151. A NEW ROBUST SCAN TECHNIQUE FOR SECURED ADVANCED ENCRYPTION STANDARDS (AES) AGAINST DIFFERENTIAL CRYPTANALYSIS ATTACKS

Sabna.K.V, PG Student Vanathi.A, Assistant Professor
Department Electronics and Communication,
GKM College of Engineering and Technology,
sabnaece91@gmail.com, gkmcetece035@gkmcet.net.in

In recent days Field-Programmable Gate Arrays (FPGAs) are becoming a popular target for implementing cryptographic block ciphers, as a well-designed FPGA solution can combine some of the algorithmic flexibility and cost efficiency of an equivalent software implementation with throughputs that are comparable to custom ASIC designs. The recently selected Advanced Encryption Standard (AES) is slowly replacing older ciphers as the building block of choice for secure systems and is well suited to an FPGA implementation. We have also described some possible biometric schemes(RETINA) that can be used for authentication along with cryptography on networked embedded computers. Public-key infrastructures are secure, but only to the extent that private keys of individuals are maintained secret. Usually this involves securing the private key(s) using a password, a PIN or a token. Biometrics alone do not provide a great deal of safety, but a combination of biometrics will provide a higherdegree of security for embedded computing devices. Finally we improve the performance of the proposed system using pipelining technique and its efficiency will be proved through hardware synthesis.

Keywords- masking, biometric authentication, key extraction.

ISBN 978-81-904760-6-5