Hardware and Software Design for Automotive Security

Gaurav Bansod

Faculty of Engineering,Symbiosis Institute Of Technology, Pune,India

Summary
Nowadays security is a major area of concern. Embedded systems are used in every automotive systems. So, attack from outside network, inside networks, bugs, hacking these are common and major concerns for an automotive security. This paper aims at providing hardware and software solution for security in automotive applications. In this paper we propose a hardware model for encryption as well as a software model that can be used for security, particularly in the Automobile domain. In Automobiles 40 to 50 microcontrollers will communicate over a CAN Bus, this communication can be encrypted, it should allow only authenticate controller to communicate inside as well as outside. In vehicle there are large no of microcontrollers called ECU's which performs specific action depending on information supplied to them by other ECU's inside vehicle or the other clusters who are outside vehicle and try to communicate. This will create a wide gateway for misusing the information and manipulations. In this paper, hardware approach is presented for security build on GRP algorithm consisting of structures of Multiplexers can be called as Hardware Security Model(HSM) and in software approach by creating a gateways and only allowing authenticate controllers to communicate .

.Key words:
ECU, Automobile, Security, Hardware, Software.

1. Introduction

Today, in vehicular networks large no of digital control units are distributed and their communication is possible over a field buses like CAN, Flex ray, MOST etc. Same information which is transmitted by one node is available with all the nodes present on the bus, proper measures should be taken to receive information correctly for the specific node. Many future applications required very high end security measures for protecting information inside automobile. This generates need for cryptographic algorithms to play an important role in security in automotive domain. Encryption like symmetric, asymmetric, encryption using digital signatures, authenticate controllers [1] these techniques will be useful to provide security from misusing or manipulating a information. In this paper above mentioned software approach is designed in Embedded C and implemented on ARM7 LPC2129 board. Similarly a software algorithm lacks rich encryption standards because of flexibility and issues like predictability. In this paper we had presented a hardware approach which is previously implemented for audio application and now can be implemented for automotive application. In this approach, a discrete structure is made by using multiplexers to do swapping with the help of control words as input to multiplexers. This control words are generated by using GRP algorithm [2] which is best suited for performing permutation and combinations. A structure is formed by using sets of multiplexers which consumes less power and can be implemented in IC form. Separate structures are created for transmitter as well as receiver. This structure provides rich encryption standards as compared to other structures [3] like EMSN, MEMS. Moreover other hardware approaches like deigning a Hardware Security Models (HSM'S) [4] is very expensive for manufacture because of inclusion of many structures like counters, algorithms though it provides top encryption standards. In this paper we are proposing a hardware model consisting of sets of 2x1 multiplexers performing permutations on GRP algorithm implemented in FPGA.

2. EVITA Model

For implementing a security application in automobiles, EVITA has proposed a hardware security model which is implemented inside automobiles. Most advanced research algorithms like AES, HASH and others are implemented to secure information. These all schemes provide rich encryption standards and it's very difficult to hack the original information. Intruder sources like an owner, service mechanic or any other person who can able to see the information and tries to corrupt it, unable to do so because of these crypto graphic algorithms. HSM's in EVITA model is implemented between sensors and microcontroller, microcontrollers and microcontroller and between microcontroller and infrastructure. These HSM's are light based, medium and heavy based HSM's depending on the crypto graphic engines inside HSM's. This method provides economically feasible approach to implement HSM's. Figure below is from EVITA model [4]

Manuscript received September 5, 2015
Manuscript revised September 20, 2015

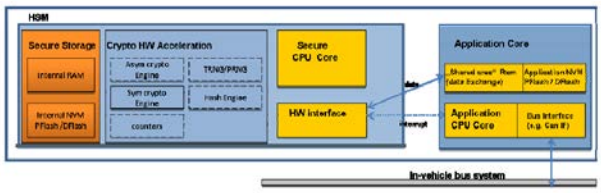

Fig1: EVITA HSM Implementation

Above figure shows implementation of HSM's in automobiles. Components used are Crypto graphic algorithms like AES, HASH engine, random no generators, counters etc. As light HSM's are implemented between sensors and microcontroller because very less information is transferred between the units. Similarly, medium based HSM's is implemented between microcontrollers, because flow of traffic is more and crucial for synchronization inside system and finally heavy based HSM's which consisting of all crypto graphic engines, counters, random number generator is implemented between microcontroller and infrastructure (Vehicle to Vehicle Communication), because most corrupt form of information, forgery messages, fake information can be expected from outside environment.

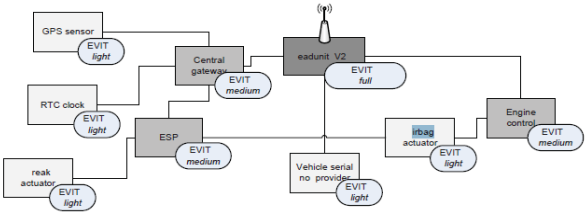

Fig 2: EVITA HSM ARCHITECTURE

3. Cryptographic hardware model

In this proposal, we are proposing a new hardware based cryptographic design which can be implemented for secure communication inside automobiles. This cryptographic hardware model(CHM) is based on GRP algorithm [3], which can be replaced with the HSM of EVITA. The algorithms like AES, HASH, are well suited for an application which runs on high volumes of data. Inside automobile, communication is limited to bytes of data. In such a scenario implementing HSM consisting of such cryptographic engines is not feasible economically. CHM provides a architecture which is perfectly used for doing encryption on information which is in bytes moreover provides rich encryption standards and have very low power consumption if implemented in IC form.

CHM architecture consisting of discrete sets of multiplexers also known as remodified enhanced merger sorter network [3] which forms a 3 stage symmetry. This architecture is a direct implementation of GRP algorithm which is based suited for doing permutations. This GRP algorithm will generate the code word for a particular arrangement and depending on code words bits will get swapped. Control word generation by GRP algorithm is explained in paper [3]

Iteration	1	2	3
P	(7,6,5,4,3,2,0,1)	(3, 7, 2, 6, 0, 1, 5, 4)	(0, 1, 3, 5, 7, 2, 4, 6)
MISes in P	(7)(6)(5)(4)(3)(2)(0,1)	(3,7)(2,6)(0,1,5)(4)	(0, 1, 3, 5, 7)(2, 4, 6)
After Alg. 1, step 1	(7,3)(6,2)(5,0,1)(4)	(3,7, 0,1,5)(2,6,4)	(0, 1, 3, 5, 7, 2, 4, 6)
After Alg. 1, step 2	Q = (3,7)(2,6)(0,1,5)(4)	Q=(0, 1, 3, 5, 7)(2, 4, 6)	(0, 1, 2, 3, 4, 5, 6, 7)
After Alg. 1, step 3	c = 10101100	c = 11010010	c = 00101010

Fig2:Code word Generation by GRP algorithm

Algorithm:

To generate GRP imstruction for a specific arrangement

INPUT: Arrangement P

OUTPUT: Arrangement Q and control bits c for GRP

INSTRUCTION

Let Pi represent the i(th) MIS in P. (x, y) denotes the operations that combine integer sequence x and y into a longer sequence. Sort(x) is a function that sorts elements in sequence x in increasing order. P can be represented by k MISes (Monotonically Increasing Sequences) as follows:

P = (P1, P2, P3,…, Pm, Pm+1 , Pm+2…,Pk-1, Pk)

Note that m = k/2 , and P1, P2, P3, …, Pm is the first half MISes.

1. Generate temporary sequences T1, T2,…,Tm: For i = 1, 2,… ,m-1
   Ti = (Pi , Pi+m)
   If (k is odd) then
   Tm = Pm else
   Tm=(Pm , Pk)
2. Generate Q:
   For i = 1, 2,… , m
   Qi= Sort(Ti)
   Let Q = (Q1, Q2,Q3,…,Qm).
3. Generate control bits c:
   Q can also be considered as a bit string:
   Q = (Q1, Q2, Q3,…,Qm) = (b0, b1, b2, …,bn-1)
   For j = 0, 1,… , n-1
   if (bj is in P1, P2, P3,… , or Pm)
   cj = 0 else
   cj = 1

Above codeword's are generated for specific arrangement In this paper we have considered from A0 to A7.Change in a arrangement of bits will generate a different control word. These codeword's are used for swapping information for a specific arrangement. A change in a bits position will

generate different control words and so the information. This architecture consumes less power as compared to other existing algorithm which is implemented for audio applications. The arrangements and swapping method for CHM based on GRP algorithm is shown below

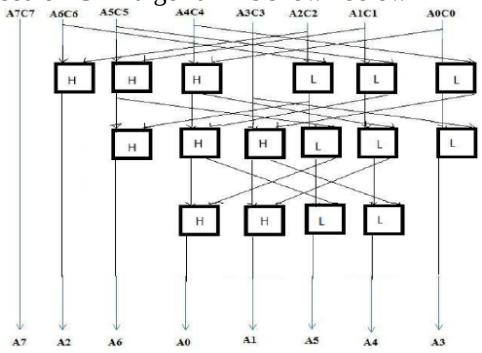

Fig 3: CHM Transmitter Architecture

Fig 3 shows CHM for transmitter section. Here bits are arranged in a monotonically increasing sequence from A0 to A7 and each bit is associated control word generated from GRP algorithm indicated by C0 to C7 respectively. Bits are swapped according to GRP algorithm based on code word. Logic to do the permutation is explained with the fig.4

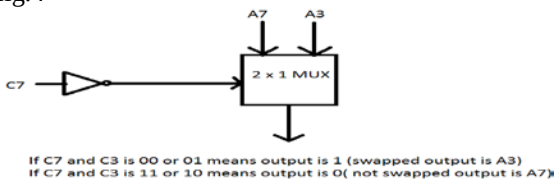

Fig 4: Control Logic

Arrangement of bits and their respective gropups are formed according to GRP algorithm[3]. A7 to A0 are grouped as (A7,A3) , (A6,A2) , (A5,A1) and (A4,A0). According to arrangement shown above in fig3 bits are swapped based on control words. Fig 6 shows its implementation

BITS	A7	A6	A5	A4	A3	A2	A1	A0
C	1	0	1	0	1	0	1	0

Fig 5:Code words with Respective bits

This control words are formed for a particular arrangement by GRP algorithm and birs are swapped in respective group and based on logic explained in fig.4

- 1st STAGE

BITS	A7	A6	A5	A4	A3	A2	A1	A0
C	1	0	1	0	1	0	1	0

(A6,A2) AND (A4,A0)

EQUIVALENT SWAPPED BITS
A7 A2 A5 A0 A3 A6 A1 A4

- 2nd STAGE

BITS	A7	A2	A5	A0	A3	A6	A1	A4
C	0	1	0	1	0	1	0	1

(A5, A2) AND (A3,A0)

EQUIVALENT SWAPPED BITS
A7 A2 A6 A0 A4 A5 A1 A3

- 3rd STAGE

BITS	A7	A2	A6	A0	A4	A5	A1	A3
C	0	1	0	1	0	1	0	1

(A1,A3)

Fig 6:Swapping of bits at Trasmitter End

So, as shown above final swapped bits will be

A7 A2 A6 A0 A1 A5 A4 A3

These encrypted bits is communicated over a CAN Bus for a particular node. As seen from table control words at each stage is different generated by GRP algorithm that increases standard of encryption. Moreover as it is using sets of 2 x 1 multiplexers ,power consumption is also less.It requires very less infrastructure which made this structure economically feasible as compared to EVITA model.

4. Cryptographic Receiver Structure

Similarly with GRP algorithm receiver structure is developed based on control words and sets of multiplexers. Main concept of GRP algorithm is to sort based on concentrating 1's on left hand side as explained in fig 7

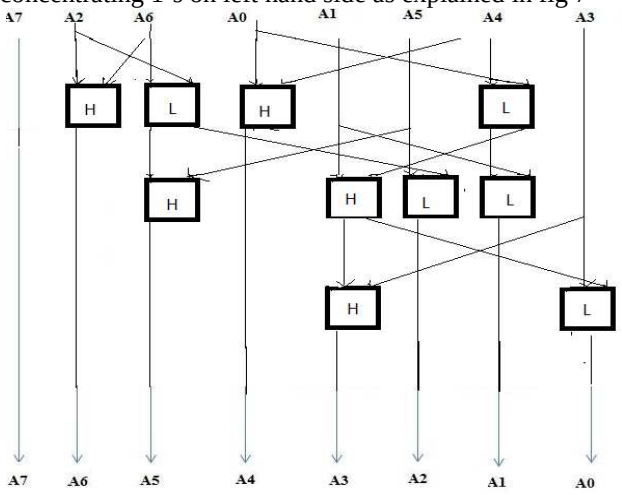

Fig 7: CHM Receiver Structure

CHM receiver structure uses less no of multiplexers, so power consumption would be more less and it can be implemented at any receiver node. Bits swapping and arrangement is shown below

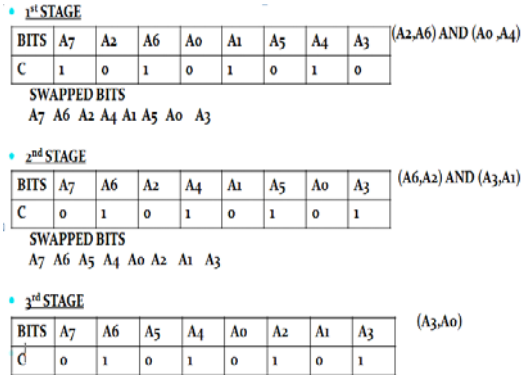

Fig 8:Swapping of Bits at Receiver end

Swapped bits are
A7 A6 A5 A4 A3 A2 A1 A0

From above arrangement at receiver end, we can able to retrieve the original information which is transmitted. This reciver structure can be implemented for every receiving node inside automobiles.

5. CHM for Security

As compared to EVITA HSM structure, CHM structure would be economically viable and as par with the encryption standards. CHM model based on GRP algorithm is implemented on FPGA and as it is a hardwired implementation, it could be difficult for intruder or for extruder to tamper the information. As hardware structures are always having edge over software structure in terms of speed, security but lags on cost. This CHM provides a midway solution for providing security in automobiles by making security solution economically viable without losing much on encryption standards.CHM model is implemented for 8 bits of data can be extended for 16bit and for any arrangement. This would add more encryption inside system such that few blocks consisting of GRP of particular arrangement and few of other, which make system more resistive and unpredictable. As GRP algorithm is highly studied and best for doing permutations, its implementation on FPGA gives an edge over other existing algorithms. This GRP algorithm is written in Verilog and implemented on Xilinx FPGA board. Power is calculated by using XPower tool of Xilinx and same can be implemented in RTL complier of Cadence tool.CHM power calculation with Xpower tool is shown in fig 6 that is implemented for transmitter section which is coming around 77mW. So receiver section would be also 77mW approximately.

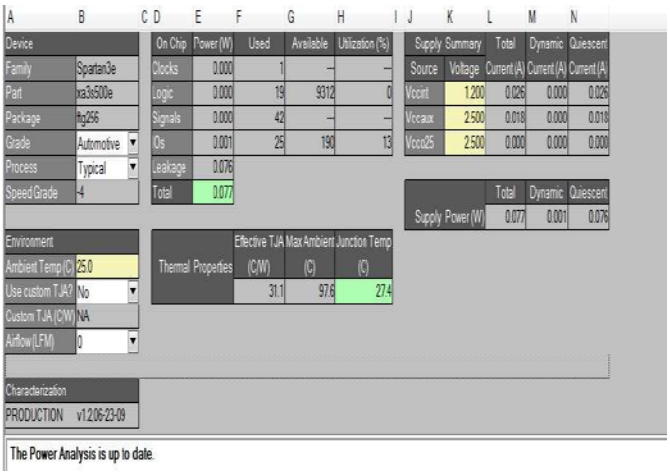

Fig 9:Power calculation by XPower Tool

Above fig shows power consumption by this algorithm is very less as compared to other existing algorithm. Detailed comparative study is discussed in paper [3]For above structure power consumption turn out is 154mW which is very less. This paper proposes a first type of cryptographic algorithm which can be implemented for automotive security application.

This CHM can be implemented between sensors and controller between controllers and between controllers and infrastructure thus replacing HSM's of EVITA model. As discussed in paper [3], this GRP structure provides fastest solution with lesser delays.

6. Secure approach by creating Gateways

To ensure security, models can be created by using gateways to authenticate controllers, messages inside automobiles as mentioned in paper [1].To authenticate controller for participation in communication over CAN bus, we should authenticate it to avoid any tampering of information or misuse. Various measures have been taken by using digital signatures, symmetric and asymmetric encryption to secure information [1]. In this paper we have implemented gateways for authenticating controllers. Keys for respective controllers are stored in a gateway and before initiating any communication over a bus first controller has to passes through gateways to authenticate itself. This will prevent an entry of any unauthorized controller to an automobile environment. Above method for authenticating a controller is written in Embedded C and implemented on ARM7 LPC2129 board. The gateways would be having all original keys from OEM's. This can be further encrypted using symmetric and asymmetric encryption by using concept of public key and private key. Figure below shows snapshot of environment where gateways are created by using Embedded C.

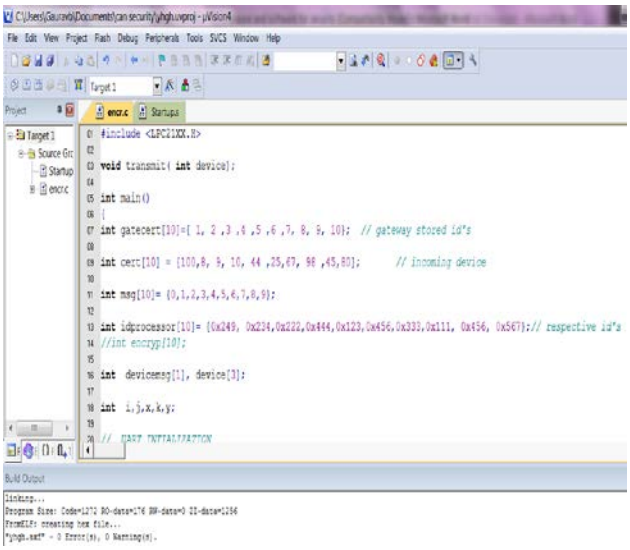

Fig 10:Creating Gateway in Keil Uvision4

Algorithm:

1. Create a Gateway which can store all ID'd from OEM's
2. Once any controller wants to communicate pass it through Gateways.
3. Using comparison algorithm , authenticate a controller
4. Respective contoller can send a message to respective node
5. This authenticate controller information can be send to other terminals by using UART.
6. Can include symmetric and assymetric encryption for guarding information

Above algorithm is implemented and dumped on ARM7 LPC2129 board. Further in this algorithm encryption standards can be increased by using symmetric and assymetric cryptographic algorithms

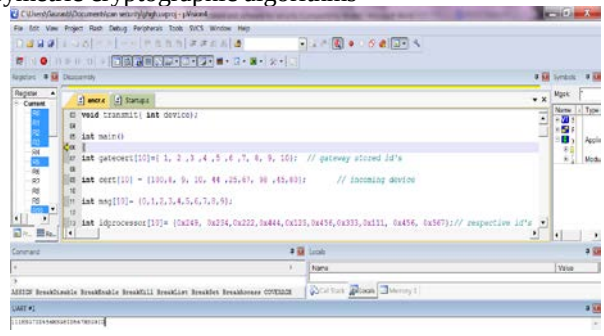

Fig 11: Simulated in Uvision 4

Above alogrithm is simulated by using Keil Uvision 4 and results are attached below showing only participation of authenticate controller and their respective messages through UART.

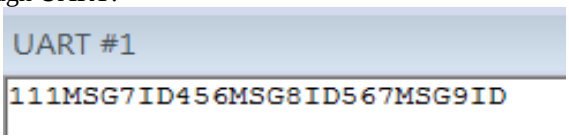

Fig 12:UART o/p only allowing authnteticate controllers

Above figure shows participation in communication of only authenticate controller and their respective messages .So in this scenario gateway has rejected other 7 controllers as their key from OEM does not match . Only 3 controllers with id's 111, 456 and 567 will participate in communication and their messages 7,8, and 9 respctively are communicated to destination node.

7. Results and Discussions

Cryptographic Hardware Model (CHM) provides the unique way of securing communication in automobiles. As compared to EVITA HSM, CHM is economically feasible to implement in a system. Moreover GRP algorithm which is a core part of CHM gives very low power consumption as compared to other existing algorithm. This CHM structure can be implemented in ASIC form and at 'n' no of nodes inside automobile. We can further extend this by putting symmetric and asymmetric encryption to achieve rich encryption standards. Moreover similar gateways can be created and implemented to avoid fake messages from external environment. This model is implemented and simulated on FPGA while method by creating Gateways is written in embedded C by using KEIL and implemented on ARM7 LPC2129 board. These methods can be simulated on vehicle infrastructure.

8. Future Work

This paper can be implemented for announcement security also. In announcement security model, a person in a car will send a message to other cars in network regarding status on traffic, valuable information regarding accidents etc. this message needs to be authenticated because person may give fake message. A system can be implemented which can only accept messages if particular message is endorsed by 'n' no of vehicles. As mentioned in [8], we can fix a particular threshold , if a particular message crosses particular threshold then can be considered as a authenticate message and allows to communicate with system. This structure with all modifications which includes implementing symmetric and asymmetric encryption, creating gateways can be simulated and implemented in vehicle system security. This whole

structure can be implemented with cadence tool generating structural layout and can be fabricated as “ASIC”.

Acknowledgement

The author would like to thank Symbiosis Institute of Technology for providing all the tools and support required to carry out this project successfully.

References

[1] Marko Wolf, Andre Weimerskirch, and Christof Paar Clerk Maxwell,”Secure in Vehicle Communication, Embedded Security In Cars, Securing current and future Automotive applications, Springer Journal

[2] Gaurav Bansod,”Audio Subword Sorter unit On Merger Sorter Network For Secure Communication”,IEEE international conference on cotrol system computing and Engineering(ICCSCE 2111), Penang, Malaysia

[3] Karthigaikumar P, Baskaran K, “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 1793-8163.

[4] Marko wolf, “The EVITA hardware security Model”, Seventh research programme of european comitee, July 2008,P.NO.34

[5] EVITA: E-safety vehicle intrusion protected applications. www.evita-project.org, 2008.

[6] M.Wolf: "Security Engineering for Vehicular IT Systems — Improving Trustworthiness and Dependability of Automotive IT Applications", Vieweg+Teubner-Verlag, 2009.

[7] Designing Security Automotive Hardware- the EVITA project- Marko Wolf escrypt GMBH , Embedded Security, CAST Workshop Mobile Security for Intelligent Cars Darmstadt, Germany, August 27th, 2009

[8] Vanesa Daza, Josep Domingo-Ferrer, Senior Member, IEEE, Francesc Sebé, and Alexandre Viejo,”Trustworthy privacy preserving car generated announcements in Vehicular adhoc networks”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 4, MAY 2009

[9] R.R. Brooks, S. Sander, Juan Deng, and Joachim Taiber, ”Automobile security concern” IEEE Vehicular technological Magazine, June 2009.

[10] Apvrille, Ludovic, El Khayari, Rachid, Henniger, Olaf, Roudier, Yves, Schweppe, Hendrik, Seudié, Hervé, Weyl, Benjamin, Wolf, Marko, ”Secure Automotive on board Electronics network architecture”,EVITA- Esafety vehicle intrusion protected applications.

Gaurav Vijay Bansod received his Btech from Nagpur university, India and Mtech degree in embedded Systems from Jawaharlal Nehru Technological University, Hyderabad, India in 2006 and 2008 respectively. He is working in Symbiosis Institute of Technology, Pune as an Assistant Professor in Electronics & Telecommunication Department. His research area includes Embedded systems, Securiy in Automobiles, Cryptography and VLSI design. He is member of IETE.