Power Optimized And Low Dense Mutual Authentication Protocol For Universally Tolerable RFID Identification

S. Naga Mallikarjun [1], S. K. Khaleel Ahmed[2]
[1]*M.Tech Student, E.C.E Department, V.R.Siddhartha Engineering College, A.P, India,*
[2]*Associate Professor, E.C.E Department, V.R.Siddhartha Engineering College, A.P, India,*

ABSTRACT:

This document specifies the radio frequency communication interface and Reader commanded functionality requirements for an Auto-ID Center Class I radio frequency identification (RFID) Tag operating in the frequency range of 860MHz–930Mhz. A Class I tag is designed to communicate only its unique identifier and other information required to obtain the unique identifier during the communication process. This project describes a universally acceptable security framework tuned especially for RFID Applications. In this brief, gated driver tree technique is introduced to reduce power consumption .By making RFID-specific setup, communication, and concurrency assumptions, we arrive at a model that guarantees strong security, privacy and availability properties, while per-mitting the design of practical RFID protocols. The framework supports modular deployment, which is most appropriate for ubiquitous applications. As an instantiation of the proposed frame-work, this project describes a set of simple, efficient, secure and anonymous (untraceable) RFID identification and authentication protocols.

KEYWORDS:Mutual Authentication,A Class I tag ,E.P.C (Electronic product code),gated driver tree,Gloable network,Constellation,C.R.C, L.F.S.R

INRODUCTION:

Radio Frequency Identification (RFID) system is thelatest technology that plays an important role forobject identification as ubiquitous infrastructure. RFID has many applications in access control, manufacturing automation, maintenance, supply chain management, parking garage management, automatic payment, tracking, and inventory control. RFID is

the name given to all technologies that use radio waves to automatically identify and account transactions on people, animals or objects [1] by means of electromagnetic proximity [2]. RFID technology is not new, as one of its first usages dates from 1940 where a RFID-based Identification Friend or Foe (IFF) system was used [3]. One of the reasons that are difficulting the implantation of RFID technology is their cost. Tag price must be in the .05 - 0.1 ¤ range, to ease its use into common packaging. This severe price restriction implies that the use of traditional cryptographic primitives is not realistic. RFID is a pervasive technology, perhaps the most pervasive technologies in history. One of the main problems that ubiquitous computing has to solve before its wide development is privacy [4]. Products labeled with insecure tags reveal sensitive information when queried by readers. Readers are frequently not authenticated, and tags usually answer in a complete transparent way. Moreover, even if we assume that tag's contents are secure, tracking (violation of location privacy) protection is not guaranteed. Tags usually answer different queries with the same identifier. These predictable tag responses allow a third party to establish an association between tags and their owners. Even if tags only contain product codes, rather than an unique serial number, tracking can still be possible by using an assembly of tags (constellation)

EPCglobal is a member-driven organization composed of leading firms and industries that are focused on creating global standards for the EPCglobal Network. EPCglobal is now leading the development of industry-driven standards for the Electronic Product Code (EPC) Network to support the use of Radio Frequency Identification (RFID) in today's fast-moving, information rich trading networks [13].

RFID SYSTEM GENERAL COMMUNICATION OVERVIEW

The radio frequency (RF) communication interface and Reader commanded functionality requirements specified herein are for a reader talks first passive RFID system. AClass I Tag will communicate only when directed by a properly decoded and interpreted command emitted from a source other than the Tag itself. We will refer to any

such source as a Reader. The data symbols communicated between the reader and the tag are referred to as a binary zero(0), a binary one (1), a null, and punctuation. The Class I RFID Tags will communicate by using backscatter modulation only. The Class I RFID Tags will not modulate their backscatter signal except when directed to by a properly decoded and interpreted command emitted from a Reader. AClass I Tag will respond to all properly decoded and interpretedsignals regardless of emitting source (unless that source is the Tag itself).Communication occurs in a half-duplex manner. ATag shall not perform communication while it is waiting for communication from a Reader. ATag shall not interpret communication from a Reader while it is communicating. An RFID system consists of three different components: RFID tag or transponder, Reader or interrogator, and backend server.

RFID tag: is a tiny radio chip that comprises a simple silicon microchip attached to a small flat aerial and mounted on a substrate. The whole device can then be encapsulated in different materials (such as plastic) dependent upon its intended usage. The tag can be attached to an object, typically an item, box, or pallet, and read remotely to ascertain its identity, position, or state. For an active tagthere will also be a battery.

The electronic product code

Item identification through the use of numbering schemes has been established worldwide, mostly because of the introduction of barcode standards that serve as the foundation for optical scanning technology. Nowadays, nearly all products sold in supermarkets and department stores are equipped with a unique GS1 (formerly known as EAN/UCC) identification number which contains information on its manufacturer and product type encoded in a one-dimensional barcode. While barcode technology was originally developed in the 1970s for the retail industry, it became a standard in many other branches of trade as well, e.g. in the automotive and the aerospace industry, albeit many of them used the barcode as a vehicle for encoding proprietary data formats. The EPC was conceived as a novel numbering scheme to identify all kinds of physical objects, not just traded goods. The main requirement to the

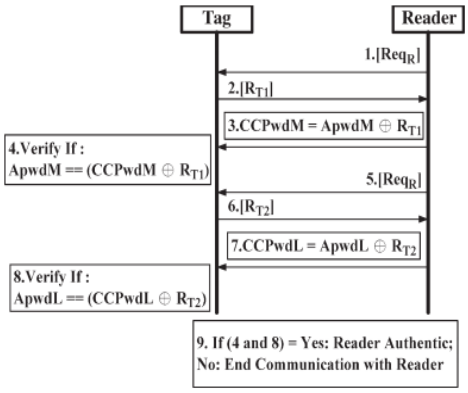
concept was that the EPC code must be sufficiently large to enumerate all objects, and to accommodate all current and future naming methods. In contrast to GS1 codes, the EPC was developed for unique identification on the item-level, i.e. each EPC-equipped object carries its own code that distinguishes it from other objects of the same type. For this purpose, the EPC is divided into hierarchically organised sections. Its total length is 96 b including an 8 b header for meta-data that declares the EPC type. The original EPC Type 1 contains three subsections, which provide information on the EPC manager (i.e. the manufacturer), the EPC object class (i.e. the product type) and a serial number (Figure 2). It is important to note that the EPC does not identify stock-keeping units only but pallets, containers and other logistical units. Since, the EPC was not made to replace but to integrate existing numbering schemes, different headers can be used for different schemes, e.g. the binary header sequence "11001111" indicates that following sections contain a UID number as it is used by the US DoD.

EPC Class-1 Gen-2 Standard:

An access password is required before data are exchanged between a reader and a single tag. The access password is a 32-b value stored in the tag's reserved memory. If this password is set, then the reader has to have the valid password before the tag will engage in a secured data exchange. These passwords can be used in activating kill commands to permanently shut down tags, as well as for accessing and relocking a tag's memory. To cover-code data or a password in Gen 2, a reader first requests a random number from the tag. The reader then performs a bitwiseXORof the data or password with this random number and transmits the cover-coded (also called cipher text) string to the tag. The tag uncovers the data or password by performing a bitwiseXORof the received cover-coded string with the original random number. In addition, the tag conforming to the EPC C1G2 standard can support only a 16-b PRNG and a 16-b CRC checksum that are used to detect errors in the transmitted data [4], [6]. Fig. 1 describes the EPCglobal C1G2 communication step between a reader and a tag. A detailed description of eachstep is as follows.

1) The interrogator issues a Req_RN and sends a request message to a tag.

2) The tag responds by backscattering a new 16-b random number RN16.



3) The interrogator then generates a 16-b ciphertext string comprising a bitwiseXORof the 16-b word to be trans-mitted with this new RN16, both MSB first, and issues the command with this ciphertext string as a parameter.

4) The tag decrypts the received ciphertext string by per-forming a bitwise XORof the received 16-b ciphertext string with the original RN16.

5) The interrogator issues a Req_RN to obtain a new RN16.

6) The tag responds by backscattering a different RN16.

7) The interrogator then transmits a 16-b ciphertext string

Generated from the 16 LSBs of the tag's access password XORed with the RN16 generated at step 6).

8) The tag performs a bitwiseXORoperation of the received 16-b ciphertext string and the RN16 to decrypt the received ciphertext string for verification.

Modified Konidala et al. Mutual Authentication Scheme:

Modified Konidalaet al.[10] utilized the tag's 32-b access and kill passwords in achieving tag–reader mutual authentication. Their scheme uses two rounds of PadGen to compute a cover-coding pad. The first round performs PadGen over the access password, while the second round performs PadGen over the kill pass-word. The PadGen function is used to create the 16-b pads for"cover coding" the access password.In the Modified Konidalaet al.[10] authentication scheme, as shown in Fig. 2, the reader issues a Req_RN command to the acknowl-edged tag. The tag then generates two 16-b random numbers, namely,RT1andRT2, and backscatters

them with its EPC to the reader. The reader forwards these messages to the manufac-turer. The manufacturer matchesthe received EPC to retrievethe tag's access password (Apwd) and kill password (Kpwd) from the back-end database. The manufacturer then generates and stores two 16-b random numbers, namely,RM1andRM2. The "cover-coded passwords" for the 16 MSBs (CCPwdM1) and the 16 LSBs (CCPwdL1) are computed by the PadGen(RTi,RMi)function fori=1,2. CCPwdM1, CCPwdL1, andEPC along with four 16-b random numbers, namely,RM1, RM2,RM3, andRM4, generated by the manufacturer are trans-mitted to the reader, which, inturn, forwards them to the tag for verification. To authenticate the tag, the tag generates another two random numbers RT3 andRT4 along with the received RM3 andRM4 used to compute CCPwdM2 and CCPwdL2 with the PadGen(RTi,RMi)function fori=3,4. CCPwdM2, CCPwdL2, and EPC along with two 16-b random numbers, namely,RT3andRT4, are transmitted to the reader, which, in turn, forwards them to the manufacturer for verification. The Modified Konidalaetal.scheme offers greater resistance against Lim and Li's attacks [12]. This scheme is also much more difficult for an adversary to recover the access password under the correlation attack or to forge successful authentication under the dictionary attack.

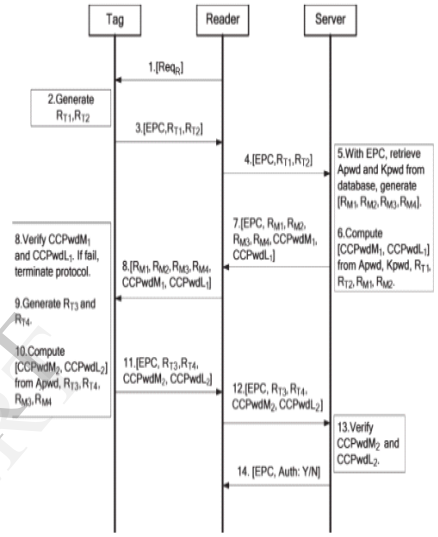


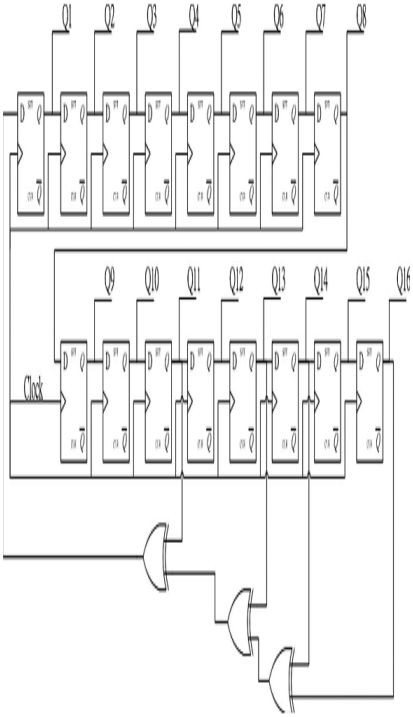
Figure.2

SECURITY ISSUES IN PROPOSED METHODOLOGY:

For accessing password authentication; two structures are implemented by using L.F.S.R. (Linear Feedback Shift Register) and C.R.C. (Cyclic Redundancy Check).

32 bit Accessing Password is divided in to two halves. First half Part is protected by L.F.S.R as well second half is protected with C.R.C.

L.F.S.R Implementation:



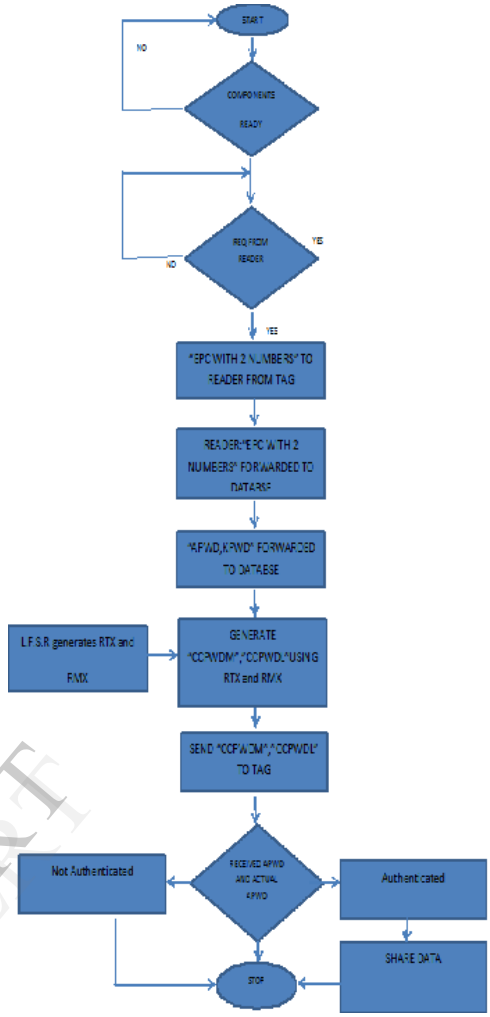


Fig:3

The PadGen function is the key function used to produce a cover-coding pad to mask the tag's access password before transmission. Theimplementation of the Pad Gen function also requires the random number generator to produce RTx and RMx. A typical 16-b linear feedback shift register (LFSR) is used to generate pseudorandom numbers.

An LFSR with a well-chosen feedback function can produce a sequence of bits that appears random and has a very long cycle. For an n-bit LFSR, the LFSR can generate a(2 n−1)-b-long pseudorandom sequence before repeating. A maximum-length LFSR produces anm-sequence (i.e., cycles through all possible 2 n−1states within the shift register except the state where all bits are zero).

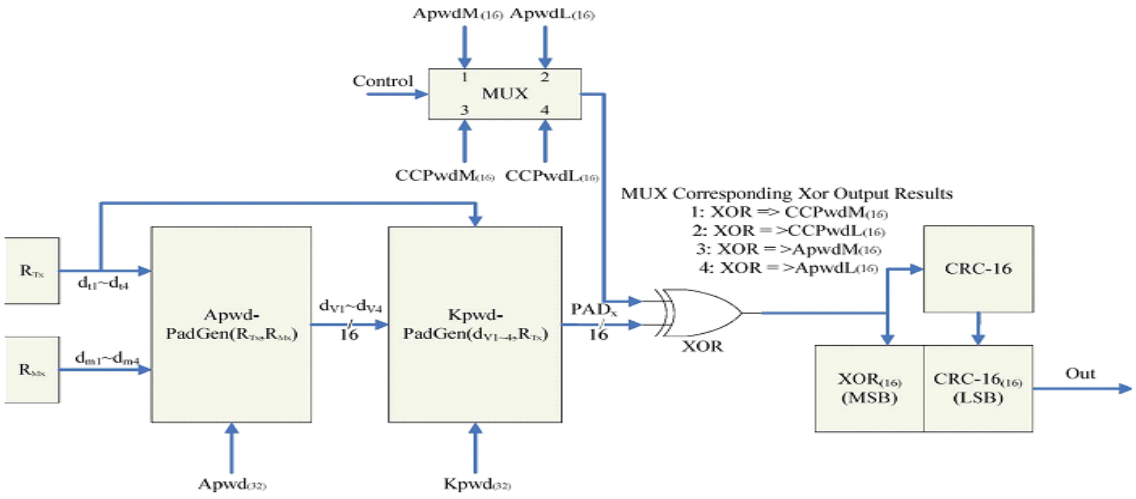
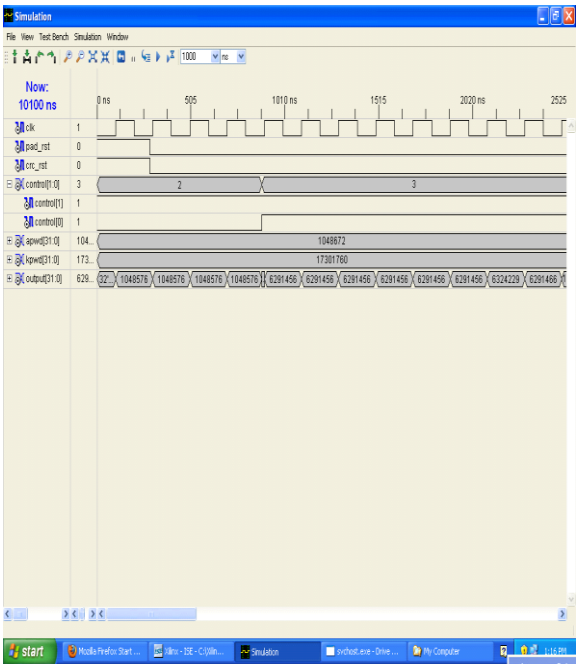


Fig.4

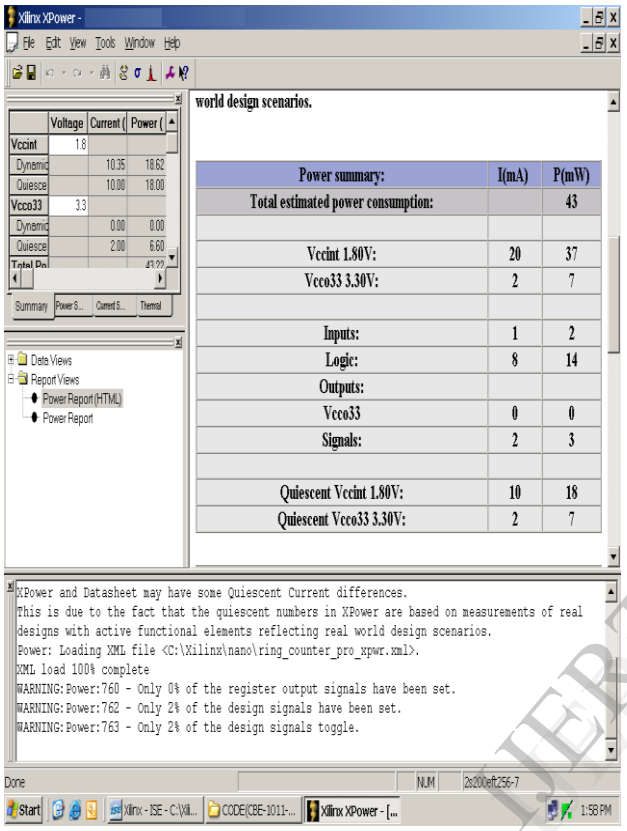
However, an LFSR with a maximal period must satisfy the fol-lowing property: The polynomial formed from a tap sequence plus the constant 1 must be a primitive polynomial modulo 2 [26]. In this paper, the Fibonacci LFSR was implemented because it is more suitable for hardware implementation than the Galios LFSR. The feedback polynomial is x16+x14+ X 13+x 11+1. The architecture of the 16-b random number generator is shown in Fig. 3. The block diagram of the PadGen function in the mu-tual authentication scheme is shown in Fig. 4.

SIMULATION RESULTS:

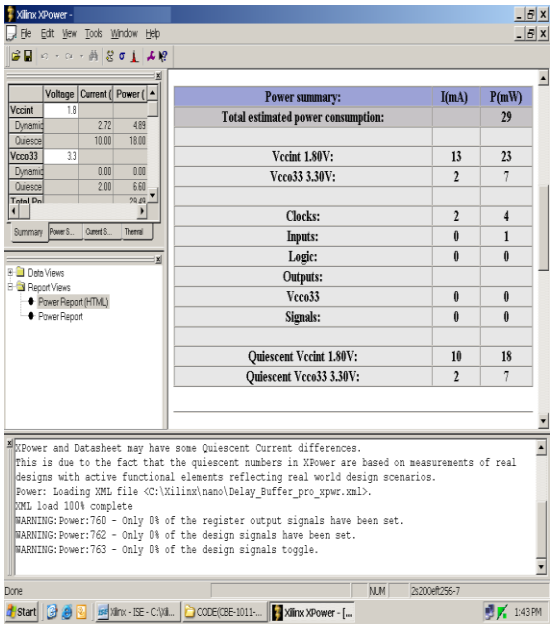


SYNTHESIS RESULT:

POWER REPORT EXISTING:



POWER PROPOSED:



DEVICE UTILIZATION SUMMARY

Selected Device: 3s100etq144-4

Number of Slices: 180 out of 960 18%

Number of Slice Flip Flops: 222 out of 1920 11%

Number of 4 input LUTs: 266 out of 1920 13%

Number of IOs: 63

Number of bonded IOBs: 63 out of 108 58%

Number of GCLKs: 2 out of 24 8%

TIMING SUMMARY

Speed Grade: -4

Minimum period: 8.741ns (Maximum Frequency : 114.410MHz)

Minimum input arrival time before clock : 4.845ns

Maximum output required time after clock : 4.450ns

CONCLUSION:

A new protocol not only resistant to standard passive attacks but also resistant to active attacks is proposed. Another interesting property is that tags canbe temporally deactivated without data loss.Instead of beginning from

scratch, we have tried to avoid past errors in the designing of our protocol. Because the EPC Gen2 standard for Class 1 tags supports only a very basic security level, three different types of pad-generation function were examined for tag–reader mutual authentication protocol in the RFID system environment. The proposed scheme is feasible in improving the weakness of the EPCglobal C1G2 communication authentication scheme with less power consumption.

FEATURE SCOPE:

The scale of the systems and high data flows of RFID will be introduced and increased by presenting a synchronous long range communication protocals by implementing an efficient modulation schemes. User perception of security and privacy will continue without any disturbance.

REFERENCES:

1. Juels, A.: RFID security and privacy: A research survey. Manuscript (2005)

2. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J., Ribagorda, A.: RFID systems: A survey on security threats and proposed solutions. In: Proc. of PWC06. Volume 4217 of LNCS. (2006) 159–170

3. Piramuthu, S.: Protocols for RFID tag/reader authentication. Decision Support Systems 43(3) (2007) 897–914

4. Sarma, S., Weis, S., Engels, D.: RFID Systems and Security and Privacy Implications. In: Proc. of CHES'02. Volume 2523., LNCS (2002) 454–470

5. Choi, E., Lee, S., Lee, D.: Efficient RFID authentication protocol for ubiquitous computing environment. In: Proc. of SECUBIQ'05. LNCS (2005)

6. Henrici, D., M¨uller, P.: Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In: Proc. of PERSEC'04.(2004) 149–153

7. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic approach to "privacy-friendly" tags. In: Proc. of RFID Privacy Workshop. (2003)

8. Yang, J., Park, J., Lee, H., Ren, K., Kim, K.: Mutual authentication protocol for low-cost RFID. Proc. of RFIDSec'05 (2005)

9. Molnar, D., Wagner, D.: Privacy and security in library RFID: Issues, practices, and architectures. In: P

roc. of ACM CCS'04. (2004) 210–219