International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

# An Advanced Encoding and Decoding Scheme for Secure Communications in RFID Systems

**C.Sabitha & m. V. Maheswara Reddy**

Department Of Ecesri Satyanarayana Engineering College (Approved By Aicte, Affiliated To J. N. T. U.K, Kakinada Ongole 523001, A.P

Associate Professordepartment Of Ece Sri Satyanarayana Engineering College (Approved By Aicte, Affiliated To J. N. T. U.K, Kakinada Ongole 523001,A.P.

***ABSTRACT***

*Privacy protection is the primary concern when RFID applications are deployed in our daily lives. Due to the computational power constraints of passive tags, non-encryption-based singulation protocols have been recently developed, in which wireless jamming is used. However, the existing private tag access protocols without shared secrets rely on impractical physical layer assumptions, and thus they are difficult to deploy. To tackle this issue, we first redesign the architecture of RFID system by dividing an RF reader into two different devices, an RF activator and a trusted shield device (TSD). Then, we propose a novelcodingscheme,namely Random Flipping Random Jamming (RFRJ), to protect tags' content. Unlike the past work, the proposed singulation protocol utilizes only the physical layer techniques that are already implemented. Analyses and simulation results validate our distributed architecture with the RFRJ coding scheme, which defends tags' privacy against various adversaries including the random guessing attack, correlation attack, ghost-and-leech attack, and eavesdropping.*

## INTRODUCTION

RADIO enable a tremendous amount of applications, such as frequency identification (RFID) technologies supply chain management [1], electric transportation payment, and warehouse operations [2]. 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 singulation [3] are not practical. Instead of relying on the traditional cryptographic operations, recent works [4], [5], [6] employ physical layer techniques i.e., jamming [7], to protect tags' data. With this approach, tags could be securely identified without preexchanged shared keys.
The issue with the existing solutions, the privacy masking [4], randomized bit encoding (RBE) [5], and dynamic bit encoding (DBE)/optimized DBE (ODBE) [6], 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 vise versa. In other words, depending on the 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 code word. 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 ghostand-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 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 nonencryption-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 code word and keeps the index of the 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.
The rest of this paper is organized as follows. Section provides background knowledge for this research. We design a new RFID architecture in Section 3, and propose the RFRJ coding scheme in Section 4. Generalization of the RFRJ coding scheme is discussed in Section 5. Security analyses are provided in Section 6 and simulation results are demonstrated in Section 7. In Section 8, we review existing works for RFID security. Section 9 concludes this paper.

**PhysicalLayerSecurity**

Jamming is widely used for secure communications at the physical layer level, in which jamming signals corrupt receiving signals. Although this indicates that alegitimatereceiver cannot decode received signals due to jamming, the full-duplex mode of wireless antennas allows the receiver to simultaneously transmit jamming signals and receive data. This can be done by canceling self-interference, in which transmitting signals interrupt receiving signals. According to [8], the current implementation can cancel self-interference up to 45 dB across 40 MHz. Therefore, with jamming techniques, an eavesdropper cannot steal communications unless it is in close proximity to a jamming source node. It is known that perfect secrecy is possible without shared secrets by degrading the signal at an eavesdropper relative to that at the legitimate receiver [9]. Thus, jamming is a physical layer security technique suitable to wireless sensor networks where encryption-based security systems are not practical due to the power constraints of sensor nodes.

**Distributed RFID Systems**

In the traditional RFID system, an RF reader has two components, a transmitter (i.e., query transmission/energizing tags) and a listener (i.e., listening to a tag's reply) as shown in Fig. 1a, where a diamond represents the transmission function of a reader, a circle represents the listening function of a reader, and a rectangle represents a tag. The communication range of the backward channel is much shorter than that of the forward channel, and thus readers must be deployed based on the short-range backward channel to access all tags in the region as shown in Fig. 2a.

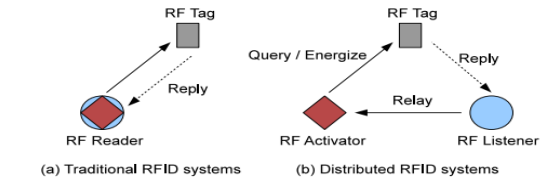


Fig. 1. Distributed RFID systems.

A recent study proposes Distributed RF Sensing model [12] that employs two kinds of devices (a single RF transmitter and a number of RF listeners) for each function of a reader as shown in Fig. 1b. The

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

model contributes to cost reduction of RFID system deployment. For example, in Fig. 2, the traditional RFID system requires nine transmitters and nine listeners, while the distributed RFID system requires one transmitter and nine listeners

## PROJECT DESCRIPTION

### 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 in [7], [13], [14]. On the other hand, there is no implementation of the backward channel protection methods in [4], [5], [6]. Therefore, our assumptions are much more practical than the past research.

### New RFID System Architecture

Similar to [12], an RF reader is divided into two components, an RF activator and a trusted shield device (TSD). In our new architecture, an RF activator queries a tag with a long-range signal (i.e., the forward channel) and energizes the tag. A TSD receives a tag's reply with a short-range signal (i.e., the backward channel), and it sends the reply to the activator via an encrypted channel, which we define as the relay channel. In typical RFID applications, a reader forwards tags' data to the back-end server. For simplicity, in this paper we consider the RF activator as the final destination of a tag's data by assuming the activator forwards collected data to the back-end server. A TSD works as an RF listener and it is

Fig. 2. Distributed RFID system deployment.

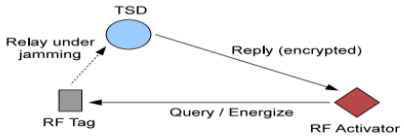


Fig. 3. The proposed RFID architecture.

A TSD is conceptually similar to the trusted masking device in [5] and a medical device shield implemented in [10], but different in the following functions. On overhearing a query from an activator to a tag, a TSD jams a bit in a codeword. As mentioned in the assumption, bit level jamming is possible. If an unauthorized reader tries to access a tag, a TSD jams against all bits of code words so that the unauthorized reader cannot read the content of the transmitted data. A similar function is implemented in [10], where a shield device jams the whole communication on detecting unauthorized accesses. This can be done by letting an authorized activator communicate with a TSD before a singulation process. Unlike the trusted masking device and medical shield, a TSD intermediates only the backward channel. With our new architecture, we can achieve the following design goals

## RANDOM FLIPPING RANDOM JAMMING CODING

In this section, we present the random flipping random jamming coding scheme. 4.1 Definition let r be an RF activator, s be a TSD, andtbeanRFtag.Anactivator 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 Eð:Þ. 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 Dð:Þ, and forwards the data to the activator via the relay channel. In general, we call lb-to-lc the RFRJ coding scheme.Forinstance, the coding scheme with lb ¼ 1 and lc ¼ 4 is said to be the 1-to-4 RFRJ coding scheme. The notations utilized inthis paper are listed in Table 1.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

**Private Tag Access Protocol**

The proposed private tag access protocol works as follows. Suppose an RF activator r plans to read an RF tag t without disclosing the tag's ID to an eavesdropper. Inthis section, we first consider the length of the encoding unit lb to be 1. Our idea can be applied to arbitrary values of lb and lc, where lb < lc. On receiving a request, the tag t extends a bit into an l c-bit codeword, where lc 4 must hold. When the tag transmits data over the backward channel, it randomly selects a bit in a codeword and intentionally flips it. Note that this process is done before the tag sends out the codeword, so the data sent by the tag always contains a one-bit error. On the other hand, the TSD, which is an RF listener with jamming capability, jams a single bit in the codeword. The jamming causes the selected bit to flip. Let pj (0 pj 1) be the probability that the bit jammed by the TSD is flipped. We denote Is and It as the indexes of the selected bits by the TSD and the tag, respectively. The TSD randomly selects any bit in the first half of the l c bits codeword, i.e., 1 Is b1 2 lcc, while a tag randomly selects a bit in the second half of the codeword, i.e., b1 2 lcc þ 1 It lc. By doing this, we can guarantee that the TSD and the tag do not select the same bit. Thus, the codeword received by the TSD or an eavesdropper contains a two-bit error when jamming flips the Is-th bit and a one-bit error when jamming fails. For instance, in Fig. 4, a source bit is encoded into a 4-bit codeword. The tag flips the third bit in the codeword, which is colored gray, and the TSD selects the first bit for jamming, which is crossed off. Assume the original codeword is 1010. Since the tag flips the third bit, it will send 1000 over the backward channel. Meanwhile, the TSD jams the first bit. Hence, the TSD and the eavesdropper will receive X000, where X could be decoded to either 0 or 1. The TSD knows I s, and thus it knows one of the three bits may contain an error after excluding the jammed bit. However, the eavesdropper does not know which bit the TSD jammed or which bit the tag flipped. For the eavesdropper, two out of the 4 bits may contain errors. Thus, the TSD and the eavesdropper have a different amount of information to decode the original codeword. In general, for 1-to-lc, TSD knows that there is a 1-bit error out of ðlc 1Þ bits while the eavesdropper knows there is a two-bit error out of l c bits at best.

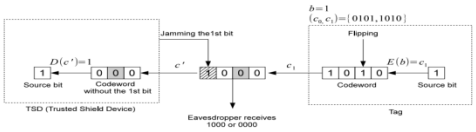
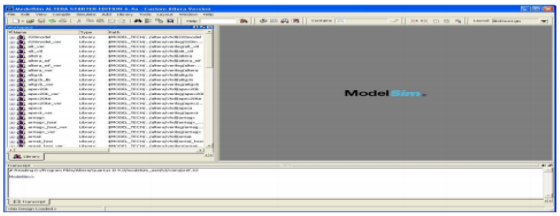
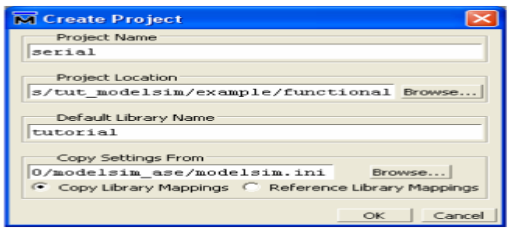


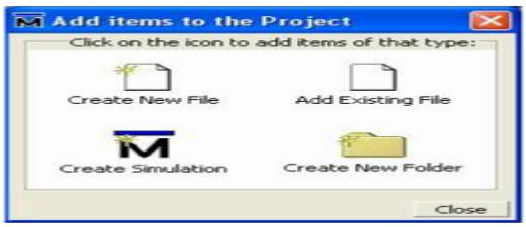
Fig. 4. The system model and basic idea.

**TOOL MODELSIM**Modelsim tool developed by Mentor Graphics is a verification and simulation tool. The installation of Modelsim tool which is used for Verilog, VHDL and System Verilog is explained in the below steps.






**Creating a new Project**Enter the project name, select the project location, select the default library and select ok. Your new project will be created with the specified name. An additional window will appear as soon as a new project is created as shown in the figure below.




**Add items to Project Window**

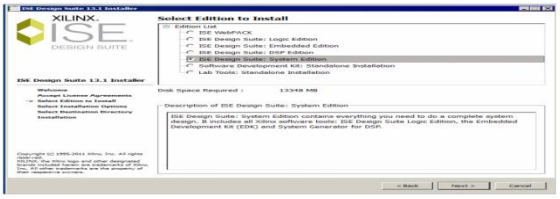
International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

When we create a new file or add an existing file, that particular file will be appeared in the workspace. The workspace window is shown in the figure below.


Figure 10. Workspace window after the project is created.

Now after adding all the designs into the project u may click on close to close the earlier add items to project window. U can now see the workspace window.

**TOOL XILINX**ISE design suite is a program tool developed by Xilinx to support their FPGAs. It also includes a bunch of other tools which are useful for creating your projects. ISE design suite is hold great importance to do any work because it actually synthesizes your designs into bit files that can be loaded into the FPGAs for testing of the designs.





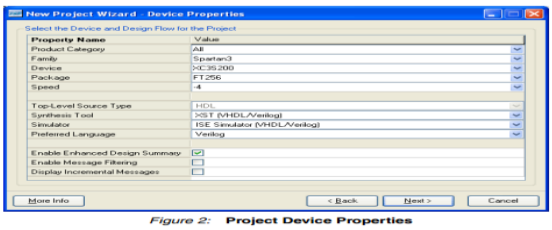



*Figure 2:* **Project Device Properties**

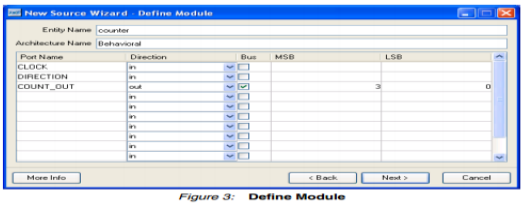



*Figure 3:* **Define Module**

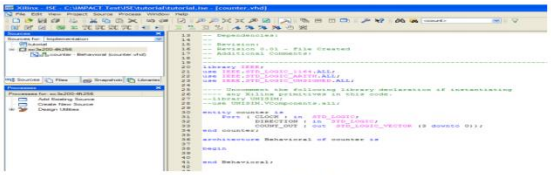


*Figure 4:* **New Project in ISE**

**Migrating Projects from Previous ISE Software Releases:**When you open a project file from a previous release, the ISE® software prompts you to migrate your project. If you click Backup and Migrate or Migrate only, the software automatically converts your project file to the current release. If you click Cancel, the software does not convert your project and, instead, opens Project Navigator with no project loaded.

**Note:** After you convert your project, you cannot open it in previous versions of the ISE software, such as the ISE 11 software. However, you can optionally create a backup of the original project as part of project migration, as described below

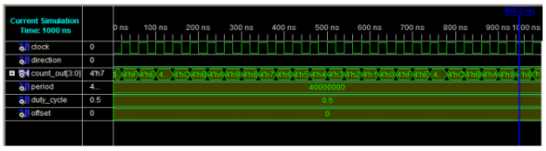



*Figure 10:* **Simulation Results**

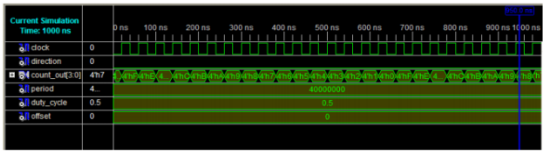



*Figure 10:* **Simulation Results**

**LANGUAGE VERILOG HDL**In the semiconductor and electronic outline industry, Verilog is an equipment portrayal language(HDL) used to show electronic frameworks. Verilog HDL, not to be mistaken for VHDL (a contending dialect), is most generally utilized as a part of the outline, confirmation, and usage ofdigital rationale chips at

the register-exchange level of reflection. It is likewise utilized as a part of the confirmation ofanalog and blended sign circuits.

**Overview:**Equipment portrayal dialects, for example, Verilog contrast from programming dialects on the grounds that they incorporate methods for depicting the proliferation of time and flag conditions (affectability). There are two task administrators, a blocking task (=), and a non-blocking (<=) task. The non-blocking task permits planners to portray a state-machine upgrade without expecting to pronounce and utilize transitory capacity variables (in any broad programming dialect we have to characterize some provisional storage rooms for the operands to be worked on along these lines; those are impermanent capacity variables). Since these ideas are a piece of Verilog's dialect semantics, architects could rapidly compose portrayals of expansive circuits in a generally minimal and succinct structure. At the season of Verilog's presentation (1984), Verilog spoke to a huge efficiency change for circuit originators who were at that point utilizing graphical schematic capturesoftware and uniquely composed programming projects to report and mimic electronic circuits. The originators of Verilog needed a dialect with grammar like the C programming dialect, which was at that point generally utilized as a part of designing programming advancement. Verilog is case-delicate, has a fundamental preprocessor (however less advanced than that of ANSI C/C++), and proportional control stream watchwords (if/else, for, while, case, and so on.), and perfect administrator priority. Syntactic contrasts incorporate variable affirmation (Verilog requires bit-widths on net/regtypes[clarification needed]), boundary of procedural squares (start/end rather than wavy props {}), and numerous other minor contrasts.

**System Verilog:**

System Verilog is a superset of Verilog-2005, with numerous new elements and capacities to help outline confirmation and configuration demonstrating. Starting 2009, the System Verilog and Verilog dialect models were converted into SystemVerilog 2009 (IEEE Standard 1800-2009). The appearance of equipment confirmation dialects, for example, OpenVera, and Verisity's e dialect empowered the improvement of Superlog by Co-Design Automation Inc. Co-Design Automation Inc was later bought by Synopsys. The establishments of Superlog and Vera were given to Accellera, which later turned into the IEEE standard P1800-2005: SystemVerilog. In the late 1990s, the Verilog Hardware Description Language (HDL) turned into the most generally utilized dialect for portraying equipment for recreation and combination. On the other hand, the initial two forms institutionalized by the IEEE (1364-1995 and 1364-2001) had just straightforward develops for making tests. As configuration sizes exceeded the check capacities of the dialect, business Hardware Verification Languages (HVL, for example, Open Vera and e were made. Organizations that would not have liked to pay for these devices rather burned through several man-years making their own particular custom devices. This profitability emergency (alongside a comparative one on the configuration side) prompted the making of Accellera, a consortium of EDA organizations and clients who needed to make the up and coming era of Verilog. The gift of the Open-Vera dialect framed the premise for the HVL elementss of SystemVerilog.Accellera's objective was met in November 2005 with the selection of the IEEE standard P1800-2005 for SystemVerilog, IEEE (2005).

**Software & Hardware Requirements—**

The softwares which are used for the implementation and simulation of the design are Xilinx Ise design suite 14.3 and Modelsim 6.4 minimum hardware requirements to test the functionality of design and simulation are:

**Processor:** Intel(R) core(TM) 2 CPU operating at 1.86 GHz

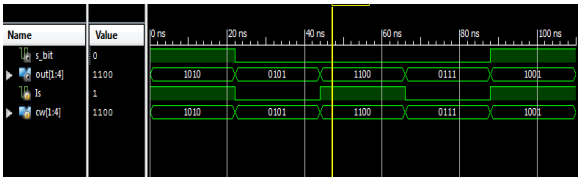
**RAM:** 2GB

**Operating System:** Windows7 (32-bit / 64-bit)

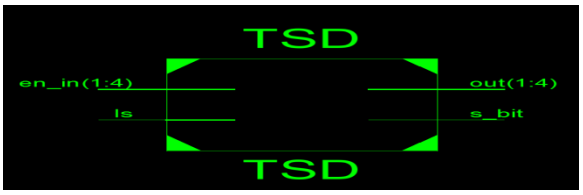
**Video Memory:** 512 MB

**SIMULATION RESULT**

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017



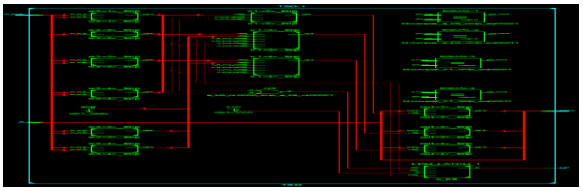

**RTL SCHEMATIC**




**BLOCK DIAGRAM TSD**

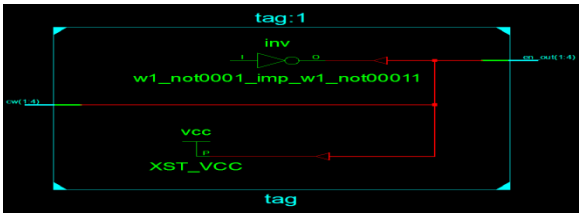
| Device Utilization Summary (estimated values) | | | |
|---|---|---|---|
| Logic Utilization | Used | Available | Utilization |
| Number of Slices | 1 | 704 | 0% |
| Number of 4 input LUTs | 1 | 1408 | 0% |
| Number of bonded IOBs | 7 | 108 | 6% |

**Summary Report of TSD**



**RTL Schematic of TSD**


**BLOCK Diagram of TAG**




**RTL schematic diagram TAG**

| Device Utilization Summary (estimated values) | | | |
|---|---|---|---|
| Logic Utilization | Used | Available | Utilization |
| Number of Slices | 1 | 704 | 0% |
| Number of 4 input LUTs | 2 | 1408 | 0% |
| Number of bonded IOBs | 9 | 108 | 8% |

**Summary Report of TAG**

## CONCLUSION

RFID systems serve as an enabling technology for the Internet of Things. However, security concerns of existing RFID systems have become a major obstacle for their wide adoption. The RFID protection mechanisms in the literature either work for only a few specific attacks or have unrealistic physical layer assumptions. In this paper, we first propose a novel distributed RFID architecture which divides the RF reader into two parts: an RF activator and a TSD, each tailoring for a specific function of an RF reader. In addition, we propose the RFRJ coding scheme, which when incorporated with the new architecture, works against a wide range of adversaries including the random guessing attack, correlation attack, ghost- and leech attack, and eavesdropping. The physical layer assumptions of the proposed RFID architecture and the encoding scheme are readily available. In addition, the hardware cost of the new architecture is theoretically cheaper than the existing RFID systems. Webelievetheproposed architecture will serve as the foundation of the next-generation RFID systems.

## REFERRENCES

[1] Y. Li and X. Ding, "Protecting RFID communications in supply chains," in Proc. 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," in Proc. 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," in Proc. 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.

12] D. D. Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: Towards distributed RFID sensing with software-defined radio," in Proc. 16th Annu. Int. Conf. Mobile Comput. Netw., 2010, pp. 97–104.

[13] L. Sang and A. Arora, "A shared-secret free security infrastructure for wireless networks," ACM Trans. Auton. Adaptive Syst., vol. 7, no. 2, pp. 23:1–23:21, 2012.
[14] L. Sang and A. Arora, "Capabilities of low-power wireless jammers," in Proc. INFOCOM, 2009, pp. 2551–2555.
[15] EPCglobal, EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID Protocol for communications at 860 MHz-960MHz version 1.0.9 [Online]. Available: http:www.epcglobalinc.org/standards, 2005.
[16] J. B. Wilker, "An extremum problem for hypercubes," J. Geometry, vol. 55, pp. 174–181, 1996.
[17] J. Myung, W. Lee, J. Srivastava, and T. K. Shih, "Tag-splitting: Adaptive collision arbitration protocols for RFID tag identification," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 6, pp. 763–775, Jun. 2007.
[18] A. Juels, R. Pappu, and B. Parno, "Unidirectional key distribution across time and space with applications to RFID Security," in Proc. USENIX Secur. Symp., 2008, pp. 75–90.
[19] M. E. Hoque, F. Rahman, and S. I. Ahamed, "AnonPri: An efficient anonymous private authentication protocol," in Proc. IEEE Int. Conf. Pervasive Comput. Commun., 2011, pp. 102–110.
[20] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in Proc. 1st Int. Conf. Security Pervasive Comput., 2003, pp. 201–212.
[21] S. A. Weis, "Security and privacy in radio-frequency identification devices," Master's Thesis, Department of Electrical Engineering and Computer Science, MIT, 2005.
[22] A. Czeskis, K. Koscher, J. R. Smith, and T. Kohno, "RFIDs and secret handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications," in Proc. 15th ACM Conf. Comput. Commun. Security, 2008, pp. 479–490.