Low-Latency Crypto: An Emerging Paradigm of Lightweight Cryptography

proposal for presentation

Santosh Ghosh

Intel Labs, Intel Corporation, USA
santosh.ghosh[at]intel.com

Recently, a memory safety mechanism called Cryptographic Capability Computing (C^3) [LRD+21] has been proposed. C^3 aims to provide a generic low-overhead solution against long-lasting memory safety problems. In particular, it hardens compute systems against attackers that exploit software bugs and vulnerabilities like buffer overflows, use-after-free etc. C^3 provides memory safety by encrypting each pointer and associated data object. It keeps each object encrypted throughout the memory hierarchy, from L1 to L3 to DRAM. The objects are decrypted only at the time of execution. More specifically, the ld pipeline in-between data-cache (L1) and execution-unit computes both pointer-decryption and data-decryption. C^3 has demonstrated significantly enhanced memory protection with less than 1% performance overhead. To achieve this, C^3 heavily relies on ultra low-latency cryptographic primitives.

In this talk, we present a brief-overview of C^3 as an emerging application and focus on investigating low-latency aspects of existing cryptographic primitives. We revisit existing NIST-standards, AES and SHA3, and show the critical-path and corresponding latency in an advanced technology node [ea17]. Then we analyze the underlying primitives of NIST LWC finalists and their expected critical-paths. Further, we analyze a few lightweight primitives outside the NIST LWC finalists and present a latency comparison. Our results show that the underlying primitives of some NIST LWC finalists provide $3x$ lower latency with $2.5x$ lower total die-area.

References

[ea17] C. Auth et al. A 10nm high performance and low-power cmos technology featuring 3rd generation finfet transistors, self-aligned quad patterning, contact over active gate and cobalt local interconnects. In *2017 IEEE International Electron Devices Meeting (IEDM)*, pages 29.1.1–29.1.4, 2017.

[LRD+21] Michael LeMay, Joydeep Rakshit, Sergej Deutsch, David M. Durham, Santosh Ghosh, Anant Nori, Jayesh Gaur, Andrew Weiler, Salmin Sultana, Karanvir Grewal, and Sreenivas Subramoney. Cryptographic capability computing. In *MICRO '21: 54th Annual IEEE/ACM International Symposium on Microarchitecture, Virtual Event, Greece, October 18-22, 2021*, pages 253–267. ACM, 2021.