ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

Implementation of RFID Tag-Reader Mutual Authentication Protocol

Anju Jagadeesh

Abstract*— Radio frequency identification (RFID) is a recent technology that utilizes radio frequencies to track the object by transmitting a signal with a unique serial identity. Generally, the drawbacks of RFID technology are high cost and weak authentication systems between the reader and tag. In this paper, RFID mutual authentication protocol using Padgen function and truncated multiplier were proposed and data encoding architectures are studied Truncated multipliers are implemented in RFID tag–reader mutual authentication protocol system due to reduction in hardware cost and dynamic power. Experimental evaluation reveals that the proposed protocol with truncated multipliers provides more security. The proposed systems are simulated using Modelsim 6.3f. The system has been successfully implemented in hardware using Spartan 3e field-programmable gate array (FPGA).

***Index Terms*— Field-programmable gate array (FPGA) implementation, mutual authentication, radio-frequency identification (RFID), linear feedback shift register, truncated multiplier.**

I. INTRODUCTION

An RFID tag stores the information electronically which can be read from several meters away without having contact between tag and reader. Tag consists of an integrated circuit for handling data and an antenna for receiving and transmitting a radio frequency signal. The RFID system utilizes one of three general band's low frequency (LF) at 125 kHz to 134 kHz, high frequency (HF) at 13.56MHz, and Ultra HF at 860MHz to 930MHz [1, 2]. RFID tags contain a unique serial number namely electronic product code (EPC) that can individually identify every single tagged item [3, 4]. Electronic product Code Class1 generation2 (EPCC1G2) provides only very basic security tools using a 16bits pseudo random number generator (PRNG) [5]. The LFSR can be created using the Galois or Fibonacci configuration of gates and registers. Fibonacci implementation, the output from some of the registers is EX-ORed with each other and feedback to the input of the shift register. Fibonacci LFSR is more suitable for hardware implementation than the Galios LFSR [6–8]. A light authentication protocols that use only efficient bitwise operations (such as EX-OR, AND, OR, addition etc.) on tags have been defined in [9].

RFID standards are a major issue in securing high investments in RFID technology on different levels (e.g., interface protocol, data structure, etc.). There are two competing initiatives in the RFID standardization arena: ISO [5] and EPC Global [4], [6]. The EPCglobal Class-1 Generation-2 (C1G2) ultrahigh 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 960 MHz). The standard specifies that a compliant RFID tag should contain a 32-b kill password (Kpwd) to permanently disable the tag and a 32-b access password (Apwd). The reader then performs a bitwise XOR of the data or password with a random number from the tag to cover-code data or a password in EPC Gen 2. However, the EPC C1G2 standards do not fully support privacy invasion and data security issues. The simple kill and access commands specified in EPC C1G2 specifications are not enough to provide secure authentication function and data/privacy protection.

EPC C1G2 provides only very basic security tools using a 16-b pseudorandom number generator (PRNG) and a 16-b cyclic redundancy code (CRC). Konidala et al. [10] proposed a protocol based on XOR operation and tag's access and kill passwords for the tag–reader mutual authentication scheme. However, this approach has not been implemented in hardware. In this paper truncated multiplier is used to encode the information during a mutual authentication process, it reduces the hardware cost, strengthening security and consumes less power to perform this multiplication. In addition to that, number of bit processing is fewer which lead to reduction in the bit length and their no possibility of finding the information by performing backward processing. The rest of this paper is organized as follows. In Section 2, the back ground and its related work on the RFID reader-to-tag authentication protocol are explained. The Design and implementation is discussed in Section 3. Section 4 shows the simulation and implementation results of the mutual authentication scheme. Finally, conclude the paper in Section 5.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

II. BACK GROUND AND RELATED WORKS

RFID systems work, whenever a reader antenna emits a radio frequency signal. Tag pick up that radio signal and respond to a reader. Reader reads the signal which is responded by tag. The reader is act as a transceiver (i.e., a combination of transmitter and receiver) because their usual role is to request a tag and receive information from tag. The antenna can be a separate device, or it can be an integrated within a reader [1].

A. EPC class-1 generation-2 Standard

The access password is a 32-bit value stored in the tag's reserved memory if this password is set, then data transfer will be established between tag and reader. Initially reader requests a random number from the tag. Tag generates a random number and sends to reader. The reader cover codes the password by performing a bitwise EX-OR between password and random number. The generated EX-OR output is transmits to the tag. The tag decodes the coded password by performing a bitwise EX-OR of the received cover-coded string with the original as shown in Fig. 1.In this scheme, both the random number sends un-encrypted form. Man in middle attack is possible to happen by carrying out EX-OR operation between the cover coded passwords with random number, which provides access password and their by malicious reader to illegally access the tag's data [12].

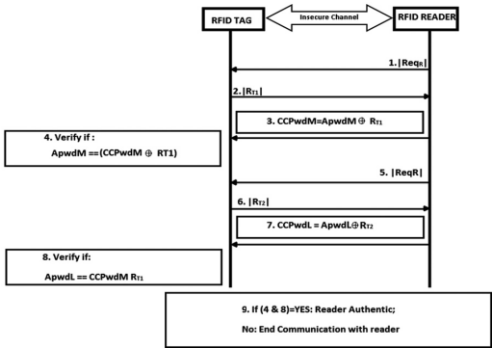

Fig. 1 Authentication scheme proposed by EPC global in [12]

B. Konidala Mutual Authentication Scheme

Konidala et al [12] proposed a scheme where the server, reader, and the tag follow a multi-step tag–reader mutual authentication procedure as shown in Fig.2. It uses the tag's 32bit access and kill passwords in order to perform tag–reader mutual authentication. This protocol uses two rounds of Pad generation function (Padgen) to compute a cover-coding pad. The first round of Padgen function performs over the access password, while the second round of Padgen function performs over the kill password. The Padgen function is used to generate a 16bit pads for "cover coding" the access password.

In this scheme, as shown in Fig. 2, the reader issues a Req_RN command to the acknowledged tag. The tag then generates two16-brandom numbers, namely, RT1 and RT2, and backscatters them with its EPC to the reader. The reader forwards these messages to the manufacturer. The manufacturer matches the received EPC to retrieve the tag's access password (Apwd) and kill password (Kpwd) from the back-end database. The manufacturer then generates and stores two 16-b random numbers, namely, RM1 and RM2. The "cover-coded passwords" for the 16 MSBs (CCPwdM1) and the 16 LSBs (CCPwdL1) are computed by the PadGen (RTi, RMi) function for i = 1, 2. CCPwdM1, CCPwdL1, and EPC along with four 16-b 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. To authenticate the tag, the tag generates another two random numbers RT3 and RT4 along with the received RM3 and RM4 used to compute CCPwdM2 and CCPwdL2 with the PadGen (RTi,RMi) function for i = 3, 4. CCPwdM2, CCPwdL2, and EPC along with two 16-b random numbers, namely, RT3 and RT4, are transmitted to the reader, which, in turn, forwards them to the manufacturer for verification. The Konidala et al. scheme offers greater resistance against Lim and Li's attacks [12]. This scheme is also much more difficult for an adversary to recover the access password under the correlation attack or to forge successful authentication under the dictionary attack.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

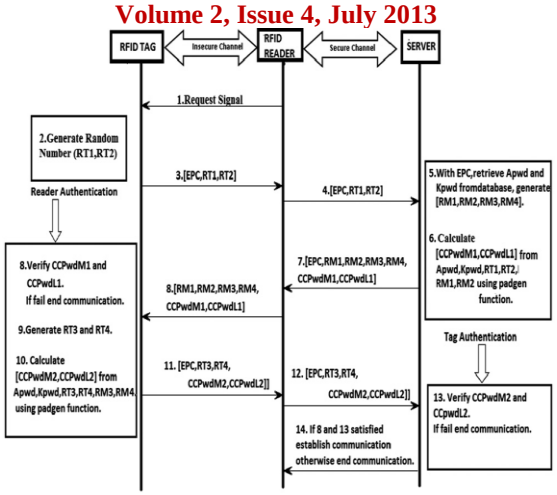

Fig. 2 Konidala tag–reader mutual authentication scheme

C. Truncated multiplier as encrypter

The protocol consists of three main component's tag, reader and server or database. In the proposed protocol, each tag has an individual EPC, Password (PWD) and a common architecture (truncated multiplier function) provided by manufacturer to encrypt PWD. The data base has the information about EPC and PWD of all tags. It also has a common protocol architecture which is embedded in all tags.

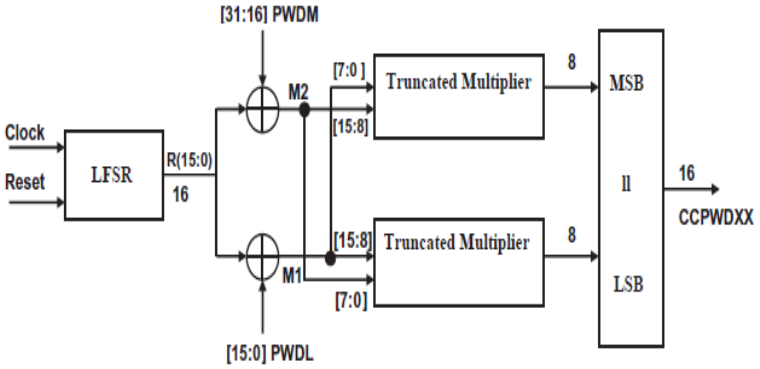

Fig.3 Functional block diagram in the mutual authentication scheme

A standard digital n–x–n multiplier computes the 2n bit product, but truncated multipliers compute only n most significant bits (MSBs) of the 2n bit product. Many researchers have been made to design a truncated multiplier [18]. Hars [22] is the first author who describes the truncated multiplier can be used for cryptographic applications. Each author can design their own truncated multiplier architecture according to their requirements, but the final output results of the truncated multiplier vary with respect to the architecture. The behaviour of truncated multiplier converts a data of n bit into some other n bit data. Hence it is used to encrypt the data send from tag to reader and vice versa. To justify the above statement, let us consider the inputs a and b for truncated multiplier where a=00011011(27), b=00011011(27). When the input is processed in truncated multiplier, actual output of standard multiplier is 0000001011011001(729), but it produces an error output as 0000001100000000(768) according to the architecture. This result shows that the truncated multiplier converts the input value from one form to some other form. Hence it can be used to encode the password. If anyone tapped the information they can able to get the encoded bits. These bits are not possible to retrieve the information until they know the architecture of truncated multiplier. The reasons behind for choosing truncated multiplier in this protocol is that it provides an efficient method for reducing the hardware cost compare to Padgen function, avoids grow thin word-size and also used as an encoder. In the protocol the efficient truncated multiplier architecture which is recently proposed by Ko and Hsiao [18] is used for encrypt the password.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

III. DESIGN AND IMPLEMENTATION

A. *Data Encoding Architecture*

According to the EPC C1G2 protocol, a tag communicates with an interrogator using backscatter modulation, in which the tag switches the reflection coefficient of its antenna between two states in accordance with the data being sent. These two kinds of encoding architectures, FM0 and Miller-modulated subcarrier (MMS), are verified.

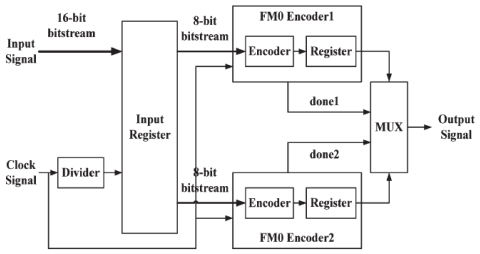

Fig.4 FM0 Data Encoding Architecture

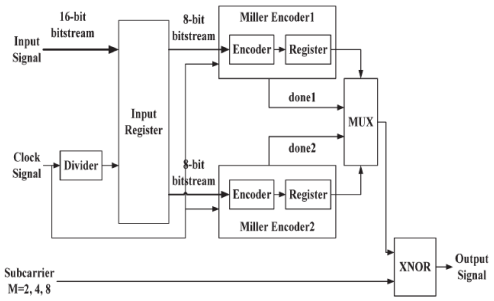

Fig. 5 MMS Data Encoding Architecture

A detailed definition of FM0 and MMS is described in [24]. The following is a brief definition of FM0 and MMS. A binary "1" is constant during a symbol time, and a binary "0" has a state transition in the middle of a symbol, or the FM0 symbol can, in turn, be XOR ed with square waves of up to eight times higher in frequency to form an MMS. In addition, baseband Miller inverts the baseband value between adjacent binary values of zero. Finally, the resulting waveform is multiplied by a square wave of *M* subcarrier cycles per bit, where *M* is equal to two, four, or eight. The design of the FM0 encoding architecture is shown in Fig. 4. The frequency divider divides the original clock signal frequency by two and is processed as a clock signal to trigger the first register. The encoder is triggered by the original clock signal. The first input register is used to save the input data for further encoding processes. The encoded information will be stored in the register and will output the final results in sequence. The coding structure of MMS is similar to that of FM0. Fig. 5 shows the MMS coding architecture. The frequency divider divides the original clock signal to trigger the first register that stores the input data. The original clock is applied to the encoder as a trigger signal. The encoding result is bit wised with a subcarrier through the XNOR gate.

B. PadGen Mutual Authentication Architecture

The PadGen function is the key function used to produce a cover-coding pad to mask the tag's access password before transmission. The implementation of the PadGen function also requires the random number generator to produce RTx and RMx. A typical 16-b linear feedback shift register (LFSR) is used to generate pseudorandom numbers. An LFSR with a well-chosen feedback function can produce a sequence of bits that appears random and has a very long cycle. For an n-bit LFSR, the LFSR can generate a $(2n - 1)$-b-long pseudorandom sequence before repeating. A maximum length LFSR produces an m-sequence (i.e., cycles through all possible $2n - 1$ states within the shift register except the state where all bits are zero). However, an LFSR with a maximal period must satisfy the following property: The polynomial formed from a tap sequence plus the constant 1 must be a primitive polynomial modulo 2. In this paper, the Fibonacci LFSR was implemented because it is more suitable for hardware

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

implementation than the Galios LFSR. The feedback polynomial is $x^{16}+ x^{14} +x^{13} + x^{11} + 1$. The architecture of the 16-b random number generator is shown in Fig. 6.

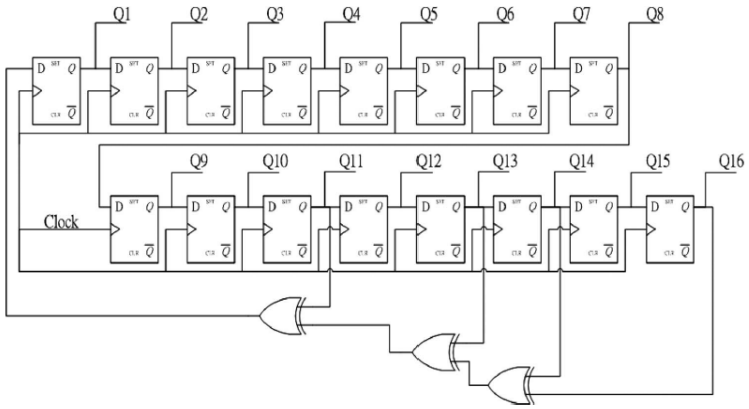

Fig. 6 Functional block diagram of 16-b random number generator

The block diagram of the PadGen function in the mutual authentication scheme is shown in Fig. 7. The function is performed on the tag's 32-b access password Apwd = a0a1a2a3 . . . a31, which is broken up into two parts—the 16 MSBs of the access password as ApwdM and the 16 LSBs denoted as ApwdL. The hexadecimal (base 16) notation of the 16-b random numbers RTx and RMx generated by the tag and manufacturer are expressed as RTx = dt1dt2dt3dt4 and RMx = dm1 dm2 dm3 dm4, respectively. Using each of the four hexadecimal digits in RTx (or RMx) to indicate a bit address within ApwdM or ApwdL, PadGen then selects those bits from ApwdM and ApwdL to form the 16-b output pad. The resulting output dv1dv2dv3dv4 together with RTx will then perform PadGen over the 32-b kill password Kpwd (k0k1k2k3 . . . k31) to form the 16-b output pad PADx.

PADx= Kpwd − PadGen (Apwd PadGen (RTx, RMx), RTx). (1)

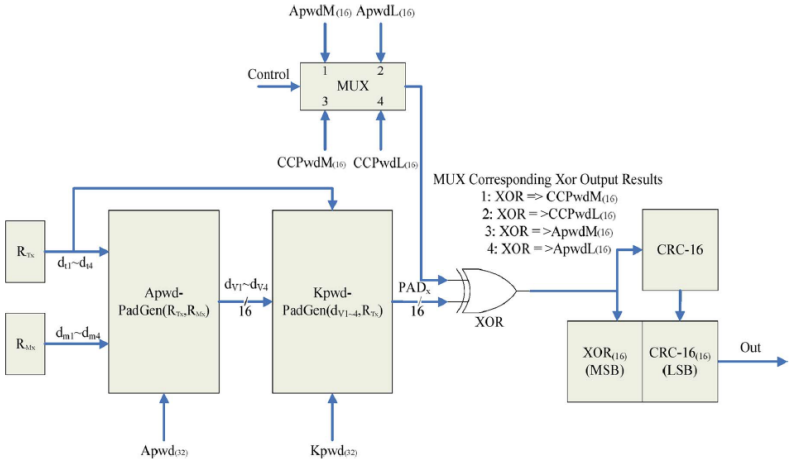

Fig. 7 PadGen functional block diagram in the mutual authentication scheme.

A multiplexer was utilized to allow for the selection of ApwdM, ApwdL, CCPwdL, or CCPwdM. The multiplexer then can perform the XOR operation to obtain the following cover-coded passwords or the access password for mutual authentication:

CCPwdM1 =ApwdM *XOR* PAD1
CCPwdL1 =ApwdL *XOR* PAD2

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

ApwdM =CCPwdM2 *XOR* PAD3
ApwdL =CPwdL2 *XOR* PAD4. (2)

The CRC function is implemented to protect and calibrate the commands/messages transmitted between tags and readers. The generator polynomials used to implement the CRC is

$$g(x) = x^{16} + x^{15} + x^2 + 1 = (x + 1)(x^{15} + x + 1). \quad (3)$$

IV. SIMULATIONS AND IMPLEMENTATION RESULTS

Simulations of the designs are implemented in a Spartan 3 FPGA. The simulation results of the PadGen function, as described in (7), are shown in Fig. 8. The two random numbers RTx = 6B79 and RMx = 06C0 were generated by the random number generator. The calculated PAD1 was equal to 88A8. For ApwdM = ABCD (hex), CCPwdM1 was calculated from APwdM xor PAD1 = 2365(hex), and the resulting CRC-16 code = 4B5D (hex). The simulation results of the final output are 23654B5D (hex), as shown in Fig. 8.Simulation results of FM0 and MMS data encoding architectures are shown in Fig 9 and 10.Simulation result of the proposed protocol using truncated multiplier is shown in Fig 11.

A. Simulation Results

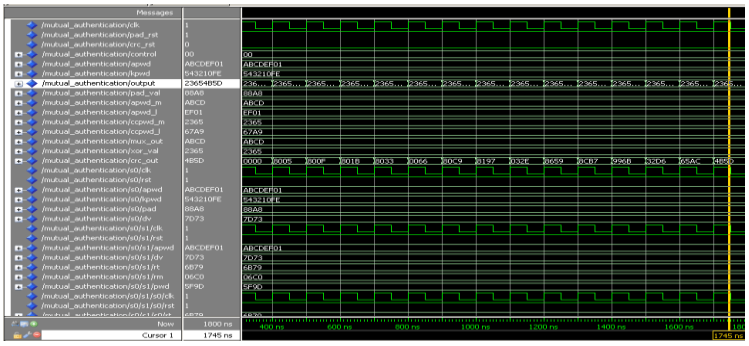

Fig. 8 Simulation Results of the PadGen Function (Fig 7).

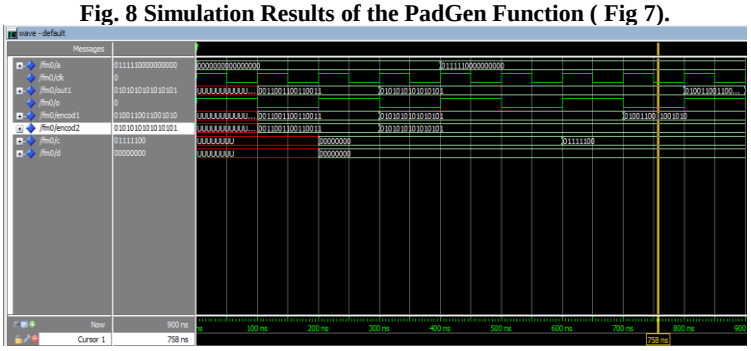

Fig.9 Simulation result of FM0 Data Encoding Architecture

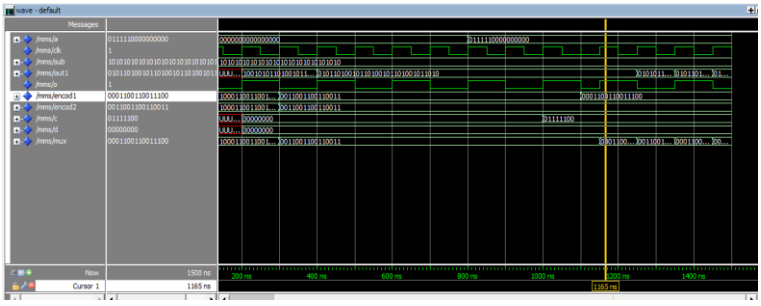

Fig.10 Simulation result of MMS Data Encoding Architecture

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

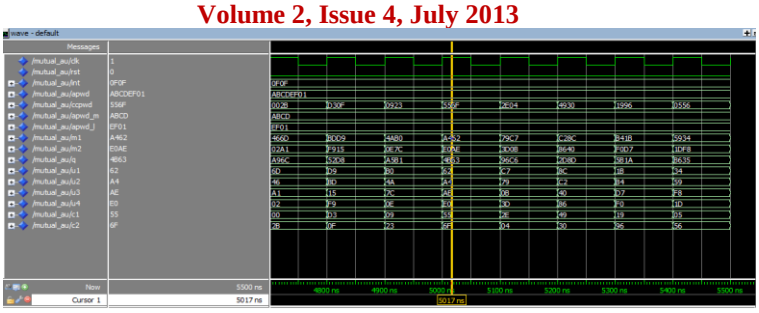

Fig.11 Simulation result of mutual authentication scheme in which truncated multiplier as encrypter

B. Comparison

	PadGen mutual authentication architecture	Proposed architecture using truncated multiplier
power	0.260W	0.227W
Delay	10.516ns	2.879ns

V. CONCLUSION

In this paper, the functionality of the MMS and FM0 designs were verified using the vhdl hardware description language. An efficient RFID mutual authentication protocol using Padgen function and truncated multiplier were proposed and their functionality is also verified using the VHSIC hardware description language. The PadGen architecture performs the PadGen function and tag's access and kill passwords in achieving tag–reader mutual authentication. Truncated multiplier functions were examined for the tag–reader mutual authentication protocol in the RFID system environment. The proposed scheme is feasible in improving the weakness of the EPC global C1G2 communication authentication scheme. The hardware implementation of proposed RFID tag–reader mutual authentication protocol has been done on Spartan 3 FPGA board and simulation counterparts using Modelsim 6.3f

ACKNOWLEDGMENT

The author extends sincere thanks to all staff members of Mangalam College of Engineering, Kerala, India for their timely help and encouragement.

REFERENCES

[1] Frank Thronton, Brad Haines, Anita Campbell, RFID security, Syngress Publishing, Inc, 2006.

[2] S. Han, H.Lim, J.Lee, An efficient localization scheme for a differential-driving mobile robot based on RFID system, IEEE Transactions on Industrial Electrons 53 (5)(2007)3362–3369.

[3] Class1Generation2UHFAirInterfaceProtocolStandard, ⟨ http://www. Epcglobalinc.org/standards.

[4] Radio Frequency Identification for Item Management, 2nd ed. ISO/IEC18000, (2008).

[5] Ver.1.0.9EPCglobal Ratified Standard, EPC Radio-Frequency Identity Protocols Class-1 Generation-2UHF RFID Protocol for Communications at 860–960 MHz, ⟨ http://www.epcglobalinc.org/standards.

[6] Mark Goresky, Andrew M.Klapper, Fibonacci and galois representations of feedback-with-carry shift registers,IEEE Transactions on Information Theory 48(11)(2002)2826–2836.

[7] P.K. Lala, Digital Circuit Testing and Testability, Academic Press, 2002.

[8] P.Peris-Lopez, J.C.Hernandez-Castro, J.M.Estevez-Tapiador, A.Ribagorda, LMAP: a real light weight mutual authentication protocol for low-cost RFID tags, in: Proceedings Second Workshop RFID Security,(2006),pp.1–12.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

[9] P.Peris-Lopez, J.C.Hernandez-Castro, J.M.Estevez-Tapiador, A.Ribagorda, EMAP: an efficient mutual authentication protocol for low cost RFID tags, in: Proceedings OTM Federated Conference and Workshop: IS Workshop, (2006).

[10] H.-Y.Chien, SASI:a new ultra light weight RFID authentication protocol providing strong authentication and strong integrity4(4)(2007)337–340.

[11] D.M.Konidala, Z.Kim, K.Kim, A simple and cost effective RFID tag–reader mutual authentication scheme, in: Proceedings International Conference on RFID Security,(2007),pp.141–152.

[12] P.Peris-Lopez,T.-L.Lim,T.Li,Providing stronger authentication at a low cost to RFID tags operating under the EPC global frame work, in: Proceedings IEEE/IFIP International ConferenceEUC,vol.2,Dec.17–20, (2008),pp.159–166.

[13] Yu-Jung Huang, Ching-ChienYuan,Ming-KunChen,Wei-ChengLin,Hsien- Chiao Teng,Hardware implementation of RFID mutual authentication protocol, IEEETransactions on Industrial Electronics57(5)(2010)1573–1582.

[14] Yu-Jung Huang, Wei-ChengLin, Hung-LinLi,Efficient implementation of RFID mutual authentication protocol, IEEE Transactions on Industrial Electronics (2011),Issue99.

[15] M.J.Schulte, J.G.Hansen, J.E.Stine, Reduced power dissipation through truncated multiplication, in: Proceedings IEEE Alessandro Volta Memorial International Workshop Low Power Design,(1999),pp.61–69.

[16] J.-P.Wang,S.-R.Kuang,S.-C.Liang,High-accuracy fixed-width modified booth multipliers for lossy applications, IEEE Transactions on Very Large Scale Integration(VLSI) System 19(1)(2011)52–60.

[17] Hou-Jen Ko,Shen-FuHsiao,Design and application of faithfully rounded and truncated multipliers with combined deletion, reduction, truncation, and rounding, IEEETransactionsonCircuitsandSystemsII:ExpressBriefs58(5) (2011)304–308.

[18] Selwyn Piramuthu, Protocols for RFID tag/reader authentication, Decision Support Systems43 (2007)897–914.

[19] Selwyn Piramuthu, RFID mutual authentication protocols, Decision Support Systems 50(2011)387–393.

[20] Jung-Sik Cho, Sang-SooYeo, SungKwon Kim, Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value, Computer Communications, 34,391–397, Elsevier.

[21] L.Hars,Fasttruncatedmultiplicationforcryptographicapplications,inProceedings of the Seventh International Workshop on Cryptographic Hardware and Embedded Systems(CHES ’05),of Lecture Notes in Computer Science, din-burgh,UK,vol.3659,(2005),pp.211–225.

[22] Ver. 1.0.9 EPCglobal Ratifed Standard, EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz [Online]. Available: http://www.epcglobalinc.org/standards.

[23] C.-C. Yuan, K.-H. Huang, H.-L. Li and Y.-J. Huang, “The design of encoding architecture for UHF RFID applications,” in Proc. Asia-Pacific Microw. Conf., Hong Kong, Dec. 16–19, 2008, pp. 1–4. DOI: 10.1109/ APMC.2008.4958410.

AUTHOR BIOGRAPHY

Anju Jagadeesh was born in Kottayam, Kerala, India**.** She has received the bachelor's degree in Electronics and Communication Engineering from M.G University Kerala,India in 2011 and currently she is doing Master's degree in VLSI and Embedded Systems from M.G University,Kerala,India.