University of Waterloo

David R. Cheriton School of Computer Science

Cloud Computing Course

Distributed Model Verification Using Map-Reduce

Presented By

Fathiyeh Faghih

March 2010

University of Waterloo

Project Objective

- Using cloud computing in software verification
- Saving time, especially for big software!

University of Waterloo

Table of Content

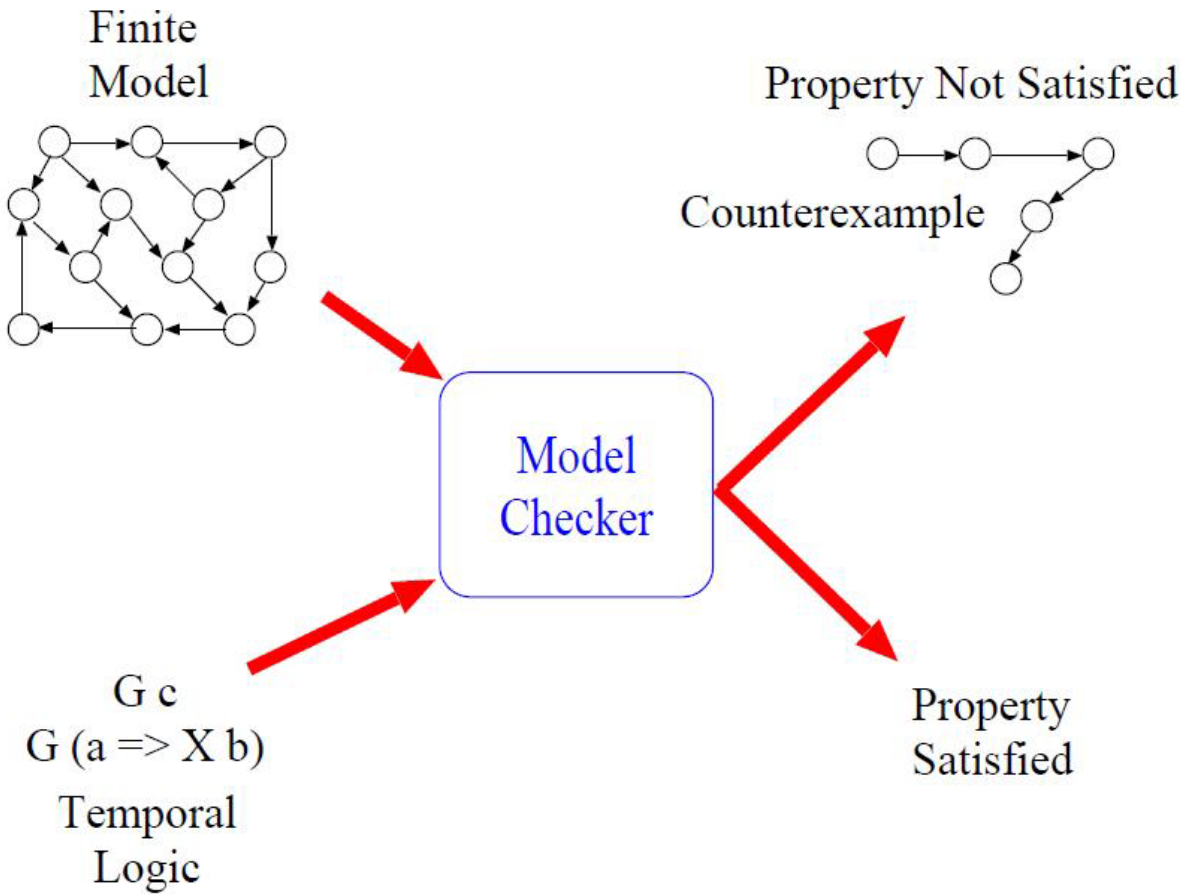
- Background of Certification
- Parallel Certification
- Implementation Details

University of Waterloo

Table of Content

- **Background of Certification**
- Parallel Certification
- Implementation Details

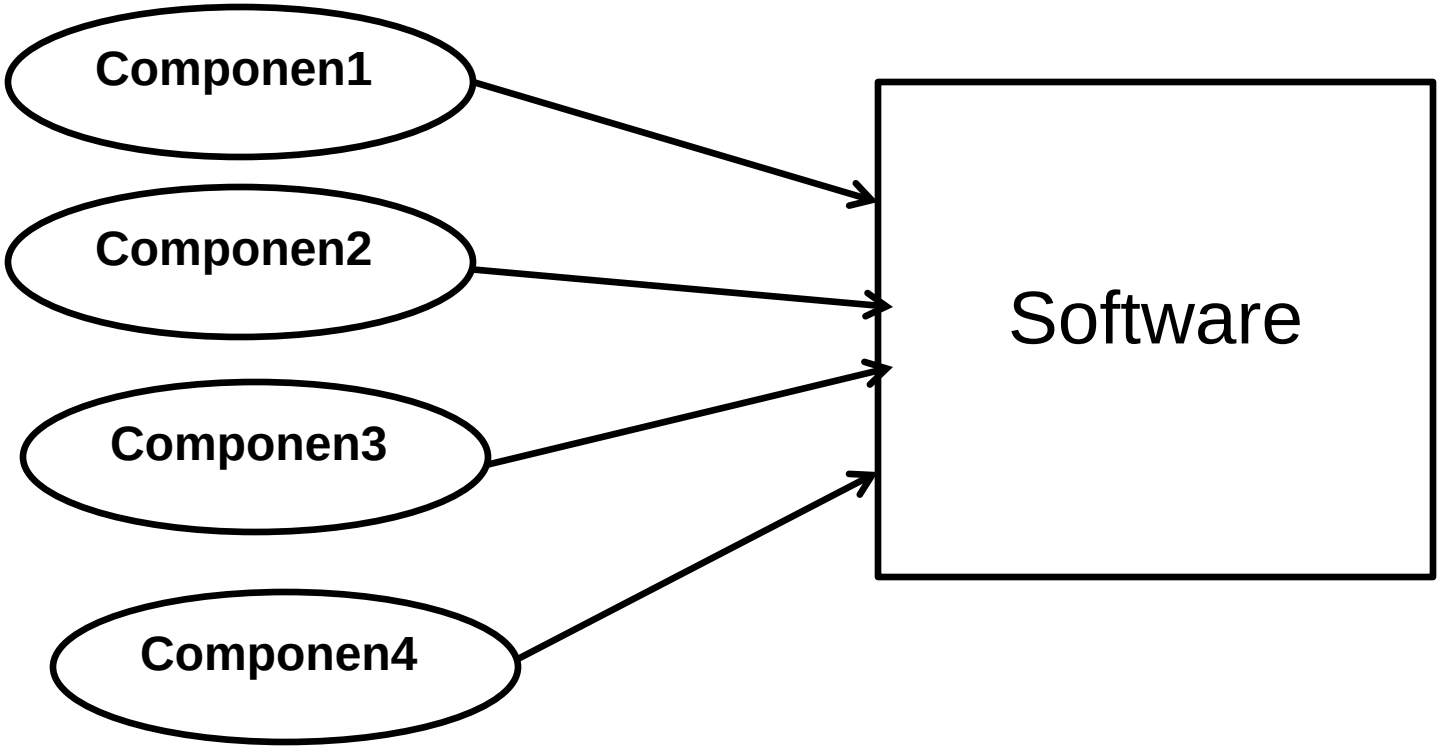
Model Checking



Ref: CS745 Course Notes, Nancy Day

Component-based Software Engineering

- Assembly of pre-existing components



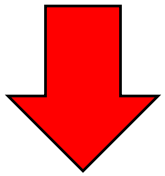
- Components' correctness

Component-based Software Engineering

- Component producer
  - Non-trusted
    - Does it work as advertised?
  - Trusted
    - Assessing additional properties

Search Carrying Code (SCC)

- Help the code consumer to do model checking
- Recording the search path in search scripts



70% saving in the model checking time

Search Carrying Code (SCC)

- Trustful certification
  - Checking additional properties
- Tamper proof certification
  - Correctness of the search script

University of Waterloo

Table of Content

- Background of Certification
- **Parallel Certification**
- Implementation Details

Search Carrying Code

- Parallel model checking
  - Huge number of states
- Known reachability graph
- Statically partitioning a search script

Parallel Certification

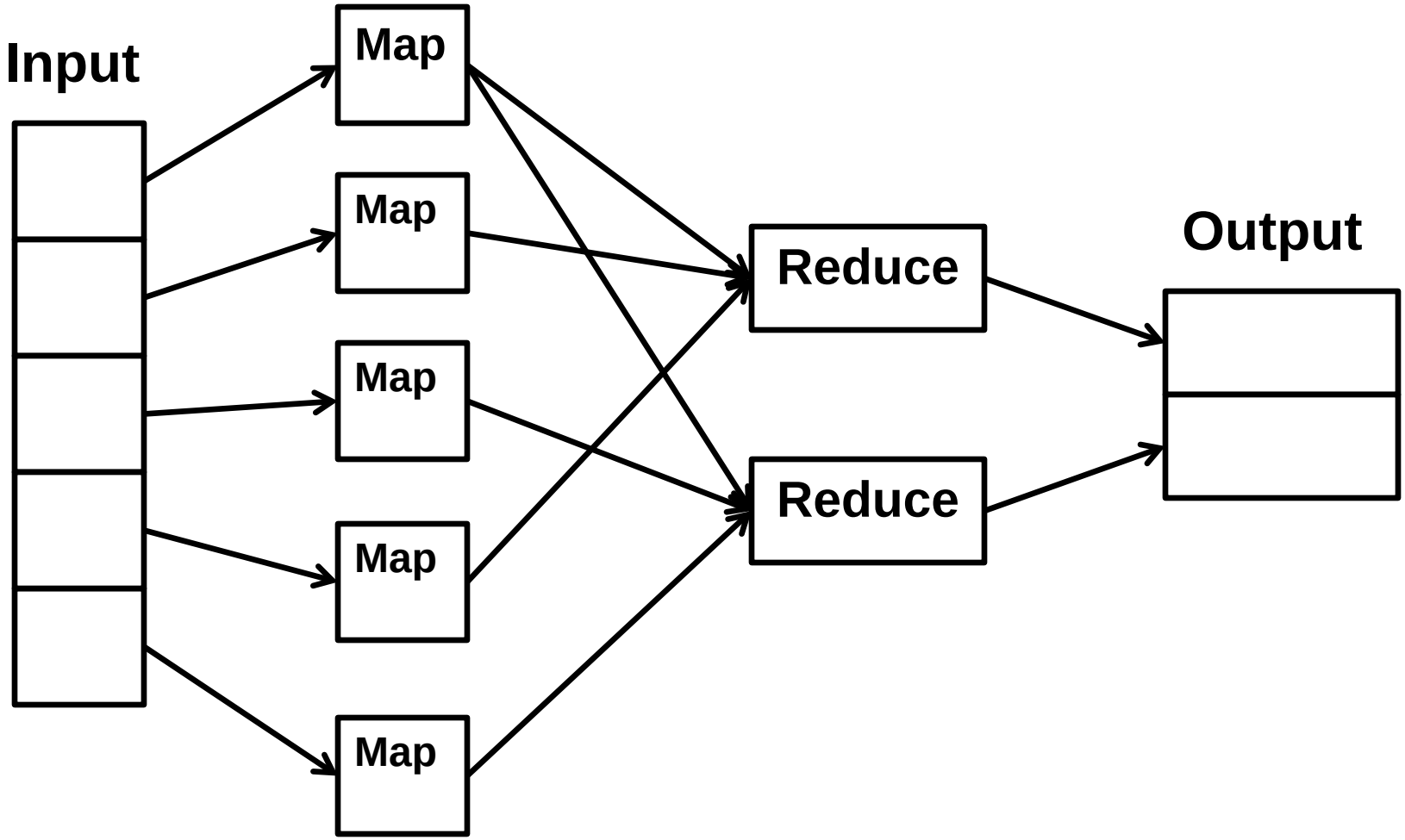
- Trustful
- Tamper proof

Parallel Certification

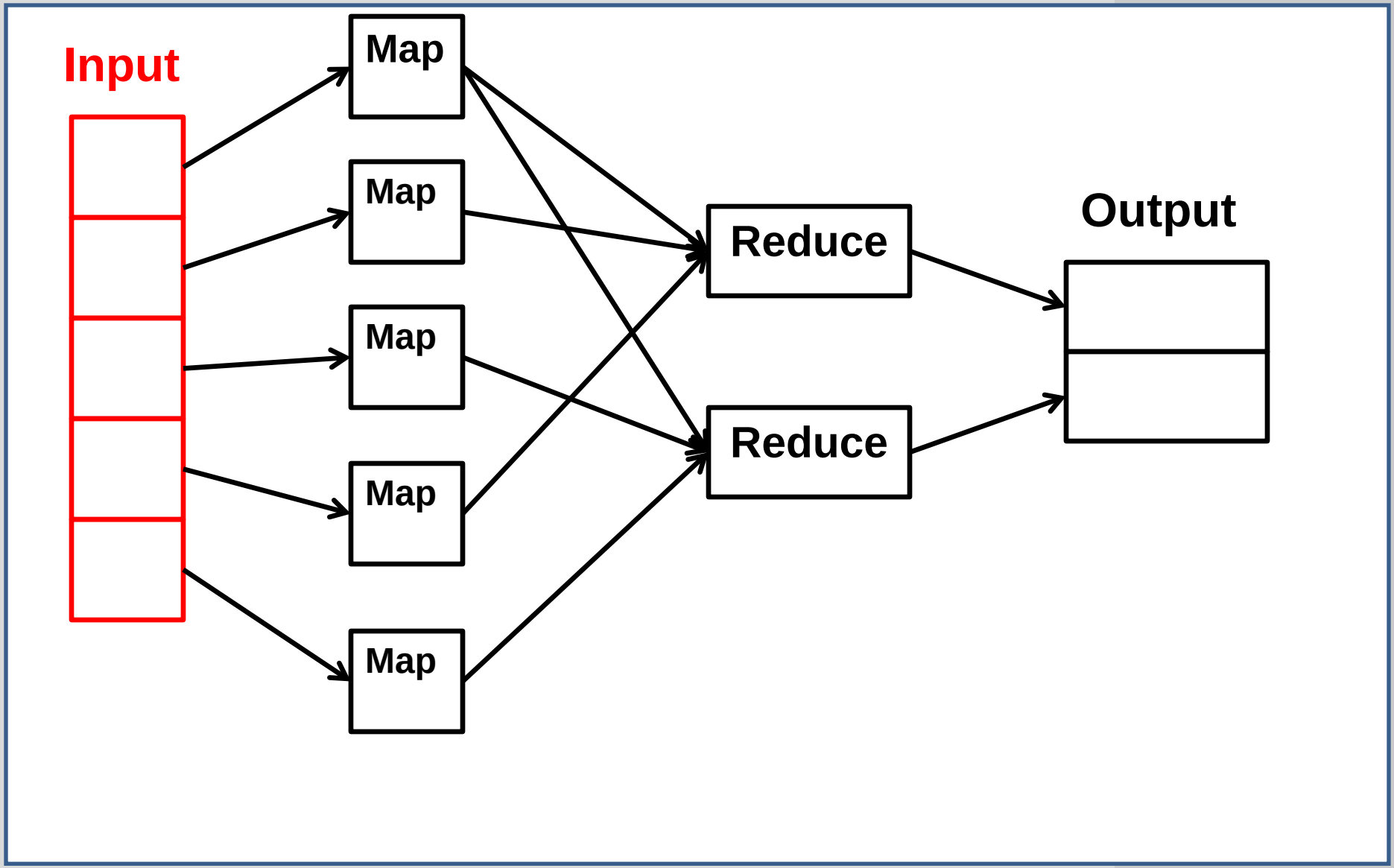
- **Trustful**
- Tamper proof

Parallel Trustful Certification

- Background of Certification
- Parallel Certification
- Implementation Details

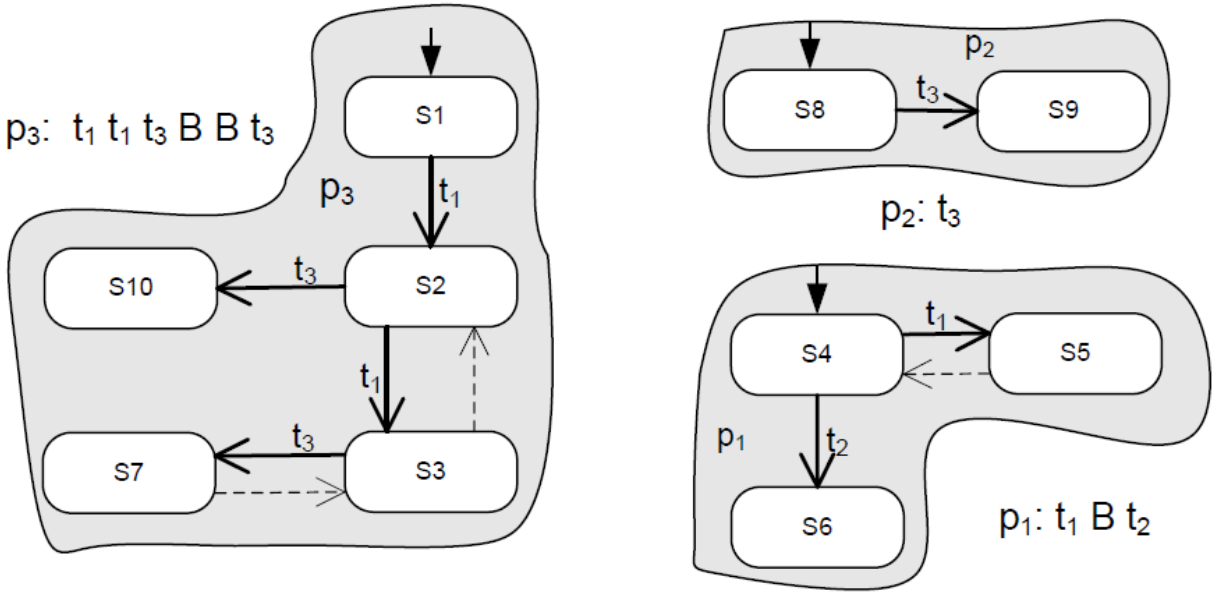


Parallel Trustful Certification

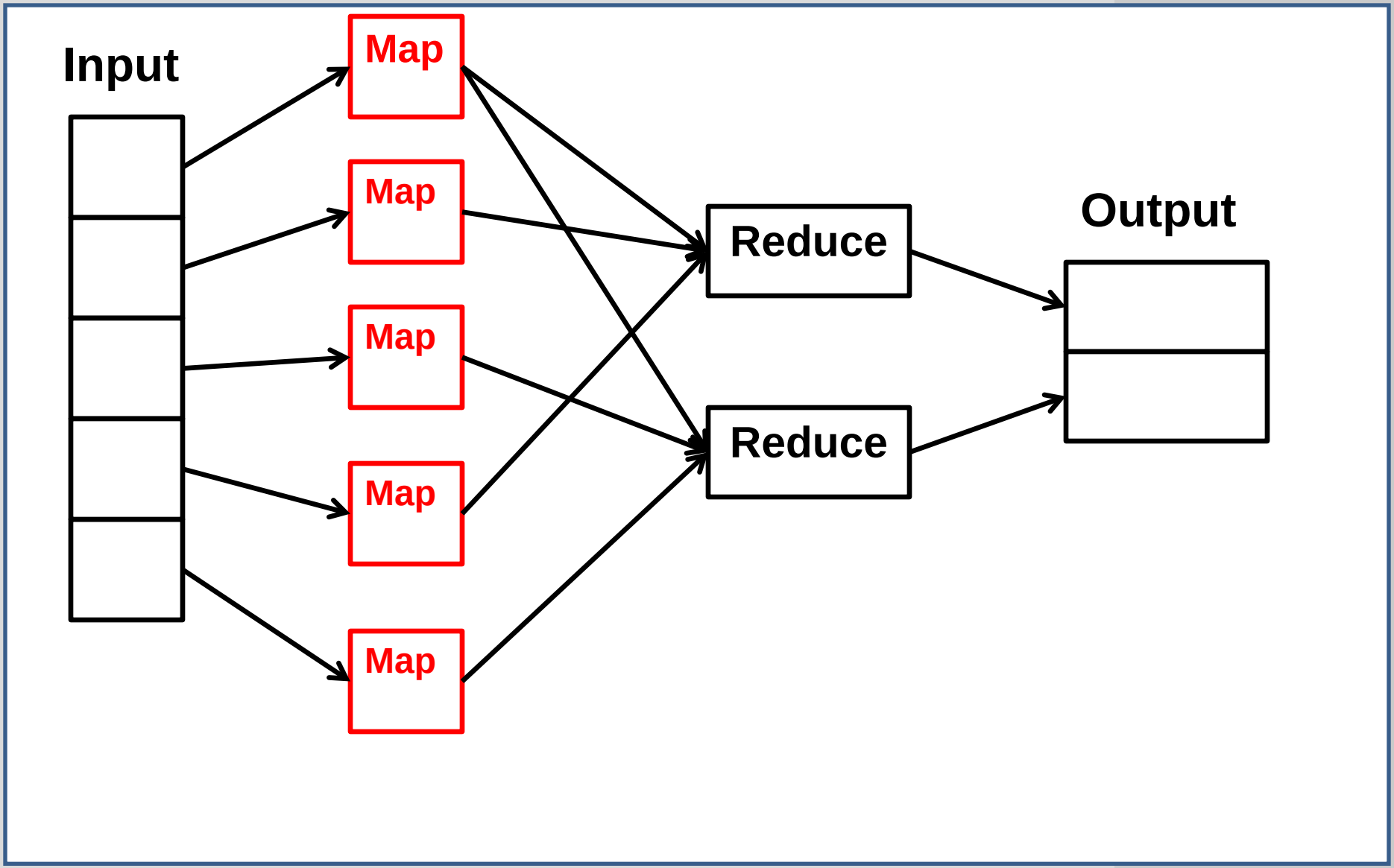


Input

- Partitions of the search script
- Forcing the Map-Reduce not to partition the input files

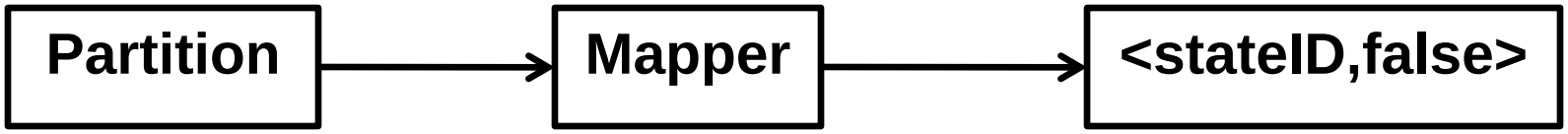


Parallel Trustful Certification

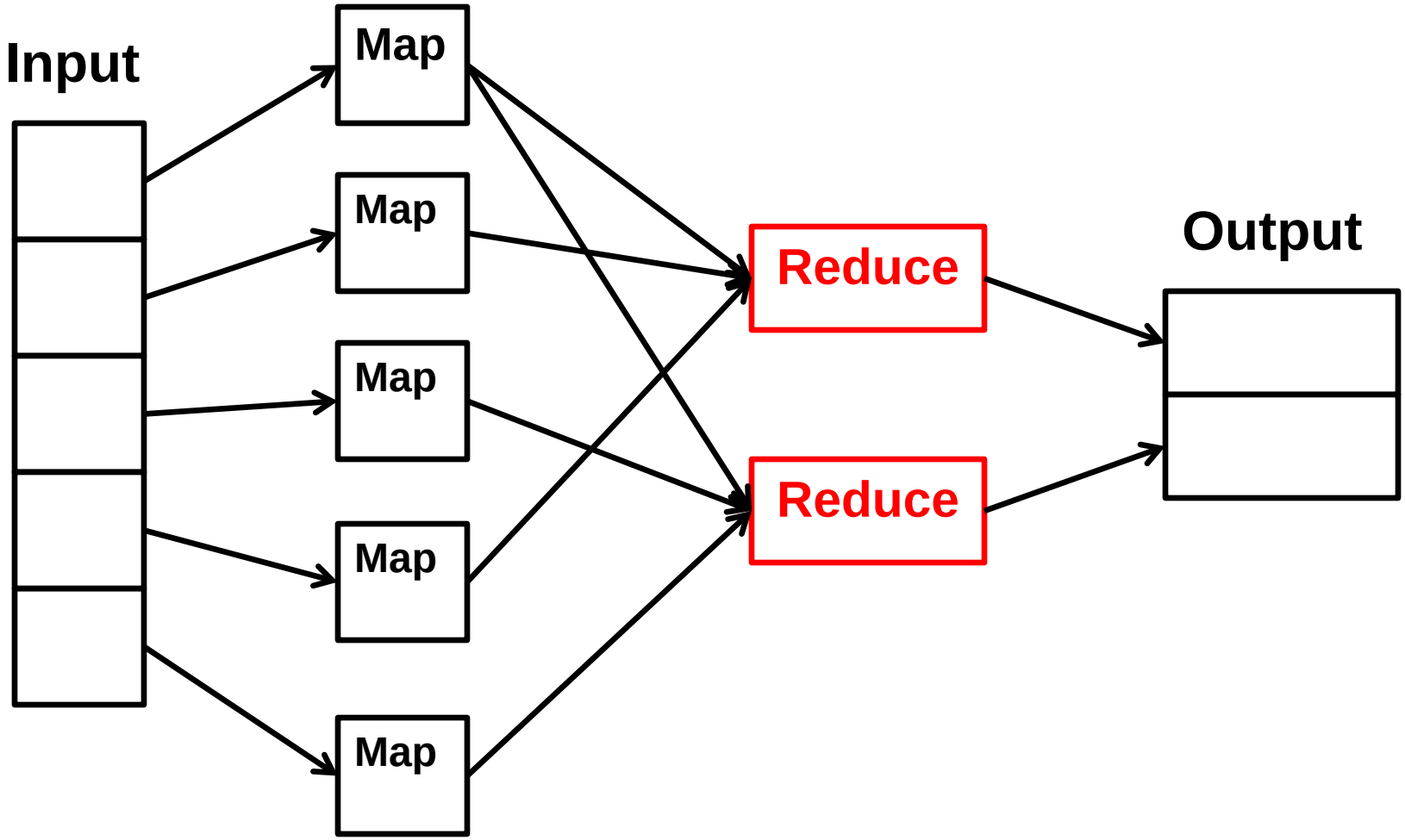


Mapper Function

- Model checking of the partition
- Java Pathfinder



Reducer Function

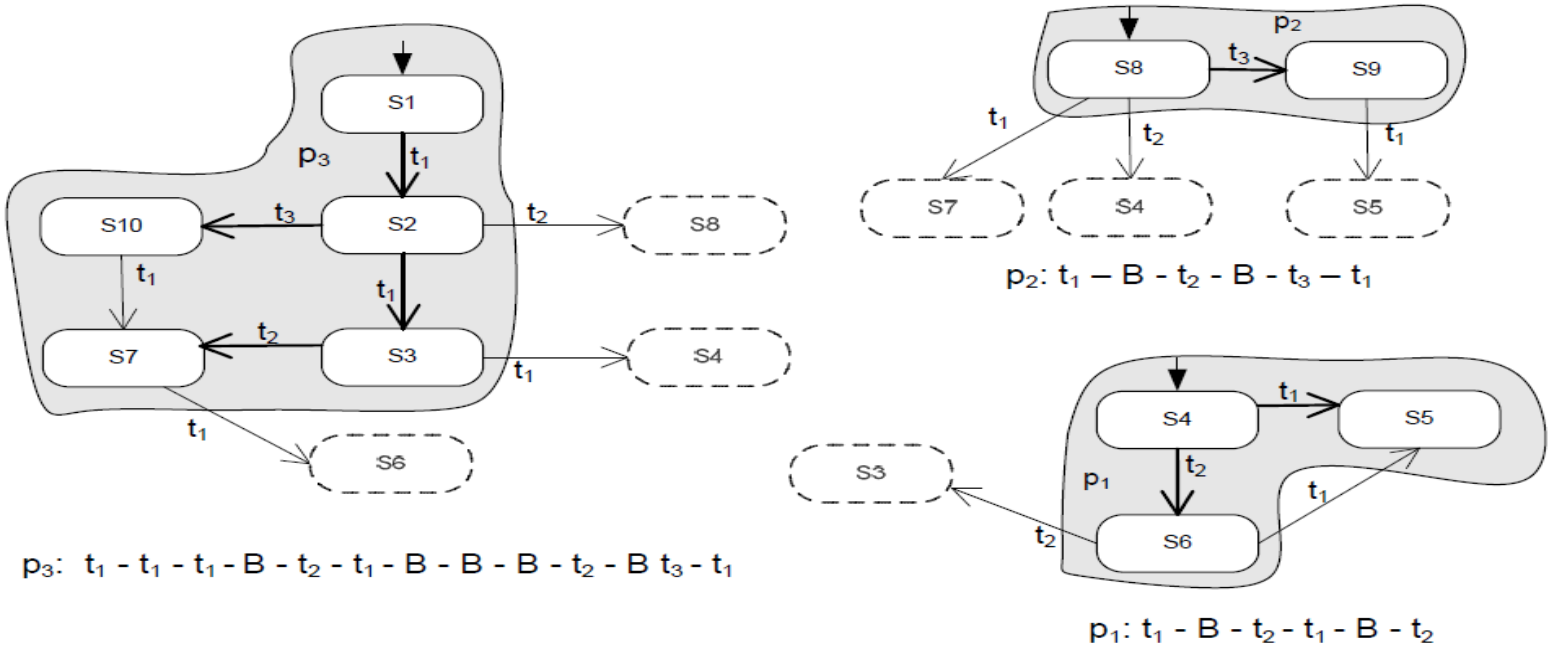


Reducer

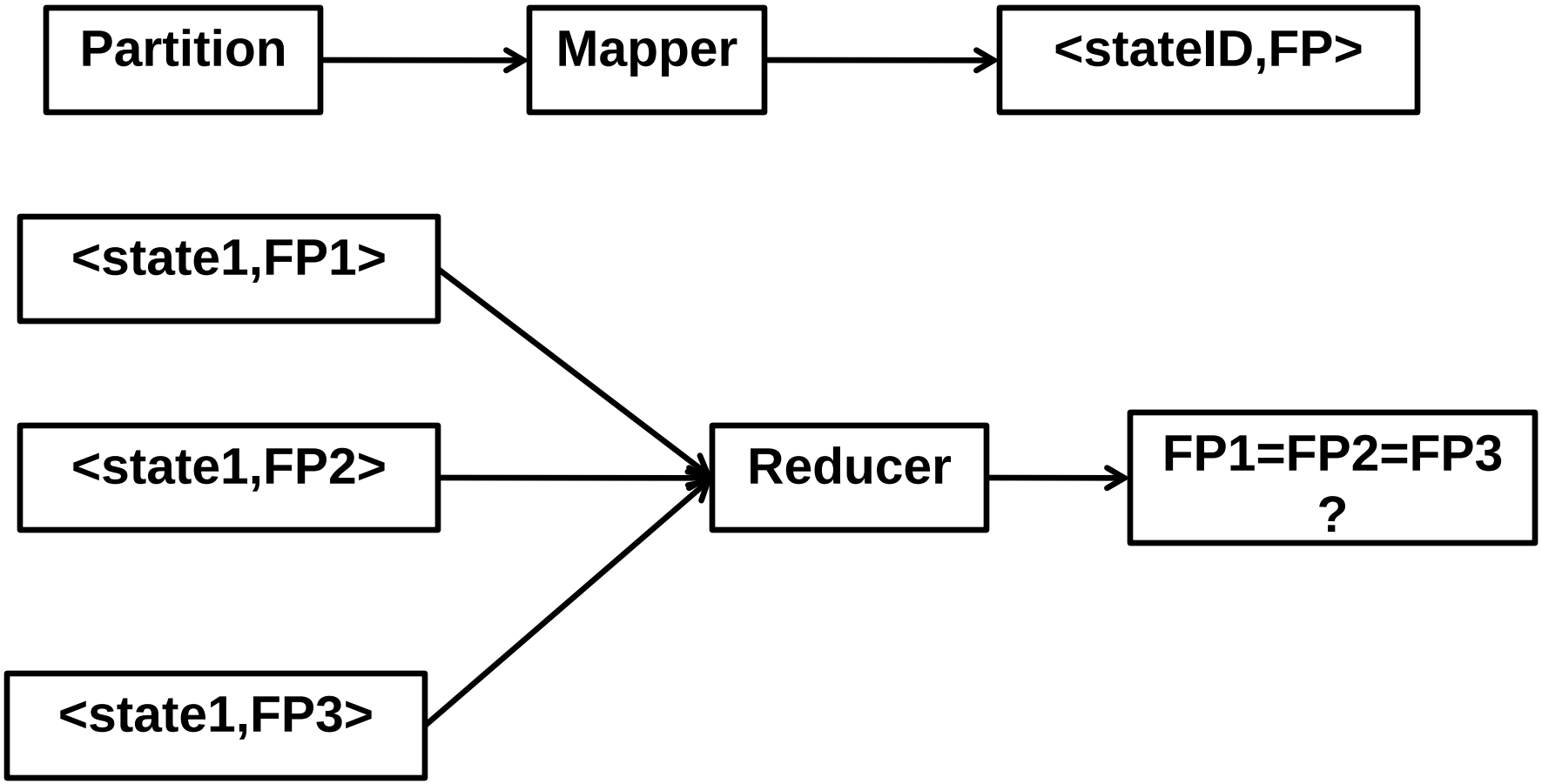
- Checking whether the program is certified or not
- Producing counterexamples

Parallel Certification

- Trustful
- **Tamper proof**



Parallel Tamper Proof Certification



University of Waterloo

Table of Content

- Background of Certification
- Parallel Certification
- **Implementation Details**

Implementation Details

- Karmasphere Studio
  - Plugin to NetBeans IDE
  - *Develop* and *debug* MapReduce jobs on your desktop
  - *Deploy* jobs to remote Hadoop clusters
- Trustful certification
  - Testing the deployment on the desktop

Future Steps

- Deploying the application on Amazon
  - Creating images with JPF installed and configured
- Using the JPF suitable for tamper proof
  - Modifying the reducer

Evaluation

- The time needed to do certification vs. the time needed for model checking
  - Trustful
  - Tamper proof
- Experimenting on different numbers of partitions
  - Optimal number for each number of states?
  - Independent of the shape of the graph?

University of Waterloo