Experimental analysis and implementation of bit level permutation instructions for embedded security

GAURAV BANSOD, AMAN GUPTA, ARUNIKA GHOSH, GAJRAJ BISHNOI, CHITRANGDHA SAWHNEY, HARSHITA ANKIT
Electronics and Telecommunication
Symbiosis Institute of Technology, Symbiosis International University
Lavale, Pune, Maharashtra
INDIA
gauravb@sitpune.edu.in

Abstract: - With the increasing use of electronic control units (ECU's) in automobile or in any embedded system security becomes an area of grave concern. Information is exchanged between ECU's over a CAN (Control Area Network) bus, vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communication. These interactions open a wide gateway for manipulating information which could lead to disastrous results. EVITA, SEVECOM, SHE are existing security models to address these concerns in automobiles but at the cost of huge footprint area and more power consumption as it uses cryptographic engines like AES-128,ECC, HMAC. We propose the use of bit level permutation GRP (group operations) in cryptographic environment which not only accelerates cryptography but also has a positive impact of providing low cost security solution that is having good encryption standards, relatively less footprint area, less cost and low power consumption. Use of GRP in cryptographic environment is a unique solution for all security applications where footprint area and power consumption are constraints .This paper shows implementation of GRP in embedded C, over a CAN bus on ARM7(LPC2129) and on FPGA. It is the first successful attempt to have universal and optimized structure of GRP and its implementation. Measures on side channel attacks on GRP like differential power analysis (DPA) are incorporated in this paper. This architecture with the use of bit permutation instruction will pave a new way in securing small scale embedded system.

Key-Words: - Security, Automobile, Embedded system, GRP, CAN bus, ECU

1 Introduction

Huge volume of data is stored and transferred from one node to another, information is being exchanged among vehicles. These nodes, information, and data needs to be protected, and authenticated in order to have reliable communication. As most of the systems are not isolated for the purpose of updating, they become more vulnerable to external or internal attacks. These sporadic attacks on system can manipulate the information or data present in the system, or can mislead the communication from one node to other and these could have dire consequences. Data or information security is an area of concern to protect the system from any external or internal threats [2]. In applications like automobiles a large no of electronic control units (ECU's) are used inside for a communication between 'n' no of nodes. These nodes communicate through a bus called CAN (Control Area network) bus. CAN bus is extensively researched, and many instances and paper shows the frames inside the bus can be studied and manipulated to disrupt the communication or to have intended communication and which would results into a non intended results and damage a system[7][15]. In automobile 30 to 40 microcontrollers communicate with each other over a CAN Bus .This communication over nodes must be protected, encrypted so that only authenticate controller can participate in communication. Electronic Control Units (ECU's) are relying on other ECU's or on environment created by ECU's for validated information [15]. With the growing need to secure this communication a number of encryption standards, algorithms have been developed, designed and implemented to make the system more secure. For automobile security, projects like EVITA (E-safety Vehicle Intrusion protected Application), SEVECOM (Secure Vehicle Communication) has 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. These models use very high ended encryption algorithms like AES-128(Advanced Encryption System), Hash engines, Elliptical Curve based system which are standard encryption algorithms and are approved and endorsed by NIST (National Institute of Standard and Technology) [4]. For these algorithms and engines cryptanalysis is done and attacks are not yet proved. Some of the Next Generation Encryption (NGE) algorithms are proposed by CISCO is mentioned in Table 1. These algorithms are expected to meet security requirement for more two decades. These encryption engines are having huge footprint area which makes the system slower and thus reduces throughput of a system. These cryptographic engines required huge computational power [11]. A system like small scale embedded system that operates on 8 to 16 bit processor have limited memory space and have less power consumption. Implementing a heavy algorithm for security in these system will be overhead on system efficiency and could not be feasible in terms of memory requirement. These systems need to be secure with light weighted secure architecture [20]. In embedded system, security architecture with less power consumption, less footprint area is the need without losing encryption standards. In embedded system, information must be conveyed with lesser no of bits and with less power to the destined node without falling prey to attacks [7]. Based on the need, requirement the approach which incorporates all constraints such as bandwidth, power, memory requirement, a methodical approach is provided in this paper that suggests use of bit permutation instructions GRP for securing automotive environment or small scale embedded system. These bit permutation instructions are rich in encryption standards, less footprint area and low power consumption. In this paper we have studied the characteristics of GRP and its role as cryptographic element to secure an environment. Side channel attacks likes differential and simple power analysis (DPA and SPA) are more popular attacks in cryptographic environment. Through these attacks one can study the analog characteristics of power supply and can find out secret key, non shared information Different preventive techniques are incorporated in this design to avoid invasive and non invasive attacks. Invasive attacks will find out information from chips (IC’s) by demounting it and studying characteristics, requires more expensive equipments. Non Invasive attacks are low cost and can be easily implemented, need to study characteristics of power variation, electromagnetic radiation. Use of balanced instructions [16] can nullify the effects of DPA by flattening the power spectrum so that no variations in power can be observed and studied.

Engines	**Functions**
AES CBC Mode	Encryption
AES GCM Mode	Authenticated Encryption
DH-2048	Key Exchange
RSA- 2048	Encryption
DSA-2048	Authentication
HMAC-SHA-1	Integrity
ECDH-256	Key Exchange
ECDSA-256	Authentication

Table1: NGE algorithms by CISCO

2 Security threats to CAN

CAN Bus has wide application in the area of automobiles. Many experiments have been performed over a CAN bus and results shown a numerous attacks on packets transferred between nodes [2][7]. In the previous work [2], [7], [15], attacks are mounted over CAN Bus in automobiles and packets have been changed. These all possible attacks are placed through OBD-II diagnostic port available just below dash board in a vehicle [7]. This port is basically used for flashing, updating the ECU’s time to time. Attackers use this port to spoof the fake message or wrong message over a CAN bus. Experimental results in[7][15] shows many vital functions like Antilock Braking system(ABS),brakes can be disabled , light switching are operated remotely, wrong messages can be displayed over a speedometer board. Most of the functions in automobiles can be hacked, remotely controlled by accessing CAN bus. In paper [2], experimental setup is shown which is displayed in fig 1, which shows the process to interface controller to ECU via OBD-II diagnostic port. As mentioned in [15], wireless tire pressure monitoring system (TPMS) can be attacked and erroneous messages will be displayed on dash board, Windows operating system on laptop can be easily interface through OBD-II port via standard SAE J2354 API. An attack has mounted through Audio CD's Disks, USB that result into display of erroneous message on GUI of MP3 player [7].

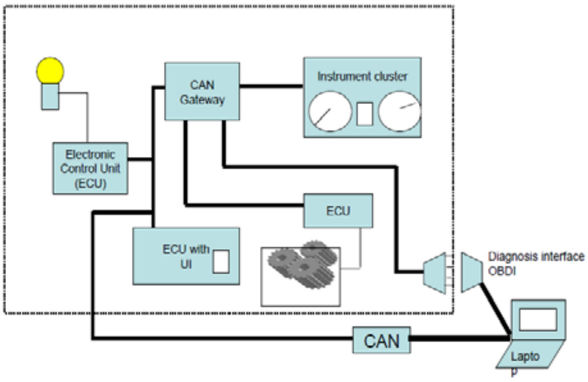


Fig1: Experimental Setup for analyzing ECU's and CAN Bus Packets

Packets over CAN bus are studied and manipulated through CANSHARK interface as shown in paper [7]. Tool is used to inject new packets over CAN bus. One can stop the car suddenly, disables the main functions through this interface. In paper [7] AVR controller is used to interface with OBD-II port that is generally used to update the ECU's or diagnosis a communication over CAN Bus. CAN bus have many weaknesses and it can be attacked. Research work in the papers [7] [15] shows that it is easy to disrupt the communication over a bus. This entire situation demands a secure environment to protect this communication from internal as well as external threats. Any field bus connected to more than one ECU's will possess a threat from external environment. The security model uses off the shelf component like AES-128, ECC, Hash engines and are mapped together to provide a secure model. In order to protect small systems that has constraints like power, memory, is these heavy cryptographic engines will be a feasible option. There should be alternative security option which could protect these small scale embedded system. Secure algorithms which can be used for these systems should not be complex in nature and should give cost effective solution.

3 GRP at GATE level

Bit level permutations are basic operations in cryptographic environment. Their inclusion in cryptographic environment not only accelerates software cryptographic process but also strengthen existing ciphers [9]. GRP (Group operation) inclusion in processor gives higher throughput and results in less power consumption which is very likely constraints in small scale embedded systems [9]. Concept of subword parallelism is also introduced in GRP where 16 bits of data is divided into 8 bits of subword. Bit level operations have applications in designing block cipher, stream cipher and hash functions. GRP is basically a group operation which is divided into two parts based on the 1's and 0's .Corresponding 1's are gathered at left hand side and 0's at right hand side. This gives the basic GRP sorting operation. The fundamental operation is explained in Fig 2

A	**B**	**C**	**D**	**E**	**F**	**G**
1	0	0	1	0	1	1
A	**D**	**F**	**G**	**B**	**C**	**E**

Fig 2: Basic operation of GRP

Algorithm is defined for generating GRP instructions[3] and code word generation based on a specific arrangement is also shown in paper[3].GRP is uded for encryption and also for key generation process. Different code words has been designed based on different arrangement and bit positions. GRP requires only few instructions for execution as compared to other existing bit level instructions like PPERM3R [3]. Many structures have been proposed and designed based on GRP instruction for sorting[13]. Enhanced merge sorter Network(EMS), Modified enhanced merge sorter network[MEMS] has been designed with the help of 2x1 multiplexers [21]. But all these structures are designed for specific arrangement and for specific bit positions, based on that it will generate a specific code word. The structure for GRP Transmitter is shown in Fig 3. This is the universal structure which consiting of series of 2x1 mulitiplexers. Based on the input positions like 7,2,3,4,5,6,0 , the structure genrates a control word that can be used as a key for doing encryption [3].In Fig 3 it shows the encryption result for specific arrangement. This structure consumes less power as basic block 2x1 multiplexer is used for doing permutation. GRP is lightweighted architecture and can be suitable for small bit processor. Research shows that GRP operation is resistive against differential and linear cryptanalysis.A GRP structure consisting of three stages as shown and swapping of bits is performed based on the control words applied to 2x1 multiplexer, that act as select lines for multiplexer.The strucure shown is implemented at GATE level by using VERILOG and implemented on FPGA.

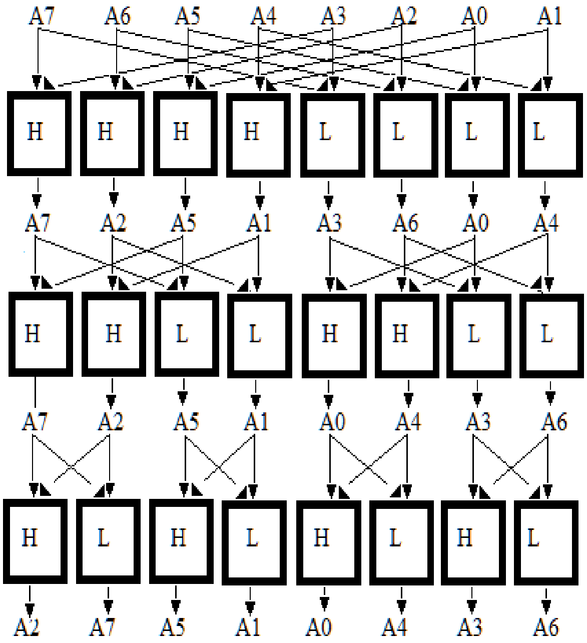


Fig 3: Transmitter GRP for 8 bits

As shown in Fig 3, inputs are given to structure and they are grouped according to GRP algorithm mentioned in paper[3]. In this arrangements groups are(A7,A3) ,(A6,A2), (A5,A1) and (A4,A0) based on no of inputs .Based on the arrangement A7,A6,A5,A4,A3,A2,A0,A1, three control words are generated and applied to three stages of a transmitter .Control words according to GRP are 10101100,11010010and 00101010.Control word generation is well explained in paper[3].H and L indicates corresponding higher order and lower order 2x1 multiplexers. Process of sorting with respect to codeword is mentioned in Fig 4.Similarly receiver structure has been designed for givrn arrangement and three control words are applied to the structure to get the original information back. Receiver for GRP 8 bit operation is shown in Fig 5. and process is explained in Fig 6. This architecture of GRP does a encryption and decryption process for 8 bits . Similar structure can be designed for 8 bits parallely that gives rise to concept of subword parallelism. Some multiplexers in a structure can be reduced to optimized power consumption .

A7	**A6**	**A5**	**A4**	**A3**	**A2**	**A0**	**A1**
1	0	1	0	1	1	0	0
A7	**A2**	**A5**	**A1**	**A3**	**A6**	**A0**	**A4**
1	1	0	1	0	0	1	0
A7	**A2**	**A5**	**A1**	**A0**	**A4**	**A3**	**A6**
0	0	1	0	1	0	1	0
A2	**A7**	**A5**	**A1**	**A0**	**A4**	**A3**	**A6**

Fig 4: Process of sorting with respect to control word at transmitter

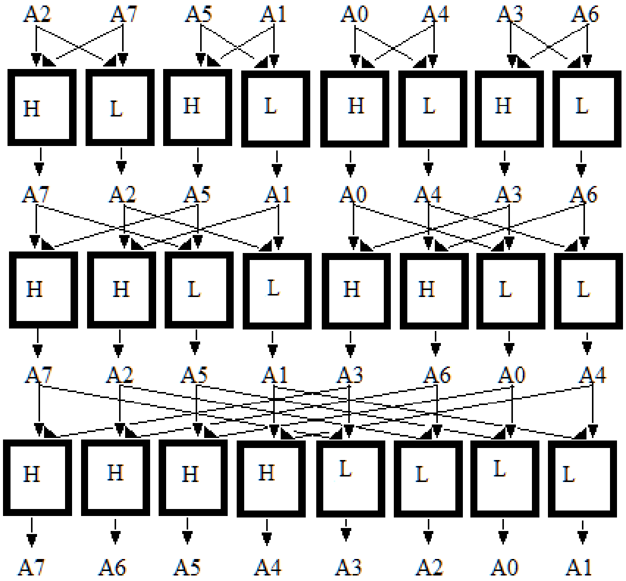


Fig 5: Receiver GRP for 8 bits

A2	**A7**	**A5**	**A1**	**A0**	**A4**	**A3**	**A6**
0	0	1	0	1	0	1	0
A7	**A2**	**A5**	**A1**	**A0**	**A4**	**A3**	**A6**
1	1	0	1	0	0	1	0
A7	**A2**	**A5**	**A1**	**A3**	**A6**	**A0**	**A4**
1	0	1	0	1	1	0	0
A7	**A6**	**A5**	**A4**	**A3**	**A2**	**A0**	**A1**

Fig 6: Process of sorting with respect to control word reciever

4 Secure GRP architecture

Side channel attacks (SCA) are very well known in cryptographic environment. Specifically differential power analysis (DPA) can observe power variations in a circuit and find out the key information based on static and dynamic power consumption. In order to secure GRP model against power attacks, we integrated circuit with Dual in rail precharge(DRP) technique used for resisting side channel attacks[16]. DRP technique uses balance instructions like and, or and not and create a structure complementary to our original structure.”AND” will be replaced by “OR” and vice versa and “NOT” itself is complementary. Input data will also get inverted and complementary results can be derived [16].This technique will flatten the power spectrum and thus helps to resist circuit against DPA. Many waveforms for protected Advanced Encryption Standard (AES) and unprotected AES are generated and explained in paper [16]. Integrated GRP structure with DRP for both transmitter and receiver is shown in Fig 7 and 8. Multiplexers are reduced if the particular bits are not swapped for specific arrangement thus reducing power consumption. The architecture shown in the Fig are implemented at GATE level by using VERILOG. This architecture uses balance instructions to provide resistance against side channel attacks. This is the first implementation of GRP with dual in rail precharge technique at GATE level which makes this model more robust for embedded security.

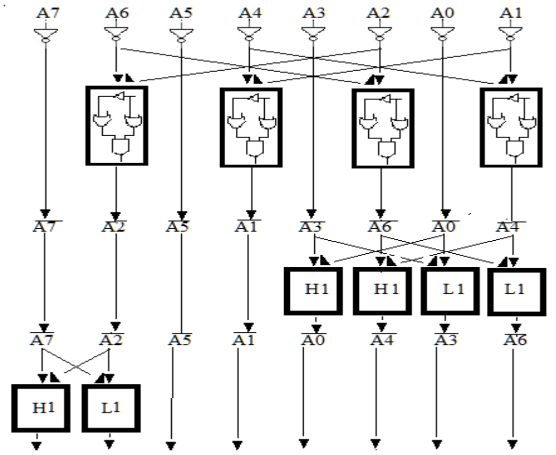


Fig 7: Integrated GRP with DRP transmitter with reduced muxes

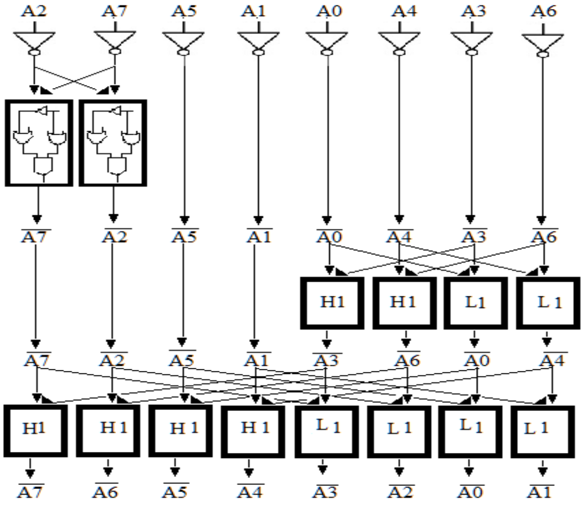
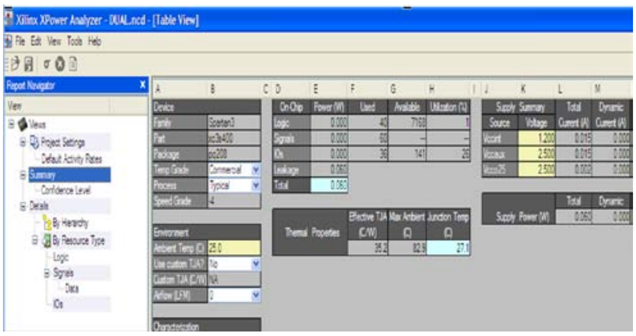


Fig 8: Integrated GRP with DRP reciever with reduced Muxes

As shown in Fig 7 and 8 complementary structure of multiplexer is created and in that “and” is replaced with “or” gate and vice versa to secure circuit against side channel attacks.Complenetary structure which uses balance instructions have been created to nullify the effect of power varaiation observed due to the bit change from 0 to 1 and vice versa. As in GATE level modelling design executed modeule by module.First in this design GATE level modelling for GRP is executed later exactly the inverse code as mentioned with the use of balance instructions.In this design , randomly we have introdeced complementary instructions so that intermediate varaiables cannot be traced and observed . As verilog is sequential the intermediate variables are sequentially calculated and thus the power variation in circuit. One can easily trace out that the first part belong to original data and the other half is complementary to it. But by putting complementary balanced instructions at random positions will sort out the problem and key will not be traceable through DPA.Power calculation for transmitter and reciver is derived for 16 bits through XPOWER tool of Xilinx ISE 11 and power for transmitter and reciver structure came around 60 mW as shown in Fig 9 and 10. For 16 bits it came around 240mW that is lower as comared to other existing structures.


Xilinx XPower Analyzer - DUAL.ncd - [Table View]

Device	
Family	Spartan3
Part	xc3s400
Package	pq208
Temp Grade	Commercial
Process	Typical
Speed Grade	-4

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	0.063			

Supply Source	Summary Voltage	Total Current (A)	Dynamic Current (A)
Vccint	1.200	0.015	0.000
Vccaux	2.500	0.015	0.000
Vcco25	2.500	0.002	0.000

	Total	Dynamic
Supply Power (W)	0.060	0.000

Environment	
Ambient Temp (C)	25.0
Use custom TJA?	No
Custom TJA (C/W)	NA
Airflow (LFM)	0

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

Characterization

Fig 9:Power calculation for transmitter on XPower

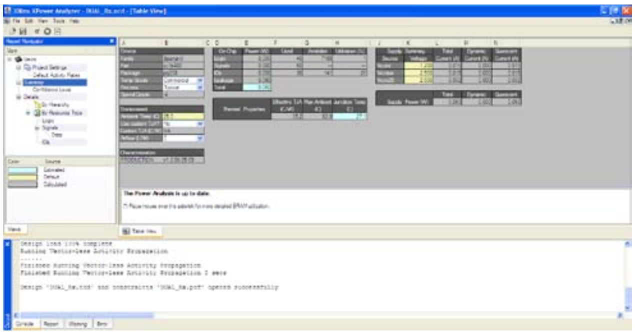

The Power Analysis is up to date.

Fig 10:Power calculation for Receiver on XPower

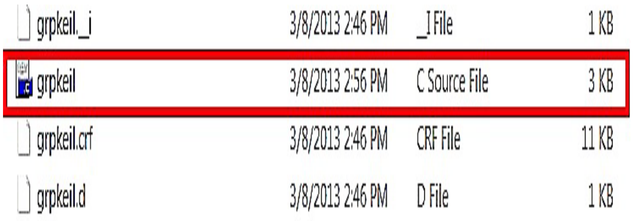
Fig 9 and Fig 10 indicates power calculation for GRP with DRP integrated designTable 2 shows power consumption and comparison of other structures based on GRP[21].The other secure models based on GRP as mentioned in paper[21] contributes more power as compared to our proposed design.

Design based on GRP	Power(mW)
Sorter Based Permutation	270
MEMS	600
Integrated GRP with DRP	240

Table 2: Comparison of GRP based structures: Power calculations

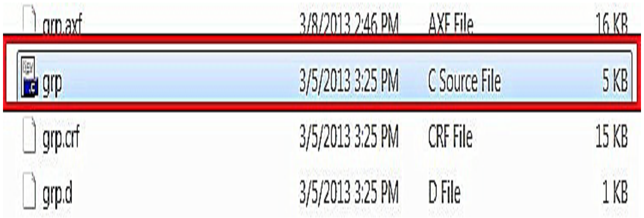
5 Universal GRP structure

In secure environment, key generation is the critical aspect. In internet applications, session keys are generated for a specific session and again after stipulated interval of time, different session key is generated. RSA is generally preferred for key generation as standardized algorithm. GRP can be used for encryption as well for key generation [3]. But the designs based on GRP are arrangement specific. It works only for a specific arrangement [21]. For some other arrangement different structure need to design. In this paper we made a first successful attempt to have a universal structure of GRP which generates the codeword for any arrangement and thus helpful for random key generation. The code is written in Embedded C. Initially universal GRP algorithm designed by using 2D arrays which conumes 5k of memory space.As it is designed for embedded system application ,memory space is always an constraint. Compressed GRP universal algorithm is designed by converting 2D arrays to 1D arrays and reduced to 3K which reuces more power consumption.Code is tested on ARM7 LPC2129 through Keil Uvision 4 .Fig 11 and 12 shows memory space for both compressed and uncompressed versions of universal GRP structure.



grpkeil_i	3/8/2013 2:46 PM	_I File	1 KB
grpkeil	3/8/2013 2:56 PM	C Source File	3 KB
grpkeil.crf	3/8/2013 2:46 PM	CRF File	11 KB
grpkeil.d	3/8/2013 2:46 PM	D File	1 KB

Fig 11: Compressed Version of GRP in terms of memory requirement

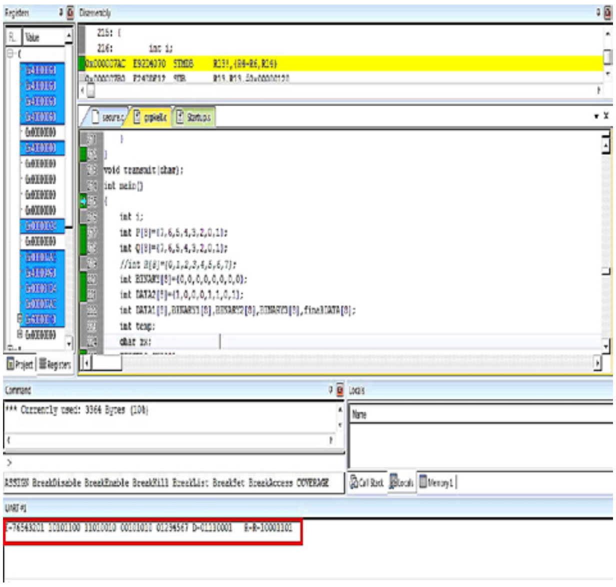


grp.axf	3/8/2013 2:46 PM	AXF File	16 KB
grp	3/5/2013 3:25 PM	C Source File	5 KB
grp.crf	3/5/2013 3:25 PM	CRF File	15 KB
grp.d	3/5/2013 3:25 PM	D File	1 KB

Fig 12: Uncompressed version of GRP in terms of memory requirement.

This universal GRP program is written for encryption as well for decryption. It can be also used for different and dynamic code word generation.GRP universal algorithm for encryption and decryption simulated on KEIL and UART act as a demonstrator. As shown in Fig. 13, on the UART window output at the bottom, first it shows basic arrangement which is 76543201, and then it shows 3 different control word based on GRP algorithm which is getting matched with the structure and arrangement discussed in this paper. It shows encrypted position which is 01234567, which will be output for any GRP last stage operation, but bits on that respective positions remains unpredicted. Finally it shows encrypted and received data.

GRP universal structure designed based on sorting, mapping, substitution and permutation. It is challenging to form the groups and in each group what will be the count for example (A3, A7) or (A6, A2, A5). Based on array position and comparison of present positing with the previous positioning we started sorting and storing index position if condition satisfies. If not, increase the variable size and repeat the loop. This procedure continues until and unless all positions are not sorted out. With the help of basic GRP algorithm explained in paper [3] we calculated the monotonically increasing sequences (MIS) and sorted it based on the value of m which is k/2, where m indicates no. of bit positions and k indicates grouping no. This universal GRP structure can randomly changes bit position and that results into change in control words.



```
215: {
216:        int i;
0x000007AC  E92D4070  STMDB     R13!,{R4-R6,R14}
```

```
    }
}
void transmit(char);
int main()
{
    int i;
    int P[8]={7,6,5,4,3,2,0,1};
    int Q[8]={7,6,5,4,3,2,0,1};
    //int R[8]={0,1,2,3,4,5,6,7};
    int BINARY[8]={0,0,0,0,0,0,0,0};
    int DATA2[8]={1,0,0,0,1,1,0,1};
    int DATA1[8],BINARY1[8],BINARY2[8],BINARY3[8],finalDATA[8];
    int temp;
    char tx;
```

```
*** Currently used: 3364 Bytes (10%)
>
ASSIGN BreakDisable BreakEnable BreakKill BreakList BreakSet BreakAccess COVERAGE
```

```
I-76543201 10101100 11010010 00101011 01234567 D-01110001   E-R-10001101
```

Fig 13 :UART as demonstrator for Universal GRP algorithm

6 GRP implementation over CAN bus

GRP is used to design block ciphers which are basic building blocks in cryptographic structures. Fast bit level permutations will get included in future processor architectures.GRP has good cryptographic properties, easy to implement and will take only 1-2 cycles of execution, while MULTIPLY instruction itself will take 3-4 cycles of execution[9].In this paper we have implemented GRP universal algorithm over CAN Bus to show the demonstration of GRP as a secure algorithm over two nodes on 32 bit processor LPC2129 levels. We have transmitted encrypted message from one node and it got decrypted at other destined node after adding security levels over a bus. Similarly entire communication over 40 nodes can be encrypted by using this light weighted crypto algorithm. In this paper we have implemented half duplex as well as full duplex encrypted communication over a CAN Bus. GRP is serving as cryptographic engine to secure an environment over a CAN bus. As shown in a setup we have communicated information through two nodes, which can be further extended till 40 nodes with 1Mbps speed. Fig 14 shows basic setup on ARM7 LPC2129 board. It consisting of on board 10 bit A/D converter and 4 analog input channels. One of the channels should be selected and connected to any sensor or to any analog source. Data from that sensor should be encrypted through GRP and sent to other node through CAN bus.

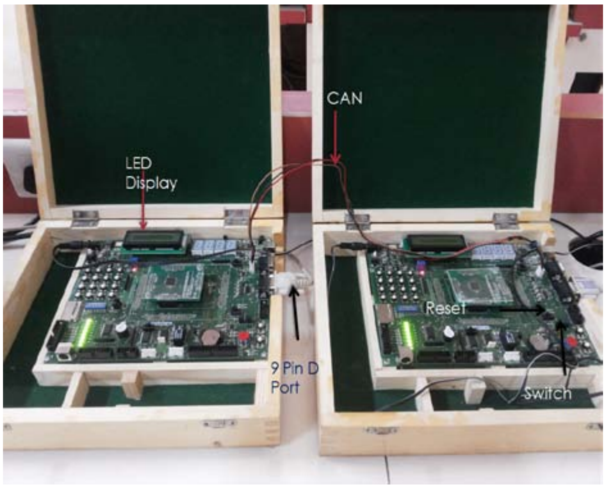
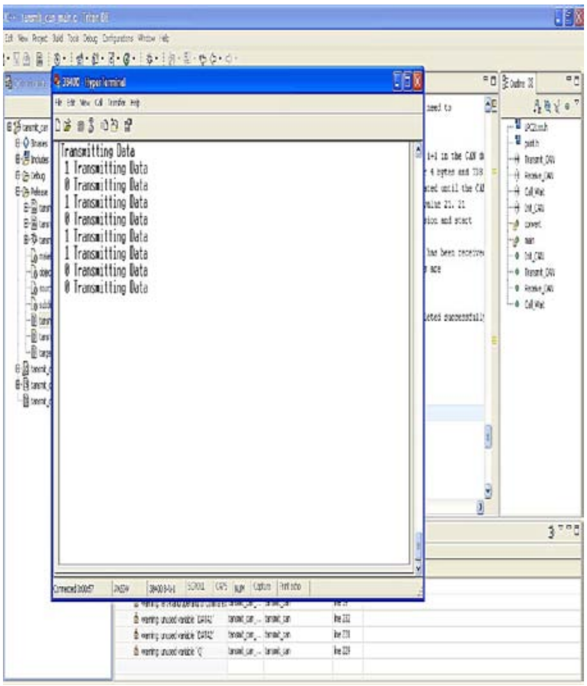


Fig 14: Basic Setup of CAN Bus over ARM7 (LPC2129)

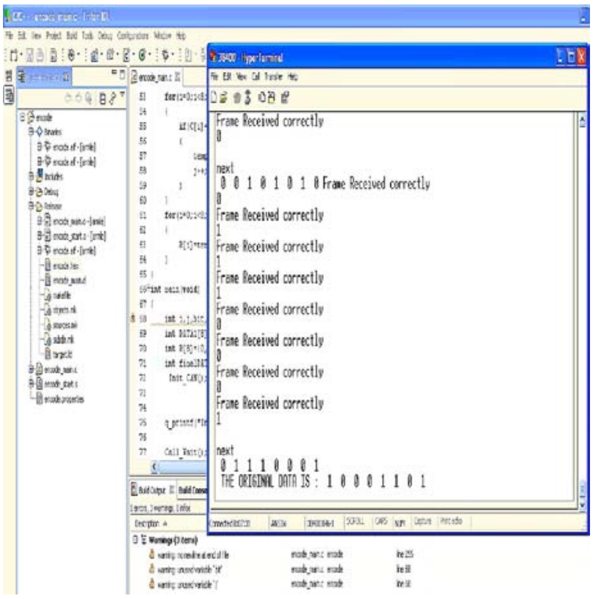
CAN bus registers are configured to have basic communication over two nodes. Both half duplex and full duplex encrypted communication can be seen over a HyperTerminal window which is configured at 38500bps. This entire function is simulated through Titron IDE licensed tool. Fig 15 and 16 shows full duplex transmitter and receiver encrypted communication over a CAN Bus.



```
Transmitting Data
 1 Transmitting Data
 0 Transmitting Data
 1 Transmitting Data
 0 Transmitting Data
 1 Transmitting Data
 1 Transmitting Data
 0 Transmitting Data
 0 Transmitting Data
```

Fig 15 : Encyption over a CAN bus at hyperterminal

GRP implementation over a CAN bus is a demonstrator that shows a cryptographic algorithm based on GRP can be implemented foa any apllications where no of ECU's are connected through a bus and also for point to point communication.



```
Frame Received correctly
0


next
 0 0 1 0 1 0 1 0 Frame Received correctly
0
Frame Received correctly
1
Frame Received correctly
1
Frame Received correctly
1
Frame Received correctly
0
Frame Received correctly
0
Frame Received correctly
0
Frame Received correctly
1


next
 0 1 1 1 0 0 0 1
 THE ORIGINAL DATA IS : 1 0 0 0 1 1 0 1
```

Fig 16 : Decryption over a CAN Bus at Hyperterminal

7 Discussion and scope

In this paper GRP is suggested to be an attractive alternative in cryptographic environment for embedded security application. Its use not only accelerates software cryptography but also computation speed and throughput [3][13][21]. Use of bit level permutations in cryptography will achieve a tangible target of good encryption standards with less footprint area which results in less power consumption. Small scale embedded system which requires security and use of standard heavy engines like RSA ,ECC will not offer a feasible solution, there exist a bit level permutations instruction like GRP that can give a holistic and methodical approach. GRP use in securing small scale embedded system will be having a positive impact in terms of speed, power consumption and footprint area. All standardized cryptographic algorithms have huge footprint area and complex process which makes them infeasible for small scale embedded systems where memory is the constraint. In automobiles communication is done over CAN Bus, literature review shows that the information over CAN Bus is not secured and can be manipulated, thus need to provide measures to secure CAN Bus. Software implementation of cryptographic algorithms consumes more power as compare to its hardware implementation. Need to design a hardware implementation of cryptographic algorithm which accelerates sorting and permutation process in encryption. Standard algorithm decryption process will consume more power than encryption, like in case of AES 128 decryption consumes 30% more power than encryption [18]. Measure should be taken to dissipate less energy while securing an environment. Hardware architecture accelerates cryptography but lacks flexibility while software versions have high flexibility but consumes more power [8]. We need to have balance between hardware and software design in securing an embedded system environment. Based on applications, module can be designed into software while other in hardware to reach out perfect balance between flexibility and speed.

GRP, a bit permutation instruction has only "diffusion" property while "confusion" is not introduced in the architecture. By generating a key size more than 64 bit through GRP, architecture can become more robust and a "confusion" process can be added in this design. In this design randomly keys are refreshed based on bit positions in order to make circuit more resistive against attacks. Very less time attacker has to predict the generated key, as GRP has minimal latency as compared to other bit permutation instructions. In this paper we have shown a communication over two nodes can be encrypted through GRP.

8 Conclusion

In this paper an alternative approach is shown and implemented to secure a small scale embedded systems. Our main aim is not to compare AES and GRP, by considering the fact AES has good robust design and no attacks are proven yet. In AES, system is so complex due to long key size and nearly twenty rounds of permutations and complex design that makes the system more resistive against attacks. Bit permutation instruction is having good cryptographic properties and easy to implement. The research carried out by Zhijie Jerry Shi shows GRP differential and linear cryptanalysis. Its use in applications like where there are more than one ECU's are communicating over a bus , instead of using standard engines like AES we can adopt architecture based on bit permutation instructions. This architecture support less memory requirement, flexible design and less computational power. These all properties are the constraints for small scale embedded systems. The only weakness that design is as compared to AES is rich and robust encryption design. These can be overcome by randomly changing the bit positions and using 128 bit key size. By using bit permutation instructions with longer key size and randomly refreshing key will provide a robust architecture which meets all constraints of small scale embedded system.

There is wide scope in the area of securing embedded system as no of ECU's are increasing rapidly. System should be more secure against internal and external attacks. In process of securing a system standard cryptographic algorithms whose cryptanalysis is done can be useful. AES-128, ECC, HMAC engines can be used to provide authenticity, Encryption/Decryption, key exchange and generation [6][10]. Software versions are slow and consume more power while their hardware implementation can accelerate sorting and permutations in cryptographic environment [3][9][13][14][21]. Side channel attacks should be carefully studied and measure should be taken to avoid power attacks which are common in cryptographic environment. Dual rail precharge circuits (DRP) can be used to nullify power attacks. It uses balanced instructions to flatten the power spectrum [16]. The use of dual rail precharge circuit adds complexity to a system, but by carefully designing the logic elements so as to avoid mismatches can make system more robust. The architecture, model suggested in this paper which uses a bit level permutation will meet all needs and requirements for securing an embedded system.

Acknowledgement

The authors would like to thank Symbiosis Institute of Technology (SIT), Dr. Narayan Pisharoty from SIT, a guide and mentor for providing all the tools, support and discussions required to carry out this project 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 networks", SAFECOMP 2008,LNCS5219, Springer,2008.

[3] 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.

[4] Hendrik Schweppe,Yves Roudier,"Security issues in vehicular system", SAR-SSI2010,5TH conference on network architectures and information system security, EVITA project, 2010.

[5] Marko Wolf, "The EVITA hardware security module", Embedded security in cars conference, Hamburg,Nov2009, EVITA project,2009.

[6] L. Apvrille, R. El Khayari, O. Henniger, Y. Roudier, H. Schweppe, H. Seudié, B. Weyl, M. Wolf, Secure automotive on-board electronics network architecture, FISITA 2010 World automotive congress, Budapest, Hungary, May/June 2010.

[7] 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.

[8] Falk Salewski, Stefan Kowalewski, “Hardware/Software design consideration for automotive embedded system” , IEEE Transactions on Industrial Informatics, Vol.4 , No.3, Aug 2008.

[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] Marko Wolf, Timo Gendrullis , “Design, implementation and evaluation of a vehicular hardware security module”, 14th International conference on information security and cryptology, Seoul, South Korea, November/December 2011 .

[11] 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.

[12] J.Pelzl, Marko wolf, T. Wollinger, Dr. Simon Burton , “Embedded security in automobiles”, Embedded World Conference ,Nuremberg,Germany,Feb-2013.

[13] 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.

[14] Zhijie Shi and Ruby B. Lee, “Subword sorting with versatile permutation instructions” , Proceedings of the 2002 IEEE International Conference on Computer Design, VLSI in Computers and Processors (ICCD’02).

[15] 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” ,USENIXSecurity,August10–12,2011.

[16] 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.

[17] Patrick Schaumont and Kris Tiri , “Masking and dual rail logic don’t add up” ,CHES, LNCS, vol. 4727, Springer, 2007, pp. 95-106, vienna, Austria,2007.

[18] Patrick Schaumont, Ingrid Verbauwhede, “Domain specific codesign for embedded security”, IEEE Computer, vol. 36, no. 4, pp. 68-74, April 2003.

[19] H. Schweppe, B. Weyl, Y. Roudier, M.S. Idrees, T. Gendrullis, M. Wolf, “Securing car2X applications with effective hardware-software co-design for vehicular on-board networks”,27th Joint VDI/VW Automotive Security Conference, Berlin, Germany, October 2011. VDI Berichte 2131,2011.

[20] David Hwang P. Schaumont, K. Tiri, and I. Verbauwhede, “Securing embedded system” , IEEE Security & Privacy, 4(2):40–49, 2006.

[21] Karthigaikumar , K Baskaran, “Hardware implementation of low power audio sub word sorter unit for high security transmission”, International Journal of Computer and Electrical Engineering, Vol. 1, No. 2, June 2009.

[22] Andre Grol, Jan Holle , Marko Wolf, Thomas wollinger , “Next generation of automotive security: secure hardware and secure open platform”, 17th ITS World Congress. 2010.

[23] Vanesa Daza, Josep Domingo-Ferrer, Francesc Sebé and Alexandre Viejo, “Trustworthy privacy preserving car generated announcement in vehicular adhoc networks”, IEEE Transaction on Vehicular Technology, Vol. 58, No. 4, May 2009.