International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Extended Privacy Protection with Flexible Architecture in RFID Using Variable Key Scheme

S. Bharathi[1], CH. Srigiri[2]
[1]*MTech VLSI&ES Department of ECE Godavari Institute of Engineering and Technology Rajahmundry, A.P*
[2]*Assistant professor Department of ECE Godavari Institute of Engineering and Technology Rajahmundry, A.P*

***Abstract:** This paper presents the design of RFID system with highly secured features. Privacy protection is the major concern when RFID applications are deployed in our daily lives. The existing RFID coding scheme namely random flipping random jamming (RFRJ) is used to protect tags content. But, when a bit flipping by jamming fails, eavesdropper decodes with probability 1. otherwise, it can successfully decode with probability 0.5 by random guessing. To overcome this problem, we redesign a RFID system with more secured features using variable key scheme. A survey and brief comparison of the algorithms are performed and the modified tea is selected as a feasible solution for encryption and decryption with an acceptable level of security. In this paper, implementation of variable key scheme (MTEA) RFID tag using VHDL simulations, corroborate the functionality of the protocols and techniques are compared in terms of timing, cost, security and performance. Potential improvements to enhance the security and strengthen RF communication during authentication are explored.*
***Index Terms:** RFID Security, RFRJ, Variable key scheme.*

I. INTRODUCTION

Radio frequency identification (RFID) is a rapidly developing field and technology that emerged in the last decade. This technology is employed by using implantable microchip devices also known as RFID tags. In a security, tracking has been improved with RFID. Different objects including humans, goods, vehicles, assets, etc. can be easily tracked using RFID technology. RFID technology is typically composed of three key elements: 1.an RFID tag, or transponder, that carries object-identifying data.2.an RFID reader, or transceiver, that reads and writes tag data.3.a back-end database, that stores records associated with tag contents.

A device called an RFID tag (or simply a tag) is a key component of the technology. An RFID tag usually has at least two components: 1.an integrated circuit for modulating and demodulating radio signals and performing other functions; 2.an antenna for receiving and transmitting the signal.

An RFID tag can perform a limited amount of processing and has small amount of storage. Each tag contains a unique identity code. An RFID reader emits a low-level radio frequency magnetic field that energizes the tag. The responds to the readers query and announces its presence via radio waves, transmitting its unique identification data. This data is decoded by the reader and passed to the local application system via middleware. The middleware acts as an interface between the reader and the RFID application system. The system will then search and match the identity code with the information stored in the host database or backend system. In this way, accessibility or authorization for further processing can be granted or refused, depending on results received by the reader and processed by the database.

Tag data: RFID tags are considered as dumb devices, in that they can only listen and respond, no matter who sends the request signal. This brings up risks of unauthorized access and modification of tag data. In other words, unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service attacks.

Eavesdropping or Skimming: Radio signals transmitted from the tag, and the reader, can be detected several meters away by other radio receivers. It is possible therefore for an unauthorized user to gain access to the data contained in RFID tags if legitimate transmissions are not properly protected.

Any person who has their own RFID reader may interrogate tags lacking adequate access controls, and eavesdrop on tags contents. In this paper, we present the design and implementation of security-enabled RFID tag with flexible architecture. We target a low-area design that requires as little resources as possible such that the tag production does not exceed the practical limits of a possible commercial launch.

In this paper we proposed a new scheme. This scheme is variable key scheme by using modified tiny encryption algorithm (MTEA). The MTEA algorithm is lightweight consuming minimal resource. The proposed RFID tag security is extended by using variable key scheme.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

II. PREVIOUS WORKS

A. *Existing Method*

In existing design ,the system architecture of the non encryption based private tag access where an RF reader is divided into an RF activator and a TSD as shown in fig1.The existing architecture can built by the physical layer technologies. In previous works a novel coding scheme, named random flipping and random jamming (RFRJ) is used to protect the backward channel. In this 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 tags content with one of the secrets, but an adversary cannot obtain the content of tag. 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 a RF activator querying based on the encoded data (or pseudo ID) space by RFRJ. We generalize the RFRJ coding scheme with the arbitrary source bits and codeword lengths. In addition the maximum information rate of RFRJ scheme that achieves the perfect secret is 0.25 and RFRJ provides perfect protection against passive attacks as long as jamming is successful. In this 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 tags 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 backend server.

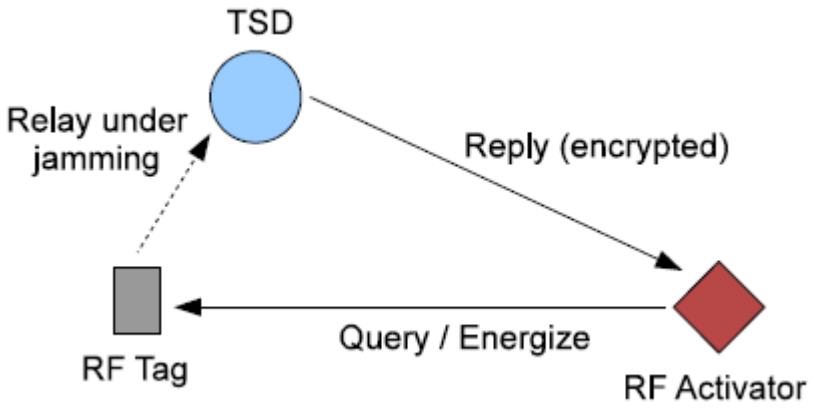

FIG 1: RFID ARCHITECTURE

On overhearing a quaery from an activator to Tag, a TSD jams a bit a codeword.if unauthorized reader tries to access a tag, a TSD jams against all bits of codewords so that the unauthorized reader cannot read the content of the transmitted data.unlike thetrusted masking device and medical shield, a tsd intermediates only the backward channel.the forward channel is protected by having an activator querying tag based on the pseudo ID space encoded by the RFRJ coding scheme.

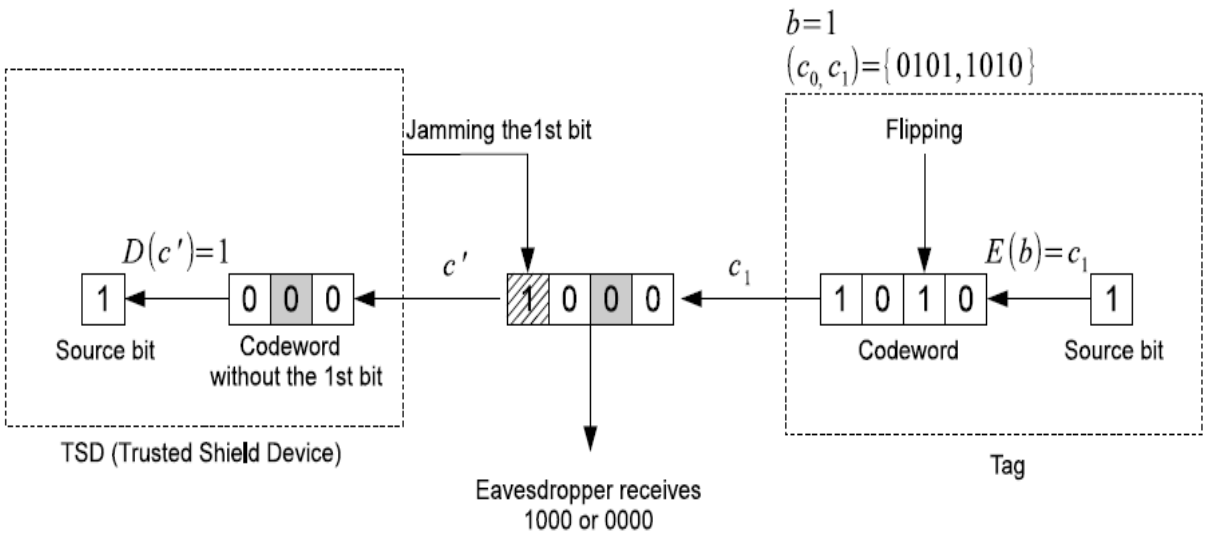

FIG 2: RFRJ System Model And Basic Idea

In above fig2 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 *Is*, 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 four bits may contain errors. Thus, the TSD and eavesdropper have a different amount of information to decode the original codeword. That means, TSD knows that there is a one-bit error while the eavesdropper knows there is a two-bit error. Both the TSD and the tag keep the indexes of the bits they jammed/flipped in secret, but the eavesdropper knows neither of them.

But, when the eavesdropper cannot decode, they may guess the source bit to be either 0 or 1 with even probability (i.e., the random g attacks).when a bit flipping by jamming fails the eavesdropper decodes with the probability 1.otherwise, it can successfully decode with the probability 0.5 by random guessing. Ghost –and leech attacks are one of the active attacks in which an adversary impersonates a tag by forwarding a readers query to the tag and the tags reply to the reader. This attack is similar to man-in –the –middle attacks in the study of cryptography.

III. PROPOSED METHOD

A. Proposed RFID Tag Using Variable Key Scheme

The many possible attacks to an RFID system have been considered and presented. This proposition utilizes tea to provide security against a few attacks. The XOR is already proved as an excellent function to encrypt values with minimal computations. The connection between the reader and the database is secure. The tag and the reader communicate over the vulnerable wireless medium. It is assumed that the tag is equipped to perform encryption/decryption using tea and the XOR operation.

If it is possible to embed XTEA in an RFID chip, it is also meant to give an indication of whether it will be possible to embed public key algorithms into RFID chips. The implementation of XTEA only makes use of one addition each cycle, while public key algorithms like RSA uses more extensive operations(such as power functions).

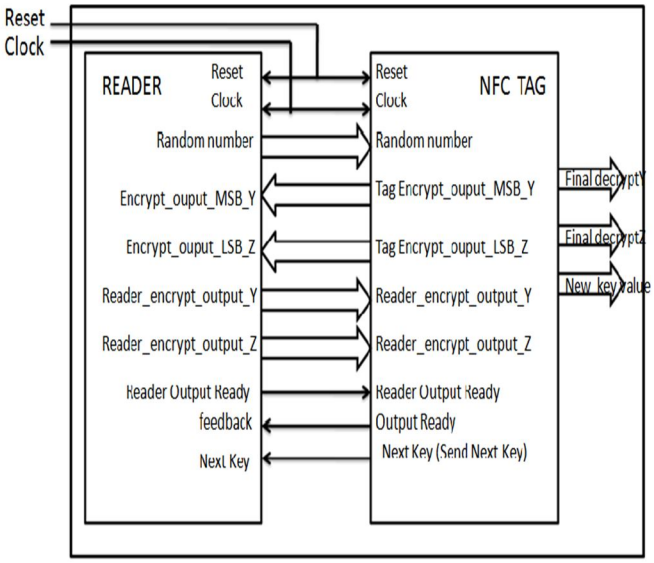

Fig 3: Components and Their Interface for Variable Keys Authentication

The scheme is implemented using VHDL simulate the interaction between the reader and tag using the variable keys protocol for authentication shown in fig 3.two separate components are designed i.e., reader and tag and encapsulated by top-level block. There are some signals that form the interface between the two modules, which are used to emulate the behavior of the system in an RF environment.

The top-level design instantiates these components and facilitates the behavior of the entire system with internal signals and feedback. Simulation waveforms illustrate the functionality of the system in addition to the timing behavior. Two assumptions are made in the design of the system. First, due to the complexity of the system, a random number generator is not used. Random number generators can be implemented as a look-up table in HDL, but for purposes of simulation and testing , a random number is chosen and applied to the system(e.g. the case where a random number is to be generated by tag and the case where a new key is to be computed by the reader as a random number).the new key generated by the reader can be implemented using many widely used

techniques such as hash function, complex random number generating scheme, by using XOR functions or a combination of them depending on the level of security desired. Since this is ultimately implemented in software on a RFID system, it can be designed to handle much more computational complexity than the tag and is easier to implement using software. A separate technique to employ this in hardware is not developed here; rather a number is chosen at random to simulate a new key generated from a reader or back-end database. Secondly, for simplicity, it is also assumed that the reader performs functions of the back-end database (such as id verification and random number generation).

IV. SIMULATION RESULT

The radio frequency identification tag using variable key scheme written in VHDL, complied and simulated using Isim in XILINX 12.1The circuit simulated and synthesized for RFID tag. The block diagram and simulation result are shown in fig4 and fig5 respectively.

A. Block Diagram;

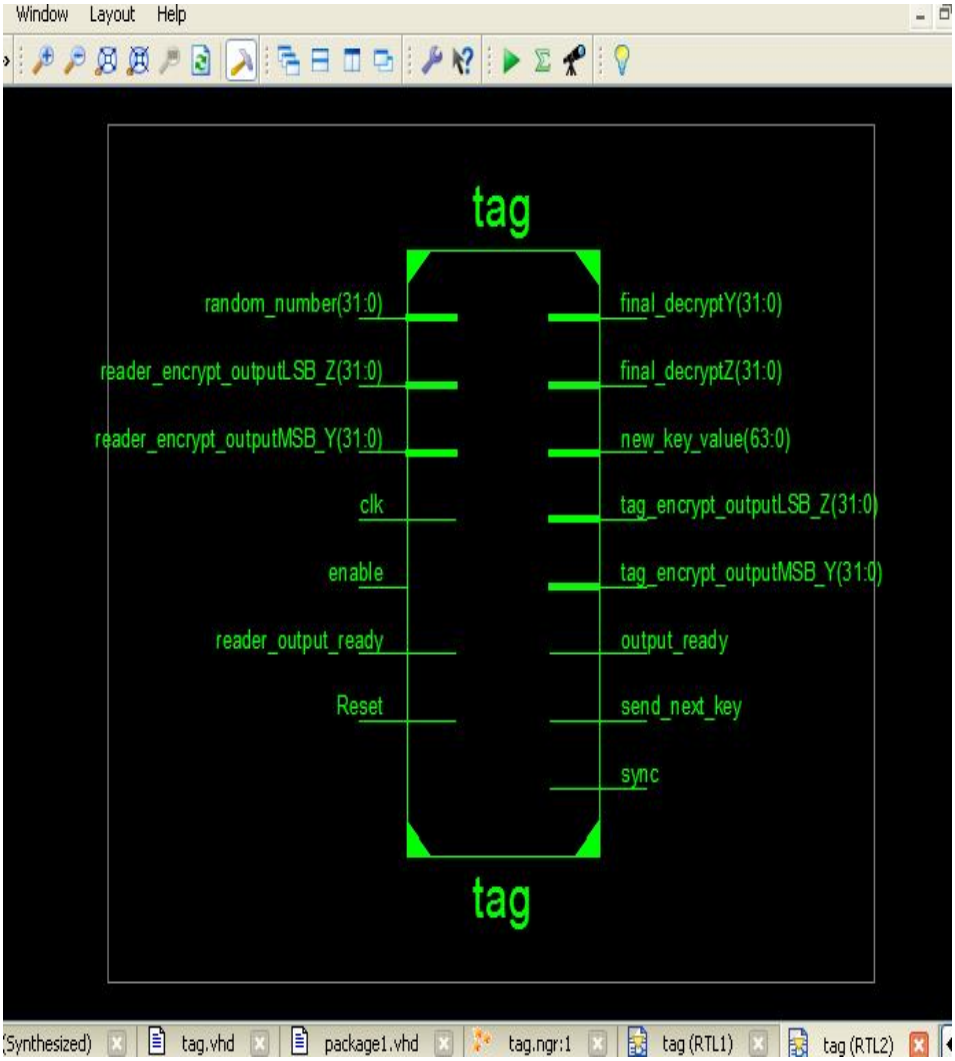

FIG 4: Variable Key Schemes Rfid Tag Rtl Schematic

1) The PID of the tag is defined as a 64-bit value of0x123456789abcdef.
2) The key used for the initial session of the protocol is a 128-bit value defined as 0x00112233445566778899aabbccddeeff.
3) The random number used by the reader is a 64bit value of 0x00000028 or 40.the number of rounds used for all encryption and decryption procedures at the reader and the tag are fixed to 0x00000032 or 50 rounds.
4) The new key generated is a value of 0x34676398ad9c23ef814574346613712b which is a random number.

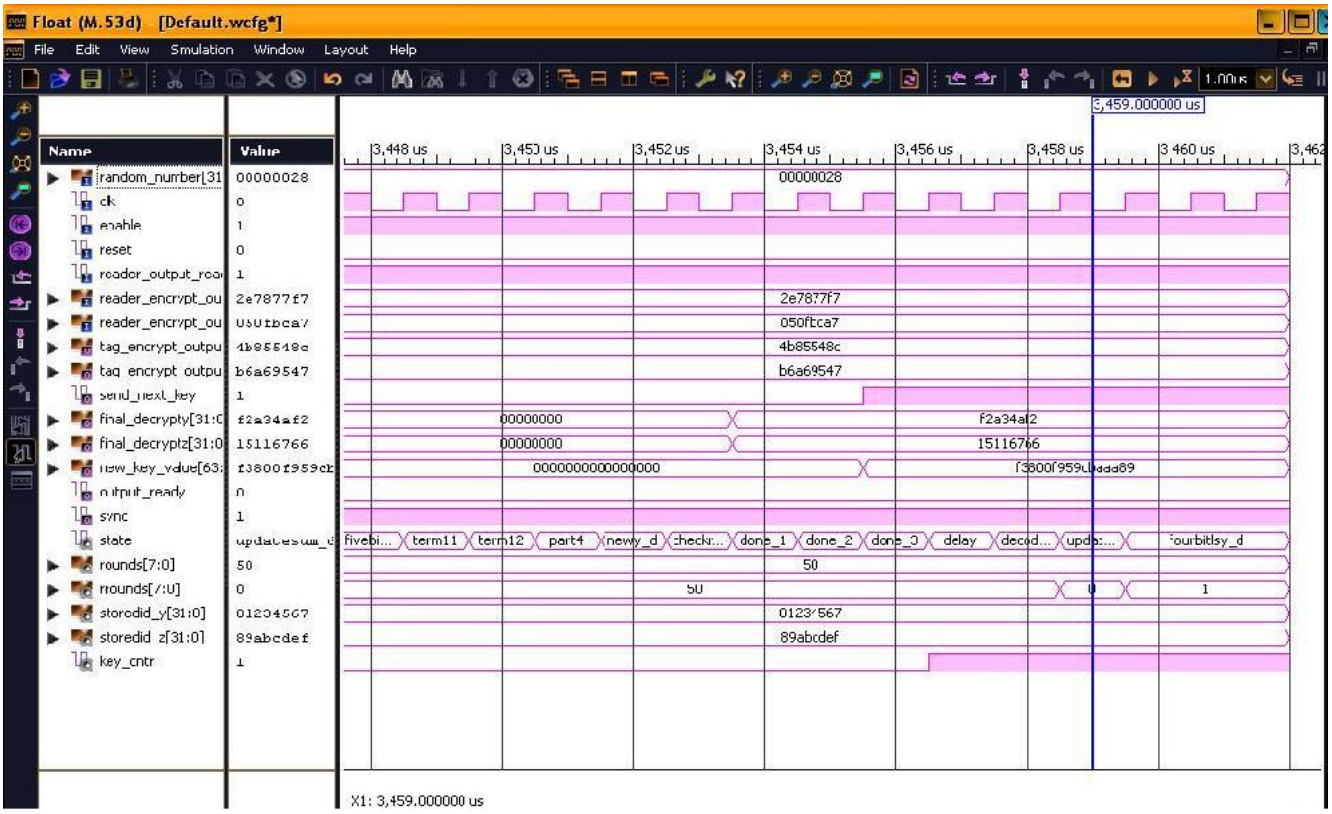

Fig 5: RFID Tag Simulation Result

V. CONCLUSION

In this paper, we presented a flexible RFID tag architecture that provides extended security features using variable key scheme. This scheme is using XTEA algorithm which is light weight, consuming minimal resource of protocols. Performance and feasibility to be adopted as an industry standard. In order to find use in credit-card transactions and other such high risk applications it is essential to strengthen security by developing robust techniques in algorithms and authentication procedures in RFID systems.

REFERENCES

[1] Thomasplos, Michael hutter "Security-Enabled Near –Field Communication Tag with flexible Architecture supporting asymmetric cryptography", IEEE Transactions ON (VLSI) SYSTEMS, VOL.21, NO.11, NOVEMBER 2013.
[2] D.J.Wheeler, R.M.needham, "TEA, a Tiny Encryption a Algorithm", in the Proc.Fast software encryption: second international workshop, lecture notes in computer science, vol.1008, Leuven, Belgium, Dec 1994, pp.363-366
[3] L.Batina, J.Guajarado, T.Kerins, N.Mentens, P.Tuyls and I.Verbauwhede, "Public-key cryptography for RFID tags", in proc.RFIDsec, 2006, pp.1-16.
[4] S.S.Weis,S.Sarma, R.Rivest and D.Engels, "Securityand Privacy Aspects of Low Cost Radio Frequency Identification Systems",Is1 International Conference on Security in Pervasive Computing, Springer, Berlin, Germany, Mar.2003, LNCS vol.2802, pp.201-212.
[5] P.Israsena, "Design and Implementation of Low Power Hardware Encryption for Low Cost Secure RFID using TEA", pro c. International Conference on Information and Communication Systems, Bangkok, Thailand, Dec.2005, pp.1402-1406.
[6] A.V.Reddy, "A Cryptanalysis of the Tiny Encryption algorithm", Master of Science, The University of Alabama, 2003.
[7] S.A.Weis, Security and Privacy in Radio Frequency Identification Devices, Master Thesis, MIT, 2005.
[8] M.Feldhofer, M.J.Aigner, M.Hutter, T.Plos, E.Wenger and T.Baier, "Semi-Passive RFID development platform for implementing and attacking security tags", in Proc. Int. Conf. RISC, 2010, pp.1-6.
[9] Y.Li and X.Ding, "Protecting RFID Communications in Supply Chains", in ASIACCS, 2007, pp.234-241.
[10] A. Juels, "RFID Security and Privacy: A Research Survey, IEEE journal on selected areas in communications, vol.24.no. 2. pp.381-394, 2006.