Volume: 2 Issue: VI Month of publication: June 2014

DOI:

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

FPGA Implementation OF RFID Mutual Authentication Protocol

Chetna Devi Kh[1], Mrs.Ashwini[2]

PG Scholar at PESIT Bangalore[1] ,Asst. Prof, Dept of E&C PESIT, Bangalore[2]

Abstract: Radio frequency identification, or RFID, is a generic term for technologies that use radio waves to automatically identify people or objects. The wide deployment of RFID also incurs many security concerns and practical attacks. Many authentication schemes have been proposed. But these schemes have not been verified with hardware implementation.This project focuses on solving the security problem related to RFID tag reader.A specially designed pad generation (PadGen) function will be included to improve security. The PadGen function is used to produce a cover-coding pad to mask the tag's access password before the data are transmitted .The optimization of the area utilization is also done .The hardware implementation of the project is done using FPGA kit. Simulation of the codes is done with the help of XILINX and ModelSim.

Keywords-RFID,FPGA,Mutual authentication,Security.

I.INTRODUCTION

Due to the low cost and the convenience in identifying an object without physical contact, Radio Frequency Identification (RFID) systems have become more and more popular. It uses a wireless system that can provide enterprises with efficient real-time product track-and-trace capability.An RFID application contains three basic roles: tag, reader and back-end database.Each tag contains a unique identification, often called the tag identification (TID). The reader is used to query the tag's TID and forward it to the back-end database. Once the tag is found valid, the back-end database will look up its product information for further processing. RFID tags are classified into three types: active, semi-passive, and passive.

The wide deployment of RFID also incurs many security concerns and practical attacks . The ISO 18000-6C protocol, also known as the EPC C1G2 protocol, provides basic security tools using a 16-b pseudorandom number generator (PRNG) and a 16-b cyclic redundancy code (CRC).

An authentication scheme was originally included as part of the EPC C1G2 industrial standard to secure RFID transactions. However, the Gen2 specification has the vulnerability that the TID is transmitted without any guard.Solving the authentication protocol with the area optimisation is very important.

II.LITERATURE SURVEY

Till now papers are published based on the security requirements and detailed study of challenges . A clear survey was done for recent technical research on the problems of privacy and security for radio frequency identification(RFID.) A detailed analysis of the security weakness of the one-way reader-to-tag authentication scheme has been provided.

III.PROPOSED SYSTEM

The proposed system aims at solving the authentication problem. The RFID tag–reader mutual authentication (TRMA) scheme will be utilised to solve the problem. A protocol using the XOR operation tag's Apwd and Kpwd for achieving a TRMA scheme. Designing new authentication protocols conforming to the standard and providing an adequate security level are therefore exciting challenges.

In the authentication scheme based on the ISO 18000-6C protocol the RFID systems are vulnerable to cloning attacks as well as password disclosure and information leakage .To solve this problem PadGen function is proposed. The PadGen function is the key component in constructing the 16-b pads to cover-code the two 16-b Apwd halves ApwdM (comprising the 16 most significant bits) and ApwdL (comprising the 16 least significant bits). The PadGen function is used to produce a cover-coding pad to mask the tag's Apwd before transmission. PadGen takes two 16-b random numbers RT_x and RM_x as its inputs.

IV.WORK METHODOLOGY

The proposed scheme based on XOR or MOD operation to generate PadGen function is an improvement over the weak one-way reader-to-tag authentication scheme proposed by the 18000-6C protocol.

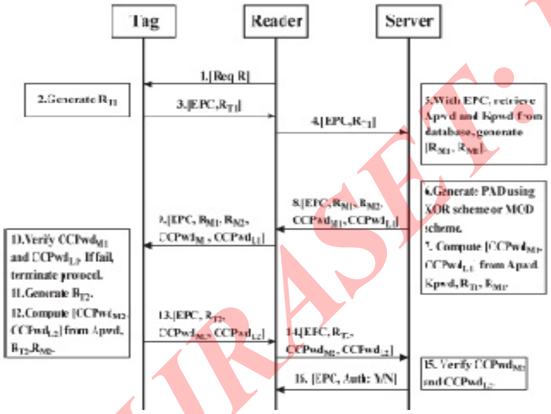

Tag
Reader
Server
1.[Req R]
2.Generate R_{T1}
3.[EPC,R_{T1}]
4.[EPC,R_{T1}]
5.With EPC, retrieve Apwd and Kpwd from database, generate [R_{M1}, R_{M2}].
6.Generate PAD using XOR scheme or MOD scheme.
7. Compute [$CCPwd_{M1}$, $CCPwd_{L1}$] from Apwd, Kpwd, R_{T1}, R_{M1}
8.[EPC, R_{M1}, R_{M2}, $CCPwd_{M1}$, $CCPwd_{L1}$]
9.[EPC, R_{M1}, R_{M2}, $CCPwd_{M}$, $CCPwd_{L1}$]
10.Verify $CCPwd_{M1}$ and $CCPwd_{L1}$. If fail, terminate protocol.
11.Generate R_{T2}.
12.Compute [$CCPwd_{M2}$, $CCPwd_{L2}$] from Apwd, R_{T2}, R_{M2}.
13.[EPC, R_{T2}, $CCPwd_{M2}$, $CCPwd_{L2}$]
14.[EPC, R_{T2}, $CCPwd_{M2}$, $CCPwd_{L2}$]
15. Verify $CCPwd_{M2}$ and $CCPwd_{L2}$.
16. [EPC, Auth: Y/N]

Fig 1 : Tag-reader authentication using the xor or mod scheme

Xor scheme is utilised because it does not require the implementation of any special cryptographic hash functions/keys within the tag and a center server/database.

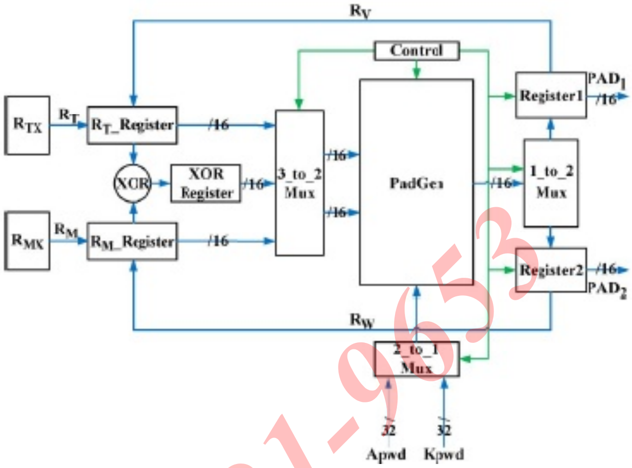


Fig 2: Functional block diagram of the xor-padgen operation

The present approach will obtain PAD_1 and PAD_2 using one set of (R_{Tx},R_{Mx}). As compared with the design, the present approach is an efficient way to generate PAD function for mutual authentication.

V.RESULT

Simulations of the proposed design will be conducted in the Xilinx 12.2 and modelsim. The verified Verilog code will be then downloaded on FPGA.

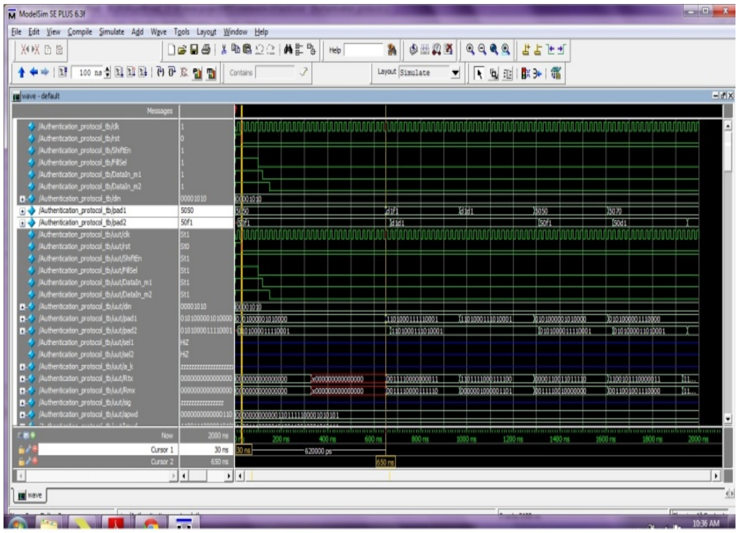
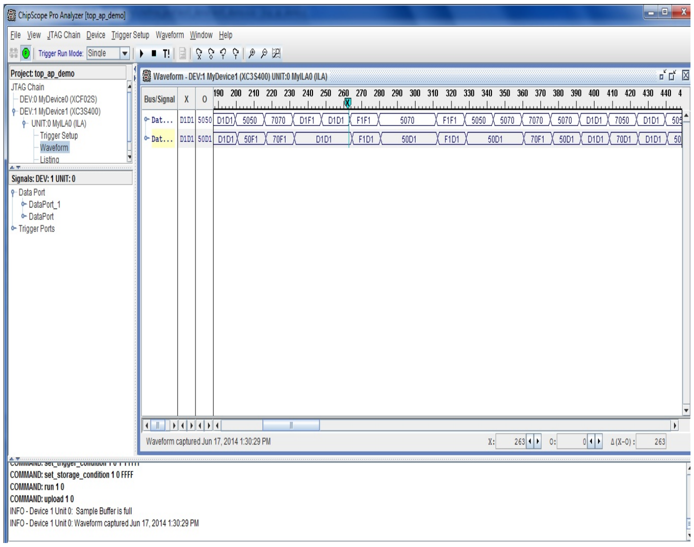

ModelSim SE PLUS 6.3f
File Edit View Compile Simulate Add Wave Tools Layout Window Help
wave - default
Messages

Fig 3: Simulation result using Modelsim


ChipScope Pro Analyzer [top_ap_demo]
File View JTAG Chain Device Trigger Setup Waveform Window Help
Trigger Run Mode: Single
Project: top_ap_demo
JTAG Chain
DEV:0 MyDevice0 (XCF02S)
DEV:1 MyDevice1 (XC3S400)
UNIT:0 MyILA0 (ILA)
Trigger Setup
Waveform
Listing
Signals: DEV: 1 UNIT: 0
Data Port
DataPort_1
DataPort
Trigger Ports
Waveform - DEV:1 MyDevice1 (XC3S400) UNIT:0 MyILA0 (ILA)
Bus/Signal
X
O
190 200 210 220 230 240 250 260 270 280 290 300 310 320 330 340 350 360 370 380 390 400 410 420 430 440
Dat... D1D1 5050 D1D1 5050 7070 D1F1 D1D1 F1F1 5070 F1F1 5050 5070 7070 5070 D1D1 7050 D1D1 505
Dat... D1D1 50D1 D1D1 50F1 70F1 D1D1 F1D1 50D1 F1D1 50D1 70F1 50D1 D1D1 70D1 D1D1 50
X: 263 O: 0 Δ(X-O): 263

```
Waveform captured Jun 17, 2014 1:30:29 PM
COMMAND: set_trigger_condition 1 0 1 11111
COMMAND: set_storage_condition 1 0 FFFF
COMMAND: run 1 0
COMMAND: upload 1 0
INFO - Device 1 Unit 0:  Sample Buffer is full
INFO - Device 1 Unit 0: Waveform captured Jun 17, 2014 1:30:29 PM
```

Fig 4: Verilog simulation result using FPGA downloaded data

Table I

FPGA resource utilizations of the proposed design

Resources		Xor scheme	
		Proposed work	Previous work
.Xilinx 12.2 Vertex5 XC5VLX30	Number of slice registers	416	599
	Number of slice LUTs	330	427

VI. CONCLUSION

The PadGen functions are used to protect the Apwd against exposure. The main advantage of the proposed scheme is that it does not require the implementation of any special cryptographic hash functions/keys within the tag and a center server/database. There is also no need for the tag and the reader to synchronize security keys/hash values. The PadGen function was modified to strengthen the security of the mutual authentication scheme in this project. Area can also be effectively reduced in the process. In future design can be still made robust by implementing search based mechanism to improve the recolonization time.

REFERENCES

[1] A. Juels, “RFID security and privacy: A research survey,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[2] D. M. Konidala, Z. Kim, and K. Kim, “A simple and cost effective RFID tag–reader mutual authentication scheme,” in *Proc. Int. Conf. RFIDSec*, Jul. 2007, pp. 141–152.

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

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

[5] Yu-Jung Huang ,Wei-Cheng Lin, and Hung-Lin Li, “Efficient Implementation of RFID Mutual Authentication Protocol,” *IEEE Trans. Ind. Electron.*, vol. 59, no. 12, Dec. 2012.

ACKNOWLEDGEMENT

The satisfaction that allows the successful completion of any work is incomplete without the mention of the names of the people who made it possible. I consider it as my privilege to express my gratitude and sense of appreciation to Mrs.Ashwini,Asst.Prof ECE Dept.,PESIT for her valuable guidance and dynamic support.