Implementation of Efficient Bit Permutation Box for Embedded Security

NISHCHAL RAVAL, GAURAV BANSOD, DR. NARAYAN PISHAROTY
Electronics and Telecommunication
Symbiosis Institute of Technology, Symbiosis International University
Lavale, Pune, Maharashtra
INDIA
nishchal.raval@sitpune.edu.in, gauravb@sitpune.edu.in, narayanp@sitpune.edu.in

Abstract: - Security in every real time applications is of utmost importance. The secure architecture implemented in the automobiles such as EVITA (E-safety Vehicle Intrusion protected Application), SEVECOM (Secure Vehicle Communication) has rich cryptographic properties, but has more footprint area and high power consumption. This existing architecture uses standard engines like AES (Advanced encryption standard), Elliptical curves, Hash Engines which are heavy in memory requirement and consumes more power. So its reach is limited only to high end systems that consisting of large bit processors and coprocessors. Role of a bit permutation instruction in cryptographic environment is well proven. GRP (Group Operations) and OMFLIP (Omega-Flip) networks are bit permutation instructions and its implementation in hardware not only accelerates software cryptography but also results in less footprint area and low power consumption. This paper proposes a novel implementation and analysis of GRP and OMFLIP architecture for security in small scale embedded networks. In this paper a hybrid implementation is analysed and its results are compared with 'P' box of standard algorithms like AES and DES (Data Encryption Standard). This paper shows that GRP needs very less memory space as compared to other bit permutation instructions and will be useful to design lightweight ciphers.

Key-words: - OMFLIP, GRP, Embedded Security, Automotive, Encryption, Bit permutation

1 Introduction

Every system in the digital world is connected to many nodes and servers through which a large volume of data is exchanged and stored. This data can be transferred from one node to another over a wired or wireless medium. As data is transferred from one node to other it is open to threats from the environment [1]. Many systems are connected to external world through internet, Bluetooth or by any other media. This opens a wide gateway for mounting an attack and disrupts the operation. Data or information security is therefore an area of grave concern [2]. In application like automobiles where large number of microcontrollers are used popularly known as electronic control units (ECU's) and these ECU's communicate through a popular bus called CAN (Control Area Network) bus. CAN bus is extensively researched bus and the results from the papers shows that frames inside the bus can be manipulated to disrupt the communication or to have intended communication, that could results in damaging a system [3]. In present automobiles, there are at least 30 to 40 microcontroller that can communicate with each other over a CAN bus. This communication between nodes must be encrypted, so that only an authenticate controller can participate in communication. With the growing need to secure this communication a number of encryption standards and algorithms have been developed, designed and implemented to make a system secure. For automobile security projects like EVITA, SEVECOM have given deep insight in the area of secure communication. These models are based on threat to automobile communication from inside as well as from external environment [4]. These models uses heavy cryptographic algorithms like AES -128 (Advanced Encryption System), Hash engines, Elliptical Curve based system which are standard algorithms and are approved and endorsed by NIST (National Institute of Standard and Technology) [5]. For these algorithms and engines, cryptanalysis has been done and attacks are not yet proven. These cryptographic engines have a huge footprint area which makes the system slower and thus reduces throughput. Because of huge memory requirement, they are overkill for 8 bit systems [6]. As technology is advancing the need and necessity in cryptography is towards less

5 Hybrid Cryptosystem by using GRP and OMFLIP

GRP has better differential property while OMFLIP has good linear property, the combination of these two algorithms will make good permutation box that can be suited for light weighted embedded security [9][10]. The OMFLIP has 128 bit inputs for Encryption-Decryption and GRP will generate 128 bit (16 Hex values) key based on 16 bit hex value. OMFLIP-128 works exactly the same as OMFLIP-8 network. GRP generates the key based on 16 hex values and it is fed to OMFLIP network which performs encryption. User has to enter two hex values to decide number of stages of OMFLIP network. Two hex value results in 8 stages OMFLIP network which consisting of OMEGA and FLIP state. If user inserts 4F as input then system take it as 01001111 which selects three OMEGA and four FLIP stages. '0' represent OMEGA stage while '1' represents FLIP stage. OMFLIP network has less latency as compared to GRP [10] that is why it is used for performing encryption. GRP is used for key generation as it has shown good resistance to linear and differential cryptanalysis. This hybrid implementation is implemented on 32 bit processor LPC2129 by using KEIL 4.0 simulator. The fig. 8 shows block diagram of AES-128 which is implemented in Embedded C on LPC2129 at bit level. All standard algorithms in this paper we have implemented and compared on the same platform.

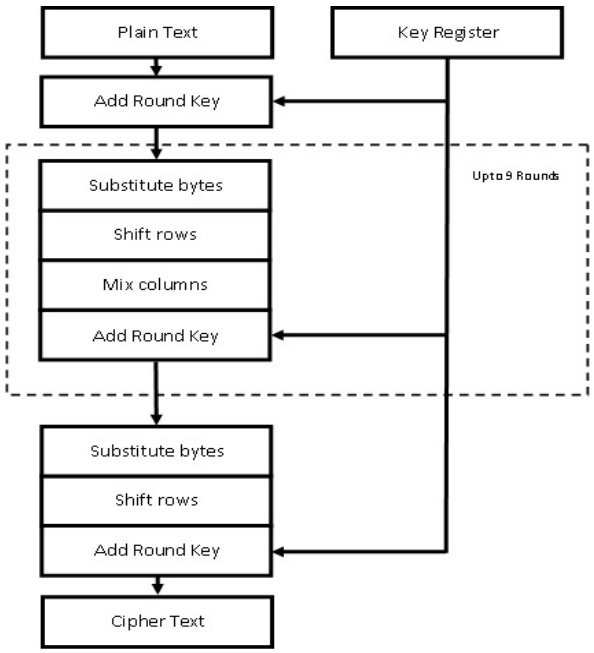

Fig. 8: AES-128 block diagram

In order to compare this hybrid system, we have also implemented AES-128 bit and DES on ARM processor. The fig. 8 shows comparative study of AES, DES, with our hybrid cryptosystem.

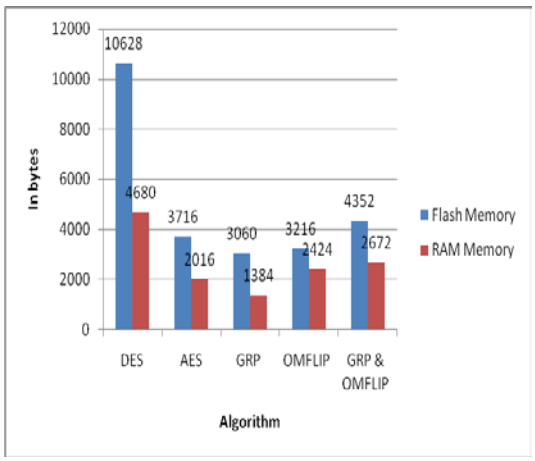

Fig. 9: Comparison with standard algorithm

From the Fig. 9, GRP and OMFLIP memory requirement is clearly depicted which requires around 3060 and 3216 bytes while AES needs 3716 and DES needs 10628 bytes of Flash memory. As GRP and OMFLIP have only diffusion properties, in Fig 9, only 'P' box of standard algorithms is compared with GRP and OMFLIP. 'P' box of GRP consumes very less memory among all algorithms which is around 1520 bytes of RAM while AES 'P' box results in 2384 bytes of Flash memory which is higher than GRP and near about same as OMFLIP. To the best of our knowledge this is the most optimized version of GRP which need 3060 bytes of Flash memory. From the fig. 10, 'P' box of GRP and OMFLIP does only permutation while in Fig 9 GRP and OMFLIP does key generation and encryption both individually that results into higher memory requirement.

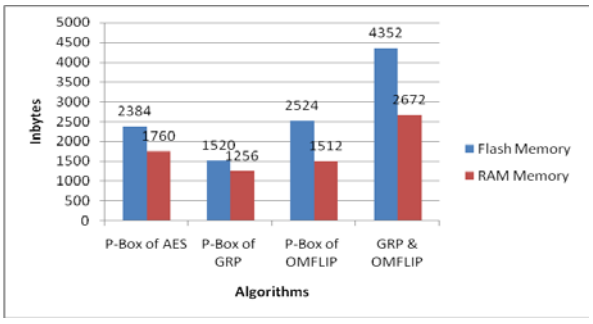

Fig. 10: 'P' box comparison

Bit permuation instructions are well known for compact hardware implementation. Even in the

lightweight cipher like PRESENT, bit permutation instructions are used in designing its 'P' box. The fig. 9 also depicts the memory required for implementation of GRP 128 bit would be very less compared to other bit permuatation instructions and also with AES. This work and result clearly shows a importance of bit permutation instructions in designing lightweight ciphers. By using GRP, one can optimized cipher memory requirements, thus helping reducing power consumption and number of processsing elements like transistors.

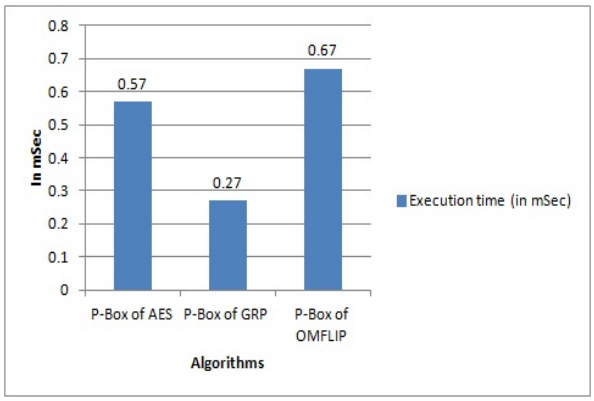

Fig. 11: 'P' box Comparison of execution time with standard algorithm

Fig 11 shows performance of GRP, OMFLIP and comparison with AES on 32 bit processor with clock frequency as 60Mhz. GRP takes only 0.27 milliseconds which is least as compared to other bit permutation instruction. OMFLIP have higher execution time as compared to AES and GRP due to number of Omega and Flip stages. Fig 11 depicts efficiency of GRP over other standard algorithms in terms of execution time.

D	E	F	G	H
On-Chip	Power (W)	Used	Available	Utilization (%)
Logic	0.000	40	7168	1
Signals	0.000	60	---	---
IOs	0.000	36	141	26
Leakage	0.060			
Total	0.060			

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	35.2	82.9	27.1

Fig. 12: Power consumption

Fig 12 shows power consumption of GRP bit permutation instruction which comes around 60milliwatts which is best suitable for small scale embedded applications. Power consumption is calculated based on Xilinx Xpower tool. For this hardware implementation and power consumption, code is written in Verilog. Previous papers on bit permutation instructions shows around 200-300milliwatts power consumption [12].This power consumption also includes method for reducing side channel attacks by using dual in rail package(DRP) by using balance instructions[21].Differential power analysis(DPA) attacks can be reduced by using balanced instructions.

6 Discussions and Conclusion

Role of bit permutation instructions in cryptographic environment is indisputable. Implementation of these instructions will accelerate not only cryptography, but also results in faster throughput, less power consumption and less footprint area. In the past, bit permutation instruction have been suggested and implemented for multimedia processing. Group operations (GRP), Omega flip (OMFLIP) networks are the more popular network in cryptographic environment. These networks require less memory space, less power consumption and have good cryptographic properties. Comparison shows OMFLIP architecture performs faster than GRP and requires less footprint area, while GRP has a minimum delay and can be implemented with different techniques by modifying or inserting elements in an existing basic model. These instructions are having edge over the existing secure architecture in terms of area, power and throughput of a system.

In this paper, OMFLIP design is made to be more flexible and robust. User can select the number of stages and which are the stages will be included in design and in what order, based on these parameters OMFLIP design will produce encrypted results. Moreover control words that are applied to each stages of OMFLIP are varied randomly each time [13]. This makes design more robust and induced good cryptographic properties. At the decryption end, the reverse process is applied and original data will be retrieved out. As in block ciphers, same key is used for decryption which is used at encryption level, but this key is stored at the receiver side. In this paper, we are dynamically during run time. We are sending encrypted data and the keys which are generated randomly at transmitter end to perform permutation. This avoids tampering of data at receiver end as keys are not stored but increases a channel over head. To the best of our knowledge, this is the first implementation of OMFLIP design on 32 bit processor. OMFLIP

design will be preferred because of less memory requirements and less power consumption for small scale embedded system security which operates on 8 to 16 bits of data. This design provides good performance with less power consumption which is generally a constraint for small hand held devices. OMFLIP can perform permutation for 'n' bits with maximum of log (*n*) steps.

OMFLIP hardware implementation performs faster than GRP as there are fixed number of stages, so size of 'n' can be of any length. Latency is also less as compared to GRP permutation and it completes permutation in one machine cycle [8][9][13]. These all parameters will provide an edge to OMFLIP network over GRP. OMFLIP network with 4 stages has latency of 13.8 while GRP has 22.7 clearly depicted in paper [13]. Two stage implementation of OMFLIP is the fastest solution and its implementation for 64 bit permutation requires only 48 bytes of memory [10].

In this paper, we have implemented a bit level permutation in hardware and evaluated its superiority by comparing it with an existing encryption method for a set of parameters and also for their resilience under an external and internal threat. OMFLIP and GRP design is best fit for providing rich security solution as efficient permutation box for small scale embedded system. It guards the constraints like less power consumption, less footprint area, faster throughput which are core of any embedded system design.

Implementation of bit permutation instructions will always results in compact hardware design. The RAM and ROM requirement for GRP would be very less as compared to other bit permutation instructions. Number of processing elements required for bit permutation instruction is also less. Lightweight cryptography is the field where use of bit permutation instructions will result in more compact hardware design. Only disadvantage about GRP is its latency. Time required for execution of GRP would be slightly more compared to other instructions. Future work will include implementation of bit permutation instructions in designing lightweight block ciphers. GRP lacks substitution property. Designing 'S' box for GRP may make the design more compact and more robust. Implementation of bit permutation instruction for embedded system security will emerge as lone robust solution in an eternal world of low power security design.

Acknowledgement

The authors would like to thank Symbiosis Institute of Technology, Pune, Symbiosis International University, Pune for providing resources to carry out this research successfully.

References:

[1] Marko Wolf, Andre Weimerskirch, Christof Paar, "*Secure –In Vehicle Communication*", Embedded Security in Cars, Springer, 2006.

[2] Tobias Hoppe, Stefan Kiltz, Jana Dittmana, "*Security Threats to automotive CAN network*", SAFECOMP 2008, LNCS5219, Springer, 2008.

[3] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, "*Experimental security Analysis of a Modern automobile*", IEEE symposium on security and privacy, Oakland, CA, May 2010.

[4] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, "*Comprehensive Experimental Analysis of Automotive Attack Surfaces*" , USENIX Security, August 10–12, 2011.

[5] Hendrik Schweppe, Yves Roudier, "*Security issues in Vehicular System*", SAR-SSI 2010, 5TH Conference on Network architectures and information system security, EVITA project, 2010.

[6] Alireza Hodjat, Ingrid Verbauewhede, "*The Energy cost of secrets in adhoc Network*", Proceedings of the IEEE Circuits and Systems Workshop on Wireless Communications and Networking, 2002.

[7] Hwang P. Schaumont, K. Tiri, and I. Verbauwhede, "*Securing Embedded System*", IEEE Security & Privacy, 4(2):40–49, 2006.

[8] Zhijie Shi and Ruby B. Lee, "*Sub word sorting with Versatile Permutation Instructions*", Proceedings of the 2002 IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD'02).

[9] Ruby B. Lee, Z. J. Shi and Y. L. Yin, Ronald L. Rivest, M.J.B. Robshaw "*On Permutation Operations in Cipher Design*" Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference 5-7 April 2004.

[10] Zhijie Jerry Shi, "*Bit Permutation Instructions: Architecture, Implementation and Cryptographic Properties*", Princeton, June 2004.

[11] Miller Alexander, Prof. Dr.-Ing Gunar Schorcht, *Embedded systems security: Performance Investigation of various cryptographic techniques in embedded systems*, http://www.kaspersky.com/images/miller,_alexander_embedded_systems_security_performance_investigation_of_various_cryptographic_techniques_in_embedded_systems-10-98478.pdf

[12] Gaurav Bansod**,** Aman G, Arunika G, Gajraj B, Chitrangdha S, Harshita A, "*Experimental analysis and implementation of bit level permutation instructions for embedded security*". *WSEAS Transactions on Information Science and Applications*, 10(9): 303-312 (Scopus; ISSN: 1790-0832), 2013.

[13] Z.J.Shi and R.B.Lee, "*Implementation Complexity of Bit Permutation Instructions*", in Proc. Asilomar Conf.Signals Stst. Computer, pp 879-886, 2003.

[14] Yedidya Hilewitz, Zhijie Jerry Shi and Ruby B. Lee, "*Comparing Fast Implementations of Bit Permutation Instructions*" Signals, Systems and Computers, *2004.* Conference Record of the Thirty-Eighth Asilomar Conference 7-10 NOV 2004.

[15] Zhijee Shi, Ruby B. Lee, "*Bit Permutation Instructions for accelerating Software cryptography*", Application-Specific Systems, Architectures, and Processors, 2000. Proceedings. IEEE International Conference, JULY 2000.

[16] Giorgos Dimitrakopoulos, Christos Mavrokefalidis, Kostas Galanopoulos and Dimitris Niolos, "*Sorter based permutation units for Media-Enhanced Processors*" IEEE Transactions on VLSI systems, vol 15, no. 6, pp 711-715, June 2007.

[17] Jer Min Jou, Yun Lung Lee, Chen Yen Lin and Chien Ming Sun, "*A Novel Reconfigurable computation unit for DSP applications*", IEEE comp. society annual symp. On VLSI, ISVLSI'07, pp 439- 444, 9-11 March 2007.

[18] Navid Lashkarian, Ed Hemphi, Helen Tarn, Hemang Parekh and Chris Dick, "*Reconfigurable Digital Front End Hardware for wireless base-station transmitters: Analysis, Design and FPGA implementation*", IEEE transactions on circuits and systems, vol 54, No. 8, pp 1666-1677, Aug 2007.

[19] Souvik Kolay, Sagar Khurana, Anupam Sadhukhan, Chester Rebeiro and Debdeep Mukhopadhyay, "*PERMS: A Bit Permutation Instruction For Accelerating Software Cryptography"*, 16th Euromicro Conference on Digital System Design, Sept 04-06, 2013.

[20] Philipp Grabher, Johann Grobschadl, and Dan Page, "*Light-Weight Instruction Set Extensions for Bit-Sliced Cryptography*", Lecture Notes in Computer Science - CHES2008, Volume 5154, 2008, pp 331-345.

[21] Zhimin chen, Ambuj sinha,Patrick schaumont, "*Using virtual secure circuit to protect embedded software from side channel attacks"*IEEE Transactions on Computers, VOL 62, No 1, JAN 13.