International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S3, December 2019

Authenticated Encryption using Lightweight Cryptographic Primitives for Wireless Sensor Networks

Rajkamal P, Ramkumar E, Prathiba A., Kanchana Bhaaskaran V. S.

Abstract*— Wireless Sensor Networks (WSN) transmits sensitive data from physical environment to digital medium. Thus, security is essential to transmit these vulnerable data. Authenticated Encryption aim to provide security in WSN with integrity, confidentiality, and authentication of data transmitted. Block cipher modes of operations provide different cipher text for identical plain text which further enhances the security. Sensor nodes have its own operational constraint which makes security algorithm to be light in terms of area and low power consumption. In this paper novel architecture of authenticated encryption of lightweight symmetric cipher PRESENT and lightweight hash function SPONGENT in OFB mode is proposed. Proposed design is evaluated in terms of Gate Equivalent (GE), operating frequency and power consumption using Cadence Genus® tool using 180 nm technology library.

Keywords—Authenticated Encryption, low area, low power, PRESENT, SPONGENT.

I INTRODUCTION

In today's world, Wireless Sensor Network (WSN) is a contemporary technology which is best suited for Internet of Things (IoTs) applications such as agriculture, military, healthcare, industrial automation and home security [1]- [3]. WSN contains senor nodes, which helps to collect data and transmit to other nodes and eventually to computational unit. Notably the sensor nodes communicate wirelessly and smaller in size and operable in batteries. Information transmitted is prone to attack in the network. These attacks could be severe security threats which hinder implementation and adoption of WSN. To overcome these, several researches have been carried out to ensure integrity, confidentiality and authenticity [4]-[6]. However, it is laborious to provide the integrity and confidentiality in WSN. The primary reason for these difficulties is slow processing capability due to availability of fewer resources. Another issue in WSN is, it collects larger number of data which will further burden the processing ability. These two aspects should be satisfied without comprising the security in the network, which is the primary goal towards offering integrity and confidentiality solutions in WSN.

Manuscript published on 30 December 2019.
***** Correspondence Author (s)
Rajkamal P, Perusing Masters, Department of Electronics and Communication, Anna University VLSI, VIT University.
Ramkumar E., Masters Student Specialized VLSI Design, VIT University, Chennai.
Prathiba A., Assistant Professor, VIT University Chennai.
V S Kanchana Bhaaskaran, Department of Electronics and Communication Engineering, Institution of Engineers (India),

An intruder would be crack the information from cipher text by simply knowing the various distributions of the message parts, without decoding the complete cipher code. To overcome this threat, plaintext block is combined with ciphertext block and output of the cipher block is provided as the input to succeeding block in block cipher modes. The various block cipher modes are Cipher Block Chaining (CBC) mode, Output Feed Back (OFB) Mode, Counter (CTR) mode, the Cipher Feedback Mode and Electronic Code Book (ECB) mode. Authenticated Encryption (AE) is designed by combination of symmetric encryption and Message Authentication Code (MAC) algorithm. The literature shows three types of operations modes for authenticated encryption, namely, *MAC-then-encrypt, Encrypt-then-MAC, and Encrypt-and-MAC* [6]. Security of these designs has been estimated assuming that the given symmetric encryption algorithm is protected to chosen-plaintext attacks (CPA) and the given MAC algorithm is authentic under chosen-message attacks (CMA).

The confidentiality mode Output Feedback (OFB) which iterates the forward cipher on an initialization vector (IV) to produce a sequence of output blocks that are EX-OR with the plaintext to yield the ciphertext, and vice versa [11]. This results in generation of different cipher text for the same plain text. Under OFB operation mode, only the encryption block of the cipher is needed to encrypt or decrypt the data. This is beneficial for area and power constrained devices.

The objective of this paper is to preserve the information in WSN through guaranteed data confidentiality and integrity and assure the user authenticity with efficient hardware design. A lightweight symmetric block cipher PRESENT of ISO/IEC standard is best suited for data confidentiality and integrity. Many novel hardware implementations of PRESENT have been published to prove this algorithm as area constrained and energy efficient [7]. SPONGENT is a lightweight hash function which uses PRESENT type permutation and is suitable for user authenticity. Implementation of SPONGENT-88 has been proposed in Ref. 8 which proposes a novel hardware design with less area occupancy and low power consumption.

II LITERATURE SURVEY

Many researches have proposed the generic authenticated encryption which includes different modes of operation. It is based on the shared-key transformation to provide the confidentiality and authenticity of the data transformed [6].

This process will convert the plain text to cipher text using the key. Similar key is used to again to convert back the cipher text to plain text. Failure of proper decryption of original plain text indicates the problem with data integrity.

Table-I: Security notion for AE

Composition Method	Confidentiality		Authentication	
	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	Insecure	Insecure	Secure	Insecure
MAC-then-Encrypt	Secure	Insecure	Secure	Insecure
Encrypt-then-MAC	Secure	Secure	Secure	Secure

The indistinguishability and integrity are the two major security goals for any symmetric encryption system. The indistinguishability is a property in which the attacker has an ability to distinguish between the random text and ciphertext. Chosen-Plain text Attack (CPA) and Chosen-Cipher text Attack (CCA) are employed to study these security properties. [6]. If the indistinguishability is strong, it can be claimed that particular symmetric encryption has strong security notions and cannot be attacked easily. The chosen-plain text and the chosen-cipher text attacks of the indistinguishability security notions are abbreviated as IND-CPA and IND-CCA, respectively.

The integrity of plaintexts and the integrity of cipher texts are considered the important notion for authentication. The integrity of plaintext and integrity of ciphertext are denoted as INT-PTXT and INT-CTXT respectively. The goal of the INT-PTXT is to ensure that the original plaintext by the decryption block is not generated unless it is transmitted by the sender. The objective of the INT-CTXT is to ensure that creation of ciphertext for which the sender has already sent the data.

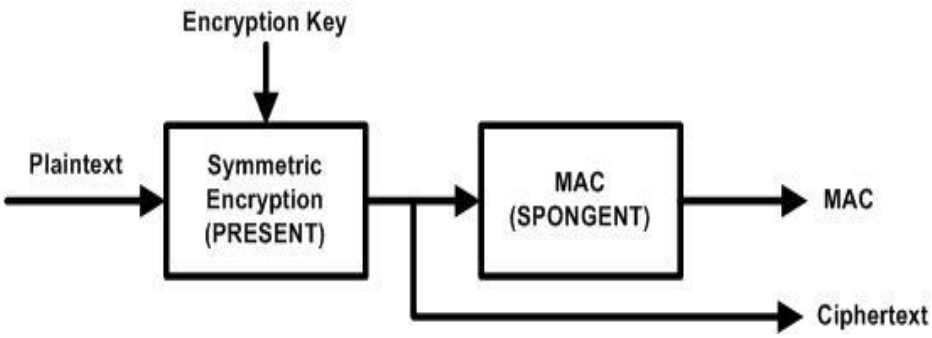

Fig. 1. Authenticated encryption: Encrypt-then-MAC

These are the well-known security notions carried out for the authenticated encryption [6]. Table 1 represent the security analysis of the three different variant of authenticated encryption (AE), namely *Encrypt-and-MAC*, *MAC-then-Encrypt*, or *Encrypt-then-MAC* and evaluated under INT-CTXT, INT-PTXT, IND-CPA and IND-CCA [6]. From the table 1, it is concluded that Encrypt-then-MAC variant will provide both confidentiality and authenticity simultaneously. Thus, in this paper we design the AE structure in Encrypt-then-MAC mode of operation. Several authors have proposed novel architecture for PRESENT cipher algorithm [7] which is best suited for the constrained environment and categorize as lightweight when compared against Advanced Encryption Standard (AES). These proposals are implemented in Field Programmable Gate Arrays (FPGA) and Application-Specific Integrated Circuits (ASIC). The studies already proved that PRESENT is employed in IoTs and WSNs due to its computation power and less area occupancy. In this paper, lightweight PRESENT algorithm in ASIC with unrolled structure has been implemented Thus, PRESENT provides encryption block of the AE as proposed in Fig. 1. The lightweight hash function is an interesting area of research and many new hash functions have been constructed. Out of many lightweight hash functions based on a SPONGE construction, SPONGENT [8] has many variant and suitable for the IoTs and WSN for its small weight and compact design. The SPONGENT-88 version is chosen in this paper, since it produces 88 bit of output digest. The cipher is applied to a set of inputs called counter values, which produces the sequence of output blocks, which are in turn EXORed with given plaintext to produce cipher text and vice versa. The sequence of counters must be unique.

This paper discusses the ASIC implementation of the novel architecture of AE using PRESENT for encryption and SPONGENT for MAC.

This design is based on NIST standard operated in OFB mode. Design is evaluated using Cadence Genus tool with 180 nm technology and evaluated in terms of gate equivalents, power consumption and operating frequency.

The rest of the paper is organized as follows. Section III brief about PRESENT algorithm. Section IV elaborates the design of SPONGENT. Section V elaborates OFB mode of encryption. Finally, Section VI discusses implementation results and simulation results of Authenticated encryption.

III PRESENT ALGORITHM

According to the specification, the block cipher PRESENT algorithm was designed which is suitable for lightweight applications [3]. It has a block size of 64-bits, and a key size of either 80 or 128-bits. It is a Substitution-Permutation Network (SPN) based algorithm consisting of 31 rounds, which has 3 basic operations, as discussed below.

- *Add Round Key:* Each round the 64 bit State is EXORed with 64 bit key bit provided from the Key scheduler.
- *S-Box*: Replaces the 4-bit values from Add Round Key 16 times using traditional Look-Up-Table (LUT).
- *P-Box:* The permutation box is simply shuffling of 64 bits.

IV SPONGENT ALGORITHM

SPONGENT-88 architecture has been developed in basic loop architecture with a single register. STATE hold values are initialized to all zeroes in the beginning phase. When the first round starts, the input is exclusive OR-ed with the value in the register. At each round this register is exclusive OR-ed with the input from the Linear Feedback Shift Register (LFSR) which is controlled by the mod-45 counter. After the Exclusive OR operation, substitution and permutation layers are employed. The design of SPONGENT-88 is shown in Fig. 2. The SPONGENT-88 has the following blocks and its functionality has been explained.

- *LFSR*: It is 6-bit counter which is generated by the register for every round. Its value is Exclusive OR-ed with the least significant bits of the STATE register and its reversed value is Exclusive OR-ed with the most significant bits of the STATE register.

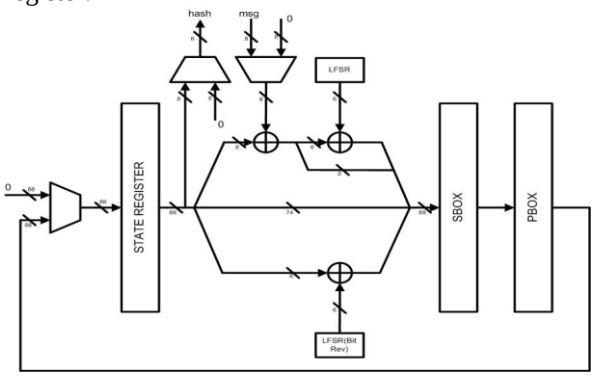

Fig. 2. Design of SPONGENT-88

- *S-Box*: The output of the Exclusive OR-ed operation is then mapped to nonlinear block of substitute box which cipher the input using table 4. In this design, we are using 22 S-box which can parallel perform the substitute to the STATE provided. The S-box number can be reduced and optimize the design but with the cost of latency.
- *P-Box*: This layer is just a wiring of the previous value from the S-box. This not cost any area and it involves just a rewiring.

The design SPONGENT 88 required 45^{th} cycle to generate the hash output. The output is directly taken from the register output. To reduce the switching activity which is directly related to power consumption and protect the cost of hardware resource.

V. OUTPUT FEEDBACK MODE

The Output Feed Back (OFB) Mode necessitates a unique initialization vector (IV) which provides the further confidentiality. For the OFB encryption process, the IV is modified by the encryption function block to produce the output of first block. This block is then exclusive OR-ed with first plaintext as shown in Fig.3 to yield the cipher text of the first block. In OFB mode, the output of first block is feed back to the second stage and same process in continue as required. Thus, previous output block serves an input to the next block then it is exclusive OR-ed with plaintext to give the ciphertext. The final block, the most significant bit is alone exclusive OR-ed used for operation. The remaining bits are ignored. In OFB decryption process, the IV is modified by the encryption block to produce the output of first block. This block is then exclusive OR-ed with first ciphertext as shown in Fig.3 to recover the plaintext of the first block. This process is repeated for successive blocks.

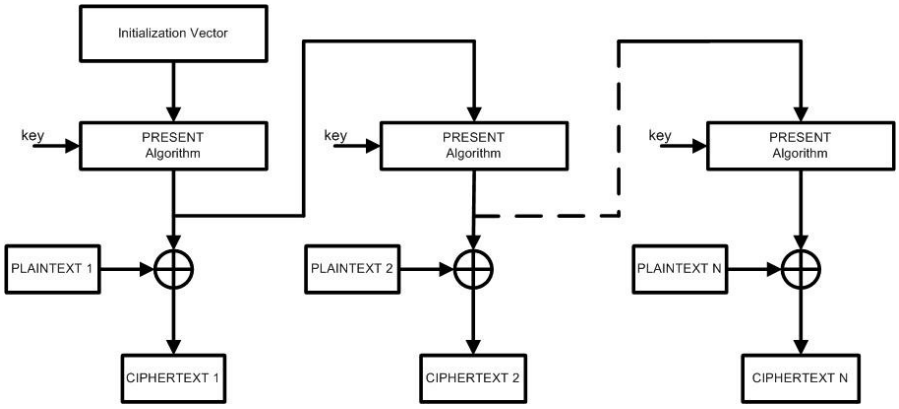

Fig. 3. Output Feed Back Mode

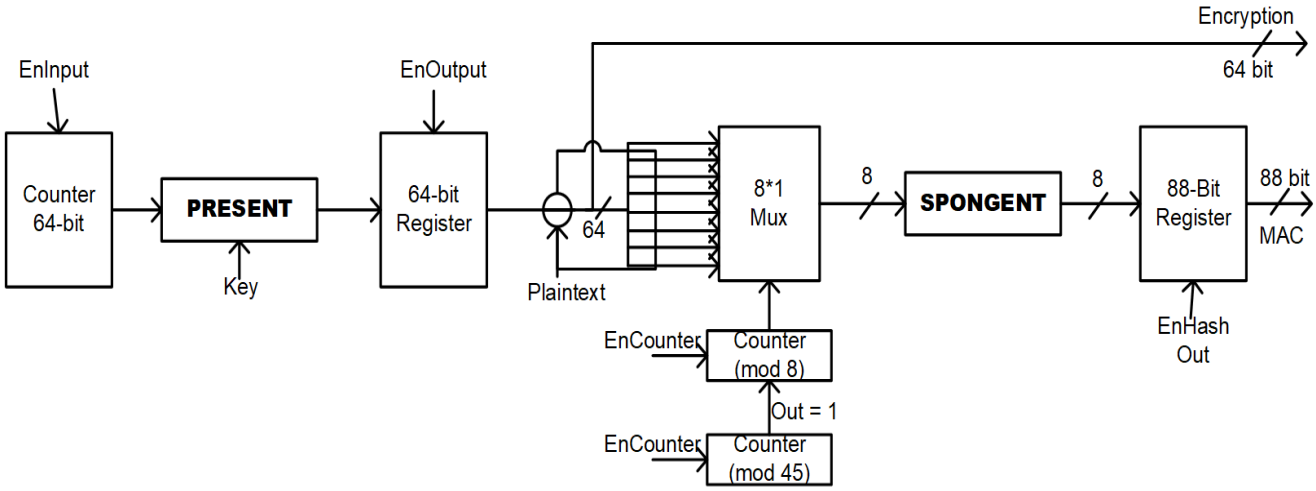

Fig. 4. Authenticated Encryption with OFB mode

VI. AUTHENTICATED ENCRYPTION

The primary design of the proposed architecture uses lightweight encryption algorithm PRESENT and for MAC SPONGENT is employed. The security of the design is further enhanced by employing the architecture in OFB mode. The proposed design has been illustrated in Fig. 4.

***Process Unit*:** When the device is ON or reset the PRESENT will take *Initial vector* as an input. Once the *enInput* is enabled the input key (80 bits) and the plain text (64 bits) is fed into the Encryption module. It is encrypted in 1 clock cycle. Once the *enOutput* is enabled, the cipher text (64 bits) is passed to the Authentication module. The MAC tag generation process executes once the *enCounter* signal is sent. In this phase, the cipher text is passed in terms of 8 bits using 8x1 MUX starting form MSB into SPONGENT module where SPONGENT process it for 45 cycles before it generates an 8 bit output and it is stored in the LSB of the 88 bit left shift register. This process is repeated 8 times. So the total of 360 cycles is required for creating the MAC tag. Finally, once the *enOutput* is enabled MAC tag will be available. This operation is repeated for the successive input messages but instead of IV
the previous cipher text serves as the IV. Total clock cycle for AE = 1(Encryption) + 360(Authentication) + 1(Input) + 1(Output tag) = 364.

***Control unit*:** The proposed state machine of the AE design is shown in Fig. 5. Once *Reset* state *Sel* signal is made low the process begins. And it moves to *InputCheck* (S0) state where the control waits for the *inputReady* signal. The state control transfer to state S1 and the signal to enable the input will be generated. After which it moves to S2 the signal for sending the cipher text will be triggered. Followed by this authentication module is made active. After sending *enOutput* signal it moves to S3. This state is used for beginning the authentication module and the control waits in the same state until it gets the disable counter signal which is used to shut down the authentication module. This is sent after 360 cycles after the MAC generation process starts. Finally, S4 state enables output register to get the final MAC tag for output plaintext generation.

Table II: ASIC results for Authenticated Encryption

Library	Design	Cell Count	Cell Area (μm^2)	Gate Equivalent	Power (mW)	Slack (ps)	Freq (MHz)	Setup Time (ps)
FAST	OFB (proposed)	13487.00	237338.64	23974.00	177.12	672.00	55.55	296.00
	COUNTER	13582.00	241529.91	24397.00	68.05	1936.00		296.00
SLOW	OFB (proposed)	13719.00	243093.31	24555.00	160.21	659.00	25.00	712.00
	COUNTER	13794.00	249293.72	25182.00	159.09	2191.00		712.00
TYPICAL	OFB (proposed)	13923.00	239514.11	24194.00	218.24	168.00	40.00	432.00
	COUNTER	13991.00	244846.33	24732.00	230.92	261.00		330.00

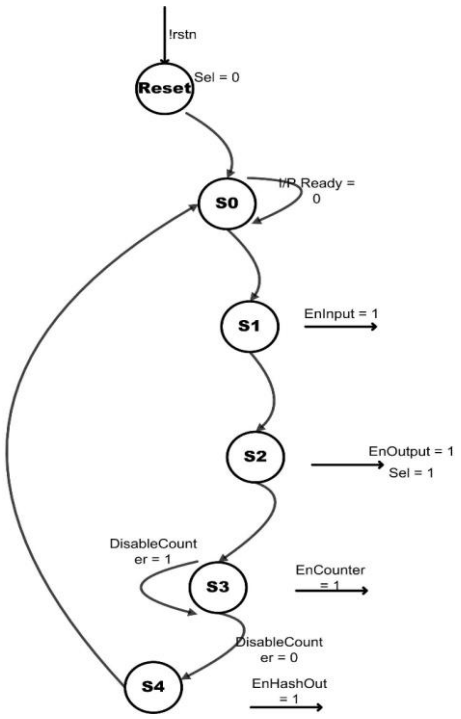

Fig. 5. Proposed Finite State Machine

VII. RESULTS AND CONCLUSION

The implementation results for three different PVT operating corners are tabulated in Table 6. The designs are specified in Verilog HDL and synthesized using Cadence® Genus tool with different clock periods, namely, 18ns, 40ns and 25ns for fast, slow and typical library, respectively under the operating frequencies 55.55 MHz, 25 MHz and 40 MHz for fast, slow and typical, respectively. From the table, it has been observed that area of the proposed OFB design is better than Counter mode design across all three libraries. OFB mode is 1.73%, 2.48%, 2.17% lesser in area than the counter mode in fast, slow and typical library, respectively. This is because of the feedback circuit employed in the OFB which results in lesser gate equivalent compared against counter mode. The power consumption of the both designs has been found to be similar.

REFERENCES

1. T. Eisenbarth, C. Paar, A. Poschmann, S. Kumar, and L. Uhsadel, "A Survey of Lightweight Cryptography Implementations," IEEE Des. Test, vol. 24, no. 6, pp. 522–533, Nov. 2007.
2. D. Maimut and K. Ouafi, "Lightweight Cryptography for RFID Tags," IEEE Security & Privacy, vol. 10, no. 2, pp. 76–79, Mar 2012.
3. A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 4727. Berlin, Germany: Springer, 2007, pp. 450–466.
4. "Specification for the Advanced Encryption Standard (AES)," in Federal Information Processing Standards Publication, vol. 197, 2001.
5. M. J. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality," National Institute of Standards and Technology NIST SP 800-38c, 2007.
6. M. Bellare and C. Namprempre, "Authenticated encryption: relations among notions and analysis of the generic composition paradigm," Journal of Cryptology. The Journal of the International Association for Cryptologic Research, vol. 21, no. 4,pp. 469–491, 2008.
7. C. A. Lara-Nino, M. Morales-Sandoval, and A. Diaz-Perez, "Novel FPGA-based low-cost hardware architecture for the PRESENT block cipher," in *Proc. Euromicro Conf. Digit. Syst. Design*, Aug./Sep. 2016,pp. 646–650.
8. C. A. Lara-Nino, M. Morales-Sandoval, and A. Diaz-Perez, "Small lightweight hash functions in FPGA," in Proceedings of the 2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS), pp. 1–4, Puerto Vallarta, Feburary 2018.
9. X. Zhang, H. M.Heys, andC. Li, "Energy efficiency of encryption schemes applied to wireless sensor networks," Security and Communication Networks, vol. 5, no. 7, pp. 789–808, 2012.
10. K. Bok, Y. Lee, J. Park, and J. Yoo, "An energy-efficient secure scheme in wireless sensor networks," Journal of Sensors, vol. 2016, 2016.
11. P. Rogaway, M. Bellare, and R. S. Ferguson, "OCB: a blockcipher mode of operation for efficient authenticated encryption," ACM Transactions on Information and System Security, vol. 6, no. 3, pp. 365–403, 2003.

AUTHORS PROFILE

Rajkamal P received his bachelor degree in Electronics and Communication from Anna University in the year 2013. He is currently perusing Masters in VLSI in VIT University. His area of interest is FPGA and ASIC.

Ramkumar E is a final year masters student specialized in VLSI Design at VIT University, Chennai. He obtained his bachelor's degree in Electronics and Communication in the batch of 2015. Currently, he is doing an internship at Intel in the field of FPGA. His area of interest in Low Power design, FPGA and ASIC.

Prathiba A received her bachelor degree in Electronics and Communication in the year 2002. She obtained her Masters in Communication Systems in the year 2006. She is working as an Assistant Professor in VIT University Chennai. Currently she is pursuing her Ph.D. degree and her research areas are hardware design of cryptographic architectures, vulnerability modeling of side channel attacks and lightweight cryptography.

V S Kanchana Bhaaskaran obtained her undergraduation degree in Electronics and Communication Engineering from Institution of Engineers (India), Calcutta and her M.S. degree in Systems and Information from Birla Institute of Technology and Sciences, Pilani and Ph D from V I T University. She has more than 35 years of industry, research and teaching experience by serving the Department of Employment and Training, Government of Tamil Nadu, IIT Madras, Salem Cooperative Sugar Mills' Polytechnic College, SSN College of Engineering and VIT University Chennai. Her specializations include Low Power VLSI Circuit Design, Microprocessor architectures and Linear Integrated Circuits. She has published around 100 papers in International Journals and conferences. She is a reviewer for peer reviewed international journals and conferences. She is the Fellow of the Institution of Engineers (India), Fellow of the Institution of Electronics and Telecommunication Engineers, Life Member of the Indian Society for Technical Education and Member of the Institute of Electrical and Electronics Engineers Inc., USA.