Need for Low-latency Ciphers - A Comparative Study of NIST LWC Finalists

Authors: Tolga Yalcin, Samaneh Ghandali

Abstract: In this study, we present detailed results of latency analyses of the hardware implementation of finalist ciphers. We start our presentation with a discussion of where and why low-latency ciphers are needed. We then present our findings for latency analyses of the AES and block cipher configurations of the KECCAK hash function of the SHA3 Standard. Finally, we compare the latency of the competition finalist ciphers with respect to unrolled and round-based implementations and possible maximum frequencies achievable with both design approaches. We finish our presentation with requests and proposals for support for low-latency in the coming NIST Lightweight Cryptography Standard.

Keywords: Low-latency, AES, SHA3, LWC competition