**ARCHITECTURE OPTIMIZATION AND PERFORMANCE COMPARISON OF NONCE-MISUSE-RESISTANT AUTHENTICATED ENCRYPTION ALGORITHMS**

**Abstract:**

This paper presents a performance comparison of new authenticated encryption (AE) algorithms which are aimed at providing better security and resource efﬁciency compared to existing standards. Speciﬁcally, these algorithms improve the security of existing AE standards by providing a critical property termed nonce-misuse resistance. This paper addresses algorithm to architectural mappings of several candidates from the ongoing Competition for AE: Security, Applicability, and Robustness as well as a submission from the Crypto Forum Research Group. Implementations of the architectures on both ﬁeld-programmable gate arrays and application-speciﬁc integrated circuits platforms are provided and compared with the architecture of a popular standard: Advanced Encryption Standard in Galois Counter mode (AES-GCM). Optimizations that are applicable to AE, in general, and nonce-misuse-resistant architectures, in particular, are presented. A hardware–software codesign approach to optimization is also discussed. The implementations via proposed optimizations demonstrate that new AE algorithms can provide comparable performance as standard AES-GCM while enhancing security and resource utilization for speciﬁc use-case scenarios.

**Index Terms—**Advanced Encryption Standard in Galois Counter mode (AES-GCM), AES-GCM-synthetic IV (SIV), authenticated encryption (AE), Competition for AE: Security, Applicability, and Robustness (CAESAR) competition, Deoxys, nonce-misuse resistance, pipelineable on-line encryption with authentication tag (POET), PRIMATE-APE.

**TOOLS:**

1. **XilinxISE 14.7**

**LANGUAGE:**

1. **VerilogHDL**