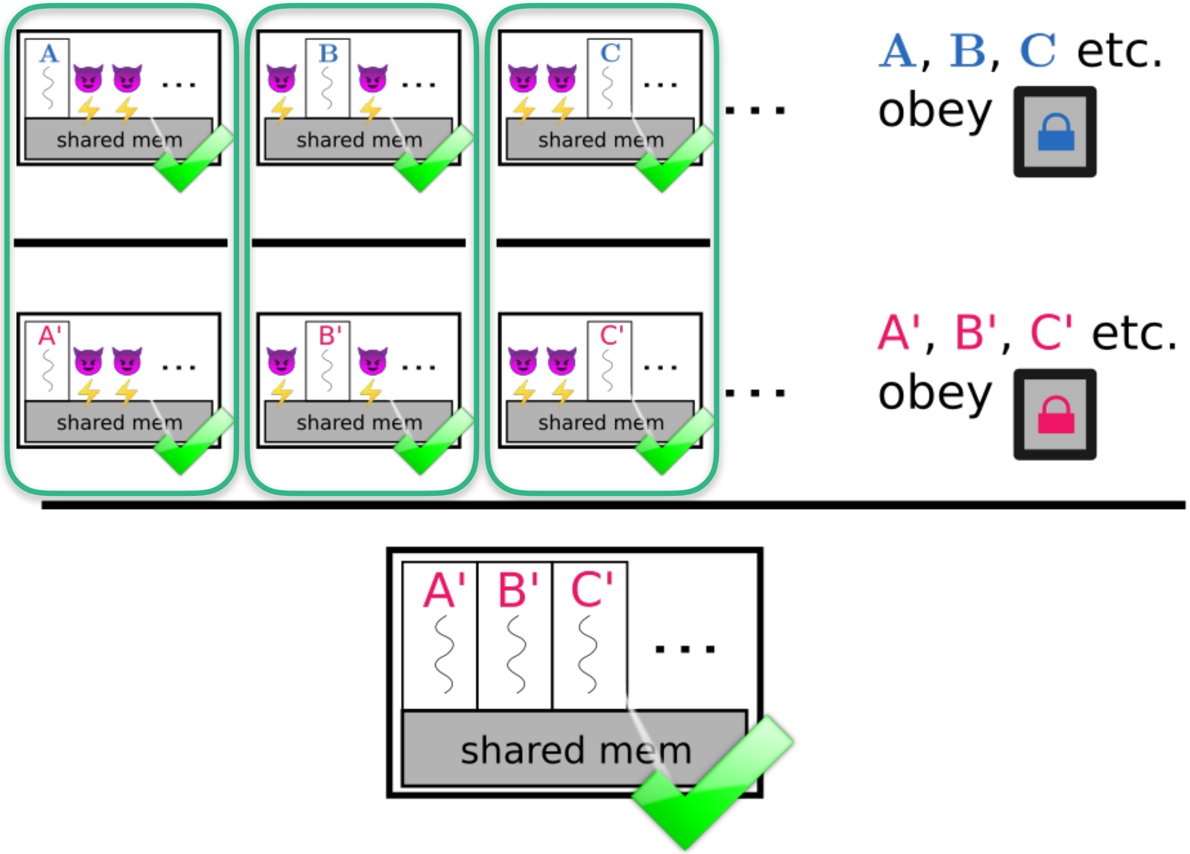
A', B', C' etc. obey 🔒

Source

Target

My PhD focus

Infoflow security-preserving compilation



A, B, C etc. obey 🔒

A', B', C' etc. obey 🔒

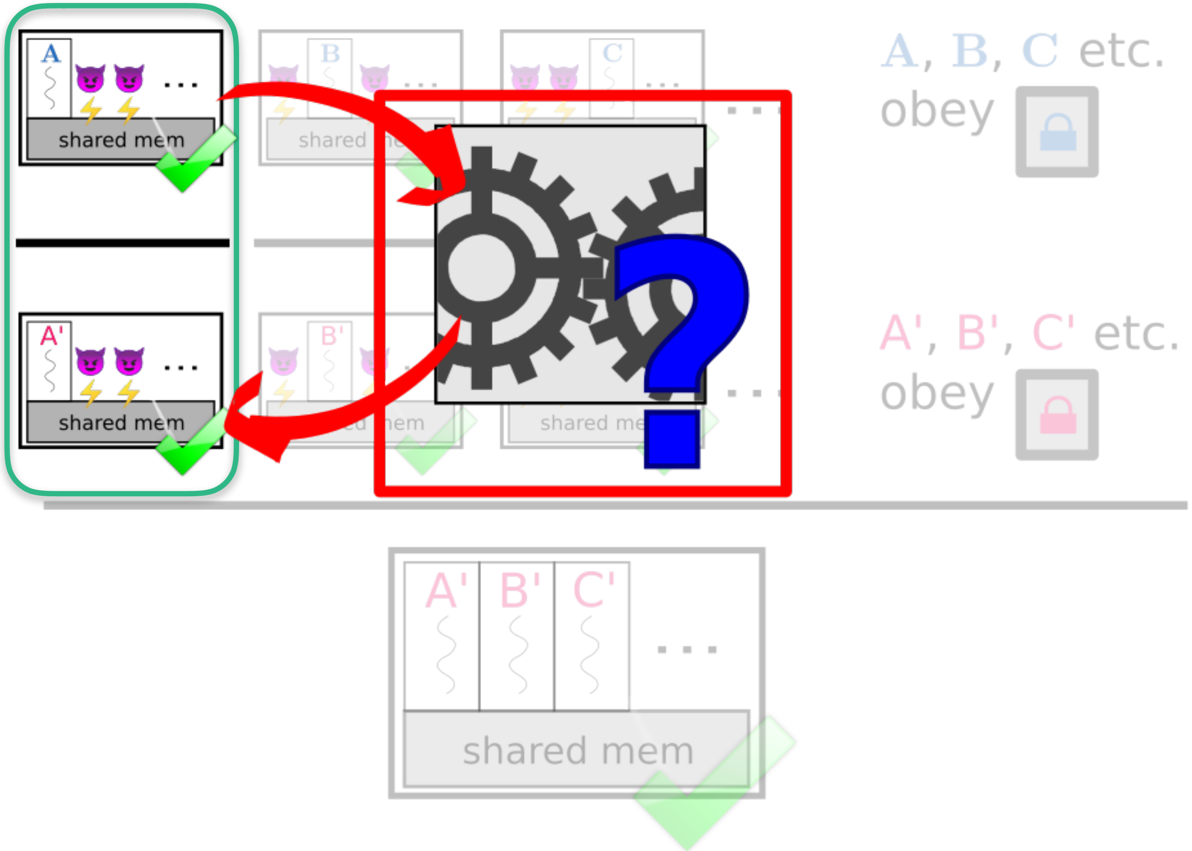
Source

Target

My PhD focus

Infoflow security-preserving compilation

What does it take to prove this?



A, B, C etc. obey 🔒

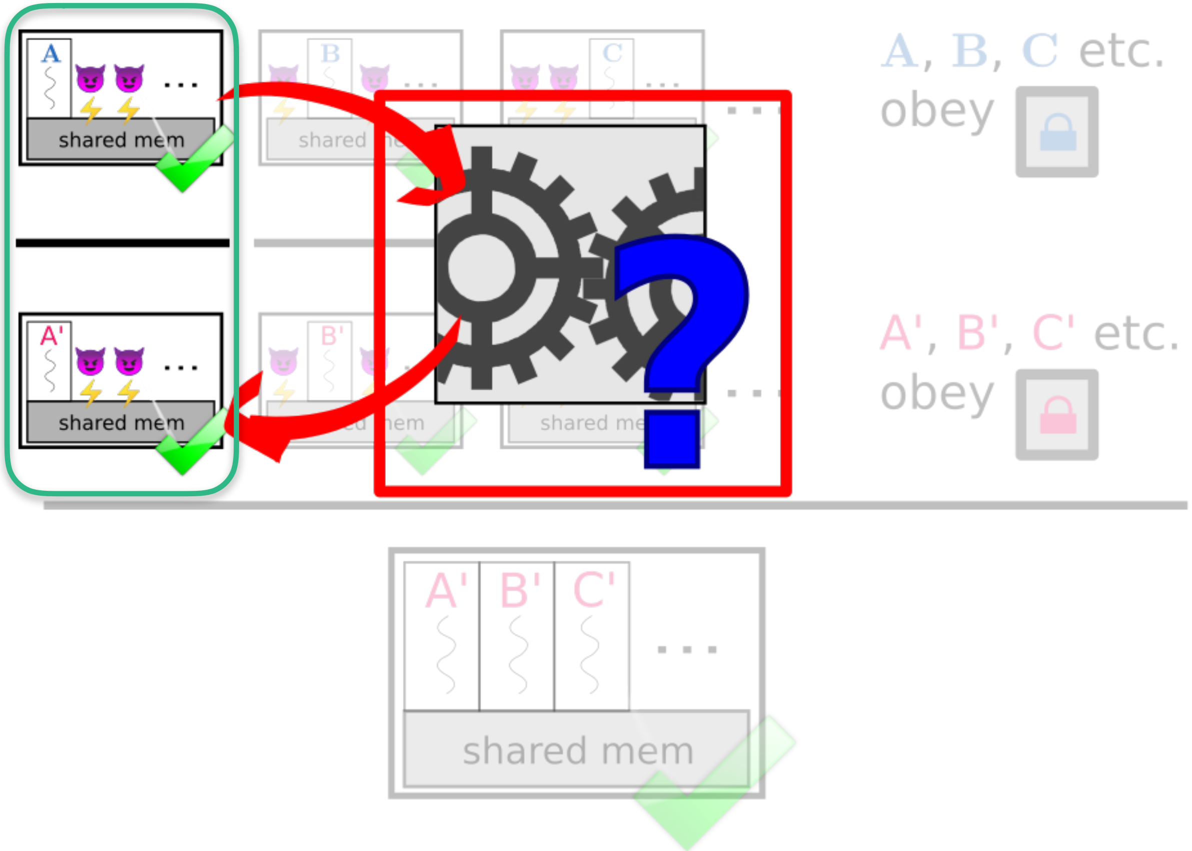
A', B', C' etc. obey 🔒

Source

Target

My PhD: so far

Infoflow security-preserving compilation



A, B, C etc. obey 🔒

A', B', C' etc. obey 🔒

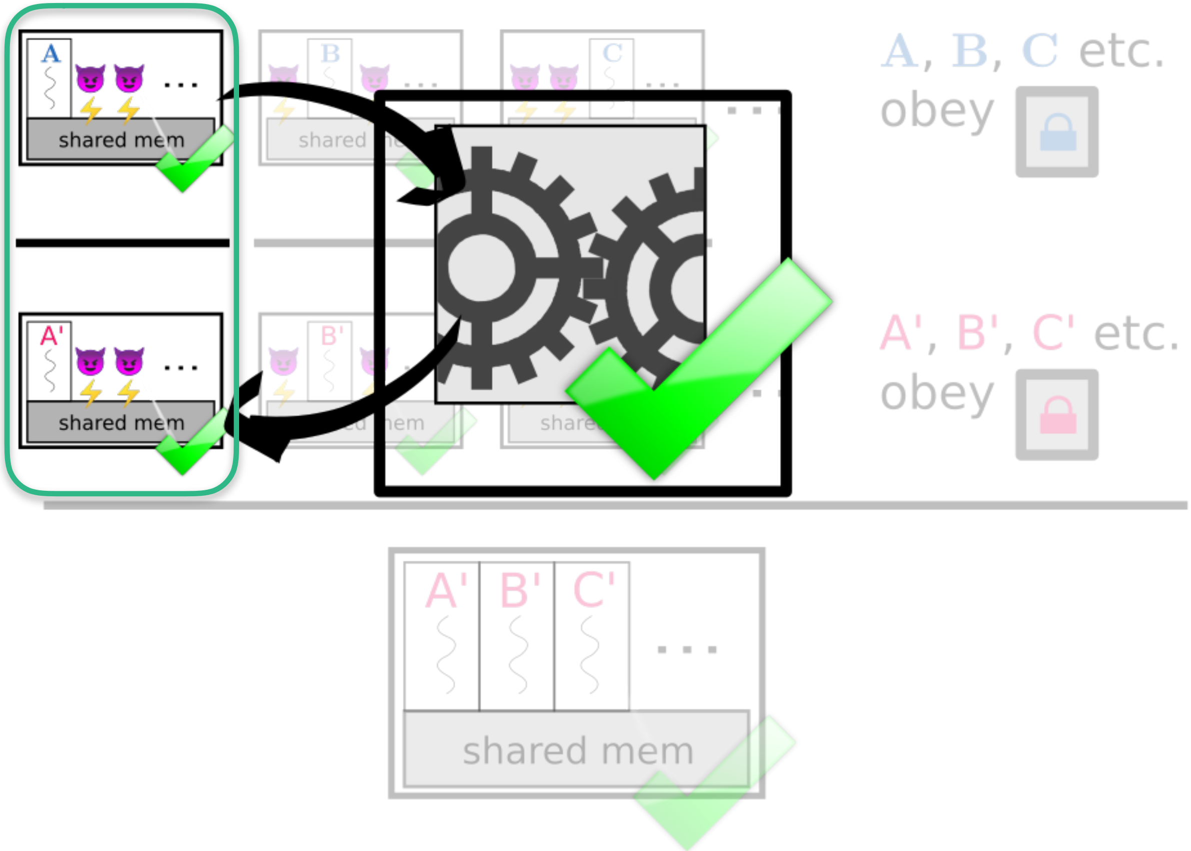
Source

Target

My PhD: so far

Infoflow security-preserving compilation

- With no H-branching: (Instantiation of [Murray et al, CSF'16])



Source

Generic "While"

Target

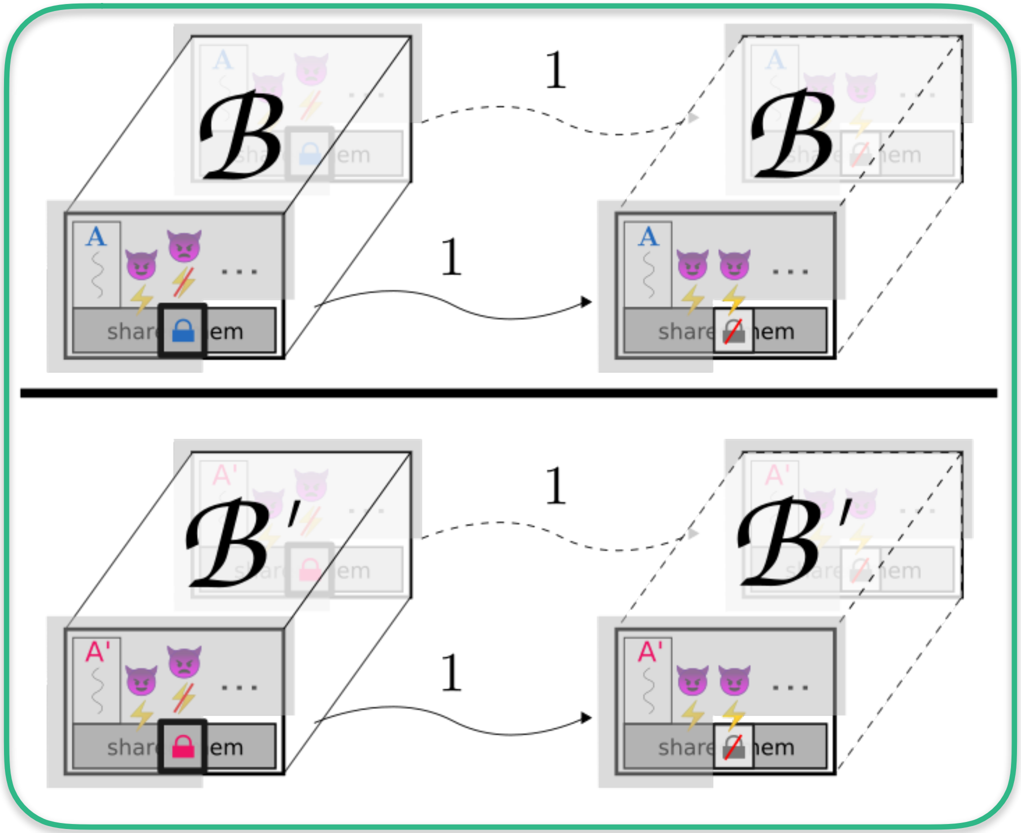
Generic "RISC"

(Formalized in Isabelle/HOL, open source: www.covern.org)

My PhD: so far

Infoflow security-preserving compilation

- With no H-branching: (Instantiation of [Murray et al, CSF'16])



Source

Target

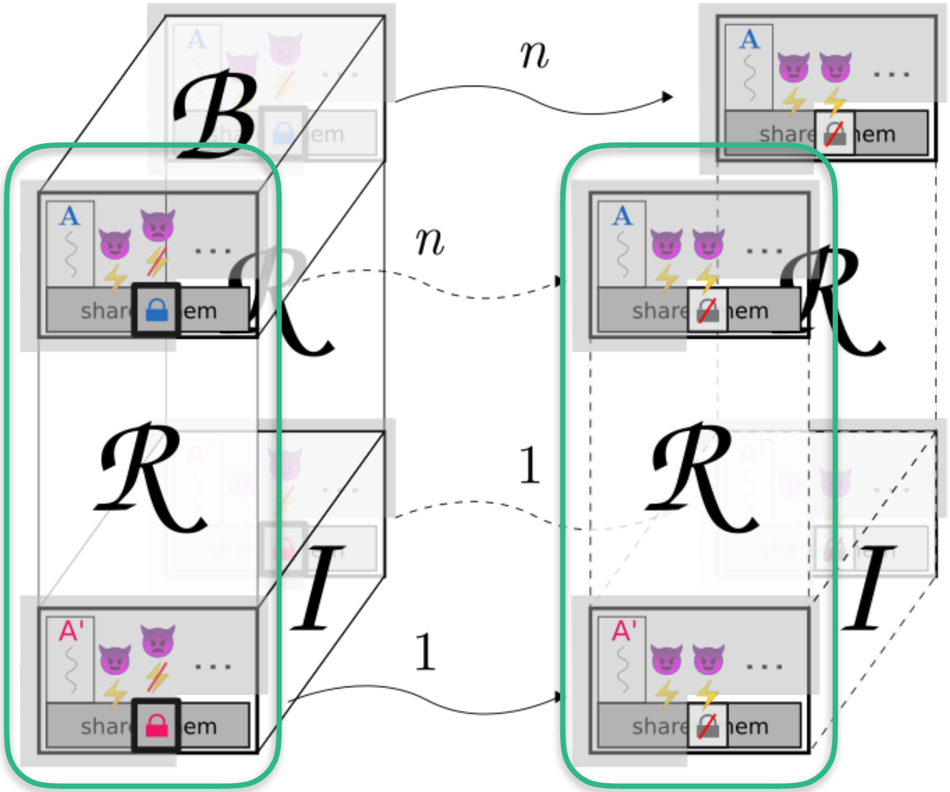
Bisimulations B, B'

(Formalized in Isabelle/HOL, open source: www.covern.org)

My PhD: so far

Infoflow security-preserving compilation

- With no H-branching: (Instantiation of [Murray et al, CSF’16])



Refinement relation *R*

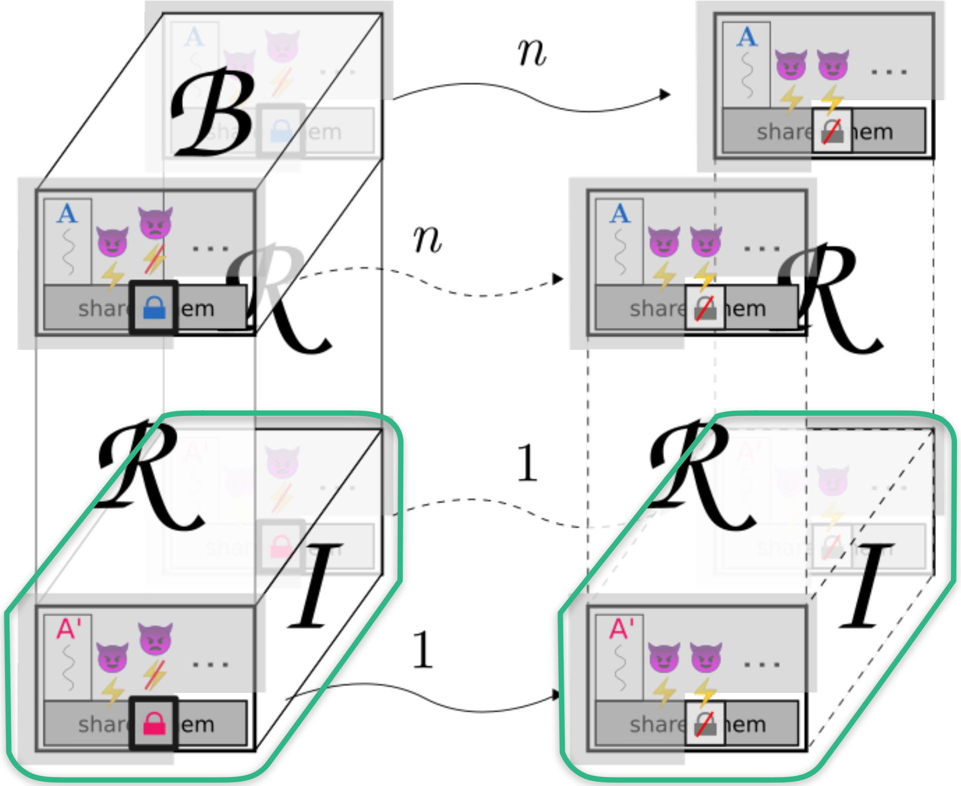
Bisimulations *B, B’*

(Formalized in Isabelle/HOL, open source: www.covern.org)

My PhD: so far

Infoflow security-preserving compilation

- With no H-branching: (Instantiation of [Murray et al, CSF'16])



Refinement relation R

Coupling invariant I (pc-security)

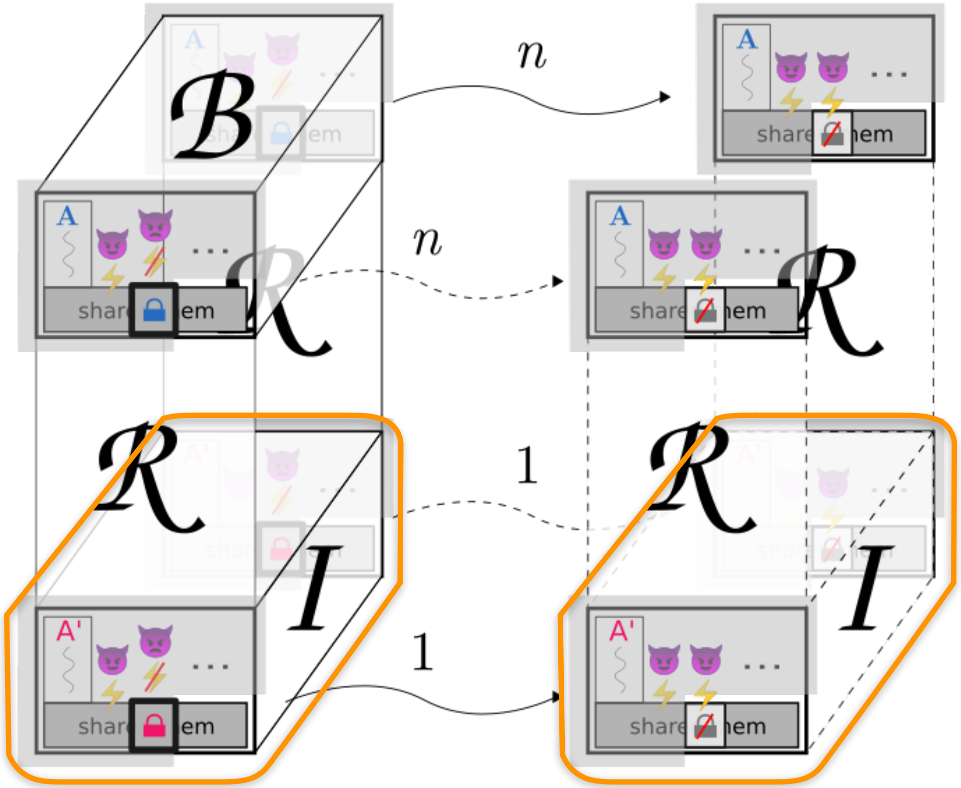
Bisimulations B, B'

(Formalized in Isabelle/HOL, open source: www.covern.org)

My PhD: work in progress

Infoflow security-preserving compilation

- With H-branching? (Relaxation of coupling invariant)



Refinement relation *R*

Coupling invariant *I*
(~~pc-security~~)

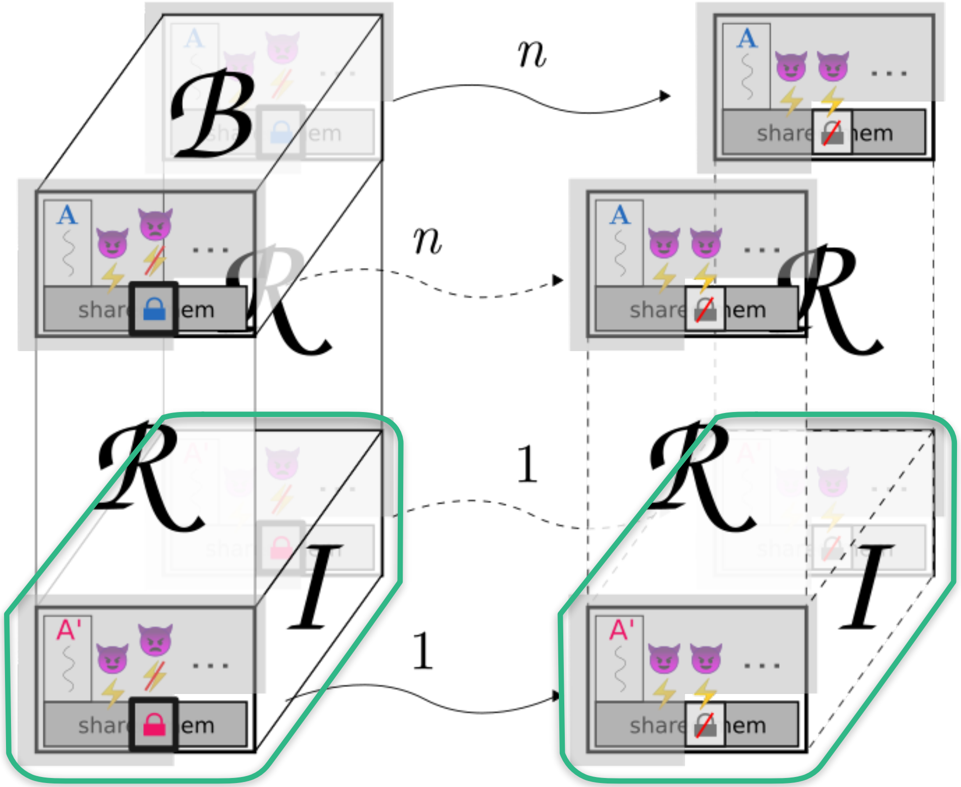
Bisimulations *B*, *B’*

(See: www.covern.org, branch “h-correction”)

For feedback

Infoflow security-preserving compilation

- Applicable to CompCert?



Refinement relation R

Coupling invariant I (pc-security)

Bisimulations B, B'

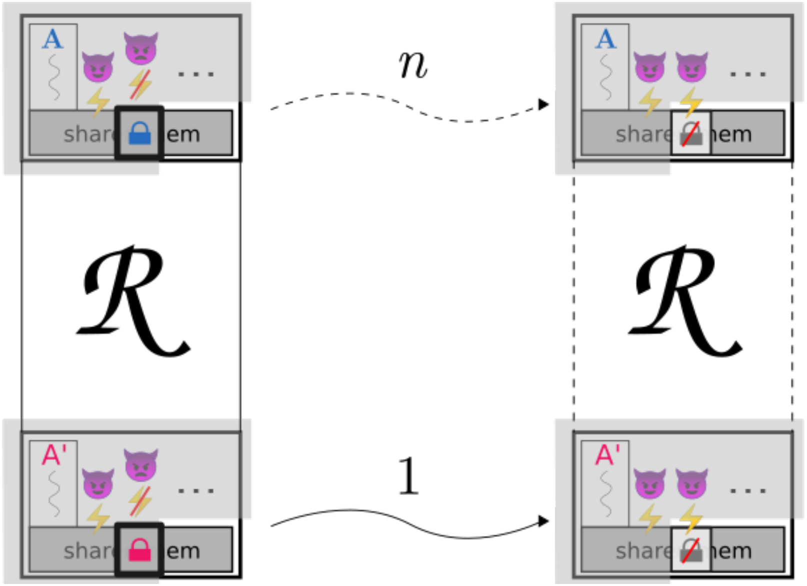
(Simplifications, requirements from [Murray et al, CSF’16])

For feedback

Infoflow security-preserving compilation

- Applicable to CompCert?

$\exists n \ . \ n = \text{abs\_steps } A \ A'$



Refinement relation R

Coupling invariant I (pc-security)

Bisimulations B, B'

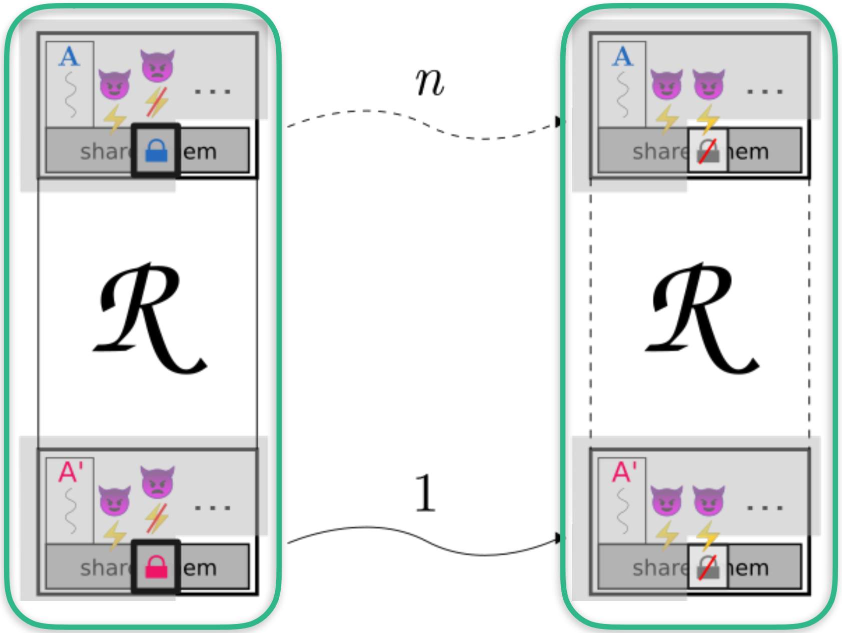
(Simplifications, requirements from [Murray et al, CSF’16])

For feedback

Infoflow security-preserving compilation

- Applicable to CompCert?

$\exists n \,.\, n = \text{abs\_steps}\ \mathbf{A}\ \text{A'}$



Refinement relation R

Coupling invariant I (pc-security)

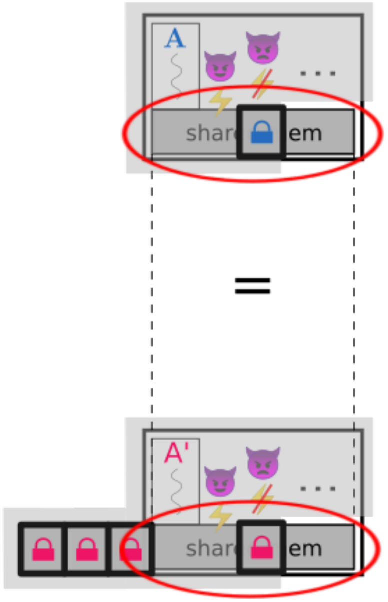
Bisimulations B, B'

(Simplifications, requirements from [Murray et al, CSF’16])

For feedback

Infoflow security-preserving compilation

- Applicable to CompCert? Provisos on R include:
  - Must preserve *all* shared mem contents
  - *No* new shared state allowed



Refinement relation R

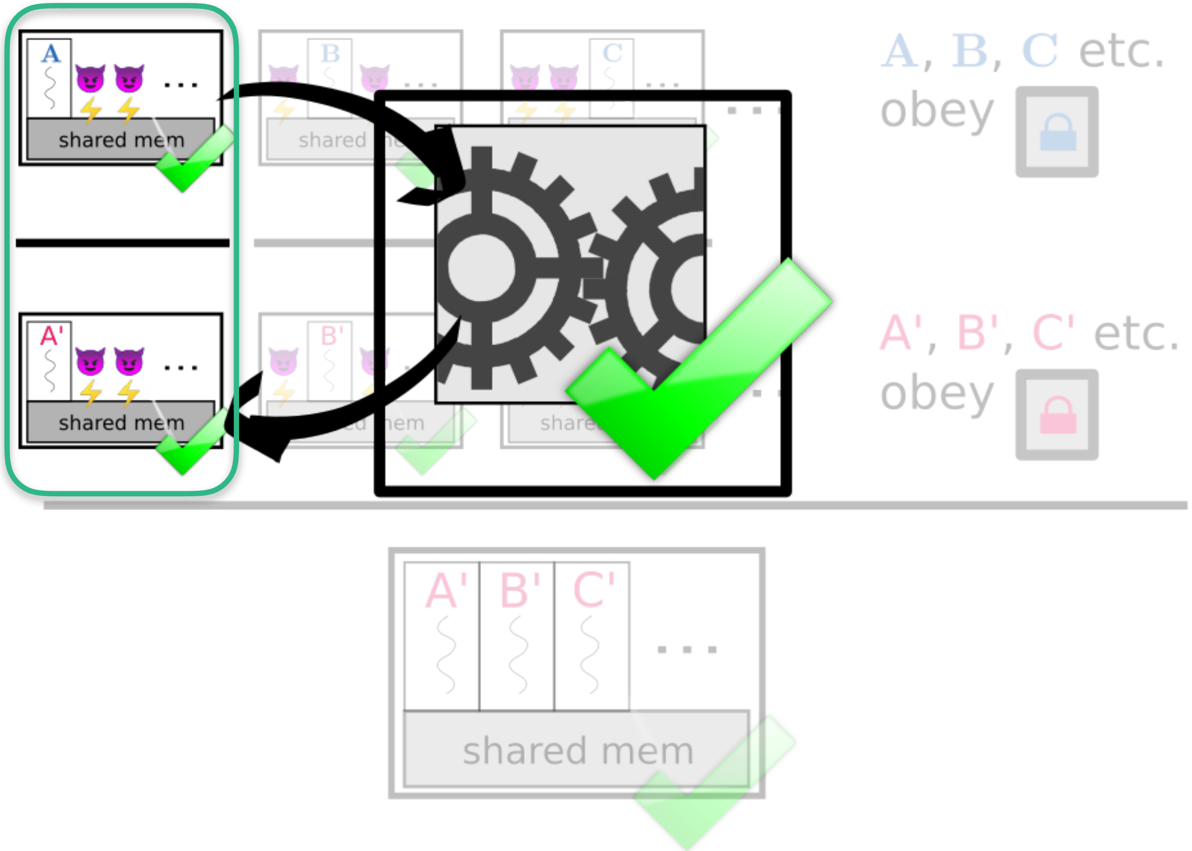
Coupling invariant I (pc-security)

Bisimulations B, B'

(Simplifications, requirements from [Murray et al, CSF'16])

In summary

Infoflow security-preserving compilation



Source

Generic “While”

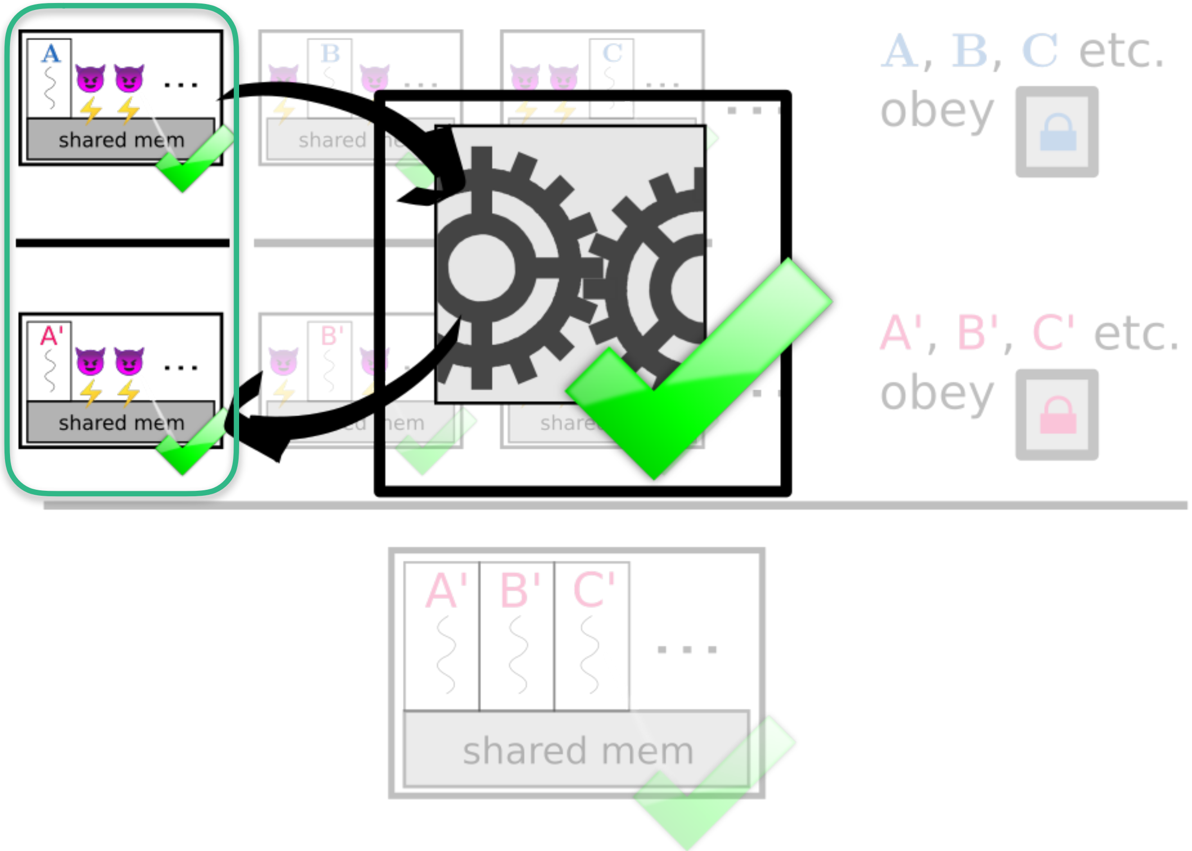
Target

Generic “RISC”

In summary

Infoflow security-preserving compilation

- Proof-of-concept (Isabelle/HOL formalization: www.covern.org)



Source

Generic “While”

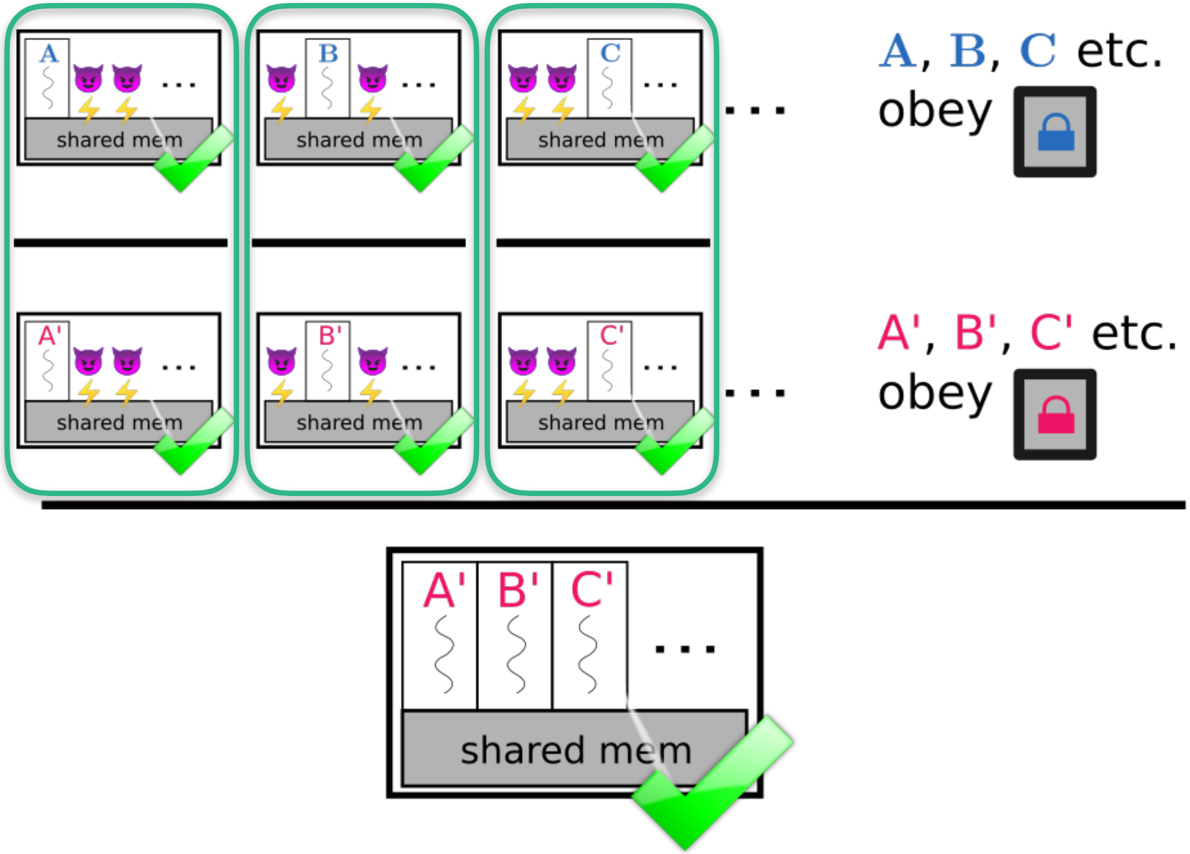
Target

Generic “RISC”

In summary

Infoflow security-preserving compilation

- Proof-of-concept (Isabelle/HOL formalization: www.covern.org)



A, B, C etc. obey 🔒

Source

Generic "While"

A', B', C' etc. obey 🔒

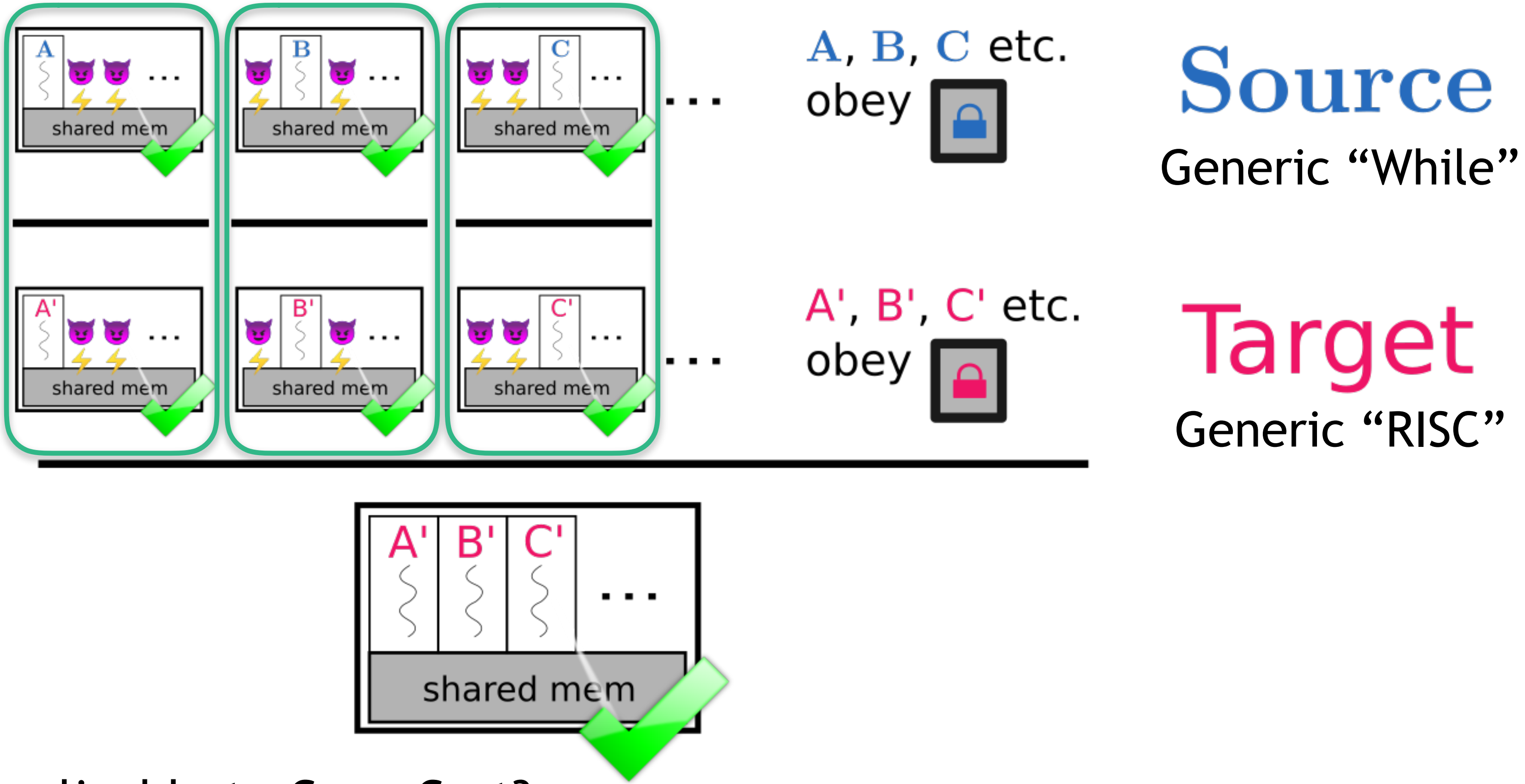
Target

Generic "RISC"

In summary

Infoflow security-preserving compilation

- Proof-of-concept (Isabelle/HOL formalization: www.covern.org)



A, B, C etc. obey

Source

Generic “While”

A', B', C' etc. obey

Target

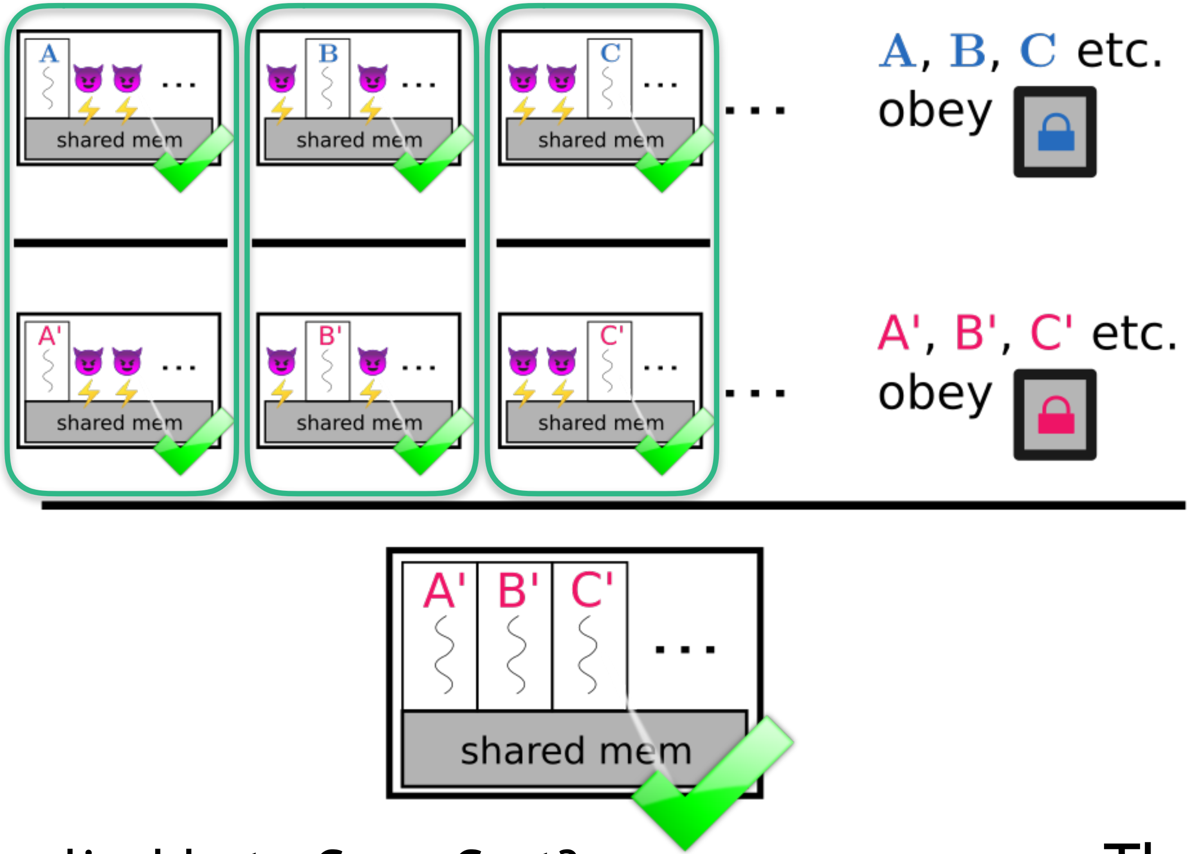
Generic “RISC”

- Applicable to CompCert?

In summary

Infoflow security-preserving compilation

- Proof-of-concept (Isabelle/HOL formalization: www.covern.org)



A, B, C etc. obey 🔒

A', B', C' etc. obey 🔒

Source

Generic "While"

Target

Generic "RISC"

- Applicable to CompCert?

Thank you! Q & A

DATA 61

Thank you

Trustworthy Systems
Robert Sison
PhD Student

e Robert.Sison@data61.csiro.au
w ts.data61.csiro.au/people/?cn=Robert+Sison

THE UNIVERSITY OF
NEW SOUTH WALES

CSIRO