Cloudflare Candidate Interview

Armando Faz Hernández

PhD Candidate
University of Campinas, Brazil
www.ic.unicamp.br/~armfazh

Position: Cryptography Engineering
Hiring Manager: Nick Sullivan

Background

- RSA is currently supported by Cloudflare.
  - RSA Signatures (PKCS 1)
  - Encryption/Decryption (RSA-OEAP).

- RSA public operations are fast.
  - However, private operations are slow to compute.

Two-day Challenge

- Can RSA run faster?
  - Using Go
  - Targeting 64-bit architectures

Mentoring: Vlad Krasnov

Improvement Ideas

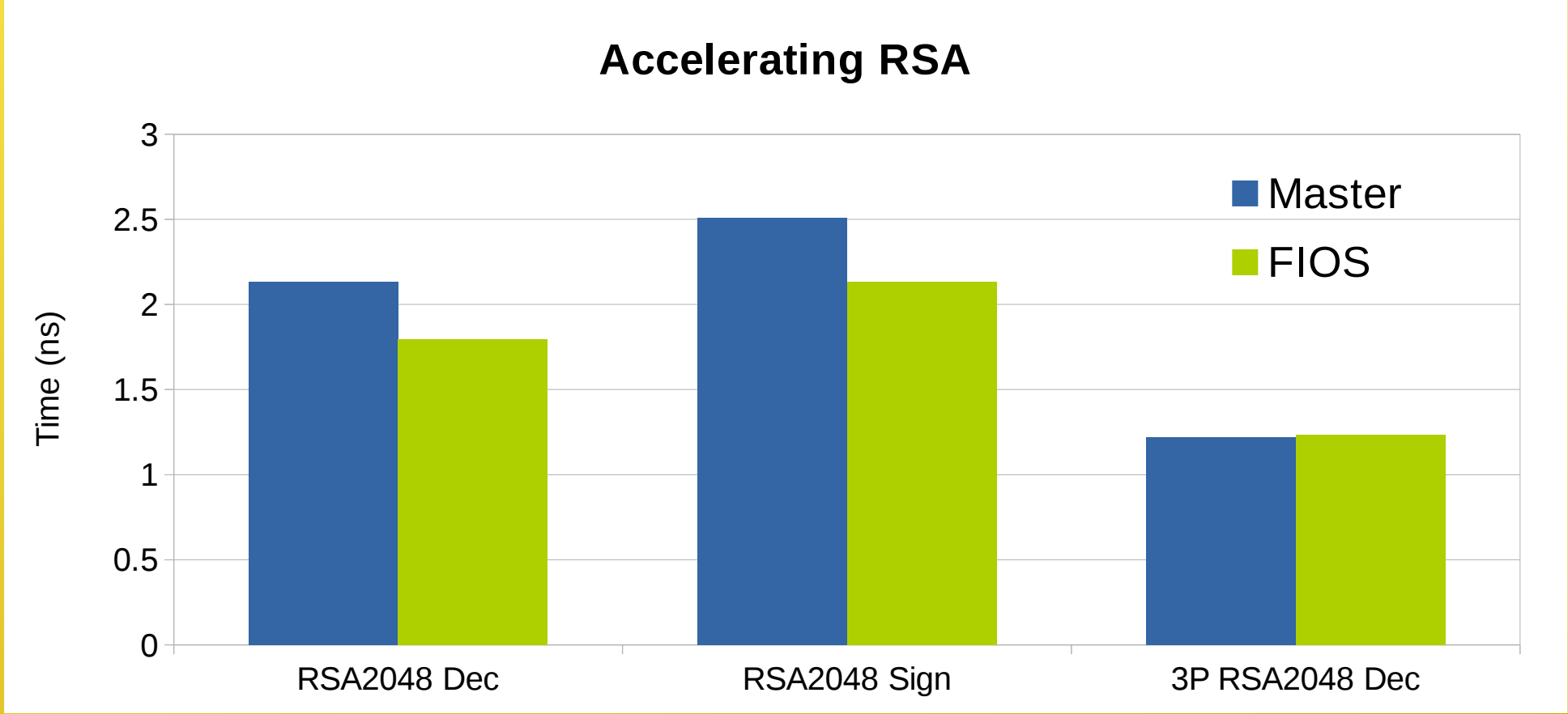
Key idea: *Modify Montgomery multiplication implementation*

1) Replace CIOS algorithm by FIOS algorithm
   - A better register scheduling
   - Reduce the number of write memory operations

2) Replace CIOS algorithm by SOS algorithm
   - Faster integer multiplication

Benchmark Results

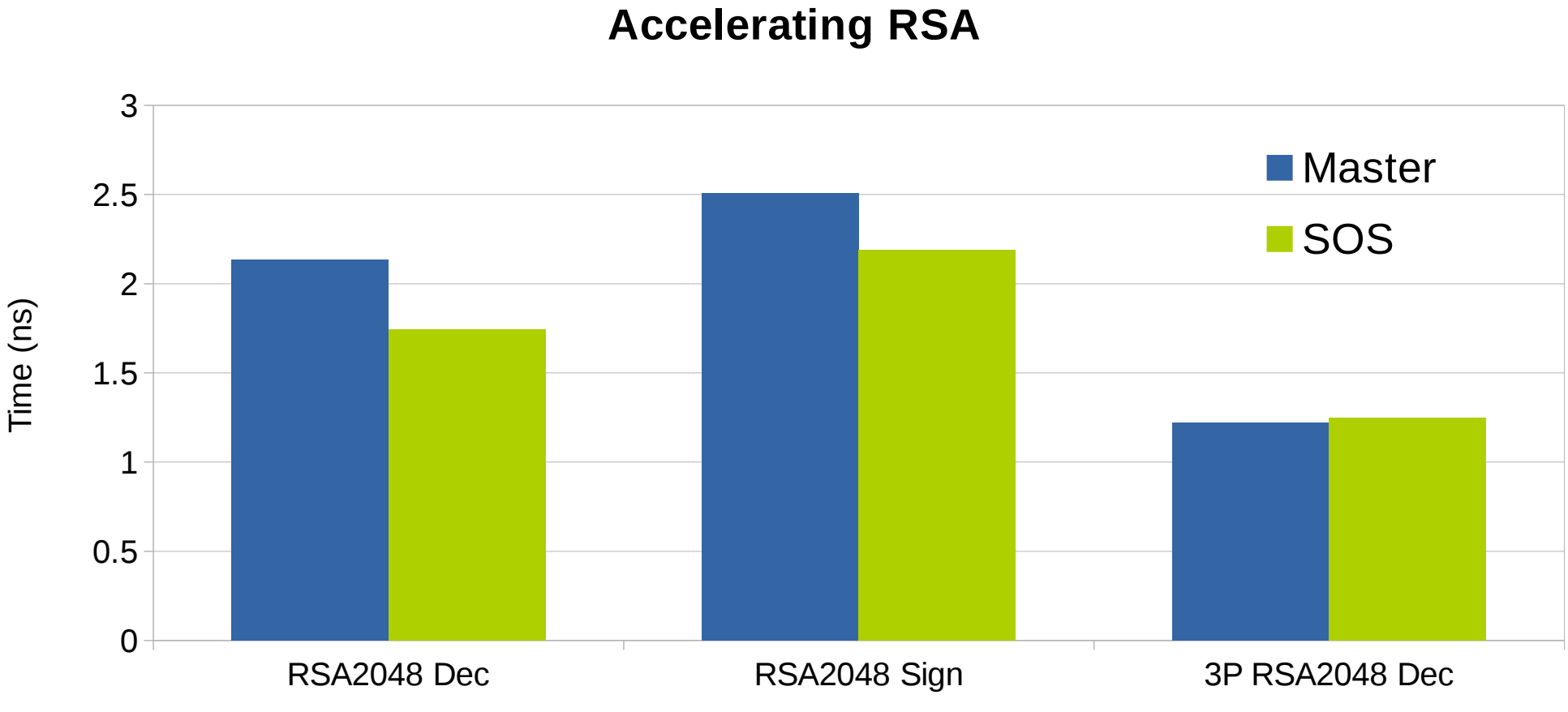
CIOS → FIOS



15.8 % ***14.8 %*** ***-1.8 %***

Benchmark Results

CIOS → SOS



18.5 % ***12.7 %*** ***-2.2 %***

Summary

- Fine tuning of Montgomery mult speedups RSA significantly.
- There still other venues of optimization
  - Dedicated code for squaring
  - Protect look-up table accesses.
- Code available in: http://github.com/armfazh/go
  - Branch: opt2 (CIOS→ FIOS)
  - Branch: fios (CIOS→ SOS)