Pipeline Implementation of Three Authenticated Encryption Algorithms

Cuauhtemoc Mancillas-López and Lilian Bossuet

Laboratoire Hubert Curien, UMR CNRS 5516, University of Lyon, Saint-Etienne, France

Abstract. In the context of CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) many submissions have been presented. In this work we implemented three of them which are based on block ciphers: COPA, ELmD and OTR. COPA and ELmD are *nonce* misused resistance and their structure is very similar, with our results we show that when the message is enough large to justify the use of a pipeline architecture, both reach almost the same throughput but the area of ELmD is significantly less. OTR is *nonce* based, its structure is based on a Fiestel Network and encryption layer of the block cipher. Our pipelined implementation of OTR uses two encryption cores of AES and achieves high throughput that easily improves the speed of construction that need the decryption layer of block cipher.