International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

FPGA Based Network Security Using Cryptography

Madhuri B. Ghodke [1], Dr. Suresh N. Mali[2]

[1]Student M.*E. (VLSI &Embedded system), Sinhgad Institute of Technology and Science, Narhe, Pune.*
[2]*Principal of Sinhgad Institute of Technology and Science, Narhe, Pune.*

Abstract - Secured communication is most important thing in present day situation. Need of security is increasing rapidly. No one wants their data to be seen by others. Every individual wants their data to be secured and privacy must be maintained. This requirement can be fulfilled by the use of cryptography. In this process encryption is carried out while sending the data and the decryption is carried out while receiving the data, to retrieve the original data. with the development of encryption algorithms, security systems are becoming more powerful to grab high level of security.AES algorithm can keep the data secure and have faster processing speed.

Key Words: **Cryptography; FPGA; AES algorithm**.

1.INTRODUCTION

The art of keeping the messages secure is cryptography. Cryptography provides great significance in the security of data. It makes possible to store sensitive information or transmit the data across networks so that unauthorized persons cannot read it. The exigency for secure exchange of digital data resulted in large quantities of special encryption algorithms which can be classified into two groups: symmetric key algorithms which uses private key and asymmetric key algorithms which uses private key as well as public key. Symmetric key algorithm makes use of only one key for encryption as well as decryption. The asymmetric key algorithm needs two different keys, one for encryption and other for decryption. The enormous advancement in network technology has resulted in great prospective for changing the way we communicate and do huge business over the internet . But for handling confidential data, the cost-effectiveness and globalism provided by the internet are reduced slowly by the main disadvantage of public networks. The expressively increasing growth in the confidential data traffic over the internet makes the security issue a fundamental problem . With this increasing insistence of security in the communication channel, the development of a new, simple and efficient hardware security module has become the primary preference. AES is extensively adopted for a variety of applications from high-end computers to low power portable devices.

1.2.Cryptography

skill of defending information by transforming it into an unreadable arrangement, called cipher text. Only those who have a secret key be able to decipher the message into plain text. Encrypted messages can sometimes be broken down by cryptanalysis, also known as codebreaking. Cryptography systems can be generally classified into symmetric-key systems that utilize a single key that in cooperation with the sender and receiver, and public-key systems that make use of two keys, a public key known to everyone and a private key that only the recipient of messages uses.

1.2 Symmetric key cryptography:

In this encryption system sender and receiver of the message utilizes the identical key, this unique key is used for encryption and decryption of the message. on the contrary with the public key cryptography , which uses two keys one key for encryption and other for decryption of the message.

1.3 Asymmetric key cryptography

In aysmmetric cryptography a pair of keys is used for encryption and decryption of the message to provide security. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who desires to send an encrypted message can get the proposed recipient's public key from a public directory. They use this key for encryption of the message and they send it to the recipient. When the recipients gets the message, they decrypt it with their private key, which no one else should have access to.

2.LITERATURE REVIEW

AES algorithm have been standardized and considered as more secure than other algorithms[1]. Advanced encryption algorithm now become the prime preference in numerous of applications[1]. Hardware and software implementation can be done at faster speed and with high efficiency by use of AES algorithm. Protecting authentication and integrity of data, as well as access control, encryption, integrity checking and data masking are some of the data security techniques[2]. Cryptography is the one of the well-organized method for data security [2].Block level encrypted data operation can be carried out efficiently and confidentiality and integrity can be achieved by data encryption before outsourcing and decryption algorithm at the other end[2]. cryptographic FPGA in which an advanced encryption standard (AES) algorithm used to process on the set of plaintext and by this equivalent circuit model can be analyzed with commercial analog circuit simulator for avoiding the side channel attacks[3]. This algorithm is successful encryption algorithm in various applications like internet to provide cyber security and can be also used to provide security for smart cards. FPGAs are the capable

solution for the performance progression. The main focus is to increase the security through AES algorithm[4].

3. ENCRYPTION AND DECRYPTION

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. In an encryption scheme, the proposed communication information or message, referred as plaintext, is encrypted by making use of an encryption algorithm, generating ciphertext that can only be read if it is successfully decrypted by using the same key, as shown in figure 1.

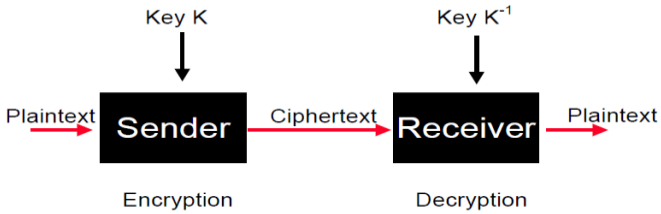

Fig -1: Cryptographic technique.

Encryption is the process which converts the plain text into unreadable format, it is called as ciphertext. the conversion from plain text to ciphertext involves mathematical operation only

4. AES ALGORITHM

The majority of recent embedded applications need AES algorithm implementations of small size and low power consumption to give surety of safe information transference. Implementation of AES is compact and its hardware encryption core is appropriate for resource-limited applications based on FPGA technology. The core has 8-bit data path structure and supports encryption by means of 128-bit keys. AES can be implemented in software or hardware but, hardware implementation is more appropriate for high speed applications in real time. Main objective AES hardware implementation is high throughput design and low-area design work at utmost operating frequency. This paper devotes most efforts to reduce size of the design and lower the power utilization.

In Key Expansions process of AES, round keys are derived from the cipher key using Rijndael's key schedule. AES needs a separate 128-bit round key block for each round plus one more. In initial round key , each byte of the state is combined with a block of round key by making the use of bitwise xor. Then the rounds like SubBytes, ShiftRows, Mixcolumns and Add_round_key are carried out.

The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are adequate to guard classified information up to the level of secret and top secret information will need use of either the 192 or 256 key lengths. The implementation of AES in products aimed to protect national security systems and information must be reviewed and certified by NSA prior to their acquirement and utilization.

5. AES ENCRYPTION PROCESS

AES is known as a private key algorithm and it has three different Rijndael cipher family members and each member from these has 128 bits size of data block. The three different lengths of the keys are 128 , 192 or 256 bits length. and these are made of 10, 12, 14 iterations. Each iteration cycle jumbles plain data with a round key. this round key is obtained from the cipher key and in decryption reverts the cycles of recurrence bringing about in part, a dissimilar data path.

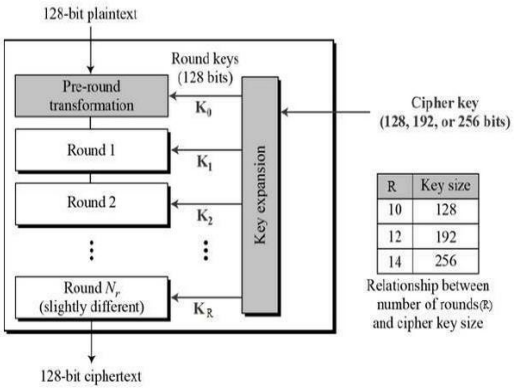

Fig -2: Schematic of AES structure.

AES is iterative and It is based on the network of substitution permutation. It includes of a series of linked operations from which some involves substitutions and the remaining other involves permutation that is mix up bits around. AES carry outs all its operations on bytes rather than bits.

In Byte Substitution process the 16 input bytes are alternated by looking up a secured table (S-box) given in design. The result is provided in a matrix of four rows and four columns. In Shiftrows process each of the four rows of the matrix is moved to the left. Any entries that 'fall off' are re-placed on the right side of row. In MixColumns each column is of four bytes these bytes are now transformed using a unique mathematical function. Now this function takes which is four bytes of one column and output is taken as four absolutely new bytes. These replace the original column. In Addroundkey 16 bytes of matrix is regarded as 128 bits and XORed to 128 bits of the round key.

6. CONCLUSION

Network security is more important for personal computer users and organizations , the handling of confidential data requires proper security options. The primary goal is to develop RSA algorithm on FPGA which will provide a significant level of security as well as can provide a faster processing time. The VHDL/Verilog language provides a useful tool of practicing the algorithms without drawings of large amounts of logic gates.

ACKNOWLEDGEMENT

It is my duty and desire to express my gratefulness to everyone who has provided their valuable guidance during this work. I am grateful all those who have helped me in the endeavor of completing this work.

REFERENCES

[1] Atef Ibrahim, "FPGA-based Hardware Implementation of Compact AES Encryption Hardware Core," WSEAS transactions on circuits and systems. ISSN: 2224-266X Volume 14, 2015

[2] Prakash G L ,Dr. Manish Prateek , Dr. Inder Singh," Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 4 April, 2014 Page No. 5215-5223

[3] Kengo Iokibe, Tetsuo Amano, Kaoru Okamoto, and Yoshitaka Toyota," Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Information Security Design", IEEE transactions on electromagnetic compatibility, 2013.

[4] J.Saira Banu, Dr.S.Subha," Loop Parallelization And Pipelining Implementation Of AES Algorithm Using OpenMP And FPGA", IEEE international conference 2013.

[5] Dr.R.V.Kshirsagar, M.V.Vyawahare, " FPGA Implementation of High speed VLSI Architectures for AES Algorithm", 2012 IEEE Fifth International Conference on Emerging Trends in Engineering and Technology.

[6] Selva Kumar M., Thamarai P., Arulselvi S.." Network Data Security Using FPGA", International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) Volume 2 Issue 5, pp : 454-457, 2013.

[7] Massoud Masoumi and Mohammad Hadi Rezayati," Novel Approach to Protect Advanced Encryption Standard Algorithm Implementation against Differential Electromagnetic and Power Analysis", IEEE Transactions on Information Forensics and Security, 2013.