Project Summary

Collaborative Research: SHF: Medium: Making Analog Side Channels a First-Class Consideration in Architecture-Level Design

Milos Prvulovic, Alenka Zajic, and Rakesh Kumar

Overview

Analog side-channels (power, electromagnetic, acoustic, etc.) have long been a potential source of attacks that circumvent traditional protections and security measures. Many such attacks have been demonstrated over the past several decades, followed by countermeasures that prevent specific attacks by modifying the software that has been demonstrated to leak sensitive information. However, recent analog side channel attacks have shown that both attacks and mitigations are becoming increasingly dependent on microarchitectural behavior and potentially fragile to future microarchitectural changes. Ideally, the potential for information leakage through analog side channels and "breaking" existing software mitigation approaches would be considered in early stages of design for both hardware and software, guided by tools that can predict the impact a specific design has on analog side channels. This would be analogous to how performance and power consumption are predicted by cycle-accurate simulators, which allows the tradeoff between performance, power, and cost to be investigated at design time, years before the first prototype of that processor is fabricated.

However, early-design tools such as cycle-accurate simulators do not model analog side channel signals, so these side channels can only be considered when they can be physically measured on already-fabricated chips. At that time, however, time-to-market concerns prevent introduction of overall design changes that would adjust the design tradeoffs in a more desirable direction. Additionally, most software developers have neither the know-how nor the equipment to assess their software's potential vulnerability to analog side channels, so such considerations are typically either absent or qualitative/abstract when software is designed, giving first-mover advantage to attackers, and resulting in mitigation via localized patches, which themselves are becoming increasingly microarchitecture-dependent.

We propose to develop 1) techniques that allow architecture-level simulators to efficiently generate estimated side channel signals, to help computer architects, researchers, and software developers assess the impacts of microarchitectural and software changes on the tradeoff between performance, power, and side channel leakage, 2) methods for efficient circuit-level exploration of caches and functional units that can be integrated into architecture-level simulators, analogous to how Cacti and McPat are used to obtain per-event latency and power estimates in cycle-accurate simulators, and 3) methods for "calibration" of simulation parameters against measured signals from real systems.

Intellectual Merit

Our work will demonstrate the feasibility of modeling analog side-channels at the microarchitectural level and provide proof-of-concept integration of such modeling into a cycle-accurate simulator. This will allow analog side channels to become a first-class consideration, along with performance and power, in processor designs, allowing computer architects to avoid introducing significant new vulnerabilities and "breaking" existing software mitigations, and possibly even to reduce leakage and/or enable new mitigations. It would also allow programmers and even compilers to include analog side channel considerations in their tradeoff space during design and/or optimization.

Broader Impacts

We expect that our results will help the inclusion of analog side channels among early design considerations and will help reduce the cost of side-channel resistant designs by addressing side-channel-related problems early in the design process, when side-channel resilience may be improved (or preserved) with little or no sacrifice in performance, power, cost, weight, etc. The proposal also includes 1) developing an interactive demonstrator to educate and raise awareness about analog side channels 2) visits and activities in local schools to improve K-12 education and participation of women and minorities in STEM, and 3) course and curriculum development activities at the undergraduate and graduate level.

Keywords: cycle accurate simulation; analog side channels; microarchitecture