IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN (E): 2321-8843; ISSN (P): 2347-4599
Vol. 4, Issue 2, Feb. 2016, 7-24
© Impact Journals

FPGA IMPLEMENTATION OF 30GBPS SECURITY MODULE FOR GPON SYSTEMS

KALYANI PEDDINA, SUNIL KUMAR DASARI & SATISH KUMAR REDDY M V

Department of Electronics and Communications, GITAM School of Technology, GITAM University

Bangalore, Karnataka, India

ABSTRACT

The need for privacy has become a high priority for both governments and civilians desiring protection from signal and data interception. Widespread use of personal communications devices has only increased demand for a level of security on previously insecure communications. Both DES (Data Encryption Standard) and AES are defined as symmetric key block ciphers [1], with the main difference being the bit length of the key (56 bit for DES).

These symmetric-key encryption schemes use the same key for both the sender and receiver, and as a result eliminate the need for the verification server needed in public keying. Symmetric keying lends itself to work independently of an open network and in turn a higher level of system interoperability.

Ever since DES [2] was phased out in 2001 and its successor, the Advanced Encryption Standard (also known as Rijndael) took its place, various AES implementations have been proposed both in software and hardware. This paper presents low cost and low power hardware architecture for the Advanced Encryption Standard (AES). In 1997, the National Institute of Standards and Technology promoted worldwide research into a replacement for DES, or the widely accepted Data Encryption Standard. In this brief, we present an efficient and cost-effective AES co-processor design [3]. To minimize cost, focusing on efficiency reduced overall hardware complexity.

A VHDL hardware implementation [4] is also presented, utilizing a field programmable gate array (FPGA) as a prototyping platform. In this architecture, the main priority was not to increase throughput or decrease processing time but to balance these factors in order to minimize cost. A focus on low power and cost allows for scaling of the architecture towards vulnerable portable communications devices in consumer and military applications such as cellular phones, PDAs, digital radios, pagers, and similar lower speed communication embedded systems.

KEYWORDS: Module for GPON, Security