VLSI Implementation of a Key Distribution Server based Data Security Scheme for RFID system

Joyashree Bag
Dept. of Electronics and Tele-Communication Engineering,
Jadavpur University,
Kolkata-700032, India
e-mail: joyashree_bag@yahoo.co.in

Subir Kumar Sarkar, *Senior IEEE member*
Dept. of Electronics and Tele-Communication Engineering,
Jadavpur University,
Kolkata-700032, India
e-mail: subirsarkar@ieee.org

***Abstract*— RFID Technology is now a globally accepted technology which is rapidly emerging in every field of science and applications. It's excellent feature of very fast auto-identification without line of sight has made it popular in different areas of wire-less communication based system. But, during data transmission/exchange, security of personal or confidential data, it exposes serious threats to the security and privacy of individuals and organizations. Data security for RFID technology is now a mandatory condition to be provided by the manufacturer for better customer support and services. In this paper, we have proposed a security scheme which introduces a trusted Key management system. In this system, not a single key but several keys will be maintained, controlled and provided by the Key distribution server system (KDSS). It will be extremely useful for military persons in remote places where it is useful to identify specific item or guide to right route. Data will be encrypted using different programmable cellular automata (PCA) rules which is also provided with the key by the server. The system processor has been implemented up to RTL schematic level using Xilinx ISE14.3 simulation tool and virtex-7 FPGA board for real time verification of its functionality.**

.

Key words- Data security, RFID technology, KDSS, PCA rules, VLSI, FPGA

I. INTRODUCTION

There was a great deal of interest in RFID from researchers, developers and academic institutions in the 1970s and RFID technology achieve its momentum. Commercial applications of RFID enter mainstream in early 1980's and RFID emerged as wide applications in 1990's period. Recently, developments continued in the 1990s with integrated circuit development and size reduction until microwave RFID tags were reduced to a single integrated circuit. Considerable work is being undertaken in many commercial applications. There are now more than 350 patents have been registered with the US Patent Office related to RFID and its applications [1,2].

The Mexican Government has implanted RFID chips into its higher officials to provide tracking of them for their security [3].

It is also used for access control. There are other applications under consideration, for example, the incorporation of RFID tags into important documents such as birth certificates, driver licenses, educational certificates, manuscripts, medical registrations and so on. In fact it is used in any document where authenticity and veracity are essential [4].

RFID devices must be very low cost to provide successful globalization in every field. To cut down the cost, these are generally passive devices with limited functionality. Affordable tags having only 500–5000 gates, cannot perform standard cryptographic operations necessary for privacy and security. Advanced Encryption Standard (AES) algorithm for data security requires almost 20,000–30,000 gates to manage the cryptographic security [5]. Security for the current generation of passive RFID tags therefore represents a considerable challenge. We have introduced PCA to encrypt data or information stored in a Tag using a single and specific Key in our paper, 'Data security scheme using PCA for RFID system'. Only the authentic Reader would be provided with this key and PCA rule, so that only the authorized Reader will be able to read/decrypt data. This security scheme secured information stored in a tag very effectively reducing the side channel attack and other data hackers [6]. Research paper, 'Advanced Multi-step security scheme' proposed a novel data security scheme where data/information stored in a tag has been divided into parts and each part has been encrypted by different PCA rules but the Key used is same for all the cases. Moreover, Reader can't access data at a time rather step by step in formation will be decrypt by Reader and finally the reader will receive data [7].

In our present work, we have proposed such a security scheme for RFID system which introduces a novel Key management system. In this system, not a single key but several keys will be maintained, controlled and provided by the Key distribution server system. Data will be encrypted using different PCA rules which are also provided with the key by the server.

2327-0659/15 $31.00 © 2015 IEEE
DOI 10.1109/ACCT.2015.55

In a high security zone, this scheme will work excellent. For example, post-mortem-report of individual is very confidential and it is much prone to be tampered by other unwanted person, sometimes corrupted police official or doctors itself. As a preventive measure, if the report is recorded in such a way that it couldn't be retrieved by unauthentic person, it will be effective. Any confidential official document also can be recorded in this way where data can't be retrieved without specific code or permission of server. Moreover, to send the information to distant official, it is safe. The special feature of RFID technology gives the system more efficient performance. RFID tags can be detected instantly and without line of sight once it enters the detection zone of a Reader. A tag cannot be damaged easily and removal of data from it is not possible. Security scheme added with it protect the data from hackers i.e. any leakage or alteration is not possible.

II. PROPOSED HIGH SECURITY RFID SYSTEM

In a security zone like defense, it is more important to deliver right message to right person without intimating others. Extreme secret is maintained during data reporting related to defense plan or operating manuals of specific weapons for special activities. In a remote area where some specific identification node is placed to guide the traveler to reach the destination or to find the friend node (station) to get correct information, this service will play excellent. Only the authentic Reader will be successful in retrieving proper information after decryption of the data stored in the detected tag. In this system, user can choose Key and specific PCA rule to encrypt data to be stored in a tag. The **Key Distribution Server** will distribute keys and PCA rules and control them. To decrypt data from a specific tag, the Reader will request the server to provide key & PCA rule for that tag. Server will check the authentication of this Reader and provide the information.

A. Proposed High Security Algorithm:

Step1: User request the Key Distribution server for key(Ki)
Step2: User request server for PCA rule(PCAi)
Step3: Information is encrypted using Ki and PCAi
Step4: Encrypted information is stored in tag

Key Distribution server maintains a LUT of key(Ki) & PCA rule(PCAi)

Step5: Reader detects tag, request the Key Distribution server to provide Ki & PCAi quoting tag ID and its own identity code
Step6: The Server checks authentication of Reader looking into the LUT of authenticated Reader with specific ID code of each
If it matches then
go to Step7
else Step9
Step7: Server provides Ki & PCAi for that specific tag ID
Step8: Reader decrypt information stored using this Ki & PCAi
Step9:Exit

B. Key distribution system:

Use of single Key may cause leakage and security may break, another major drawback is 'replay attack' where user may use the secret key when he is even out of the scenario and harm the security system. To avoid these problems we have proposed a random distribution of key and PCA rules through a trusted server which will store several combination of keys and PCA rules. User may choose any combination at a time, but once it is chosen, it will be recorded by the server as Look-up-table along with tag's identity and secret code for its authentic Reader's identity. When a Reader detects a tag within its detection range, it request the server to provide K & PCA informing the ID of the detected tag and its own code for authenticity. As the server checks authenticity of the reader, it acts accordingly. The prime advantage of the system is that the responsibility and security entirely depends on the trusted server. Neither the Reader nor the Tag has to store or remember the Keys and PCA rules. Memory size, thus reduce the size of the Reader processor. A single server can control several readers and tags but a large number of users cause congestion and malfunctioning of the server.

C. Proposed server based RFID security system

In Fig.1, the proposed model for high security RFID system has shown. The trusted server working as the middle-person takes the responsibility to provide right information to the right person. In modern age of RFID technology, where hackers can attack and hack data from information stored in a tag, proper security measure of stored information plays an important role.

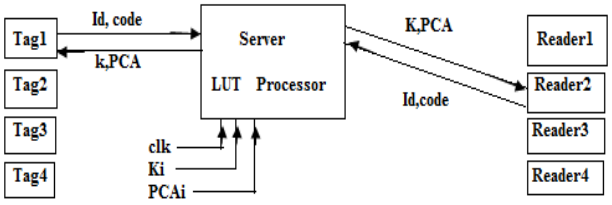

Fig.1. Proposed system using trusted Key Distribution Server

Figure 1 shows that the server maintains a LUT of tag ID and its corresponding security information. It consists of a series of keys and PCA rules combination. For experimental purpose, we have used four keys and four PCA rules. Several readers and tags come in to the scenario. Each time

the key & rule combination differs and maintained by a simple clock triggered way.

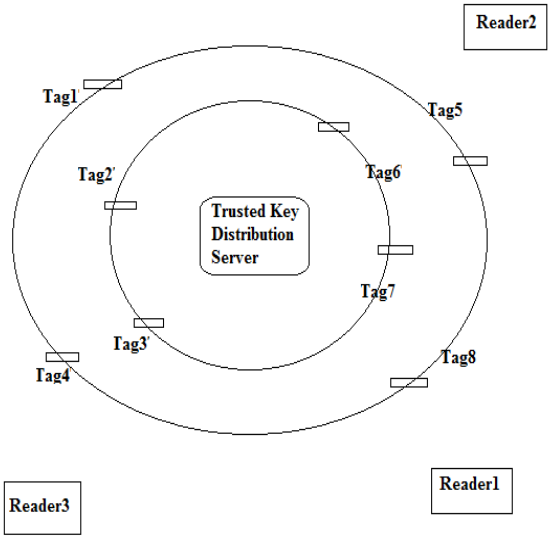

Fig.2. Proposed Scenario for the high security RFID system

Proposed Scenario for the high security RFID system is shown in Fig.2. This figure shows three Reader and eight tag working at a time, where only tag1,2,3 are readable by Reader1 whereas tag4&5 are readable by Reader2 and tag6,7&8 are readable by Reader3 though all the tags are detected by all Readers, data read permission is given to specific reader only. This is very important feature of this scheme that it imposes an extra data read protection to the RFID system reducing extra memory/chip size of reader/tag. The data format of a tag will be as shown in Fig.3

ID	Information (I)	Code

Fig.3 Data format of RFID tag

Data frame of RFID tag consists of three main particulars, Tag ID, information stored by the user and the 'Code', which denotes the ID code for specific Reader. Either tag or reader need not remember the encryption key or PCA rule. Once data has been encrypted and stored into tag by the user, the Trusted key distribution server store as a LUT in its memory along with tag ID and 'code' to detect the right Reader. In a scientific research laboratory, it is very common to steal the experimental reports by other person having bad intention or may cause harm to the people. Though several techniques are which are adopted by the scientist to keep secrecy of their results, our server based security scheme will provide good performance. Some time, researcher's contribution may be leaked through resource person to another research lab inside/outside country.

III. DESIGN AND IMPLEMENTATION

A. Processor for Server:

This module consists of a look-up-table incorporating a list of authentic Readers, their specific identification code, targeted tag IDs for respective Readers. Another table consists of different cellular automata rules and different Key matrices. In this work, for simplicity, we have chosen four rules with four different keys. Whenever the server receives request from a Reader, it looks in to the identification LUT and check whether the code matches with the list of authenticated Reader or not. If it is reliable, then the server acknowledges the Reader otherwise neglects the request. After receiving acknowledgement from server end, the Reader request for specific key and CA rule to decrypt the information from the tag identified by it sending the ID of the tag to the server. The server sends the information instantly to the reader.

a) Programmable Cellular Automata Rules:

Different Cellular Automata Rules are depicted in Table 1 and their rules are logical expression are listed below: The binary number (01011010)2 represents the decimal number 90 and the binary number (10010110)2 represents the decimal number 150 and so on [8-12].

TABLE 1: PROGRAMMABLE CELLULAR AUTOMATA RULES

Rules	7 111	6 110	5 101	4 100	3 011	2 010	1 001	0 000
51	0	0	1	1	0	0	1	1
60	0	0	1	1	1	1	0	0
90	0	1	0	1	1	0	1	0
102	0	1	1	0	0	1	1	0
150	1	0	0	1	0	1	1	0
153	1	0	0	1	1	0	0	1
195	1	1	0	0	0	0	1	1
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

b) The PCA rules can be expressed as follows:

$Sc_i (t + 1) = NOT\ Sc_i (t)$ …….....Rule. 51
$Sc_i (t + 1) = Sc_i (t)\ XOR\ Sc_{i-1}(t)$…….....Rule. 60
$Sc_i (t + 1) = Sc_{i-1} (t)\ XOR\ Sc_{i+1} (t)$…….....Rule. 90
$Sc_i (t + 1) = Sc_i (t)\ XOR\ Sc_{i+1} (t)$……..Rule. 102
$Sc_i (t + 1) = Sc_{i-1} (t)\ XOR\ Sc_i (t)\ XOR\ Sc_{i+1} (t)$….Rule. 150
$Sc_i (t + 1) = Sc_i (t)\ XNOR\ Sc_{i+1}(t)$ ……...Rule. 153
$Sc_i (t + 1) = Sc_{i-1} (t)\ XNOR\ Sc_i (t)$ ……...Rule. 195

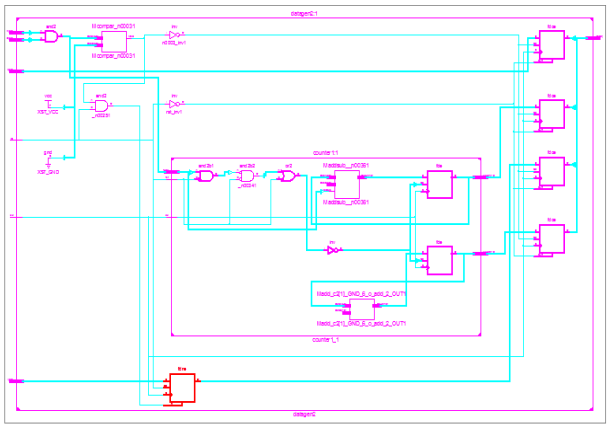

Fig.4 RTL schematic view of proposed Key Distribution Server

Figure 4 depicts the RTL schematic view of the Key Distribution Server for proposed security scheme for RFID system.

B. Tag Frame Generator:

In this proposed scheme, Tags are consists of a module named as secret code generator, which generates the code and encrypted the stored information within the tag itself. Here is an example of code generation following CA rules 90 & 150.

Secret code Generation:

Suppose we choose key Matrix as K = $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

Now, according to condition we have applied for this scheme, if the Ki0='0' then the entire row of the Key matrix will follow the rule 150 and if Ki0='1' then it will follow rule 90. From the chosen key Matrix, 1st, 3rd and 4th row will follow rule 90 whereas only 2nd row will follow rule 150.

For rule 90:
Data of 1st column of secret code Matrix Sc will be as
Sci = Ki $\oplus$ Ki+1
Data of 4th column of secret code Matrix Sc will be as
Sci = Ki-1$\oplus$ Ki
Data of other column of secret code Matrix Sc will be as
Sci = Ki-1$\oplus$ Ki $\oplus$ Ki+1

For rule 150:
Data of 1st column of secret code Matrix Sc will be as
Sci = Ki+1
Data of 4th column of secret code Matrix Sc will be as
Sci = Ki-1
Data of other column of secret code Matrix Sc will be as
Sci = Ki-1$\oplus$ Ki+1
Following these rules,

The code Matrix for Sc will be as, Sc = $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

Now if this code Matrix is integrated with the tag ID, only the Reader, who knows the exact Key Matrix, will be able to decode the ID and the data or information stored within the tag. Thus prevents the data hacking by unauthorized Reader.

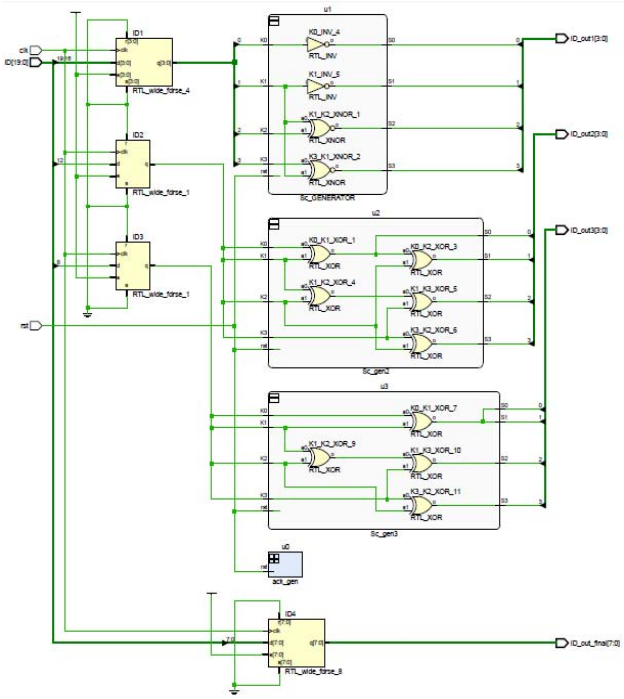

Fig.5 RTL schematic view of specific secret code generator

In Fig.5 the RTL schematic view of the secret code generator module within a tag is shown.

Design and hardware implementation is performed in VHDL code and Xilinx Plan ahead 14.3 tools. Synthesizable module of reader processor is also developed. A virtual environment is used to check the real time functionality of the proposed system. High performance FPGA Kintex7 and Zynq-7 have been used to implement the system. The high speed performance in RF frequency range is the most important feature of Virtex7 series FPGAs. Low power and high speed operation is observed. In Table 2, the advance HDL synthesis and Device utilization chart for the server only is enlisted.

TABLE 2 SYNTHESIS REPORT [SERVER]

Selected Device : 7K325TFFG900-2

Advanced HDL Synthesis Report		**Device utilization summary**	
Counters	2	No. of Slice Registers	8
Registers:	8	No. of Slice LUTs	13
Comparator	5	No. of LUT Flip Flop pairs	15
Xors	2	No. of fully used LUT-FF pairs:	6
Min .period (ns)	0.980	No. of unique control sets	3
Max. Freq. (MHz)	1020.2	Number of IOs	28
		IOB Flip Flops/Latches	4
Max. required time after clock	0.575 (ns)	No. of BUFG/BUFGCTRLs	1

IV. CONCLUSION

A novel trusted key distribution server based high security scheme for RFID based system has been proposed and implemented in this work. Where communication system is abruptly disturbed/ unavailable, this security scheme provides ultimate security of information and person. Application of RFID is now in advance stage in defense and military and other high ends, this scheme are useful to protect data and access data securely. FPGA implementation of this scheme provides a single chip solution with minimum hardware, high speed operation with negligible power consumption.

ACKNOWLEDGEMENT

Subir Kumar Sarkar thankfully acknowledges the financial support obtained from CSIR RFID Project. Ref. No: 22(0588)/12/EMR-II Dated 02-04-2012.

REFERENCES:

[1] http://www.rfidjournal.com, RFID Journal FAQs,

[2] http://www.aimglobal.org, The history of RFID, Association for Automatic Identification and Mobility, October 2001.

[3] http://www.eetimes.com. E E Times, 19 December 2001, Euro bank notes to embed RFID chips by 2005,

[4] http://www.afcea.org. Radio frequency identification ready to deliver, Signal Magazine, January 2005, Armed Forces Communications and Electronics Association (AFCEA),

[5] http://www.rsasecurity.com. RSA Laboratories, Technical characteristics of RFID,

[6] Joyashree Bag and Subir Kumar Sarkar "Design and VLSI Implementation of a Data Security scheme for RFID system using Programmable Cellular Automata" Published in the Int. Journal of RFID technology and Applications, Inderscience, IJRFITA].Pages:197-211, 2013.

[7] Joyashree Bag, Subhashis Roy and Subir Kumar Sarkar, "Advanced Multi-step Security Scheme(AMSS) using PCA for RFID system and its FPGA Implementation" [accepted, Int. Journal of RFID technology and Applications, Inderscience, IJRFITA, 2014]

[8] T. K. York, Ph. Tsalides, B. Srisuchinwong, P. J. Hicks, and A.Thanailakis, "Design and VLSI implementation of a mod- 127 multiplier using cellular automaton-based data compression techniques," in IEEE Proc. E. Comput. Digit. Tech., vol. 138, no. 5, pp. 351-356. 1991

[9] P. D. Hortensius, R. D. Mcleod, W. Pries, D. M. Miller, and H. C.Card, "Cellular automata based pseudorandom number generators for built-in self-test," IEEE Trans. Cornput.-Aided Design, vol. 8, no 8, pp.842-59, Aug. 1989.

[10] P. Tzionas, Ph. Tsalides, and A. Thanailakis, "Design and VLSI implementation of a pattern classifier using pseudo @D cellular automata," IEE Proc. G, vol. 139, no. 6, pp. 661-668, Dec. 1992.

[11] D. Roy Chawdhury, I. Sengupta, S. Basu, and P. Pal Chaudhuri, "Cellular automata based error correcting codes (CAECC)," IEEE Trans.Comput., vol. 43, no. 6, pp. 759-764, June 1994

[12] P. Dasgupta, S. Chottopadhyay and I. Sengupta, "An Asic for cellular automata based message authentication". Conference proceedings of thirteenth IEEE International Conference on VLSI Design,. pp. 538 – 541;2000