Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.133 – 139

RESEARCH ARTICLE

FPGA Implementation of Mutual Authentication Protocol Using Modular Arithmetic

T.Sadaiyappan[1], K.K.Manoj[2], S.A.Subhasakthe[3]

[1]PG Scholar,VLSI Design & Bannari Amman Institute Of Technology, India

[2]PG Scholar, VLSI Design & Bannari Amman Institute Of Technology, India

[3]PG Scholar ,VLSI Design & Bannari Amman Institute Of Technology, India

[1] sadaiyappanece@gmail.com; [2] kkm.apt@gmail.com; [3] saktheanand@gmail.com

Abstract— Radio-Frequency Identification (RFID) is a modern technology that utilize radio frequencies to locate the object. In this paper, we study the radio-frequency identification (RFID) tag–reader mutual authentication (TRMA)scheme. Two improved authentication protocols for generating the Pad Gen function are described. In this project, a protocol for RFID tag–reader mutual authentication scheme is proposed which is hardware efficient. Modified MOD scheme is implemented in protocol system to reduce the hardware cost. The proposed mutual authentication protocol with consumes less logic elements and also more secure from external attacks. The proposed protocol is described in Verilog HDL and simulated using Xilinx ISE design suite 14.2.

Keywords— Radio frequency identification; mutual identification

I. INTRODUCTION

Radio-Frequency Identification (RFID) is the use of a wireless non-contact system that uses radio-frequency electromagnetic field to transfer data from a tag attached to an object, for the purposes of automatic identifying objects. The main components of RFID system is tag and reader . The tag is at the heart of the system and consists of a small electronic circuit with an attached silicon chip. A typical reader contains an antenna to transmit information to the tag as well as receive it from the tag. The size and form of the antenna will be dependent on the specific application as well as frequency chosen. RFID is a versatile technology, capable of being used by businesses and the government. For high security purpose, automobile industries like Toyota, Lexus and Audi uses a RFID based car locking system. Sports-using RFID tags to track marathon runners and other sports participants. Ticketing–RFID embedded tickets for major sporting events such as the Tennis.

In the commercial setting, RFID tags contains a Electronic Product Code (EPC) that can uniquely identify each tagged object. The RFID tag stores its unique EPC with related product information inside the tag's memory and sends these data whenever the reader requests them. The reader reads data from and writes data to tags by distributing the RF signals.

II. BACKGROUND AND RELATED WORK

Generally, in RFID system 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. These passwords can be used in activating kill commands to permanently shut down tags, as well as for accessing and relocking a tag's memory.

To codecover data or a password the reader first requests a random number from tag. The reader then performs a bitwise XOR of the data or password with this random number and transmits the cover-coded (also called cipher text) string to the tag. The tag uncovers the data or password by performing a bitwise XOR of the received cover-coded string with the original random number. In addition, the tag conforming to the EPC C1G2 standard can support only a 16-b PRNG and a 16-b CRC checksum that are used to detect errors in the transmitted data [2]. Fig. 1 describes the EPC global C1G2 communication step between a reader and a tag.

The EPC C1G2 specification provides little security [4], This makes RFID systems vulnerable to cloning attacks as well as password disclosure and information leakage [9]. Recently, Konidala *et al.* have pointed out the weakness in the EPCC1G2 reader-to-tag authentication protocol and proposed an alternative scheme. In the Konidala *et al.* [3] authentication scheme, as shown in Fig 3.1, the reader issues a Req_RN command to the acknowledged tag. The tag then generates two 16 bit random numbers, namely, R_{T1} and R_{T2}, 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 bit random numbers, namely, R_{M1} and R_{M2}. The "Cover-Coded Passwords" for the 16 MSBs (CCPwdM1) and the 16 LSBs (CCPwdL1) are computed by the Padgen (R_{Ti},R_{Mi}) function for i = 1, 2. CCPwdM1, CCPwdL1, and EPC along with four 16 bit random numbers, namely, R_{M1}, R_{M2}, R_{M3}, and R_{M4}, 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 R_{T3} and R_{T4} along with the received R_{M3} and R_{M4} used to compute CCPwdM2 and CCPwdL2 with the Padgen (R_{Ti},R_{Mi}) function for i = 3, 4. CCPwdM2, CCPwdL2, and EPC along with two 16 bit random numbers, namely, R_{T3} and R_{T4}, are transmitted to the reader, which, in turn, forwards them to the manufacturer for verification.

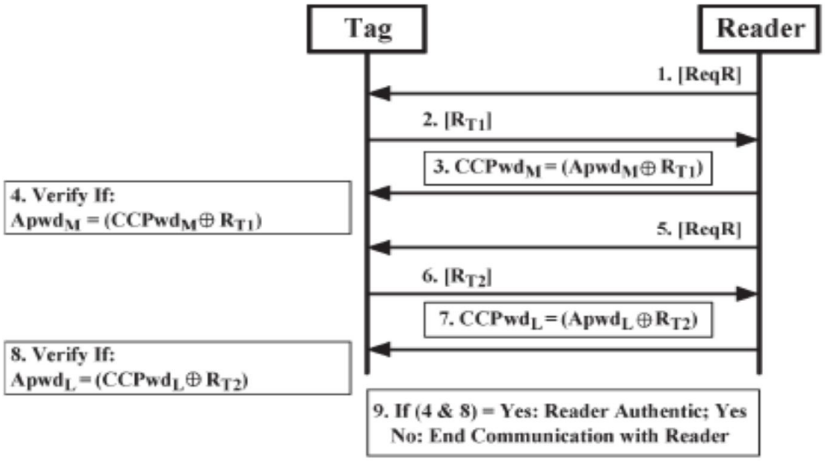

Fig 1. EPC global C1G2 communication step between a reader and a tag

Researchers have shown that the Electronic Product Code (EPC) Class-1 Generation-2 (C1G2) specification has serious security problems. To overcome these weaknesses, some authors have proposed a specially designed pad generation (Padgen) function to improve security. The Padgen function is used to produce a cover-coding pad to mask the tag's access password before the data is transmitted.

In [1], the Padgen function is the key component in constructing the 16 bit pads to cover code the two 16 bit Access Password halves (ApwdM and ApwdL). The pad-generation function retrieves the individual bits of the Apwd and Kpwd from the memory locations by manipulating random numbers and concatenates these bits to form a 16 bit pad. A brief description of the Padgen function is provided in the following. Let us represent the 32 bit Apwd and Kpwd in binary (base 2) as in equation (1) and (2).

$$Apwd = a_0a_1a_2a_3 \ldots\ldots..a_{31} \quad (1)$$

$$Kpwd = k_0k_1k_2k_3\ldots\ldots k_{31} \quad (2)$$

The 16 bit random numbers R_{Tx} and R_{Mx} generated by the tag and manufacturer in hexadecimal (base 16) are in equation (3) and (4)

$$R_{Tx}= d_{t1}d_{t2}d_{t3}d_{t4} \quad (3)$$

$$R_{Mx}= d_{m1}d_{m2}d_{m3}d_{m4} \quad (4)$$

Each digit of R_{Tx} and R_{Mx} is used to indicate a bit location in Apwd, and these bits are concatenated to form a 16 bit output in hexadecimal (base 16) representations as in equation (5).

Apwd –Padgen(R_{Tx} , R_{Mx})

$$= a_{dt1}a_{dt2}a_{dt3}a_{dt4} \,||\, a_{dt1+16}a_{dt2+16}a_{dt3+16}a_{dt4+16} \,||\, a_{dm1}a_{dm2}a_{dm3}a_{dm4} \,||\, a_{dm1+16}a_{dm2+16}a_{dm3+16}a_{dm4+16}$$
$$= d_{v1}d_{v2}d_{v3}d_{v4}$$
$$= R_v \quad (5)$$

The Padgen is again performed over Kpwd using the previously generated $d_{v1}d_{v2}d_{v3}d_{v4}$ to indicate a bit location in Kpwd, and these bits are concatenated to form a 16 bit PAD.

The resulting PAD would then be expressed as in equation (6).

Kpwd – Padgen ($d_{v1}d_{v2}d_{v3}d_{v4}$,R_{Tx})

$$= k_{dv1}k_{dv2}k_{dv3}k_{dv4} \,||\, k_{dv1+16}k_{dv2+16}k_{dv3+16}k_{dv4+16} \,||\, k_{dt1}k_{dt2}k_{dt3}k_{dt4} \,||\, k_{dt1+16}k_{dt2+16}k_{dt3+16}k_{dt4+16}$$
$$= h_{p1}h_{p2}h_{p3}h_{p4}$$
$$= \text{PAD} \quad (6)$$

Where $h_{p1}h_{p2}h_{p3}h_{p4}$ is the hexadecimal (base 16) notation.

$$\text{CCPWDM} = \text{Apwd}_m \oplus \text{PAD1} \quad (7)$$
$$\text{CCPWDL} = \text{Apwd}_l \oplus \text{PAD2} \quad (8)$$

The Equation (7) and (8) shows code cover password obtained by XOR operation performed between access password and pad functions.

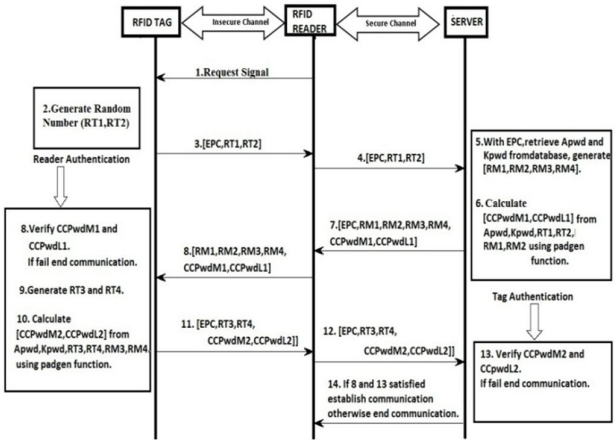

Fig 2. Tag-reader authentication using the Xor or mod scheme

A. XOR Scheme

An improved version of the Padgen function based on Exclusive-OR operation[1]. Each PAD function is computed based on one set of (R_T, R_M), which is transmitted in the open space. In contrast to the Padgen proposed and the present 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 Apwd − Padgen (R_T, R_{TM}) and Apwd-Padgen (R_{TX}, $R_T \oplus R_M$), respectively. PAD1 and PAD2 are then generated by Kpwd− Padgen (R_V, R_W) and Kpwd− Padgen (R_V, $R_V \oplus R_W$), respectively. The RV and RW values were calculated within the tags and readers. Therefore, an adversary

would not be able to correlate all the bits in Apwdm and Apwdl. In this scheme requires less area but provides less security as compared mod scheme.

B. MOD Scheme

Modulo arithmetic[1] is used as another approach to generate the Padgen function because of the scheme's 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 mod 2. In modulo mathematics, the subtraction function is replaced by exclusive OR operation. The XOR-based division (no carry in addition or subtraction) consumes very small resources. The particular advantage of exclusive-OR operation is it can thus achieve low-cost hardware implementation of the Padgen function.

III. **PROPOSED METHOD**

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 (modified MOD Function) provided by manufacturer to encrypt PWD. The database has the information about EPC and PWD of all tags. It also has a common protocol architecture which is embedded in all tags.

A. modulo 2^n+1 Adder

Designing a modulo $(2^n + 1)$ adder[7] is a little bit tricker. Such an operator is useful in a wider range of application including for instance modulo $(2^n+ 1)$ multiplier for the IDEA block cipher. This mathematic operation is often performed in diminished-one number system, where a number x is represented by x = x−1 and the number 0 is not used or treated as a special case. Fig 3 depict hardware operators performing the modulo $(2^n + 1)$ addition according to this algorithm.

$$(x' + y' + 1)\ mod\ (2^n + 1)$$

$$= \begin{cases} x' + y' & if\ x' + y' \geq 2^n \\ (x' + y')mod\ 2^n & if\ x' + y' < 2^n \end{cases}$$

$$= (x' + y' + \bar{c}_o)\ mod\ 2^n \qquad (9)$$

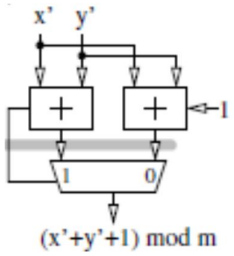

Fig 3. Modulo $2^n+ 1$ adder

Let us study the modulo $(2^n + 1)$ addition of two numbers in normal representation[13]. The algorithms described in this paper returns the desired result increased by one. Nevertheless, this property facilitate the design of circuit and can be dealt with applications. The modulo $(2^n + 1)$ addition is now defined by,

$$(x + y + 1)\ mod\ (2^n + 1)$$

$$= \begin{cases} 2^n & if\ x = 2^n\ and\ y = 2^n, \\ (x + y) mod\ 2^n + \bar{c}_o & if\ 0 \leq x + y < 2^{n+1} \end{cases} \qquad (10)$$

Mutual authentication protocol for RFID system has been proposed and analysis instead of padgen function a modified MOD scheme function are implemented in RFID tag-reader mutual authentication protocol system due to reduction in hardware cost and area. Experimental evaluation reveals that the proposed protocol with modified MOD scheme provides more security with less area and efficient than the earlier schemes.

B. Modified Mod Scheme

An improved version of the Padgen function based on 2^n+1 modulo addition operation is proposed as follows:

$R_T \oplus R_M = R_{TM}$

$R_T \mod(2^{n+1}) R_M = R_c$

$$\text{Apwd}-\text{Padgen}(R_c, R_{TM}) = d_{w1}\, d_{w2}\, d_{w3}\, d_{w4} \quad \text{(Base 10)}$$
$$= R_W \qquad (11)$$

$R_{Tm} \mod(2^{n+1}) R_{M\,l} = R_f$

$$\text{Apwd} - \text{Padgen}(R_f, R_{TM}) = R_v \qquad (12)$$

$$\text{Kpwd}-\text{Padgen}(R_V, R_W) = h_{q1}\, h_{q2}\, h_{q3}\, h_{q4}$$
$$= PDA_1 \qquad (13)$$

$R_V \oplus R_W = R_{VW}$
$= d_{s1}\, d_{s2}\, d_{s3}\, d_{s4}$

$$\text{Kpwd}- \text{Padgen}(R_V, R_{VW}) = PDA_2 \qquad (14)$$

Each PAD function is computed based on one set of (R_T, R_M), which is transmitted in the open space. In contrast to the Padgen proposed and 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 results of 2^{n+1} modulo addition applied to Apwd − Padgen (R_c, $R_T \oplus_M$) and Apwd-Padgen (R_c, $R_T \oplus R_M$), respectively. PAD1 and PAD2 are then generated by Kpwd− Padgen (R_V, R_W) and Kpwd− Padgen (R_V, R_{VW}), respectively. The RV and RW values were calculated within the tags and readers. Therefore, an adversary would not be able to correlate all the bits in Apwdm and Apwdl.

IV. RESULTS AND DISCUSSION

Xilinx ISE is a set of tools integrated into a single user interface called the "Project Navigator". The main goal of the tools is the capture and verification of design information targeted at a programmable logic implementation.

The proposed RFID mutual authentication protocol is described using structural Verilog HDL to produce gate level net list and synthesized using Xilinx ISE design suite 14.2 tool. Here different RFID tag-reader authentication protocol namely Konidala Scheme, modified scheme, Xor scheme, MOD scheme, Modified MOD scheme are considered for comparison in terms of Logic elements, Delay. Figure 4 shows that simulation output of the Modified MOD scheme.

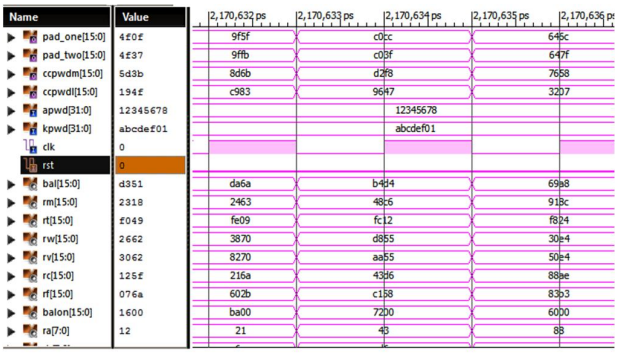

Fig 4. Simulation result of modified mod scheme

A. Area and Delay Analysis

Comparison of Logic Elements and Register Count of Proposed Protocol with Previous Approaches. The logical element requirement to perform a single time Padgen, Modified MOD function is synthesized and result has been measured. Each protocol may utilize the function eight times to complete a single authentication process. The Number of Slice Registers elements of Modified MOD scheme and number of transition required to complete a function is less compared to other functions. From the synthesis results in Table I, it is shown that the logical elements of the proposed protocol are low. The reason for increased number of transitions is that, it needs to be updating the value for each iteration by performing some logical operation after each authentication process. Protocol uses a padgen function to encrypt the password since padgen function consumes more logic elements which increases the hardware cost.

TABLE I.

Comparison of Area And Delay Estimation of Proposed Protocol with Earlier Schemes

Parameter	**Konidala[3]**	**XOR Scheme [1]**	**MOD Scheme [1]**	**Proposed**
Number of Slice Registers	32	32	42	32
Number of Slice LUTs	162	322	986	426
Number of LUT Flip Flop pairs used	177	348	975	452
Delay (ns)	9.493ns Logic 4.849ns Route 4.644ns Logic 51.1% Route 48.9%	11.514ns Logic 5.906ns Route 5.608ns Logic 51.3% Route 48.7%	31.80 Logic 8.35 Route 23.45 Logic 26.3% Route 73.7%	17.276 Logic 6.33 Route 10.94 Logic 36.6% Route 63.4%
Hardware Implementation	No	Yes	Yes	Yes
Security	Less	Average	High	High

Mutual authentication protocol for RFID system has been proposed and its simulation, implementation results has been analyzed. From this analysis instead of padgen function a modified MOD scheme function are implemented in RFID tag-reader mutual authentication protocol system due to reduction in hardware cost and area. Experimental evaluation reveals that the proposed protocol with modified MOD scheme provides more security with less area than the earlier schemes.

V. CONCLUSION

In this work, VLSI implementation of an efficient RFID mutual authentication protocol and Modified algorithm is proposed whose functionality is described in Verilog hardware description language. Modified MOD functions were examined for the tag-reader mutual authentication protocol in the RFID system environment. The proposed RFID tag-reader mutual authentication protocol has been simulated in Xilinx ISE Design Suite 14.2. In addition to that the proposed protocol outperform than the earlier schemes in terms of area.

REFERENCES

[1] Yu-Jung Huang, 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.

[2] Peris-Lopez P, Lim T.L, and Li T., "Providing stronger authentication at a low cost to RFID tags operating under the EPC global framework", in Proc. IEEE/IFIP Int. Conf. EUC, Vol. 2, pp. 159–166,april 2008.

[3] Konidala D.M., and Kim K., "A Simple and Cost effective RFID Tag-Reader Mutual Authentication Scheme", in Proc. Int. Conf. on RFID Sec, pp. 141-152, july 2007.

[4] Peris-Lopez.P, Hernandez-Castro J.C., Estevez-Tapiador J.M., and Ribagorda A ,"An Efficient Mutual Authentication Protocol for Low- Cost RFID Tags", Proceedings OTM Federated Conference and Workshop, 2006.

[5] Mark Goresky and Andrew M. Klapper, "Fibonacci and Galois Representations of Feedback-with-Carry Shift Registers", IEEE Transactions on Information Theory, Vol. 48, No. 11, pp. 2826-2836,2006.

[6] S.piramuthu, "Light weight Cryptography Authentication In Passive RFID-Tagged System", IEEE Trans.syst. ,man, cybern.c,appl.Rev., vol.38, pp.360-376, may 2008.

[7] R. Zimmermann, "Efficient VLSI Implementation of Modulo ($2^n \pm 1$) Addition and Multiplication", In Proceedings of 14th IEEE Symposium on Computer Arithmetic, pages 158– 167, Adelaide, Australia, April 1999.

[8] Hung-Yu Chien, "A New Ultra Lightweight RFID Authentication Protocol Providing Strong Authentication And Strong Integrity", IEEE Transactions in Dependable Secure Computing, Vol. 4, No. 4, pp. 337–340,2007.

[9] P.Peris-Lopez, J.C Hernandez-Castro., J.M Estevez-Tapiador., and Ribagorda A., EMAP: "An Efficient Mutual Authentication Protocol for Low- Cost RFID Tags", Proceedings of OTM Federated Conference and Workshop,2006.

[10] Ting W.C and Sun H.M , "A Gen2-Based RFID Authentication Protocol for Security and Privacy", IEEE Transactions on Mobile Computing, Vol. 8, No.8, pp. 1052–1062,aug 2009.

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

[12] Yu-Jung Huang, Ching-Chien Yuan, Ming-Kun Chen, Wei-Cheng Lin, and Hsien-Chiao Teng, "Hardware Implementation of RFID Mutual Authentication Protocol", IEEE Transactions on Industrial Electronics, Vol. 57, No. 5, pp.1573-1582, may 2010.

[13] Jean-Luc Beuchat,"Some Modular Adders and Multipliers for Field Programmable Gate Array", Laboratry de l'Informatique du Parall´elisme, 46, All´ee d'Italie.

[14] Garfinkel S.L, Juels A, Pappu R, "RFID privacy: an overview of problems and proposed solutions," Security & Privacy, IEEE, vol.3, no.3, pp. 34- 43, May-June 2005.

[15] Chris J Mitchell and Boyeon Song , "RFID Authentication Protocol for Low-cost Tags," WiSec, Alexandria, Virginia, April 2008.

