International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 06, Issue 3, May 2017, pp.126-129, ISSN:2274-1412

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

Ebtasam Ahmad Siddiqui [1], Suresh Gawande, Sanjeev Shrivastava[3]
[1]M.Tech Scholar, Bhahbha Engineering Research Institute, Bhopal, ebtasam.bh27@gmail.com, India;
[2,3]Asst. Professor, Bhahbha Engineering Research Institute, Bhopal,
suresh.gawande@rediffmail.com,sanjeev.dabbu@gmail.com, India;

Abstract *– In this paper review of key distribution server based security technique. Data security could be a vital issue for radio frequency Identification (RFID) system because it hides necessary data inside it. From each technical and business point of view, it's important to confirm the security of data for the worldwide use of RFID technology, otherwise hacker or attacker will control the info transmission. So, to secure the RFID tag from 'hacking', a knowledge security scheme for RFID tags based on programmable cellular automata has been planned.*

Keywords*: Data security, RFID technology, KDSS, PCA rules, VLSI, FPGA,*

I. Introduction

Secured information transfer is one amongst the most necessary criteria of any RFID system and it'll be the responsibility of the system to prevent any un-authorized access to special or personal information or info keep within the RFID tag, too. Users of RFID tag ought to ensure the security of any personal information or info keep on the tag or connected to them. Within the world of computing, it's vital to build the security and also the privacy safeguards into the design of RFID systems. The very important connection between tags and readers happens within the air via RF communication. This connection allows the powerful capabilities of RFID; however it additionally leaves the window open to many key threats unauthorized access to tags, rogue and clone tags and aspect channel attacks.

The Electronic Product Code or EPC world class-I Generation-I and Generation-II are popular and globally accepted normal specifications that modify the utilization of word for accessing the memory of a RFID tag. It provides one among the ultimate securities for the RFID system, however these aren't immune to 'hacking' (Thing Magic, 2005). it's possible to find the main points of personal information if anybody has the information of EPC references (ICO, 2006). Under the EPC Generation two protocol, there are many common and known factors that act as potential roadblocks to a lot of ubiquitous deployments at the consumer level. Necessary information or personal data especially sensitive personal information want an adequate level of encoding to safeguard the info (O'Connor, 2012). RFID devices should be very low value to supply successful globalization in each field. to cut down the price, these are usually passive devices with restricted functionality. Reasonable tags having only 500–5000 gates cannot perform normal cryptographic operations necessary for privacy and security. Advanced encryption standard (AES) formula for information security needs nearly 20,000–30,000 gates to manage the cryptographic security. Security for this generation of passive RFID tags so represents a substantial challenge. We've introduced PCA to encode information or data hold on during 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 only the authorized Reader are able to read/decrypt information. This security scheme secured data hold on in a very tag very effectively reducing the facet channel attack and different information hackers. RFID stands for frequency Identification, a term that describes a system of automatic identification whereas a device, known as RFID reader, uses frequency or magnetic field variations to communicate with the RFID tags connected to AN item. The 2 most significant parts of AN RFID system are the tags that are the identification device connected to the item we want to track, and also the reader, that could be a device which will recognize the presence of RFID tags and read the data keep on them. The reader will then inform another system about the presence of the tagged items. The system with that the reader communicates usually runs the code that stands between readers and applications. This software is termed RFID middleware (Ahson and Ilyas, 2008). the essential parts of a typical RFID system are shown in Figure one. During this system, RFID reader and tag will radio-communicate with one another using a range of various frequencies, and presently, most RFID systems use unlicensed spectrum. The common frequencies used are low frequency (125 kHz), high frequency (13.56 MHz), ultra high frequency (860–960 MHz), and microwave frequency (2.4 GHz) (Ahson and Ilyas, 2008; Miles et al., 2008). Dasgupta et al. (2001) have represented the Programmable Cellular Automata (PCA) rules in their article 'Theory and application of non-group cellular automata for message authentication.

II. Literature Survey

The Joyashree Baget. al. [1] "VLSI Implementation of a Key Distribution Server based Data Security Scheme for RFID system" In this paper, author planned a security scheme that introduces a trusted Key management system. During this system, not one key however many keys are maintained, controlled and provided by the Key distribution server system (KDSS). It'll be very helpful for military persons in overseas wherever it's helpful to identify specific item or guide to right route. Information are encrypted mistreatment completely different programmable cellular automata (PCA) rules that is additionally given 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 practicality. a unique trusted key distribution server based} high security scheme for RFID based system has been planned and enforced during this work. Wherever communication system is abruptly disturbed/ unavailable, this security scheme provides final security of information and person.

P. Tzionaset. al. [2] "Design and VLSI implementation of a pattern classifier using pseudo 20 cellular automata" In this paper, For the VLSI implementation of the projected pattern classifier; a 1.5 pm DLM N well CMOS method has been used. the planning and VLSI implementation of a pattern classifier based on pseudo 2nd cellular automata (CA) is given during this paper. Cellular automata exhibiting cyclic group structures are wont to give improved measures of the degree of similarity between patterns. During this paper, a new CA based pattern classifier is given. The acting distance and entropy variations induced on the patterns by the evolution of the pseudo 2nd binary HACA show that the represented pattern classifier is implemented with variable discrimination sensitivity.

Joyashree Bag et. al. [3] "Advanced multi-step security scheme using PCA for RFID system and its FPGA implementation" In this paper, programmable cellular automata (PCA) are used to achieve a multi-step security for AN RFID system. The planned scheme has high level of security, because it provides step by step encoding with different keys and PCA rules for every part. The quality of the circuit is reduced considerably by reducing the hardware size and power dissipation to a minimum level. The appliance of RFID in varied domains is increasing due to its simple use, flexibility, low price and enormous benefits of fast accessing and information transfer technology. A image hardware realization of this module for RFID application has been complete and described during this paper. The modules given during this paper are programmed using VHDL language. Overall performance of information security using PCA is satisfactory and appropriate for RFID chip planning. The most vital a part of this scheme is, not only the tag however authentication of reader has additionally been checked. Reader has the corresponding PCA to retrieve the received coded information components and it transmits the 'ack' signal with the code.

Wonseok Choi et. al. [4] "PUF-based Encryption Processor for the RFID Systems" In this papers the PUF-based encoding processor and therefore the low-priced RFID authentication protocol is planned. The challenge-response pairs (PUF's input and output) are encrypted by the PUF's characteristics, not by Hash and AES. Besides, the encryption technique is modified by the instruction code. The planned scheme defends many types of attacks that are physical, modeling, spoofing and location tracking attacks. we tend to implemented the PUF-based encryption processor at low value with small footprint and low power. This paper shows the PUF-based encryption processor and also the low-priced RFID authentication protocol. These utilize the PUF's characteristics to perform the authentication method. The PUF based mostly encryption processor consists of N-bit PUF, encryption, decryption, computer code modules. We tend to implemented the PUF-based encoding processor at low value with small footprint and low power.

Mikko O. Lehtonen et. al. [5] "Trust and Security in RFID-Based Product Authentication Systems" In this paper, we tend to study trust and security in RFID-based product authentication systems. Author initial present a proper definition for product authentication method then derive the overall chain of trust also as functional and nonfunctional security needs for product authentication. Most of the scientific literature that covers the subject focuses on cryptographic tag authentication only. This paper, however, provides a broader read as well as conjointly different known approaches, most notably location-based authentication. To derive the useful security needs, we tend to use the conception of misuse cases that extends the utilization case paradigm standard within the field of needs engineering. Author analysis of the EPC network shows that tag authentication is supported conceptually however not yet in apply, which the forthcoming EPC discovery services can play a vital role in guaranteeing the completeness of the history for location-based product authentication. Last, we tend to uncovered structural shortcomings within the EPC network's support for location-based product authentication and conferred however the shortcomings can be overcome by an EPC trace analysis service residing within the network's core service level.

III. Method

III.1. Radio Frequency Identification (RFID)

RFID is an area of automatic identification that's gaining momentum and is considered by some to emerge joined of the most pervasive computing technologies in history. In its simplest kind, RFID may be a similar conception to bar coding. It seen as a way of enhancing information processes and is complementary to existing technologies. It's a proved technology that has been in use since the 1970s.

A lot of complicated description is an electromagnetic proximity identification and information transaction system. Using "RFID tags" on objects or assets, and "readers" to gather the tag data, RFID represents an improvement over bar codes in terms of non-optical proximity communication, data density, and 2 approach communication ability. Operational RFID systems involve tags and readers interacting with objects (assets) and info systems to produce a data and/or operational perform.

RFID is used for a good kind of applications ranging from the familiar building access control proximity cards to provide chain tracking, toll collection, vehicle parking access control, retail stock management, transport access, tracking library books, theft prevention, vehicle immobilizer systems and railway rolling stock identification and movement tracking. Whereas RFID systems will yield great productivity gains, they additionally expose new threats to the protection and privacy of people and organizations.

III.2. Security of the RFID technology

The radio communications between RFID transponders and readers rises, as primarily all wireless technologies, variety of security problems. basic data security objectives, like confidentiality, integrity, availability, authentication, authorization, no repudiation and anonymity are typically not achieved unless special security mechanisms are integrated into the system. The privacy side has gained special attention for RFID systems. Consumers could carry objects with mutely communication transponders while not even realizing the existence of the tags. Passive tags usually send their identifier while not any security verification once they are powered by electromagnetic waves from a reader. The ID data may be connected to different identity information and to location info. Consumers would possibly use a private reader to identify tags in their surroundings however the large variety of different standards (see chapter 3) could render this tough. Companies face customer fears and also the privacy problems could become a significant obstacle to any RFID proliferation.

RFID security proposals either based on Cipher-based protocols and Hash-based protocols. Lack of procedure resources is denoted as state of affairs, however value issue remains a problem since it's utilized in huge numbers. And if RFID replaces barcodes on individual items, they'll well contribute value of these items. This paper address security and privacy issues of mutual authentication mechanism, throughout transmit from reader to tag and vice-versa. The System ought to be highly secured with authentication protocol that will anti-intrusion and encryption algorithmic rule, that encrypts necessary information that can't be decipher by attacker.

Due to security reasons, it's vital to deliver right message to right person while not intimating others. Extreme secret is maintained throughout information reporting associated with defense arrange or operating manuals of specific weapons for special activities. The Key Distribution Server can distribute keys and PCA rules and control them. To decode information from a particular tag, the Reader can request the server to supply key &amp; PCA rule for that tag. Server can check the authentication of this Reader and supply the data.

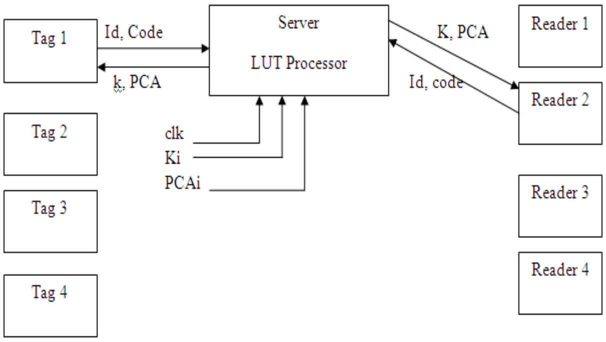

Fig.1 Key Distribution Server

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.

III.3. PCA rules

The programmable cellular automata (PCA) was first introduced in [6] and are changed CA structures, wherever the combinational logic of every cell isn't fixed however controlled by variety of control signals such totally different functions (evolution rules) is complete on a similar structure. Because the matter of reality, PCA are basically a changed CA structure. We are able to say that a CA may be a PCA if it employs some control signals that implement numerous functions dynamically in terms of various rules.

IV. Conclusion

This paper has reviewed the primarily latest analysis trends and planned the information security RFID technology. It's excellent feature of very fast automobile identification while not line of sight has made it well-liked in numerous areas of wire-less communication based system. Information verification verifies the authenticity of information generated by RFID-based data service. During this paper we tend to summary on VLSI Implementation of a Key Distribution Server based data Security scheme for RFID system.

References

1.] Bag, J., & Sarkar, S. K. (2015, February). VLSI Implementation of a Key Distribution Server Based Data Security Scheme for RFID System. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies (pp. 581-585). IEEE.

2.] .Tzionas, P., Tsalides, P., & Thanailakis, A. (1992). Design and VLSI implementation of a Pattern Classifier using pseudo 2D Cellular Automata. IEE Proceedings G-Circuits, Devices and Systems, 139(6), 661-668.

3.] Bag, J., Roy, S., Kantha, B., & Sarkar, S. K. (2015). Advanced multi-step security scheme using PCA for RFID system and its FPGA implementation. International Journal of Radio Frequency Identification Technology and Applications, 4(4), 325-341.

4.] Choi, W., Kim, S., Kim, Y., Park, Y., & Ahn, K. (2010, June). PUF-based Encryption Processor for the RFID Systems. In Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on (pp. 2323-2328). IEEE.

5.] Lehtonen, M. O., Michahelles, F., & Fleisch, E. (2007). Trust and security in RFID-based product authentication systems. IEEE Systems Journal, 1(2), 129-144.

6.] Bag, J., Rajanna, K.M. and Sarkar, S.K. (2013) 'Data security for EPC Gen-2: VLSI design and its FPGA implementation', 3rd International Conference on Advanced Computing & Communication Technologies, pp.330–336.

7.] Chawdhury, D.R., Sengupta, I., Basu, S. and Chaudhuri, P.P. (1994) 'Cellular automata based error correcting codes (CAECC)', IEEE Transactions on Computers, Vol. 43, No. 6, pp.759–764.

8.] Chen, R-J. (2010) 'Novel SCAN-CA-based image security system using SCAN and 2-D Von Neumann cellular automata', Signal Processing: Image Communication, Vol. 25, No. 6, pp.413–426.

9.] Chen, R-J. and Lai, J-L. (2007) 'Image security system using recursive cellular automata substitution', Pattern Recognition, Vol. 40, No. 5, pp.1621–1631.

10.] Chen, R-J., Lai, Y-T. and Lai, J-L. (2006) 'Architecture design and VLSI hardware implementation of image encryption/decryption system using re-configurable 2-D Von Neumann cellular automata', Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS'06), 21–24 May, Island of Kos, Greece, pp.153–156.

11.] Das, D. and Misra, R. (2011) 'Programmable cellular automata based efficient parallel AES encryption algorithm', International Journal of Network Security & its Applications, Vol. 3, No. 6, pp.197–208.

12.] Dasgupta, P., Chottopadhyay, S. and Sengupta, I. (2000) 'An ASIC for cellular automata based message authentication', Conference Proceedings of 13th IEEE International Conference on VLSI Design, 3–7 January, Calcutta, India, pp.538–541.

13.] Hortensius, P.D., Mcleod, R.D., Pries, W., Miller, D.M. and Card, H.C. (1989) 'Cellular automata based pseudorandom number generators for built-in self-test', IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 8, No. 8, pp.842–859. Information Commissioner's Office (ICO) (2013) Data Protection Technical Guidance Radio Frequency Identification, Information Commissioner's Office.

14.] Knuth, D.E. (1981) The Art of Computer Programming-Semi numerical Algorithms, Addison- Wesley, Reading, MA, USA.

15.] Man, A.S.W., Zhang, E.S., Lau, V.K.N., Tsui, C.Y. and Luong, H.C. (2007) 'Low power VLSI design for a RFID passive tag baseband system enhanced with an AES cryptography engine', 1st Annual Conference: RFID Eurasia, 5–6 September, Istanbul, pp.1–6.

16.] Nandi, S., Kar, B.K. and Chaudhuri, P.P. (1994) 'Theory and applications of cellular automata in cryptography', IEEE Transactions on Computers, Vol. 43, No. 12, pp.1346–1357.