

Who Verifies the Verifier?

Certificates for Probabilistic Model Checking

Tobias Winkler
UnRAVeL Spring WS 2025



Parts of this presentation are based on a TACAS '25 paper with Krishnendu Chatterjee, Tim Quatmann, Maximilian Schäffeler, Maximilian Weininger, and Daniel Zilken.

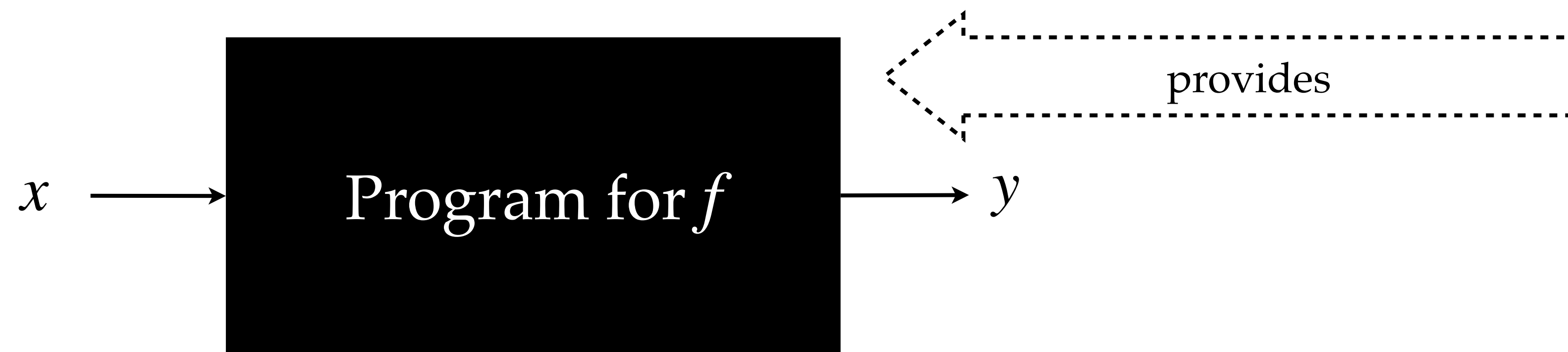
Part I: Certifying Algorithms

The Implementation Problem

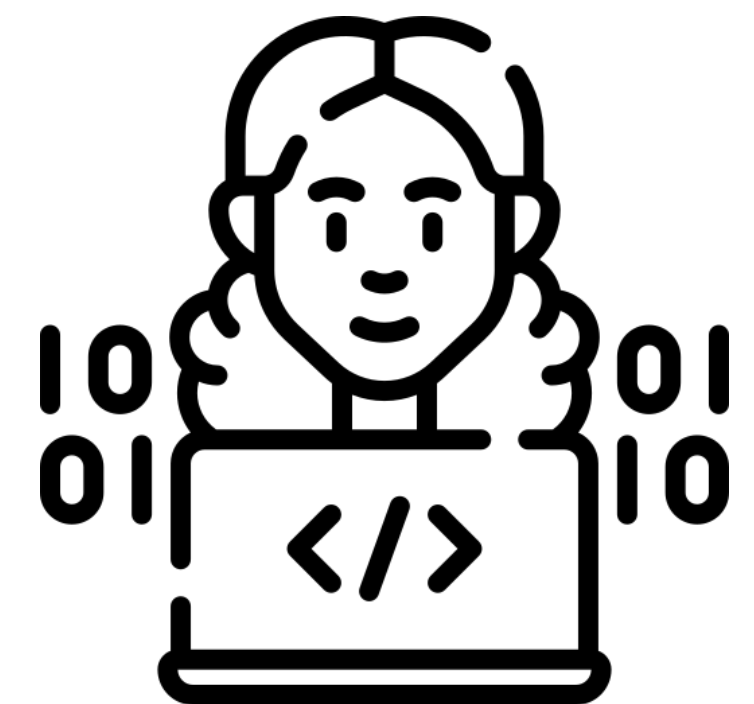
$f: X \rightarrow Y$ specification or abstract algorithm.

The Implementation Problem

$f: X \rightarrow Y$ specification or abstract algorithm.

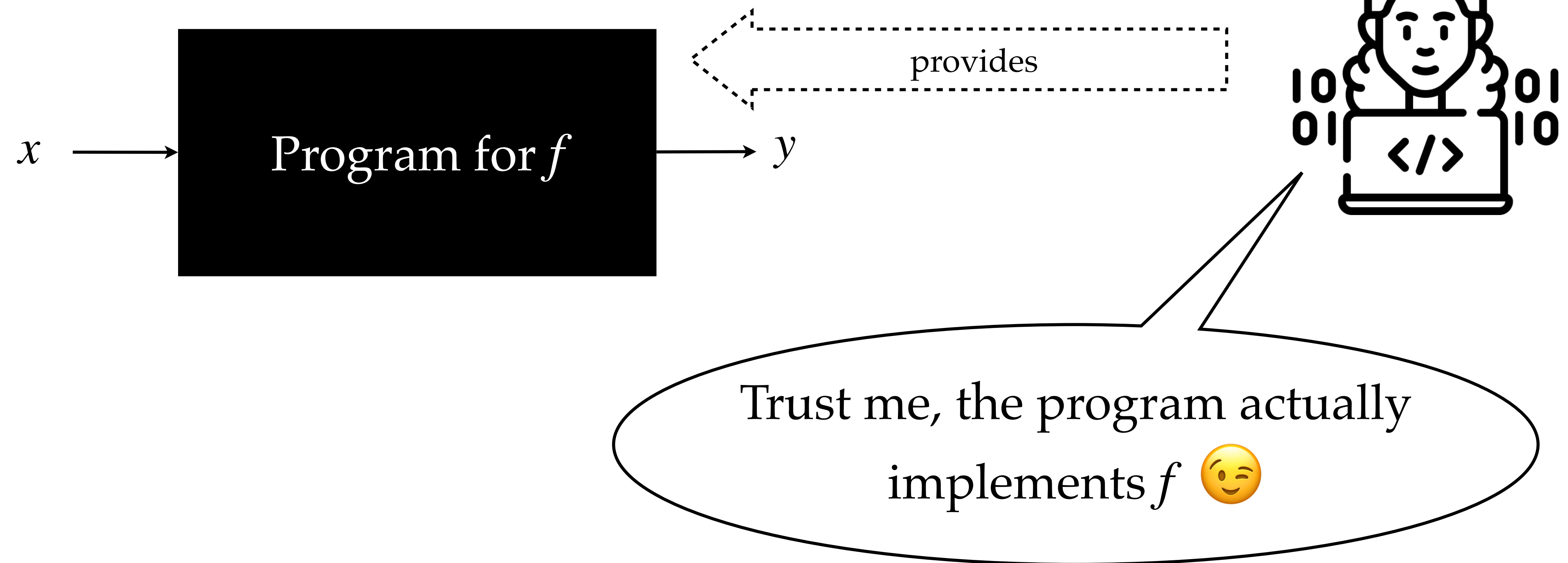


You or some other
programmer(s)



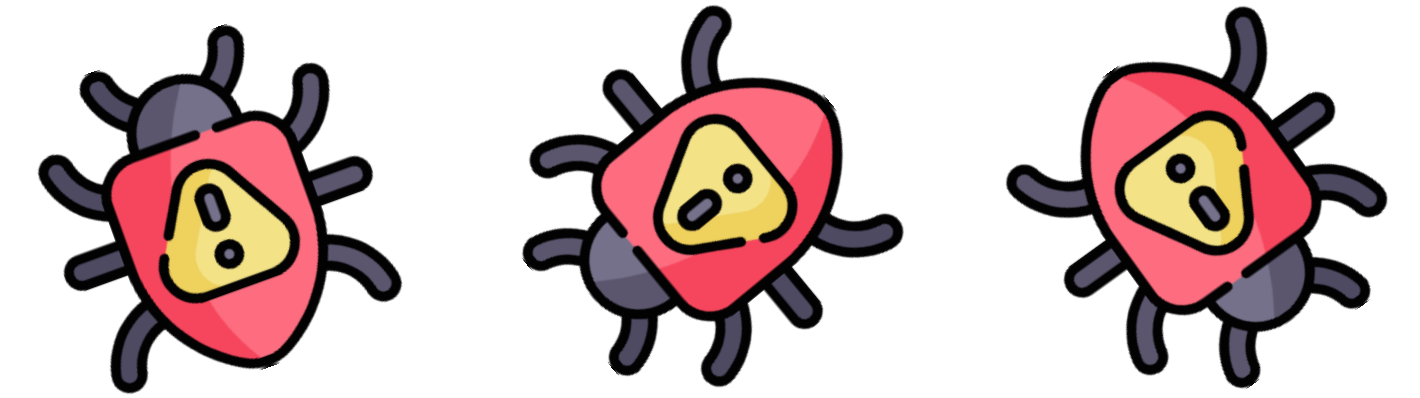
The Implementation Problem

$f: X \rightarrow Y$ specification or abstract algorithm.



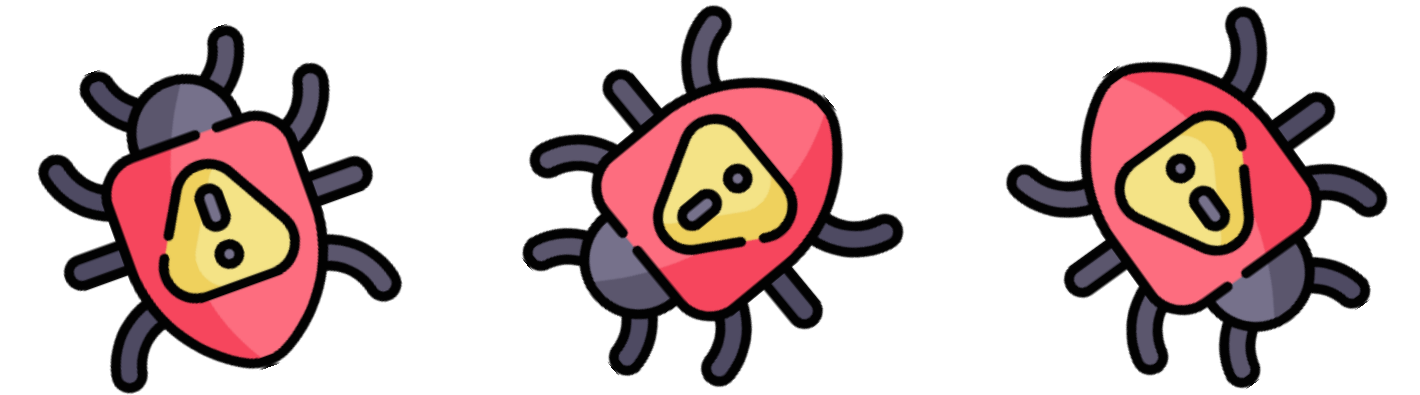
Reasons Not to Trust Your Code

(Or Someone Else's)



Reasons Not to Trust Your Code

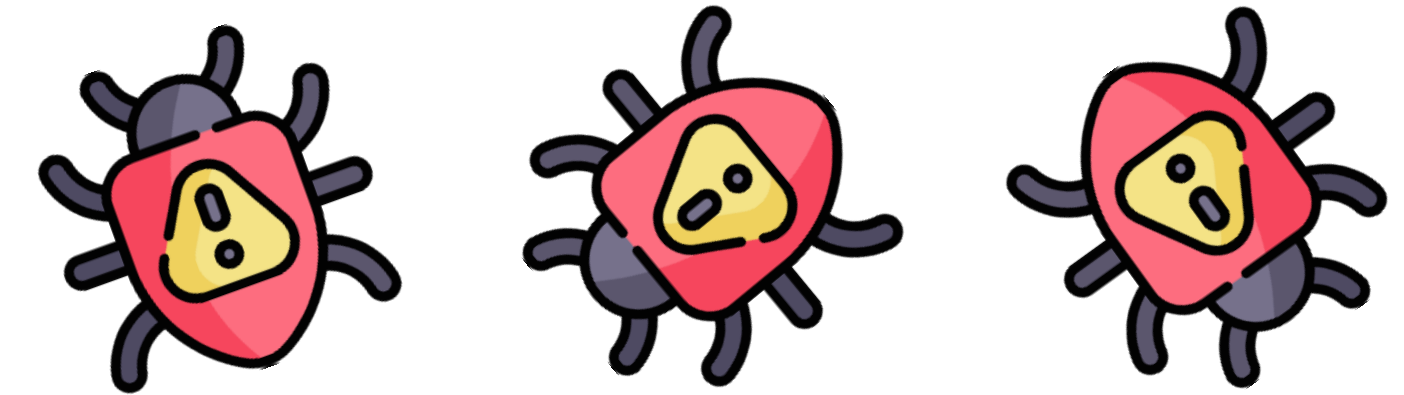
(Or Someone Else's)



- Bugs (wrong implementation of a right idea)

Reasons Not to Trust Your Code

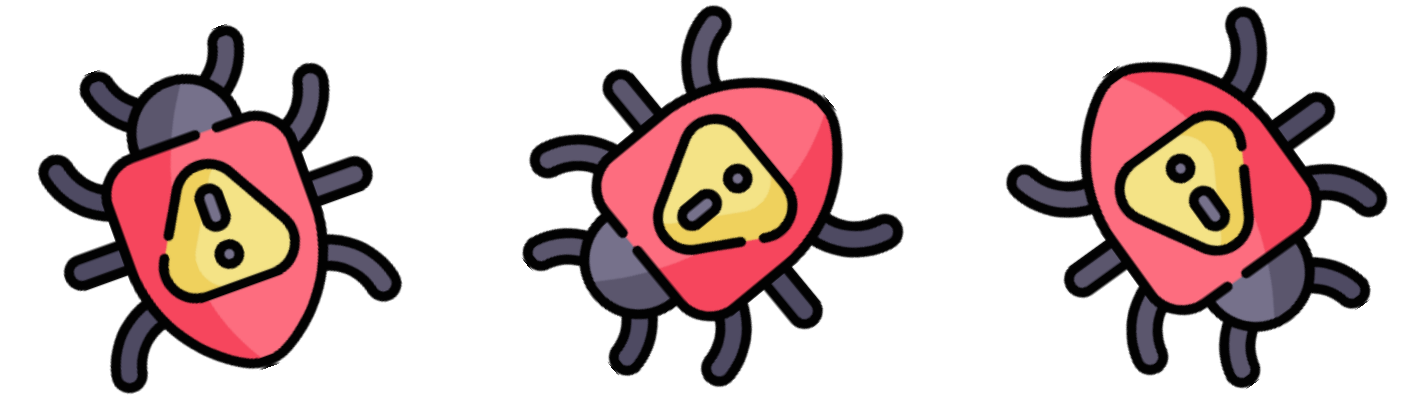
(Or Someone Else's)



- Bugs (wrong implementation of a right idea)
- Right implementation of a wrong idea

Reasons Not to Trust Your Code

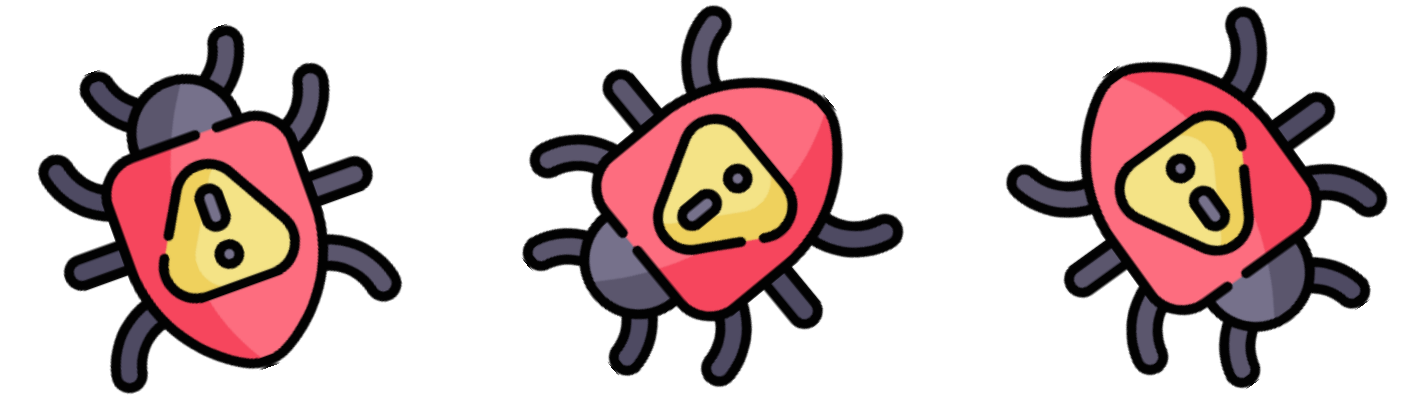
(Or Someone Else's)



- Bugs (wrong implementation of a right idea)
- Right implementation of a wrong idea
- Errors due to inexact floating point arithmetic

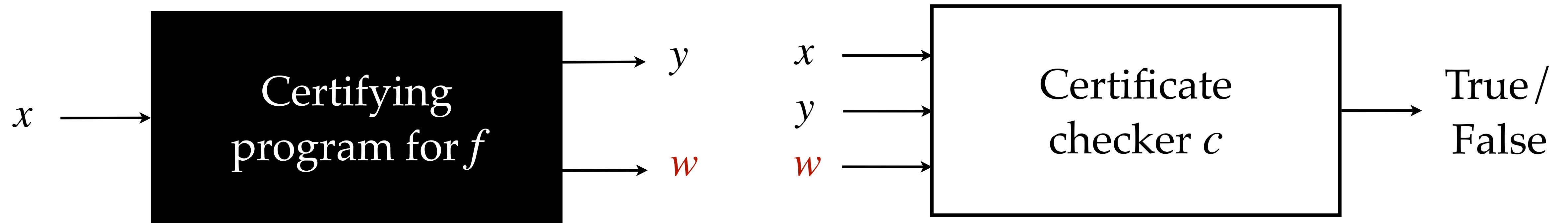
Reasons Not to Trust Your Code

(Or Someone Else's)



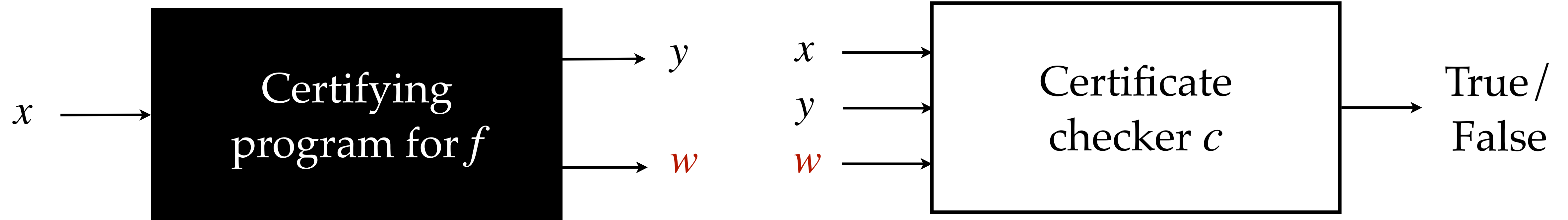
- Bugs (wrong implementation of a right idea)
- Right implementation of a wrong idea
- Errors due to inexact floating point arithmetic
- Unsound 3rd party software (e.g. LP solver, compiler, ...)

Certificates

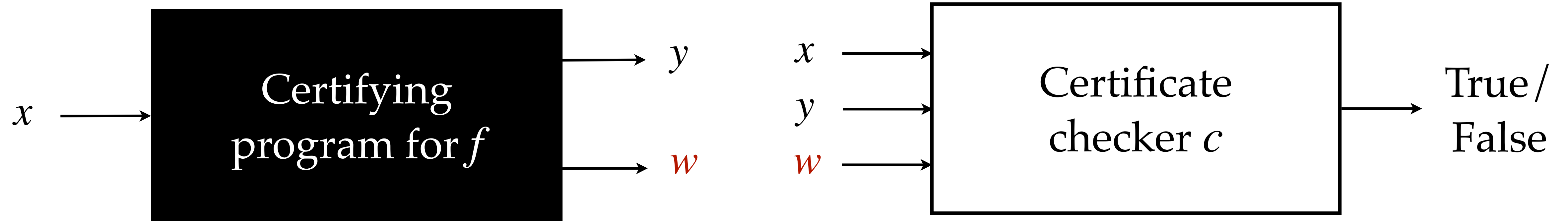


Idea: w is an easy-to-check proof that $y = f(x)$.

Certificates

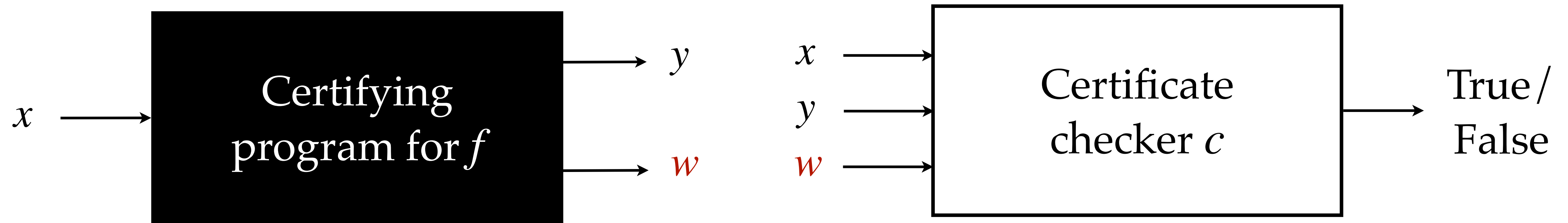


Certificates



Requirements: $\forall x, y:$

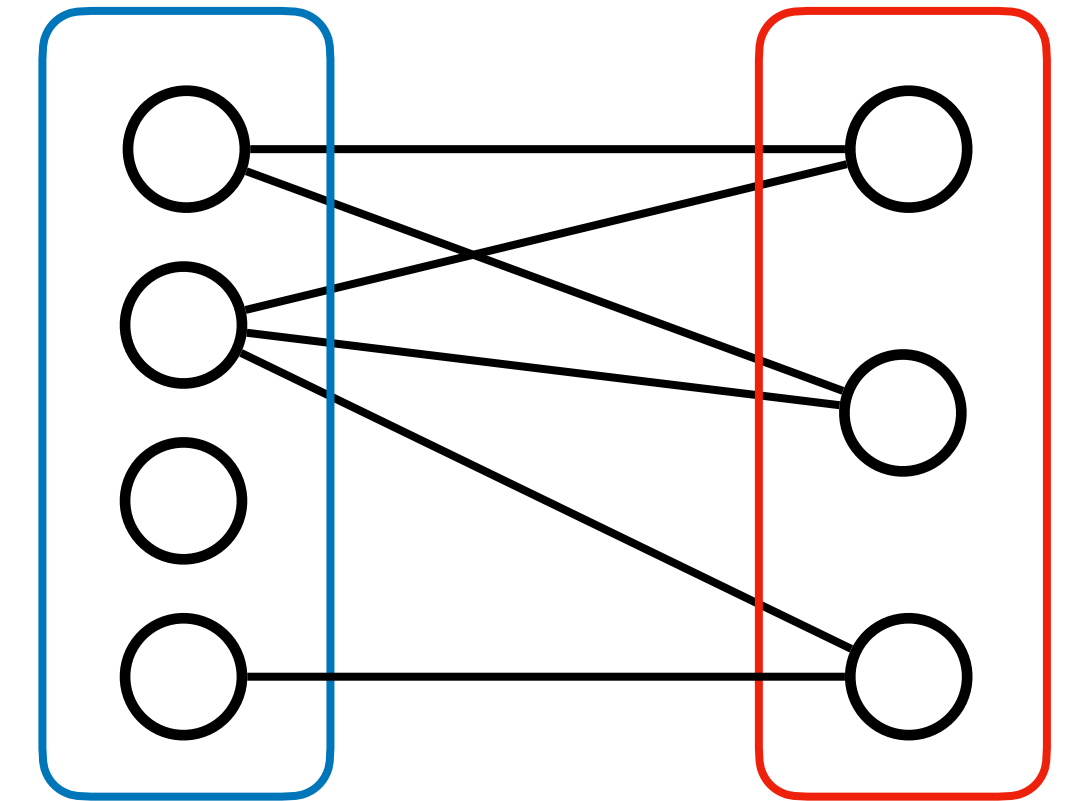
Certificates



Requirements: $\forall x, y$:

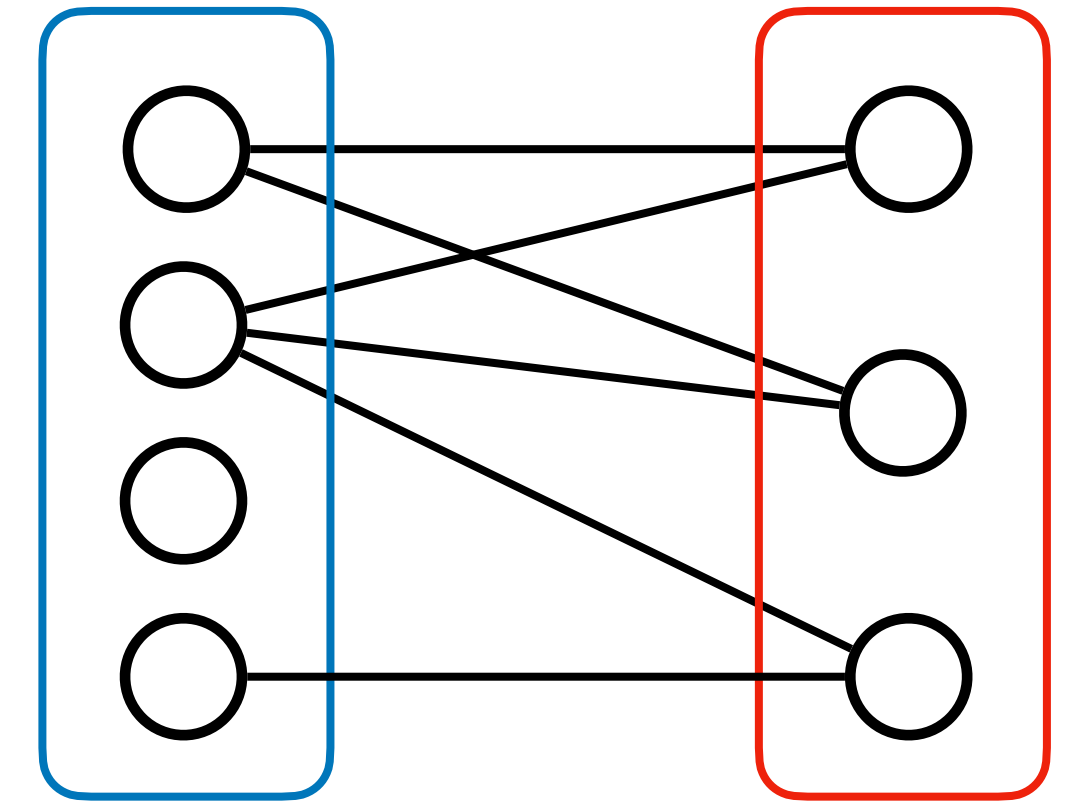
- $(\exists w: c(x, y, w) = \text{True}) \implies f(x) = y$ (*soundness*)

Exercise: Certificates for Bipartite Graphs



Exercise: Certificates for Bipartite Graphs

- **Input:** Undirected graph $G = (V, E)$



Exercise: Certificates for Bipartite Graphs

- **Input:** Undirected graph $G = (V, E)$
- **Output:** *True* if G is bipartite, otherwise *False*.

