

The Hitchhiker's Guide to *Hyperproperties*

Pre-Course Meeting

Bernd Finkbeiner, Julian Erhard, N. Ege Saraç

July 10, 2026



Spectre and Meltdown



Speculative Execution
Predictions based on **branch**
history

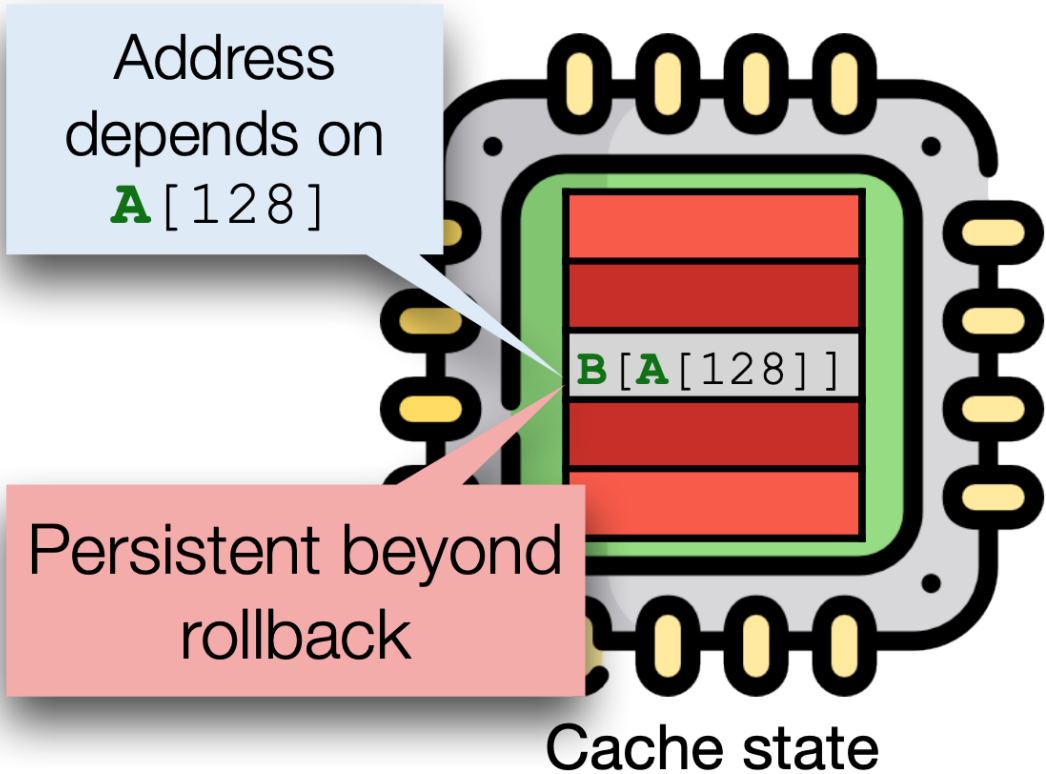
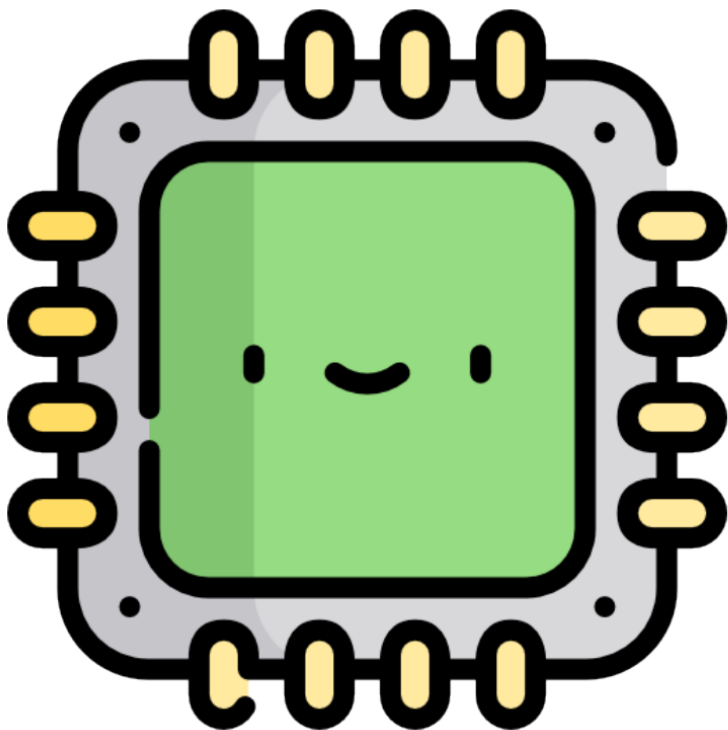
```
if (y < size)  
    temp = B[A[y]]
```

size = 16

A [0]	A [1]	...	A [128]
			key

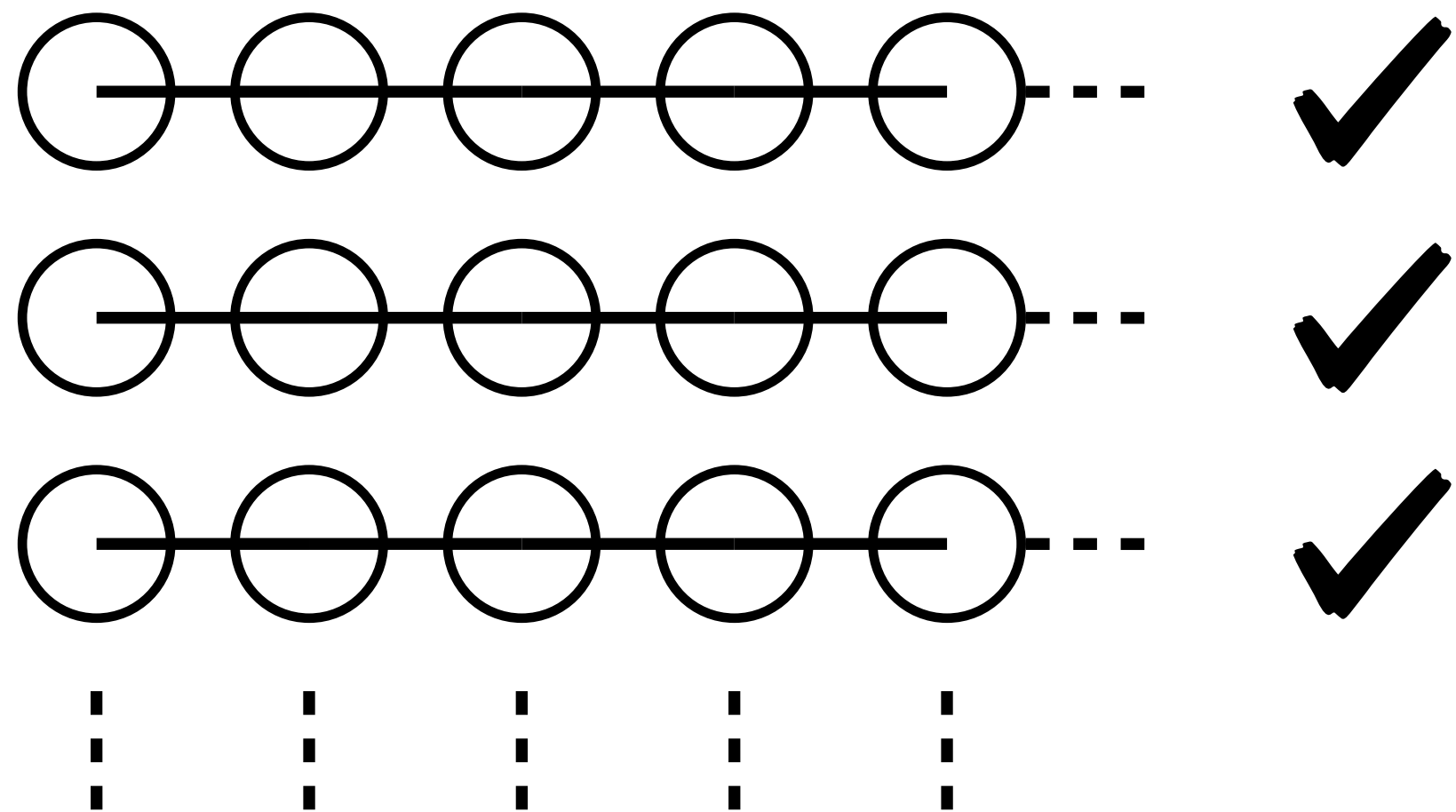
Train: y = 1; y = 2; y = 3;

Attack: y = 128



Hyperproperties

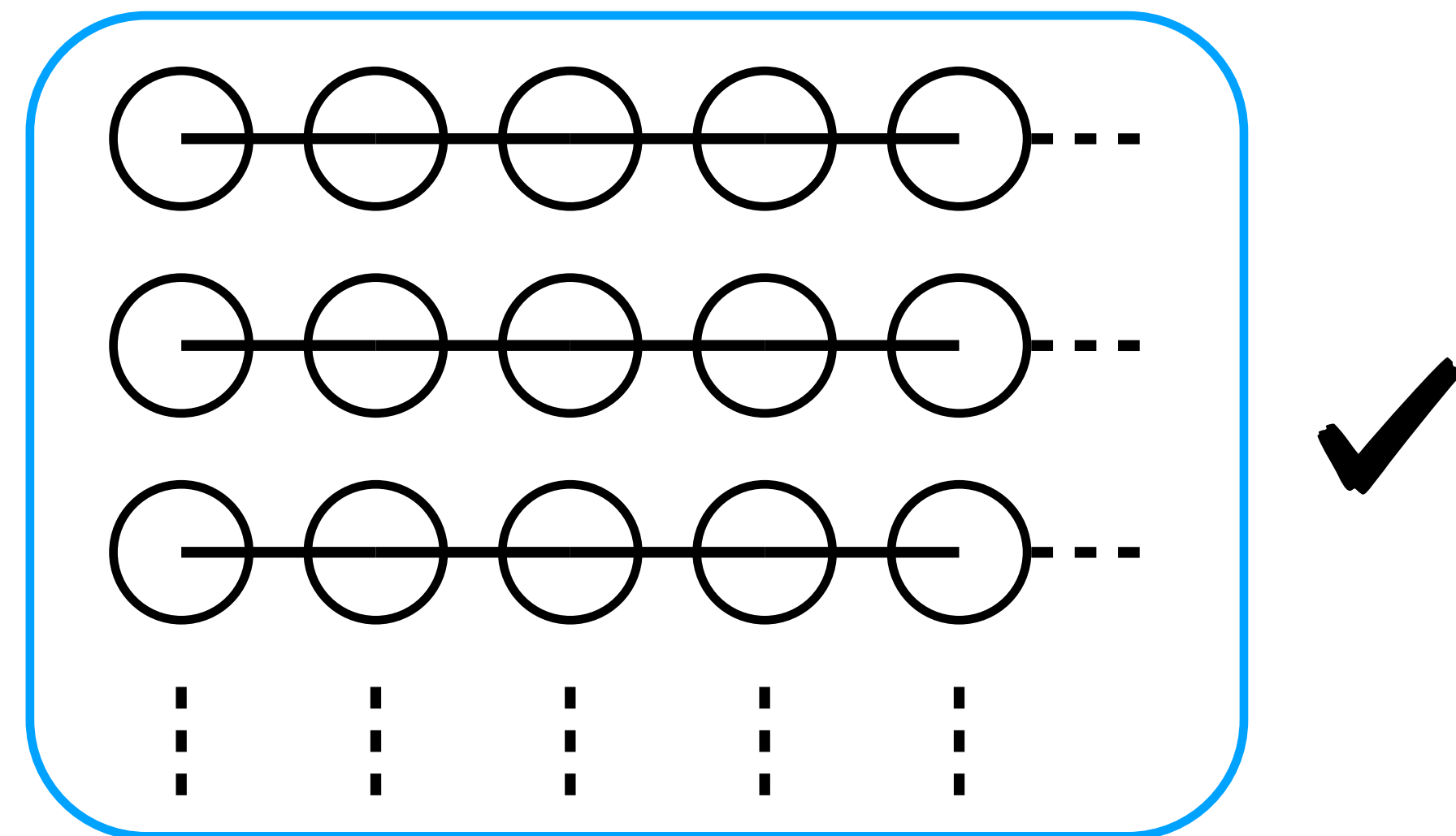
Trace Properties



“A bad state is never reached”

“The lock is always released eventually ”

Hyperproperties



“A high-security input does not impact the output”

Our Team



Bernd Finkbeiner



Julian Erhard



N. Ege Saraç

Seminar Structure

A. Group Phase

- 2 groups of 3-5 students
- Each group presents their group papers, and moderates the following discussion
- All students of the seminar have to read the key paper of each group
- Presentation should not exceed 45 minutes
- Prepare a discussion (~30 min) by, e.g., preparing a few quiz questions

B. Individual Phase

- Individual presentation on your research paper (25 min) and discussion
- Write a summary (~5 pages) on your paper in the context of the seminar

Group Phase

Basics of Information-Flow Control

Secure Information-Flow by Self-Composition

Spectre attacks: Exploiting speculative execution

Hyperproperties (key paper)

Formal Methods 101

Linear Temporal Logic

Algorithmic Methods

Temporal Logics for Hyperproperties (key paper)

Individual Phase

Hyperproperties in Practice

Paper 1 - SPECTECTOR: Principled Detection of Speculative Information Flows

Paper 2 - A Hardware Design Language for Timing-Sensitive Information-Flow Security

Paper 3 - Information Flow Control Based on Program Dependence Graphs

Paper 4 - Runtime Enforcement of Security Policies on Black Box Reactive Programs

Paper 5 - Hyperproperties of Real-Valued Signals

Theory of Hyperproperties

Paper 6 - Cartesian Hoare Logic for Verifying k-Safety Properties

Paper 7 - Epistemic Temporal Logic for Information Flow Security

Paper 8 - Algorithms for Model Checking HyperLTL and HyperCTL*

Paper 9 - The Hierarchy of Hyperlogics

Paper 10 - Smart Contract Synthesis Modulo Hyperproperties

What We Expect

A. Group Phase

- Read your group papers and the key papers of both groups
- Collaborate with your group on preparing and giving the group talk (get feedback from your advisor)

B. Individual Phase

- Read your individual paper, prepare a talk (get feedback from your advisor)
- Participate in the discussions
- Write a summary

Seminar Schedule

- Kick-off meeting – October 16 (Fri), 15:00
- Topic distribution – Second week of lectures
- Group presentations – November 12-13 (Thr-Fri), 14:00-16:00
- Individual presentations – February 4-5 (Thr-Fri), 14:00-18:00
- Individual summaries – In February, after individual presentations

Questions?

