Oct - Dec © 2014 Transactions; 1(4): 149-156

International Journal of Research and Applications

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

Research Article

FPGA Implementation DIFFIE-HELLMAN key exchange algorithm using Symmetric Encryption Algorithm

B. Keerthi Sudha [1] and P.Rajani [2]

Corresponding Author:
panthaganti189@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.1.4(30)2014

Manuscript:
Received: 16th Sep, 2014
Accepted: 25th Nov, 2014
Published: 1st Dec, 2014

ABSTRACT

Zero-knowledge proof (ZKP) plays an important role in authentication without revealing secret information. Diffie–Hellman (D-H) key exchange algorithm was developed to exchange secret keys through unprotected channels. Previously we have Diffie-hellmen key exchange algorithm. It has some security attacks like man in the middle attack to overcome this attack by using zero knowledge proof concepts. In Diffie Hellman algorithm we had generated one key. That key we have to use in des encryption and decryption .this paper is implemented in Xilinx 13.2 version and verified using Spartan 3e kit.

Keywords: Diffie-hellmen key exchange, des encryption, decryption.

[1] M.Tech (Pursuing) and [2] Assistant Professor
[1 2] Department of ECE, Vaagdevi College of Engineering (Autonomous),
Affiliated to Jawarlal Nehru Technological University, Bollikuntta, Warangal - 506 005.

IJRA - Year of 2014 Transactions:
Month: October - December
Volume – 1, Issue – 4, Page No's:149-156
Subject Stream: Electronics

Paper Communication: Author Direct

Paper Reference Id: IJRA-2014: 1(4)149-156