A Systematic TRMA Protocol for Yielding Secure Environment for Authentication and Privacy Aspects

Anusha R[1]
Department of Electronics and Communication Engineering,
N. M. A. M. Institute of technology, (Visvesvaraya
Technological University, Belagavi) Nitte 574110
Udupi District, Karnataka, India

Veena Devi Shastrimath V[2]
Professor, Dept. of ECE
NMAM Institute of Technology
NITTE, Udupi
India

***Abstract*—RFID is a system that uses the radio waves to scrutinize and capture data pertained to a tag for an object attached to it. In spite of RFID's wide application in industries, it poses a severe security issue. There is high susceptibility that RFID might be attacked with future attacks to invade the privacy and data in the system. To protect the RFID system against such attacks, the Pad-generation (Pad-Gen) function is used. This paper presents a mutual authentication scheme Tag Reader Mutual Authentication (TRMA) that is implemented using two approaches, the XOR operation and the MOD operation by modifying the Pad-Gen function. The proposed framework is executed on low-cost Artix7 FPGA XC7A100T-3CSG324, and its hardware verification is done on chip scope pro tool.**

Keywords*—Mutual Authentication; Modified Pad-Gen; Radiofrequency Identification (RFID); Privacy; Security; Tag-Reader Mutual Authentication (TRMA)

I. INTRODUCTION

RFID is an emerging wireless technology that operates over the radio signals to recognize and track the various objects that consist of a distinctive serial identification [1]. The RFID system comprises majorly of three different sections, which are the transponder/tag, a database, or an interrogator/reader. It uses the general frequency bands, which are the Ultra High-Frequency Band (860 MHz- 930MHz), High Frequency (13.56MHz), and Low Frequency (125 kHz – 134 kHz) [2]. An RFID tag individually owns a unique identification code called the Electronic Product Code (EPC) [3]. The two kinds of tags are the active tags and the passive tags separable by the implications, specifications, and storage capacity. The passive tags don't need a battery as it charges itself from the charge availed from the electromagnetic signals of the reader's request side, whereas the active tag demands battery back-up. Passive tags are built to enable lower storing capacities lesser than the values of 1KB, used in shorter applications range from those of 4 inches to 15 feet. It has the capability wherein it can read once and write many. Hence these are the read-only tags. Opposite to this, active tags have a storage ability of 512KB, implied in the utilization of massive applications until 300 feet [4]. The role of the RFID reader is to write and read the information available on the tag. The details are preserved in a database consisting of integrated circuitry that concerning the password of tags individually, EPC, and reader [5]. Usually, there is a requirement for a dynamic protocol to establish a secured communication taking place among the RFID reader and the tag. For various security applications, a vital role is played by the Linear Feedback Shift Register (LFSR) [6]. This operates generating random numbers together at the side of the tag and reader. The two kinds of LFSR architectures are the Galois and the Fibonacci LFSRs. Out of the two, the Fibonacci LFSR is the one which is most commonly applied to the hardware implementation use [7].

A new version of EPC Class-1 has been ratified. This is EPC Class-1 version in Generation 2 that is compatible along with the old version, to provide a set of a new type of featured series intends on improvising the security parameter giving an opportunity to the manufacturers to perform the customization using cryptographic authentication ways for verification of identities and avoid the unauthorized access [8]. As per the previous standard, the new EPC standard also supports Cyclic Redundancy Check (CRC), Pseudo-Random Number Generator (PRNG), and the XOR function. A security protocol is considered as EPC compliant only if it solely makes use of one or more functions [9]. Moreover, the functions mentioned are not cryptographic functions themselves. Various other measures should be ensured to provide an acceptable security level of computations as there only 500-5000 elements of gates present on a tag [10]. Therefore, this paper proposes a framework to provide a secure environment for RFID to transfer data. Section II focuses on the background of RFID along with the description of a problem statement. Section III foregrounds the existing techniques in securing the privacy concern of RFID.

Further, the hardware architecture of the proposed mechanism is given in Section IV. The results are discussed in Section V. The performance analysis of both the approaches is carried out in Section VI. The conclusion is followed in Section VII.

II. BACKGROUND AND CHALLENGING ISSUE

The RFID mutual authentication protocol establishes the communication between the reader and the tag that is encoded using a password. The communication in RFID is initiated by transferring a signal request from the reader. Radio signals are emitted from the reader section, and as the tag is made to enter the range, it responds towards the reader's request [11]. These protocols mentioned below, have a unique procedure for encrypting and decrypting along with few benefits as well as drawbacks.

A. Standard of EPC Global Class-1 Generation-2

The standard utilizes a bitwise EX-OR operation that performs the function of the cover code string. The scheme does not guarantee a secure environment as it provides support only for the reader's authentication. This helps in creating fake cloning tags that utilize the unencrypted password in the form of a cover code that is generated using primary bitwise operation. The non-volatile features that should be pertained to an RFID tag are briefed as follows:

- Password- Two passwords individually consisting of 32 bits that operate at the transmitter and receiver section to access/kill the tag forever hold space in the reserved memory.

- Object Identification and user Memory- To identify the object to which tag is attached, the memory space of the tag has an EPC section comprising of Protocol Control bits (PC-16). CRC bits (16) in the PC accomplish the task of object identification. The data that is processed as per the user's instructions are stored in the user memory [12].

B. Mutual Authentication Protocol- PadGen

A computational procedure that encrypts and decrypts the password accordingly is called the PadGen operation for a mutual authentication scheme. In a mutual authentication scheme, two passwords are made. This involves the process of four numbers randomly consisting of two rounds each; the PadGen computes the cover code password further. The initial around would of PadGen comprises of the Access password, and another round has the Kill password [13]. Also, the hardware realization of the protocol is not accomplished. Following which the same PadGen function is used but pertained to a different computational procedure [14].

C. Standard of EPC Global Class-1 Generation-2

The standard utilizes a bitwise EX-OR operation that performs the function of the cover code string. The scheme does not guarantee a secure environment as it provides support only for the reader's authentication. This helps in creating fake cloning tags that utilize the unencrypted password in the form of a cover code that is generated using primary bitwise operation. The non-volatile features that should be pertained to an RFID tag are briefed as follows:

- Password- Two passwords individually consisting of 32 bits that operate at the transmitter and receiver section to access/kill the tag forever hold space in the reserved memory.

- Object Identification and user Memory- To identify the object to which tag is attached, the memory space of the tag has an EPC section comprising of Protocol Control bits (PC-16). CRC bits (16) in the PC accomplish the task of object identification. The data that is processed as per the user's instructions are stored in the user memory [12].

D. Mutual Authentication Protocol- PadGen

A computational procedure that encrypts and decrypts the password accordingly is called the PadGen operation for a mutual authentication scheme. In a mutual authentication scheme, two passwords are made use of. This involves the operation of four numbers randomly consisting of two rounds each; the PadGen computes the cover code password further. The initial around would of PadGen comprises of the Access password, and another round has the Kill password [13]. Also, the hardware realization of the protocol is not accomplished. Following which the same PadGen function is used but pertained to a different computational procedure [14].

III. Existing Techniques in Securing the Privacy Concerns of RFID Systems

There are numerous schemes presented by various researchers concerning the aspect of RFID security. This section stresses the techniques incorporated for enabling securer RFID access in a wireless environment. Sarma et al. [16] showed that the Auto-ID Center is an emerging way to develop a cost-effective RFID system as an extension to the bar code use. Due to the constrained RFID resources and also with the interconnections, low-cost RFID is not ideal for the functioning of wireless devices. Yuan et al. [17], designed encoder architecture for UHF –Ultra High Frequency, RFID purposes. Two schemes, namely the Miller Modulated Subcarrier (MMS), and Bi-phase space applicable in Class-1, Gen 2 UHF RFID implications scenarios have been designed. Avoine and Oechslin [18] stressed that there is a chance of high susceptibility to attacks over RFID technology, threatening the privacy of the network. The study introduced a scheme for eliminating the scalability constraint in the overall mechanism. This indeed ensured that the system exhibits the function of forwarding privacy and privacy. Kim et al. [19] propose an interference model that is derived from the interference statistics from a reader-to-reader over a nominal level of the desired reader in the model.

Peris-Lopez et al. [20] presented a lightweight protocol for mutual authentication among the tag and the reader. This suggested adequate privacy and security levels, capable enough of being applicable in most systems for real-time operations as it has a fundamental requirement to accomplish the operation of only 300 gates. Garfinkel et al. [21], foregrounded the potential privacy threats faced by activists with the increasing employment of RFID in multiple areas. The work of Li and Wang [22], analyze security vulnerabilities respective to two ultra-light weighted mutual authentication protocols. By identifying two attacks, the functioning of the protocol is tested. Bogdanov et al. [23], focused on the drawback of utilizing the cheap tags for RFID operation that tend to compromise with the security and privacy measure in the network. Hash function working is described, whereas it also highlights the major issues designing lightweight functions. The study of Want [24], showed that the necessity to incorporate RFID sensors would be mostly in the use of environmental sensors. Thiesse et al. [25] presented the primary ideas and implications of the EPC network, the integration of it along with the enterprise systems involving its functionality for data communication among supply chain organizations. Eom et al. [26] concentrated on the issue of collisions among readers in RFID. The study proposed an effective algorithm for anti-collision between readers. The work of Lopez et al. [27], surveyed the crucial technical limitations of RFID systems.

Sun et al. [28] proposed a framework of the novel Gen2 authentication protocol for cost-effective RFID tags. The protocol ensures that readers can access the reading of new tags. Peris-Lopez et al. [29] proposed a new scheme of the mutual authentication protocol for the light-weight RFID tag-readers based on the EPCglobal mechanism. Konidala et al. [29], introduced a fundamental, reliable, low cost enabled, the lightweight mutual authentication scheme for the RFID tag-reader. The scheme addresses the approach of two standards, namely, a protocol of EPCglobal Class 1 Gen2 Ultra High-Frequency RFID and EPCglobal framework architecture. The schemes make use of Access and Kill Password that is indeed successful in achieving three aims of detecting the cloned fake tags, allowing the manufacturer to keep track of the genuine products and removing the malicious snooping readers.

The study of Han et al. [30] described a model for the effective localization in indoor robots used in mobiles incorporating the technology of RFID systems. Juels [31], surveyed over the difficulties in security and privacy concerns of RFID systems. The surveys investigate an approach to protect the privacy and integrity of the system.

Lee et al. [32] presented an RFID tag chip that, in the compact in size, completely integrated into the HF-band, enabling the security and authentication function. Eisenbarth et al. [33], surveyed the implementations reading the Lightweight cryptography. The high-cost requirements and implementation limitations of the products pertaining to high-volume involving the smart cards and RFID secure tags, mandatorily need cryptographic implementations. The work carried out by Piramuthu [34], carry out the study and estimation of protocols from an individual stream of security, recognizing the vulnerabilities and hence design an optimal solution. The security analysis respective to the proposed settlement is being conducted. Anusha R and Veena Devi Shastrimat [35] have presented qualitative evaluation over efficiency of the security methods to safeguarding NFC tools and its services. Anusha R and Veena Devi Shastrimat [36] have an efficient method for Mutual verification of the RFID wireless schemes. Anusha R and Veena Devi Shastrimat [37] have a proficient Lightweight cryptographic Block cipher design. The hardware architecture of Tiny Encryption Algorithm (TEA) has been designed and which is very simple, elastic, less computations needed and simple key development.

IV. Hardware Architecture

The proposed TRMA protocol hardware architecture uses 32-bit passwords. To establish mutual authentication in RFID, the tag and reader individually generates a 16-bit password, which together makes it the 32-bit password. The hardware protocol that functions on the Exclusive OR operation requires interchanging information among the tag and reader to accomplish a secure communication path. The access password and kill password are identical two 32-bit values that are stored in the memory space of tag. Before the data interchange process between the tag and reader, the reader needs to indicate a confirmation regarding the password validity. This step is mandatory to set up a password for RFID communication. Fig. 1 depicts the hardware architecture of the modified pad generated TRMA using the XOR method for RFID. To ensure a secure environment for RFID data exchange, Access Password (AP) and Kill Password (KP) reserve memory space and are represented in equations (1-6). Both the passwords use 32-bits in the memory, individually pertaining to 16 bits of data. The LSB and MSB for the two 16 bit passwords are as follows:

Access Password,

$$AP = ap0ap1\ldots\ldots..ap31 \tag{1}$$

$$\text{For MSB, } APM = ap16ap17....ap31 \tag{2}$$

$$\text{For LSB, } APL = ap0ap1\ldots\ldots.ap15 \tag{3}$$

Kill Password,

$$KP = kp0kp1\ldots\ldots\ldots..kp31 \tag{4}$$

$$\text{For MSB, } KPL = kp0kp1\ldots\ldots.kp15 \tag{5}$$

$$\text{For LSB, } KPM = kp16kp17\ldots..kp31 \tag{6}$$

The MSB (8 bits) and LSB (8 bits) are concatenated to obtain the resulting 16bits of AP and KP, respectively.

An algorithm of TRMA using XOR operation as follows:

1. *Process Initialization* $\leftarrow$ *The request (R) is transferred from the reader to tag*
2. *LFSR generates a 16-bit random number concerned to tag* (R_{Tx}).
3. *A communication path is established through EPC.*
4. *LFSR generates a 16-bit random number concerned to a manufacturer* (R_{mx}).
5. $R_T \oplus_M \leftarrow R_T \oplus R_M$
6. $Rv \leftarrow Pad\text{-}gen(R_{TX}, R_{MX})$*---[Apsd]*
7. $Rw \leftarrow Pad\text{-}gen(R_T, R_T \oplus_M)$*---[Apsd]*
8. $R_V \oplus_W \leftarrow R_V \oplus R_W$
9. $PAD1 \leftarrow Pad\text{-}gen(Rv, Rw)$ *---[Kpsd]*
10. $PAD2 \leftarrow Pad\text{-}gen\ (Rv_, Rv \oplus_W)$ *---[Kpsd]*
11. $CCPSD_M \leftarrow Apsd_M \oplus PAD1$*---(Code covered password MSB)*
12. $CCPSD_L \leftarrow Apsd_L \oplus PAD2$*---(Code covered password LSB)*
13. *Tag Verification and Authentication* $\leftarrow$ *The tag verifies the password validity and reader authenticates the tag.*

The hardware architecture modified Pad-Gen TRMA using the MOD method is illustrated in Fig. 2. The steps in involved in the operation of TRMA using MOD [15] operation are explained as follows:

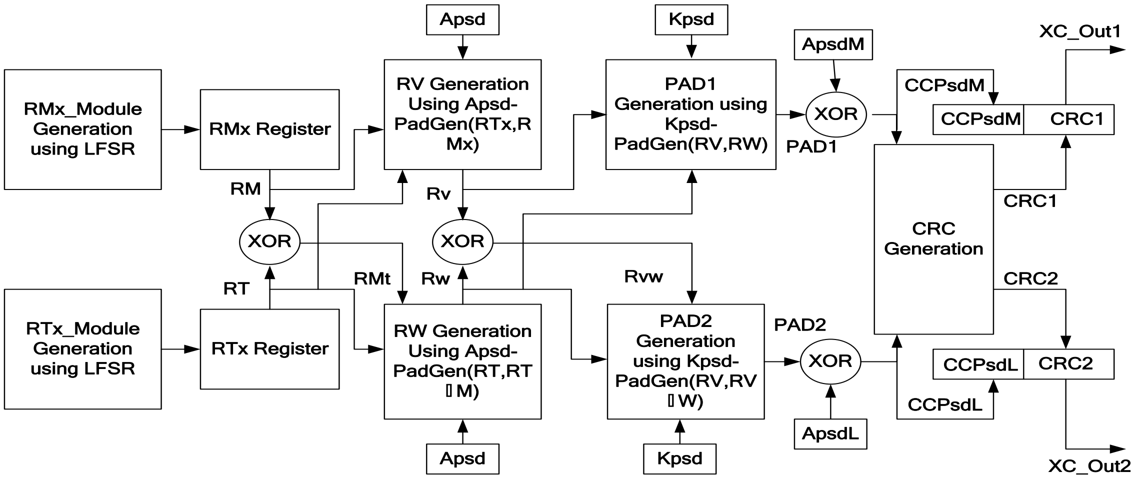
Apsd
Kpsd
ApsdM
XC_Out1
RMx_Module Generation using LFSR
RMx Register
RV Generation Using Apsd-PadGen(RTx,RMx)
PAD1 Generation using Kpsd-PadGen(RV,RW)
XOR
CCPsdM
CCPsdM
CRC1
PAD1
RM
Rv
XOR
XOR
CRC1
CRC Generation
RT
RMt
Rw
Rvw
CRC2
RTx_Module Generation using LFSR
RTx Register
RW Generation Using Apsd-PadGen(RT,RT▯M)
PAD2 Generation using Kpsd-PadGen(RV,RV▯W)
PAD2
XOR
CCPsdL
CRC2
CCPsdL
Apsd
Kpsd
ApsdL
XC_Out2

Fig. 1. Hardware Architecture of Modified Pad-Gen Design using XOR Method for RFID –TRMA Protocol.

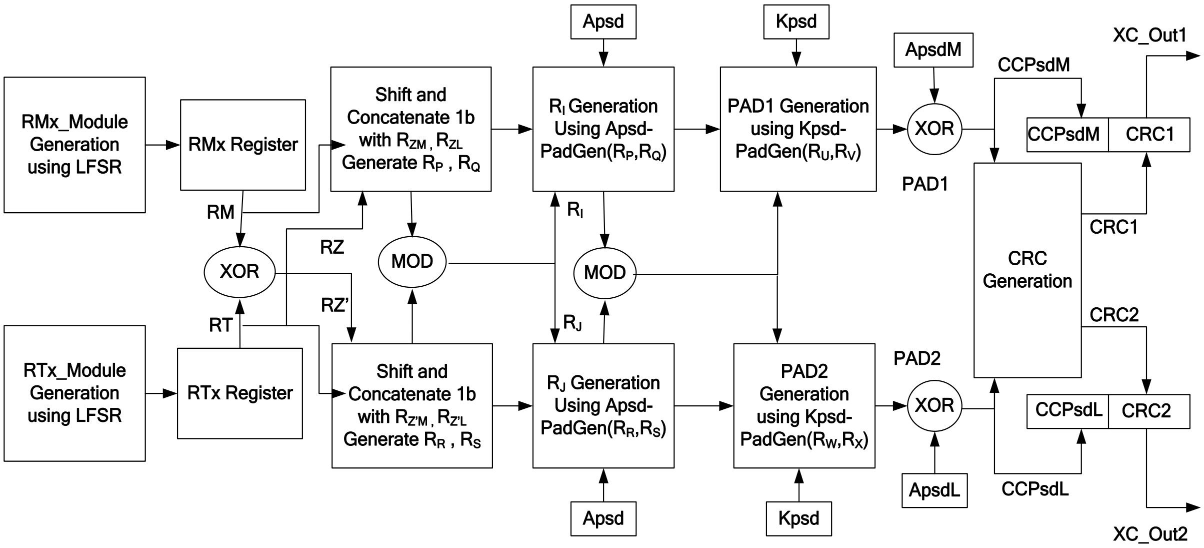
Apsd
Kpsd
ApsdM
XC_Out1
CCPsdM
RMx_Module Generation using LFSR
RMx Register
Shift and Concatenate 1b with R_ZM , R_ZL Generate R_P , R_Q
R_I Generation Using Apsd-PadGen(R_P,R_Q)
PAD1 Generation using Kpsd-PadGen(R_U,R_V)
XOR
CCPsdM
CRC1
PAD1
RM
R_I
CRC1
RZ
MOD
MOD
XOR
CRC Generation
RZ'
RT
R_J
CRC2
PAD2
RTx_Module Generation using LFSR
RTx Register
Shift and Concatenate 1b with R_Z'M , R_Z'L Generate R_R , R_S
R_J Generation Using Apsd-PadGen(R_R,R_S)
PAD2 Generation using Kpsd-PadGen(R_W,R_X)
XOR
CCPsdL
CRC2
ApsdL
CCPsdL
Apsd
Kpsd
XC_Out2

Fig. 2. Hardware Architecture of Modified Pad-Gen Design using MOD Method for RFID –TRMA Protocol.

The algorithm of TRMA using MOD operation as follows:

1. *Process Initialization ← The request (R) is transferred from the reader to tag*
2. *LFSR generates a 16-bit random number concerned to tag (R_{Tx}).*
3. *A communication path is established through EPC.*
4. *LFSR generates a 16-bit random number concerned to the manufacturer (R_{mx}).*
5. $R_T \oplus_M \leftarrow R_T \oplus R_M = R_Z$, $[RZ= R_{ZM} \| R_{ZL}]$
6. *Shifting by one bit left and concatenate*$\leftarrow R_{1+ZM} = \{1, R_{ZM}\}$, $R_{1+ZL} = \{1, R_{ZL}\}$
7. *Mod-Operation for MSB* $(R_P) \leftarrow Mod_1 (R_T) \| Mod_1 (R_M)$
8. *Mod-Operation for LSB* $(R_Q) \leftarrow Mod_1 (R_T) \| Mod_1 (R_M)$
9. $R_I \leftarrow$ *Pad-gen* (R_P, R_Q) --- *[Apsd]*
10. $R_Z' \leftarrow$ *bit reversal* (R_Z)
11. *Shifting by one bit left and concatenate*$\leftarrow R_{1+ZM} = \{1, R_{ZM}\}$, $R_{1+ZL} = \{1, R_{ZL}\}$
12. *Mod-Operation for MSB* $(R_R) \leftarrow Mod_1 (R_T) \| Mod_1 (R_M)$
13. *Mod-Operation for LSB* $(R_S) \leftarrow Mod_1 (R_T) \| Mod_1 (R_M)$
14. $R_J \leftarrow$ *Pad-gen* (R_R, R_S) --- *[Apsd]*
15. *Replace*R_P, R_Q, R_R, R_S with R_U, R_V, R_W, R_X *and repeat the process from step5*
16. *PAD1 ← Pad-gen* (R_U, R_V) --- *[Kpsd]*
17. *PAD2 ← Pad-gen* (R_W, R_X) --- *[Kpsd]*
18. *Tag Verification and Authentication ← The tag verifies the password validity and reader authenticates the tag.*
19. $CCPSD_M \leftarrow Apsd_M \oplus PAD1$*---(Code covered password MSB)*
20. $CCPSD_L \leftarrow Apsd_L \oplus PAD2$*---(Code covered password LSB)*
21. *Authentication and Verification*
22. *Cyclic Redundancy Check (CRC)← after the generation of code covered passwords, the CRC can be incorporated to provide the next level of security in the mutual authentication process.*

V. Result Discussion

The simulation outcomes relevant to the modified PadGen of TRMA are described in Fig. 3. Additionally, the physical verification of the outcomes is depicted in Fig. 4. The design is implemented using Verilog coding on Xilinx 14.7 ISE. The device used is Artix7 FPGA with Modelsim 6.5f. As the clock is triggered high along reset pulled to logic 0, the output for the PAD1 and PAD2 are observed. AP and KP are predefined values before the process of sending a request to the tag. The crc_en signal uses the LFSRs to generate the crc_out. The output XC_Out1 and XC_Out2 are attained by performing concatenation operation on CCPSDM, CCPSDL with crc_out1, and crc_out2.

And further on-chip scope pro- tool for hardware verification. The design of the TRMA protocol for XOR implementation is integrated with ILA and ICON IP core. This aids in prototyping the architecture on the FPGA platform.

The inputs are pre-defined both in case of simulation and physical verification. The input pins like reset, enable, and crc_en are provided input via FPGA pins. The values of XC_Out1 and XC_Out2 are verified on the simulation result and the chip scope pro tool. This proves that both while performing simulation and hardware verification, the same values were attained.

The simulation outcomes and physically verified results of TRMA protocol using the MOD method are shown in Fig. 5 and Fig. 6, respectively. At first, the bit file is dumped on FPGA and further over chip scope pro tool for hardware verification. As observed from the simulation result in Fig. 5, when reset is pulled low, XC_Out1 and XC_Out2 use the first four bits from $CCPSD_M$ and $CCPSD_L$. Rest to fill the place of the remaining four bits; zero is appended. In the further cycle, the zeroes are replaced by the output generated from crc_out1 and crc_out2. Hence the process keeps continuing by considering the first four bits to be taken from $CCPSD_M$, $CCPSD_{L,}$ and the next four bits to be taken from the

It can be seen that the values obtained in the simulation result and the figure depicting the hardware verification are the same. In both cases, XC_Out1 and XC_Out2 hold up the value 5A3C and 1E5A, respectively. Here, only MSB bits are taken into consideration for verifying the output of Modified Pad-Gen TRMA using the MOD method on-chip scope pro-tool.

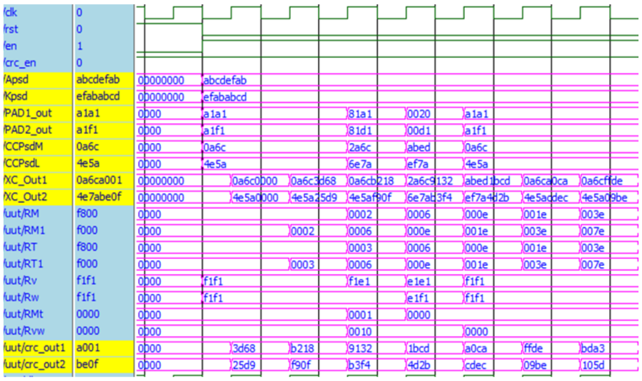
/clk 0
/rst 0
/en 1
/crc_en 0
/Apsd abcdefab 00000000 abcdefab
/Kpsd efababcd 00000000 efababcd
/PAD1_out a1a1 0000 a1a1 81a1 0020 a1a1
/PAD2_out a1f1 0000 a1f1 81d1 00d1 a1f1
/CCPsdM 0a6c 0000 0a6c 2a6c abed 0a6c
/CCPsdL 4e5a 0000 4e5a 6e7a ef7a 4e5a
/XC_Out1 0a6ca001 00000000 0a6c0000 0a6c3d68 0a6cb218 2a6c9132 abed1bcd 0a6ca0ca 0a6cffde
/XC_Out2 4e7abe0f 00000000 4e5a0000 4e5a25d9 4e5af90f 6e7ab3f4 ef7a4d2b 4e5acdec 4e5a09be
/uut/RM f800 0000 0002 0006 000e 001e 003e
/uut/RM1 f000 0000 0002 0006 000e 001e 003e 007e
/uut/RT f800 0000 0003 0006 000e 001e 003e
/uut/RT1 f000 0000 0003 0006 000e 001e 003e 007e
/uut/Rv f1f1 0000 f1f1 f1e1 e1e1 f1f1
/uut/Rw f1f1 0000 f1f1 e1f1 f1f1
/uut/RMt 0000 0000 0001 0000
/uut/Rvw 0000 0000 0010 0000
/uut/crc_out1 a001 0000 3d68 b218 9132 1bcd a0ca ffde bda3
/uut/crc_out2 be0f 0000 25d9 f90f b3f4 4d2b cdec 09be 105d

Fig. 3. Simulation Results of TRMA Protocol using XOR Method.

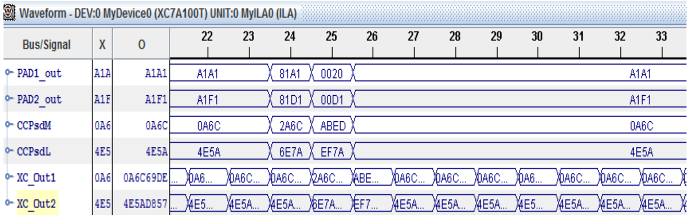
Waveform - DEV:0 MyDevice0 (XC7A100T) UNIT:0 MyILA0 (ILA)
Bus/Signal
X
O
22 23 24 25 26 27 28 29 30 31 32 33
PAD1_out A1A A1A1 A1A1 81A1 0020 A1A1
PAD2_out A1F A1F1 A1F1 81D1 00D1 A1F1
CCPsdM 0A6 0A6C 0A6C 2A6C ABED 0A6C
CCPsdL 4E5 4E5A 4E5A 6E7A EF7A 4E5A
XC_Out1 0A6 0A6C69DE 0A6... 0A6C... 0A6C... 2A6C... ABE... 0A6C... 0A6C... 0A6C... 0A6... 0A6C... 0A6C... 0A6C...
XC_Out2 4E5 4E5AD857 4E5... 4E5A... 4E5A... 6E7A... EF7... 4E5A... 4E5A... 4E5A... 4E5... 4E5A... 4E5A... 4E5A...

Fig. 4. Chip Scope Verified Results of Modified Pad-Gen Design using the XOR Method.

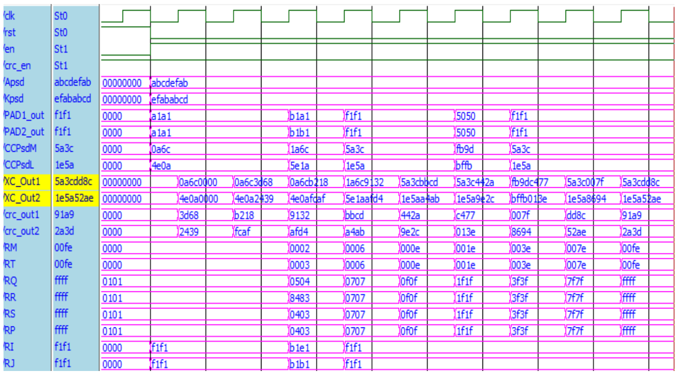
/clk St0
/rst St0
/en St1
/crc_en St1
/Apsd abcdefab 00000000 abcdefab
/Kpsd efababcd 00000000 efababcd
/PAD1_out f1f1 0000 a1a1 b1a1 f1f1 5050 f1f1
/PAD2_out f1f1 0000 a1a1 b1b1 f1f1 5050 f1f1
/CCPsdM 5a3c 0000 0a6c 1a6c 5a3c fb9d 5a3c
/CCPsdL 1e5a 0000 4e0a 5e1a 1e5a bffb 1e5a
/XC_Out1 5a3cdd8c 00000000 0a6c0000 0a6c3d68 0a6cb218 1a6c9132 5a3cbbcd 5a3c442a fb9dc477 5a3c007f 5a3cdd8c
/XC_Out2 1e5a52ae 00000000 4e0a0000 4e0a2439 4e0afcaf 5e1aafd4 1e5aa4ab 1e5a9e2c bffb013e 1e5a8694 1e5a52ae
/crc_out1 91a9 0000 3d68 b218 9132 bbcd 442a c477 007f dd8c 91a9
/crc_out2 2a3d 0000 2439 fcaf afd4 a4ab 9e2c 013e 8694 52ae 2a3d
/RM 00fe 0000 0002 0006 000e 001e 003e 007e 00fe
/RT 00fe 0000 0003 0006 000e 001e 003e 007e 00fe
/RQ ffff 0101 0504 0707 0f0f 1f1f 3f3f 7f7f ffff
/RR ffff 0101 8483 0707 0f0f 1f1f 3f3f 7f7f ffff
/RS ffff 0101 0403 0707 0f0f 1f1f 3f3f 7f7f ffff
/RP ffff 0101 0403 0707 0f0f 1f1f 3f3f 7f7f ffff
/RI f1f1 0000 f1f1 b1e1 f1f1
/RJ f1f1 0000 f1f1 b1b1 f1f1

Fig. 5. Simulation Results of TRMA Protocol using MOD Method.

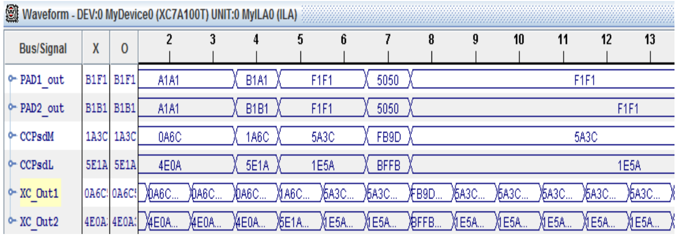
Waveform - DEV:0 MyDevice0 (XC7A100T) UNIT:0 MyILA0 (ILA)
Bus/Signal
X
0
2 3 4 5 6 7 8 9 10 11 12 13
PAD1_out B1F1 B1F1 A1A1 B1A1 F1F1 5050 F1F1
PAD2_out B1B1 B1B1 A1A1 B1B1 F1F1 5050 F1F1
CCPsdM 1A3C 1A3C 0A6C 1A6C 5A3C FB9D 5A3C
CCPsdL 5E1A 5E1A 4E0A 5E1A 1E5A BFFB 1E5A
XC_Out1 0A6C 0A6C 0A6C... 0A6C... 0A6C... 1A6C... 5A3C... 5A3C... FB9D... 5A3C... 5A3C... 5A3C... 5A3C... 5A3C...
XC_Out2 4E0A 4E0A 4E0A... 4E0A... 4E0A... 5E1A... 1E5A... 1E5A... BFFB... 1E5A... 1E5A... 1E5A... 1E5A... 1E5A...

Fig. 6. Chip Scope Verified Results of Modified Pad-Gen Design using MOD Method.

VI. Performance Analysis

On comparing the performance of the performance parameter for both XOR and MOD schemes, it was observed that the XOR method yielded better outcomes. Metrics such as the Number of slice registers, LUT-FF pairs were found to be approximately the same in both ways.

In the case of the Number of Slice LUTs, a huge variation is seen. In the XOR method, it is found to be 172 operating at a maximum frequency of 262.158MHz. For the MOD method, the number increased to 227, operating at a reduced frequency value of 222.408 MHz. On the whole, with the observation made using all the performance metrics, it can be concluded that the XOR method exhibits better performance illustrated in Fig. 7.

Fig. 8 and 9 show the comparative analysis of power and Area parameters between the XOR and MOD methods, respectively. Fig. 8 highlighting the graph of total power versus operating frequency for XOR, and the method indicates that the XOR method consumes less power when compared to the MOD method. Hence this enables the XOR method to be a more suitable approach for the mutual authentication process of the tag and reader.

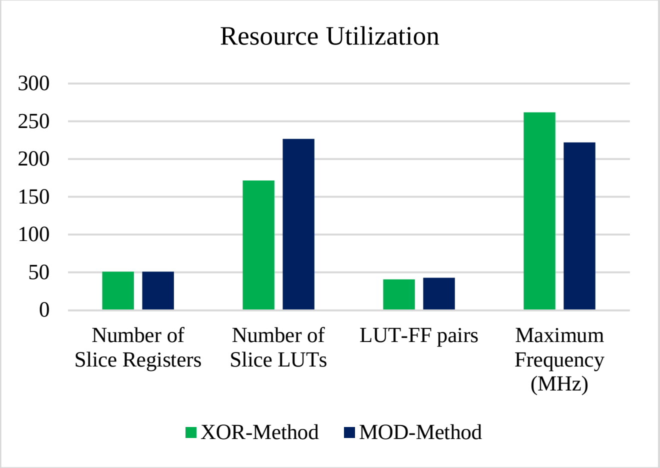

Fig. 7. Comparative Performance Analysis between XOR and MOD Method.

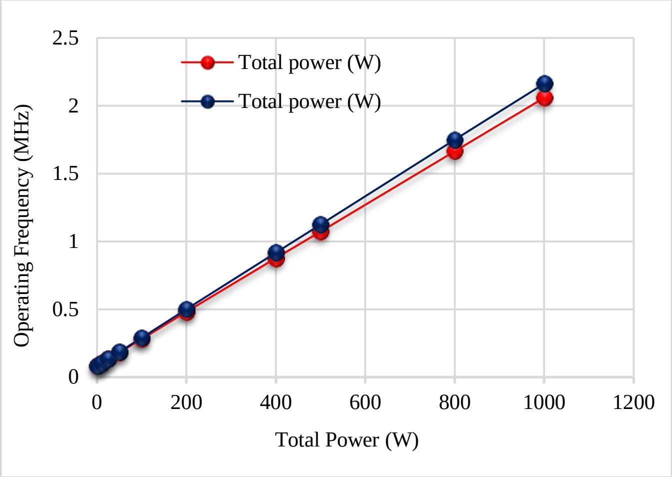

Fig. 8. Comparative Power Analysis between XOR and MOD Method.

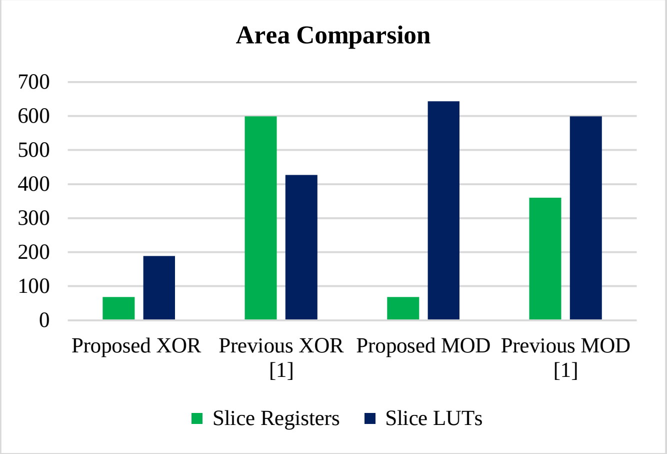

Fig. 9. Comparative Area Analysis between Proposed and Previous XOR and MOD Schemes.

The comparative analysis of the proposed and previous approach of XOR and MOD schemes are illustrated in Fig. 9. The graph foregrounds the count of slice registers and LUTs respective to both the methods. The number of slice registers and slice LUTs was found to be 68 and 189 for the proposed XOR operation of the mutual authentication protocol, respectively. That for the previous XOR approach was seen to be 599 and 427. For the proposed MOD operation, the number of slice registers and slice LUTs was 64 and 643, whereas in the case of the previous approach was found to be 360 and 599, respectively. Out of all the approaches investigated, it was seen that the proposed XOR method consumes the least power with an optimized area, utilizing fewer performance metrics and hence is an efficient way to establish mutual authentication among the tag and reader of the RFID system.

VII. Conclusion

To ensure the protection of the user's data privacy, a mutual authentication mechanism based on the modified Pad-Gen function is proposed in this paper. On comparing both the implementation methods, i.e., the XOR operation and MOD operation, it was seen that when mutual authentication is performed using XOR operation, enhanced performance metrics are yielded. The proposed design is capable of eliminating the security and privacy attacks concerns in the EPC-C1G2 authentication standard. Simulation outcomes were obtained on the cost-effective Artix-7 FPGAdevice XC7A100T-3CSG324. Physical verification of the resultant was confirmed on the Chipscope pro tool. CRC inclusion in the framework provides a security shield for the next level of operation in RFID tags. In future, incorporate the proposed work for real time NFC applications.

References

[1] Huang, Yu-Jung, Wei-Cheng Lin, and Hung-Lin Li. "Efficient implementation of RFID mutual authentication protocol." IEEE transactions on industrial electronics 59.12 (2012): 4784-4791.

[2] Korkmaz, Evsen, and Alp Ustundag. "Standards, security & privacy issues about radio frequency identification (RFID)." RFID Eurasia, 2007 1st Annual. IEEE, 2007.

[3] Chen, Chin-Ling, and Yong-Yuan Deng. "Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection." Engineering Applications of Artificial Intelligence 22.8 (2009): 1284-1291.

[4] Peris-Lopez, Pedro, et al. "EMAP: An efficient mutual-authentication protocol for low-cost RFID tags."OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer, Berlin, Heidelberg, 2006.

[5] Yeh, Tzu-Chang, et al. "Securing rfid systems conforming to epc class 1 generation 2 standard." Expert Systems with Applications 37.12 (2010): 7678-7683.

[6] Kardas, Suleyman, et al. "Cryptanalysis of lightweight mutual authentication and ownership transfer for RFID systems." Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 2011 Workshop on. IEEE, 2011.

[7] Lee, Young Sil, et al. "RFID mutual authentication protocol with unclonable RFID-tags." Mobile IT Convergence (ICMIC), 2011 International Conference on. IEEE, 2011.

[8] Yeh, Tzu-Chang, et al. "Securing rfid systems conforming to epc class 1 generation 2 standard." Expert Systems with Applications 37.12 (2010): 7678-7683.

[9] Chen, Yalin, Jue-Sam Chou, and Hung-Min Sun. "A novel mutual authentication scheme based on quadratic residues for RFID systems." Computer Networks 52.12 (2008): 2373-2380.

[10] Kulseng, Lars, et al. "Lightweight mutual authentication and ownership transfer for RFID systems." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.

[11] Rofougaran, Ahmadreza Reza. "Radio frequency identification (RFID) carrier and system." U.S. Patent Application No. 11/527,085.

[12] Mu, Haibing, and Zhenlong Zheng. "A dynamic key authentication protocol for RFID system." International Journal of Mobile Network Design and Innovation 7.3-4 (2017): 210-215.

[13] Sadaiyappan, T., K. K. Manoj, and S. A. Subhasakthe. "FPGA Implementation of Mutual Authentication Protocol Using Modular Arithmetic." (2014).

[14] Mohanavelu, S., and T. Ramya. "Secured Authentication Protocol for RFID System Using XOR Scheme."

[15] Beuchat, J-L. "Some modular adders and multipliers for field programmable gate arrays." Parallel and Distributed Processing Symposium, 2003. Proceedings. International. IEEE, 2003.

[16] Sarma, Sanjay E., Stephen A. Weis, and Daniel W. Engels. "RFID systems and security and privacy implications." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2002.

[17] Yuan, Ching-Chien, et al. "The design of encoding architecture for UHF RFID applications." Microwave Conference, 2008. APMC 2008. Asia-Pacific. IEEE, 2008.

[18] Avoine, Gildas, and Philippe Oechslin. "A scalable and provably secure hash-based RFID protocol." Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on. IEEE, 2005.

[19] Kim, Do-Yun, et al. "Effects of reader-to-reader interference on the UHF RFID interrogation range." IEEE Transactions on Industrial Electronics 56.7 (2009): 2337-2346.

[20] Peris-Lopez, Pedro, et al. "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags." Proc. of 2nd Workshop on RFID Security. 2006.

[21] Garfinkel, Simson L., Ari Juels, and Ravikanth Pappu. "RFID privacy: An overview of problems and proposed solutions." IEEE Security & Privacy 3.3 (2005): 34-43.

[22] Bogdanov, Andrey, et al. "Hash functions and RFID tags: Mind the gap." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2008.

[23] Want, Roy. "Enabling ubiquitous sensing with RFID." Computer 37.4 (2004): 84-86.

[24] Thiesse, Frédéric, et al. "Technology, standards, and real-world deployments of the EPC network." IEEE Internet Computing 13.2 (2009): 36-43.

[25] Eom, Jun-Bong, Soon-Bin Yim, and Tae-Jin Lee. "An efficient reader anticollision algorithm in dense RFID networks with mobile RFID readers." IEEE Transactions on industrial electronics 56.7 (2009): 2326-2336.

[26] Peris-Lopez, Pedro, et al. "RFID systems: A survey on security threats and proposed solutions." IFIP international conference on personal wireless communications. Springer, Berlin, Heidelberg, 2006.

[27] Sun, Hung-Min, and Wei-Chih Ting. "A Gen2-based RFID authentication protocol for security and privacy." IEEE Transactions on Mobile Computing 8.8 (2009): 1052-1062.

[28] Peris-Lopez, Pedro, Tong-Lee Lim, and Tieyan Li. "Providing stronger authentication at a low cost to RFID tags operating under the EPCglobal framework." Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on. Vol. 2. IEEE, 2008.

[29] Konidala, Divyan M., and Kwangjo Kim. "RFID tag-reader mutual authentication scheme utilizing tag’s access password." Auto-ID Labs White Paper WP-HARDWARE-033(2007).

[30] Han, Soonshin, HyungSoo Lim, and JangMyung Lee. "An efficient localization scheme for a differential-driving mobile robot based on RFID system." IEEE Transactions on Industrial Electronics 54.6 (2007): 3362-3369.

[31] Juels, Ari. "RFID security and privacy: A research survey." IEEE journal on selected areas in communications 24.2 (2006): 381-394.

[32] Lee, Jong-Wook, et al. "A Fully Integrated HF-Band Passive RFID Tag IC Using 0.18-$\mu\hbox {m} $ CMOS Technology for Low-Cost Security Applications." IEEE Transactions on Industrial Electronics 58.6 (2011): 2531-2540.

[33] Eisenbarth, Thomas, and Sandeep Kumar. "A survey of lightweight-cryptography implementations." IEEE Design & Test of Computers 24.6 (2007).

[34] Piramuthu, Selwyn. "Protocols for RFID tag/reader authentication." Decision Support Systems 43.3 (2007): 897-914.

[35] Anusha, R. "Qualitative Assessment on Effectiveness of Security Approaches towards safeguarding NFC Devices & Services." International Journal of Electrical and Computer Engineering 8, no. 2 (2018): 1214.

[36] Anusha, R., and V. Veena Devi Shastrimath. "TRMA: An Efficient Approach for Mutual Authentication of RFID Wireless Systems." In Computer Science On-line Conference, pp. 290-299. Springer, Cham, 2018.

[37] Anusha, R., and V. Veena Devi Shastrimath. "LCBC-XTEA: High Throughput Lightweight Cryptographic Block Cipher Model for Low-Cost RFID Systems." In Computer Science On-line Conference, pp. 185-196. Springer, Cham, 2019.