CHAPTER 2

LITERATURE SURVEY

The literature survey focuses its attention towards AES, particularly to utilize under low power consumption, high security, better performance and improved efficiency. The implementation feasibility in VLSI environment is also studied and analyzed in depth.

2.1 Fault Analysis in AES-CBC Algorithm Using Hamming Code for Space Applications

National institute of standard and technology (2001) presented computer security. Two FIPS publications already prove the modes of operation for two particular block cipher algorithms [60]. Four of these modes are equivalent to the ECB, CBC, CFB, and OFB modes with the Triple DES algorithm (TDEA) as the underlying block cipher. For any given key, the block cipher algorithm of the mode consists of two function that are inverses of each other.

Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat presented (2004) discussed about the Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware [31]. It addressed various approaches for efficient FPGA implementations of the Advanced Encryption Standard algorithm. In implementation of block ciphers, several strategies can produce effective designs. Inherent constraints of FPGAs were taken into account in order to define an efficient methodology. Inside these architectures, the authors proposed algorithmic optimizations for the substitution box, and also efficient combinations between the diffusion layer and the key addition.
Farhadian.A and Aref.M.R (2009) presented efficient method for simplifying and approximating the s-boxes based on power functions [29]. In this paper cipher algorithms, power functions over finite fields and special inversion functions have an important role in the S-box design structure. A new systematic efficient method is introduced to crypt analyze such S-boxes. This method is very simple and does not need any heuristic attempt and can be considered as a quick criterion to find some simple approximations. Using this new method, approximations can be obtained for advanced encryption standard (AES) like S-boxes, such as AES, Camellia, and Shark and so on. Finally as an application of this method, a simple linear approximation for AES S-box is presented.

Akashi Satoh, Sumio Morioka, Kohji Takano, and Seiji Munetoh (2011) presented a Compact Rijndael Hardware Architecture with S-Box Optimization [2]. Encryption and decryption data paths are combined and all arithmetic components are reused. An extremely small size of 5.4 K gates is obtained for a 128-bit key Rijndael circuit using a 0.11-µm CMOS standard. In order to minimize the hard-ware size, the order of the arithmetic functions were changed, and the encryption-decryption data paths are efficiently combined with respect to cell library. Logic optimization techniques such as factoring were applied to the arithmetic components, and gate counts were reduced.

Ashkan Masoomi and Roozbeh Hamzehiyan (2012) presented a new approach for detecting and correcting errors in satellite communications based on Hamming Error Correcting Code [6]. A novel model to detect and correct Single Event Upsets in on-board implementations of the AES algorithm was based on hamming error correcting code. Single Even Upset (SEU) faults occur in the on-board during encryption due to radiation. Some of the AES modes like ECB, CBC, OFB, CFB and CTR performances have been analyzed. From that, CTR mode has been recommended as the optimum choice for satellite applications.
Ramesh Babu, George Abraham and Kiransinh Borasia (2012) presented a Review on Securing Distributed Systems Using Symmetric Key Cryptography [66]. It was used to evaluate the importance of Symmetric Key Cryptography for Security in Distributed Systems. Two symmetric key cryptographic algorithms DES and AES were commonly used. These two algorithms were evaluated on the parameters such as key size, block size, number of iterations. From the literatures reviewed of various implementations and analysis of both the algorithms, it can be concluded that AES algorithm has over-shadowed the DES algorithm in many areas.

Karri, R., Wu, K., Mishra, P., and Kim, Y. (2002) Concurrent Error Detection Schemes for Fault-Based Side-Channel Cryptanalysis of Symmetric Block Ciphers [45]. They presented algorithm level, round level, and operation level CED (Concurrent Error Detection) architectures for symmetric block ciphers. The algorithm was independent and can be applied to almost any symmetric block cipher. The proposed scheme introduced moderate area overhead and interconnects complexity to achieve permanent as well as transient fault tolerance. This approach assumes that the key RAM, comparator, or both encryption and decryption modules simultaneously are not under attack or faulty.

2.2 A Secure Implementation of Nonlinear AES S-Box and Fault Analysis in AES-CM Algorithm Using Hamming Code for Space Applications.

Ross Anderson, Eli Biham, Lars Knudsen (1999) presented a Proposal for the Advanced Encryption Standard [71]. Its design is highly conservative, yet still allows a very efficient implementation. With a 128-bit block size and a 256-bit key, it is as fast as DES on the market leading Intel Pentium/MMX platforms yet we believe it to be more secure than three-key triple-DES. The linear transformations were just bit
permutations, which were applied as rotations of the 32-bitwords in the bit slice implementation. The authors also considered replacing the XOR operations by seemingly more complex operations, such as additions. Finally cognate algorithms with the same structure as Serpent but with block sizes of 64, 256 and 512 bits.

A.J. Elbirt, W. Yip, B. Chetwynd, C. Paar (2000) presented an FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists [27]. Reprogrammable devices such as Field Programmable Gate Arrays (FPGAs) are highly attractive options for hardware implementations of encryption algorithms as they provide cryptographic algorithm agility, physical security, and potentially much higher performance than software solutions. The implementations of each algorithm will be compared in an effort to determine the most suitable candidate for hardware implementation within commercially available FPGAs. A design methodology was established which in turn led to the architectural requirements for a target FPGA. The best speed-optimized implementations were identified for each AES finalist in both non-feedback and feedback modes.

Pawel Chodowiec, Kris Gaj, Peter Bellows and Brian Schott (2001) presented Experimental Testing of the Gigabit IPSec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board [64]. Full implementations of the new Advanced Encryption Standard, Rijndael, and the older American federal standard, Triple DES, were developed and experimentally tested using the SLAAC-1V FPGA accelerator board, based on Xilinx Virtex 1000 devices. Demonstration of a capability to enhance our circuit to handle the encryption and decryption throughputs of over 1 Gbit/s regardless of the chosen algorithm. For Rijndael in the basic iterative architecture, the results for encryption and decryption are different, with decryption slower than encryption by about 13% in experimental testing. The IPSec-compliant encryption/decryption units of the new Advanced Encryption Standard - Rijndael and
the older encryption standard Triple DES have been developed and tested experimentally.

Khoa Vu, David Zier (2003) presented FPGA Implementation AES for CCM Mode encryption using Xilinx Spartan-II. In this paper discusses a possible FPGA implementation of the AES algorithm specifically for the use in CCM Mode Encryption [46]. It investigates the possibility of creating an off-chip AES system for CCM so that the process can be speed up. The AES implementation on the FPGA is a viable solution for improving the speed and processing power of CCM Mode Encryption. A much larger FPGA or ASIC would be preferred, for both encryption and decryption could be implemented as well as some pipelining of processes. Although the design was implemented, it was intended to be interfaced with a micro-controller/microprocessor running the CCM Mode Encryption.

Xinmiao Zhang and Keshab K. Parhi (2004) presented high speed VLSI architectures for the AES algorithm. A novel high-speed architecture for the hardware implementation of the Advanced Encryption Standard (AES) algorithm [84]. Composite field arithmetic is employed to reduce the area requirements, and different implementations for the inversion in subfield GF (2^4) are compared. In order to explore the advantage of sub-pipelining further, the SubBytes/InvSubBytes is implemented by combinational logic to avoid the unbreakable delay of LUTs in the traditional designs. Fully Sub-pipelined encryptor/decryptors using other key lengths can be implemented by adding more copies of round units and modifying the key expansion unit slightly. Expected throughput is slightly lower than the encryptor-only implementations.

top-down, multi abstraction layer approach for embedded security design reduces the risk of security flaws, letting designers maximize security while limiting area, energy, and computation costs. Embedded systems are essentially processor-based devices. Embedded devices pose severe resource constraints on the security architecture in terms of memory, computational capacity, and energy operating under resource-constrained conditions. At the algorithm level, a designer must select or design both cryptographic and application-specific algorithms for implementation on the embedded device.

Joo, M.K., Kim, J.H. and Choi, Y.H., “A fault tolerant architecture for symmetric block ciphers,” in Proceedings of 11th Asian Test Symposium, 2002. (ATS 2002), pp. 212-217, 2002 [43]. Symmetric key encryption algorithm with low-Energy consumption is required to the applicable sensor networks. Though sensor network provides various capabilities, it is unable to ensure the secure authentication between sensor nodes. Eventually it causes the losing reliability of the entire network and many secure problems. In this paper, a solution of reliable sensor networks to analyze the communication efficiency through measuring performance of AES-128 CBC algorithm which is selected by default in sensor networks by plaintext size and cost of operation per hop according to the network scale was proposed. Finally the results from proposed was proved to be better than existing system.

Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., and Piuri, V (2002) presented Concurrent fault detection for a hardware implementation of the Advanced Encryption Standard (AES) [8]. It is very important not only to protect the encryption/decryption process from random faults. It will also protect the encryption/decryption circuitry from an attacker who may maliciously inject faults in order to find the encryption secret key. They presented a parity prediction algorithm which was designed for each of the four round transformations employed by
the Encryption module. Since all byte elements of the output state for each transformation was computed in parallel, they did the same with the output parity bits, and they showed that the proposed scheme leads to very efficient and high coverage fault detection.

Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., and Piuri, V presented Error analysis and detection procedures for a hardware implementation of the advanced encryption standard [12]. They presented two fault detection schemes. The first was a redundancy-based scheme while the second uses an error detecting code. The latter was a novel scheme which leads to very efficient and high coverage fault detection. It was based on the use of parity codes, exhibits very good fault coverage, limited hardware overhead cost, and short detection latency. For single bit faults and multiple bit faults of odd order, it proved that (under reasonable assumptions) the fault coverage of the parity-based detection technique was good compared with the existing one.

Breveglieri, L., Koren, I., and Maistri, P., “An operation-centered approach to fault detection in symmetric cryptography ciphers,” IEEE Transactions on Computers, vol. 56, no. 5, pp. 635-649, 2007 [14]. An operation-centered approach to fault detection in symmetric cryptography ciphers is presented. They proposed a general framework for error detection in symmetric ciphers based on an operation-centered approach. They first enumerated the arithmetic and logic operations included in the cipher and analyze the efficiency and hardware complexity of several error-detecting codes for each such operation. They recommended an error-detecting code for the cipher as a whole based on the operations it employs. The trade-off between the checkpoint frequency and the error coverage was also evaluated.

detection for the advanced encryption standard [83]. In this they presented a new low-cost concurrent checking method for the Advanced Encryption Standard (AES) encryption algorithm. In this method, the parity of the 128-bit input is determined and modified step-by-step into the parity of the 128-bit output according to the processing steps of the AES encryption. For the parity preserving AES steps Shift-Rows and Mix-Column no parity modifications are necessary. The modified parity is compared in any round with the actual parity of the outputs of the round. The method detects technical faults and deliberately injected faults during normal operation.

Yen, C. H. and Wu, B.F., “Simple error detection methods for hardware implementation of advanced encryption standard” [85]. IEEE Transactions on Computers, vol. 55, no. 6, pp. 720-731, 2006. In this they proposed a simple, symmetric, and high-fault-coverage error detection scheme for AES. Although the erroneous bits were diffused in AES, this work used the linear behavior of each operation in AES to design a detection scheme. It is possible to use only one 8-bit register for storing the parities during hardware implementation. This error detection may also be used in encryption-only or decryption-only designs. Because of the symmetry of the proposed detection scheme, the encryption and decryption circuit can share the same error detection hardware. The proposed schemes can be applied in the implementation of AES against differential fault attacks and can be easily implemented in a variety of structures, such as 8-bit, 32-bit, or 128-bit structures.

2.3 Design and Analysis of Nonlinear AES S-Box and Mix-Column Transformation with the Pipelined architecture

LAN MAN Standard committee of the IEEE Computer Society (1999) presented ANSI IEEE STD 802.11 [50]. The medium access control unit in this standard is designed to support physical layer units as they may be adopted dependent on the availability of spectrum. This standard contains three physical layer units: two radio
units, both operating in the 2400–2500 MHz band, and one baseband infrared unit. One radio unit employs the frequency-hopping spread spectrum technique, and the other employs the direct sequence spread spectrum technique. The purpose of this standard is to provide wireless connectivity to automatic machinery, equipment, or stations that require rapid deployment, which may be portable or hand-held, or which may be mounted on moving vehicles within a local area. This service provides peer LLC entities with the ability to exchange MAC service data units (MSDUs). The MAC sub-layer security services provided by WEP rely on information from non-layer 2 management or system entities.

Ramesh Karri, Kaijie Wu, Piyush Mishra, and Yongkook Kim (2002) presented Concurrent Error Detection Schemes for Fault-Based Side-Channel Cryptanalysis of Symmetric Block Ciphers [67]. Straight forward hardware and time redundancy-based concurrent error detection (CED) architectures can be used to thwart such attacks, they entail significant overheads. The proposed techniques have been validated on FPGA implementations of Advanced Encryption Standard (AES) finalist 128-bit symmetric encryption algorithms. Decrease in fault detection latency/increase in area and decrease in fault detection latency/decrease in throughput ratios are more significant between algorithm level CEDs and round level CEDs than they are between round level CEDs and operation level CEDs. A decryption round is realized by applying the inverse of the operations used in the encryption round (s-box, shift-row, mix-column, and key addition) in the reverse order.

Orlando J. Hernandez, Thomas Sodon, and Michael Adel (2005) presented Low-Cost Advanced Encryption Standard (AES) VLSI Architecture for Minimalist Bit-Serial Approach [61]. In this paper a novel minimum cost architecture for the Advanced Encryption Standard (AES) algorithm. By utilizing a true bit-serial design, this architecture can be used for cost sensitive applications that require high security,
such as security system human interfaces, point of sale terminals, and infotainment kiosks. The critical paths in the hardware implementation have shown to be SubBytes, MixColumns, and the decrypt key schedule. The hardware testing phase would reveal the actual delays in algorithm processing. The SubBytes and MixColumns algorithms can also be merged as other implementations have done. With an advanced chip process, the architecture would perform much faster, and the design can be scaled accordingly.

Samir ElAdib and Naoufal Raissouni (2012) presented AES Encryption Algorithm Hardware Implementation Architecture [74]. Resource and Execution Time Optimization. Rijndael algorithm is the new AES adopted by the National Institute of Standards and Technology (NIST) to replace existing Data Encryption Standard (DES). The first factor to be considered on implementing AES is the application. Architecture presented uses memory modules (i.e., Dual-Port RAMs) of Field-Programmable Gate Array for storing all the results of the fixed operations, and Digital Clock Manager (DCM) that we used effectively to optimize the execution time, reduce design area and facilitates implementation in FPGA. The new architecture presented allows the implementation of the AES Rijndael Algorithm using an approach which includes modules memory and lookup tables.

Shylashree.N, Nagarjun Bhat and V. Sridhar (2012) presented FPGA implementations of advanced encryption Standard [76]. AES based on the Rijndael Algorithm is an efficient cryptographic technique that includes generation of ciphers for encryption and inverse ciphers for decryption. Higher security and speed of encryption/decryption is ensured by operations like SubBytes (S-box)/Inv. SubBytes (Inv S-box), MixColumns/Inv MixColumns and Key Scheduling. Extensive research has been conducted into development of S-box /Inv. S-Box and MixColumns/Inv. MixColumns on dedicated ASIC and FPGA to speed up the AES algorithm and to
reduce circuit area. This is an attempt, to survey in detail, the work conducted in the aforesaid fields. The prime focus is on the FPGA implementations of optimized novel hardware architectures and algorithms.

Ewa Idzikowska and Krzysztof Bucholc (2007) presented Concurrent Error Detection in S-boxes [28]. It presents low -cost, concurrent checking methods for multiple error detection in S -boxes of symmetric block ciphers. Some studies of parity based concurrent error detection in S - boxes. The techniques used for error detection in digital circuits are based on adding redundancy to the circuit. It can be relatively small redundancy, a few percent of the circuit area. Parity code based solutions require relatively small increase in the hardware complexity.

Can right, D. and Batina, L. (2008) presented A very compact ‘perfectly masked’ S-box for AES [17]. The key of this proposal was the occurring of side channel attacks such as differential power analysis while implementations of the Advanced Encryption Standard (AES), including hardware applications with limited resources (e.g., smart cards). One countermeasure against such attacks was adding a random mask to the data. This randomizes the statistics of the calculation at the cost of computing mask corrections. The single nonlinear step in each AES round is the S-box (involving a Galois inversion), which incurs the majority of the cost for mask corrections. They finally proposed a compact masked S-box so far, with perfect masking giving suitable implementations immunity to first-order differential side-channel attacks.

Carlet,C., Goubin, L., Prouff, E., Quisquater, M. and Rivain, M., (2012) presented Higher-order masking schemes for S-boxes [18]. The main issue while applying masking to protect a block cipher implementation is to design an efficient scheme for the s-box computations. Actually, masking schemes with arbitrary order
only exist for Boolean circuits and for the AES s-box. Although any s-box can be represented as a Boolean circuit, applying such a strategy leads to inefficient implementation in software. The design of an efficient and generic higher-order masking scheme was hence until now an open problem. They introduced the first masking schemes which can be applied in software to efficiently protect any s-box at any order. They first described a general masking method and introduced a new criterion for an s-box that relates to the best efficiency achievable with this method. Finally they proposed a concrete scheme that aims to approach the criterion.

Gaj, K., and Chodowiec, P. (2001) presented Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays. In this they presented and analyzed five AES final candidates using Virtex Xilinx Field Programmable Gate Arrays [32]. For all five ciphers, they obtained the best throughput/area ratio, compared to the results of other groups reported for FPGA devices. Additionally, they implemented four AES algorithms using full mixed inner- and outer-round pipelining suitable for operation in non-feedback cipher modes. They developed the consistent methodology for the fast implementation and fair comparison of the AES candidates in hardware and found the performance measure for feedback and non-feedback modes of ciphers.

Guurkaynak, F.K., Burg, A., Felber, N., Fichtner, W., Gasser, D., Hug, F., and Kaeslin, H. (2004) presented A 2 GB/s balanced AES crypto-chip implementation [38]. In this they presented a balanced 2 GB/s en-/decrption ASIC realization of the AES algorithm that supports all standard operation modes and key lengths. Rather than optimizing only for throughput, special care was taken to balance the more involved decryption path with that of the encryption path using a number of high-level architectural and register transfer level optimizations. In terms of raw measured
throughput performance for all modes of operation fast core compares fairly well to other published AES implementations.

Hodjat, A., Verbauwhede, I. (2006) presented Area-Throughput Trade-Offs for Fully Pipelined 30 to 70 Gbits/s AES Processors [39]. In this the area-throughput trade-off for an ASIC implementation of the Advanced Encryption Standard (AES) was presented. Different pipelined implementations of the AES algorithm as well as the design decisions and the area optimizations that lead to a low area and high throughput AES encryption processor was also presented. Loop unrolling and inner and outer round pipelining was used to reduce the critical path and increase the maximum throughput. By using a pipelined design of the composite field implementation of the byte substitution phase of the AES algorithm, the area was reduced up to 35 percent. Also, by designing an offline key scheduling unit for the high speed AES processor, an area reduction of an extra 28 percent is achieved. Therefore, the total area cost of the final architecture is reduced up to 48 percent without any loss in throughput. The area efficient AES architecture with throughput rate of over 30 Gbits/s is used in the counter mode of operation for the encryption of data streams in optical networks.

Hodjat, A., and Verbauwhede, I. (2004) presented A 21.54 Gbits/s fully pipelined processor on FPGA [40]. In this they presented the architecture of a fully pipelined AES encryption processor on a single chip FPGA. By using loop unrolling and inner-round and outer-round pipelining techniques, a maximum throughput of 21.54 Gbits/s was achieved. A fast and area efficient composite field implementation of the byte substitution phase was designed using an optimum number of pipeline stages for FPGA implementation. A 21.54 Gbits/s throughput was achieved using 84 Block RAMs and 5177 Slices of a Virtex II-Pro FPGA with a latency of 31 cycles and throughput per area rate of 4.2 Mbps/Slice.
Mangard, S., Pramstaller, N., and Oswald, E. (2005) presented successfully attacking masked AES hardware implementations [53]. The chip features an unmasked and two masked AES-128 encryption engines that can be attacked independently. In addition to conventional DPA attacks on the output of registers, they mounted attacks on the output of logic gates. Based on simulations and physical measurements the proposed scheme showed that the unmasked and masked implementations leak side-channel information due to glitches at the output of logic gates.

Cheng Wang and Howard M. Heys, presented a Pipelined S-Box in Compact AES Hardware Implementations [20]. In this area and speed performance of applying a pipelined S-box to compact AES hardware implementations was examined. A new compact AES encryption hardware core with 128-bit keys was proposed. The proposed design employs a single 4-stage pipelined S-box that is shared by the data path operation and the key expansion operation. Compared with the previous smallest encryption-only ASIC implementation of AES, The new design was featured with a 4-stage pipelined S-box. The implementation results show that, compared with the previous smallest encryption only AES hardware implementation.

M.Gnanambika S.Adilakshmi, and Dr.Fazal Noorbasha, presented AES-128 Bit Algorithm Using Fully Pipelined Architecture for Secret Communication [33]. In this they proposed an efficient method for high speed hardware implementation of AES algorithm. Mainly the degradation effected the Sub Byte transformation in various ways. These methods of implementation was based on combinational logic and was done in polynomial bases. In the proposed architecture, it was done by using composite field arithmetic in normal bases. In addition, efficient key expansion architecture suitable for 6 sub pipelined round units was also presented.
Hyeopgeon Lee, Kyounghwa Lee, Yongtae Shin, presented Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs [41]. In this they proposed the solution of reliable sensor networks to analyze the communication efficiency through measuring performance of AES-128 CBC algorithm which was selected by default in sensor networks by plaintext size and cost of operation per hop according to the network scale. They measured the encryption and decryption operation time by the plaintext size. As a result, scale of the sensor networks grows, the delay doubled. And energy consumption has also increased accordingly.