July - Sep © 2014 Transactions; 1(3): 120-131

International Journal of Research and Applications

ISSN (online): 2349-0020 http://www.ijraonline.com/

Research Article

Implementation of AES-GCM encryption algorithm for high performance and low power architecture using FPGA

V. Arun [1], K. Vanisree [2] and D. Laxma Reddy [3]

Corresponding Author:
icetet2014@yahoo.com

DOI:
http://dx.doi.org/
10.17812/IJRA.1.3(26)2014

Manuscript:
Received: 15th Sep, 2014
Accepted: 22nd Sep, 2014
Published: 30th Sep, 2014

ABSTRACT

Evaluation of the Advanced Encryption Standard (AES) algorithm in FPGA is proposed here. This Evaluation is compared with other works to show the efficiency. Here we are concerned about two major purposes. The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography in use today. The design uses an iterative looping approach with block and key size of 128 bits, lookup table implementation of S-box. This gives low complexity architecture and easily achieves low latency as well as high throughput. Simulation results, performance results are presented and compared with previous reported designs. Since its acceptance as the adopted symmetric-key algorithm, the Advanced Encryption Standard (AES) and its recently standardized authentication Galois/Counter Mode (GCM) have been utilized in various security-constrained applications. Many of the AES-GCM applications are power and resource constrained and requires efficient hardware implementations. In this project, AES-GCM algorithms are evaluated and optimized to identify the high-performance and low-power architectures. The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. The Cipher Block Chaining (CBC) mode is a confidentiality mode whose encryption process features the combining ("chaining") of the plaintext blocks with the previous Cipher text blocks. The CBC mode requires an IV to combine with the first plaintext block. The IV need not be secret, but it must be unpredictable. Also, the integrity of the IV should be protected. Galois/Counter Mode (GCM) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption. Galois Hash is used for authentication, and the Advanced Encryption Standard (AES) block cipher is used for encryption in counter mode of operation. To obtain the least-complexity S-box, the formulations for the Galois Field (GF) sub-field inversions in GF (2^4) are optimized By conducting exhaustive simulations for the input transitions, we analyze the synthesis of the AES S-boxes considering the switching activities, gate-level net lists, and parasitic information. Finally, by implementation of AES-GCM the high-performance GF (2^{128}) multiplier architectures, gives the detailed information of its performance. An optimized coding for the implementation of Advanced Encryption Standard-Galois

Counter Mode has been developed. The speed factor of the algorithm implementation has been targeted and a software code in Verilog HDL has been developed. This implementation is useful in wireless security like military communication and mobile telephony where there is a grayer emphasis on the speed of communication.

Keywords: Cipher block chaining, GaliosField, Advanced Encryption Standard, finite field, Galois/Counter Mode, high performance.

---

[1] Assistant Professor, Dept., of ECE, MLRIT, Dundigal, Hyderabad-500043, Telangana
[2] Associate Professor, Dept., of ECE, ACE College of Engineering, R. R. - 501301, Telangana
[3] Assistant Professor, Dept., of ECE, MLRIT, Dundigal, Hyderabad-500043, Telangana

IJRA - Year of 2014 Transactions:
Month: July-September
Volume – 1, Issue – 3, Page No's: 120-131
Subject Stream: Electronics

Paper Communication: Through Conference of ICETET-2014

Paper Reference Id: IJRA-2014: 1(3)120-131