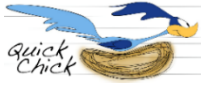
Formally Verified Security

1. Security Goal
2. Enforcement
3. Formal Validation

ROCQ



Secure compilation against Spectre side-channel attacks

SPECTRE

1. **Relative security**: speculation doesn't cause extra leaks
2. **Flexible Speculative Load Hardening (SLH), Intel CET, ...**
3. ROCQ **proofs** in simplified settings [CSF'25, CSF'26]
3. **Property-based testing LLVM SLH** against **x86 HW-SW contract**

Team: Jonathan, Yonghyun, Julay, Yan, ...

Group:

- **Cătălin Hriţcu** (Tenured Faculty)
- **Abigail Pribisova** (PhD student)
- **Cezar Andrici** (PhD student)
- **Jonathan Baumann** (PhD student)
- **Yonghyun Kim** (PostDoc)
- **Yan Farba** (Student Assistant)

F* proof-oriented programming language

- **Most Influential POPL'16 Paper Award**
  + key idea now behind the main Lean verification frameworks
- **Secure compilation of F* code, linked with unverified code**
  + machine-checked proofs using F* and Claude
  + [..., POPL'24, ICFP'25, ICFP'26]
- **Dijkstra monads for incorrectness** (i.e. finding correct bugs)

Team: Cezar, Abigail, ...