ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

ARM and FPGA Implementation of Secured Authentication Protocol for RFID System

S.Mohanavelu[1], T.Ramya[2]

PG Student [VLSI], Department of ECE, SRM University, Kattankulathur, Tamilnadu,India[1]
Assistant Professor, Department of ECE, SRM University, Kattankulathur, Tamilnadu,India[2]

Abstract: The authentication process of RFID tag's the tag/reader/server communicates ***over*** an insecure channel due to weak authentication protocols. The Electronic Product Code (EPC) Class-1 Generation-2 (C1G2) specification have some serious security problems, so the password either leak directly over the network or leaks the sufficient information i.e., while performing authentication, that allow hackers to deduce or guess the password. To overcome this weak authentication a specially designed pad generation (Pad Gen) function is used to improve security. The Pad Gen function is used to produce a cover-coding pad to mask the tag's access password before the data transmission. Hence a mutual authentication protocol with XOR scheme and MOD Scheme is proposed to avoid the data leakage and data traceability during the data transmission .This system model is simulated and synthesized using Xilinx ISE software. The performance of this authentication scheme will be verified in hardware using ARM 7 and Spartan 3E FPGA.

Keywords: RFID-Radio frequency Identification, EPC-Electronic Product Code,C1G2-Class 1 Generation 2,ARM-Advance RISC Machine

I.INTRODUCTION

RADIO-FREQUENCY identification (RFID) is a contact-less identification technology that enables remote and automated Gathering and sending of information between RFID tag's or transponders and readers or interrogators using a wireless link. In recent years, RFID technology has gained a rapid acceptance as a means to identify and track a wide array of manufactured objects. It is composed of three main components: tag, reader and Server.

RFID tag's come in a range of forms and can vary in storage capacity, memory type, radio frequency and power capability. Most of these tag's contain only a unique Electronic Product Code(EPC) number and further information about the product is stored on a network of databases, called the EPC-Information Services(EPC-IS).Through the wireless interface, each tag can report data when queried over radio by an RFID reader.

RFID readers can only recognize tag's in proximity; a data tag that is out of range cannot be read by a reader. Secured Authentication protocol is described in this paper. The rest of this paper is organized as follows. In Section 1, we present the Background and previous work in the RFID reader-to-tag authentication protocol in section 2. The enhanced pad generation (PadGen) function is discussed in Section 3. Section 4 shows implementation results of the proposed mutual authentication scheme. Finally, we conclude this paper in Section 5.

II.EPC GLOBAL CLASS-1 GENERATION-2 STANDARD

The EPC global Class-1 Generation-2 (C1G2) ultra-high frequency (UHF) RFID standard defines a specification for passive RFID technology and is an open and global standard. The EPC C1G2 standard specifies the RFID communication protocol within the UHF spectrum (860 to 960MHZ).The standard specifies that a complaint RFID tag should contain a 32-bit kill password (Kpwd) to permanently disable the tag and a 32-bit access password (Apwd). The reader then performs a bitwise XOR of the data or password with a random number from the tag to cover coded data or a password in EPC Gen 2.

III.COMPONENTS OF AN RFID SYSTEM

The RFID system consists of various components which are integrated. This allows the RFID system to deduct the objects (tag) and perform various operations on it. The integration of RFID components enables the implementation of an RFID solution. The RFID system consists of following three components

- Tag (attached with an object, unique identification).
- Reader (receiver of tag information, manipulator).
- Server (overall information about the tag and the manufacturer).

A) Tag's

Tag's contain microchips that store the unique identification (ID) of each object. The ID is a serial number stored in the RFID memory. The chip is made up of integrated circuit and embedded in a silicon chip. RFID memory chip can be permanent or changeable depending on the read/write characteristics. Read only and rewrite circuits are different as read-only tags contain Fixed data and cannot be changed without re-program electronically. On the other hand, re-write tags can be programmed through the reader at any time without any limit. There are three types of tag's the passive, semi-active and active. Semi-active tags have a combination of active and passive tag's characteristics. So, mainly two types of tag's (active and passive) are being used by industry and most of the RFID system.

B) Reader

RFID reader works as a central place for the RFID system. It reads tag's data through the RFID antennas at a certain frequency. Basically, the reader is an electronic apparatus which produce and accept a radio signals. The antennas contains an attached reader, the reader translates the tag's radio signals through antenna, depending on the tag's capacity. The readers are expected to collect or write data on to tag (in case) and to pass computer systems.

C) RFID System

The RFID tag's 32-bit Access password and 32-bit kill passwords achieve tag–reader mutual authentication. Their scheme uses two rounds of PadGen to compute a cover-coding pad. The first round performs PadGen over the access password, while the second round performs PadGen over the kill password. The PadGen function is used to create the 16-bit pads for "cover coding" the access password.

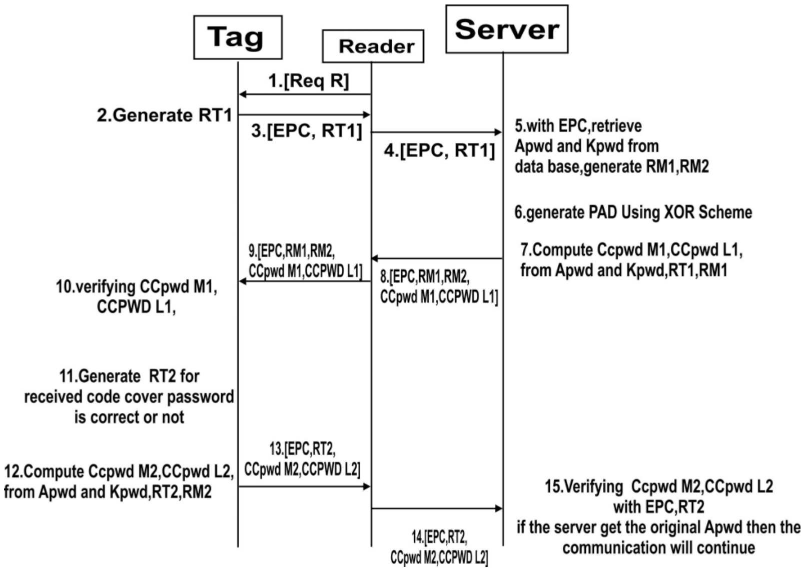

Tag
Reader
Server
1.[Req R]
2.Generate RT1
3.[EPC, RT1]
4.[EPC, RT1]
5.with EPC,retrieve Apwd and Kpwd from data base,generate RM1,RM2
6.generate PAD Using XOR Scheme
7.Compute Ccpwd M1,CCpwd L1, from Apwd and Kpwd,RT1,RM1
8.[EPC,RM1,RM2, CCpwd M1,CCPWD L1]
9.[EPC,RM1,RM2, CCpwd M1,CCPWD L1]
10.verifying CCpwd M1, CCPWD L1,
11.Generate RT2 for received code cover password is correct or not
12.Compute Ccpwd M2,CCpwd L2, from Apwd and Kpwd,RT2,RM2
13.[EPC,RT2, CCpwd M2,CCPWD L2]
14.[EPC,RT2, CCpwd M2,CCPWD L2]
15.Verifying Ccpwd M2,CCpwd L2 with EPC,RT2 if the server get the original Apwd then the communication will continue

Figure 1: Functional Block Diagram of RFID System.

D) A Stepwise description of RFID System

1. The reader issues a Req_RN command to the acknowledged tag.
2. The tag then generates two 16-bit random numbers, namely, RT1 and RT2, and backscatters them with its EPC to the reader. The reader forwards these messages to the manufacturer.
3. The manufacturer matches the received EPC to retrieve the tag's access password (Apwd) and kill password (Kpwd) from the back-end database.
4. The manufacturer then generates and stores two 16-bit random numbers, namely, RM1 and RM2. The "cover-coded passwords" for the 16-bit MSBs (CCPwdM1) and the 16-bit LSBs (CCPwdL1) are computed by the PadGen function.
5. CCPwdM1, CCPwdL1, and EPC along with four 16-bit random numbers, namely, RM1, RM2, RM3, and RM4, generated by the manufacturer are transmitted to the reader, which, in turn, forwards them to the tag for verification.
6. To authenticate the tag, the tag generates another two random numbers RT3 and RT4 along with the received RM3and RM4 used to compute CCPwdM2 and CCPwdL2 with the PadGen (RTi,RMi) function.
7. CCPwdM2, CCPwdL2, and EPC along with two 16-bit random numbers, namely, RT3 and RT4, are transmitted to the reader, which, in turn, forwards them to the manufacturer for verification.

IV.AUTHENTICATION SCHEMES

Today security is imperative in many network-based applications. When dealing with data transfer, it is crucial to determine whether the data that is being received has been corrupted. In this system, we propose an authentication protocol, which mutually authenticates readers and tag's. It can resist man-in-the-middle attacks and reduce re- authentication overhead. The main advantage of our proposed scheme is that it does not require the implementation of any special cryptographic hash functions/keys within the tag. There is also no need for the tag and the reader to synchronize security keys/hash values. We propose to improve the existing one-way reader-to-tag authentication scheme.

E) Padgen

This scheme utilizes the tags 32-bit access and kill password in achieving tag-reader mutual authentication scheme. It uses two rounds of PadGen to compute a cover-coding pad. The first round performs PadGen over the access password, while the second round performs PadGen over the kill password.

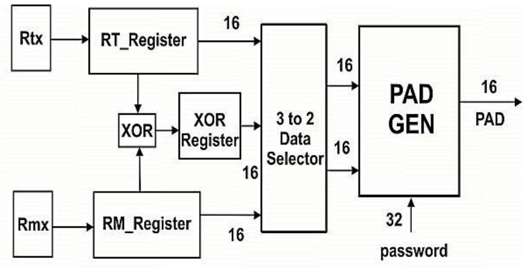


Figure 2: Functional block diagram of Padgeneration

The PadGen function is used to create the 16-bit Pads for covercoding the access password. This scheme is also much more dicult for an adversary to recover the access password under the correlation attack or to forge successful authentication under the dictionary attack.The PadGen function is the key function used to produce a cover-coding pad to mask the tags access password before transmission. The implementation of the PadGen function also requires the random number generator to produce RTx and RMx.

F) Access Password

An access password is required before data are exchanged between a reader and a single tag. The access password is a 32-bit value stored in the tag's reserved memory. If this password is set, then the reader has to have the valid password before the tag will engage in a secured data exchange.

G) Kill Password

The access passwords can be used in activating kill commands to permanently shut down tag's, as well as for accessing and re locking a tag's memory.

H) Data Selector

In electronics, a multiplexer or mux is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2n inputs has n select lines, which are used to select which input line to be sent to the output.An electronic multiplexer makes it possible for several signals to share one device or resource.A multiplexer is often used with a complementary demultiplexer on the receiving end. Multiplexer are combinational logic switching devices that operate like a very fast acting multiple position rotary switch. They connect or control, multiple input lines called "channels" consisting of either 2, 4, 8 or 16 individual inputs, one at a time to an output. Then the job of a multiplexer is to allow multiple signals to share a single common output.Multiplexers are used as one method of reducing the number of logic gates required in a circuit or when a single data line is required to carry two or more different digital signals.Generally, multiplexers have an even number of data inputs, a number of "control" inputs that correspond with the number of data inputs and according to the binary condition of these control inputs, the appropriate data input is connected directly to the output.

V.XOR SCHEME

In XOR Scheme each Pad function is computed based on PAD Function using one set of (RTx,RMx), which is transmitted in the open space. In contrast to the PadGen the present proposed PAD function is computed based on one set of (RV ,RW), which is not transmitted openly.

RV and RW are computed based on Apwd-PadGen (RTx,RMx)and Apwd PadGen(RTx,RTxRMx),respectively. PAD1 and PAD2 are then generated by Kpwd-PadGen(RV,RW)and Kpwd PadGen(RV,RvRW),respectively. The RV and RW values were calculated within the tag's and readers.Therefore,an adversary would not be able to correlate all the bits in ApwdM and ApwdL.

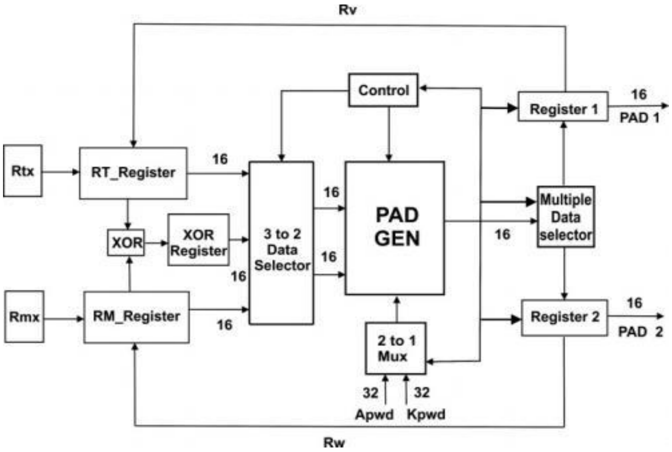


Figure 3: Functional block diagram of XOR Scheme.

I) Implementation of XOR Scheme

In 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. R_V and R_W are computed based on A_{pwd}-PadGen(R_{Tx},R_{Mx}) and A_{pwd}-PadGen(R_{Tx},$R_{Tx} \oplus R_{Mx}$), respectively.

PAD1 and PAD2 are then generated by K_{pwd}-PadGen(R_V,R_W) and K_{pwd}-PadGen(R_V,$R_V \oplus R_W$), respectively. The R_V and R_W values were calculated within the tag's and readers. Therefore, an adversary would not be able to correlate all the bits in A_{pwdM} and A_{pwdL}.

1. A_{pwd}-PadGen(R_{Tx},R_{Mx})=$d_{v1}d_{v2}d_{v3}d_{v4}$=R_V.R_{Tx},R_{Mx},and A_{pwd} are selected as the inputs for PadGen operation,and the calculation results R_V by XOR-PadGen operation are stored in register for further manipulation.

2. A_{pwd}-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 A_{pwd} are chosen as inputs for PadGen operation. The calculation result R_W is stored in register for further computation.

3. K_{pwd}-PadGen (R_V,R_W) = $h_{q1}h_{q2}h_{q3}h_{q4}$=PAD1. The PAD1 can then be obtained by mux selecting R_V, R_W, and K_{pwd} as inputs for XOR-PadGen operation.

4. K_{pwd}-PadGen(R_V,$R_V \oplus R_W$)=$h_{r1}h_{r2}h_{r3}h_{r4}$=PAD2. Similarly, the PAD2 can then be obtained using R_V,$R_V \oplus R_W$, along with K_{pwd} for XOR-PadGen operation.

VI.MOD SCHEME

Modulo arithmetic is used as another approach to generate the PadGen function because of the schemes simplicity.Modulo arithmetic does not require carry or borrow operations.In computing hardware, the carry circuitry is a major part of arithmetic computation and is a major contributor to speed limitations. The simplicity of modulo arithmetic allows several different approaches not available in the previous generation of PadGen function. These operations are done on modulo arithmetic based on modulo 2.

In modulo-2 mathematics, the subtraction function is replaced by the XOR operation. The XOR-based division (no carry in addition or subtraction) consumes very small resources. The particular advantage of XOR operation is that it can thus achieve low-cost hardware implementation of the PadGen function.

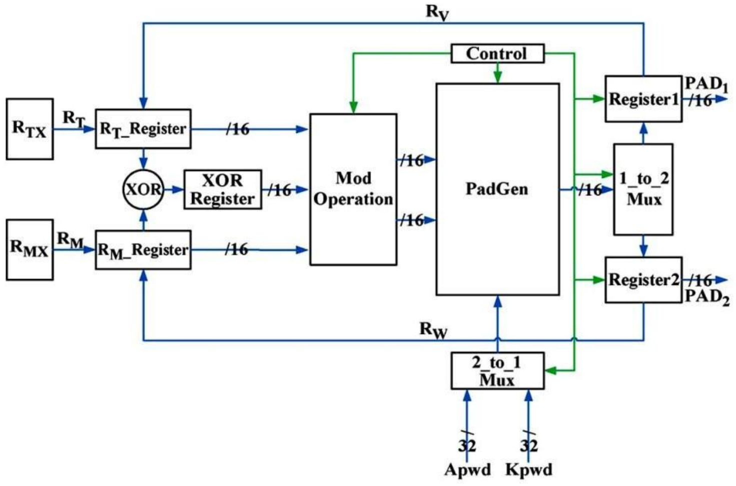


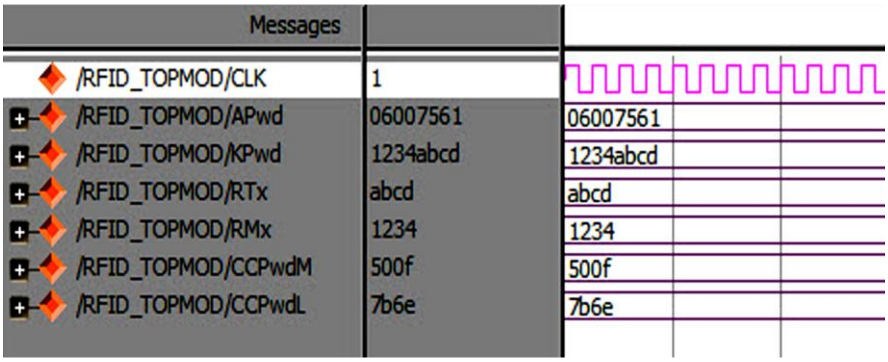
Figure 4: Functional block diagram of MOD Scheme.

J) Implementation of MOD Scheme

To implement the PadGen operation based on modulo arithmetic, a modulo-2 circuit module is inserted before PadGen operation. After RTx and RMx are generated, a multiplexer was utilized to allow an Apwd or Kpwd to be selected for MOD-PadGen operation.The details of the functions performed are described as follows.

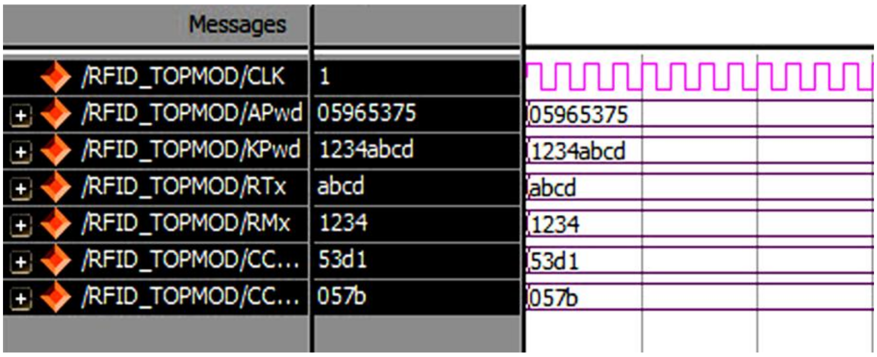
1) Apwd-PadGen(RA,RB) = di1di2di3di4 = RI. The mod1 and mod2 listed in are used to generate RA and RB, respectively.
2) RI is then calculated by performing PadGen over the Apwd, and the results are stored in Register1 for further manipulation.
3) Apwd-PadGen(RC,RD)=dj1dj2dj3dj4=RJ. The mod3 and mod4 listed are used to generate RC and RD, respectively. RJ is then obtained by executing PadGen over the Apwd, and the results are stored in Register2 for further calculation.
4) Kpwd-PadGen(RE,RF)=dk1dk2dk3dk4=PAD1. PAD1 is then calculated by performing PadGen over the Kpwd.
5) Kpwd-PadGen(RG,RH)=do1do2do3do4=PAD2. PAD2 is then calculated by performing PadGen over the Kpwd.

VII.SIMULATION AND HARDWARE RESULTS



Messages		
/RFID_TOPMOD/CLK	1	
/RFID_TOPMOD/APwd	06007561	06007561
/RFID_TOPMOD/KPwd	1234abcd	1234abcd
/RFID_TOPMOD/RTx	abcd	abcd
/RFID_TOPMOD/RMx	1234	1234
/RFID_TOPMOD/CCPwdM	500f	500f
/RFID_TOPMOD/CCPwdL	7b6e	7b6e

Figure 5: Simulation Output of XOR Scheme For Tag A.



Messages		
/RFID_TOPMOD/CLK	1	
/RFID_TOPMOD/APwd	05965375	05965375
/RFID_TOPMOD/KPwd	1234abcd	1234abcd
/RFID_TOPMOD/RTx	abcd	abcd
/RFID_TOPMOD/RMx	1234	1234
/RFID_TOPMOD/CC...	53d1	53d1
/RFID_TOPMOD/CC...	057b	057b

Figure 6: Simulation Output of XOR Scheme For Tag B.

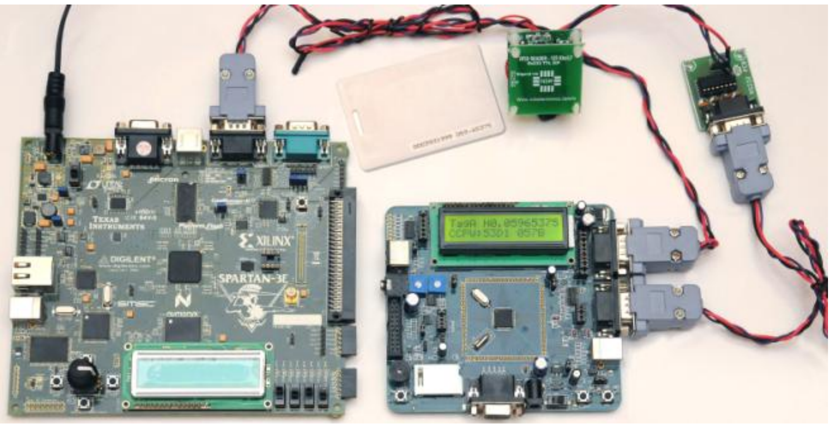


Figure 7: Hardware Output of XOR Scheme for Tag A.

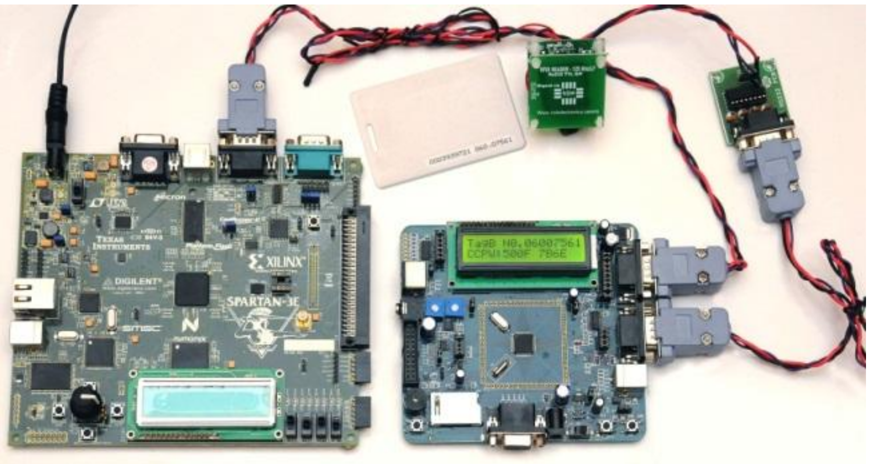
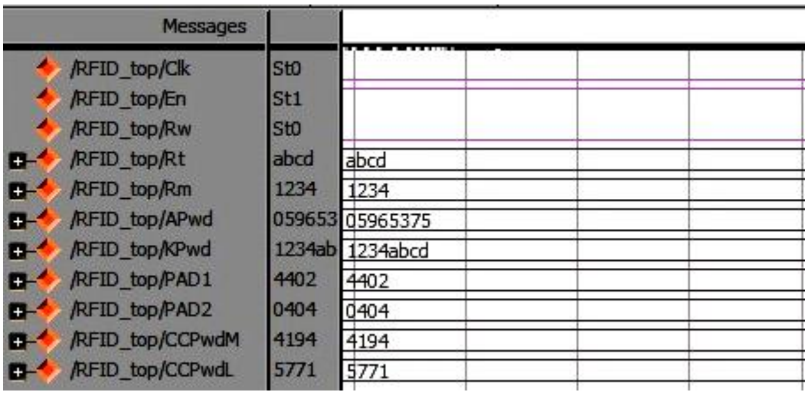


Figure 8: Hardware Output of XOR Scheme For Tag B.



```
Messages
/RFID_top/Clk      St0
/RFID_top/En       St1
/RFID_top/Rw       St0
/RFID_top/Rt       abcd    abcd
/RFID_top/Rm       1234    1234
/RFID_top/APwd     059653  05965375
/RFID_top/KPwd     1234ab  1234abcd
/RFID_top/PAD1     4402    4402
/RFID_top/PAD2     0404    0404
/RFID_top/CCPwdM   4194    4194
/RFID_top/CCPwdL   5771    5771
```

Figure 9: Simulation Output of MOD Scheme.

Simulations of the proposed design were conducted in the Spartan 3E environment. The verified Verilog code was then downloaded on a Xilinx Spartan 3E FPGA running with a 50-MHz clock in the Spartan 3E board to verify the hardware. The output waveforms are displayed using ModelSim for real-time verification. The FPGA implementation result on the Spartan 3E and ARM 7 are shown in Fig. 7 and Fig 8. The LCD displays were used to denote the 16-b random numbers RT = abcd and RM =1234 , and the cover-coded Apwd =05965375 as shown in Fig. 7, The Verilog simulation results under the same input conditions as for FPGA implementation are shown in Fig.5 and Fig 6. Only Simulation verification done in Modelsim for MOD operation are shown in Fig 9.

VIII.CONCLUSION

To improve the security level of the original reader-to-tag authentication protocol proposed under the EPC C1G2 speciation, the PadGen functions are used to protect the Access password against exposure. The main advantage of the proposed scheme is that it does not require the implementation of any special cryptography hash functions/keys within the tag and a center server/database. The PadGen functions based on XOR operation and MOD operation in association with the tags Apwd and Kpwd are used to generate the PADi. The proposed protocol using the manipulated values within the tag's and reader to enhance the PadGen operation is more security for mutual authentication for the tag and reader.In Future Hash Functions for every components and it make more complexity to hack the password during the data transactions

REFERENCE

[1] Mohanavelu.S and Ramya.T, "Secured Authentication Protocol for RFID System Using XOR Scheme", IJSR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH,Vol 2,No.5,May 2013

[2] Yu-Jung Huang, Senior Member, IEEE, Wei-Cheng Lin, and Hung-Lin Li, "Efficient Implementation of RFID Mutual Authentication Protocol", IEEE transactions on industrial electronics, vol. 59, no. 12, december 2012.

[3] 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, pp. 15731582, May 2010.

[4] S. Piramuthu, "Lightweight cryptographic authentication in passive RFID-tagged sys- tems", IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.,vol. 38, no. 3, pp. 360376, May 2008.

[5] A.Juels, "RFID security and privacy: A research survey", IEEE J. Sel.Areas Commun.,, vol. 24, no. 2, pp. 381394, Feb.2006.

BIOGRAPHY

Mohanavelu.S received his Bachelor’s Degree in Electronics and Communication Engineering from SCSVMV University, Tamil Nadu,India in the year 2011 and obtained his Master’s Degree in VLSI Design from SRM University,Tamil Nadu,India in the year 2013. He Research interest includes also in Digital Circuits, Embedded Systems and Broadcast Engineering.

T.Ramya received her Bachelor’s Degree in Electronics and Communication Engineering from Madras University, Tamil Nadu,India in the year 2000 and obtained her Master’s Degree in Communication Systems from Anna University,Tamil Nadu,India in the year 2005.She started her career as a Lecturer in SRM University and presently working as Assistant Professor (Sr.G) in the School of ECE,SRM University,India .She has nearly eight years of Teaching Experience and her research interest includes Wireless Communication ,Network Security and Mobile Ad-Hoc Networks .