MAES Base Data Encryption and Description Using VHDL

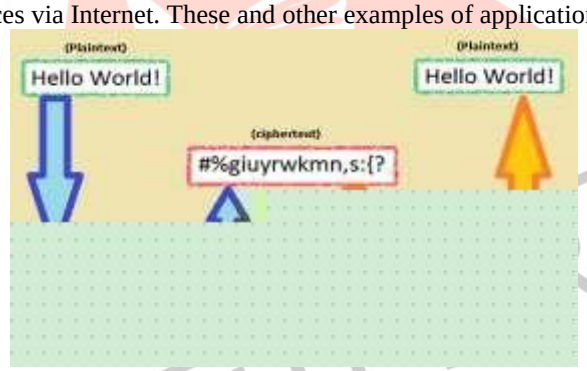
Vakkayil Megha Gopinath

***Abstract* - In this era of information, need for protection of data is more pronounced than ever. Secure communication is necessary to protect sensitive information in military and government institutions as well as private individuals. Current encryption standards are used to encrypt and protect data not only during transmission but storage as well. Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), and categorized as Computer Security Standard. The AES algorithm is a block cipher that can encrypt and decrypt digital information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits. The major advantage lay in the non-linearity of the key-schedule which eliminated the possibility of weak and semi weak keys. This encryption algorithm is virtually crack-proof till date but research has concluded that side channel attacks can be a concern if the encryption and crack are running on the same server. In this paper we introduce the concept of hybridizing the AES and DES standards with comparison of MAES using ROW-SHIFT techniques. The MAES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt dates. This methodology uses VHDL implementation over FPGA. We have programmed in Xilinx – 12.1 xst software and implemented on FPGA families which are Spartan2, Spartan3.**

***Index Terms* - AES Algorithm, RC6, Encryption, Cryptography, Cipher text, AES, DES, Hybrid algorithm, security enhancement, VHDL, FPGA implementation, Xilinx**

I. INTRODUCTION

Each day millions of users generate and interchange large volumes of information in various fields, such as financial and legal files, medical reports, and bank services via Internet. These and other examples of applications



Data hiding

Deserve a special treatment from the security point of view, not only in the transport of such information but also in its storage. In this sense, cryptography techniques are especially applicable. For a long time, the Data Encryption Standard (DES) was considered as a standard for the symmetric key encryption. DES has a key length of 56 bits. However, this key length is currently considered small and can easily be broken. For this reason, the National Institute of Standards and Technology (NIST) opened a formal call for algorithms in September 1997. A group of fifteen AES candidate algorithms were announced in August 1998. Next, algorithms were subject to assessment process performed by various groups of cryptographic researchers all over the world. In August 2000, NIST selected five algorithms: Mars, RC6, Rijndael, Serpent and Two fish as the final competitors. These algorithms were subject to further analysis prior to the selection of the best algorithm for the AES. Finally, on October 2, 2000, NIST announced that the Rijndael algorithm was the winner. Field Programmable Gate Arrays (FPGAs) are hardware devices whose function is not fixed which can be programmed in system. The potential advantage of encryption algorithm implemented in FPGAs includes: Algorithm agility- This term refers to the switching of cryptographic algorithm during operation. Algorithm upload- It is perceivable that fielded devices upgraded with new encryption algorithm which did not exist at design time.

II. ALGORITHM MODIFICATION

There are applications which require modification of a standardized algorithm. Architecture efficiency- With FPGAs it is possible to design and optimize architecture for specific parameter set. Throughput- Although typically slower than ASIC implementation, FPGA have potential of running substantially faster than software implementations. Cost efficiency- Time and cost for developing an FPGA implementation of a given algorithm are much lower than for an ASIC implementation.

In cryptography, the AES is also known as Rijndael. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. This paper deals with an FPGA implementation of an AES encryptor/decryptor using an iterative looping approach with block and key size of 128 bits. This method gives very low complexity architecture and is easily operated to achieve low latency as well

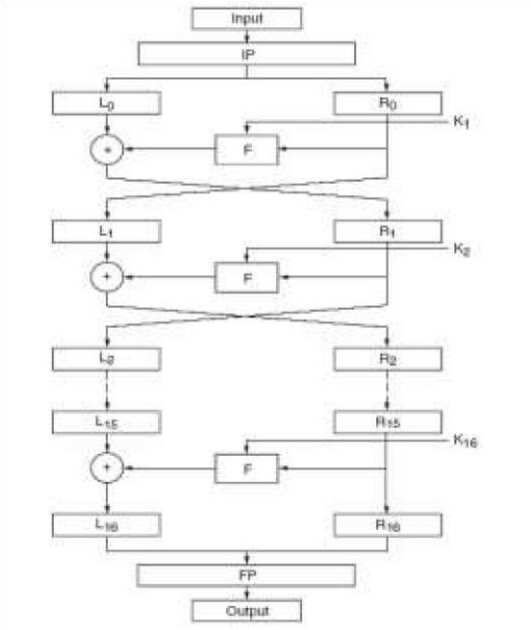
as high throughput.Each day millions of users generate and interchange large volumes of information in various fields, such as financial and legal files, medical reports, and bank services via Internet. With the rapid development and wide application of computer and communication networks, the information security has aroused high attention. Information security is not only applied to the political, military and diplomatic fields, but also applied to the common fields of people's daily lives. With the continuous development of cryptographic techniques, the long-serving DES algorithm with 56-bit key length has been broken because of the defect of short keys. So AES (Advanced Encryption Standard) substitutes DES and has already become the new standard. AES algorithm is already supported by a few international standards at present, and AES algorithm is widely applied in the financial field in domestic, such as realizing authenticated encryption in ATM, magnetism card and intelligence card. In 1997, an effort was initiated to develop a new American encryption standard to be commonly used well into the next century. This new standard was given a name AES, Advanced Encryption Standard. A new algorithm was selected through a contest organized by the National Institute of Standards and Technology (NIST). By June 1998, fifteen candidate algorithms have been submitted to NIST by research groups from all over the world. After the first round of analysis was concluded in August 1999, the number of candidates was reduced to final five. The five algorithms selected were MARS, RC6, RIJNDAEL, SERPENT and TWOFISH. The primary criteria used by NIST to evaluate AES candidates included security, efficiency in software and hardware, and flexibility. Rijndael Algorithm developed by Joan Daemen and Vincent Rijmen. Was chosen since it had the best overall scores in security, performance, efficiency, implementation ability and flexibility. Hence chosen as the standard AES (Advanced Encryption Standard) algorithm's a symmetric block cipher that can process data blocks of 128 bits through the use of cipher keys with lengths of 128, 192, and 256 bits. The hardware implementation of the Rijndael algorithm can provide either high performance or low cost for specific applications. in this system are high speed, high reliability, a smaller chip area, and high cost-effective. These will effectively promote the AES algorithm to be used in the terminal equipment's. Hardware security solution based on highly optimized programmable FPGA provides the parallel processing Capabilities and can achieve the required encryption performance benchmarks. The current area-optimized algorithms of AES are mainly based on the realization of S-box mode and the minimizing of the internal registers which could save the area of IP core significantly. This paper presents an idea of integrating AES into the fiestal architecture of DES, embracing advantages from either of the constituent standards. This results in a much more efficient and crack resistant hybrid encryption algorithm. It utilizes a 128-bit cipher key on a 256-bit plaintext to give rise to a cipher text of 256 bits approached its end. With the limitations of DES's 56-bit key and the advent of faster computers, DES could no longer be considered a secure algorithm.

III. DATA ENCRYPTION STANDARD (DES)

Data Encryption standard (DES) is designed and developed by IBM. It's published 1977 by National Institute of Standards and Technology as official standard for unclassified info. A lot of us government regulations refer for DES. Widely adopted by the trade to be used in security products. It may be simply implemented in hardware. Its high speed, up to gigabit/s with special chips. Data Encryption standard (DES) primarily adopted by business for security merchandise. Algorithmic program style for Encryption and decryption method has been finished same key. Data Encryption standard (DES) is a block cipher, with a 64-bit blocks size and a 56bit keys. Data Encryption standard (DES) consists of a16-round series of substitution and permutation. In every spherical, knowledge and key bits square measure shifted, permutated, XORed, and sent through, 8 s-boxes, a group of search tables that square measure essential to the DES algorithmic rule. Decryption is basically a similar method, performed in reverse.

IV. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard (AES) is published 1999 by Independent Dutch cryptographers. Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard re commended by NIST to replace DES. The Advanced encryption standard (AES) algorithmic rule is capable of using crypto graphical keys of 128, 192, and 256 bits to inscribe and rewrite information in blocks of 128 bits. As the AES algorithm may be used with three different key lengths, these three different flavors are generally referred to as AES=>128,192,256.

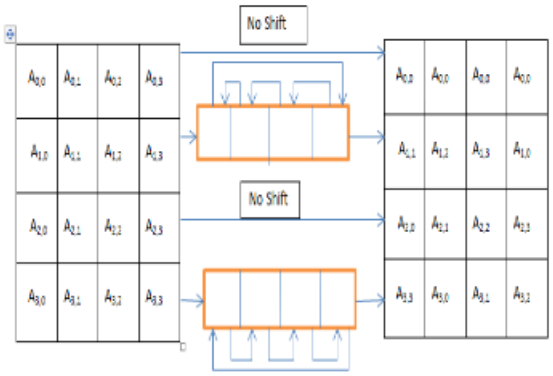


Development flow

AES uses several rounds in which each round is made of several stages. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. .it can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. To provide security AES uses kinds of transformation. Substitution permutation, combination and key adding every round of AES accept the last uses the four transformations.

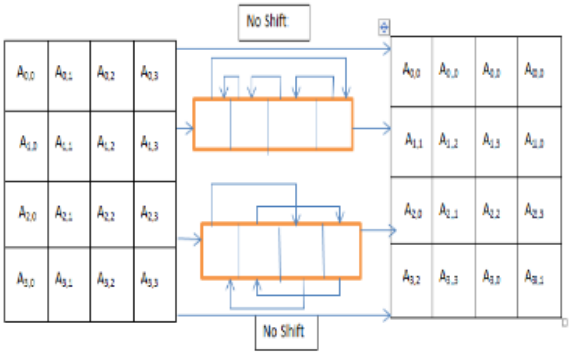
V. II.MODIFYADVANCED ENCRYPTION STANDARD (MAES)

We will modify the AES to be additional efficient and secure approach by adjusting the Shift Row Transformation. Instead of the initial Shift row, we have a tendency to modify it as:Examine the value within the initial row and initial column, (state [0] [0]) is Even or odd. If it's odd, The Shift Rows step operates on the rows of the state; it cyclically shifts the bytes in every row by a particular offset. For MAES, the primary and third rows are unchanged and every computer memory unit of the second row is shifted one to the left. Similarly, the fourth row is shifted by three to the left.



Shift Row Transformation for Odd Rows

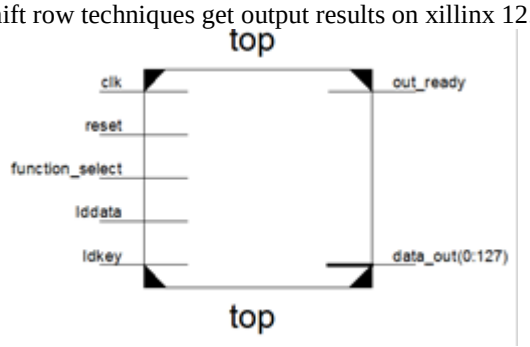
Rows step operates on the rows of the state; it cyclically shifts the bytes in every row by an exact offset. The initial and fourth rows area unit unchanged and every computer memory unit of the second row is shifted three to the right. Similarly, the third row is shifted by tow respectively on to the right.



Shift Row Transformation for Even Rows

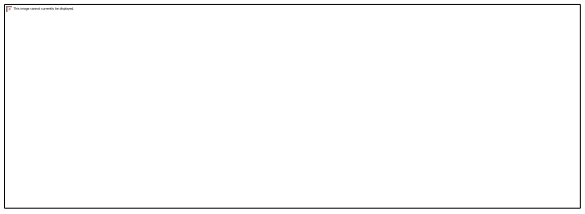
Results:

Design and Implement MAES using shift row techniques get output results on xillinx 12.1 using vhdl on sparten 3e

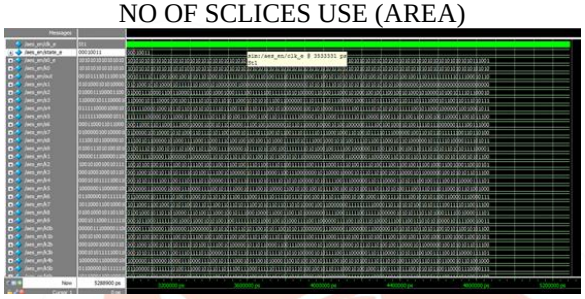


(xc3s500).

MAES ENCODER



NO OF SCLICES USE (AREA)



Final waveform

MAES DECODER

MAES DECODER SLICES (AREA)

As we see that using using modified aes reduce AREA more than 30%

VI. CONCLUSION

In Image Data communication, encryption algorithm plays an important role. My thesis work surveyed the existing encryption techniques like AES, DES and MAES algorithms. Based on my thesis work, it was concluded that MAES algorithm consumes least encryption and decryption time. I also observed that decryption of MAES algorithm is better than other algorithms. Again from the reviewed stuff, I evaluated that MAES algorithm is much better than DES, AES algorithm.

VII. REFERENCES

[1] B. Padmavathi, S. Ranjitha Kumari "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.
[2] Shashi Mehrotra Seth, Rajan Mishra ,"ComparativeAnalysis Of Encryption Algorithms For Data Communication",Ijcst Vol. 2, Issue 2, June 2011 I S S N : 2 2 2 9 - 4 3 3 3 (P R I N T) | I S S N : 0 9 7 6 - 8 4 9 1 (On L I N E).
[3] Arjen K. Lenstra, "Unbelievable Security Matching AES security using public key Systems".
[4] Eman A. Abdel-Ghaffar, Mahmoud E. Allam, Hala A. K. Mansour, and M. A. Abo-Alsoud, "A Secure Face Recognition System",978-1-4244-2116-9/08/$25.00 ©2008 IEEE.
[5] Eustace Painkras, "Efficient Modeling and Implementation of Advanced Encryption Standard using S ystemC",0-7803-8689-2/04/$20.00 Q2004 IEEE.
[6] K. Guo, Y. Xue and C. Li, "An FPGA Implementation of the Advanced Encryption Standard with Composite Field S-box"
[7] Kevin Allison,KeithFeldman,Ethan Mick, "Blowfish"
[8] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994. B. Schneier, Description of a New Variable-Length Key, 64-BitBlock Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings(December 1993), Springer-Verlag, 1994, pp. 191-204.