Keystone Annual Review

Confidential Computing Consortium

Dayeol Lee dayeol@berkeley.edu

University of California, Berkeley

Keystone

CONFIDENTIAL COMPUTING CONSORTIUM

Goals of the Project

- ❑ Enable TEE on (almost) **all RISC-V processors**
  - Follow RISC-V standard ISA
  - Standard TEE specification for various RISC-V sub-ISA
- ❑ Make TEE **easy to customize** depending on needs
  - Base implementation vs. platform-specific implementation
  - Reuse the implementation across multiple platforms
- ❑ **Reduce the cost** of building TEE
  - Reduce hardware integration cost
  - Reduce verification cost
  - Integrate with existing software tools

Summary of 2021

- Improved portability
  - New platforms: MPFS, CVA6, Renode
- Code quality
- New subprojects
- More collaboration
  - Fully open-source hardware in RIOS Lab
- Documentation & examples
  - Attestation tutorial, Redis, Sqlite3
- Increased academic users

New Platforms Available

- Renode (by AntMicro)
  - https://renode.io/
  - Software framework for hardware (e.g., SoC) simulation
- MPFS (by Microchip)
  - https://microchip.com/polarfire
  - Polarfire FPGA board with RISC-V processors
- CVA6 (by OpenHW group)
  - https://github.com/openhwgroup/cva6
  - Open-source RISC-V CPU (6-stage, in-order)

Code Quality

- Refactoring
  - Massive refactoring on Keystone SDK
  - Supporting both RV32 and RV64
  - Auto formatting & format checking via clang-format and cpplint
- CI/CD --- Circle CI
  - Dockerfile and pre-built docker image
  - Adding unit tests

New Subprojects (ongoing)

Trusted Loader and Dynamic Library
Cathy Lu, Anay Wadhera

Improving Measured Boot and Attestation
Rohit Mittal

Scalable Memory Isolation with RISC-V H-extension
Aniruddha Alawani

Preventing Side-Channel Attacks on Dynamic Libraries
Cathy Lu

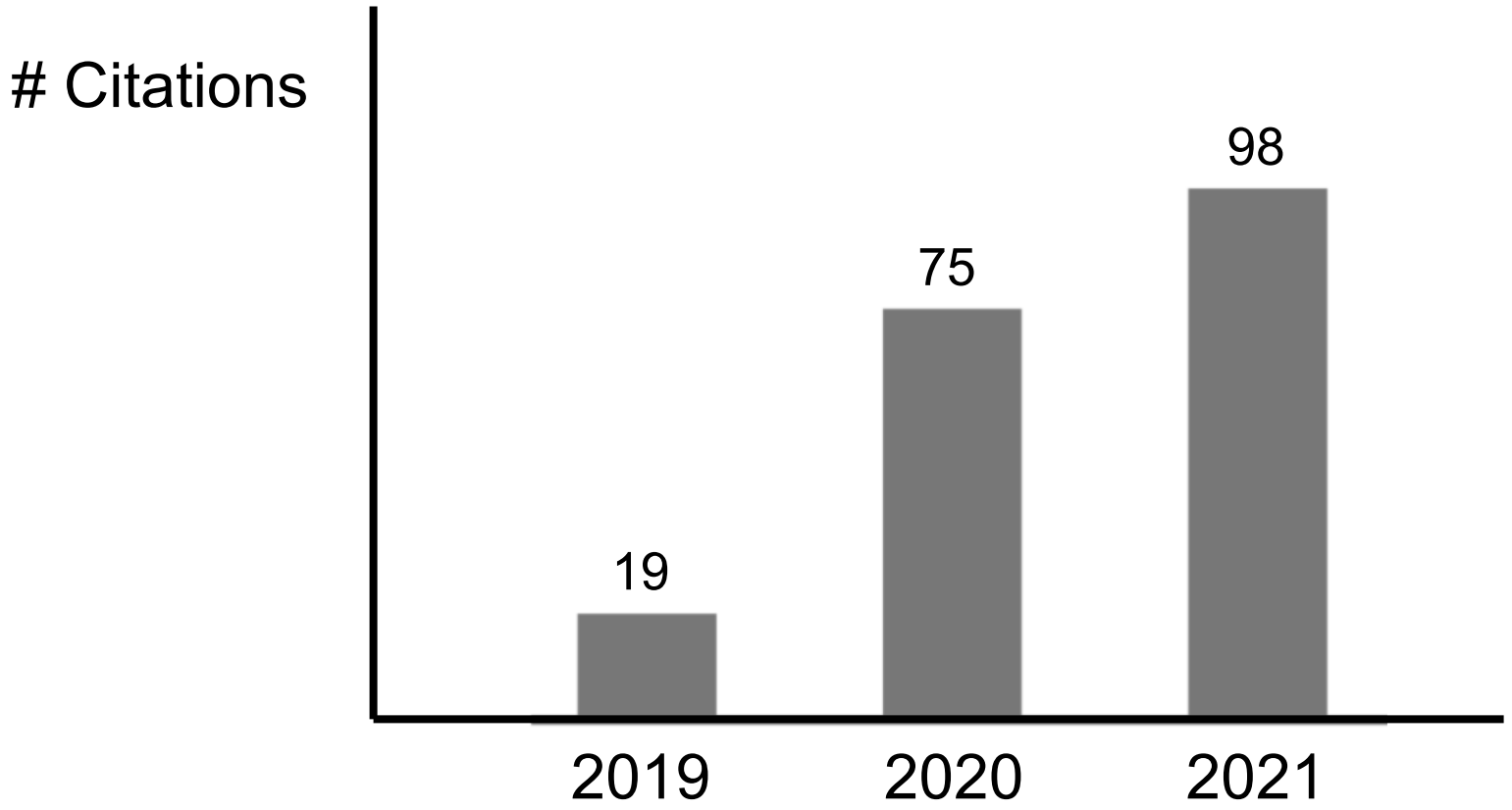
Collaboration on Hardware (ongoing)

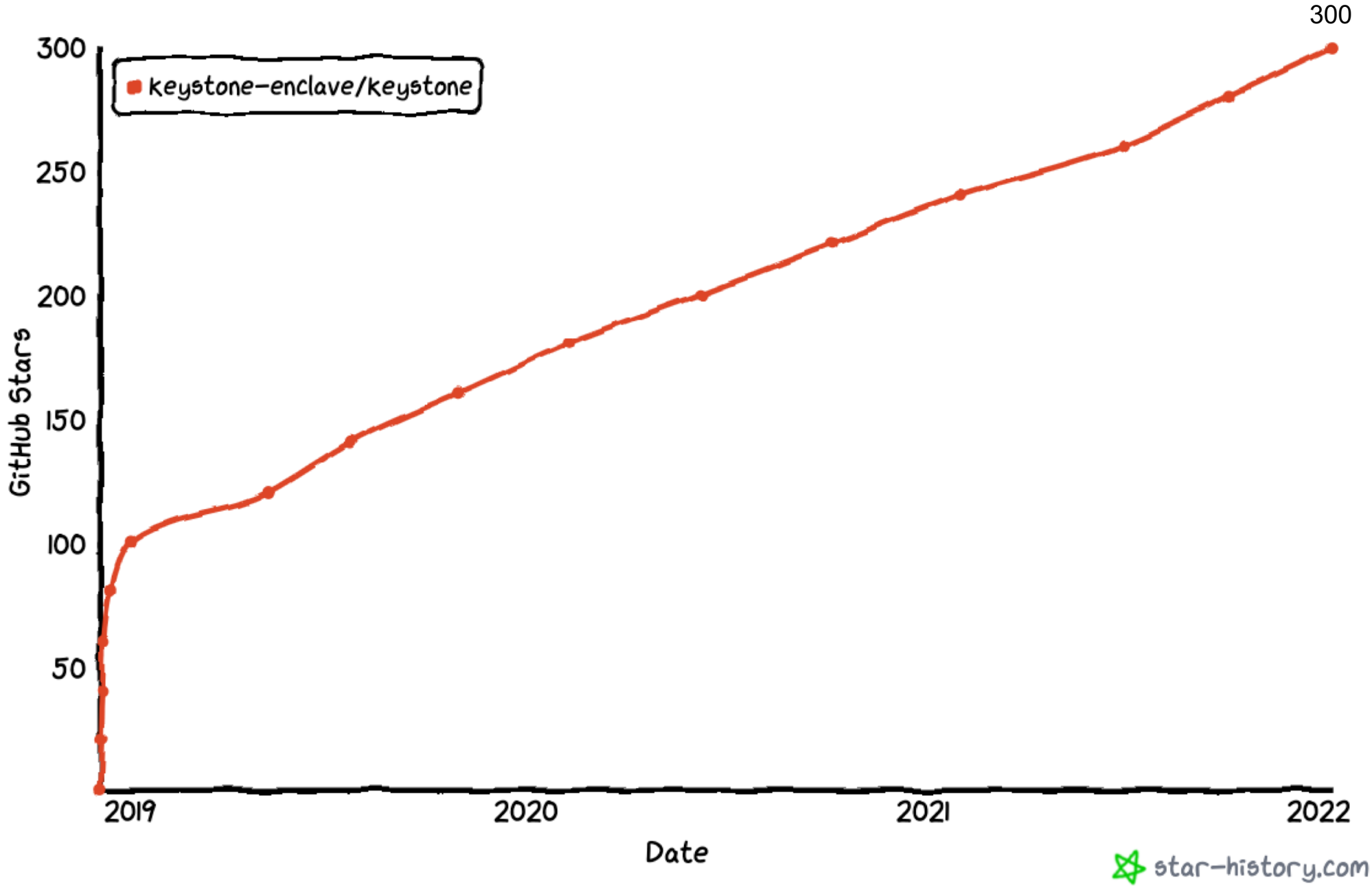
- Fully Open-Source HW project (PicoRio) from RIOS Lab
  - https://rioslab.org/
  - ”fully” means not just core RTL, but all the peripherals including the IPs (potentially also the memory controller)
  - Planning to tape out by the end of 2022

Documentation & Examples

- Attestation Tutorial
  - http://docs.keystone-enclave.org/en/dev/Getting-Started/Tutorials/Remote-Attestation.html
- Redis database
  - C/C++, statically compiled, in-memory
- Sqlite3 database
  - C/C++, statically compiled, in-memory

Increased Academic Users




300
keystone-enclave/keystone
300
250
200
150
100
50
GitHub Stars
2019
2020
2021
2022
Date
star-history.com

Thank You!

Dayeol Lee (dayeol <at> berkeley <dot> edu)