CRII: SATC: Secure Instruction Set Extensions for Lattice-Based Post-Quantum Cryptosystems

Aydin Aysu, North Carolina State University

https://research.ece.ncsu.edu/aaysu/research/pq-nsf.html

Key Problems and Significance:

Side-channel attacks are a major threat for the cyberinfrastructure and *physical* side-channels are fundamental to CMOS technology

Side-channels of next-generation cryptography is unknown as they gear for mass deployment

Existing work on algorithmic side-channel defenses *(masking)* is ad-hoc and must be tuned for each algorithm

Can we automate side-channel secure design?

Scientific Impact:

Project seeks secure-by-design solutions through custom instruction extensions and compiler support

Methodology broadens the scope: Automated solutions can address the ad-hoc nature of side-channel protection research and enable extensions to other applications

Targeting the open-source RISC-V ISA helps incorporate or complement other architectural security research

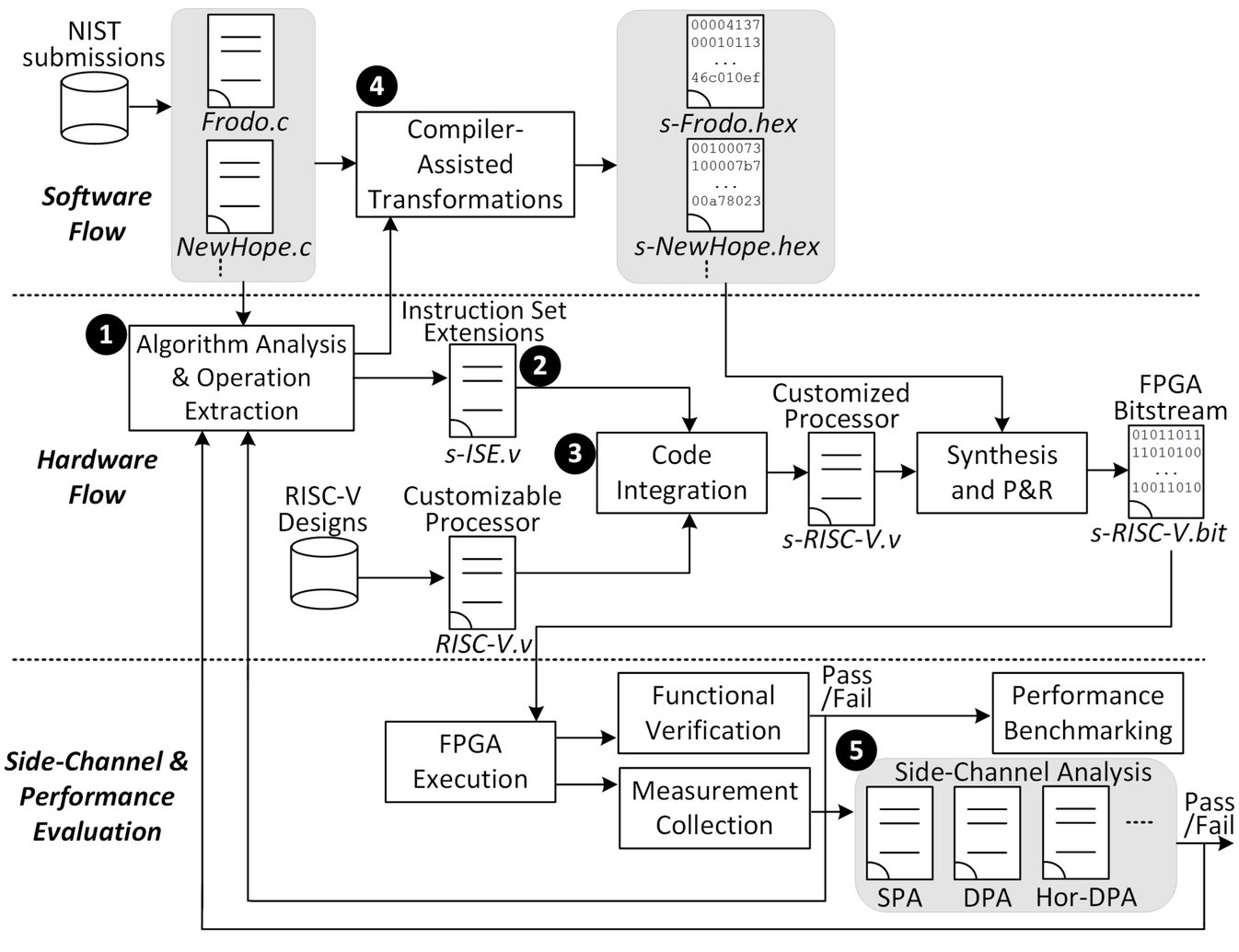
Technical Approach:

Software Flow: Decompose algorithms into a set of common instructions

Hardware Flow: Design side-channel protected custom instruction extensions for the vulnerable instructions

Hardware/Software Integration: Enable compiler support for the extensions

Side-Channel & Performance Benchmark: Automate side-channel analysis, compare the security and cost of baseline vs. protected solutions



Broader Impact on Society:

Helps NIST's ongoing quantum-secure encryption standard, which enables large-scale deployment

RISC-V open source integration can facilitate further research

Trains undergraduate and graduate students on the theory and implementation of next-generation cryptosystems

Educational Component:

Aysu, Aydin. "Teaching the Next Generation of Cryptographic Hardware Design to the Next Generation of Engineers." In Proceedings of the 2019 on Great Lakes Symposium on VLSI, pp. 237-242. ACM, 2019. **Best Paper Award MSE Track**

Resulted in a hardware security course focusing on lattice-based cryptography

Broader Impact Quantification:

NIST's cryptography standards are deployed in virtually all computers, resulting tools/methods can be used for implementing this standard

A prior NIST standard, AES, resulted in 250 billion USD economic benefit with a benefit-to-cost ratio of 1,976-to-1 [1]

[1] Leech, David P., Stacey Ferris, and John T. Scott. "The economic impacts of the advanced encryption standard, 1996–2017." Annals of Science and Technology Policy 3, no. 2 (2019): 142-257.

Award ID#: 1850373