Abstract

Now-a-days internet is one of the most important sources of communication and thousands of people interact electronically. For sending sensitive messages over the internet, we need security. Hence for secure communication required the algorithms. Among these algorithms is Twofish, a promising 128-bit block cipher and one of the competitors in National Institute of Standards and Technology’s (NIST) AES competition, for the replacement of DES at the core of many encryption systems world-wide. In this paper the security algorithm, twofish has been explained with all of its modules (some modules has been modified) for both 128 and 192-bit key size. Implementation on VHDL using Xilinx – 6. 1 xst software has been done taking delay as main constraint.

References

- Mark De Clercq, Vincent Levesque "A VHDL Implementation of the Twofish Block Cipher"; in IEEE, 2006
- Hani H. JABER &quot;Relational Database Security Enhancements;&quot;, in Arab University, 2008
- Dr. S. A. M Rizvi, Dr. Syed Zeeshan Hussain, Neeta Wadhwa, "Performance Analysis of AES and TwoFish Encryption Schemes;&quot; in International Conference on Communication Systems and Network Technologies of IEEE Computer Society, 2011, pg. 76-79, vol-3
- G. Catalini, F. Chiaraluce, L. Ciccarelli, E. Gamhi, P. Pierleoni, M. Reginelli, "modified twofish algorithm for increasing security and efficiency in the encryption of video signals;&quot; in IEEE, 2005
- Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, Mike Stay "The Twofish Team's Final Comments on AES Selection;&quot;
- Rabie A. Mahmoud1, Magdy Saeb2, "A Metamorphic-Enhanced Twofish Block Cipher And Associated FPGA Implementation;&quot; in The International Journal of Computer Science and Communication Security (IJCSCS), Volume 2, January 2012

Index Terms

Computer Science

Algorithms

Keywords

Twofish MDS PHT DES Function F and g