Hybrid wireless crypto processor using FPGA

[1]Kavitha S Patil, [2]Veeresh Basavaraj Hatti, [3]Dr.Indrajit Mandal

[1]Asst Professor, [2] Asst Professor, [3]Professor
[1]Department of Information Science and Engineering,
[1]Atria Institute of Technology, Bengaluru, India

Abstract: **Network security is concerned with the protection of network resources against alteration, destruction and unauthorized use, cryptography and encryption are most critical components of network security. There are many algorithms to protect the sensitive data that is sent on the communication media. Implementing this cryptographic algorithm on software platform will overburden the server. To offload the server from cryptographic operations a lot of efficient hardware implementation of AES are available in open literature on ASIC and FPGA platforms. In modern technology, FPGAs are equipped with some special embedded features to achieve high performance design and density. These embedded features to be used efficiently to enhance the performance in terms of both area and speed. Here we propose hardware efficient Hybrid Wireless Crypto Processor (HWCP) which combines two block ciphers such as enhanced advanced encryption standard (AES) and side-channel resistant authenticated encryption with masking (SCREAM). This proposed HWCP system maximizes the security via increasing the complexity of cracking keys.**

***IndexTerms*- Cryptography, Cryptographic operations, AES, FPGA, SCREAM, HWCP**

Introduction

With technological evolution of computerized systems, security and confidentiality have become one of the main concerns for these systems to avoid frauds. Cryptography plays a vital role in this regard to provide privacy, authentication and integrity protection. Nowadays, cryptography is largely used in cellular phones, cable/sat TV broadcasts, radio modems, smart cards, ATM networks, garage door openers, and online banking etc. Advanced encryption standard (AES) algorithm [1] is one of the most popular and widely used algorithms for symmetric key cryptography to protect sensitive data.

A lot of efficient hardware implementations of AES are available in open literature on both Application Specific Integrated Circuit (ASIC) [2–5] and FPGA [6–9] platforms. FPGA platforms are ideal for the implementation of cryptographic algorithms. They are reconfigurable that give both time and cost effective solutions as compared to ASICs, that require largest development time and are expensive [10]. In addition to this, FPGAs also provide far better speed performance than software implementations and at the same time can be re-programmed on the fly to store updated encryption standard. Modern generations of FPGA apart from LUTs are now equipped with special embedded features such as Multi-mode Clock Manager (MMCM) and BRAM for the implementation of high-density and high performance designs. An active area of research in optimization of crypto-system on FPGAs focuses not only to use these new embedded features of FPGA but how efficiently and effectively these features are to be used in order to enhance the performance of these crypto-system in terms of both area and speed [11,12].

For efficient implementation of AES on FPGA, two Look-Up-Table based approaches exist; S-box and T-box. In these approaches, all the computational complexities of most critical transforms of AES are replaced by a simple Look-Up-Table. But encryption and decryption based on these Look-Up-Tables are not only memory intensive but also asymmetric in nature due to AES operations and sequence of transformations in encryption and decryption. Therefore in most of these Look-Up-Table based AES implementations [7–9, 13], encryption and decryption cores are implemented separately and occupied considerable amount of BRAM resources on FPGA. So there is a need to design a unified AES encryption and decryption module to minimize BRAM resources and also to efficiently utilize full memory space of 32 Kb BRAM available in new generations of FPGA devices. The designs target maximizing speed, minimizing area or achieving a trade-off between speed and area, by means of techniques such as loop unrolling, pipelining and data path word length customization. The multiple encryption algorithms are combined to form new security scheme, which screw something up than to get any meaningful security gain with little bit tricky. In hybrid system, modern ciphers appear to be effectively unbreakable; if that's correct, multiple encryption is possible and it is required. For example, KEM works just like a public key encryption scheme, except that the encryption algorithm takes no input other than the recipient's public key. A secure KEM, combined with an appropriately secure symmetric-key encryption scheme, yields a hybrid encryption scheme which is secure in the sense of IND-CCA [14].

II. RELATED WORKS

The implementation of the cryptographic algorithm in hardware has been carried out since past few years. Several architectures have been proposed to implement the encryption algorithm by different authors.

Priya *et al.* [15] have proposed efficient structural architecture for AES Encryption process to achieve high throughput with less device utilization. Breakable and controllable structures for main AES blocks at the gate level are designed and used here. The control unit using high speed combinational logic circuit is designed to control the AES structural architecture. In addition Encryption process Mix-columns transformation is modified to reduce the hardware complexity. The five stage sub pipelining is introduced in AES MUX based S-Box with six pipelining stages in AES encryption process to increase throughput further.

Kundi *et al.* [16] have presented unified FPGA based AES encryption/decryption design with symmetric ST-Box structure. This structure fully utilizes high capacity (32 Kb) Block RAM (BRAM) by accommodating all encryption and decryption lookup operations within a single BRAM in the form of single integrated Look-Up-Table. This design also caters the inherent asymmetric nature of encryption and decryption coefficients for a unified hardware. Further the symmetry at BRAM output is maintained to use a single XOR network during both encryption and decryption. The performance of design is enhanced by duty-cycle based accessing technique. It explores the switching capabilities of BRAM and effectively minimizes the ON time of BRAM by changing duty-cycle of input clock. This enables us to access single BRAM 4 times per clock. Effectiveness of design is further measured by implementing it, in both iterative and pipelined architectures.
Nedjah *et al.* [17] have proposed efficient pipelined hardware implementation of AES-128; it is used in almost all network based applications to ensure security. The core computation of AES, which is performed on data blocks of 128 bits, is iterated for several rounds, depending on the key size. The strength of AES is proportional to the number of rounds applied. So far, the number of rounds is fixed to 10, 12 and 14 for a key size of 128, 192 and 256 bits respectively. Most cryptographers feel that the margin between the number of rounds specified in the cipher and the best known attacks is too small. On the other hand, it is clear that the overall efficiency of a given AES implementation is inversely proportional to the number of rounds imposed.
Wang *et al.* [18] have proposed reconfigurable cryptographic processor. Several optimization methods have been introduced into the design process. The interconnection tree between rows (ICTR) method reduces the interconnection complexity and results in a small area overhead. The hierarchical context organization (HCO) scheme reduces the total context size and increases the dynamic configuration speed. Most symmetric ciphers, including AES, DES, SHACAL-1, SMS4, and ZUC, can be implemented using the proposed architecture. This architecture has obvious advantages over above mentioned different architectures in terms of performance, area efficiency (throughput/area) and energy efficiency (throughput/power).
Soltani *et al.* [19] have investigated storage space problem and proposed area, memory efficient AES algorithm. S-box is main block in AES. In contrast to many previous works which have employed only one of memory or non-memory based approaches to implement S box. They perform area-delay efficient multipliers and multiplicative inverters in GF (128). They employ loop-unrolling, fully pipelining, and sub-pipelining techniques in all methods. These reasons demonstrate that proposed methods not only try to keep the advantages of other works but also try to decrease their disadvantages.

Pirpilidis et al. [20] have analyzed the effects of the ring oscillator length and the Trojan size in the ring oscillator sensitivity towards detecting malicious alterations of FPGA implementations of the AES cryptographic algorithm. A cryptographic algorithm is a fundamental building block for realizing security, especially in highly-critical environments. Subtle modifications of the underlying implementation result in disastrous outcomes, while the search space prohibitively large for detecting Trojan activation through guided and random testing.
Senouci et al. [21] have presented a rapid prototyping method based on device independent and widely accessible for a seamless study, simulation and implementation of chaos generators in one single environment. The method relies on MATLAB HDL coder and fixed point toolbox to obtain a synthesizable description of chaotic models constructed under Simulink. This environment allows full control of all system parameters from the integration time step, initial conditions and parameters of chaotic system, to the number representation format. This permits to perform extensive study on all the aspects affecting the dynamics of the chaotic system with great flexibility.

GranadoCriado et al. [22] have presented the two cryptographic algorithms are international data encryption algorithm (IDEA), advanced encryption standard (AES) which permits to encrypt several data blocks independently. Additionally, the electronic codebook (ECB) employed to implement both algorithms because it is a cryptographic mode without data dependence. The FPGA implementations have performed by the Virtex-II 6000 FPGA and an NVIDIA TESLA T10 GPU FPGA family.
Sone et al. [23] have proposed a convolutional cryptosystem which combines residue number system (RNS), public-key cryptography and convolutional codes. Convolutional codes ensure the implementation of a dynamic cryptosystem and the minimization of time spread introduced in the transmitted signal in the wireless channel. To secure the plaintext, the convolutional coding technology associated with RNS-based RSA public-key cryptography. The RNS-based cipher text transmitted through the communication channel from the transmitter to receiver using M-array orthogonal signaling based on Walsh functions and implemented in a Virtex-4 FPGA.

III. PROPOSED SYSTEM

In this paper, hardware efficient Hybrid Wireless Crypto Processor (HWCP) is proposed, which combines two block ciphers such as enhanced advanced encryption standard (AES) and side-channel resistant authenticated encryption with masking (SCREAM). The hardware cost of hybrid processors are very high, here, we use composite field arithmetic (CFA), on the fly key expansion, and order change to reduce the hardware parts in the proposed hybrid algorithm. Additionally, hybrid chippers are very complex but not easy to crack the keys from malicious. The proposed HWCP system maximizes the security via increasing the complexity of cracking keys. Number of architecture like parallel and pipelined parallel are used to increase the throughput of AES algorithms. Moreover, the hybrid cipher reduces the throughput, but the parallel sub-pipeline architecture is used to maximize the throughput.

A detailed analysis of symmetric block encryption algorithms is presented on the basis of different parameters. The graph in figure 1a and 1b shows generic scalability. (memory usage & encryption performance) of different algorithm, the analysis are derived from different research papers. The above graph analyzes the performance of the most popular symmetric key algorithms

in terms of Authentication, Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application. During this analysis it was observed that AES (Rijndael) was the best among all in terms of security, flexibility, memory usage, and encryption performance. Although the other algorithms were also competent but most of them have a trade-off between memory usage and encryption performance with few algorithms been compromised.

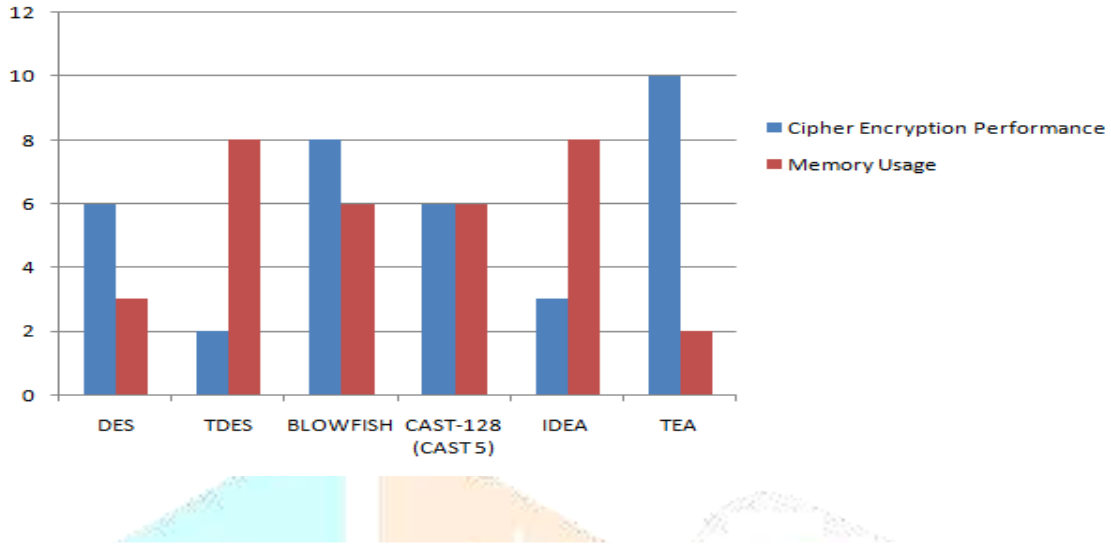

Fig 1a: Generic Scalability (Memory Usage & Encryption Performance) of Different Algorithm

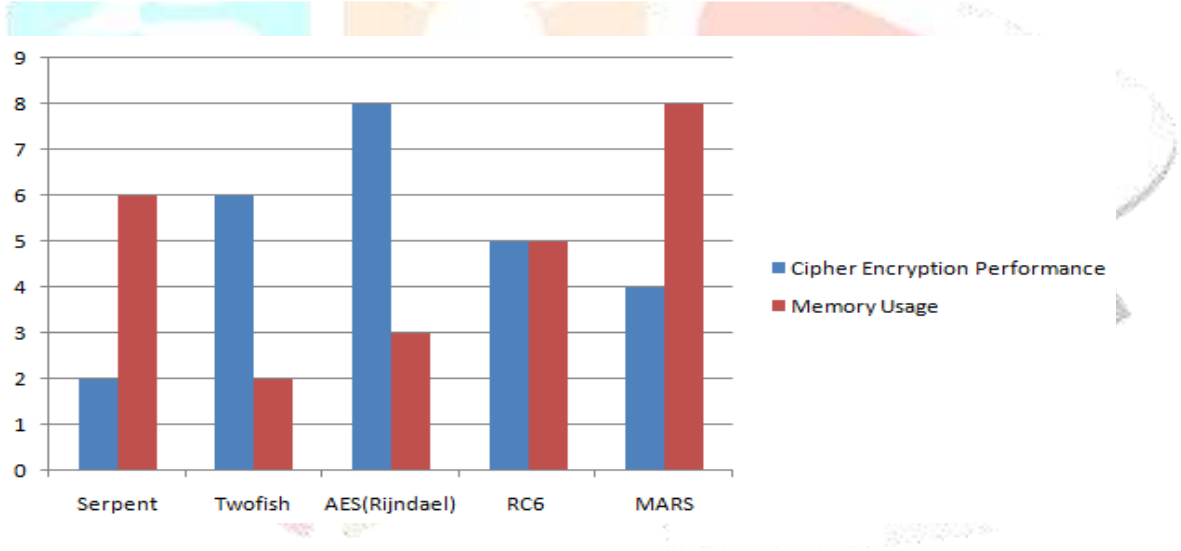

Fig 1b: Generic Scalability (Memory Usage & Encryption Performance) of Different Algorithm

IV. PROBLEM METHODOLOGY

At et al. [24] have presented a compact 8-bit coprocessor for the AES encryption, decryption, and key expansion; and the cryptographic hash function Grøstl. The additional arithmetic and logic units have only one instruction that allows for implementing AES encryption, AES decryption, AES key expansion, and Grøstl at all levels of security. The various addressing schemes required for the different steps of Grøstl and the AES, this control unit remains compacts and generated by modulo-128, 256 counters. The compression function implemented by an alternative description of Grøstl. The parallelism adopts with the Grøstl to deeply pipeline the ALU to achieve a high clock frequency and avoid data dependencies by interleaving independent tasks. The fully autonomous implementation of Grøstl and AES on Virtex-6 FPGA required 169 slices and a single 36 k memory block, and achieves competitive throughput up to 217 and 92 Mbps for encryption and hashing, respectively. The design was minimize the area utilization compare with several existing crypto processors, but, security level is very low. Furthermore, the above surveyed crypto processers [15]-[24] are not suitable for the wireless applications, because power consumption problems. In this modern era, communication plays an important role in a human's life and communications are carried out in wireless medium. It is necessary to transmit the confidential data in wireless media in secure manner. Cryptography is technique to protect electronic data in a communication network.

V. CONCLUSION

In this paper hardware efficient wireless crypto processor combines hybrid ciphers which maximizes the security via increasing the complexity of cracking the keys. These algorithms are implemented in hardware which enhances the performance in terms of both area and speed and also minimize BRAM resources to utilize full memory space of BRAM by means of various technique mentioned above.

REFERENCES

[1]NIST -Advanced Encryption Standard, National Institute of Standards and Technology, FIPS-197, 2001. URL http://csrc.nist.gov/publications/fips/fips197/fips-197. pdf
[2]M.-Y.Wang, C.-P. Su, C.-L. Horng, C. Wu, C.-T. Huang, Single and multi-core configurable AES architectures for flexible security, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 18 (4) (2010) 541–552. ISSN 1063-8210.
[3]H. Li, Efficient and flexible architecture for AES, IEE Proc. Circuits Devices Syst. 153 (6) (2006) 533–538.
[4]A. Hodjat, I. Verbauwhede, Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors, IEEE Trans. Comput. 55 (4) (2006) 366–372. ISSN 0018- 9340.
[5]T. Good, M. Benaissa, 692-nW advanced encryption standard (AES) on a 0.13-um CMOS, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 18 (12) (2010) 1753–1757.
[6]G. Saggese, A. Mazzeo, N. Mazzocca, A. Strollo, An FPGA-based performance analysis of the unrolling, tiling, and pipelining of the AES algorithm, in: Field Programmable Logic and Application (FPL 2003), in: LNCS, vol. 2778, Springer, Berlin, Heidelberg, Lisbon, Portugal, 2003, pp. 292–302. ISBN 978-3-540-40822-2.
[7]S. Drimer, T. Güneysu, C. Paar, DSPs, BRAMs, and a pinch of logic: extended recipes for AES on FPGAs, ACM Trans. Reconfigurable Technol. Syst. 3 (1) (2010) 3:1–3:27. ISSN 1936–7406.
[8]P. Bulens, F.-X. Standaert, J.-J. Quisquater, P. Pellegrin, G. Rouvroy, Implementation of the AES-128 on Virtex-5 FPGAs, in: Progress in Cryptology, AFRICACRYPT 2008, in: LNCS, vol. 5023, Springer, Berlin, Heidelberg, 2008, pp. 16–26. ISBN 978-3-540-68159-5.
[9]A. Aziz, N. Ikram, A Look-Up Table implementation of AES, in: International Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-07), Orlando, Florida, USA, 2007, pp. 187–191.
[10]F.R. Henrquez, A.D. Prez, N.A. Saqib, C.K. Koc, Cryptographic Algorithms on Reconfigurable Hardware, Signals and Communication Technology, Springer, 2007.
[11]D.-S. Kundi, A. Aziz, N. Ikram, Resource efficient implementation of T-boxes in AES on Virtex-5 FPGA, Inf. Process. Lett. 110 (10) (2010) 373–377. ISSN 0020-0190.
[12]K. Latif, A. Arshad, A. Mahboob, Optimal utilization of available reconfigurable hardware resources, Comput. Electr. Eng. 37 (6) (2011) 1043–1057.
[13]L. Ali, I. Aris, F.-S. Hossain, N. Roy, Design of an ultra-high speed AES processor for next generation IT security, J. Comput. Electr. Eng. 37 (6) (2011) 1160–1170.
[14]V. Shoup, Using Hash Functions as a Hedge against Chosen Ciphertext Attack, EUROCRYPT 2000, pp.275-288 (2000)
[15]S. Priya, P. Karthigaikumar, N. Siva Mangai and P. Kirti Gaurav Das, "An Efficient Hardware Architecture for High Throughput AES Encryptor Using MUX Based Sub Pipelined S-Box", Wireless Pers Commun, 2016.
[16]D. Kundi, A. Aziz and N. Ikram, "A high performance ST-Box based unified AES encryption/decryption architecture on FPGA", Microprocessors and Microsystems, vol. 41, pp. 37-46, 2016.
[17]N. Nedjah, L. de Macedo Mourelle and C. Wang, "A Parallel Yet Pipelined Architecture for Efficient Implementation of the Advanced Encryption Standard Algorithm on Reconfigurable Hardware", Int J Parallel Prog, vol. 44, no. 6, pp. 1102-1117, 2016.
[18]B. Wang and L. Liu, "Dynamically reconfigurable architecture for symmetric ciphers", Science China Information Sciences, vol. 59, no. 4, 2016.
[19]A. Soltani and S. Sharifian, "An ultra-high throughput and fully pipelined implementation of AES algorithm on FPGA", Microprocessors and Microsystems, vol. 39, no. 7, pp. 480-493, 2015.
[20]F. Pirpilidis, K. Stefanidis, A. Voyiatzis and P. Kitsos, "On the effects of ring oscillator length and hardware Trojan size on an FPGA-based implementation of AES", Microprocessors and Microsystems, vol. 54, pp. 75-82, 2017.
[21]A. Senouci, H. Bouhedjeur, K. Tourche and A. Boukabou, "FPGA based hardware and device-independent implementation of chaotic generators", AEU - International Journal of Electronics and Communications, vol. 82, pp. 211-220, 2017.
[22]J. Granado-Criado and M. Vega-Rodríguez, "Hardware coprocessors for high-performance symmetric cryptography", The Journal of Supercomputing, vol. 73, no. 6, pp. 2456-2482, 2016.
[23]M. Sone and N. Ningo, "A simple fpga-based wireless transmitter/receiver convolutional cryptosystem", International Journal of Computers and Applications, vol. 33, no. 2, 2011.
[24]N. At, J. Beuchat, E. Okamoto, I. San and T. Yamazaki, "A low-area unified hardware architecture for the AES and the cryptographic hash function Grøstl", Journal of Parallel and Distributed Computing, vol. 106, pp. 106-120, 2017.