On Compositional Information Flow Aware Refinement

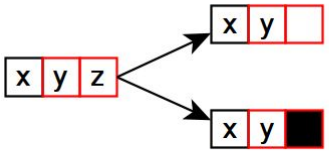
Christoph Baumann
Mads Dam
Roberto Guanciale
Hamed Nemati

CSF 2021

CISPA

Modular verification based on refinement

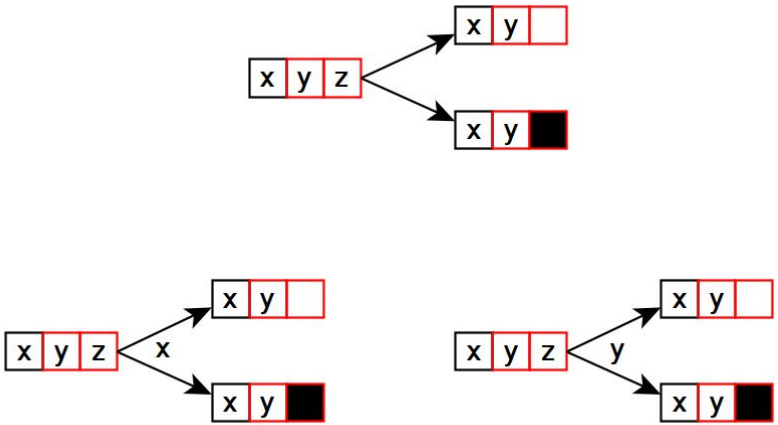
But relationship between Info flow security and refinement is troubled.



J. McLean: A general theory of composition for a class of ”possibilistic” properties

Modular verification based on refinement

But relationship between Info flow security and refinement is troubled.

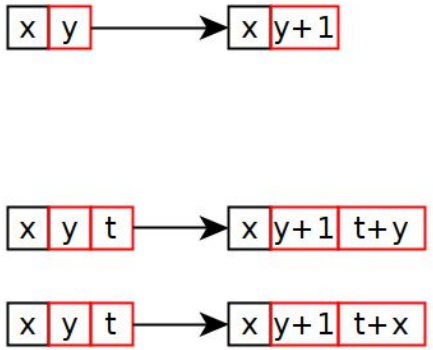


J. McLean: A general theory of composition for a class of ”possibilistic” properties

Well-formed refinement ⇓

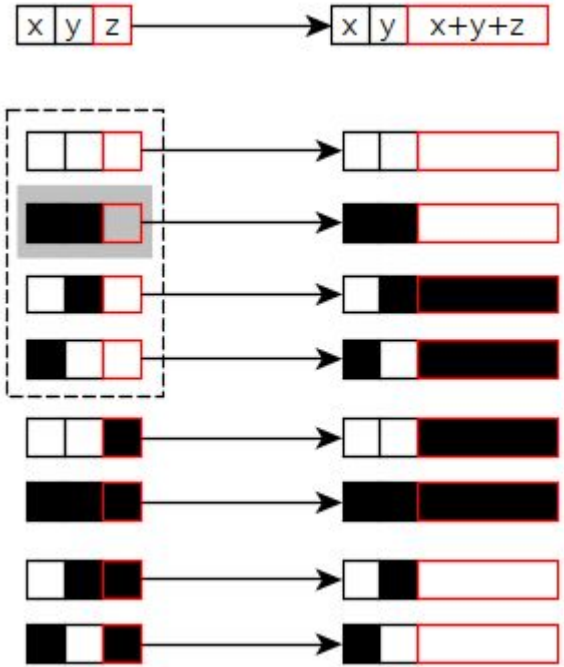
⇓ is a simulation that

- can reduce non-determinism
- can add new variable that introduce discriminating power (e.g. cache state, time)



Ignorance - Knowledge

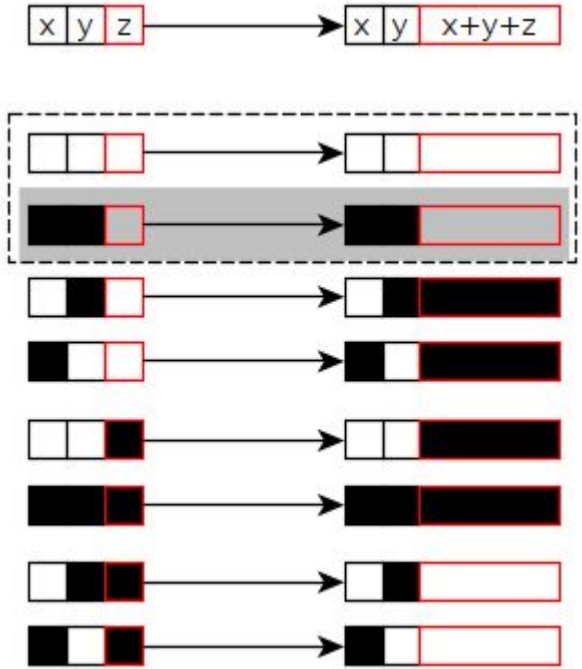
- Semantic justification in terms of the knowledge an observer gains
- Given a run , ignorance = all runs that are observational equivalent (~)



A. Askarov and S. Chong: Learning is change in knowledge: Knowledge-based security for dynamic policies

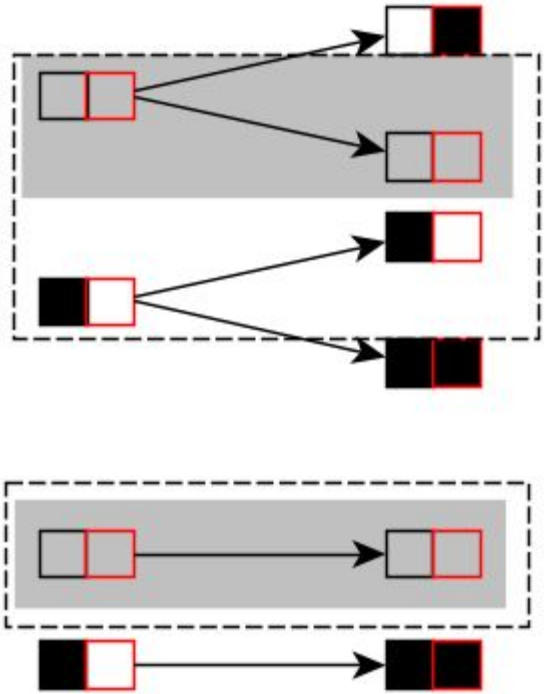
Ignorance - Knowledge

- Semantic justification in terms of the knowledge an observer gains
- Given a run , ignorance = all runs that are observational equivalent (~)



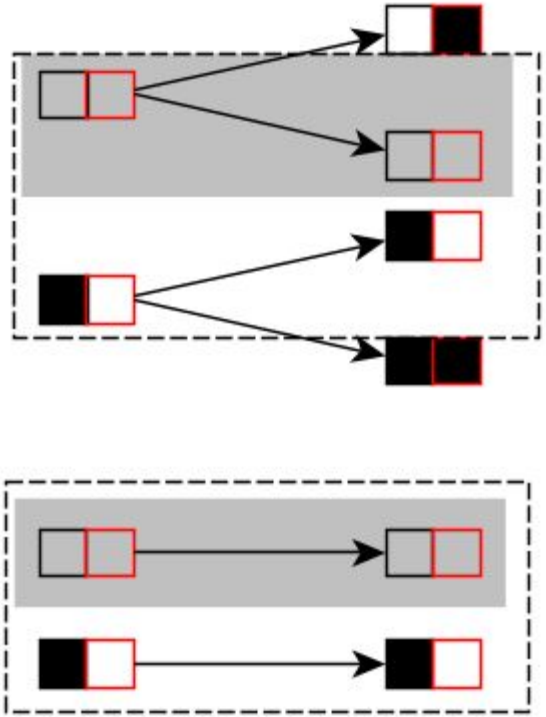
A. Askarov and S. Chong: Learning is change in knowledge: Knowledge-based security for dynamic policies

Ignorance Preserving Refinement (IPR)



C. Morgan, “The Shadow Knows: Refinement and security in sequential programs”

Ignorance Preserving Refinement (IPR)

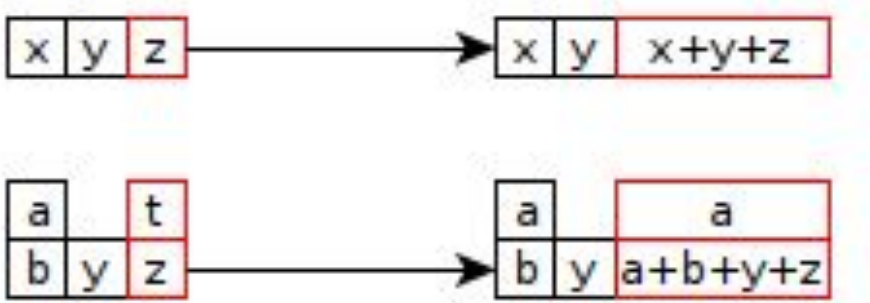


C. Morgan, “The Shadow Knows: Refinement and security in sequential programs”

Ignorance Preserving Refinement (IPR)

$\blacksquare^{a\Downarrow} \blacksquare^{c}$ implies that $\boxed{\ }^{a} = \boxed{\ }^{c\Uparrow}$

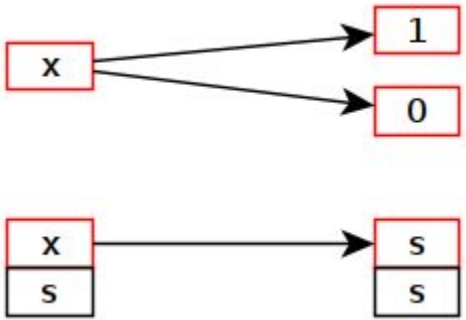
covers the intentional leakage of abstract secret information (e.g. pwd check) and data refinement



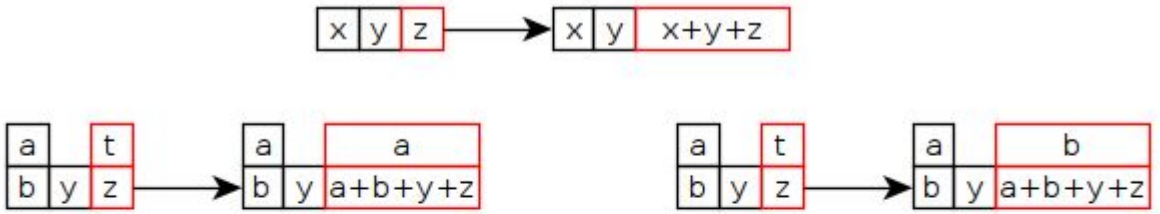
Ignorance Preserving Refinement (IPR)

$\blacksquare^{a\Downarrow} \blacksquare^{c}$ implies that $\boxed{\ }^{a} = \boxed{\ }^{c\Uparrow}$

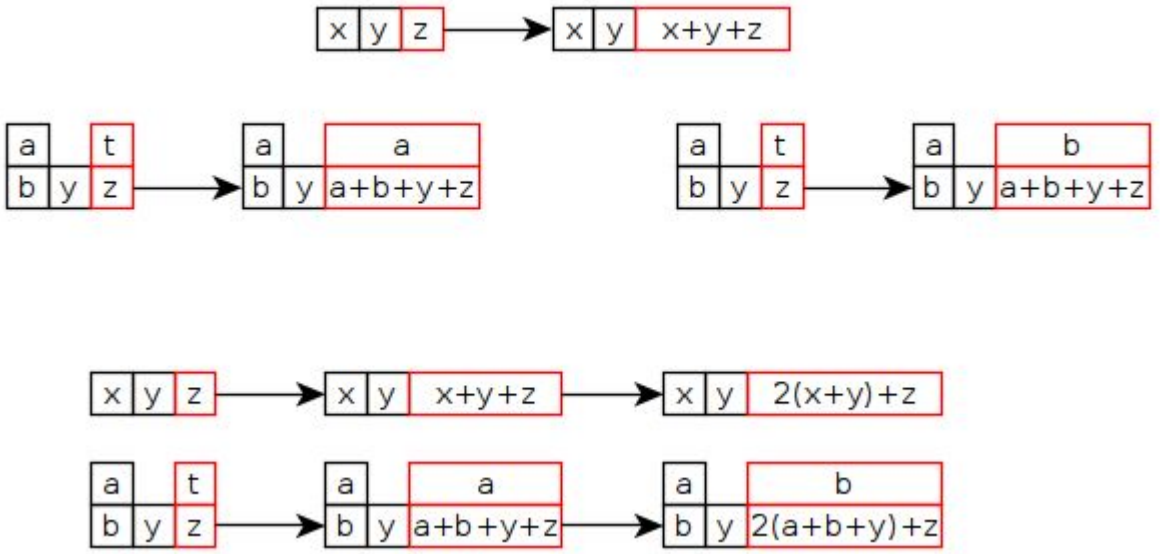
covers the intentional leakage of **abstract** secret information (e.g. pwd check) and data refinement



Compositionality

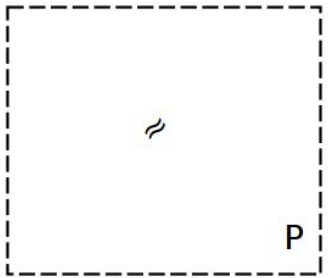


Compositionality



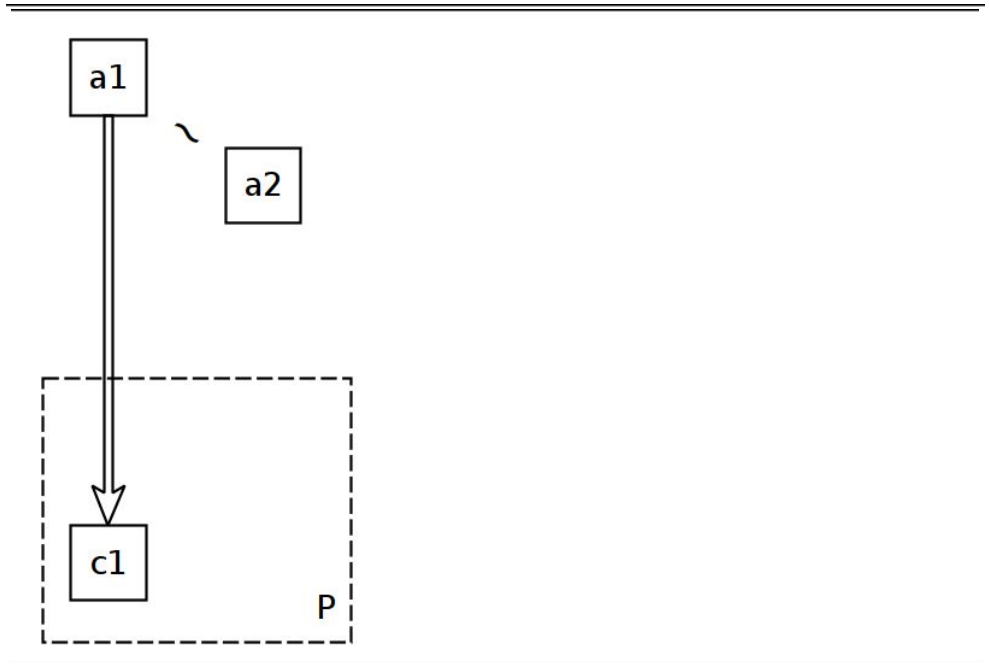
Relational Refinement

{P} ⇓ {Q} is a relational refinement iff



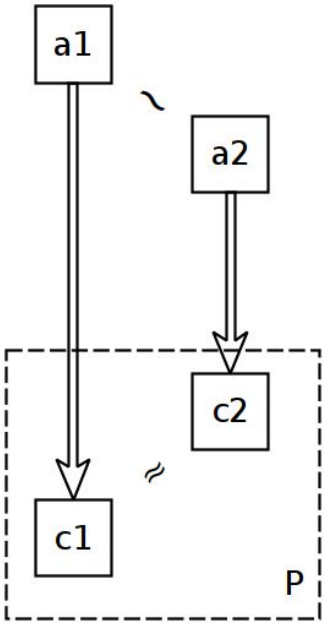
Relational Refinement

{P} ⇓ {Q} is a relational refinement iff



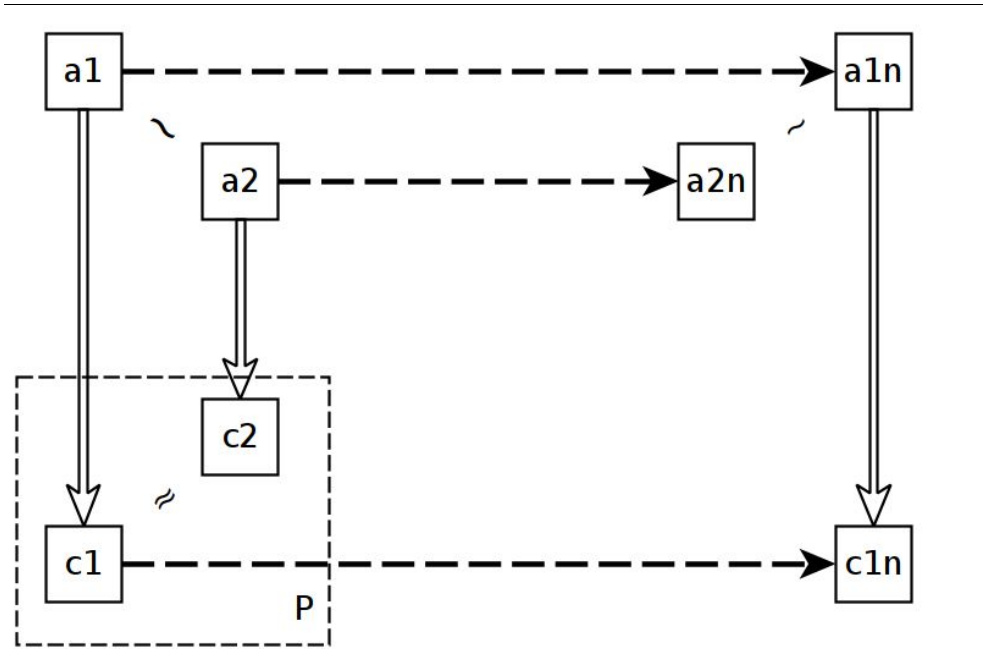
Relational Refinement

{P} ⇓ {Q} is a relational refinement iff



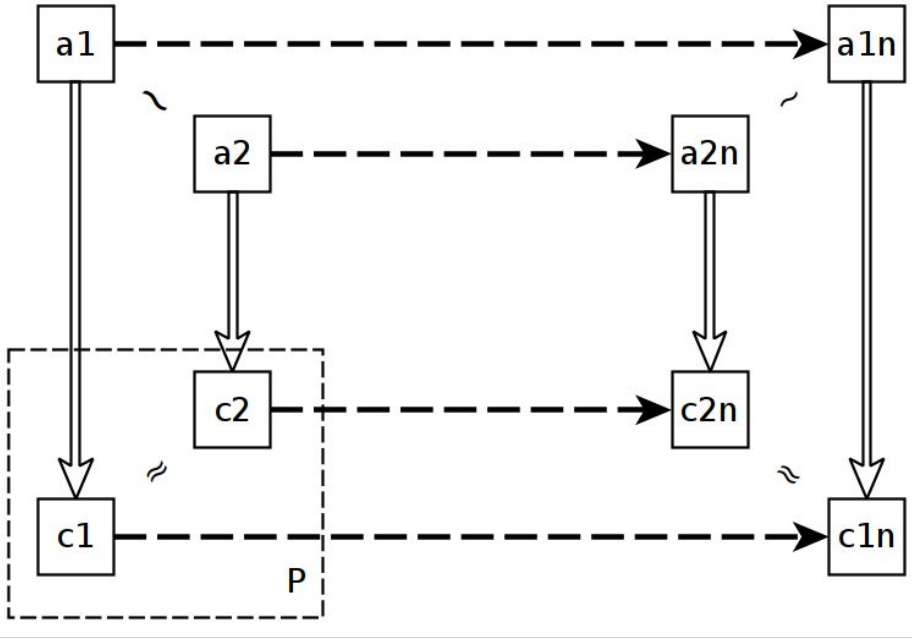
Relational Refinement

{P} ⇓ {Q} is a relational refinement iff



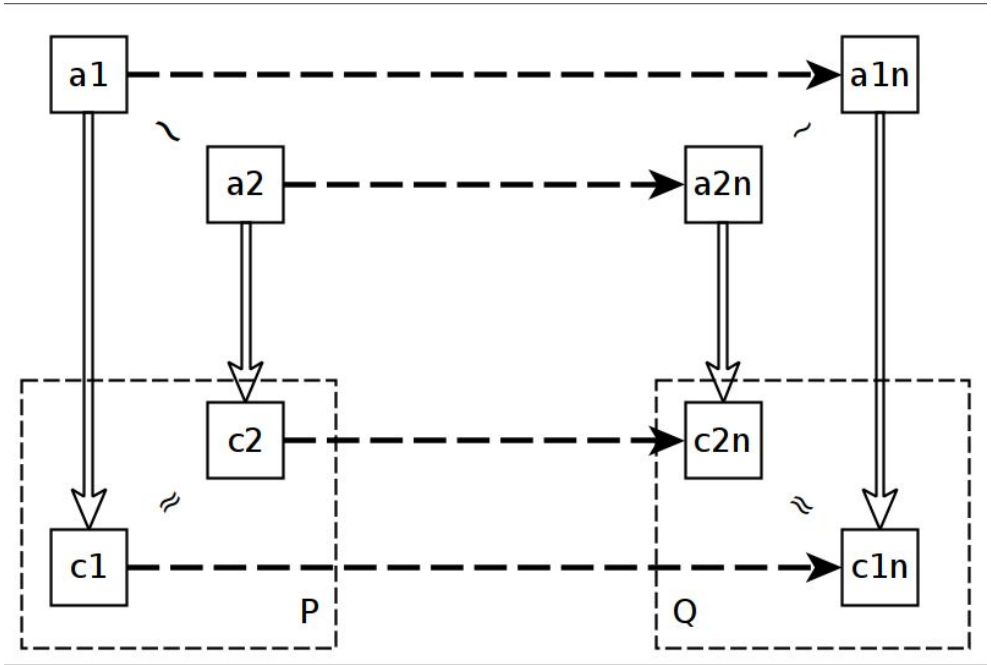
Relational Refinement

{P} ⇓ {Q} is a relational refinement iff



Relational Refinement

{P} ⇓ {Q} is a relational refinement iff



Relational Refinement

If $\{P\} \Downarrow \{Q\}$ is a relational refinement the it is an IPR

If $\{P\} \Downarrow_1 \{Q\}$ and $\{Q\} \Downarrow_2 \{R\}$ are relational refinements then

$\{P\} \Downarrow_1 : \Downarrow_2 \{R\}$ is a relational refinement

In the paper

- Two example applications:
  - SMC addition
  - Oblivious RAM
- Vertical composition
- Related work