Article

IMPLEMENTATION OF EFFICIENT CRYPTOGRAPHIC ARITHMETIC UNITS

June 2020 · International Journal of Security and Its Applications 14(2):1 - 18
DOI:10.33832/ijsia.2020.14.2.01

Authors:

Kiran KUMAR V.G
A J Institute of Engineering and Technology, Mangaluru

C. Shantharama Rai
A.J.Instite of Engineering and Technology

Abstract

In the era of Internet of Things (IoT), there has been enormous increase in the implementation of smart devices with constrained resources to implement various cryptographic arithmetic primitives. Most of the conventional cryptographic algorithms like the IDEA, RSA etc. involve simple operations like addition, multiplication and complex operations like addition-modulo, multiplication-modulo etc. such algorithms may not be fit the resource constrained devices. While the current conventional algorithms approved National Institute of Standards and Technology (NIST) - can be implemented to route the resource constrained devices, their performance may not be satisfactory. Over the years, extensive research has been carried out configuring the cryptographic arithmetic structures, the basic arithmetic modules using different design styles, algorithms and aspects. In this paper efficient cryptographic arithmetic modules is implemented by combining the reversible logic and Vedic mathematics. The synthesis and implementation show that the proposed modules have considerable amount of improvement in the Area, power dissipation and delay.

Citations (1) References (17)

DESIGN AND IMPLEMENTATION OF AN EFFICIENT FPGA ARCHITECTURE FOR CRYPTOGRAPHIC ALGORITHMS

Thesis

Aug 2021

Kiran KUMAR V.G · C. Shantharama Rai

View Show abstract