Relaxed Systems

Current State + Future Plans

Ben Sinner

Thibaut Pérami

Jean Pichon-Pharabod

Ohad Kammar

Christopher Pulte

Peter Sewell

Chung-Kil Hur

FOWM @ CAM

- pKVM verification (c.f. PriSC keynote)

FOWM @ Cam

- pKVM verification (c.f. PriSC keynote)
- Arm Semantics

FOwM @ Cam

- pKVM verification
  (c.f. PriSC keynote)

- Arm Semantics

- Reasoning tools
  (c.f AxSL @ PuPL)

Protected KVM

Production Hypervisor (Android 14+)

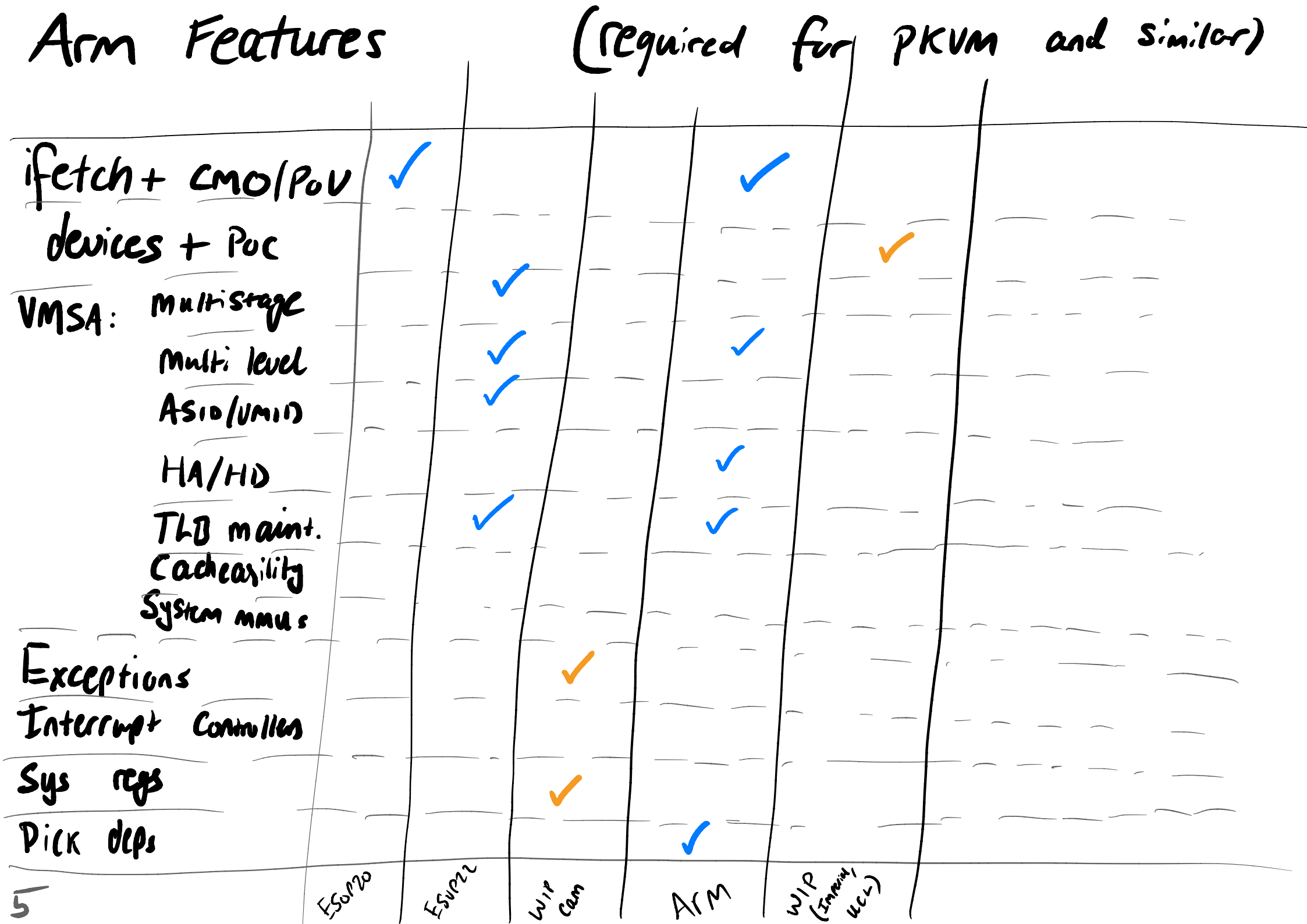
Google

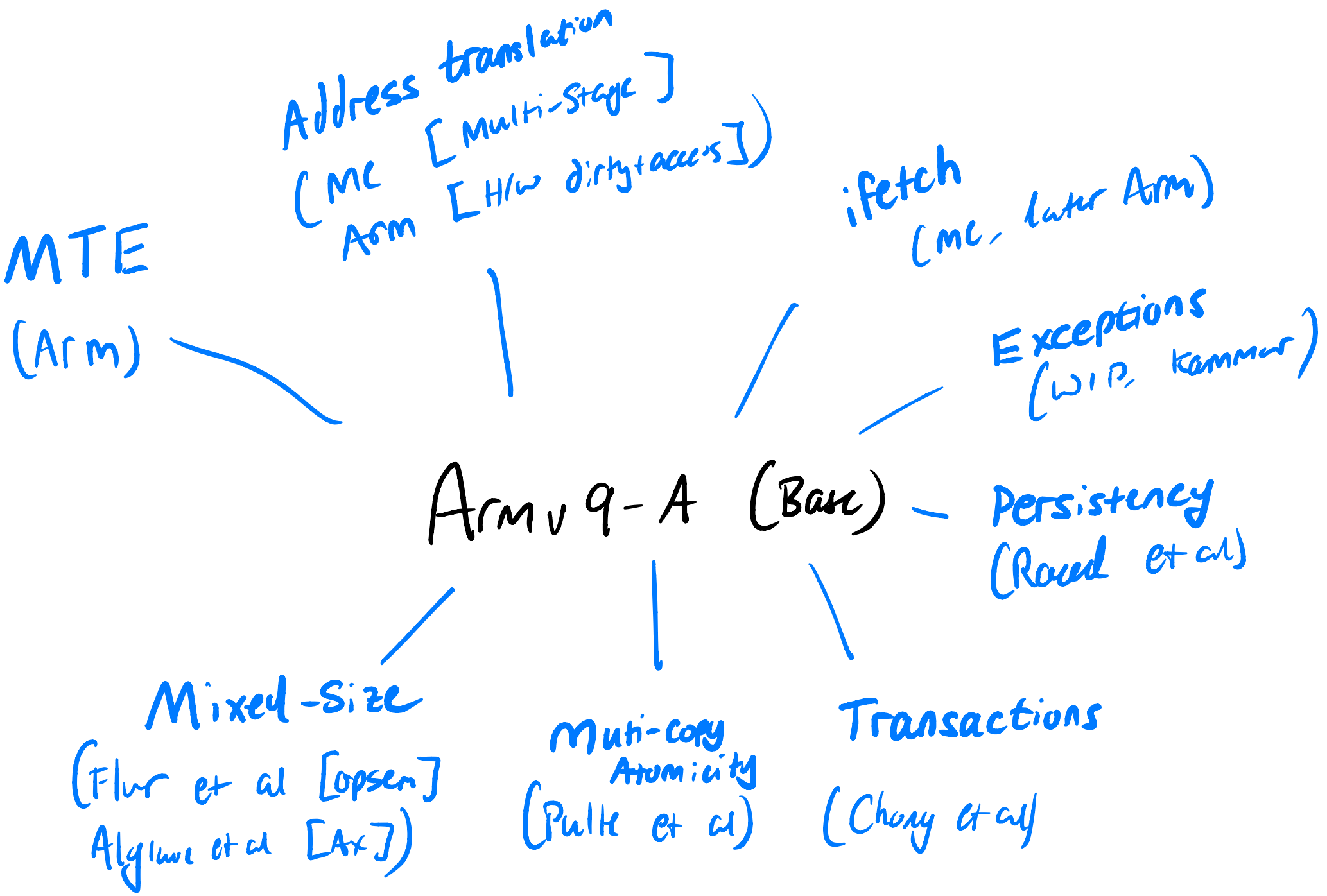
Protected KVM

Plan: verify security properties w.r.t. relaxed Arm semantics

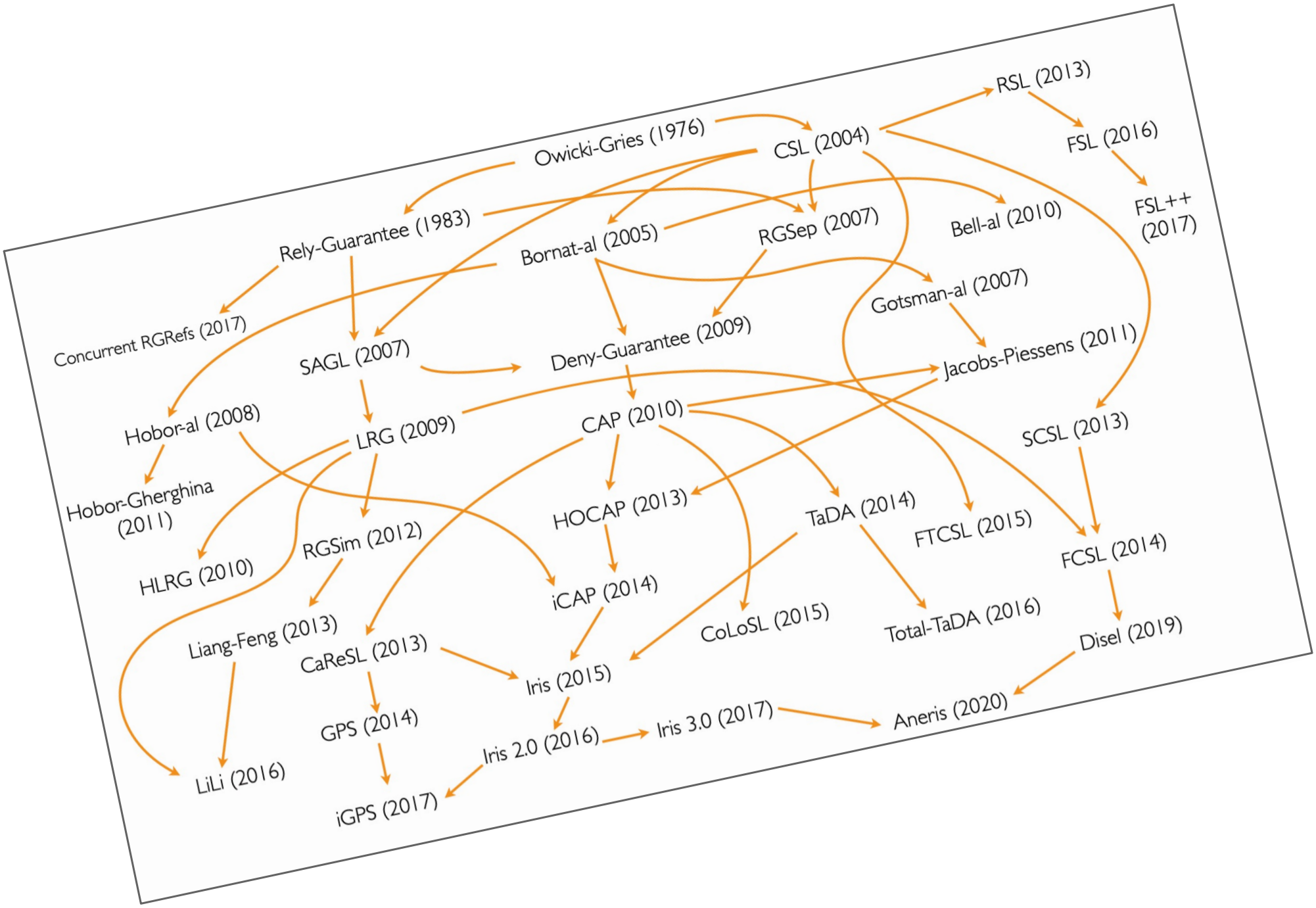
Armv9-A

Arm Features (required for pKVM and similar)




Address translation
(ME [Multi-Stage]
Arm [H/w dirty+access])
MTE
(Arm)
ifetch
(ME, later Arm)
Exceptions
(WIP, Kammar)
Armv9-A (Base)
Persistency
(Raad et al)
Mixed-Size
(Flur et al [Opsem]
Alglave et al [Ax])
Multi-copy Atomicity
(Pulte et al)
Transactions
(Chong et al)

Reasoning about Software



Credit: Ilya Sergey

Program Logics and refinement...

By Abstracting Language

Reasoning about Software

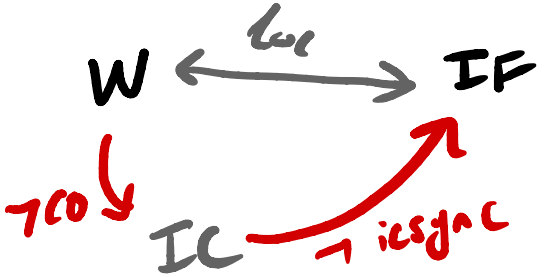
Model Directed

Abstracting away Complexity:

Data

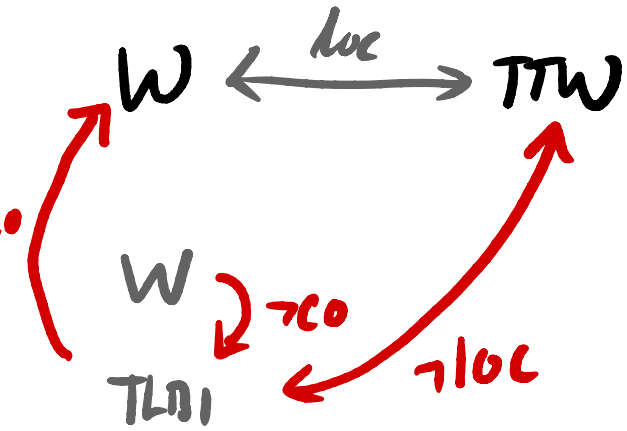
"DRF"

ifetch



"bad ifetch"

VM



"BBM Violation"

Simplified Model

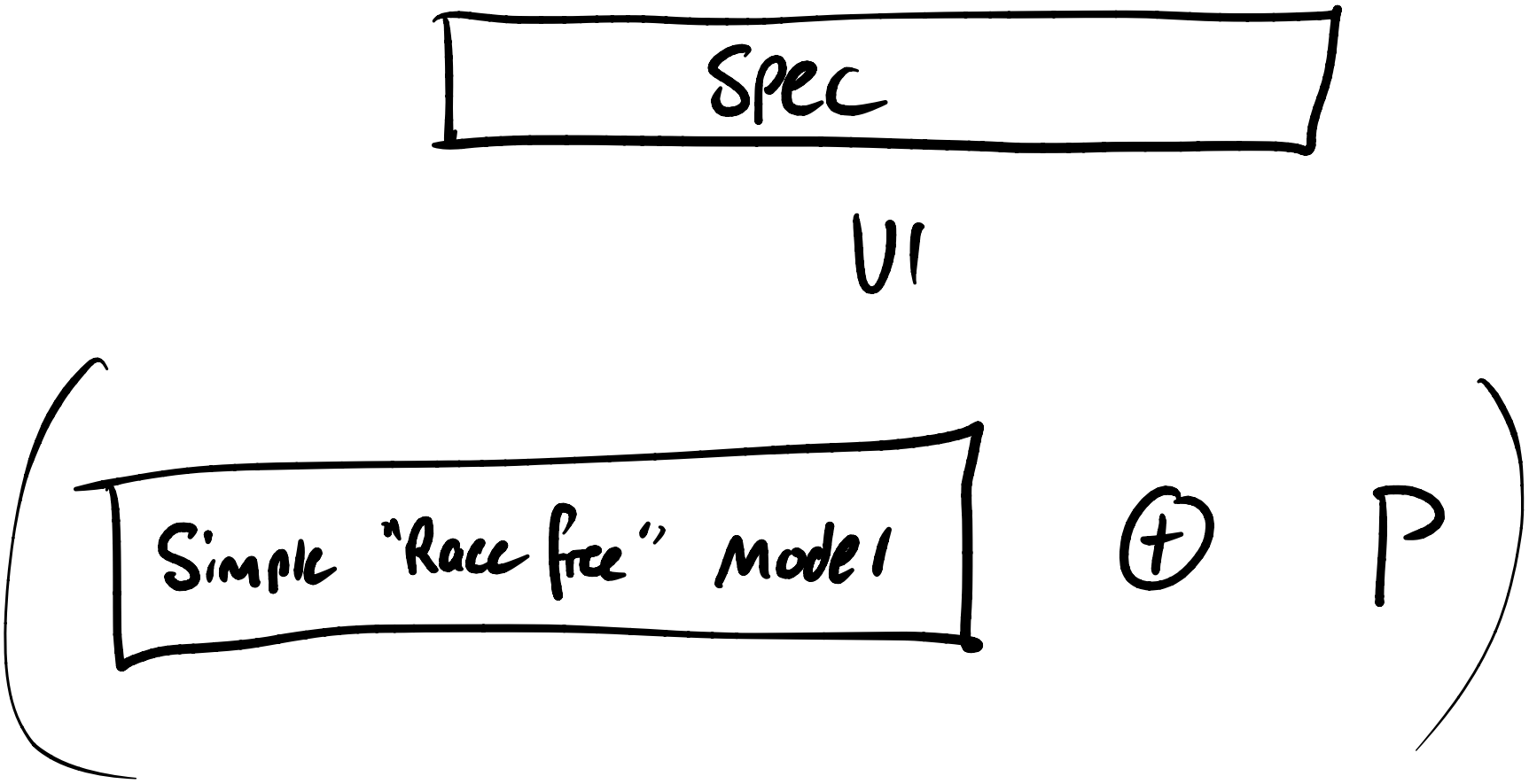
Simple "Race free" Model

VI

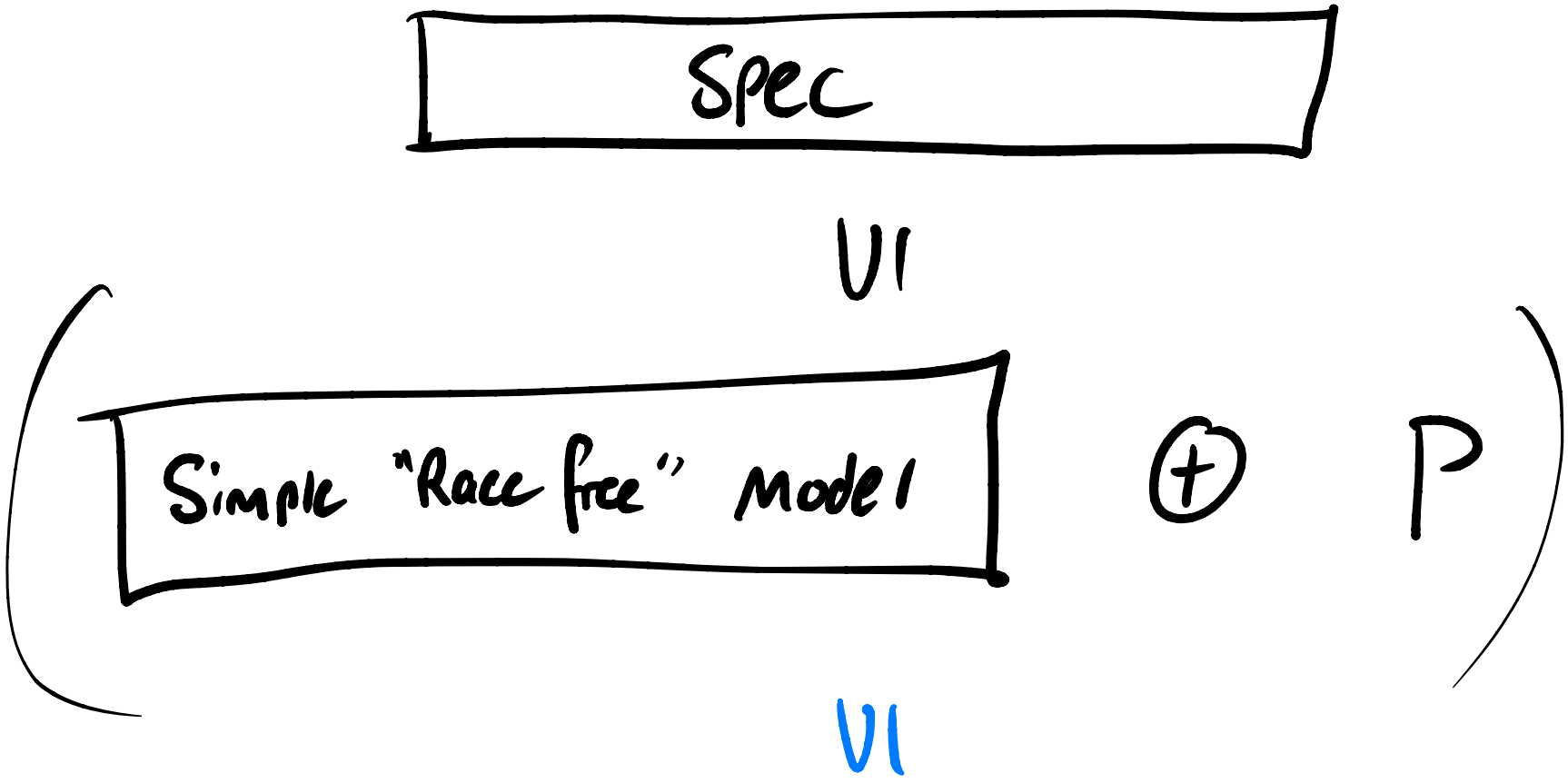
Armv9-A

Simplified Model

Simplified Model



Simplified Model



Racy Programs?

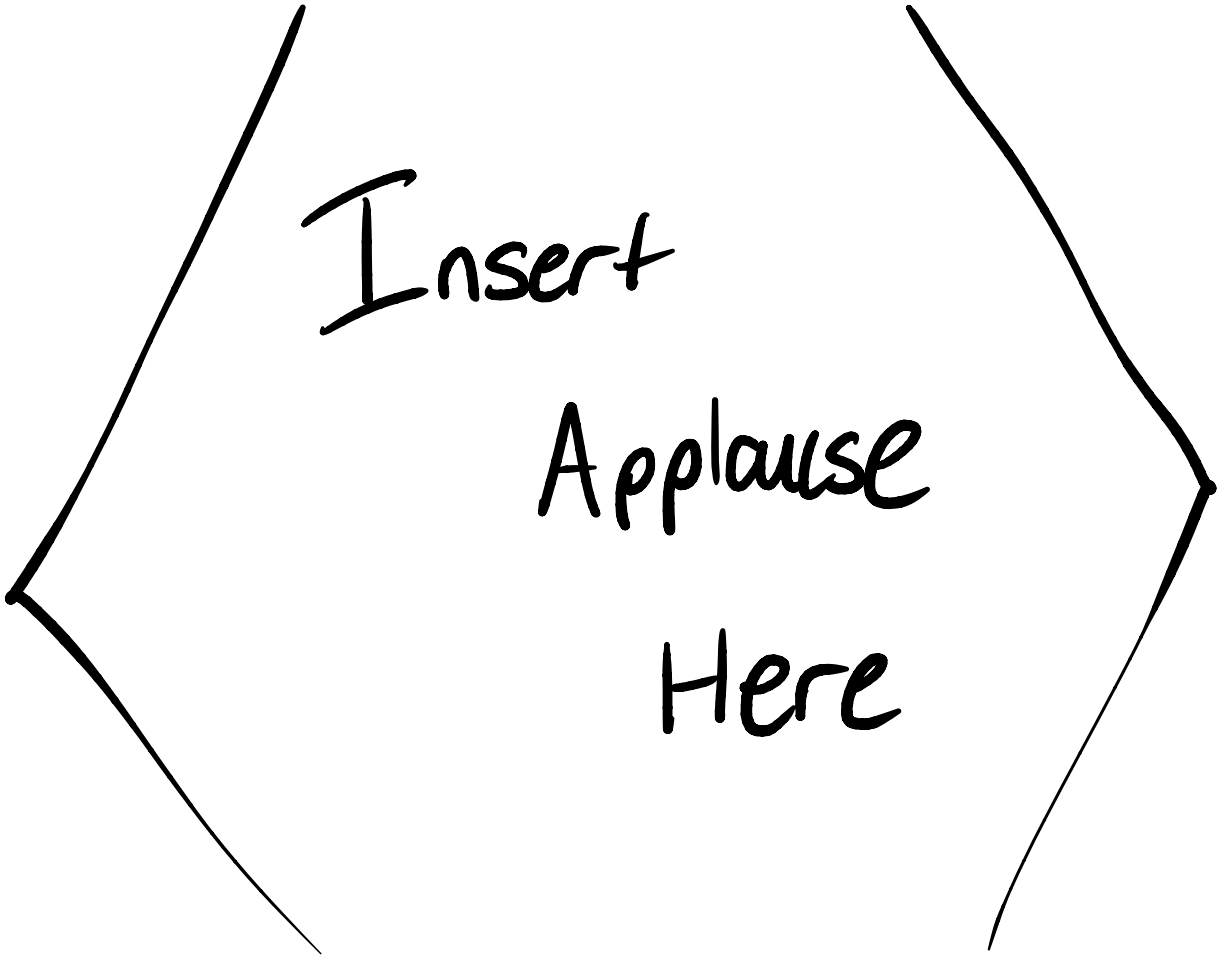
AxSL

Hammond, Lin et al
POPL '24

No

Conclusion

... yet


Insert
Applause
Here