Enhancing Debian Update Service

Gaspard Zoss

School of Computer and Communication Sciences
Decentralized and Distributed Systems lab
Semester Project
January 2017

Responsible
Prof. Bryan Ford
EPFL / DEDIS

Supervisor
Eleftherios Kokoris Kogias
EPFL / DEDIS

Supervisor
Kirill Nikitin
EPFL / DEDIS

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Content

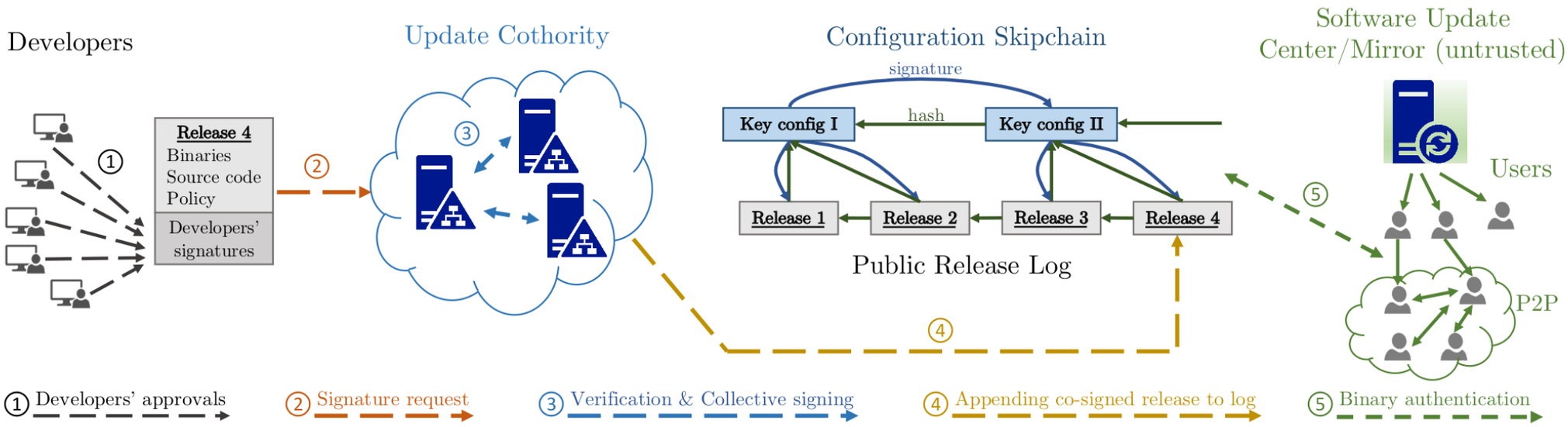
- Introduction
- Background
- Goals and Motivation
- Implementation
- Results and Evaluation
- Conclusion and Future Work

Introduction

- Software updates essential in securing an software
- Several attack vectors
- Signed updates
- Secure channel
- Reproducible builds

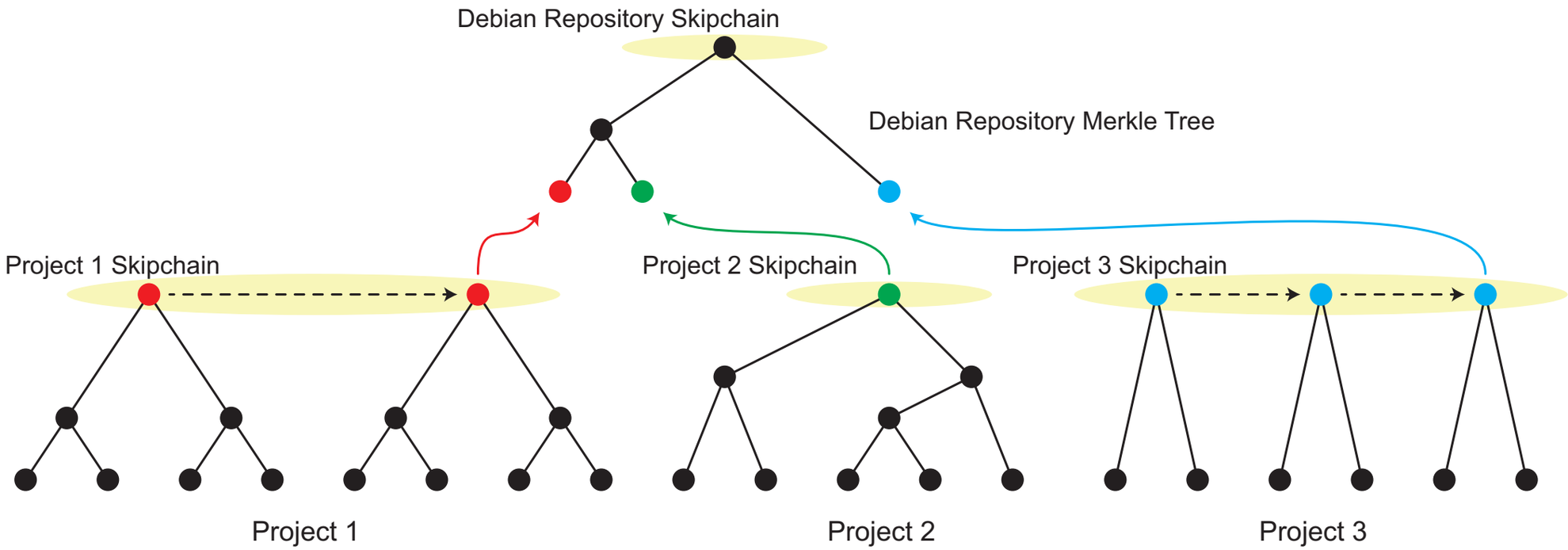
Background

- Debian Release System
  - Separation in repository with different release cycle and stability
  - GPG signature on root description file containing hashes
- Built on and extending Chainiac

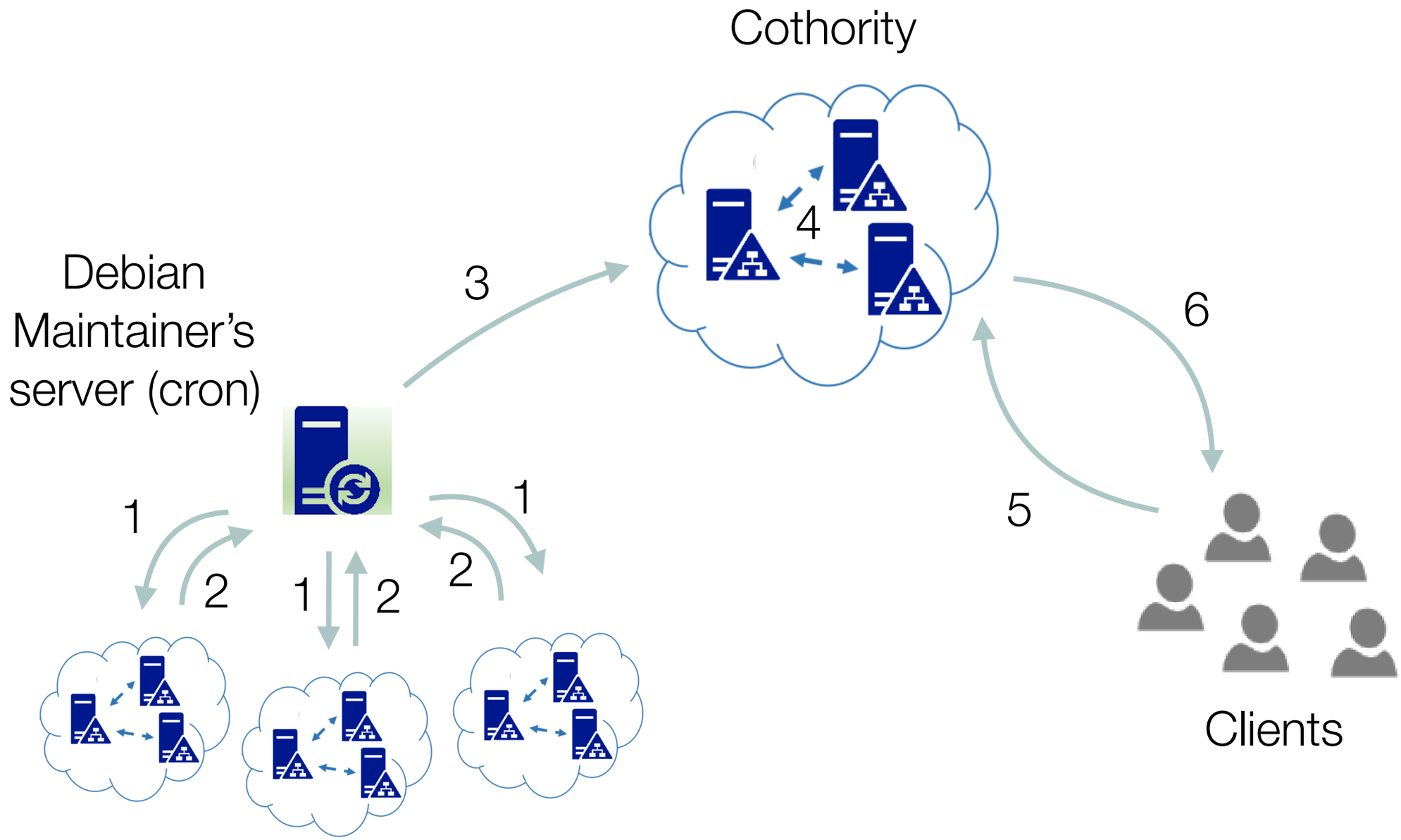


Goals & Motivation

- Explore the scalability of Chianiac on the Debian Project
- Extends it by adding a layer on top
- Merkle tree of individual skipchain's roots

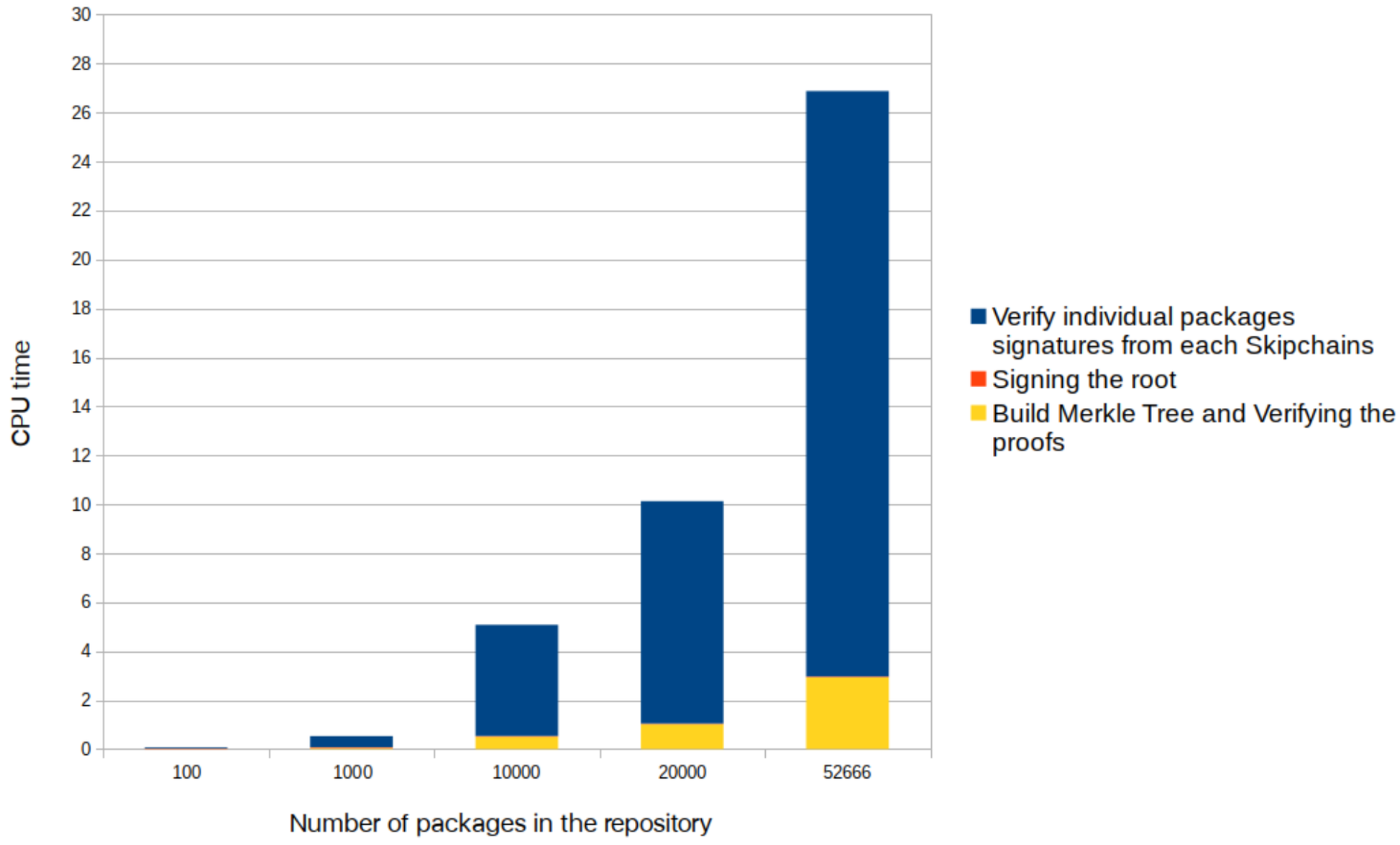


Infrastructure



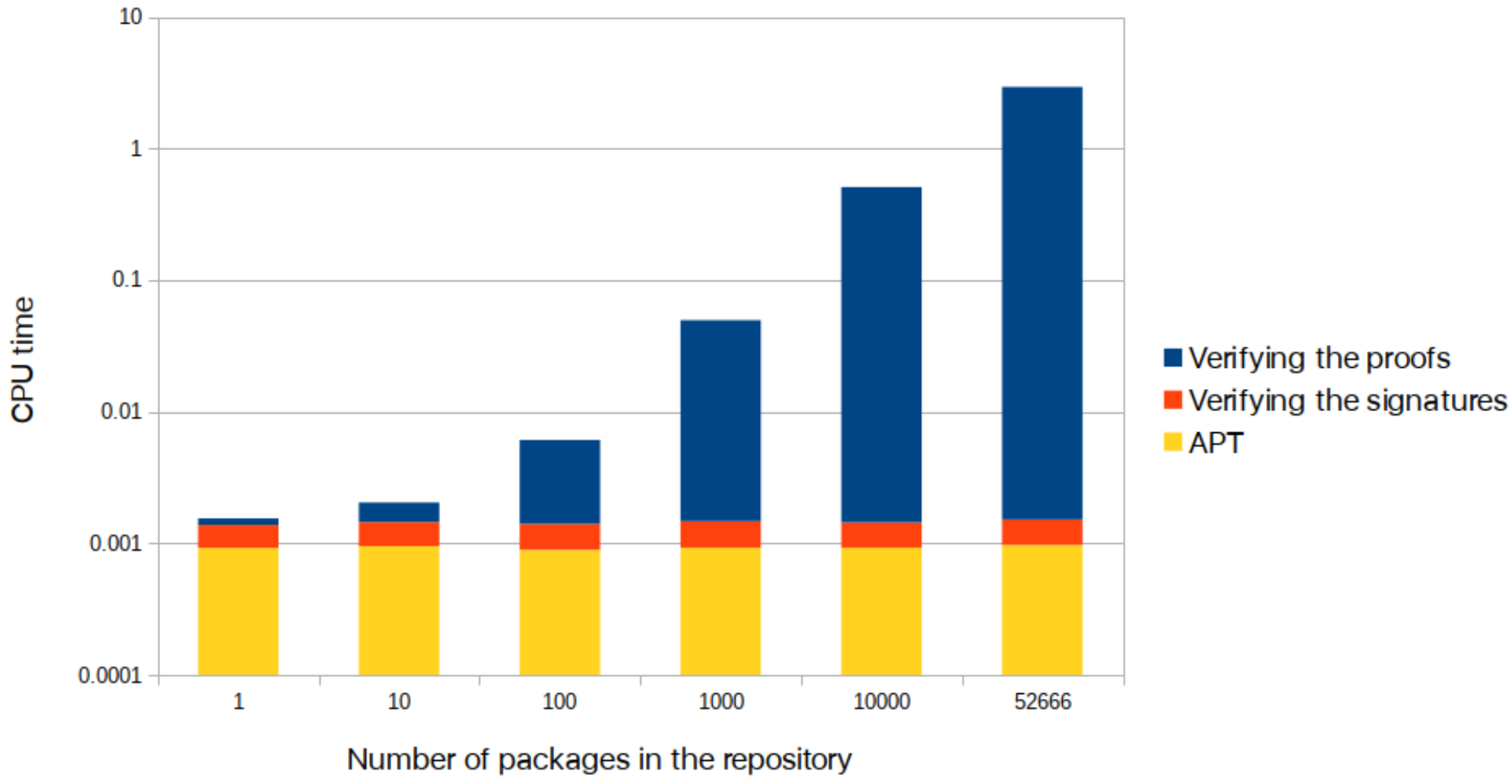
Results and Evaluation

- Metrics on Cothority (4 nodes)



Results and Evaluation

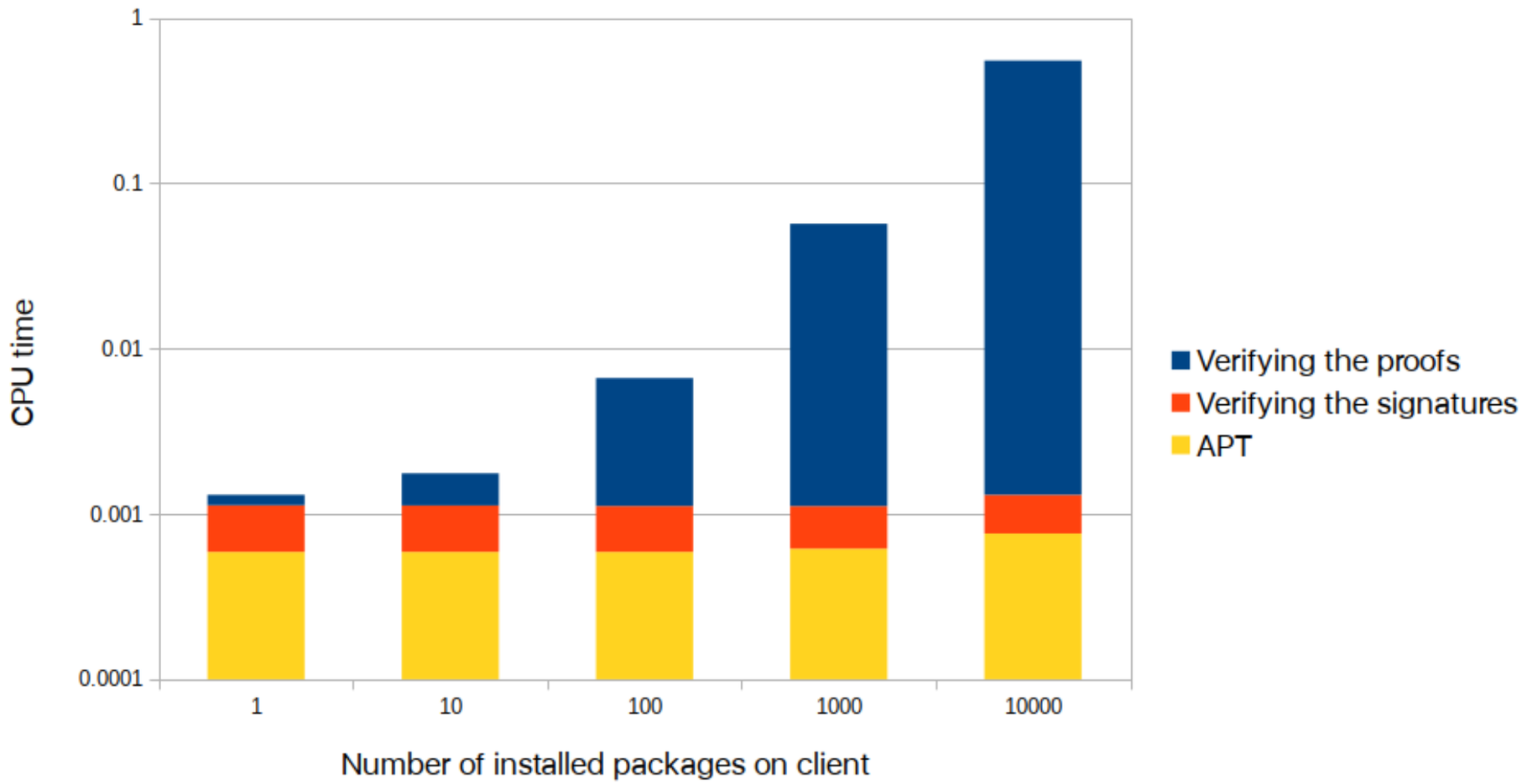
- CPU metrics on client



for this simulation, all packages available in the repository where installed

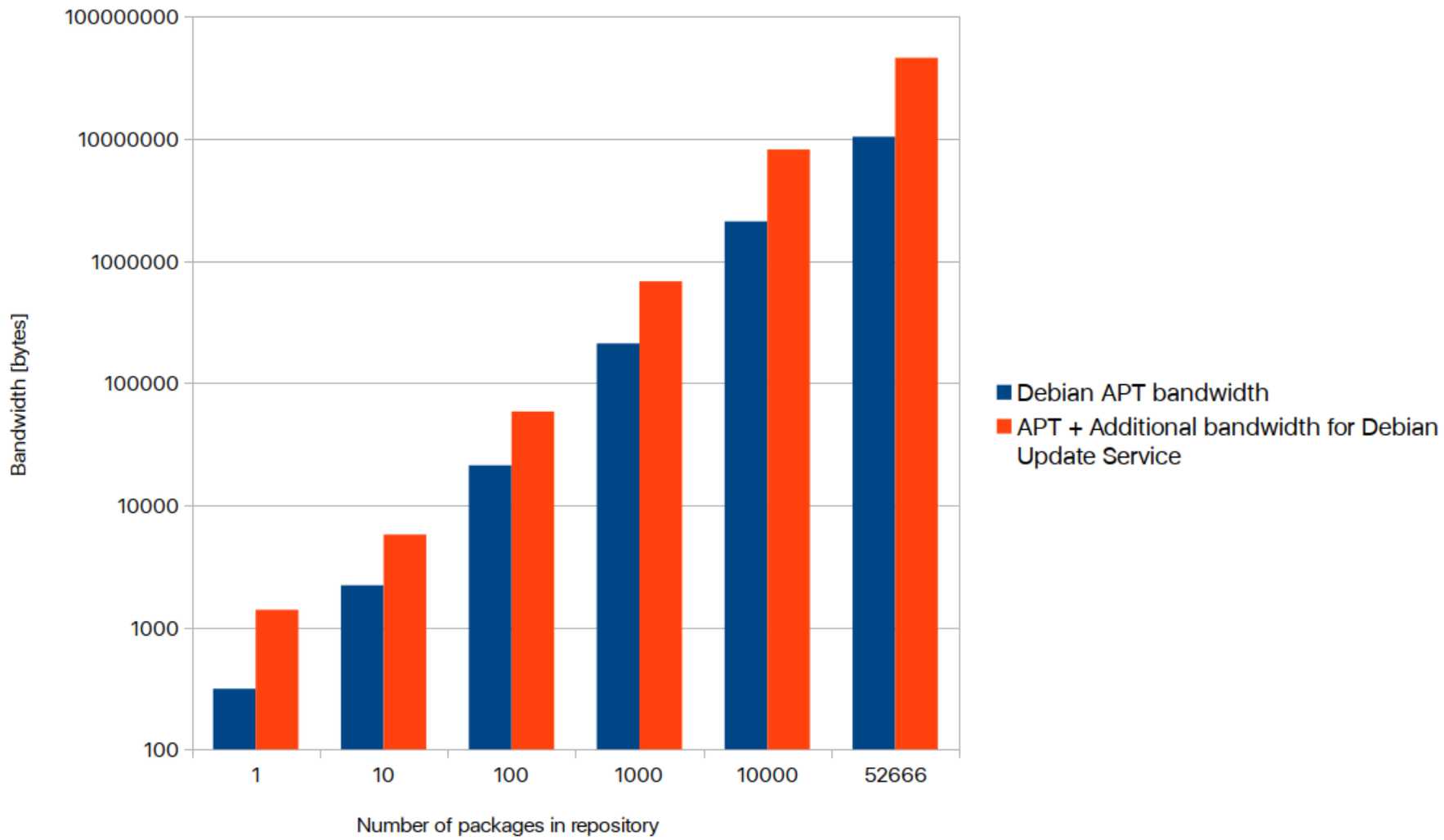
Results and Evaluation

- CPU metrics on client



Results and Evaluation

- Bandwidth metrics on client



Conclusion

- Enhanced Debian Update with collectively signed Skipchains
- Simulation on main Debian repositories
- Additional price to pay in terms of bandwidth and CPU for greater security
- Small APT wrapper

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Future Work

- Privacy preserving software updates
- Porting the framework to Arch Linux or OS X Homebrew
- Future future work; include this framework in APT

References

- *K. Nikitin, L. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, I. Khoffi, J. Cappos and B. Ford*. Back to the Future: Transparent Software-Updates with Collectively Signed Skipchains and Build Verification

- *Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford*. Keeping Authorities" Honest or Bust" with Decentralized Witness Cosigning. 2015

- Overview of various statistics about reproducible builds. https://tests.reproducible-builds.org

- Debian Snapshot project. http://snapshot.debian.org/

Questions ?

Skipchain Structure