# SINGLE CHIP IMPLEMENTATION OF MASKED AES WITH QPSK MODULATION FOR LONG DISTANCE TRANSMISSION

**S.Sankar Ganesh[1], J.Jean Jenifer Nesam[2]**

*1.Asst.Professor(s),VIT University*

*Vellore,Tamil Nadu.*

*Email:s.sankarganesh@vit.ac.in*

*Email:jeanjenifer@rediffmail.com*



## ABSTRACT

*The major drawbacks in the construction of wireless devices are security, speed and attack free architecture. In order to overcome these drawbacks, we present AES encryption with masking module that can be capable of providing security and reliability. In addition, we modulate the output data of masked AES. In this paper we introduce the concept of joint encryption, masking and modulation (QPSK) for highly secured, modulated data for high speed and long distance transmission.*

*Key words: AES, QPSK Modulation, masking, highly secured, long transmission.*

## INTRODUCTION

Communication between any two in any corner of this world made easy today. Even communication between each get easier, the security transmission of the message is very important today. Transmitting and receiving the secured data becomes tougher in nowadays. Encryption algorithms are used to protect the data from hackers. There are so many algorithms present like,Triple DES,AES,,,,etc.. Among them AES is very strong encryption standard that will give more secure encrypted data.

Even though AES is very strong algorithm, the hardware implementation sometimes leaks the information. The hackers attack the data in different ways to trace the key or the plaintext. We must protect our information from hackers. There are several research works going on for secure transformation. In our paper we use separate masking module which can be enabled by external enable button. The one thing is long distance transmission; our paper presents the joint modulation. We have a single chip implementation of AES and masking and also modulation.

## INTRODUCTION TO AES

### *A. Explanation of Rijndael Algorithm*

The Rijndael as Advanced Encryption Standard (AES) was published by NIST ( National Institute of Standards and Technology) in 2001[3].The AES is strong security

standard that become effective on May 26, 2002 by NIST to replace DES. The AES uses 128 bit input and the key length is 128 bit, 192 bit or 256 bits. AES can be implemented easily on software and also the hardware. Rijndael algorithm consists of encryption and decryption and key schedule algorithm. The main operations among three parts of Rijndael algorithm have four main operations[10]. They use a) Byte substitution (sub bytes) b) The shiftrows c) Mixcolumns d) Round key adding (Add round key).

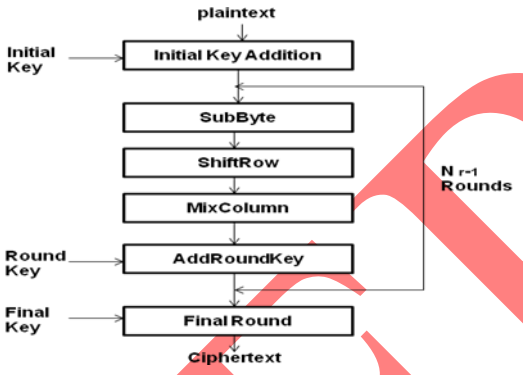


Fig.1. AES Encryption Structure

AES-128 encryption consists of 10 rounds of transmission of the input plaintext for the cipher text. For AES-128 bit the corresponding key length is 128 bits. In this paper only AES-128 encryption scheme with 128 bit key is considered [10][2].

## PROPOSED ARCHITECTURE

The overall architecture can be easily explained by below diagram

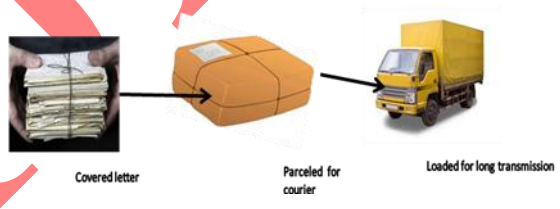


Fig.2. Example for the Proposed Architecture

For example, the written letter is covered by the letter cover and then it will be covered by courier cover then it will load over to the truck for long transmission. The new integrated architecture of masked AES with modulation is done as below block diagram.

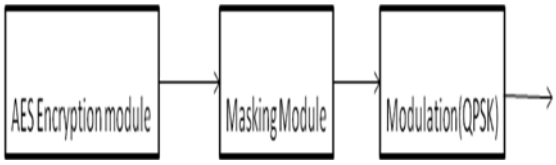


Fig.3. Proposed Architecture

Same can be done in our scheme means, the message information is encrypted by AES then it will be masked with pseudorandom sequence then modulated by QPSK for long signal transmission.

## MASKING MODULE

### *A. Side channel attacks*

A side-channel is any observable information emitted as a byproduct of the physical implementation of the cryptosystem [8]. Possible Side Channels are Power, Time, Faults Electro-Magnetic radiations, Sound, Scan Chains and may many more..

→Timing Attacks→Works by correlating timings of a target machine to those of an identical reference machine with a known key.

→Power Analysis Attack→Analysis the power of the circuit with the reference machine able to find the key. In order to resist the SCA we introduce the PN sequence generation method which is used to mask the actual information to be sent.

### *B. Pseudorandom sequence generation*

The separate module with some internal "AND" operation and shuffler and combiner are used for generating the pseudorandom sequence [5]. We enter 4 bit external input to PN module. By doing internal operation it will generate 128 bit pseudorandom sequence. The outcome of encrypting module is "XOR"ed with this 128 bit PN sequence and produce 128 bit sequence which is differ from the original AES encrypted information. Thus we masked the original data [8].

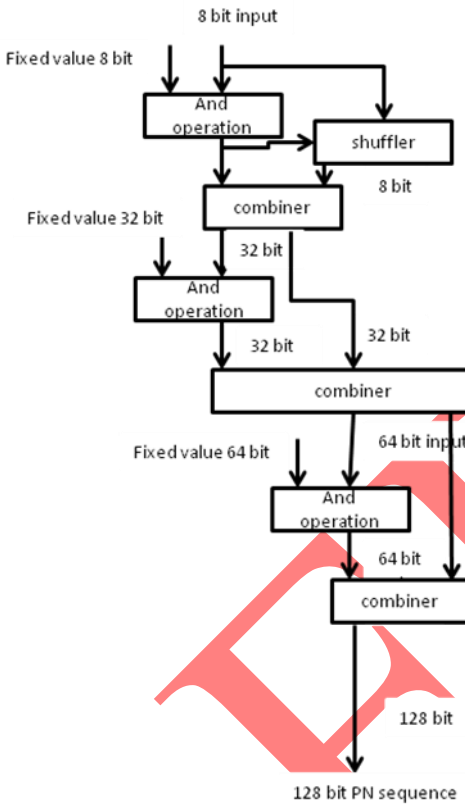


Fig.4. PN Sequence Generator

At the receiver side, another PN module is used to remove the mask and to get the original data. The same 4 bit (input of transmitter side PN module) enter as a PN module[3] input at the receiver side it will generate same 128 bit output again "XOR"ed with masked information gives the required original information.

## MODULATION TECHNIQUE

Modulation means to vary or change. In wireless we first take a signal, say a telephone conversation, and then impress it on a constant radio wave called a carrier. Once done the voice signal varies or modulates this radio wave. The two go together over the air. A voice frequency in the audible or audio range, what we can hear, thus modulates or varies a constant frequency in the radio range, which we can't hear. That's an important point. Modulation makes voice band and radio band frequencies work together. Different modulation techniques, such as A.M., F.M., P.C.M. and so on, represent different ways to shape or form electromagnetic radio waves. In our scheme we use QPSK binary modulation for modulate the encrypted and masked data [7]. In QPSK modulation, transmitter and receiver can transmit and receiving the combination of 2 bit at a time.

*A .Quadrature Phase Shift Keying:-*

This scheme, used by most high speed modems, allows quicker data transfer than FSK. And it gives at least four states to send information. Quadrature phase shift keying changes a sine wave's normal pattern. It shifts or alters a wave's natural fall to rest or 0 degrees. By forcing changes in a sine wave you can convey information. You don't stop or abbreviate the sine wave; you change its shape or angle of attack. Check out the diagram below.

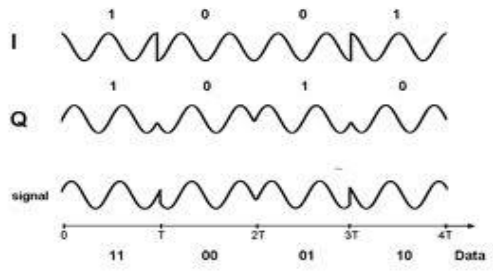


Fig.5. QPSK Waveforms

In our paper, sine, inverse sine, cosine, and inverse cosine might be represented by binary digits 00,01,10, and 11 respectively. The modulation is mainly for the long transmission. The QPSK modulation is done as the below diagram.

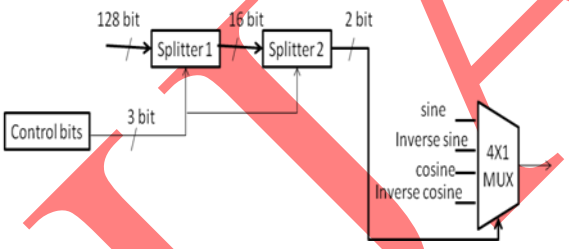


Fig.6. QPSK Modulation Module

The masked 128 bit data is divided into 16 separate 16 bit data then it given to second splitter that will divide the 16 bit data into 2bit data. This output of the splitter2 is given as a selection bit fo4x1 mux. Depending on the selection the corresponding wave will transmit. Here we set sine wave for “00”, inverse sine for “01”, cosine for “10”, and inverse cosine for “11”. In the receiver side all these actions are done in opposite direction. First we demodulate the data. Same PN sequence is generated by applying the bit which is forced in the transmitter side that can be used as re-mask bits. Only the receiver knows the bit only retrieve the data hence we increase the security and then the AES decryption is used to obtain the transmitted message.

## SIMULATION RESULTS and SYNTHESIS RESULTS

*A. Simulation result using Modelsim Altera 6.6d:*

The codes are written by using VHDL language and then is simulated by using Modelsim Altera 6.6d version. The obtain waveform is given below

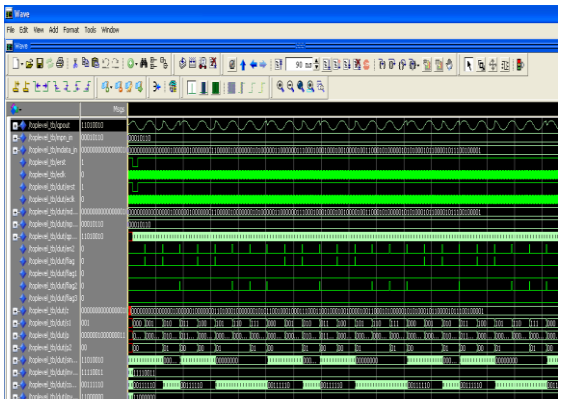

Fig.7. Simulated Waveform of Proposed Architecture

*B.Synthesis result:*

The simulated output then synthesized using ISE 9.2i. The Target Device is Virtex XCV600 BG 560 Speed Grade:-6. The synthesis results shows that all inputs are fitted correctly and all mapping functions and routing functions are done successfully.

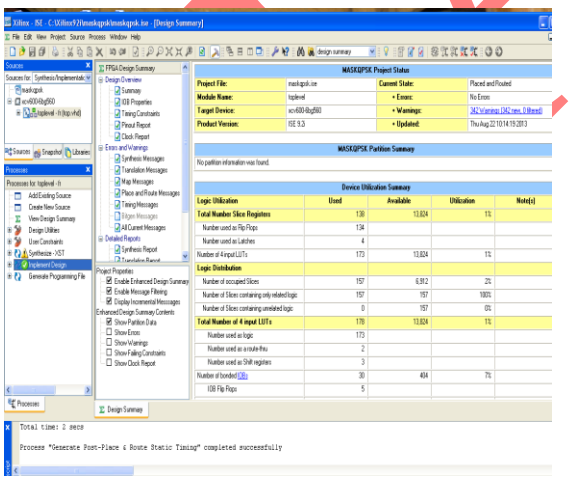

Fig.8. Synthesis Result

*A.* Synthesis Report

The design summary is given in the below table .1.

| | |
|---|---|
| Selected Device : | virtex XCV600 BG 560 |
| Speed grade | -6 |
| Number of Slices: | 99 out of 6912 1% |
| Number of Slice Flip Flops: | 141 out of 13824 1% |
| Number of 4 input LUTs: | 178 out of 13824 1% |
| Number used as logic: | 175 |
| Number used as Shift registers: | 3 |
| Number of IOs: | 146 |
| Number of bonded IOBs: | 31 out of 404 7% |
| Number of GCLKs: | 1 out of 4 25% |
| Clock period | 5.337ns |
| Max frequency | 187.37 MHZ |
| Total memory usage is | 156424 kilobytes |

TABLE.1. SYNTHESIS REPORT

## CONCLUSION

In his paper, we have presented a integrated chip for masked AES with QPSK modulation for high secure and long distance transmission. Our proposed architecture design is simulated by altera 6.6d and implemented Xilinx ISE 9.2i. Thus our implementation runs successfully on the target device virtex xcv600-6bg560 and the internal connection are successfully placed and routed.

## REFERENCE

[1]. D.Canright and Lejla Batina "A *Very Compact "Perfectly Masked" S-box for AES".*

[2] Deamen and Vincent Rijimen "*ASpecification for the AES Algorithm Rijidael".*

[3] Dipwrnabeit Zur Erlangung des Magister grades an der Naturwissenschaftli dhen Fakult at der "*Pseudo Random Number Generation for Cryptographic Applications*" ,march 2003.

[4] Liu Zhenglin,Zang Yonghong, Zou Xuechang, Han Yu, Chen Yicheng "*A High Security and low power AES S-box Full Custom Design for Wireless Sensor Network*" 1-42441312-5/07 IEEE 2007.

[5] Ned Ruggeri "*Principles of Pseudorandom Number Generation in Cryptography"* August 2006.

[6] NIST "*Advanced Encryption Standard (AES)*", NIST,FIPS-197,2001.

[7] Pascal Junod "*cryptographic Secure Pseudo-Random Bits Generation, The Blum-Blum-Shub Generator"* August 2009.

[8] S.Sankar Ganesh, J.Jean Jenifer Nesam, "*FPGA Based SCA Resistant AES S-Box Design"* International Journal of Scientific and Engineering Research,volume4,Issue 4,April 2013.

[9] S.Sankar Ganesh, J.Jean Jenifer Nesam, "*Fully Pipelined High Speed SB and MC of AES Based on FPGA*" International Journal of Engineering and Technology (IJET), ISSN : 0975-4024,Vol 5 No 4 Aug-Sep 2013 .

[10] William Stallings "*Cryptography and Network Security"* Prentice Hall, 3rd ed,2003.