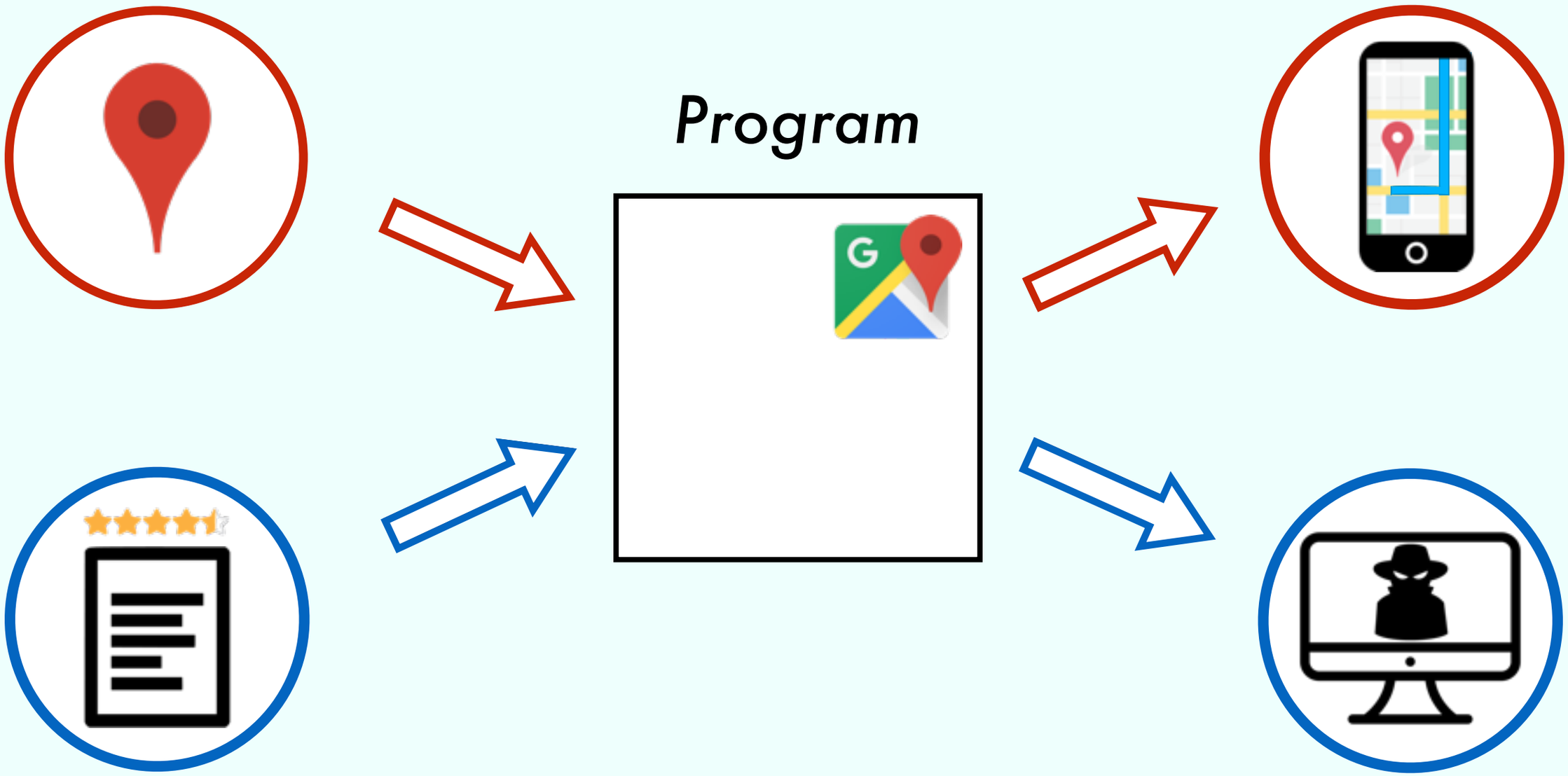
MAC
A Verified Information Flow Control Library

Marco Vassena

Non Interference

Secret Input

Secret Output



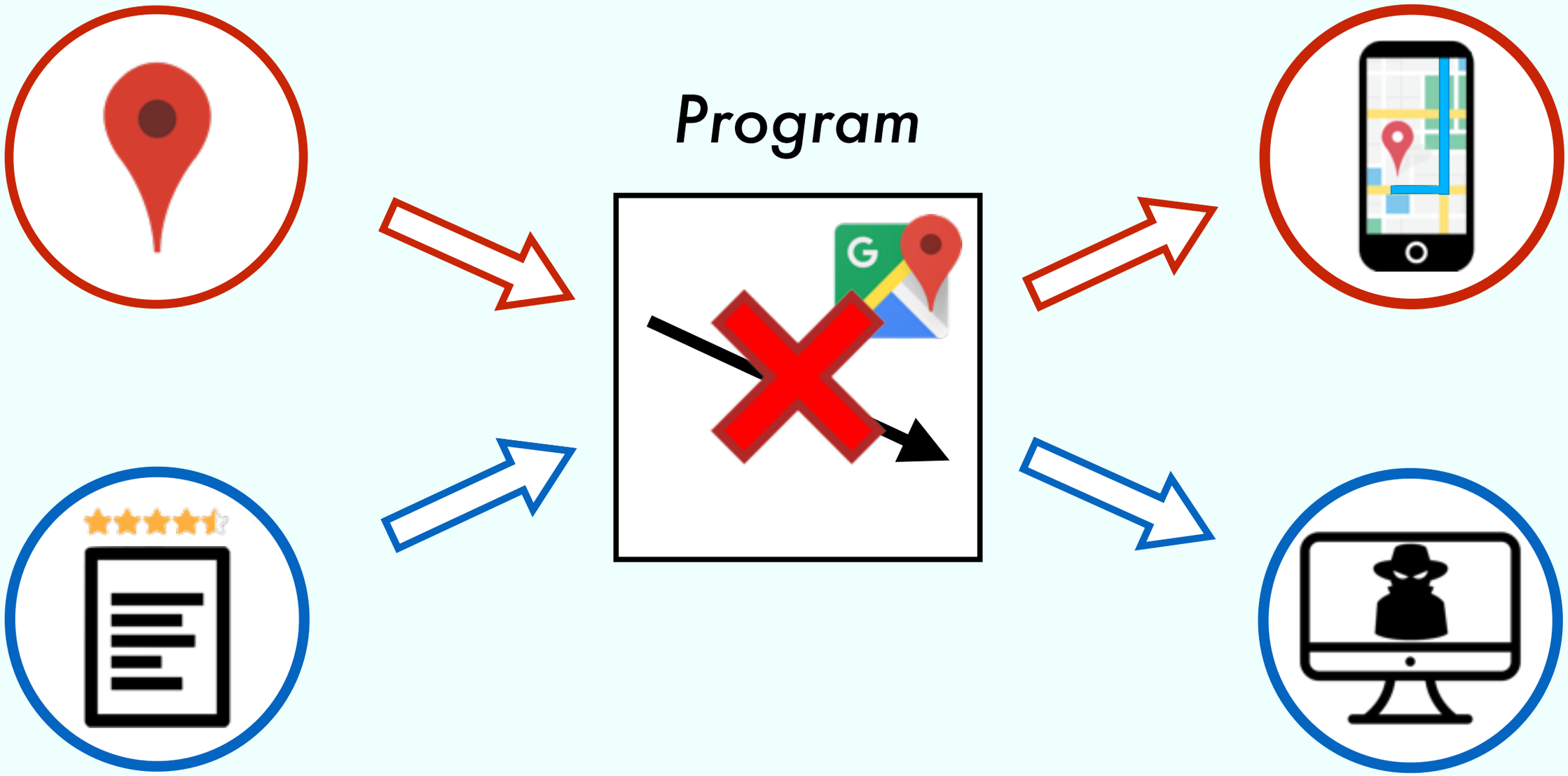
Public Input

Public Output

Non Interference

Secret Input

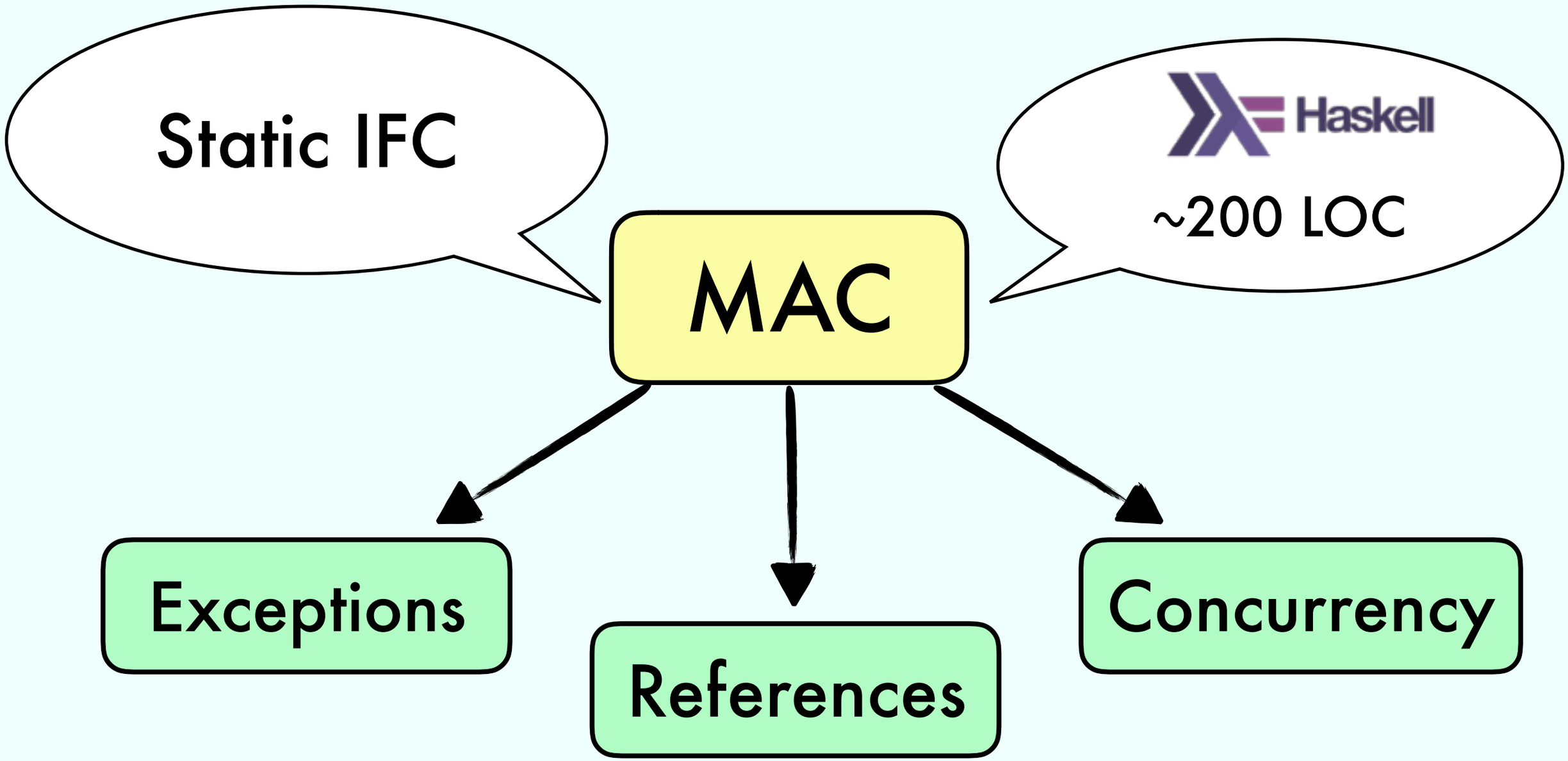
Secret Output



Public Input

Public Output

Previous Work



Functional Pearl: Two can keep a secret, if one of them uses Haskell
Alejandro Russo, ICFP 2015

MAC

Expressive Power

ESORICS'16

Proof Technique

PLAS'16

Covert Channels

CSF'17

Functor Structure

Two-Steps Erasure

NPWT'16

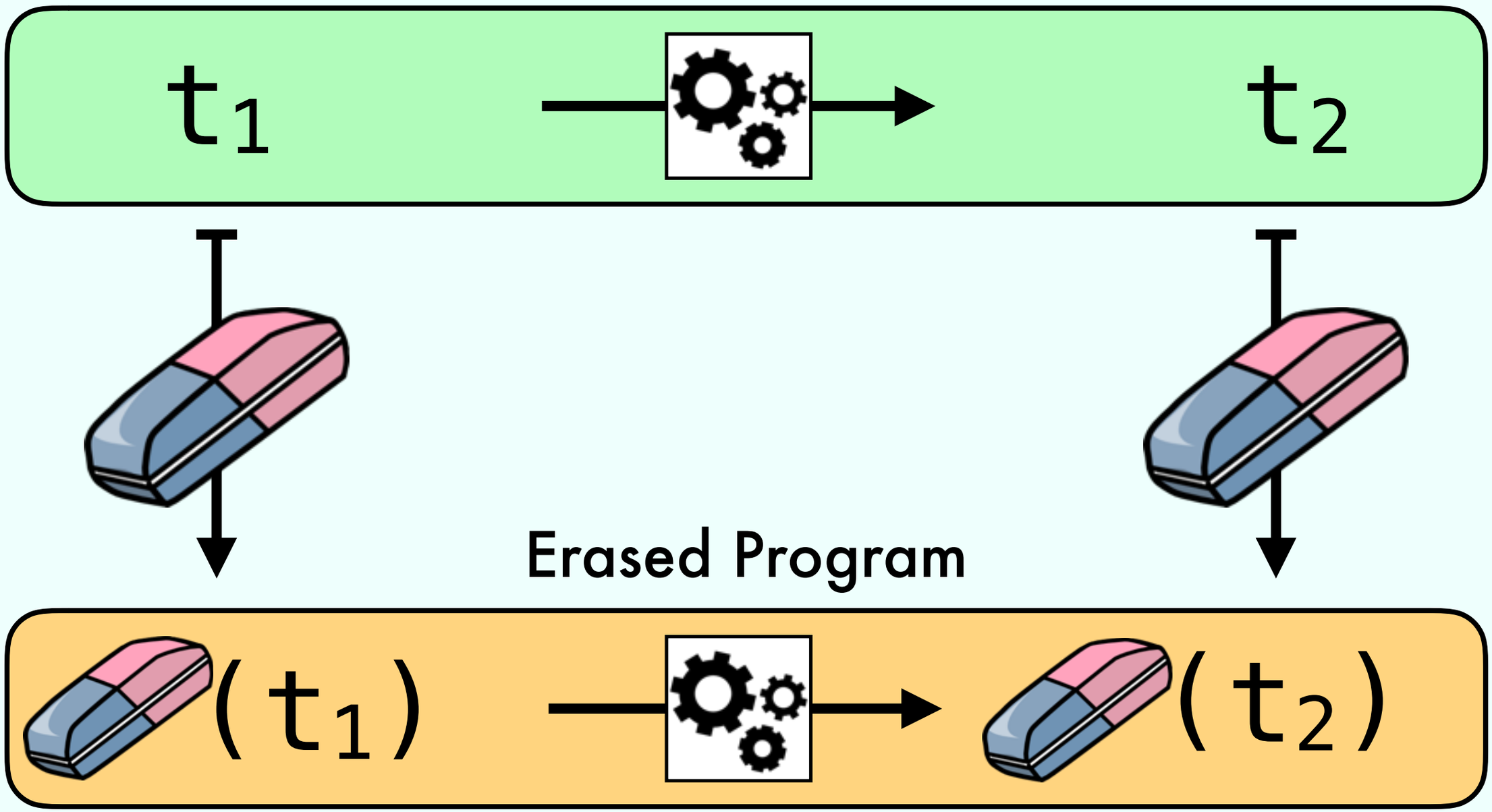
Lazy Evaluation

Journal Article

In submission JLAMP

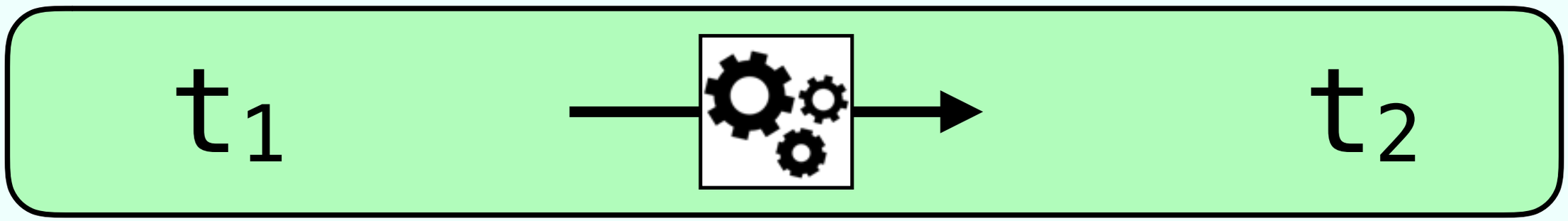
+ = ~8000 LOC (Agda)

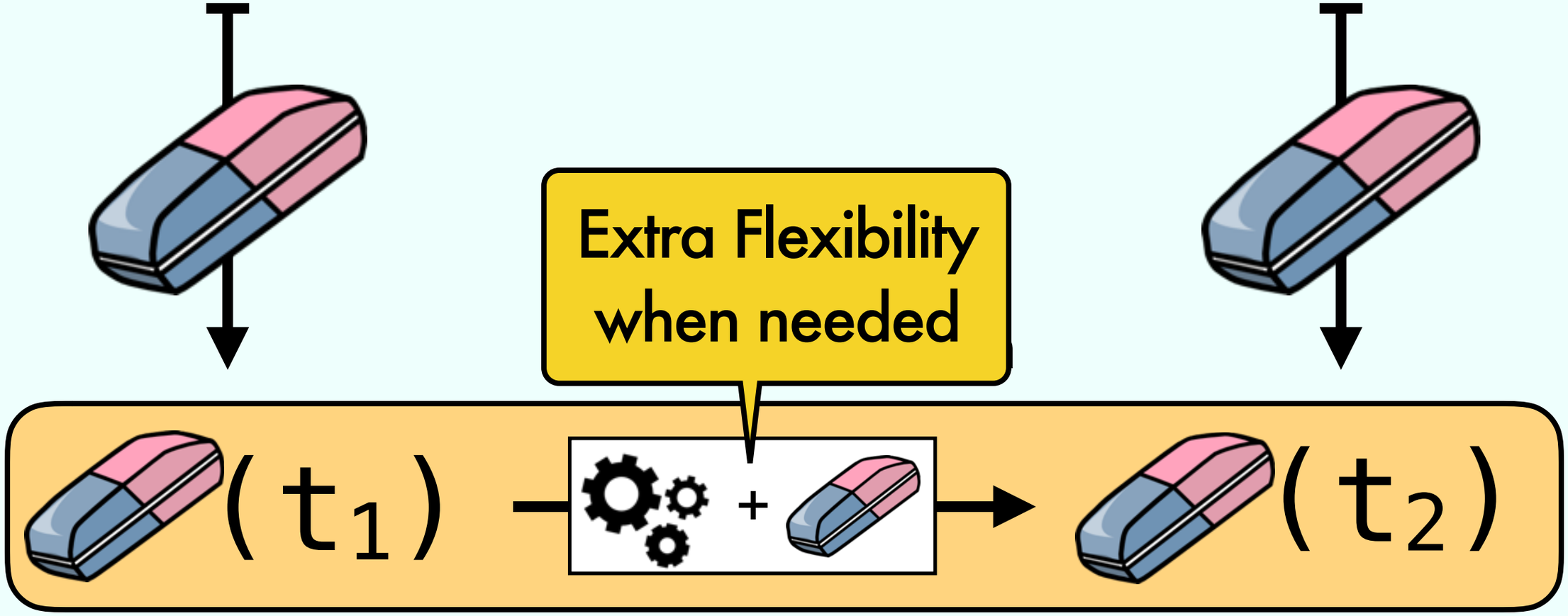
Proof Technique



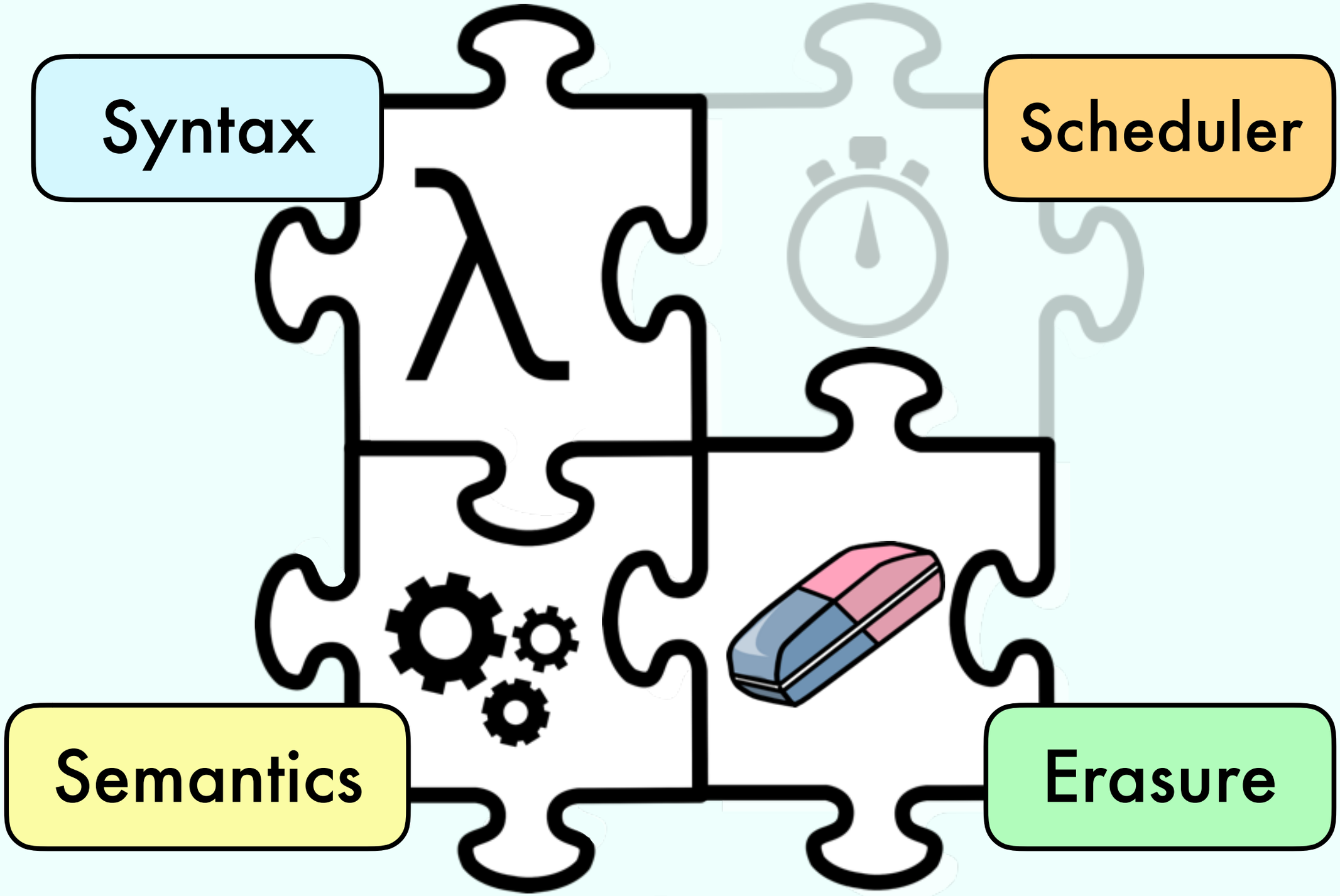
2 Steps Erasure

Original Program

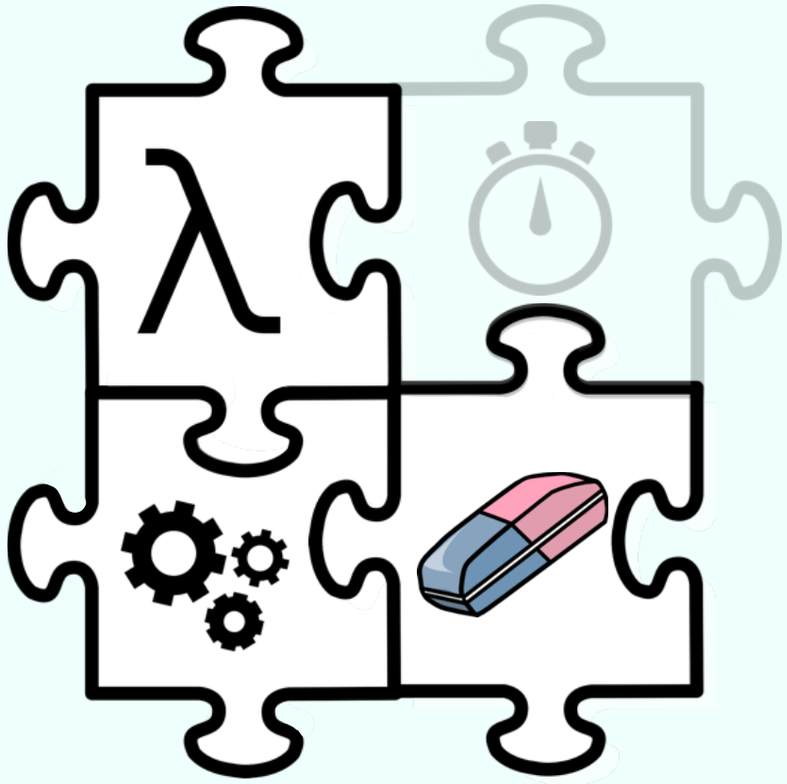




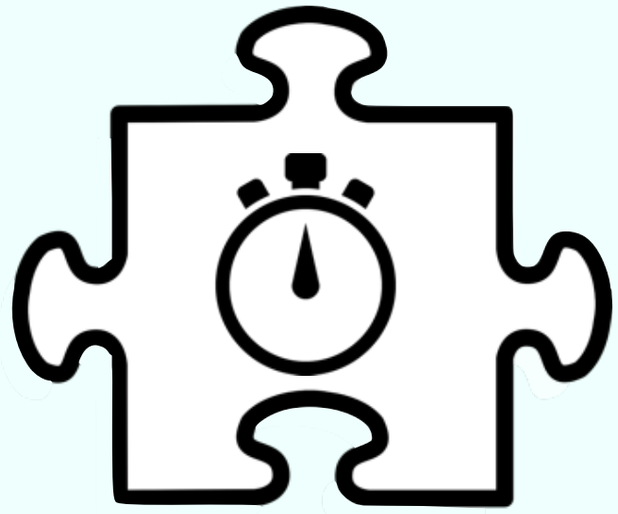
Scheduler Parametric Model



Parametric Model

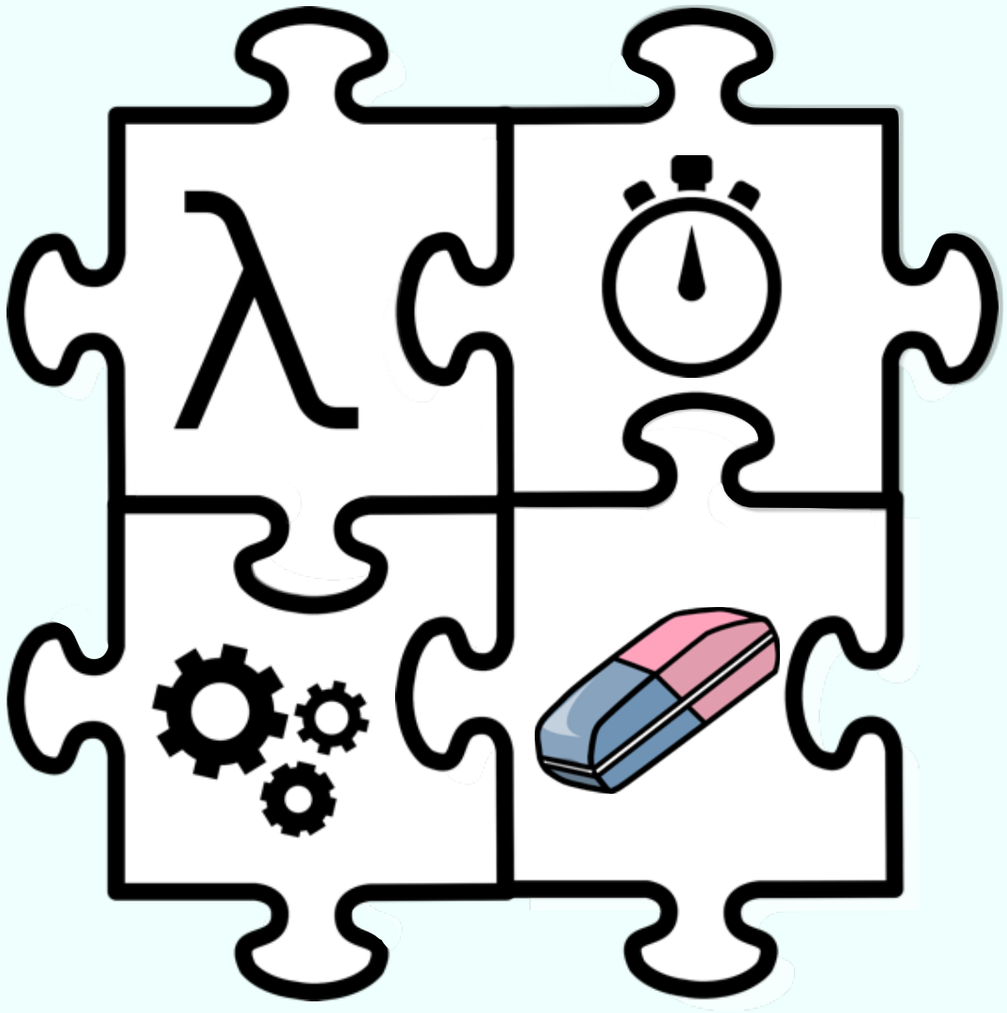


Round Robin



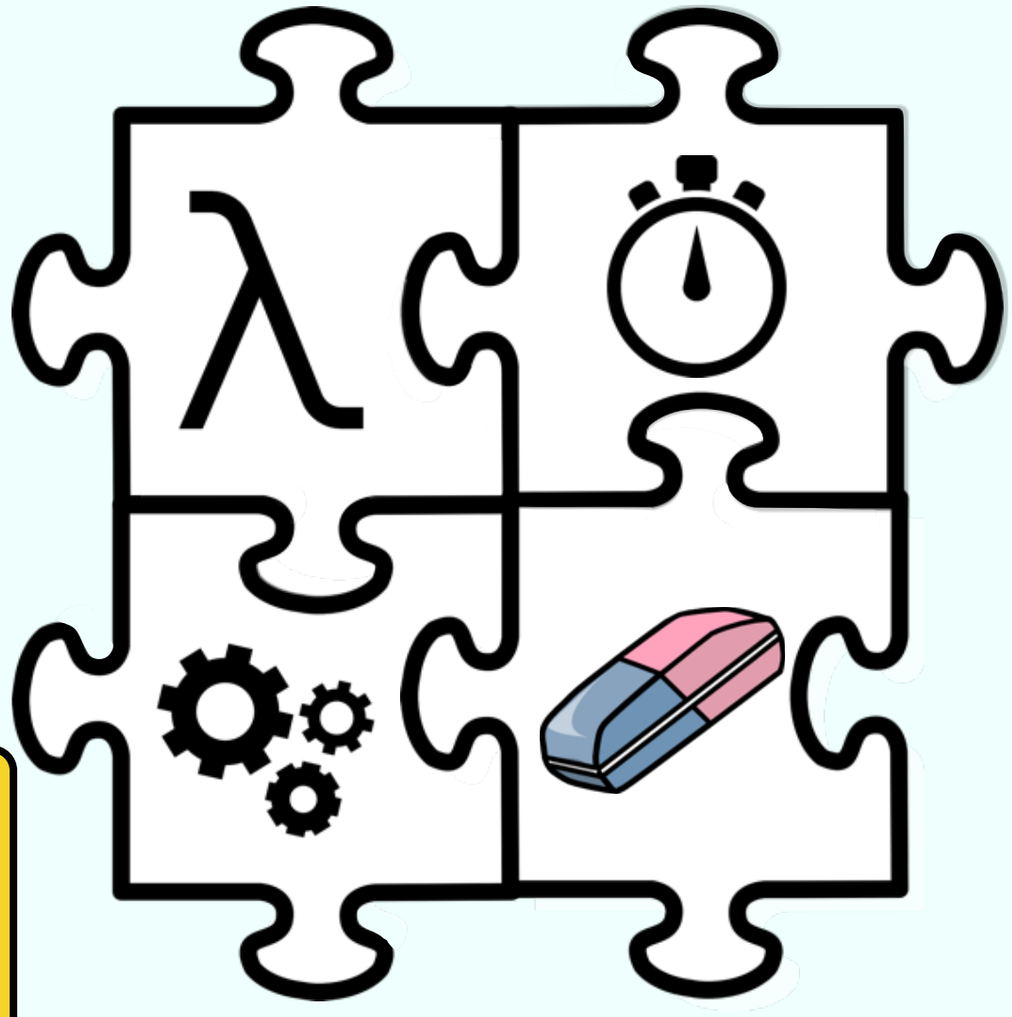
Parametric Model

Round Robin



Parametric Model

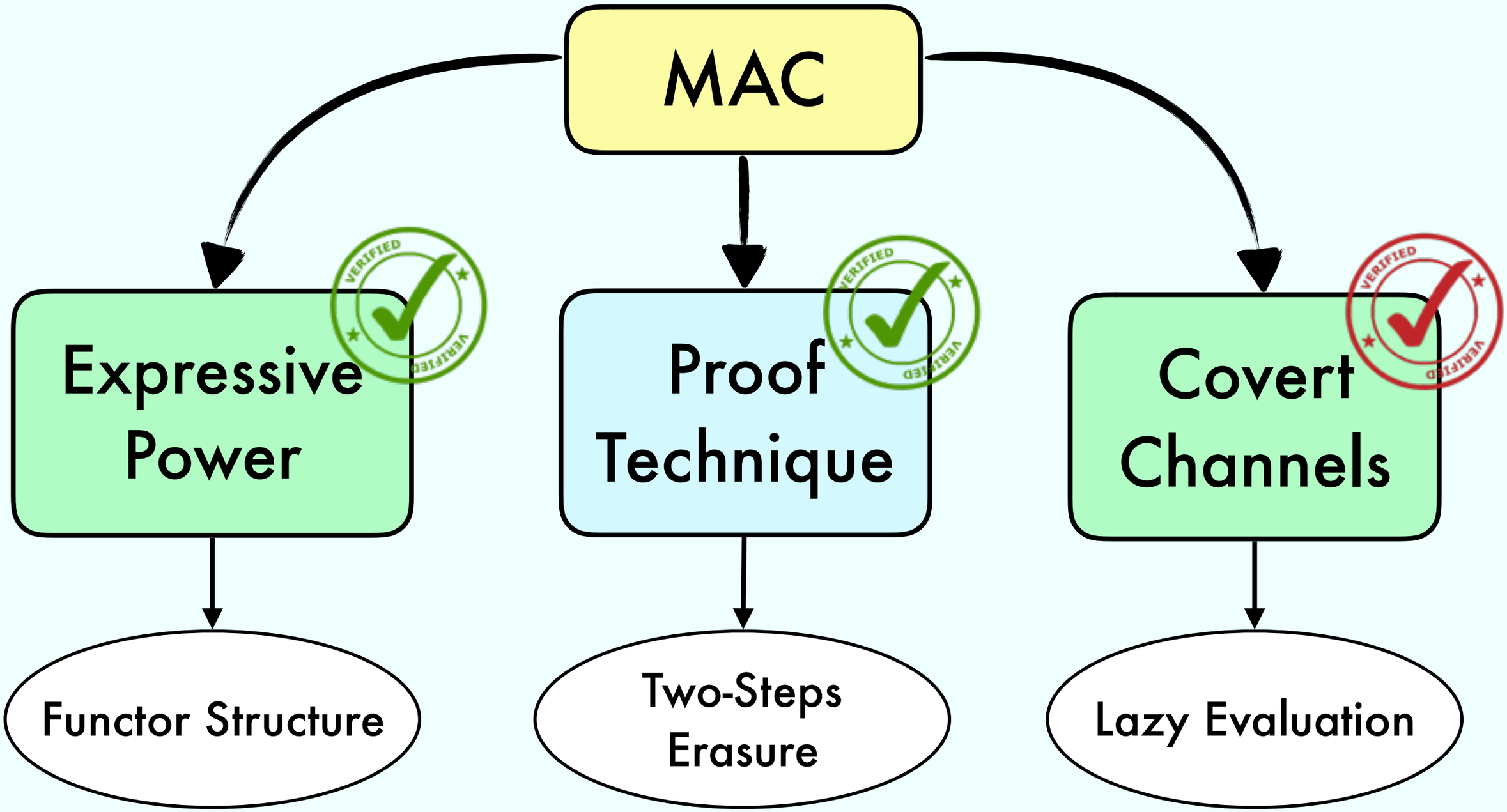
Round Robin



Progress Sensitive
Non Interference

MAC is Secure

Summary


MAC
Expressive Power
Proof Technique
Covert Channels
Functor Structure
Two-Steps Erasure
Lazy Evaluation