Energy-Adaptive Lightweight Hardware Security Module using Partial Dynamic Reconfiguration for Energy Limited Internet of Things Applications

Nagham Samir[1], Yousef Gamal[1], Ahmed N. El-Zeiny[1], Omar Mahmoud[1], Ahmed Shawky[1], AbdelRahman Saeed[1],
and Hassan Mostafa[1,2]
[1]Electronics and Communications Engineering Department, Cairo University, Giza 12613, Egypt.
[2]Nanotechnology Department at Zewail City for Science and Technology, Cairo, Egypt.
naghamsamir2014@gmail.com, youssef_hassan_gamal@hotmail.com, ahmed.nagy.elzeiny@gmail.com,
omar.mahmoud.yahya@gmail.com, ahmed.shawky.awwad@gmail.com, abdelrahman.saeed.a@gmail.com,
hmostafa@uwaterloo.ca

***Abstract*—Data security is the main challenge in Internet of Things (IoT) applications. Security strength and the immunity to security attacks depend mainly on the available power budget. The power-security level trade-off is the main challenge for low power IoT applications, especially, energy limited IoT applications. In this paper, multiple encryption modes that provide different power consumption and security level values are hardware implemented. In other words, some modes provide high security levels at the expense of high power consumption and other modes provide low power consumption with low security level. Dynamic Partial Reconfiguration (DPR) is utilized to adaptively configure the hardware security module based on the available power budget. For example, for a given power constraint, the DPR controller configures the security module with the security mode that meets the available power constraint. ZC702 evaluation board is utilized to implement the proposed encryption modes using DPR. A Lightweight Authenticated Cipher (ACORN) is the most suitable encryption mode for low power IoT applications as it consumes the minimum power and area among the selected candidates at the expense of low throughput. The whole DPR system is tested with a maximum dynamic power dissipation of 10.08 mW. The suggested DPR system saves about 59.9% of the utilized LUTs compared to the individual implementation of the selected encryption modes.**

Keywords*—Internet of Things (IoT), Security, Dynamic Partial Reconfiguration (DPR), Encryption Modes, Competition for Authenticated Encryption: Security, Applicability and Robustness (CAESAR).

I. Introduction

Internet of Things (IoT) is a network of interconnected objects such as: transportation, wearable devices, and appliances, that enable these objects to exchange information [1] [2] [3]. The growth of IoT systems puts two main challenges on the designers road especially for low power IoT devices, namely security and privacy [2] [3] [4] [5]. The possibility of secured data to be attacked is increasing when the provided security level is not quite enough [2] [3] [6]. Encryption is used to secure confidential information by carrying out effective algorithmic schemes based on complex cryptographic mathematics. The objective of conducting data encryption is developing a cryptographic system that achieves confidentiality, authentication, data integrity, and non-repudiation of message [7].

The restricted value of the available power budget is the main challenge for the low power IoT devices, and this power restriction provides either vulnerable data or data not sufficiently secure. Low power IoT devices are mainly battery based devices that mean maximizing the battery life is a must [8]. One of the applicable solutions to prolong the battery life is implementing a rechargeable battery. The rechargeable batteries are relying on energy harvesting system that utilizes various sources in order to extract power such as: temperature gradient, solar energy, and wind [8] [9] [10] [11]. Correspondingly, this solution provides unstable power conditions depend on the power source of the harvester system. The utilization of this solution arises different issue which is how to adapt the security level of data according to the available power budget [8]. This work suggests Dynamic Partial Reconfiguration (DPR) technology as a method to resolve the power constraint issue by implementing multiple encryption modes that have various security levels. The objective of this work is introducing the answer of the following questions: which encryption mode is suitable for low power IoT applications among the selected candidates? and what is the optimum configuration of DPR implementation for the selected encryption modes?.

The rest of this paper is organized as follows. Section II gives an overview on DPR technology and the proposed DPR system architecture. Authenticated Encryption with Associated Data (AEAD) architecture in section III. Section IV provides comparison results and discussion about the two suggested scenarios. Section V concludes the results and the outcomes of this work.

II. SYSTEM ARCHITECTURE

Dynamic Partial Reconfiguration (DPR) technology is the ability to dynamically change the function of certain block

978-1-7281-0397-6/19/$31.00 ©2019 IEEE

that is hardware implemented using Field Programmable Gate Array (FPGA). A full bit file is used to program the whole FPGA logic, while the reconfiguration process is conducted by utilizing various partial bit files. This dynamic switching relax the power-security level trade-off through various run time configurations of the hardware security module. A power adaptive solution is performed by selecting among several encryption modes based on the power margins.

The hardware implementation of any specific design using DPR technique includes partitioning of the design functionality into two main parts: static design, and dynamic design. The logic of the static design is performed fixed number of operations that are not required to be changed during run time operation. Dynamic part configures the design functionality during run time operation, and it is denoted by Reconfigurable Partition (RP). The RP uses various Reconfigurable Modules (RM) that perform the different functions of the RP. A partial bitsream file is generated for each RM in order to change the function of the dynamic design. The reconfiguration process is performed through changing the partial bitstream files for each RM.

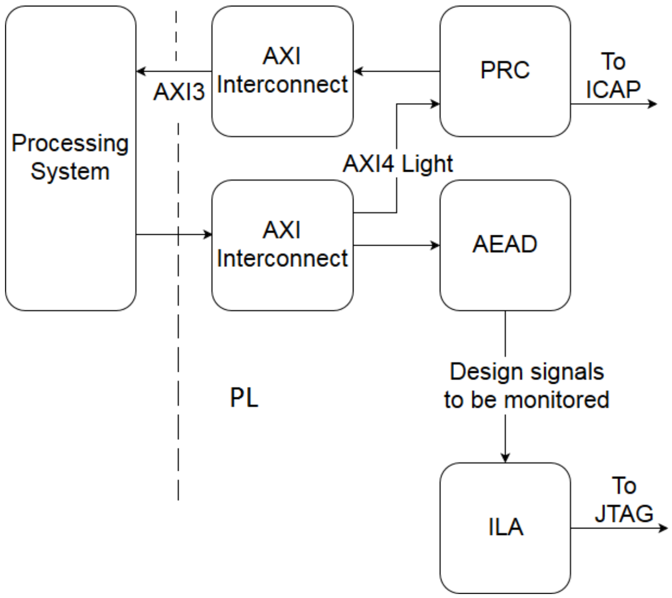

Fig. 1: Block diagram of the proposed DPR system

Fig. 1 shows the block diagram of the proposed DPR system. AEAD is the reconfigurable region that runs the desired RM based on the required function that is adopted to be implemented. Two AXI interconnect blocks are used to convert from AXI3 interface to AXI4-Light interface. Organization of the reconfiguration process is performed by using Partial Reconfiguration Controller (PRC) core. Moreover, Integrated Logic Analyzer (ILA) Intellectual Property (IP) core is utilized to debug and test the design.

III. AEAD Architecture

Authenticated Encryption with Associated Data (AEAD) architecture is one of the universal hardware Application Programming Interface (API) for authenticated ciphers [13]. The top level of AEAD is composed of four units as in [14], are namely preprocessor, postprocessor, command (CMD) FIFO, and cipher core. Preprocessor is responsible for understanding and executing the instruction (i.e., loading key, encryption, and decryption instructions), serial-in-parallel-out conversion of the input block, and padding for the input block. Postprocessor is carried out the following functions: clearing any portion of the output block that does not belong to the message, parallel-in-serial-out conversion of the output blocks, and generates the status block. The first-in-first-out (FIFO) contains 4x24 first-word-fall-through (FWFT) FIFO that stores all instructions bits, original tag created by encryption process, and segment headers that are passed to the output [14].

The selected encryption modes are adopted from Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) [5]. The chosen candidates are namely ACORN[15], JAMBU [16], MORUS [17], Compact Low-Overhead Cipher (CLOC) [18], and Pi-Cipher[19]. This work introduced a comparative study for these encryption modes that involves two scenarios. The first scenario is implementing each encryption mode separately. Following, a quantitative comparison is performed among the selected encryption modes to pick up the most suitable mode for low power IoT applications from power dissipation, area utilization, and throughput perspectives. The second scenario is carried out the DPR concept on the selected encryption modes. DPR implementation helps dynamic changing for the available encryption modes based on the available power budget. Power adaptive authentication encryption model is accomplished by applying this scenario. This suggested implementation provides less area utilization than implement each encryption mode individually. In addition, increasing the security level by hopping among various encryption modes in a way that makes tracking of the encrypted data much harder or even impossible.

IV. Experimental Results

The selected encryption modes are simulated, synthesized, and implemented, using Vivado 2015.2 and ZC702 FPGA board. Results are adopted in maximum Process, Voltage, and Temperature (PVT) conditions, with no loading. The Switching Activity Interchange Format (SAIF) file is included in power calculation in order to provide accurate results.

TABLE I: Experimental Results Prior DPR Technique

Encryption Mode	Dynamic Power (mw)	LUTs	Throughput (Mbit/sec)	Latency (Cycle/Byte)	FoM
ACORN	1.279	491	7.27	10.475	9962.63
Pi-Cipher	8.502	3824	256	3.437	427.437
JAMBU	1.37	887	9	14.8	105.07
MORUS	7.466	4761	426.67	0.3129	352.46
CLOC	3.158	2879	128	1.484	4874.02

Table I depicts that ACORN encryption mode consumes the minimum power because it depends on stream cipher that utilizes narrow data bus width. While Pi-Cipher provides the highest power consumption due to the large number of adders that are used to achieve tag second preimage resistance. This result proves that ACORN encryption mode is the most suitable mode for lightweight IoT applications.

FPGA utilization depends on several parameters such as: block size, key size, tag size, number of rounds, and bus width. MORUS is found that it consumes the largest utilization area because of large block size. While ACORN utilizes the smallest area because of the simple hardware implementation that is constructed using XoR & AND operations that are not require large implementation area.

Equation 1 is followed to calculate the throughput of the selected candidates in Mbis/sec [20]. Latency is figured out to measure the required average time to finish the encryption/decryption. Table I demonstrates that MORUS algorithm is recommended for high speed applications because it achieves the highest throughput and the smallest latency. ACORN algorithm provides the smallest throughput because of small block size, while JAMBU gives the highest latency.

$$Throughput = \frac{Block\ Size}{(Number\ of\ Rounds + C) * TCLK} \quad (1)$$

A FoM is suggested in order to provide fair comparison among the selected encryption modes and then choose the suitable encryption mode for low power IoT applications. The formula is developed such that it combines the main parameters that contribute the good profile of low power IoT applications. FOM is calculated as follows:

$$FoM = \frac{2^{KeySize(Bytes)}}{(Area\ (LUTs) * Power(w) * Latency(Cycle/Byte))} \quad (2)$$

Table I demonstrates that ACORN achieves the best performance because it gives the highest FoM due to the minimum estimated power consumption and area utilization at the expense of high latency. While JAMBU gives the lowest performance as it achieves the lowest FoM.

TABLE II: Comparison Among Implemented Designs

Design	Dynamic Power (mw)	LUTs Memory	LUTs Logic
Static Design	14.156	2786	13181
DPR Design	10.08	2469	7104

The suggested DPR system achieves the target security and privacy with the minimum power and area utilization. The area utilization required to implement the selected encryption modes individually is larger than the area adopted by the dynamic design of the suggested DPR system, as shown in Table II. The DPR system saves the required LUTs utilization by 59.9% than the needed by the static design. Also, the power consumption of static design is larger than the maximum power consumption when using DPR.

TABLE III: Encryption Modes Results Using DPR Technique

Encryption Mode	Dynamic Power (mw)	LUTs Memory	LUTs Logic
ACORN	1.83	2521	3704
Pi-Cipher	10.08	2853	6332
JAMBU	2.243	2469	4295
MORUS	5.66	2469	7104
CLOC	3.66	2469	5997

The DPR implementation of the suggested encryption modes involve extra area utilization as shown in Table III because of the additional hardware of the DPR system that is added to the implementation such as: FIFOs, and PRC. However, PRC gives a good configuration time of 11.1545 msec. The static design increases the utilized area when more than one encryption mode is used, while the area of the DPR implementation becomes the same.

V. Conclusion

A comparative analysis is performed among multiple encryption modes. MORUS provides the largest throughput at the expense of the largest utilization area. Pi-Cipher consumes the largest power. ACORN, which is the only stream cipher among the selected encryption modes, consumes the minimum power and area at the expense of a small throughput in the range of Kbits/s. A FoM is calculated to compare between the selected modes. The best mode, after taking all factors (i.e., power, area, throughput, latency, and security) into consideration, is ACORN. Accordingly, ACORN is highly recommended specially when the used protocol does not require very high speed communication rates. Static implementation of all encryption modes on FPGA consumes power of 14.156 mW. However, DPR implementation is conducted to change among these modes during run time, giving that the maximum dynamic power is 10.08 mW.

Acknowledgment

This work was partially funded by ONE Lab at Zewail City of Science and Technology and Cairo University, NTRA, ITIDA, ASRT, Mentor Graphics, NSERC.

References

[1] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., "Internet of Things Strategic Research Roadmap," Internet of Things-Global Technological and Societal Trends, vol. 1, pp. 9-52, 2011.

[2] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in *IEEE Internet of Things Journal,* vol. 4, pp. 1250 - 1258, April 2017.

[3] Ruinian Li, Tianyi Song, Nicholas Capurso, Jiguo Yu, Jason Couture, and Xiuzhen Cheng, "IoT Applications on Secure Smart Shopping System," in *IEEE Internet of Things Journal,* vol. 4, pp. 1945 - 1954, May 2017.

[4] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao, ”A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,”in *IEEE Internet of Things Journal,* vol. 4, pp. 1125 - 1142, March 2017.

[5] C.-I. Cluster, ”Visions and Challenges for Realising the Internet of Things,” European Commission, 2010.

[6] M. Katsaiti, A. Rigas, I. Tzemos, and N. Sklavos, ”Real-World Attacks Toward Circuits & Systems Design, Targeting Safety Invasion,” in *Proceedings of the 4th International Conference on Modern Circuits and System Technologies (MOCAST),* 2015.

[7] U. Mamidi, ”Lightweight Authenticated Encryption for FPGAs,” 2016.

[8] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval, ”Lightweight Hardware Architectures for the Present Cipher in FPGA,” in *IEEE Transactions on Circuits and Systems,* vol. 64, pp. 2544 - 2555, April 2017.

[9] Mohammed Moness; Ahmed Mahmoud Moustafa,”A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy,” in *IEEE Internet of Things Journal,* vol. 3, pp. 134 - 145, September 2015.

[10] C. Alippi and C. Galperti, ”An adaptive system for optimal solar energy harvesting in wireless sensor network nodes,” in *IEEE Trans. Circuits Syst. I, Reg. Papers,* vol. 55, no. 6, pp. 17421750, Jul. 2008.

[11] A. A. R. Haeri, M. G. Karkani, M. Sharifkhani, M. Kamarei, and A. Fotowat-Ahmady, ”Analysis and design of power harvesting circuits for ultra-low power applications,” in *IEEE Trans. Circuits Syst. I, Reg. Papers,* vol. 64, no. 2, pp. 471479, Feb. 2017.

[12] F. Abed, C. Forler, and S. Lucks, ”General Overview of the First-Round CAESAR Candidates for Authenticated Encryption,” IACR ePrint, Report 2014/792, 2014.

[13] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, M. U. Sharif, and K. Gaj, ”GMU Hardware API for Authenticated Ciphers,” *IACR Cryptology ePrint Archive*, Report 2015/669, 2015.

[14] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, and K. Gaj, ”Implementer’s Guide to the CAESAR Hardware API”, 2016, available at https://cryptography.gmu.edu/athena/index.php?id=CAESAR

[15] H. Wu, ”ACORN: A Lighweight Authenticated Cipher (v3),” Candidate for the CAESAR Competition. See also https://competitions.cr.yp.to/round3/acornv3.pdf, 2016.

[16] Hongjun Wu and Tao Huang, ”The JAMBU Lightweight Authentication Encryption Mode (v2. 1),” http://competitions.cr.yp.to/caesar-submissions.html, 2016.

[17] A. Mileva, V. Dimitrova, and V. Velichkov, ”Analysis of the Authenticated Cipher MORUS (v1),” in *International Conference on Cryptography and Information Security in the Balkans*, pp. 45-59, 2015.

[18] T. Iwata, K. Minematsu, J. Guo, and S. Morioka, ”CLOC: Authenticated Encryption for Short Input,” in *International Workshop on Fast Software Encryption*, pp. 149-167, 2014.

[19] D. Gligoroski, H. Mihajloska, S. Samardjiska, H. Jacobsen, M. El-Hadedy and R. E. Jensen, ”πCipher v1” *CEASER Competition,* 2014.

[20] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, M. X. Lyons, P. Yalla, et al., ”Toward Fair and Comprehensive Benchmarking of CAESAR Candidates in Hardware: Standard API, High-Speed Implementations in VHDL/Verilog, and Benchmarking Using FPGAs,” 2016.

[21] A. Kamaleldin, A. Mohamed, A. Nagy, Y. Gamal, A. Shalash, Y. Ismail, et al., ”Design Guidelines for the High-Speed Dynamic Partial Reconfiguration Based Software Defined Radio Implementations on Xilinx Zynq FPGA,” in *Circuits and Systems (ISCAS), 2017 IEEE International Symposium on*, pp. 1-4, 2017.