ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

VLSI Design of a New Technique for Secure Communications in Distributed RFID Systems

Raiilla Shyamala[1], Dr.S.P.V.Subba Rao[2]

PG Scholar, Dept of ECE, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India. [1]

Professor (HOD), Dept of ECE, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India. [2]

ABSTRACT: In recent years there is an enormous increase in the usage of multimedia data over Internet. While transmitting secret data over Internet our whole concern is to make it secure before transmission so that it should not be disclosed to pirates. we propose a novel coding scheme, namely Random Flipping Random Jamming (RFRJ), to protect tags' content. In this paper we also proposed a Reliable and Cost Effective Anti-collision technique (RCEAT) to achieve a reliable and cost effective identification of the tag. The RCEAT architecture consists of two main subsystems; PreRCEAT checks error in the incoming packets using the CRC scheme. PostRCEAT identifies the error free packets using Binary Tree based technique. The architecture has been synthesized using Xilinx Synthesis Technology (XST). The result shows that the architecture has smaller cell area, power Consumption and number of gates. Therefore minimize the implementation and operating costs.

KEYWORDS: RFID System, RFRJ Coding, Pseudo Random Number, Secret Sharing, Secret Communication.

I. INTRODUCTION

RADIO enables a tremendous amount of applications, such as frequency identification (RFID) technologies supply chain management electric transportation payment, and warehouse operations. Objects and their owners are automatically identified by an attached RF tag, which causes the privacy threat to individuals and organizations. Thus, privacy protection is the primary concern when RFID applications are deployed in our daily lives. Since passive tags are computationally weak devices, encryption-based secure singulations are not practical. Instead of relying on the traditional cryptographic operations, employ physical layer techniques i.e., jamming, to protect tags' data. With this approach, tags could be securely identified without pre-exchanged shared keys. The issue with the existing solutions, the privacy masking, randomized bit encoding (RBE), and dynamic bit encoding (DBE)/optimized DBE (ODBE), is the impractical assumptions. In these solutions, all the bits transmitted. by a tag are masked (jammed) under the assumption of an additive channel, where the receiver can read a bit only when 2 bits (the data bit and mask bit) are the same. When the 2 bits are different, it is assumed that the receiver is unable to recover the corrupted bit. However, this assumption is too strong since a reader should be able to detect signals from two different sources. In reality, a receiver of a data bit will decode it as either 0 or 1 without knowing the bit collision.

If there is a bit collision, either the signal strength of data bits from the tag is stronger than that of the jamming bits, or vice versa. In other words, depending ont he location of the reader, it can either read all the data bits or all the jamming bits. Also, masking requires the perfect synchronization between data bits and mask bits, which is difficult to achieve in practice. In addition to this, DBE and ODBE have two drawbacks. One is encoding collision, where two different source data bits could be encoded into the same codeword. This causes the singulation process to fail. The other drawback is more serious. Tags' data encoded by DBE or ODBE could eventually be cracked, should an adversary repeatedly listen to the backward channel (i.e., signals from a tag to a reader). This approach is called the correlation attack. Moreover, none of the aforementioned solutions protect tags against ghost and-leech attacks, i.e., impersonation of RF tags, similar to man-in-the-middle attacks. To tackle these issues, we put forth a new RFID

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

architecture and a novel coding scheme for privacy protection against various adversary models. The contributions of this paper are as follows:

We redesign the system architecture of the non encryption-based private tag access where an RF reader is divided into an RF activator and a TSD. The proposed architecture can be built by the current physical layer technologies, and thus our assumptions are much more practical than those of the existing solutions. The proposed distributed RFID architecture physically defends tags against ghost-and-leech attacks. We propose a novel coding scheme, named random flipping and random jamming (RFRJ), to protect the backward channel from passive adversaries, i.e., the random guessing attack, correlation attack, and eavesdropping. In our scheme, a tag/TSD randomly flips/jams a bit in a codeword and keeps the index of these bits in secret. RFRJ guarantees that the TSD can recover a tag's content with one of the secrets, but an adversary cannot obtain the content of tags. Since the backward channel is protected by the RFRJ coding scheme, we can protect the forward channel (i.e., signals from a reader to a tag) by having an RF activator querying based on encoded data (or pseudo ID) space by RFRJ. We generalize the RFRJ coding scheme with the arbitrary source bits and codeword lengths. In addition, we prove the maximum information rate of our RFRJ scheme that achieves the perfect secret is 0.25.We conduct theoretical analyses for security of the proposed scheme, and prove that RFRJ provides perfect protection against passive attacks as long as jamming is successful. We evaluate our RFRJ coding scheme with the existing solutions by extensive simulations, and illustrate that the new architecture and coding scheme achieve our design goals.

II. RELATED WORK

The security and privacy concerns posed by RFID technology can be roughly classified into corporate data security, which primarily affects corporations and organizations inside supply chains, and personal privacy, which primarily affects individual customers outside supply chains. Typical existing schemes include: (i) tag killing , in which tags of sold items are disabled or removed at the point-of-sale, (ii) tag blocking , in which a blocker tag creates an radio frequency environment that prevents unauthorized scanning of consumer items, (iii) encryption, in which the information stored in tags is encrypted in a dynamic manner, (iv) using passwords, in which a tag responses to a reader only if it receives the right password, (v) using pseudonyms, in which each tag is associated with a set of pseudonyms and cycles through them each time it is read, (vi) distance-sensitive tag reading , in which the tag changes its behavior according to the distance to its reader, and (vii) policy making, in which guiding principles for RFID system creation and deployment are stipulated. The privacy and security aspects of RFID systems have also been investigated in the context of libraries, banknotes, and recent theoretical development. Most of these schemes focus on addressing the privacy concerns related to individual customers or the security concerns related to single reader-tag channel.

1. Choi and Roh proposed a method to strengthen the randomized tree-walking scheme by protecting the backward channel[4] when the tag reports its actual identifier. The method involves the reader transmitting a mask at the same time when the tag is transmitting its identifier. This induces a collision between the tag's identifier and the mask that can only be resolved if the mask is known. Hence, an eavesdropper would not be able to identify the tag without knowledge of the mask.

2. Recent years have seen much growing attention on RFID security. However, little work has been performed to address the security issues in the context of supply chain management[1], which is exactly the major field for RFID applications. Existing RFID solutions cannot be applied directly in this field because of a set of special RFID security requirements to be addressed for supply chain management. The major contribution of this paper is to identify the unique set of security requirements in supply chains and to propose a practical design of RFID communication protocols that satisfy the security requirements.

3. The RFID technique is extensively applied in e-Business scope. It mainly supports the quickly and accurately work for the advanced assets management. But it is still lack of privacy protection on the EPC code. For the worse case, some hackers may steal the code content easily during the cooperative business transmissions. It will cause the business secret leaking or even the consumer privacy damage. To encrypt the EPC code, we

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

propose a two phase identification and authentication protocol with RBAC architecture to assure security. The EPC code is separates randomly into two parts by the secret sharing method. Only the one half of the EPC code is encrypted and stored in the RFID tags. The other part of the EPC code was encrypted by the private key and stored at the backend system for later decrypted used. The EPC code is decrypted when these two parts are decrypted and merged. When the owner of the tag is changed, the encrypt EPC code is merged then separated again. In this way, it is impossible has the same encrypt EPC code on the RFID tag when the owner is changed. The reader must be authorized to get the secret key before scanning and extracting the corresponding product information. Hence, it can ensure that RFID tag will not reveal important information even though it is scanned by fake or non-authorization reader. We also proposed a key management based on role-base access control method to distribute the access key and the encryption/decryption key, which aligns well with the role and the business process in a supply chain. The secret keys are managed by the role-based assignment at the enterprise level rather than at the individual level. It not only provides with more efficiency and flexibility on the role's key management, but also enhances the security of the enterprise-level RFID system. Therefore, the number of the secret key to be managed is also reduced.

Physical Layer Security:

One of the most challenging tasks in backscatter systems, such as RFIDs, is the ability to secure the transmission against eavesdropping when confidential information needs to be sent from the tag to the reader. Unlike the traditional cryptographic approach, in this work, we explore the potential of incorporating physical layer security techniques for confidential message transmission from the tag to the reader in the presence of an eavesdropper. Figure 1 shows an illustrative example of such a backscatter communication model. Similar to the received signal model for the reader, the received signal at the eavesdropper is:

yE = hTEhRTxs +nE + hTEnT E (4)

where hT E is the tag-eavesdropper channel gain (with the antenna gains taken into account), nE is AWGN at the eavesdropper with power σ2 E , and nT E is the AWGN backscattered from the tag to the eavesdropper with power σ2 T E .The assumption of perfect signal separation is commonly used in most existing literature of backscatter communication systems. Note that the difficulty of signal separation at the reader increases as the transmitted signal deviates from a pure CW carrier signal in which case a more advanced transceiver is required to keep the signal leakage at a minimal level. In this work, we assume a good transceiver design at the reader and hence the signal leakage is not considered in our analysis.

Distributed RFID Systems:

In order to accomplish a large-scale distribution of RFID tags, there are a variety of possible tag distribution patterns to choose from. Typical distribution patterns include: – Random uniform distribution: Tags are uniformly distributed over a certain area in a random manner. – Regular distribution: Tags are distributed in a regular pattern, but usually with random tag identification numbers. Typical regular patterns are:

• Grid pattern: Given a grid with edge length d, each non-border tag has four nearest adjacent neighbors at a distance d and four farther adjacent diagonal neighbors at a distance sqrt(2) ∗ d.

• Equilateral triangulation pattern: Each tag has six equidistant neighbors at a distance d. From the perspective of a mobile object, random tag distribution patterns have inherently different properties compared with regular patterns. One example is illustrated in Fig. 2. We expect there to be other generally advantageous patterns for the distribution of RFID tags, such as irregular but non-random distribution patterns, for example. This calls for the investigation of suitable tag distribution patterns and their respective properties as part of future research.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

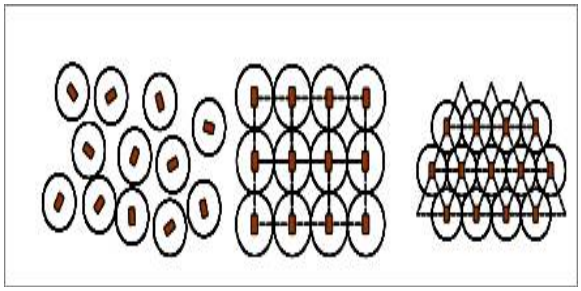

Fig. 1. Distributed RFID Systems. (a).Random Uniform Distribution. (b). Grid Pattern. (c). Equilateral triangulation pattern

III. PROPOSED ARCHITECTURE

In this section, we propose a new RFID system architecture for a secure singulation.

Assumptions:

We begin with listing physical layer assumptions as follows. Bit level jamming is feasible. An eavesdropper does not know if a bit is jammed. Probabilistic flipping model is used for a jamming environment. As we discussed in Section 2, the first and second assumptions are already implemented and validated. On the other hand, there is no implementation of the backward channel . Therefore, our assumptions are much more practical than the past research.

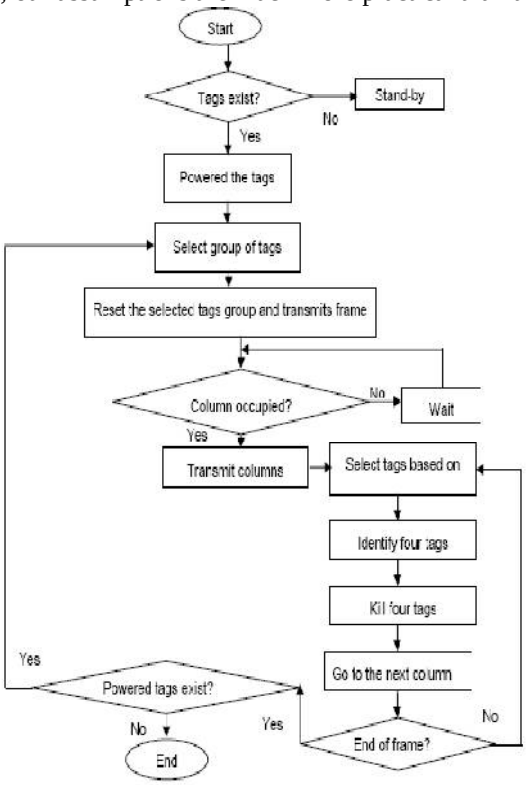

Fig. 2. RCEAT identification

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

RANDOM FLIPPING RANDOM JAMMING CODING:

In this section, we present the random flipping random jamming coding scheme. Let r be an RF activator, s be a TSD, and t be an RF tag. An activator which intends to obtain data from a tag sends a query on the forward channel. When the tag replies to the TSD, it encodes every lb bits in the data into an lc bits codeword with an encoding function. Note that lb is not the length of an ID, but the unit to be encoded into a codeword. A coding scheme for private tag access is defined by the parameters, lb, lc, and C. Here, C is a set of code words that could be used for encoding. During the transmission of a pseudo ID on the backward channel, the TSD conducts bit level jamming. On receiving the tag's reply, the TSD decodes the received codeword by a decoding function, and forwards the data to the activator via the relay channel. In general, we call lb-to-lc the RFRJ coding scheme. For instance, the coding scheme with lb ¼ 1 and lc ¼ 4 is said to be the 1-to-4 RFRJ coding scheme.

Tag Identification:

A tag identification system consists of one reader and n tags. The reader is a powerful entity with abundant memory and computation power. On the other hand, the tags are limited in memory and computation power. There is a single communication channel between the reader and the tags. However, the tags are not able to exchange messages among each other. The reader can broadcast messages to the tags. Upon receiving a message, each tag can optionally send a response back to the reader. If only one tag responds, the reader receives the message. But if more than one tag respond, their messages would collide on the communication channel, and thus cannot be received by the reader. In this case, the reader detects a collision on the channel but nothing else. Each tag has a unique ID, where k is the length of the ID string. At the beginning, the reader does not know anything about the tags. Tag identification protocol species the algorithms for the reader and the tags, so that the reader can collect all the tag IDs.

Like many technologies, low-cost Radio Frequency Identification (RFID) systems will become pervasive in our daily lives when affixed to everyday consumer items as "smart labels". While yielding great productivity gains, RFID systems may create new threats to the security and privacy of individuals or organizations. This paper presents a brief description of RFID systems and their operation. We describe privacy and security risks and how they apply to the unique setting of low-cost RFID devices. We propose several security mechanisms and suggest areas for future research.

IV. IMPLEMENTATION & RESULTS

It requires Xilinx software where Verilog source code can be used for design implementation. Simulation is performed before synthesis process to verify RTL code and to confirm that the design is functioning as intended. Using the above architecture verilog code is developed and simulated on Xilinx tool for its functional verification which is shown below fig. 5.

Simulation Result:

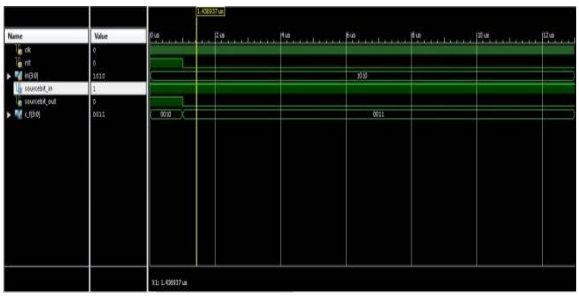

Fig . 3. Simulated Waveform

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Synthesis Result:

The developed project is simulated and verified their functionality. Once the functional verification is done, the RTL model is taken to the synthesis process using the Xilinx ISE tool. In synthesis process, the RTL model will be converted to the gate level netlist mapped to a specific technology library. This design is synthesized and its results were analyzed as follows.

RTL Schematic:

Xilinx ISE tool can be used to create, implement, simulate, and synthesize Verilog designs for implementation on FPGA chips.

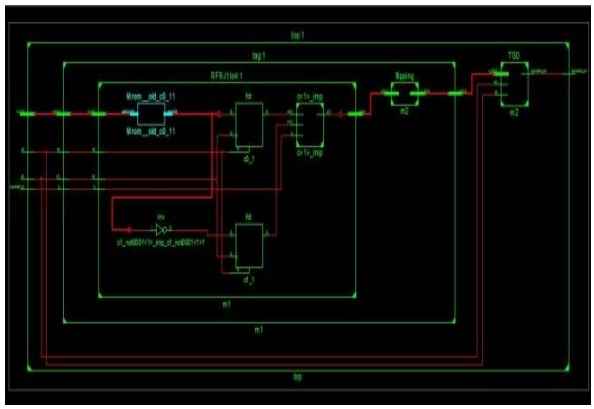

Fig. 4. RTL Schematic

TECHNOLOGY Schematic:

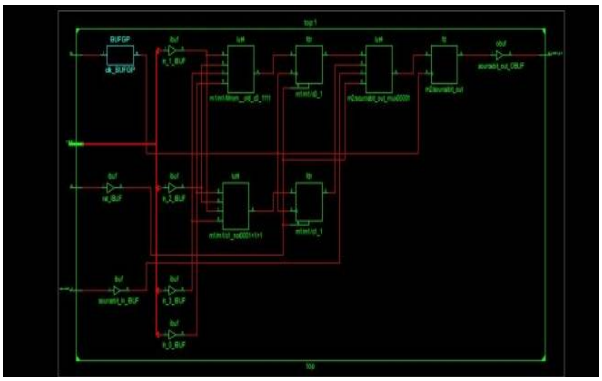

Fig. 5. Technology Schematic

Device Utilization Summary:

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	2	960	0%
Number of Slice Flip Flops	3	1920	0%
Number of 4 input LUTs	3	1920	0%
Number of bonded IOBs	8	66	12%
Number of GCLKs	1	24	4%

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Timing report:

```
Data Path: m2/sourcebit_out to sourcebit_out
                           Gate     Net
  Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
  ----------------------------------------  ------------
   FD:C->Q               1   0.514   0.357  m2/sourcebit_out (m2/sourcebit_out)
   OBUF:I->O                 3.169          sourcebit_out_OBUF (sourcebit_out)
  ----------------------------------------
  Total                      4.040ns (3.683ns logic, 0.357ns route)
                                     (91.2% logic, 8.8% route)
```

V. CONCLUSION

The proposed Reliable and Cost Effective Anti-collision technique (RCEAT) is designed to achieve a reliable and cost effective identification technique of the tag. The RCEAT architecture consists of two main subsystems; PreRCEAT checks error in the incoming packets using the CRC scheme. PostRCEAT identifies the error free packets using Binary Tree based technique. The architecture has been synthesized using Xilinx Synthesis Technology (XST). The result shows that the architecture has smaller cell area, power Consumption and number of gates. Therefore minimize the implementation and operating costs.

REFERENCES

[1] Y. Li and X. Ding, "Protecting RFID communications in supply chains," inProc. 2nd ACM Symp. Inf., Comput. Commun. Security, 2007, pp. 234–241.
[2] H. K. H. Chow, K. L. Choy, W. B. Lee, and K. C. Lau, "Design of a RFID case-based resource management system for warehouse operations,"Expert Syst. Appl., vol. 30, no. 4, pp. 561–576, Feb. 2006.
[3] A. Juels,"RFID security and privacy: A research survey," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 381–394, 2006.
[4] W. Choi, M. Yoon, and B.-h. Roh, "Backward channel protection based on randomized tree-walking algorithm and its analysis for securing RFID tag information and privacy,"IEICE Trans., vol. 91-B, no. 1, pp. 172–182, 2008.
[5] T.-L. Lim, T. Li, and S.-L. Yeo, "Randomized bit encoding for stronger backward channel protection in RFID systems," in Proc. IEEE 6th Annu. Int. Conf. Pervasive Comput. Commun., 2008, pp. 40–49.
[6] K. Sakai, W.-S. Ku, R. Zimmermann, and M.-T. Sun, "Dynamic bit encoding for privacy protection against correlation attacks in RFID backward channel,"IEEE Trans. Comput., vol. 62, no. 1, pp. 112–123, Jan. 2013.
[7] L. Sang, "Designing physical primitives for secure communication in wireless sensor networks," Ph.D. dissertation, Department of Computer Science and Engineering, The Ohio State University, 2010.
[8] M. Jain, J. L. Choi, T. M. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," inProc. 17th Annu. Int. Conf. Mobile Comput. Netw., 2011, pp. 301–312.
[9] A. D. Wyner,"The wire-tap channel," Bell Syst Tech. J., vol. 54,no. 8, pp. 1355–1387, 1975.
[10] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," inProc. ACM SIGCOMM Conf., 2011, pp. 2–13.
[11] H. Delfs and H. Knebl,Introduction to Cryptography: Principles and applications, 2nd ed. New York, NY, USA: Springer, 2007.