IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 5, Issue 5 (Mar. - Apr. 2013), PP 51-55
www.iosrjournals.org

Implementation of XOR Based Pad Generation Mutual Authentication Protocol for RF Link

Ramya K[1], Asst.Prof Priyadarshini G[2]
[1 (]*Department of ECE, Mount Zion College of Engineering & Technology, Tamil Nadu, India)*
[2(]*Department of ECE, Mount Zion College of Engineering & Technology, Tamil Nadu, India)*

Abstract: *In RF link, without security the messages exchange between the two devices are monitoring by an eavesdropper. So the exclusive-OR (XOR) based pad generation protocol is used to safely transfer the data to the other point with necessary security and it maintaining confidentiality. This protocol produce the cover coding pad to mask the access password before the datas are transmitted. A specially designed pad generation will be implemented in digital domain to solve the insecurity problem in data communication RF link. This protocol developed under regulation of ISO 18000 – 6 type C protocol also known as EPC C1G2 RFID protocol. The linear feed back shift register (LFSR) generate the pseudo random binary sequence (PRBS) and it is used as data source to the pad generation function. The Xilinx 13.x software is used for synthesize and modelsim SE6.0 is used for simulating the result. The pad generation algorithm has been implemented in FPGA Spartan 3 PQ208-4 board to verify the result.*

Keywords- *Field-programmable gate array (FPGA) implementation, mutual authentication, RF link, security, Zigbee.*

I. Introduction

Radio Frequency Identification (RFID) technology uses a wireless system that can provide efficient real-time device track-and-trace capability. The ultra high frequency (UHF) RF for data communication using devices operating in industrial-scientific-medical (ISM) band. The EPC global Inc. is the leader in developing industry-driven specifications for the electronic product code (EPC) to support the use of RFID in supply chain management [1].The international standard organization (ISO) has incorporated the EPC class-1 generation-2 (C1G2) UHF standard into its ISO/IEC 18000-6 amendment type C. The ISO 18000-6C protocol also known as EPC C1G2 protocol, provides only basic security tools using a16-b pseudo random number generator and 16-b cyclic redundancy code. However, the EPC C1G2 specification do not fully support privacy invasion and data security issues [2].

A passive eavesdroppers monitoring the message exchange between the sender and the receiver by simply computing an exclusive-OR (XOR) operation [3]. To exposed this weakness a proposed sender and receiver (tag- reader) mutual authentication scheme protect the access password [4]. But after simple computations an attacker could acquire the access password (Apwd) and kill password (Kpwd) with high probability [4]. Many light weight authentication protocols that use only efficient bitwise operations like XOR, AND, OR etc, have been proposed [5]. However, most of the proposed protocols have not been verified with hardware [2]. The Field programmable gate array (FPGA)-based systems gain particular flexibility for verifying hardware implementations. Due to the advantages of FPGA prototyping based verification, a large number of systems have been implemented in FPGAs in different fields, such as radio communication protocol [6], robotics [7], [8], power system [9] and signal processing [10].

PRBS is generated using the linear feed back shift register and it is the data source to the pad generation function. Pad generation function produce the cover coding pad to mask the access password. The design of X-OR based pad generation protocols achieving the mutual authentication between the sender and the receiver. This protocol providing an adequate security for data communication RF link. An efficient hardware implementation of X-OR based pad generation mutual authentication protocol is described in this paper.

This paper is organized in the following way. In section II LFSR functions and In section III pad generation operations are designed and provided. In section IV the implementation design of the pad generation protocol in FPGA is provided and discussed. In section V simulation and schematic results are presented and discussed. Finally, this paper is concluded in section VI.

II. Linear Feed Back Shift Register Function

The pad generation (PadGen) function is the key function used to produce cover-coding pad to mask the access password before transmission. The implementation of the PadGen function also requires the random number generator to produce R_{Tx} and R_{Mx}. A typical linear feedback shift register (LFSR) is used to generate pseudo random numbers (2^N-1). A Linear Feedback Shift Register (LFSR) is a shift register whose input bit is

a linear function of its previous state. Mostly used linear function of single bits is XOR, thus normally it is a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle.

An LFSR with an ell-chosen feedback function can produce a sequence of that appears random and has a very long cycle. For an n-bit LFSR, the LFSR can generate a $(2^N - 1)$-bit long pseudo random sequence before repeating. A maximum-length LFSR produces an m-sequence (i.e., cycles through all possible $2^N - 1$ states within the shift register except the state where all bits are zero). In this paper, the parallel load count PRBS was implemented because it is more suitable for hardware implementation.

III. Xor Based Pad Generation Operation

An access password is required before data are exchanged between a sender and a receiver. The access password is a 32-b value. Konidala uses a specially designed pad generation function to produce the cover coding pad to mask the access password before the data are transmitted [4].The main problem with the scheme is infact if that inputs in the pad generation are known to an eavesdropper and this information can be used to obtain correlations to recover the access password under a correlation attack[3].To mitigate this drawback, the inputs to the pad generation function must be hidden from the eavesdropper. So, this is done by X-OR pad generation mutual authentication protocol .The detailed steps of the XOR schemes to generate the Pad generation function are presented as follows.

Lets us represent the 32-b Apwd and Kpwd as

$Apwd = a_0a_1a_2 \ldots\ldots\ldots..a_{30}a_{31}$ (base 2) (1)

$Kpwd = k_0k_1k_2 \ldots\ldots\ldots..k_{30}k_{31}$ (base 2) (2)

The 16-b random numbers are represent as input in below

$R_{Tx} = h_{t1}h_{t2}h_{t3}h_{t4}$ (base 16)

$= d_{t1}d_{t2}d_{t3}d_{t4}$ (base 10) (3)

$R_{Mx} = h_{m1}h_{m2}h_{m3}h_{m4}$ (base 16)

$= d_{m1}d_{m2}d_{m3}d_{m4}$ (base 10) (4)

Apwd-PadGen (R_{Tx}, R_{Mx})

$= ad_{t1}adt_2ad_{t3}ad_{t4}||ad_{t1}+16ad_{t2}+16ad_{t3}+16ad_{t4}+1||ad_{m1}ad_{m2}ad_{m3}ad_{m4}||ad_{m1}+16ad_{m2}+16ad_{m3}+16ad_{m4}+16$

$= d_{V1}d_{V2}d_{V3}d_{V4}$ (base 10)

$= R_V$ (5)

$R_T \oplus R_M = R_T \oplus_M$

$= d_{x1}d_{x2}d_{x3}d_{x4}$ (6)

Apwd-PadGen (R_T, $R_T \oplus_M$)

$= ad_{t1}ad_{t2}ad_{t3}ad_4||ad_{t1}+16ad_{t2}+16ad_{t3}+16ad_{t4}+16\times||ad_{x1}ad_{x2}ad_{x3}ad_{x4}||ad_{x1}+16ad_{x2}+16ad_{x3}+16ad_{x4}+16$

$= d_{W1}d_{W2}d_{W3}d_{W4}$ (base 10)

$= R_W$ (7)

Kpwd-PadGen(R_V,R_W)

$=kd_{V1}kd_{V2}kd_{V3}kd_{V4}||kd_{V1}+16kd_{V2}+16kd_{V3}+16kd_{V4}+16\times||kd_{W1}+kd_{W2}+kd_{W3}+kd_{W4}\times||kd_{W1}+16kd_{W2}+16kd_{W3}+16kd_{W4}+16$

$= h_{q1}h_{q2}h_{q3}h_{q4}$ (base 16)

$= PAD_1$ (8)

$R_V \oplus R_W$

$= R_V \oplus_W$

$= d_{s1}d_{s2}d_{s3}d_{s4}$ (9)

Kpwd-PadGen (R_V, $R_V \oplus_W$)

$=kd_{V1}kd_{V2}kd_{V3}kd_{V4}||kdV1+16kd_{V2}+16kd_{V3}+16kd_{V4}+16\times||kds1kds2kds3kds4\times||kds1+16kds2+16kds3+16\ kds4+16$

$= h_{r1}h_{r2}h_{r3}h_{r4}$ (base 16)

$= PAD_2$ (10)

By performing XOR operation the following cover-code Apwd is obtained

$CCPwd_{M1} = Apwd_M \oplus PAD_1$ (11)

$C\ CPwd_{L1} = Apwd_L \oplus PAD_2$ (12)

For the Pad generation proposed by Konidala et al. [4] , each PAD function is computed based on one set of (R_{Tx}, R_{Mx}), which is transmitted in the open space. In contrast to the PadGen proposed by Konidala et al.,

the present proposed pad function is computed based on one set of (R_V, R_W), which is not transmitted openly. RV and RW are computed based on Apwd–PadGen (R_{Tx}, R_{Mx}) and Apwd-PadGen (R_{Tx}, $R_{Tx} \oplus R_{Mx}$), respectively. PAD_1 and PAD_2 are then generated by Kpwd-PadGen (Rv, Rw) and Kpwd-PadGen (R_V, $R_V \oplus R_W$), respectively.

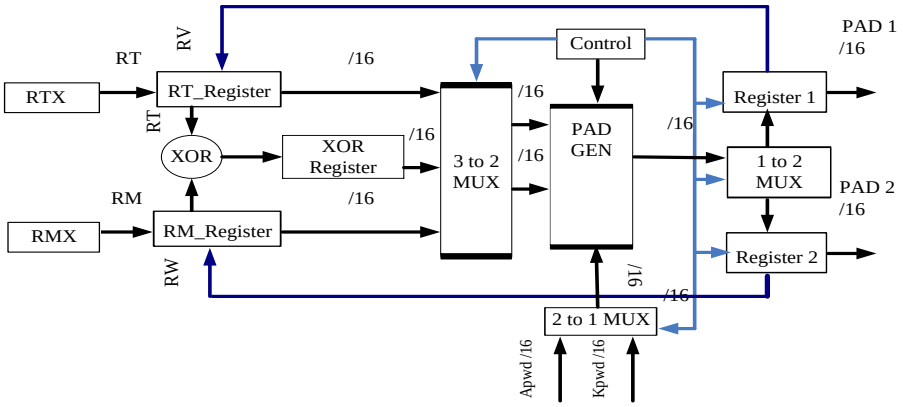

Figure 1 Functional block diagram of the XOR pad generation operation

IV. Design And Hardware Implementation

The proposed system block diagram of Transmitter and receiver is respectively shown in "Fig. 2" and "Fig. 3".The proposed system working principles and detailed description is given below. The datas are transmitted with secure manner by Xor pad generation (PadGen) protocol. Here, pad generation protocol produce cover coding pad to mask the access password and FPGAs are chosen for implementation. Zigbee is the RF transreceiver to transmit and receive the data.

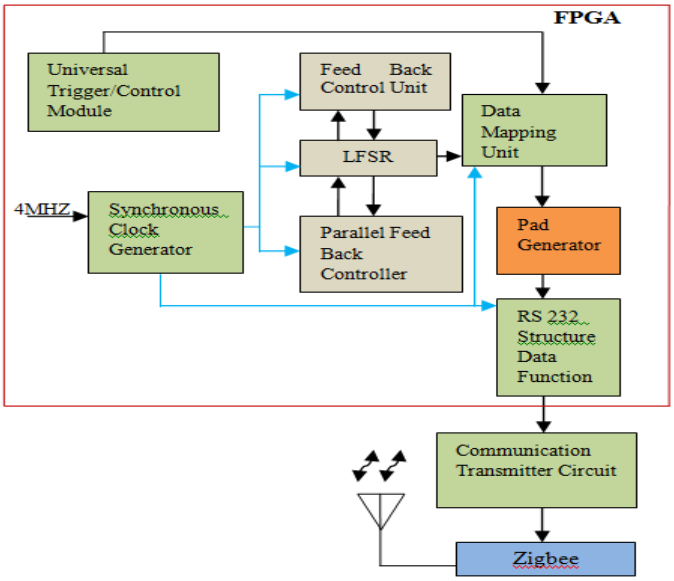

Figure 2 Block diagram of transmitter

The FPGAs running with 4MHZ clock. First we generate the parallel load PRBS by using LFSR and then result is given to the data mapping unit to converts the serial output came from the LFSR to parallel form, then it is given as the input to the pad generator. Universal trigger/control unit control each module in the implementation. Then generated PAD is convert into serial which is suitable for RF transmission and it is transmitted through RS 232 to the communication transmitter circuit, Here this communication transmitter circuit has Zeener diode as a regulator. The outcoming pads is transmitted through the zigbee in the RF link. The transmitted data through the RF link is received by the Zigbee in the receiver side and then it is given to communication receiver circuit which has LM317 regulator. The received data is transfer to the pad degenerator through the Data demapper unit. Finally, In the receiver side the obtained cover coding pad is degenerated by

pad degenerator. It is verified and displayed through LCD display, then error is calculated by Bit error calculator therefore if it has an error it will be displayed through the 7- segment display.

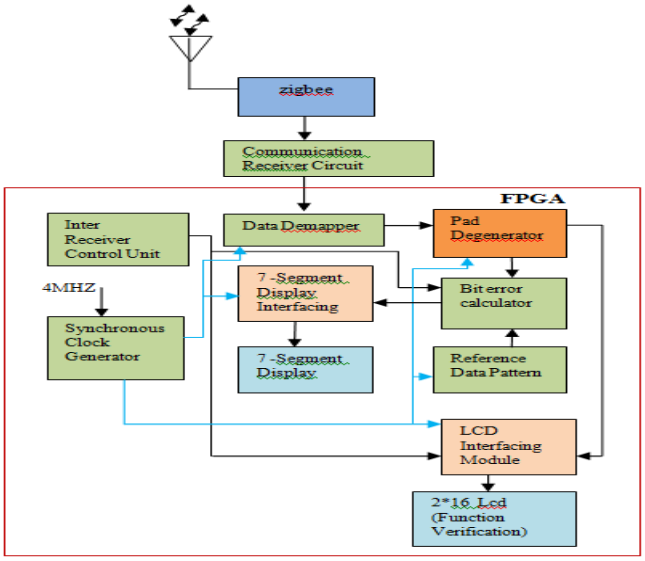

Figure 3 Block diagram of receiver

V. Results And Discussions

The Verilog schematic and simulation results of FPGA implementation are shown in "Fig. 4.a & Fig 4.b" and "Fig. 5" respectively. Initially the 4-MHZ synchronous clock is applied to the FPGA board. The master clock and start_in are given as the input to the LFSR. Initially start_in is in'0' then output is zero, If start_in is '1' then PRBS starts to generate. The generated PRBS output is nothing but the random number (R_{TX} and R_{MX}).The random number is given as the input to the XOR based pad generation function.

The functional block diagram of the XOR-PadGen function for mutual authentication is described in the previous section as shown in "Fig. 1". This approach can obtain PAD_1 and PAD_2 using one set of (R_{Tx}, R_{Mx}). This approach is a more efficient way to generate PAD function for mutual authentication. After the initial input of random numbers R_{Tx} and R_{Mx}, a multiplexer was utilized to control the selection of Apwd or Kpwd for PadGen operation. PAD_1 and PAD_2 are then simultaneously generated to cover-coded Apwd for mutual authentication. As shown in "Fig. 1", the details of the functions performed are described as follows.

- Apwd-PadGen $(R_{Tx},R_{Mx})=d_{v1}d_{v2}d_{v3}d_{v4}=R_V$. R_{Tx}, R_{Mx}, and Apwd are selected as the inputs for PadGen operation and the calculation results RV by XOR-PadGen operation are stored in register for further manipulation.
- Apwd-PadGen $(R_T,R_T \oplus R_M)=d_{w1}d_{w2}d_{w3}d_{w4}= R_W$. Through mux selection, R_T, $(R_T \oplus R_M)$, and Apwd are chosen as inputs for PadGen operation. The calculation result RW is stored in register for further computation.
- Kpwd-PadGen $(R_V,R_W)= h_{q1}h_{q2}h_{q3}h_{q4} = PAD_1$. The PAD_1 as shown in can then be obtained by mux selecting RV, RW, and Kpwd as inputs for XOR-PadGen operation.
- Kpwd-PadGen$(R_V,R_V \oplus R_W)=h_{r1}h_{r2}h_{r3}h_{r4}=PAD_2$. Similarly, the PAD_2 can then be obtained using $R_V,R_V \oplus R_W$, along with Kpwd for XOR-PadGen operation.

Simulations of the design were conducted in the modelsim SE 6.0. The verified Verilog code will be then downloaded on an Virtex Spartan 3 PQ208-4 board. FPGA running with a 4-MHz clock to verify the hardware. The simulated result of XOR pad generation protocol is shown below in "Fig.5".

Figure 4.a

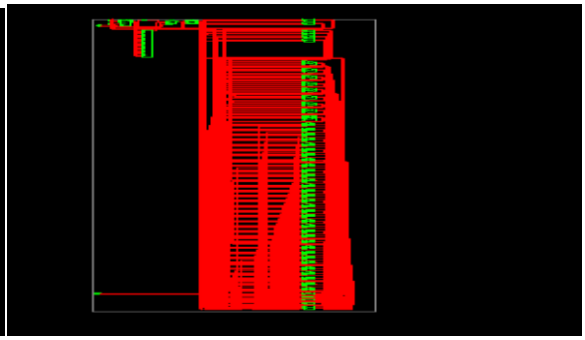

Figure 4.b

Figure 4.a & 4.b RTL Schematic diagrams of xor pad generation

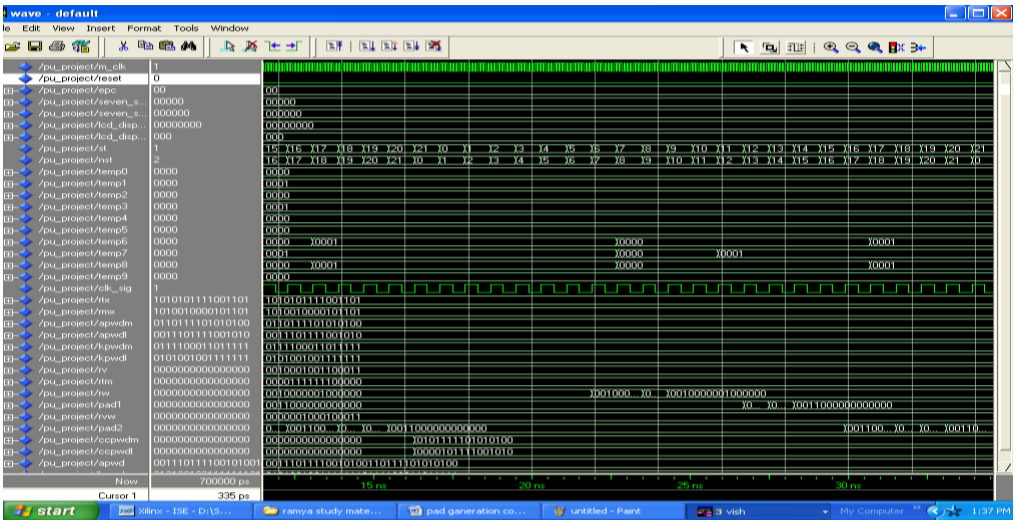

Figure 6 Verilog simulation result of xor pad generation

VI. Conclusion

This research work is to improve the security level of the data communication RF link by authentication protocol proposed under the EPC C1G2 specification, the pad generation functions are used to protect the Apwd with cover coding against exposure. In this paper, the Pad generation function strengthen the security of the mutual authentication scheme. The Pad generation functions based on XOR operation and in association with the Apwd and Kpwd are used to generate the PAD_1 and PAD_2. Each cover-coding pad then used to perform the subsequent authentication responses. In conclusion, the main feature of this approach is to design pad generation mutual authentication protocol for secure data communication RF link.

References

[1]. Class 1 Generation 2 UHF Air interface Protocol Standard. [Online]. Available: http://www.epcglobalinc.org/sta

[2]. H. M. Sun and W. C. Ting, A Gen2-based RFID authentication protocol for security and privacy, IEEE Trans. Mobile Comput., vo8,no.8,Aug.2009,1052–1062.

[3]. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, Practical attacks on a mutual authentication scheme under the EPC Class-1 Generation-2 standard, Comput Commun., vol.32, no.7–10, May 2009, 1185–1193.

[4]. D. M. Konidala, Z. Kim, and K. Kim, A simple and cost effective RFID tag–reader mutual authentication scheme, in Proc. Int. Conf. RFID Sec, Jul.2007, 141–152.

[5]. Y.J. Huang, C.C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, Hardware implementation of RFID mutual authentication protocol, IEEE Trans. Ind. Electron., vol. 57, no. 5, May 2010, 1573–1582.

[6]. H.-Y. Chien, SASI: A new ultra lightweight RFID authentication protocol providing strong authentication and strong integrity, IEEE Trans. Dependable Secure Comput., vol. 4, no. 4, pp. 337–340, Oct.–Dec. 2007.

[7]. H. Tanaka, K. Ohnishi, H. Nishi, T. Kawai, Y. Morikawa, S. Ozawa, and T. Furukawa, Implementation of bilateral control system based on acceleration control using FPGA for multi-DOF haptic endoscopic surgery robot, IEEE Trans. Ind. Electron., vol. 56, no. 3, Mar. 2009, 618–627.

[8]. J. U. Cho, Q. N. Le, and J. W. Jeon, An FPGA-based multiple-axis motion control chip, IEEE Trans. Ind. Electron., vol. 56, no. 3, Mar. 2009, 856–870.

[9]. M.-H. Lee, K.-K. Shyu, P.-L. Lee, C.-M. Huang, and Y.-J. Chiu, Hardware implementation of EMD using DSP and FPGA for online signal processing, IEEE Trans. Ind. Electron., vol. 58, no. 6, Jun. 2011, 2473–2481.

[10]. P. Cole and D. Ranasinghe, Eds., Networked RFID Systems Lightweight Cryptography — Raising Barriers to Product Counterfeiting (1st e Berlin, Germany: Springer-Verlag, 2008).

[11]. S. Piramuthu, Lightweight cryptographic authentication in passive RFID-tagged systems, IEEE Trans. Syst., Man, Cybern. C, Appl. Rev. ,vol. 38, no. 3, May 2008, 360–376.