Design Exploration of the NIST LWC Competition Lilliput-AE

Julien Francq, Gaetan Leplus
Airbus Defence & Space - CyberSecurity

Abstract

Around 60 candidates will be competitors of the new upcoming NIST Lightweight Cryptographic Standardization Process.

Among them, Lilliput-AE is a candidate which has serious advantages from security and performance point of view.

It has been already shown in its specification package that Lilliput-AE performs very well on software on 8-bit (e.g., ATMega 128) and 16-bit (e.g., MSP430) platforms since it has comparable or smaller execution time than the two final members of CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) lightweight portfolio: Ascon and Acorn.

This talk will detail implementation results on FPGAs and ASICs for 3 architectures: straightforward, serial and thresholded. Comparisons will also be done with Ascon and Acorn.

This will show that Lilliput-AE is also well suited for hardware constrained environments.