Low Power AES Algorithm Implementation For Wireless Communication

Supratim Saha
Dept. Of E.C.E
TGPCET,Nagpur University

***Abstract*— This paper discusses the efficient usage of the Advanced Encryption Standard (AES) that may be used to correct erroneous errors and its implementation as aerror correction algorithm with a view of lowering the power as a part of secured wireless communication. Our low power AES crypto module has optimized architecture of data encryption unit and key schedule unitwhich could be applicable to wireless sensor networks. We also details low power design methods used to design our low power AES module.**

***Keywords*— AES, Turbo coding,Data transmission,Low power circuitry,Key schedule unit**

I. INTRODUCTION

The Advanced Encryption Standard (AES) has been lately accepted by NIST as the symmetric key standard for encryption and decryption of blocks of data and is widely accepted for error detecting and correction codes,however in wireless networking security system,the need of lowering of power requirements has been on the rise and often regarded as one of the prime requirements of many advances in the industries of today.

Generally sensor nodes are used for many a wireless security purposes and are generally consisting of limited chip size and limited computing power.Inspite of this the whole system can consist different sensor modules,operating systems,microcontroller communication modules and many a peripheral systems.Other than this security issues are another aspect which forces us to use more security systems in order to prevent impersonating,cloning identity related issues and various channel analysis.

Therefore it becomes the need of the hour to strike a balance between lowering the power needs along with the non compromising of security issues and its successful implementation in an efficient way.

This paper aims at developing a reconfigurable environment for successful lowering of power usage and providing wireless network security while using AES algorithm.

II. LOW POWER AES MODULE

The use of codes that are used for correcting errors with AES has been very fruitful a process to overcome data corruption in digital wireless communication channels. Convolutional codes, which can be used to make efficient soft-decision decoding, are widely employed in wireless communication systems.The AES implementation for low power usage can be extremely valuable for many wireless communication systems, such as WiMAX and 3G systems.This can solve lot of security concerns related to wireless communication system.

In a wireless communication system, there are a lot of occasions arising where data corruption is a possible threat and sometimes the possible precautions can compel us to go for security measures which are high end and cost a lot in terms of power managements as well.Another aspect is tha to protect the memories used for storing the expanded key and the state matrix used in AES various codes are utilized and a perfect scenario appears where a module can be efficiently be used to curb the power usage in this process.

III. AES ARCHITECTURE FOR LOW POWER

Most of the wireless communication network systems have limited circuit area and computing power by its nature. A special architectural consideration is needed to design AES algorithm.In this portion we review the characteristics of AES algorithm [5] after which. we describe the features of our low power AES module that we are working on.

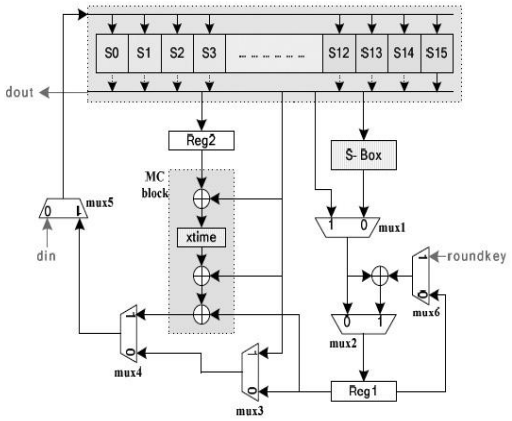

Figure. 1. AES data encryption unit for Low power module in wireless communication

The AES module for low power here works on turbo-code error correction decoding method [4], with N as the number of information bits submitted to turbo-code decoding, comprising the steps of: (a) calculating a forward path metric based on a branch metric after calculating said branch metric for a transition to an adjacent time point; and (b) calculating N bits of soft decision information based on said branch metric, said forward path metric, and a backward path metric after calculating said backward path metric based on said branch metric.compared to other methodologies turbo code error

correction can be utilized in a more compact way and had more chances of meeting the ongoing demands in the industry that is changing its course rapidly and is a very difficult one to cope with in terms if constant changes in the industry.

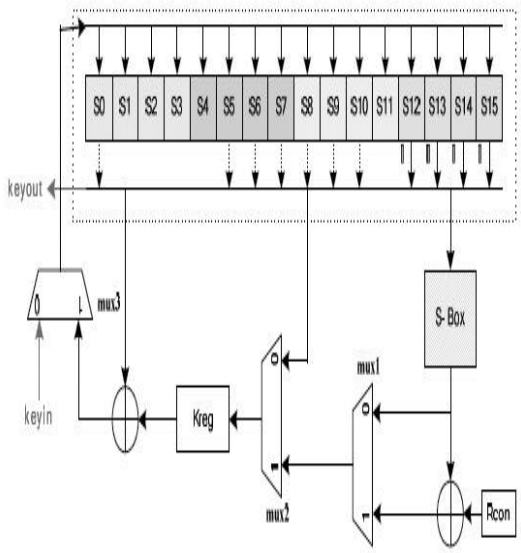

Figure 2. Key schedule unit for low power

Key scheduling is shown in the above figure in an advanced error correction technique in order to achieve the best possible data reception with the fewest possible errors along with fulfilling our goal of lowering the power usage. The basis of turbo coding is used here to introduce redundancy in the data to be transmitted through a channel.

The redundant data helps to recover original data from the received data. In data transmission, turbo coding helps achieve near Shannon limit performance.Lattice provides a Turbo Decoder IP core that is both flexible and compliant with two different standards, 3GPP and CCSDS. 3GPP is widely used in WCDMA and MC-CDMA applications while CCSDS is most commonly found in telemetry and space communications.Lattice also supplies users with a Turbo Encoder core providing users a complete state of the art error correction solution.

Register-based key data memory block loads initial secret key and then stores round key at each iteration of the key generate rounds. The structure of memory and S-box is the same as the one of data processing unit. Round constant generator can be implemented using simple 8-bit shift and rotate register which has initial binary value.Mux1 is a data path selector which selects data in case of either using round constant value or not. Mux2 selects the data path in case of between when it needed to using S-box output and when using key memory data. Mux3 selects data path for key memory's input data. Kreg in figure 2 is 8-bit register used to store intermediate key data during the key scheduling. The key schedule unit can be implemented by 3714 gates and uses 17 clock cycles for single round key generation.

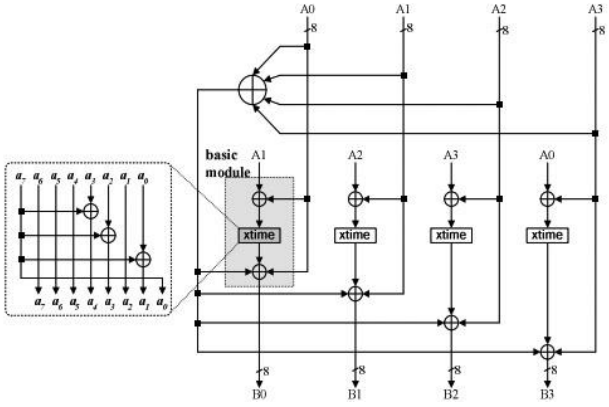

Figure 3. mixcolumn entropy block

The whole process puts much value on the process of interleaving,the main components are four in number and combined they end up generating the error correction code that is implemented in correcting errors present if any in a communication system.

We also optimized the area of MixColumn. The matrix multiplication of MixColumn could be represented as a multiple of 8 in order to process in a more efficient way.we could know that MixColumn could be designed easily using just one basic module which imposes one xtime block, two or three byte-XOR logics and additional data path selector. This idea is depicted in Fig. 3. The basic module of MixColumn is represented by the dashed linepreviously computed LLR to get a new estimate of the LLR for the data. By repeating four times of basic module, MixColumn operation is executed. Xtime module used in MixColumn can be implemented easily with combinations of XOR gates and hard-wired logic shift operations.

From what have discussed above, we could design the architecture of optimized data encryption unit using 16-byte of data memory, one combinational S-box, MixColumn basic module, data path selectors and some 8-bit length data registers used to contain intermediate data.trellis is a form of a state transition table, of the encoder input/output. Based on the data and parity information, the MAP decoder computes the probability of the encoder being in a particular state. Depending on the soft data, parity value and the weight from the previous state, the probability that the data is a '1' or '0' can be computed. The MAP decoder [1] computes the weight for each data symbol in a given block for both the forward and reverse directions. This results in the computation of forward and reverse metrics. Using these two values the probabilities are computed. After the probabilities are determined they are compared and a decision is made. The Turbo Decoder IP core uses the logarithm of the probability to reduce computation; this is known as Log Likelihood Ratio (LLR).The computation

of the probabilities is done iteratively to obtain a reliable result. Once the result is considered reliable, one can make a final decision as to whether the data symbol is a '1' or '0'.

We use two registers, Reg1 and Reg2, to store intermediate state value during round operations and shorten the delay of data paths. During transformation of one byte, the next byte could be read from memory. The transformed data is written to the memory of current reading address. Reg1 used for SubByte, ShiftRow, AddRoundKey and some part of MixCoulmn transformations. Reg2 mainly used for MixColumn operation.Each register could be implemented using 67 gates.Under these circumstances the (G/T) ratio shows signs that the desired result is being approached.

IV . CONCLUSION

We have described about the hardware architecture for low power AES crypto module. The designed low power AES module using optimized architecture of data processing unit and key schedule unit are applicable to security applications which require low power characteristics such as a sensor node for sensor network and ubiquitous computing systems. We have designed our low power AES crypto module using several low power techniques such as architectural optimization, clock gating, operand isolation, synthesis level optimization, and etc. Among applied low power design techniques, clock gating and operand isolation was effective to reduce the switching power of data and key memory and other register units. Using combinational S-box also reduced the operating power. We believe that there are a lot of alternatives and other techniques to reduce operating power if we use more techniques.

From the evident low power consumption brought out by the AES low power module implemented by us,we can claim our low power module can be a valuable prospect for processes involving wireless security along with various constraints regarding resources.

REFERENCES

[1] C. Gehrmann, J. Persson, and B. Smeets, Bluetooth Security.
Artech House, 2004.
[2] B. A. Miller and C. Bisdikian, Bluetooth Revealed.
PrenticHall, 2001.
[3] R. Shorey and B. Miller, "The Bluetooth technology: merits and limitations," in Personal Wireless Communications, 2000
IEEE International Conference on, 2000, pp. 80–84.
[4] A. Satoh, T. Sugawara, N. Homma, and T. Aoki, "High-performance concurrent error detection scheme for AES hardware," in *Proc. CHES*, Aug. 2008, pp. 100–112.
[5] "Error Correction Coding: Mathematical Methods and Algorithms" by Todd k.Moon , June 6, 2005 .
[6] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. Spins: Security protocols for sensor networks. Wireless Networks,8:521-534, 2002.
[7] Abdel-Karim R. Al Tamimi, "Security in Wireless Data Networks".
[8] William Stallings, "Cryptogrphy and network Security principles and practices",2007 pp 134-165.