Efficient Kernel Template AES Algorithm to Minimize Power Consumption and Maximize Security in Low Power Application

V.Nandan, R. Gowri Shankar Rao

Abstract: Cryptography involved in offering of secure data by generation of secret key through encryption process. At present, almost every applications require security scheme due to increased threats. Low power applications are limited to power sources where incorporation of attacks leads to certain challenges in terms of reduced throughput, data loss and increased power consumption hence it is necessary to adopt effective security scheme for low power application. Generally, in power circuits advanced encryption standard (AES) is incorporated which is defined as S-box. This substitution box is designed by 2 transformations (i.e) inversing the multiplication part in Galois field directed with modified affine transformation. The limitation of S-Box is more time and power consumption. In this paper, proposed a kernel based AES scheme for improving the performance of low power application. The proposed Kernel approach uses logic gate design with cipher text operation. The Kernel AES technique is implemented in CMOS devices with 45nm standard cell technology. Results obtained for proposed Kernel-AES approach provides reduced power consumption rate of 28.5A which is comparatively less than conventional AES technique.

Keywords— Cryptography, XOR, Kernel, AES, Cipher text

I. INTRODUCTION

At present cryptography is considered as major concern for every technological aspects. In cryptographic devices physical properties involved in extraction of secret information. For effective prevention of low power application from several attacks cryptographic technique need to be implemented. The implementation of attack in the circuit leads to leakage of information and leakage of information. Information leakage in circuit increases utilization of heat, timing, power and electromagnetic field. Attacker able regain information through the processed devices in form of ciphertext and plaintext while attackers focused on cryptographic key. Cryptography technique involved in provision of secure and protection for plaintext by means of secret key. This secret key has been generated in the encryption process also known as cipher textting. Cryptography has been widely adopted in vast fields such as mobile handsets, military, banking and smart cells [1]. The major of the application uses Advanced Encryption Standard (AES) for cyber security for improving adaptability. Even though AES subjected to side-channel attack due to inbuilt substitution box [2, 3].

For Galois field (2m) involves process of substitution permutation network and fiestel architecture with arithmetic function also known as substitution function. In cipher application inverse process has been considered as modern application. Few standard AES cipher operation adopted inversion of GF(2)8 and the affine transform GF(2)8. Due to light weight process AES algorithm has been adopted in several cryptography application process [4]. In other hand, circuit design involved in construction of functions of heuristic approach. Those approaches are minimal complex with exponential characteristics with calculation of time and inbuilt components. This methods are involved in construction of minimal budget components. Heuristic method involves several operation such as matrix, arithmetic and complex function.

In low power application it is necessary to minimize power utilization level but those are in IP construction level. In this IP based construction power levels are build at transistor level. Through analysis of power levels in low power application now researchers focused towards gate level power optimization techniques [5]. In this scenario adoption of AES algorithm is complex for achieving desirable throughput, clock speed and assists in library due to arrangement complexity, scheduling and dynamic nature. Another challenge associated with AES circuit is calculation of power utilization hence in existing researches it is suggested that segments of sub-bytes which is S-box provides complete power utilization of low power applications. The S-box uses clock those are smaller in nature since it is constructed through folding circuit several times. The folding of circuit causes minimal impact over minimal energy utilization. In existing reduction of power is still challenging hence few researchers focused on development of block ciphers for prevent attack and reduce energy consumption rate [6, 7].

In this paper, kernel based AES cryptography technique modeling is implemented for efficient performance of low power applications. The proposed technique is implemented in CMOS devices with 45nm standard cell technology. In first step, designed as simple logic gates for CMOS technology. In next step, Kernel based technique is implemented integrated with AES approach for improving security in low power application specifically for smart cards, RFID tags and microcontroller.
Simulation results demonstrated that proposed approach effectively reduces the power consumption level significantly compared with existing cryptography technique.

II. RELATED WORKS

For sensing amplifier design is constructed based on the various logic wave dynamic, marking logic through pre-charge [8] switching logic of dual-rain approach [9] and half-buffer weaker condition [10]. Among this sensing amplifier is considered as logic design with minimal characteristics of transformation acquisition regionally. This circuit subjected to limitation of complex design. Yang Jun et al., [11] introduced the methodology that minimize the hardware complexity because of its fewer usage of resources for hardware and more cost. It includes both key expansion & encryption models. Xinniao Zhang et al [12] exhibited different methodologies for proficient equipment execution of the AES calculation. They streamlining strategies dismiss shall be isolated into 2 classes: compositional advancement & algorithm based enhancement.

Archna Garg et al [13] presented an effectual field programmable gate array based AES structure. The efficiency is done by designing 2 structures namely, basic AES & entire pipeline based AES. Both these structures are applied in Hardware Description Language. The cryptograms had remained manufactured by means of Xilinx ISE software with Virtex three Field Programmable Gate Array device. Parameters such as max(pin), delay, clk_delay, slice FFs are taken into account for comparison purpose. M. komala subhadra et al [14] recommended a productive FPGA execution of cryptogram utilizing Hardware Description Language. An AES encrypt is structured &executed in FPGA. An AES decrypt is additionally planned & coordinated by AES encrypted to produce occupied useful AES cryptogram.

Bertoni et al. designed the architecture and that is best in AES substitution box implementation architecture [15]. The circuit design is expected to be very small while taking the critical path architecture and hence it induces less signal when there is changes in the input. Nevertheless an enterprise occasioned with truncated energy consumption, the situation of the extent is around 3epoch postlargest that of the untainted CFA effort. Tuan Anh Pham et al.[16] concluded that the implemented algorithm uses the 277 logic element and provides 5.88mw energy dissipation. Some techniques were developed to decrease the controlingesting i.e.1-hot coding, timepiece gating. Here, AES algorithm implemented on Altera Cyclone II EP2C672C6. The algorithm was implemented on 8-bit architecture. Hassan Anwar et al.,[17]suggested that Media access control layer (MAC) had the capability to function on altered frequencies &affords elasticity. Algorithm was implemented with 32-bit processor. The 2 processor were used i.e. general purpose and crypto co-processor. Use of crypto processor provides the quantity of 58Gbps, expectancy of 240ns &least energy feasting about 76mw at frequency of 553MHZ.

Drolet [18] described the usage of practical reliable rate (PRR) by mathematically calculating the polynomial range of xn+1 this design makes the circuit as simple as possible for arithmetic calculations. Rudra et al., [19] discussed the importance of arithmetic calculations based Galois field copulation purpose of compact delivery in hardware architecture. Satoh et al., [20] proposed finite Galois field architecture of GF (28) which is represented as GF(22)(2)in terms of composite field. Apart from this the gate based pass transmission (GPT) are enchanted with logical calculations of substitution bon. This will results in compact architecture of designing substitution box and lower power consumption. Tellich et al., [21] constructed 0.25mm CMOS technology by the rebuilt way of positive polarity reed-muller (PPRM) using substitution box. The box constructed is lower power consumption of fielding function. The results showed that this design is efficient to operate in low voltage technology. Ali akbars et al., [22] designed an authorization raised matrix transform method using asynchronous multicores processor (AMP) to obtain letter throughput of securing the AES counters mode. The proposed processors contains for features. The final result shows that the final throughput is about 13.54Gbps with the encryption rate of 8.32Gbps and makes the speed in better way.

III. PRELIMINARIES

This method is appropriate for the inbuilt multipliers whereas the XNOR tree based architecture is chosen for the partial products performance. For the generation of partial products 1 bit input operand is doing AND operation with m-bit process to construct the multipliers. In our work a serial digital multipliers is used along with the AND blocks are equated with d for every block rate is m for 2 input AND gates. Another option for AND gate chosen is NAND- NOT gates with CMOS technology. In this any 2 input AND gate is being implement with 6 numbers of transistors (i.e 4 for NAND and 2 for inverter operation). Here, the properties of XOR is considered and then it is implemented in AND gate based NAND gates. As seen in the below figure the structure of multipliers, the output and AND blocks in the summation part are bit wise XNOR by XNOR tree.

Figure 1: Construction of Digital Logic Gates
The designed structure with above mentioned instructions has to be implement in 180nm CMOS technology. Moreover it will be further compassed with existing XNOR topologies. The simulations are done by the testing platform within the parameters of delay for dissipated power. The voltage supply is about 0.6-1.2v and the capacitance rate of 50F with throughput rate of 500MHZ. The reason for under micro based CMOS is that more manufacture efficient and lowered clock frequency. The frequency rate with total power is enhanced by the cost effective manner. Moreover, the fraudulent attacks makes complex along with optical glitch operation. Some countermeasures are needed to protect the attacks with the inbuilt sensor rate of voltage, light of clock. This seems to be further exist with chip based structure.

A. Proposed Kernel - AES approach

Kernel function involved in designing probability density function (PDF) for detection of data. For detection of attack function of kernal is combined with PDF estimation with similar point xᵢ. The kernel function is defined as k(.) [23]:

\[ f(x) = \frac{1}{nh} \sum_{i=1}^{n} k \left( \frac{x - x_i}{h} \right) = \frac{1}{n} \sum_{i=1}^{n} h_i \left( x - x_i \right) \]

Where, hᵢ is denoted as circuit power

\[ f(x) = \frac{1}{n[H]} \sum_{i=1}^{n} k \left(H^{-1} (x - x_i)\right) = \frac{1}{n} \sum_{i=1}^{n} h_i \left( x - x_i \right) \]

where H is a d × d bandwidth matrix composed of elements hᵢⱼ, 1≤i, j≤d. The kernel function incorporates different mathematical function such as cosine, Gaussian and Epanechnikov. The kernel function involves arbitrary function in which it is observed that minimal difference obtained for data fitting and function [24]. The kernel based traces are performed with each set k with different sub key k ∈ [0, k−1] in which generated vector are performed using different sub keys. In which traces of M are obtained from target devices using unknown key and plaintexts.

B. Encryption Process

In this target circuit attacker focused on entire circuit in this first block considered for attack is S-box which incorporates cipher PRESENT [25]. The structure of S-box is presented in below figure 2, this block contains S-box which perform XOR operation of 4 - bit and 4 - bit register count of three.

\[ \text{Ciphertext} = \text{Key} \oplus \text{Sbox(Plain text)} \]

In the above diagram sbox(.) denoted as function of S-box. This structural circuit can be mimic through structure of iteration count where attacker focused on last cipher block round where value lies in intermediate location is stated as “plaintext”. This labels are performed with cryptographic function of kernal and AES and last round is XORED. The generated cipher block contains periods of 8 clock for performance of complete encryption process. In this, 4-bit plaintext is encrypted and shifted through shift register of 4 clock periods. At last 4 cycle’s multiplexers perform register parallel output operation with generation of ciphertext of 4-bit with clock output.

IV. EXPERIMENTAL RESULTS

The proposed kernel based encryption mechanism is implemented using FPGA system with direct testing process. For analysis Xilinx is evaluated through pipelined approach of Xilinx ISE system. Evaluation is examined using 180nm CMOS technology for low power applications. The designed approach considers gate level of 180nm using standard cell. The parameters considered are provided in following table 1.

| TABLE 1: DESIGNED PARAMETERS |
|-------------------------------|
| **Factors** | **Configuration/ Value** |
| Software | Xilinx |
| Technology | CMOS |
| Gate level | 180nm |
| Voltage | 1.5 Volt |
| XOR Gate | 4 -bit |
| Register | 4-bit |

For the designed Kernel-AES approach evaluation is performed through comparison of different approaches specifically power consumption level. The comparison of level is presented in design of various AES technology for various power consumption level. The below table 2 provides the comparative analysis of different CMOS technology.
TABLE 2 COMPARISON OF CRYPTOGRAPHY

| Techniques                        | Encryption | Decryption | Power Consumption |
|----------------------------------|------------|------------|-------------------|
| 692-nW (AES) on a 0.13- m CMOS   | 450 MHZ    | 350 MHZ    | 45.5              |
| 65 nm AES core                   | 120 MHZ    | 170 MHZ    | 35.5              |
| 180nm CMOS with XNOR tree        | 250 MHZ    | 270 MHZ    | 32.5              |
| 180nm CMOS with Kernel-AES       | 280MHz     | 300MHz     | 28.5              |

Figure 3 Circuit diagram of AND gate using static CMOS logic.

For AND gate design, PMOS_1 and PMOS_2 (Inputs ‘a’ and ‘b’) are coupled in parallel and NMOS_1 and NMOS_2 are connected in series and both are linked in series as shown in Figure 3. The output of this combination is given to CMOS inverter for AND operation as shown in Figure 3.

Figure 4 Circuit diagram of XOR gate using static CMOS logic.

Construction of XOR gate using static CMOS technique is shown in the Figure 4. The XOR gives the sum of two 1 bit numbers. EXOR Gate can also be designed using other gates. For designing a EXOR gate only 4 NAND gates are required also if we want to design EXOR gate using NOR gates only then only 5 gates are required to yield an EXOR gate.

Low power AES cryptography core with a small S-box and an improved digit-serial Galois field transformation basis multiplier. The initial AES step, which is Add-RoundKey between the block and the key, is performed during the loading with the XOR gate in the input of the byte permutation unit. After ten rounds of operation the ciphertext block can be unloaded byte by byte from the output port data_out. As round-keys overwrite the encryption key, it must be resupplied to the core along with a new plaintext block.

Figure 5 Kernel-AES Key Performance

Since histograms are non-parametric and do not pose any assumption on characteristics of the observed PDF, we use histograms to characterize the trace data and plot the results in order to numerically analyze the difference between Gaussian and kernel modeling. We reproduce both phases of the template attacks. That is, we take the profiling traces and compute the MISE between the histograms and the profiling results (Gaussian and kernel), then we model the target traces using Gaussian and kernel, and compute the MISE between the modeled target traces and the modeled profiling traces. We do this to determine how close the derived Gaussian and kernel model are from the histogram in the profiling phase. Note that strictly computing the MISE requires a closed-form equation of functions f and g. However in a nonparametric fitting problem, we are not able to derive the a priori PDF without any assumption of the original distribution, hence we are using histograms to estimate the MISE. To ease the process of our analysis, we work on the projected traces of one specific key, but the conclusion holds for all other keys since the distribution of different key sets are very similar.

Figure 6. Variation of key
Overall the kernel method outperforms the Gaussian approach in fitting the data since the general distribution is not Gaussian-like, despite the fact that Gaussian has less error in fitting the attack set.

V. CONCLUSION

Cryptography has been widely emerging field for almost all application since it subjected to several security concern. The attacks in low power application causes several challenges in terms of higher power consumption level, data loss, voltage variation and reduced throughput. Further low power applications are subjected to limited power sources this put another challenge over the application. This paper developed a Kernel based AES cryptography technique for low power application. The developed scheme is based on development of cipher text to protect data with reduced power consumption level. Kernel-AES technology is implemented and tested in CMOS technology. Analysis of proposed Kernel-AES exhibits reduced power consumption level compared to conventional AES technique.

REFERENCES

1. W. Rankl and W. Effing, Smart Card Handbook. Honoken, NJ: Wiley, 2003.
2. S. B. Ors et al., “Power-analysis attack on an ASIC AES implementation,” Proc. ITC, vol. 2, pp. 546-552, Apr. 2004.
3. P. C. Kocher et al., “Differential power analysis,” Proc. Annu. Int. Cryptology Conf. on Advances in Cryptology, pp. 388-397, 2010.
4. Canright, D.: A very compact S-box for AES. In: 7th International Workshop on Cryptographic Hardware and Embedded Systems (CHES). Lecture Notes in Computer Science, vol. 3659, pp. 441–455. Springer. (2005)
5. V. Fischer et al, "Two methods of Rijndael implementation in reconfigurable hardware,"IEEE Journal of Solid-State CircuitsVol. 2162, pp. 81–96, 2011
6. S. Chari, J.R. Rao, P. Rohatgi, Template attacks, in: Cryptographic Hardware and Embedded Systems-CHES 2002, Volume 2523 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2002, pp. 13–28.
7. J.Xu, Heyse,M., “Kernel-based template attacks of cryptographic circuits using static power",Integration, the VLSI Journal, 2019, https://doi.org/10.1016/j.vlsi.2019.01.004.
8. Popp et al., “Masked dual-rail pre-charge logic: DPA-resistance without routing constraints,” Proc. CHES, pp. 172-186, 2005.
9. Z. Chen et al., “Dual-rail random switching logic: A countermeasure to reduce side channel leakage,” Proc. CHES, pp. 242-254, 2006.
10. S. Moore et al., “Balanced self-checking asynchronous logic for smart card applications,” J. of Microprocessors and Microsystems, vol. 27, no. 9, pp. 421-430, Oct. 2003.
11. Yang Jun Ding Jun Li Na GuoXiyong “FPGA-based design and implementation of reduced AES algorithm,” EEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 25, no. 2, pp. 402–415, 2017.
12. Xinniao Zhang and Keshab K. Parhi “Implementation Approaches for the Advanced Encryption Standard Algorithm” International journal on Application-specific Systems , Architectures and Processors IEEE 2002.
13. ArchnaGarg et al, “Efficient Field Programmable Gate Array Implementation of Advanced Encryption Standard Algorithm using VHDL”, International Journal of Engineering Trends and Technology (IJETT) - Volume 4 Issue 9, pp. 3956-3961, September 2013
14. M. komalasubhadra et al, “Advanced Encryption Standard - VHDL Implementation”, International Journal For Technological Research In Engineering, ISSN (Online): 2347 - 4718, Volume 1, Issue 3, pp.132-137 November – 2013
15. G. Bertoni, M. Macchetti, L. Negri, and P. Fragneto, “Power-efficient asic synthesis of cryptographic boxes,” in Proceedings of the 14th ACM Great Lakes Symposium on VLSI, ser. GLSVLSI ’04. New York, NY, USA: ACM, 2004, pp. 277–281
16. Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu “Area and Power optimization for AES encryption module implementation on FPGA” International journal on Automation & Computing, Loughborough University, Leicestershire, UK, 8 September 2012
17. Hassan Anwar, Masoud Daneshshtalab, Masoumeh Ebrahimi, Juha Plosila, Hannu Tenhunen “FPGA Implementation of AES-based Crypto Processor”, IEEE vol-37 pp668-473, 2013.
18. Drolet, G.: A new representation of elements of finite fields GF(2m) yielding small complexity arithmetic circuits. IEEE Transactions on Computers Vol. 47(9), pp. 938–946. (2017)
19. Rudra, A., Dubey, P.K., Julta, C.S., Kumar, V., Rao, J.R., Rohatgi, P., 2001. Efficient Rijndael encryption implementation with composite field arithmetic. LNCS, 2162: 171-184
20. Satoh, A., Morioka, S., Takano, K., Munetoh, S., 2001. A compact Rijndael hardware architecture with S-Box optimization. LNCS, 2248:239-254.
21. Tillich, S., Feldhofer, M., Großschädl, J., 2006. Area, delay, and power characteristics of standard-cell implementations of the AES S-Box. LNCS, 4017:457-466. [doi:10.1007/11796435_46]
22. Ali Akbar Pamun, Weng-Geng Ho,” A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor” IEEE Transactions on Information Forensics and Security, Year: 2019 Volume: 14 , Issue: 4 Pages: 1023 - 1036
23. D. W. Scott, S.R. Sain, 9 - multidimensional density estimation, in: C. Rao, E. Wegman, J. Solka (Eds.), Data Mining and Data Visualization, Vol. 24 of Handbook of Statistics, Elsevier, 2005, pp. 229–261. https://doi.org/10.1016/S0169-2013(05)28128-9
24. T. Schneider, A. Moradi, F.-X. Standaert, T. Günaysu, Bridging the gap: advanced tools for side-channel leakage estimation beyond Gaussian templates and histograms, in: Conference on Selected Areas of Cryptography (SAC 2016), Volume 10532 of Lectures Notes in Computer Science, Springer Cham, 2017, pp. 58–78, https://doi.org/10.1007/978-3-319-69453-5_4
25. Y. Yano, K. Iokibe, Y. Toyota, T. Teshima, Signal-to-noise ratio measurements of side-channel traces for establishing low-cost countermeasure design, in: 2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), 2017, pp. 93–95, https://doi.org/10.1109/APEMC.2017.7975433.