ISBN: 978-93-5780-385-4

An Efficient VLSI Implementation of High Speed 1024 AES Using Cryptography

Lakshmi Mythri Dasari[1], Sheik Shabeena[2],
[1,2]Assistant Professor, Dept of ECE, DIET, Visakhapatnam

Abstract
Cryptography is the technique to improve the signal security for the transmission of data to reduce the hacking effects. The cryptography is mainly done in two stages they are symmetric cryptography and asymmetric cryptography. The plain text is encrypted with the key and at the decryption side same key is used to extract the original information. The encryption is done in the different symmetric key algorithms like DES, RC2, RC4, AES etc. are improved to secure the information. In this paper a new algorithm is used to improve the signal security to avoid the hacking effects. The proposed technique is implemented in the 1024 bits along with the 1024 key and the decryption is also done with the same key to obtain the plain text. In the proposed method the signal security is improved while varying the different key lengths, due to this hacking is not possible. The proposed technique achieves high speed and signal security compared with previous AES algorithms.

Key words: Advanced Encryption Standard, RC4, Plain text, Cryptography.

Introduction

Cryptography is used to encode the information in a very high secure manner and when the data is highly confidential key is used to encrypt the data. Using the key is also done in two ways either by using the public key or the private key. The public key is used for the known purpose and for the transmission of open secured information. The private key is used for the transmission of very confidential data and these public keys are only known by the sender and receiver. Here the information is called as the plain text and the plain text is encrypted with the key to obtain the encrypted data. The encrypted that is transmitting is unable to read and the encrypted message contains only different symbols which are in unreadable format and not understandable format. At the receiver side the encrypted messaged is decrypted with the

ISBN: **978-93-5780-385-4**

same key to extract the original information called as plain text.

Previously Blowfish algorithm is used to encrypt the data but using these techniques two different keys are used in the encryption process. Due to the use of asymmetric use of keys the speed of the encryption is getting reduced and the signal is also easy to hack. Hence the encryption of 128 bit plain text along with the key is unsatisfactory and to overcome this new 1024 AES algorithm is implemented to improve the signal security along with the speed. Hence the results show that the proposed architecture is going through odd and even substitutions only. The complete data is splatted into two parts and the first half will perform the left shift operations and the second half will do the right shift operations. The key is also used here to reduce the rounds hence instead of sixteen rounds in this architecture there are only eight rounds are using to obtain the encrypted data. The proposed design consists of AES algorithm with a little reduction of the plain text and the key size. Hence for the 1024 AES used 512 bits to implement the encryption process.

Related work

To understand the AES in an easier manner different AES architectures are studied in the literature. Here, the AES architectures are implemented which not more than 128 bit such as the work is presented in [8] [9] [10]. Previously different encryption algorithms are implemented to improve the signal security. The main purpose of designing the AES is to avoid the data hacking and information leakage. Different encryption algorithms are implemented and studied for the better understanding of the AES hardware implementation in [3] [7] [18] [19] [20]. In these papers different AES architectures are implemented, analyzed and shows the improvement in terms of area consumption, delay and power consumption along with the signal security. Theauthors in [7] and [8] have given a brief comparison of the FPGA hardware performance of the AES candidates.

At present, AES shows the better signal security compared to all the previous encryption algorithms. When there is a transmission of confidential and high priority data to the