Secured Mutual Authentication Protocol for Radio Frequency Identification Systems

C. Kalamani, S. Sowmiya, S. Dheivambigai, G. Harihara Sudhan

***Abstract*—**Radio Frequency Identification (RFID) is a blooming technology which uses radio frequency to track the objects. This technology transmits signals between tag and reader to fetch information from the tag with a unique serial identity. Generally, the drawbacks of RFID technology are high cost, high consumption of power and weak authentication systems between a reader and a tag. The proposed protocol utilizes less dynamic power using reversible truncated multipliers which are implemented in RFID tag-reader with mutual authentication protocol system to reduce both leakage and dynamic power consumption. The proposed system was simulated using Xilinx and Cadence tools.

***Keywords*—**Mutual authentication, protocol, reversible gates, RFID.

I. Introduction

THE RFID is a recent technology that utilizes radio frequency to track object by transmitting a signal with unique serial identity. RFID has been used in multiple environments such as access control system, electronic traceability, food traceability and product anti-counterfeiting [1]. Many colleges and universities have set up digital campuses, provided basic security alarms and other information technologies combined with the construction or renovation of campus facilities, campus cards including access control systems, firefighting systems, etc.

There are varieties of RFID authentication protocols for privacy and security of the RFID systems using a one-way hash function. The protocols work with a static identifier to protect privacy and security and can work better in a ubiquitous environment. Properties of pseudorandom binary sequences are important in many areas of communications and computing, such as cryptography, spread-spectrum communications, error-correcting codes, and Monte Carlo integration. Linear feedback shift registers (LFSRs) provide an economical, fast, and efficient method for generating a wide variety of pseudo random sequences.

A RFID tag is a vital element of the equipment [2]. It has minimum two modules:

1. An integrated circuit consists of RF transceiver and carrying out other roles;
2. An RF transceiver antenna.

The RFID system consists of three components: tag, reader and backend database. The unique identification tag information is transmitted to the reader via radio frequency communication without any processing. The tag transmits its own unique identification information when there is a query in any reader. Communication between a b1ack-end server and reader is secure.

RFID consists of active and passive tags. Passive tag collects energy from nearby RFID readers interrogating radio waves. Active tags have local power source (battery) and it can operate up to hundreds of meter from RFID reader. RFID is one of the methods of Automatic Identification and Data Capture (AIDC).

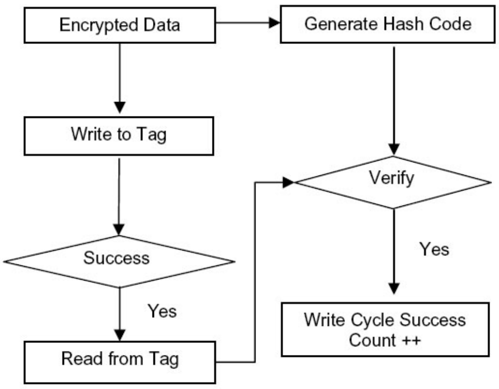

Fig. 1 Flow diagram of passive RFID Tag/Reader

Fig. 1 shows read and write steps for RFID Tag/Reader. The write and read steps are follows:

1. Earlier announcement of the novel data can be directed to the tag, here it generates the hash code and this key and data are stored.
2. The program writes the original data to the tag in form of blocks of 4 bytes each.
3. If the reader returns a flag for the write operation, then the program desires the reader to acquire the real tag data.
4. The program produces the tag data's hash code and relates it with the original data's hash code to decide if two groups of data equal, it is believed as completion of the write cycle.

The step used for read is as:

1. The program reads the data from the tag.
2. It relates the hash code of the tag's data and the hash code generated by the original data [3].

There are three types of RFID system: low frequency, high frequency and ultra-high frequency. It also consists of Microwave RFID. Low-frequency RFID system ranges from

C. Kalamani is from ECE department, Dr. Mahalingam College of Engineering and Technology, Coimbatore, India.(Corresponding author; phone: 09688077825; e-mail: kalamec18@gmail.com).

Sowmiya S., Dheivambigai S., and Harihara Sudhan are from ECE department, Dr. Mahalingam College of Engineering and Technology, Coimbatore, India (e-mail: sowmiyas@gmail.com, sdheivambigai@gmail.com, hari@gmail.com).

30 KHz to 500 KHz, the typical frequency is 125 KHz. High frequencies RFID ranges from 3 MHz to 30MHz, typical HF frequency is 13.56 MHz. Ultra-High frequency ranges from 300 MHz to 960 MHz with typical frequency of 433 MHz. Microwave RFID system runs at 2.45 GHz [3], [4].

RFID uses electromagnetic field to track tag with data. Readers have the control block and the high frequency (HF) interface with transmitter and receiver. Reader communication is based on the cover-code the data or a password, reader first requests a random number from the tag. The reader performs the encoding process of the data or password with the random number and transmits the cover-coded (also called cipher text) password to tag. On the other side tag will perform the same encoding process. If the cover-coded password from the tag and reader are equal, the communication continues. A back-end database is used to stores related data with tag substances.

RFID tags are also responding to the request signal. This carries dangers of unlicensed contact and alteration of tag data. An undefended tag may be susceptible to spying, transportation scrutiny, fooling.

For the encoding process, the protocol architecture consists of LFSR, 8 bit EXOR and a truncated multiplier. LFSR has Galois representation and Fibonacci configuration with 16 bit pseudorandom sequence. Fibonacci LFSR is more suitable for hardware implementation than Galois LFSR. LFSR is used to generate random numbers. Truncated multiplier is used for encoding purpose in the protocol architecture. When comparing the existing protocol consists of truncated multiplier with the proposed protocol using reversible gates, it is hardware efficient and consumes less dynamic power.

To propose a secured mutual authentication protocol the power of the proposed protocol should be reduced when compared to the existing protocol. The proposed protocol consists of reversible gates which are used to reduce the power dissipation.

II. Literature Survey

The security of the tag-reader mutual authentication can be improved in many ways. But at the same time concentration is needed to reduce the three major parameters area, power and delay. There are so many methods which are extracted from different journals in different periods. The following survey is mainly focused on the security, area and power.

The proposed is a simple and cost-effective RFID tag-reader mutual authentication scheme [4]. This scheme adheres to two ratified standards: EPC global architecture framework specification and EPC global class 1 gen 2 UHF RFID protocol. This scheme utilizes tag's access and kill passwords for the tag-reader mutual authentication scheme based on the EX-OR operation and beware of cloned fake tags, malicious snooping readers and unauthorized tag's data manipulation. In this scheme, the tag's access password is never exposed even to the stockholder's reader. They will formally improve the security of their proposed scheme and analyze its performance on a RFID-based supply chain test-bed. However, the security level can be increased but the hardware cost and the power consumption is also increased.

In Hardware Implementation of RFID Mutual Authentication Protocol [5], it is said that widespread distribution of RFID tools may create new extortions to security and user privacy. The main drawback of RFID communication is the weak authentication system between the tag and reader. This gives detailed study about the RFID tag-reader and hardware implementation of the mutual authentication protocol for the RFID system. It was verified using the verilog hardware description language. Three diverse types of pad generation function were studied for tag-reader mutual authentication protocol in the RFID system situation. This architecture performs the PadGen function and tag's access and kills passwords in achieving tag-reader mutual authentication. This architecture has increased in gate count and power dissipation.

The electronic product code (EPC) class-1 generation-2 (C1G2) description has severe security complications as said in an efficient implementation of RFID mutual authentication protocol [5]. To overcome this weakness, Pad generation (PadGen) function is used to improve the security. This paper describes about two improved authentication protocols for generating the PadGen function. The experimental results show that the area and power consumption of MOD (Modulo arithmetic) scheme are higher than those of the XOR scheme. This is because the computation cost of PadGen for the MOD scheme is more than that of the XOR scheme. However, the security level can be increased for the MOD scheme by sacrificing the increase in the area and power consumption.

A mutual authentication protocol is defending against the various attacks by hash function-based methods [6]. An improved protocol is to avoid DoS and replay attacks using a shared PRNG algorithm between the server and tag to produce the same output that is used in updating the protocol values. Also, the confidentiality in the protocol is based on protecting the secret value data using reader ID (RID value), which is only known to a legitimate reader and server. The improved protocol of Chang et al. is considered to be efficient and secure against DoS attack, traceability, and forward secrecy. However, the proposed protocol has the same computational complexity as the general hash-based protocol.

An efficient Mutual Authentication Protocol for RFID systems [7] proposed that every RFID tag has a unique identification number. The possible privacy threats are information leakage of a tag, traceability of a consumer, DoS attack and impersonation of a tag. There would be a large number of complex hash computations in the database side for each and every tag to create a secret value. To reduce the computation overhead many protocols are used as group secret value for tags in the database side. This suggests a new authentication protocol which offers privacy and security in a more efficient manner using individual secret values for each tag and also escapes many complex hash operations in the database side. By the analysis of the proposed protocol, it requires a low storage, computation and communication cost but offers larger ranges of privacy and security protection.

The proposed Fibonacci and galois representations of feedback-with-carry shift registers [8] conclude that LFSRs provides an economical, fast and efficient method for generating a wide variety of pseudorandom sequences. Feedback-with-Carry Shift Register (FCSR) architecture is used to generate sequences similar to the "galois" architecture for the LFSR. The galois is more efficient than the Fibonacci architecture because the feedback computations are performed in parallel. Galois representation is simpler and its circuitry is faster than the Fibonacci. But Fibonacci architecture is more suitable for hardware implementation than the galois LFSR.

The proposed Mutual Distance Bounding Protocol [9] enables one entity to determine an upper bound on the physical distance to the other entity as well as to authenticate the other entity. It has been found that distance-based attacks like Mafia fraud become a threat in RFID systems. This paper asserts that distance bounding protocol provides a lower faults acceptance rate under Mafia-fraud attack. It is shown in two ways that their security margins have been over estimated. First they show that their analysis is not correct. Second they introduce a new attack that achieves a higher false acceptance rate. Furthermore they introduce a method that modifies existing protocol with unilateral authentication. But one serious disadvantage is that security analysis is flawed beyond some incorrect calculations.

The proposed an Ultralightweight RFID Reader-Tag Mutual Authentication discusses that in an RFID scheme [10], a tag with a sole ID is involved to an object and a reader can distinguish the object by recognizing the devoted tag. With this recognized tag ID, the reader can then recover the associated information of the item from the backend server database. The communication between the reader and tags is susceptible to attacks. This recommends an enhanced mutual authentication system using only ultra-lightweight operations to resist further attacks and/or realize lower communication, calculation, and tag memory overheads. Rabin algorithm is used to encrypt messages by executing one multiplication operation on a tag and to decrypt messages by executing one square root operation on a reader. This paper will lag in memory, energy and computation power.

A hardware implementation of tag-reader mutual authentication for RFID systems has been described [11], the weaknesses of RFID technology are costlier and authentication systems between a reader and a tag become weak. The protocol for RFID tag-reader mutual authentication system is hard wire competent and consumes less dynamic power. Truncated multipliers are realized in RFID tag-reader mutual authentication protocol schemes due to decrease in hardware cost and dynamic power. Experimental evaluation tells that the proposed protocol with truncated multipliers delivers more security than the former systems.

The proposed 2n-2k-1 Modulo Adder Based RFID Mutual Authentication Protocol with RFID plays a major role in the security system for secured data communication [12]. The main challenge in RFID based security system is to design a more secured, better area and power efficient encoder architecture for tag-reader mutual authentication protocol. The proposed encoder design utilized 2n-2k-1 Modulo adder for attaining greater security. Experimental results of the proposed scheme offer superior performances in terms of area, power and delay when compared with the existing schemes. The formal security investigation has been done using the Burrows-Abadi-Needham (BAN) logic to display that the proposed protocol is secured. The shortcoming of this encoder architecture was rise in cost. To overcome these disadvantages the truncated multiplier architecture is modified using reversible logic gates instead of irreversible logic gates as they dissipate less amount of power and thus dropping the overall power in the RFID system.

III. Existing Method

Fig. 2 shows the block diagram of existing method.

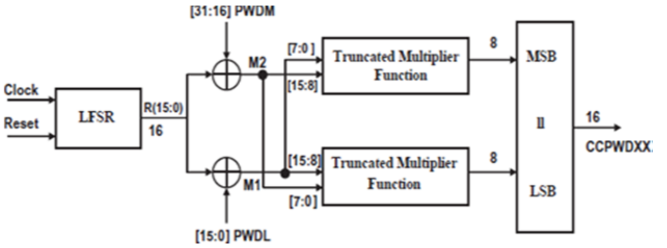

Fig. 2 Block Diagram of Existing method

The method consists of the 32 bit length password, a clock and a reset and 2 truncated multiplier. LFSR will produce a random number of 16 bit lengths. A two 8 bit Exor whose inputs are the random number and the lower and higher bits of the password which will generate the outputs M1, M2 of 16 bits long. The lower 8 bits of M1 and higher 8 bits of M2 are given to the first truncated multiplier and vice-versa to the second truncated multiplier. The major output of the truncated multipliers is concatenated to get the cover-coded password.

Truncated multipliers are used in RFID tag–reader mutual authentication protocol system to reduce hardware cost and dynamic power. A truncated multiplier is an n x n multiplier with n-bits output. In the truncated multiplier the n less significant bits of the full width product are discarded, some of the partial products are removed and replaced by a suitable compensation function. As more columns are eliminated, the area and power consumption of the arithmetic units are reduced and delay also decreased. There are two types of compensation function constant correction and variable correction method. Here we use constant correction method.

IV. Proposed Method

Fig. 3 shows the block diagram of proposed method. It consists of a 32 bit length password as input, a clock, a reset and 2 truncated multiplier which is designed using reversible logic. LFSR will produce a random number of 16 bit length. The random number is exor with the lower password bits (0-15) and results as M1. The random number is again exor with higher bits of the password to generate M2. The lower 8 bits of M1 and higher 8 bits of M2 are given to the first truncated multiplier and vice-versa to the second truncated multiplier. The major parts of the truncated multiplier output are concatenated to get the covercoded password.

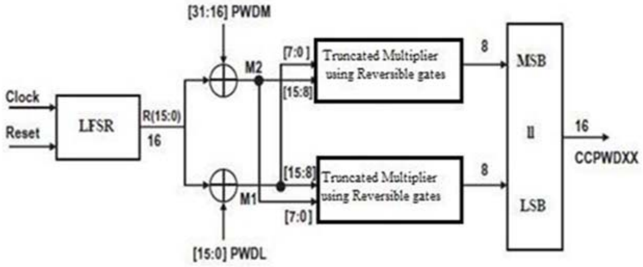

Fig. 3 Block Diagram of Proposed method

The proposed protocol is functioned same as the existing protocol. This protocol majorly aims to reduce the power dissipation. Hence the reversible gates were used in the truncated multiplier architecture. The results were remaining same as the existing. Only the power dissipation gets reduced and the security will get strengthen.

Steps used for Mutual Authentication are

1. Initially, reader sends a request message to a tag.
2. The tag responds by generating a new random number RTI.
3. The EPC, RT1information is sent to the server through the reader.
4. The server then computes a CCPWDRT (covercoded password computed by reader from RT1) from truncated multiplier function and generates new random number RM1 and transmitted to the tag.
5. The tag performs a truncated multiplier function with RT1 and PWD to compute CCPWDTT (covercoded password computed bytagfromRT1).
6. Verification of CCPWDRT = CCPWDTT is done. If it is satisfied, the process continues otherwise communication is ended.
7. The tag computes a CCPWDTM (covercoded password computed by tag from RM1) from truncated multiplier function, and the same is transmitted to the server.
8. The server performs a truncated multiplier function with RM1 and PWD to compute CCPWDRM (covercoded password computed by reader from RM1).
9. Verification of CCPWDRM = CCPWDTM is done. If it is satisfied, the process continues otherwise communication is ended.

Ideally, a reversible circuit has zero interior power dissipation since it does not miss data. A circuit is reversible if and only if the input vector can be uniquely recovered from the output vector. That is, there is a one-to-one correspondence between its input and output assignments [13]-[15]. So the truncated multiplier is designed using reversible logic to reduce the power dissipation.

V. Results

The existing and proposed methods are designed using Verilog program and simulated using Xilinx software. The simulated output existing methods is shown in Fig. 4.

Fig. 5 shows the schematic view of the existing methods. The simulation is done through NC sim simulator in Cadence tool using GPDK 90 nm technology.

The simulated output proposed methods is shown in Fig. 6.

Fig. 7 shows the schematic view of the proposed methods. The simulation is done through NC sim simulator in Cadence tool using GPDK 90 nm technology.

The power analysis is obtained using cadence EDA tool at 180 nm technology. The power analysis of both methods is given in Table I. The leakage and dynamic power are lesser than existing method by 34.87 nw and 186 nw respectively.

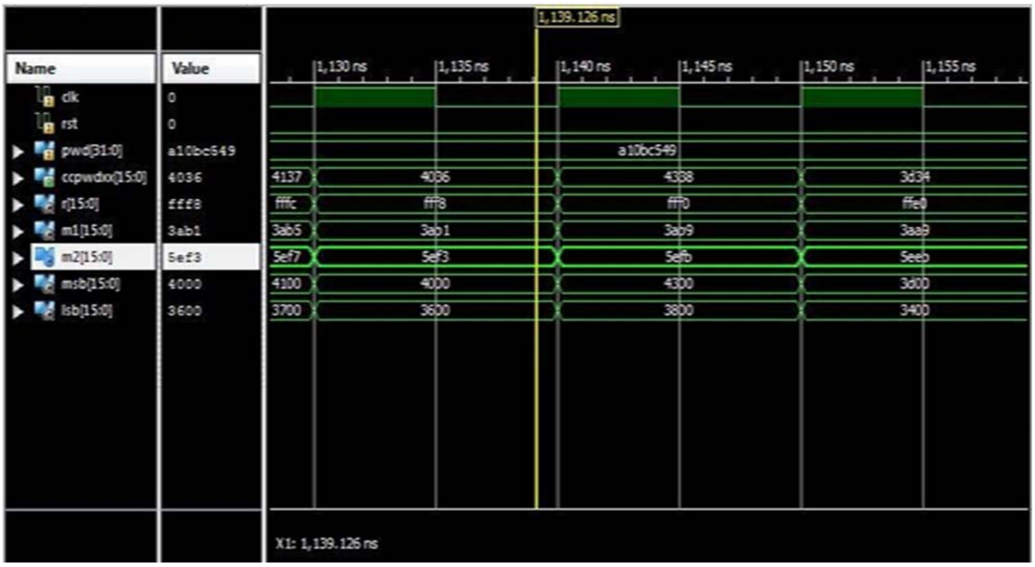
1,139.126 ns
Name
Value
1,130 ns
1,135 ns
1,140 ns
1,145 ns
1,150 ns
1,155 ns
clk 0
rst 0
pwd[31:0] a10bc549 a10bc549
ccpwdxx[15:0] 4036 4137 4036 4338 3d34
r[15:0] fff8 fffc fff8 fff0 ffe0
m1[15:0] 3ab1 3ab5 3ab1 3ab9 3aa9
m2[15:0] 5ef3 5ef7 5ef3 5efb 5eeb
msb[15:0] 4000 4100 4000 4300 3d00
lsb[15:0] 3600 3700 3600 3800 3400
X1: 1,139.126 ns

Fig. 4 Simulation output of existing protocol

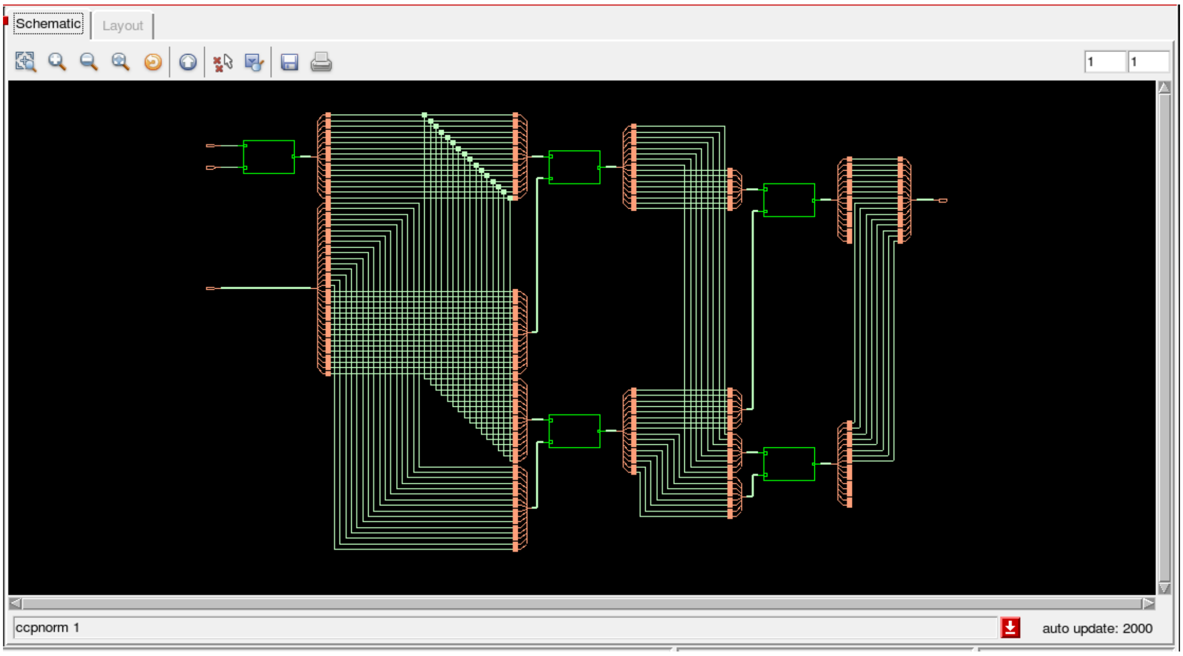

Fig. 5 Schematic of existing method

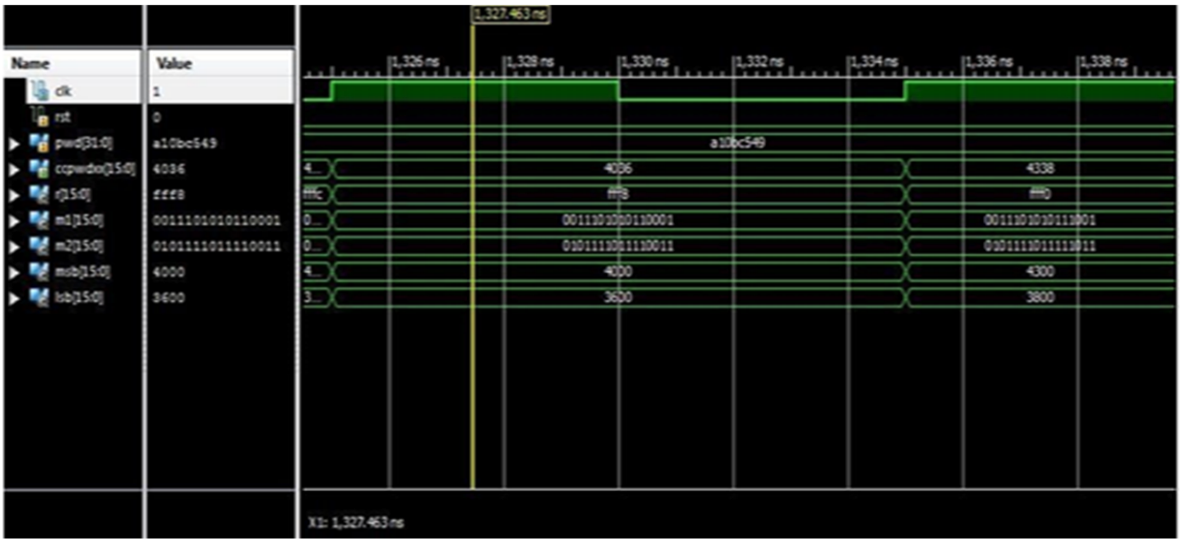

Fig. 6 Simulation output of proposed protocol

TABLE I
POWER ANALYSIS OF EXISTING AND PROPOSED METHODS

Parameter	Existing	Proposed	Difference
Leakage Power (nw)	12274.809	12239.938	34.871
Dynamic Power (nw)	605387.833	605201.825	186.008

TABLE II
ORIGINAL AND COVER CODED PASSWORD

Original password	A10BC549
Covercoded password	4036

The covercoded password is entirely different from the original password. Only who knows about the protocol architecture can able to decode the password. The protocol architecture was known only by the tag and reader. So, the man in the middle cannot fetch the information from the tag. Thus, security increases and also the power dissipation gets reduced, which is proved from table results (Tables I, II).

VI. CONCLUSION

Truncated multiplier using the reversible gates in the tag–reader mutual authentication protocol in the RFID is power efficient. Due to the mutual authentication scheme, the middle attackers are able to get the information from the tag. Thus the proposed protocol is well secured. This protocol outperforms the earlier schemes in terms of power dissipation as well as security.

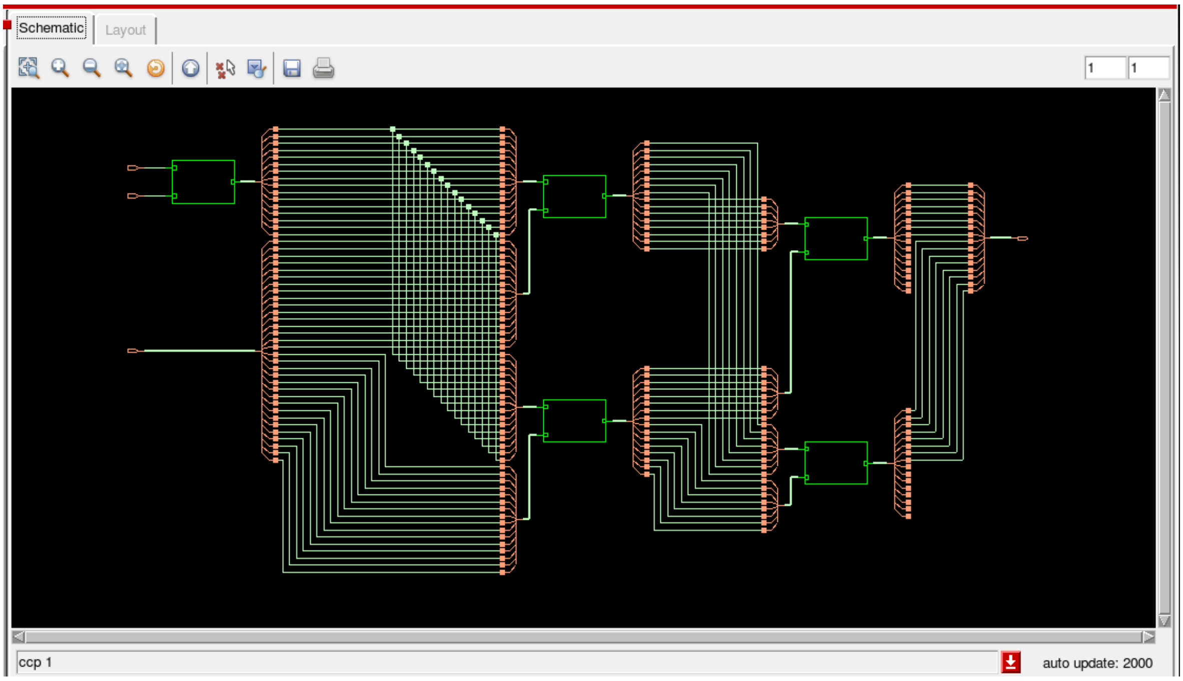

Fig. 7 Schematic of proposed method

References

[1] X.L. Jia, Q.Y. Feng, C.Z. Ma, “An efficient anti-collision protocol for RFID tag identification,” IEEE Communications Letters, vol.14, no.11, pp.1014-1016, 2010.

[2] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, New York: Wiley, 2010.

[3] Chih-Cheng Ou Yang, B.S. Prabhu, Charlie Qu, Chi-Cheng Chu, ‘Read / Write Performance for low memory passive HF RFID tag-reader system’, Journal of Theoretical and Applied Electronic Commerce Research,vol.4 ,no: 3 2009, pp-1-16.

[4] Kim. K, Kim. Z and Konidala D.M, “A simple and cost effective RFID tag–reader mutual authentication scheme”, in: Proceedings International Conference on RFID Security .year 2007, pp 141-152.

[5] Ching-Chien Yuan, Wei-Cheng Lin and Yu-Jung Huang, “Hardware Implementation of RFID Mutual Authentication Protocol”, IEEE Transactions on Industrial Electronics , vol.57,year 2010 pp 1573-1582.

[6] Chong Hee Kim and Gildas Avoine, “Mutual Distance Bounding Protocols”, IEEE Transactions on Mobile Computing, vol.12,year 2013 pp 830-839.

[7] Atkins. A, Yu. H and Md.M. Morshed, “Efficient Mutual Authentication Protocol for Radio Frequency Identification systems”, IET communications, vol.6, year 2012, pp 2715-2724.

[8] Andrew M. Klapper and Mark Goresky, “Fibonacci and Galois representation of Feedback-With-Carry Shift Registers”, IEEE Transactions on Information Theory, vol.48,year 2012, pp 2826-2836

[9] Chung Huang.Y u and Jehn-Ruey Jiang, “Ultralightweight RFID Reader-Tag Mutual Authentication”, IEEE 39th Annual International Computers, Software and Applications Conference, year 2015, pp-613-616.

[10] Jung-Sik Cho, Sang-Soo Yeo and Sung Kwon Kim, “Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value, computer communications”, vol.59, year 2012,pp 391-397.

[11] Elango. S and Vijaykumar V.R, “Hardware implementation of tag reader mutual authentication for RFID systems, Integration”, the VLSI journal, vol.3(2), year 2014, pp 1-7.

[12] Elango. S, Rajasekar. S, Ramakrishnan. S and Vijaykumar V.R, “Implementation of 2^n-2^k-1 Modulo Adder Based RFID Mutual Authentication Protocol”, IEEE Transactions on Industrial Electronics year 2017.

[13] M. Perkowski, A. Al-Rabadi, P. Kerntopf, A. Buller, M. Chrzanowska-Jeske, A. Mishchenko, M. Azad Khan, A. Coppola, S. Yanushkevich, V. Shmerko and L. Jozwiak, Ageneral decomposition for reversible logic, Proc. RM’2001, Starkville, (2001) pp. 119-138.

[14] M. Perkowski and P Kerntopf, Reversible Logic. Invited tutorial, Proc. EURO-MICRO, Warsaw, Poland, (2001).

[15] H. Thapliyal and M. B. Srinivas, Novel reversible TSG gate and its application for designing reversible carry look ahead and other adder architectures, Proceedings of the 10th Asia-Pacific Computer Systems Architecture Conference (ACSAC 05), Lecture Notes of Computer Science, Springer-Verlag 3740 (2005) 775-786.