INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2021, VOL. 67, NO. 4, PP. 623-629
Manuscript received July 3, 2020; revised November, 2021 DOI:10.24425/ijet.2021.137855

RFID-MA XTEA: Cost-Effective RFID-Mutual Authentication Design Using XTEA Security on FPGA Platform

R Anusha, and V Veena Devi Shastrimath

***Abstract*—RFID systems are one of the essential technologies and used many diverse applications. The security and privacy are the primary concern in RFID systems which are overcome by using suitable authentication protocols. In this manuscript, the cost-effective RFID-Mutual Authentication (MA) using a lightweight Extended Tiny encryption algorithm (XTEA) is designed to overcome the security and privacy issues on Hardware Platform. The proposed design provides two levels of security, which includes secured Tag identification and mutual authentication. The RFID-MA mainly has Reader and Tag along with the backend Server. It establishes the secured authentication between Tag and Reader using XTEA. The XTEA with Cipher block chaining (CBC) is incorporated in RFID for secured MA purposes. The authentication process completed based on the challenge and response between Reader and Tag using XTEA-CBC. The present work is designed using Verilog-HDL on the Xilinx environment and implemented on Artix-7 FPGA. The simulation and synthesis results discussed with hardware constraints like Area, power, and time. The present work is compared with existing similar approaches with hardware constraints improvements.**

***Keywords*—RFID, Mutual Authentication, (MA), XTEA, FPGA, NFC, EPC, Encryption, Reader, Tag, CBC Mode**

I. INTRODUCTION

THE Radio-Frequency Identification (RFID) systems are one of the substantial technologies used in many applications, which includes Reader, Tag, and Database Server. In general, RFID tag Identity reads by the reader and sends the request identity to the server. The Database server indexed the tag information. RFID Tags are categorized based on power usage, which includes passive, semi-active, and Active Tags. The RFID Tags are also divided based on Frequency ranges, which include Ultra High Frequency (860-960MHz), High frequency (13.56MHz), and Low Frequency (125-134 kHz) Ranges. The Limitations of the RFID system is security and privacy. There are many authentication protocols presented, which can be classified as Lightweight Protocols, Simple protocols, Ultra-Lightweight, and Fully-Fledged protocols to improve these limitations. The goal of these authentication protocols is to provide services to threats and services[1-2]. The RFID-systems are embedded with smartcards and used in many applications like Healthcare services, Education systems, E-Commerce, Finance, Computer security, Mobile communications, Transportations, and Government Resources [3]. RFID-system places a significant role in healthcare and medical treatments, which is used to track the patients and also provides security, privacy, and reliability [4]. The future of Internet Thing (IoT) includes RFID, sensor technology, and many more, which faces many challenges in security, hardware issues, and storage problems [5].

The Lightweight authentication protocols with a block cipher are divided into based on the structure like Add-Rotate-XOR (ARX), Hybrid, Feistel networks, and Substitution Permutation Networks (SPN). These block ciphers are used in RFID systems for MA [6]. The security attacks in MA include Denial-of-Service (DoS), Tracking attack; Full-disclosure, Replay, Cloning, Impersonation, Man-in Middle, and De-synchronization Attacks have appeared between Reader and Tag [7]. The advanced algorithms like symmetric block ciphers and hash functions are used in RFID-MA for improving the security of hardware includes ASIC and FPGA [8-10]. The analysis of security concerns and challenges in authentication protocol using hardware is a difficult task. In our present work, the cost-effective hardware implementation is performed for RFID-MA using XTEA-CBC and also a comparison with existing similar methods with hardware constraints improvements.

This manuscript presents the RFID- MA protocol design using XTEA security on the FPGA Platform to improve the authentication between tag and reader and suitable for NFC enabled applications. The present work offers the mutual authentication between Tag and reader is communicated by using XTEA and also provides security from the attacks. The present design provides low-cost hardware implementation with high speed and less execution time on FPGA. Section II explains the different RFID authentication approaches using different security algorithms both on software and hardware approaches for different applications. Section III elaborates on the XTEA and XTEA-CBC hardware architecture for RFID-MA. Section IV describes the proposed RFID-MA with XTEA security in detail with architectures. The Results and comparative analysis are elaborated in section V. Finally, and section VI concludes the overall work with improvements and future scope.

II. BACKGROUND

This section deals with the review of existing approaches towards RFID-mutual authentication with security algorithms

Authors are with Department of Electronics and Communication Engineering, N.M.A.M Institute of Technology, Visvesvaraya Technological University, Belagavi, Karnataka, India (e-mail:- anu4research@gmail.com)

for different applications and also highlights the limitations with problem identification. Baashirah et al. [11] present the security algorithms like Humming-bird (HB), XTEA, and PRESENT for RFID devices with GEN2 protocol. The PRESENT design integrated with PUFFIN cipher to increase the level of security. The computational complexity is high with these architectures and not suitable for NFC applications. Dinarvand et al. [12] present the secured authentication protocol for RFID devices using Elliptic Curve Cryptography (ECC), which offers privacy; minimize the computational complexity with high security. The authentication includes setup phase, authentication phase, and updating phase for reader and Tag. The security analysis using ECC includes mutual authentication, forward privacy, scalability, availability, and data integrity. The design also prevents attacks includes replay attack, cloning attack, de-synchronization attack, Tag masquerade attack, server spoofing attack, and DoS attack resisting. The complete design is implemented on software approaches and challenging to use in hardware devices.

Multi-Tags with authentication in RFID protocol security is presented by Kang [13] for omnipresent environments. The single, double, and multiple tag authentication protocols are discussed. The different attacks experiment are conducted for multi-tag authentication using software with security improvements. Yu et al. [14] present an RFID protocol using XTEA encryption based on system C modeling. The design offers a communication establishment between the backend server with Reader and Tag. The key updating mechanism is incorporated in security protocol for different attacks, which improves the authentication against the significant attacks. The improved version of the [14] work is presented by khan et al. [15] using the FPGA platform. Different attack models are designed with a different basic setup for tag response and attacker message response. The design is implemented on the NIOS system and evaluates the code size and communication cost and also analyzes the timestamp difference measurement.

Khan et al. [16] present the RFID protocol with a key updating mechanism using XTEA security. The key updating technique is incorporated using XTEA between Tag and Reader authentication also analyzes the security level with different attacks. The protocol is tested with Zigbee devices to perform the computation cost, communication cost, and storage space. The Zhu et al. [17] continue the same work of Khan [16] with minor changes in authentication protocol with key updation improvements. Khan et al. [18] present the low-cost RFID authentication protocol for performance improvements. The work is compared with yet-another Trivial Authentication protocol with improvements in the computational effort and implemented in real-time environments. The EPC GEN-2 protocol design with Humming-bird (HB), XTEA, and PRESENT security algorithms are designed for mutual authentication by Seshabhattar et al. [19]. The GEN2 protocol includes command detection module, Finite state machine (FSM) along with Response module for Tag identification. These designs consume more chip areas and difficult for real-time usage.

Saxena et al. [20] describe the hash-based RFID protocol design for mutual authentication (MA) with a software approach. The hash-based work contains pre-phase for random number generation, Reader query for Tag, Tag response, Tag authentication with server response, followed by the reader's response, and secret value updation with server authentication. The different attacking mechanisms are also incorporated in protocol against the attacks. The group RFID tag protocol is designed by Zang et al. [21] with security, which includes protocol process with initialization, certification, and protocols security analysis. The certification has group proof generation and grouping proof verification process. The Zhu et al. [22] present the RFID-MA with physically unclonable functions (PUFs), which includes the arbiter based PUF between server and Tag has a secure channel. The RFID-MA process has setup and authentication phase with the analysis of the insecure and secure channel also performs the different attacks in RFID-MA with performance improvements. The comparative analysis of XTEA and Scalable Encryption Algorithm (SEA) on FPGA is present by Jain et al. [23], which includes the algorithms architecture, and performance constraints between SEA and XTEA.

The research problems for the RFID-MA with security approaches are addressed as follows: i) Most of the existing security approaches of the XTEA method are made individually and which is inapplicable when the design is altered. ii) Very few works towards XTEA with Mutual authentication on the FPGA platform with computational complexities and more resource constraints utilization on a single chip.

III. XTEA ARCHITECTURE

The XTEA was developed to overcome the limitations of the TEA and to enhance the authentication effectively. The XTEA and XTEA with Cipher block chaining (CBC) mode are explained in this section and used in RFID-MA.

A. Extended TEA (XTEA) Module

The XTEA uses 64-bit data for encryption and decryption with128-bit symmetric Key and also is known as a lightweight block cipher algorithm. The XTEA has mainly Key scheduling, Round function operation, along with encryption and decryption process. The XTEA key scheduling architecture based on counter mode is represented in figure 1. The key scheduling mechanism has a 128-bit symmetric key, which is divided into 4-sub keys {K [3], K [2], K [1], and K [0]} as a 32-bit memory location. XTEA Key scheduling starts the initial round by adding and subtracting the constant values when the counter is at 2'b00 for encryption and decryption, respectively, and are represented by equation (1) and (2).

$$\text{Encryption: } A_e = \Delta_1 + \alpha_1 \quad (1)$$

$$\text{Decryption: } A_d = \Delta_2 - \alpha_2 \quad (2)$$

The generation of 32-bit key output (K_{out}) for encryption based on the count =2'b00 and 2'b10 is represented in the equations (3-4). Similarly, for Decryption in equations (5-6).

$$\text{Encryption: } K_{out} = A_e + K[A_e \,\&\, 3]; \text{ (when count=00)} \quad (3)$$

$$K_{out} = A_e + K[A_e >> 11 \,\&\, 3]; \text{ (when count=10)} \quad (4)$$

$$\text{Decryption: } K_{out} = A_d + K[A_d >> 11 \,\&\, 3]; \text{ (when count=00)} \quad (5)$$

$$K_{out} = A_d + K[A_d \,\&\, 3]; \text{ (when count=10)} \quad (6)$$

Where '&' denotes Logical AND operation, '>>' denotes Logical right shift, '<<' denotes left shift operation, and '^' denotes XOR operation.

The round function is the Feistel structure in XTEA, which performs 64-rounds for both encryption and decryption, which receives the key round outputs are input along with round inputs for round operations. The round function operation output (R_{out}) is represented by equation (7) as follows

$$R_{out} = K_{out} \wedge ((R_{in}<<4 \wedge R_{in}>>5) + R_{in}) \quad (7)$$

The proposed XTEA works either as an encryption and decryption by using control signal 'ed.' If the ed = 0, then encryption else decryption will be performed. The XTEA has 64-bit input text (I_T) has divided into two parts, like I_0 has $I_T[31:0]$, and I1 have $I_T[63:32]$.

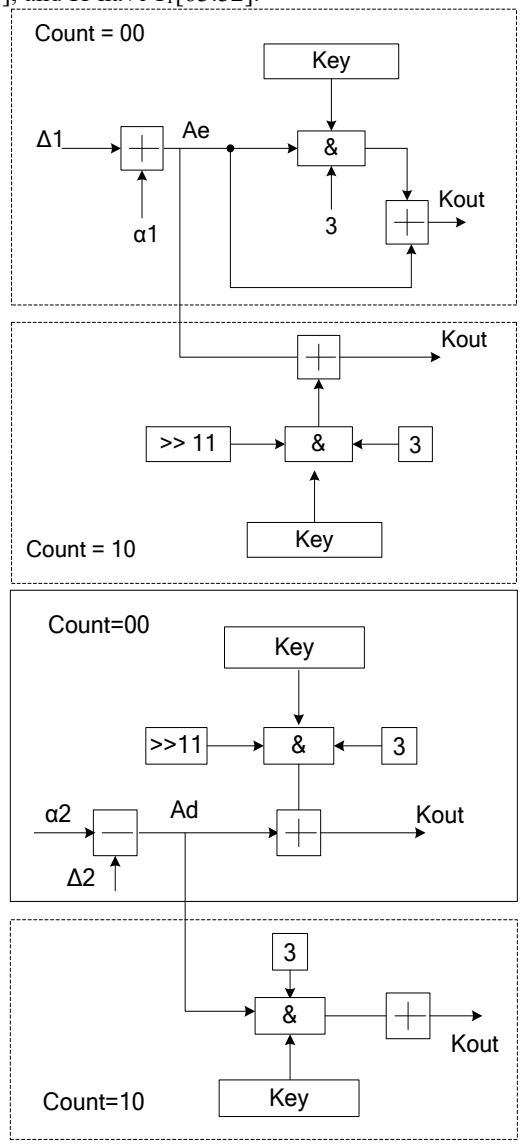

Fig.1. XTEA Key Scheduling, 1(a): Encryption 1(b): Decryption

The complete algorithmic-1 flow of XTEA encryption and decryption is described in the below section for the generation of encryption and decryption outputs (C_T).

Algorithm 1: For XTEA:
Input: I_T, R_{in}, R_{out},ed
Output:C_T

1. Initialization:
   a. If (ed =0) then $I_1 = I_T[63:32]$ and $I_0 = I_T[31:0]$
   b. else $I_0 = I_T[63:32]$ and $I_1 = I_T[31:0]$
2. Rounding Operation:
   a. Count=00: $R_{in} = I_{1;}$
   b. Count =01: if (ed =0) then $I_0 = I_0 + R_{out}$ else $I_0 = I_0 - R_{out}$;
   c. Count = 10; $R_{in} = I_{0;}$
   d. Count = 11; if (ed =0) then $I_1 = I_1 + R_{out}$ else $I_1 = I_1 - R_{out}$;
3. Output Generation:
   a. If (ed =0) then $C_T = \{I_1, I_0\}$ else$C_T = \{I_0, I_1\}$;

B. XTEA-CBC Module

The XTEA used as a block cipher, mainly in near field communication (NFC) applications like RFID Reader and Tag authentication and other electronic security applications. The XTEA Cipher block chaining (CBC) encryption and decryption operation are represented in figure 2 (a-b). The XTEA-CBC provides a suitable authentication mechanism and has a better resistive mechanism.

In XTEA-CBC, The Input text (I_{T1}) is XOR with an initialization vector (IV) followed by the XTEA encryption to generate first Ciphertext (C_{T1}) output, which is XOR with next input text (I_{T2}) to perform next encryption process to generate the second Ciphertext (C_{T2}) output. Similarly, decryption is the inverse process of encryption, as represented in figure 2(b). The 128-bit key input (K_{in}) is symmetric and standard for both encryption and decryption process.

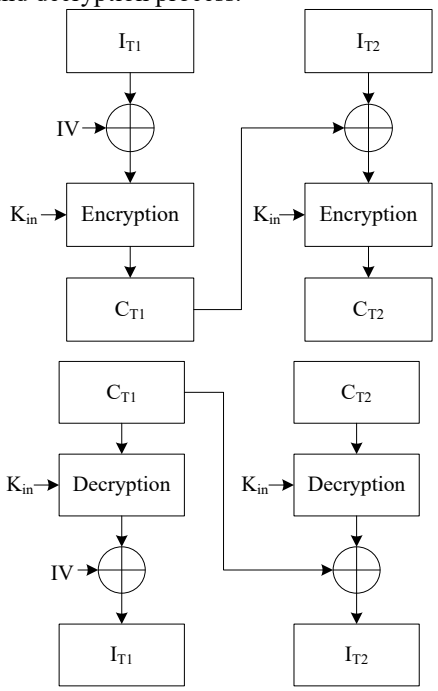

Fig.2. XTEA-CBC 2(a): Encryption 2(b): Decryption

The XTEA and XTEA-CBC mode synthesis results are tabulated in table I, and graphical representation is shown in figure 3. The XTEA utilizes 316 slice registers, whereas XTEA-CBC utilizes 652 slice registers. The XTEA-CBC uses two times of encryption and decryption process. So XTEA-CBC utilizes more chip areas than XTEA Process.

TABLE I
FPGA SYNTHESIS RESULTS FOR XTEA AND XTEA-CBC MODE

Resources	XTEA	XTEA CBC Mode
Slice Registers	316	652
Slice LUTs	641	942
LUT-FF pairs	243	336

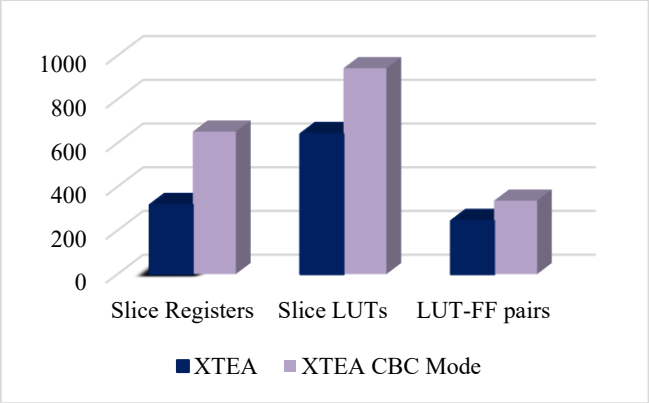

Fig.3. Graphical representation of XTEA and XTEA-CBC mode (Encryption)

TABLE II
COMPARISON OF EXISTING AND PROPOSED XTEA APPROACHES

Resources	XTEA[19]	XTEA [23]	Proposed-XTEA
Slices	947	332	362
Slice-FFs	204	450	238
4-Input LUT's	1833	NA	660
Frequency (MHz)	74.56	39.85	125.937
Power (mW)	NA	110	86
FPGA Device	XC3S100E	XC3S500E	XC3S500E

The XTEA design is compared with existing similar architectures [19] [23] with improvements and is tabulated in table II. The Slices and 4-input LUT utilization of present work consumed a very less amount of chip area than the previous approach [19]. The Slices and 4-input LUT's utilization around 61.77%, and 63.9 % improved over previous work [19]. The operating frequency is also improved over previous work [19] with 40.77 % overhead. The power utilization of present works consumes 21.8 % less overhead than the previous approach [23].

IV. RFID-MUTUAL AUTHENTICATION (MA) USING XTEA

The RFID- MA protocol is designed and implemented using XTEA-CBC, which provides the reader and Tag authentications. Firstly, providing the security to Tag Identification using XTEA-CBC and, secondly, perform Mutual identification (MA) for the same.

The reader sends the request to tag for communication establishment, and The Tag generates the Random data as Secure Identity (SI) using Random number generator (RNG). Perform the XTEA Encryption process for the SI to generate the ciphertext (CT). The reader decrypts the CT data and generates the Secure Identity (SI) data. If decrypted data is the same as SI data, then the Tag Identification is successful.

Once the Tag Identification is successful, then Mutual authentication between Reader and Tag has started, and typical flow for the same is represented in figure 4.

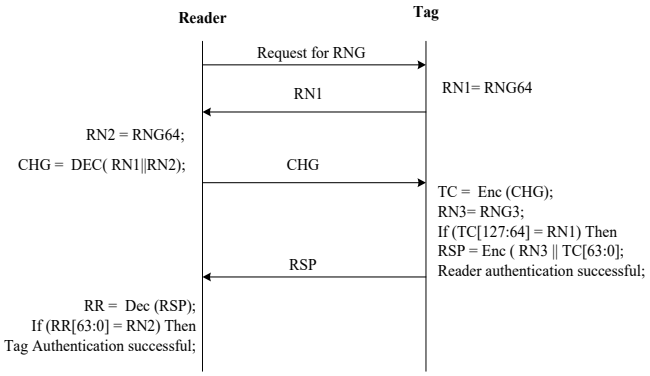

Fig.4. RFID-Mutual Authentication Typical flow

The algorithm-2 of RFID-Mutual Authentication is represented here, which elaborates the reader and Tag authentication process. The Reader sends the query to the Tag for Random Number Generation (RNG). The Tag generates the Random number (RN1) for communication with Reader. The reader generates the Random number (RN2) for Challenge (CHG) creation to Tag. Perform the XTEA-CBC Decryption for RN1 and RN2 to generate the CHG. The Tag accepts the CHG data and performs XTEA-CBC Encryption to generate the Tag challenge (TC). The Tag generates the Random number (RN3) for response (RSP) creation. The response (RSP) data is generated by Tag using XTEA-CBC Encryption of RN3 with TC [63:0]. Reader Authentication is successful in Tag. The reader receives the Tag's Response (TR) and performs the Decryption process to generate the Reader-response (RR) for Tag authentication. If the RN2 is the same as RR [63:0] data, then Tag is authenticated in Reader.

Algorithm 2: For RFID-MA WITH XTEA-CBC
Input: RNG_request
Output: Reader_Auth, Tag_Auth

1. Tag: Request for Random number generator (RNG) from reader
   a. Generation of RNG: RN1 = RNG64;
2. Reader :
   a. Generation of RNG: RN2 = RNG64;
   b. Challenge(CHG) generation from Reader:RC: (RC1 ||RC2) = XTEA _Dec (RN1|| RN2);
3. Tag: Accepts the Challenge (CHG)
   a. Perform the Encryption for challenge: TC: (TC1 || TC2) = XTEA _Enc (RC1 ||RC2);
   b. Generation of RNG : RN3= RNG64;
   c. If (TC2= RN1) Then
   d. Response (RSP) generation from Tag : TR: (TR1||TR2) = XTEA _Enc (RN3 ||TC1);
   e. Reader Authentication is successful.
4. Reader :
   a. Perform Decryption using RSP :RR: (RR1, RR2) = XTEA _Dec (TR1||TR2);
   b. If (RR1= RN2) Then
   c. Tag Authentication is successful.

V. Result Analysis

The results and performance analysis of the RFID-MA model using XTEA is elaborated in this section. The RFID-MA model is designed using Verilog-HDL on the Xilinx ISE platform and implemented on Artix-7 FPGA. The Simulation, synthesis, and implementation results like Area, time, and Power, along with a comparison of similar existing approaches with present work, are discussed. The XTEA lightweight protocol is incorporated in the RFID-MA model to improve the authentication process while transforming data between tag and reader. The XTEA lightweight protocol is operating based on Cipher block chaining (CBC) mode for Mutual Authentication. The XTEA-CBC protocol process parallelly two 64-bit plaintexts and generates two 64-bit ciphertexts for encryption and vice-versa for decryption using the 128-bit symmetric key.

The simulation results of RFID-MA using XTEA lightweight protocol is represented in Figure 5. As discussed in an earlier section, the design has three 64-bit Random generator models (Random_Gen1, Random_Gen2, and Random_Gen3), 64-bit Reader's challenge and Response signals, 64-bit Tag's challenge and Response signals for Reader and Tag Authentication. Once the clock is activated, The RFID-MA process starts, the reader sends the request to Tag to process for data transfer, and The Tag generates 64-bit Random data (Random_gen1) and sends back to Reader for Future process. The reader generates the 64-bit Random data (Random_gen2) internally to perform the challenge. The reader's challenge is obtained by performing the decryption process of XTEA in CBC mode and generates the 64-bit Reader_Challenge1 and Reader_Challenge2. The Tag receives the Reader_Challenge1, and Reader_Challenge2 signals perform the XTEA-CBC encryption process for reader authentication and generate the 64-bit Tag_Challenge1 and Tag_Challenge2. The tag internally generates the 64-bit Random data (Random_gen3) to respond to the reader. If the Tag_Challenge1 is equal to theRandom_gen1, then the tag is ready to perform the response operation for the reader. The Tag response obtained by performing the XTEA-CBC encryption process using Random_gen3 and Tag_Challenge1 and generates the 64-bit Tag_Response1 and Tag_Response2. Once a response is ready by the tag, if the Tag_Challenge1 is equal to theRandom_gen1, then Reader authentication (Reader_Auth) is successful.

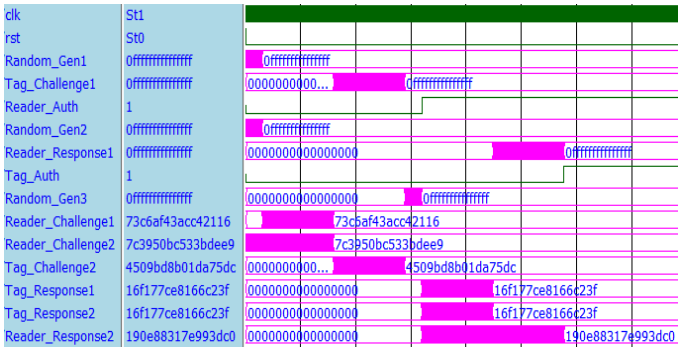

Fig.5. Simulation results of RFID-MA Model using XTEA

Tag is ready to send the acknowledge through response signals, Once the reader authentication is successful. The reader receives the response signals like 64-bit Tag_Response1 and Tag_Response2 and performs the XTEA-CBC decryption for tag authentication and generates the 64-bit Reader_Response1 and Reader_Response2. If the Reader_Response1 is equaled to Random_gen2, the Tag authentication is a success (Tag_Auth) in Reader. If the Tag authentication fails, The Mutual authentication is not established between Tag and Reader.

The Execution time per process, according to the above simulation results for the Reader and Tag authentication in the RFID-MA model, is tabulated in Table III. The RFID-MA with XTEA-CBC security execution time (response time) per process is noted. The reader and authentication are completed at 6.395µsec and 11.55 µsec. The overall execution time for the RFID-MA with XTEA-CBC Security is 11.555µsec.

Table III
Execution Time per Process in RFID-MA with XTEA Security

Sl.No	RFID-MA process	Execution Time/Process
1	Random Generation (Random_Gen-1,2)	0.605 µsec
2.	Challenge Generation from Reader (Reader_Challenge-1,2)	2.585 µsec
3.	Challenge perform in Tag (Tag_Challenge-1,2)	2.580 µsec
4.	Random Generation (Random_Gen-3)	0.610 µsec
5.	Reader Authentication successful	0.020 µsec
6.	Tag Response Generation (Tag_Response-1,2)	2.560 µsec
7.	Reader Response Generation (Reader_Response-1,2)	2.580 µsec
8.	Reader Authentication Successful	0.020 µsec
Total Execution Time		**11.555 µsec**

The RFID-MA with XTEA security is implemented on Atrix-7 FPGA. The resource constraints like Area, Time, and power results are obtained after the place and route operation, and it is tabulated in table 4. The area utilization is < 1% on Artix-7 FPGA, which is having 1604 slice registers, 2307 slice LUT's and 937 LUT-FF pairs. The RFID-MA with XTEA Security works at a high operating frequency of 263.76 MHz on FPGA. The power utilization is calculated using an X-power analyzer, which includes static and dynamic power of 0.082W and 0.09W, respectively. The total power utilization of RFID-MA with XTEA security is 0.172W, which is quite less and useful for low-cost NFC enables devices.

Table IV
Resource Utilization of RFID-MA with XTEA

Resource Utilization	RFID_MA_XTEA
FPGA Device: Artix-7 100T-3CSG324	
Area	
Slice Registers	1604
Slice LUTs	2307
LUT-FF pairs	937
Time	
Minimum period (ns)	3.79
Max.Operating Frequency (MHz)	263.762
Power	
Dynamic Power (W)	0.09
Total Power (W)	0.172

The RFID-MA with the XTEA security model is compared with existing similar architecture [19] with improvements and is tabulated in table 5. The Slices and 4-input LUT utilization of present work consumed a very less amount of chip area than the previous approach [19]. The Slice-FF's utilization is improved over previous work [19] with 56.35% overhead. The operating frequency is also improved over previous work with 51.71 % overhead. Both the design works are synthesized on the same FPGA device-Spartan -3E.

TABLE V
COMPARISON OF PROPOSED RFID-MA WITH EXISTING APPROACH [19] WITH XTEA SECURITY

Resources	RFID-MA_XTEA [19]	Proposed
Slices	22553	1212
Slice-FFs	2603	1136
4-Input LUT's	43312	2234
Frequency (MHz)	60.6	125.51
FPGA Device	XC3S100E-5	XC3S100E-5

VI. CONCLUSION

The RFID-Mutual Authentication with XTEA security is designed and implemented on low-cost FPGA. The RFID-MA includes Reader and Tag authentication by providing Reader's and Tag's challenge and Response using XTEA security. XTEA has pipelined architecture for Encryption and decryption process along with parallel execution of Key scheduling, which improves the overall speed of the RFID-MA process. XTEA with CBC mode is used in RFID-MA for better computation and hardware constraints improvements. The RFID-MA with XTEA model is simulated using Modelsim simulator and implemented on Artix-7 FPGA. The XTEA and XTEA-CBC both the models are synthesized, and hardware constraints are tabulated. The XTEA is also compared with existing approaches with improvements. The execution time of each process in RFID-MA with XTEA is analyzed, and the total execution time for the whole process is 11.555µSec. The design works at 263.762MHz operating frequency and consumed 0.172W power. The proposed work is compared with existing approaches with an improvement of 56.35% in Slice-FF's and 51.71% in operating frequency. In the future, the same RFID-MA protocol incorporated with Different security attacks and analyzes the performance of the system.

REFERNCES

[1] A. Ibrahim and G. Dalkılıc, "Review of different classes of RFID authentication protocols," *Wireless Networks*, Vol.25, No. 3, pp.961-974, 2019, https://doi.org/10.1007/s11276-017-1638-3

[2] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou and C. Manifavas. "A review of lightweight block ciphers," *Journal of Cryptographic Engineering,* Vol. 8, No. 2, pp.141-184, 2018, https://doi.org/10.1007/s13389-017-0160-y

[3] J. Kaur, A. Kumar, M. Bansal. "Lightweight cipher algorithms for smart cards security: A survey and open challenges," *4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 541-546, 2017, https://doi.org/10.1109/ISPCC.2017.8269738

[4] X. Chen, K. Ma, D. Geng, J. Zhai, W. Liu, H. Zhang, T. Zhu, and X. Piao. "Untraceable Analysis of Scalable RFID Security Protocols," *Wireless Personal Communications*, pp.1-21,2019, https://doi.org/10.1007/s11277-019-06650-1

[5] M.G. Samaila, M. Neto, D. AB. Fernandes, M. M. Freire, and P. RM. Inácio. "Security challenges of the Internet of Things," *Beyond the Internet of Things*, pp. 53-82, 2017.

[6] M. M-Kermani, K. Tian, R. Azarderakhsh, and S. B-Sarmadi, "Fault-resilient lightweight cryptographic block ciphers for secure embedded systems," *IEEE Embedded Systems Letters*, Vol. 6, No. 4, pp.89-92, 2014, https://doi.org/10.1109/LES.2014.2365099

[7] Y.S. Kang, E.O. Sullivan, D. Choi, and M. O'Neill, "Security Analysis on RFID Mutual Authentication Protocol," in *International Workshop on Information Security Applications*, *Springer, Cham, pp.* 65-74, 2015, https://doi.org/https://doi.org/10.1007/978-3-319-31875-2_6

[8] M. Feldhofer and J. Wolkerstorfer, "Hardware implementation of symmetric algorithms for RFID security," in *RFID security*, Springer, Boston, MA, pp. 373-415, 2008, https://doi.org/10.1007/978-0-387-76481-8_15

[9] B. Toiruul and K.O. Lee, "An advanced mutual-authentication algorithm using AES for RFID systems," *International Journal of Computer Science and Network Security*, Vol. 6, No. 9B, pp.156-162, 2006

[10] M. Feldhofer, S. Dominikus and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, Berlin, Heidelberg, pp. 357-370, 2004.

[11] R. Baashirah, A. Kommareddy, S. K. Batchu, V. Sunku, R. S. Ginjupalli, and S. Abuzneid, "Security implementation using present-puffin protocol in RFID devices," in *IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pp. 1-5, 2018, https://doi.org/10.1109/LISAT.2018.8378024

[12] N. Dinarvand and H. Barati, "An efficient and secure RFID authentication protocol using elliptic curve cryptography," *Wireless Networks*, Vol. 25, No. 1, pp.415-428, 2019, https://doi.org/10.1007/s11276-017-1565-3

[13] J. Kang, "Lightweight mutual authentication RFID protocol for secure multi-tag simultaneous authentication in ubiquitous environments," *The Journal of Supercomputing*, Vol. 75, No. 8, pp. 4529-4542, 2019, https://doi.org/10.1007/s11227-016-1788-6

[14] J. Yu, G. Khan, and F. Yuan, "XTEA encryption based novel RFID security protocol," *In 24th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 000058-000062, 2011, https://doi.org/10.1109/CCECE.2011.6030408

[15] G.N. Khan, X. Yu, and F. Yuan, "A novel XTEA based authentication protocol for RFID systems," in *URSI General Assembly and Scientific Symposium*, pp. 1-4, 2011, https://doi.org/10.1109/URSIGASS.2011.6050584

[16] G.N. Khan and G. Zhu, "Secure RFID authentication protocol with key updating technique," in *22nd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-5, 2013, https://doi.org/10.1109/ICCCN.2013.6614192

[17] G. Zhu and G. N. Khan, "Symmetric key based RFID authentication protocol with a secure key-updating scheme," in *26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1-5, 2013, https://doi.org/10.1109/CCECE.2013.6567741

[18] G.N. Khan and M. Moessner, "Low-cost authentication protocol for passive, computation capable RFID tags," *Wireless Networks*,

Vol. 21, No. 2, pp. 565-580, 2015, https://doi.org/10.1007/s11276-014-0803-1

[19] S. Seshabhattar, S. K. Jagannatha, and D. W. Engels, "Security implementation within GEN2 protocol," in *IEEE International Conference on RFID-Technologies and Applications*, pp. 402-407, 2011, https://doi.org/10.1109/RFID-TA.2011.6068669

[20] M. Saxena, R. N. Shaw, and J.K. Verma. "A Novel Hash-Based Mutual RFID Tag Authentication Protocol," in *Data and Communication Networks*, pp. 1-12, 2019, https://doi.org/10.1007/978-981-13-2254-9_1

[21] K. Zang, H. Xu, F. Zhu, and P. Li, "Analysis and Design of Group RFID Tag Security Authentication Protocol," in *Conference on Complex, Intelligent, and Software Intensive Systems*, Springer, Cham, pp. 637-645, 2019, https://doi.org/10.1007/978-3-030-22354-0_57

[22] F. Zhu, P. Li, H. Xu, and R. Wang, "A Lightweight RFID Mutual Authentication Protocol with PUF," *Sensor,* Vol. 19, No. 13, pp. 2957, 2019, https://doi.org/10.3390/s19132957.

[23] R. Jain , K. G. Maradiab, "Comparative Analysis of SEA and XTEA for Resource Constrained Embedded Systems," *International Journal of Innovative and Emerging Research in Engineering*, Vol. 3 No.4, pp. 78-82, 2016

[24] R. Anusha and V.V. D.Shastrimath "LCBC-XTEA: High Throughput Lightweight Cryptographic Block Cipher Model for Low-Cost RFID Systems," in *Computer Science On-line Conference, Springer, Cham,* pp. 185-196, 2019, https://doi.org/10.1007/978-3-030-19813-8_20