IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 September 2023, accepted 22 September 2023, date of publication 28 September 2023,
date of current version 5 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3320277

RESEARCH ARTICLE

Secured Authentication of RFID Devices Using Lightweight Block Ciphers on FPGA Platforms

ANUSHA R[1], RAGHAVENDRA RAO P[2], AND PRATHEKSHA RAI N[3]
[1]Department of Electronics and Communication Engineering, Nitte (Deemed to be University), NMAM Institute of Technology, Nitte, Karnataka 574110, India
[2]Department of Mechatronics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka 576104, India
[3]Department of Electronics and Communication Engineering, A. J. Institute of Engineering and Technology, Mangalore 575006, India

Corresponding author: Raghavendra Rao P (p.raghavendra@manipal.edu)

ABSTRACT Near Field Communication (NFC) has emerged as a pivotal wireless technology for short-range data exchange between devices, including smartphones and wearables. Leveraging Radio Frequency (RF) signals and robust authentication, NFC ensures secure communication in proximity. Mutual authentication (MA) holds paramount importance for establishing trust between device pairs. A prime example of NFC technology is Radio Frequency Identification (RFID), wherein seamless communication occurs between a reader and a tag. However, security and privacy concerns are critical factors in RFID systems, necessitating effective authentication protocols. This paper introduces an efficient and secure MA mechanism for RFID devices, using lightweight block ciphers (LBCs). Specifically, the extended tiny encryption algorithm (XTEA) and the hummingbird algorithm (HBA) using the cipher block chaining (CBC) mode is designed. These tailored algorithms establish a secure communication channel between RFID tags and readers. Notably, the proposed RFID-MA using XTEA and HBA occupies less than 2% of the chip area, encompassing slices and lookup tables (LUTs), and achieves authentication with execution times of 11.6 μs and 1.34μs, respectively. In comparison to the RFID-MA approach employing the XTEA methodology, the proposed algorithm reduces the chip area overhead by 24.6%, total power consumption by 3.5%, and execution time by 88.36%. The proposed algorithm is implemented using Verilog hardware description language (HDL) within the Xilinx environment and is realized on a Artix-7 field programmable gate array (FPGA) platform, utilizing the ModelSim simulator. The proposed research extensively presents simulation and synthesis results while considering the critical hardware constraints such as time, power, and area. Furthermore, this study has also conducted a comprehensive performance analysis, comparing essential metrics with existing LBC and authentication methodologies, showcasing substantial improvements.

INDEX TERMS Authentication, ciphers, cryptography, encryption, field programmable gate array, near field communication, performance analysis, radio frequency identification, simulation.

I. INTRODUCTION

One of the promising devices used in diverse fields, such as reader, tag, and server software, is RFID technology. In general, the reader reads the identities of an RFID tag and transmits the demand identification to the server. The tag's content isÂ indexed by the database server. The RFID system is limited by concerns over privacy and security. Numerous authenticating methods are available that can be categorized as basic methods, fully-fledged methods, lightweight, and ultra-lightweight methods to reduce these restrictions. These authenticating procedures aim to offer security against risks and applications [1], [2]. The RFID–technology, involves observing, and offers stability, confidentiality, and security, and plays a vital part in medical and healthcare procedures. These technologies will, however, face several issues with regard to storage, architecture, and safety [3], [4].

To address security and privacy concerns, there are a variety of alternative authenticating algorithms available. These authentication methods are often used to secure data and other information from attacks in accordance with their intended use, providing good protection capabilities and

The associate editor coordinating the review of this manuscript and approving it for publication was Luca Barletta.

services [5]. For secure mutual authentication with readers, the RFID tags require uniformity of security mechanisms, flexible lightweight approaches, effective lightweight / ultra-lightweight authenticating cryptosystems, and effective key repudiation techniques. Ultra-lightweight block cipher approaches are better suited to ensure effective mutual authentication between the tag and reader [6], [7], [8].

Several literature discuss about authentication of different devices using ciphers. The internet of things (IoT) based encryption algorithms and their performance analysis concerning the memory, energy, and timing parameters is presented in [9]. Advanced encryption standard (AES) and XTEA ciphers security algorithms are implemented on the peripheral interface controller (PIC) microcontroller. The LBC-based MA protocol for low-resource devices is discussed in [10]. A craft block cipher is used for security analysis along with the new cipher LBCbAP for MA. It also analyzes different attacks such as disclosure, impersonation, replay, etc. The simple and secured RFID-MA protocol for healthcare applications is described in [11]. The article explores the drawbacks of the existing works, such as forward secrecy and scalability issues. In addition, it analyzes the security performance and computational cost of the server, reader, and tag with existing approaches. The authors in [12] and [13] describes the new RFID-MA protocol model with strong adversary features. The model has set up server–less authentication, server–mounted authentication, and tag-searching phases. The same work is extended with a new MA protocol to improve the computational cost and security performance [13].

The authors in [14] discuss the secured authentication approach involving different phases with additional tags for RFID applications. The article evaluates brute–force attacks, impersonation attacks, and counterfeiting attacks. The elliptic curve cryptography (ECC) based RFID-MA protocol for IoT applications is presented in [15]. The threat model is applied to RFID-based MA protocol to realize the different attacks. It analyzes the tag, reader, and server's communication, computational, and storage space costs. The lightweight physical unclonable functions (PUFs) based authentication protocol for IoT devices using a secret pattern recognition approach is used in [16]. The approach uses simple bitwise operators, a truly random generator, and a PUF circuit to construct the authentication process. The work analyzes the different attacks, accuracy levels, and throughput. Reference [17] describes the ECC-enabled RFID-MA protocol for the internet of vehicles (IoV). It analyzes the different attacks and communication costs, computational costs, and storage space costs using the AVISPA tool. The gimli-based hash and authentication encryption (AE) implementation for RFID devices is used in [18]. The chip area, frequency, latency, and throughput parameters on hardware is evaluated experimentally.

The RFID-based authentication approach using hyperelliptic curve signcryption (HCS) is used in [19]. The HCS uses an 80-bit key with a high-security feature to tolerate potential attacks. The work evaluates the different security attacks and computational overheads. The hybrid authentication using electrocardiogram (ECG) and block cipher for wireless body area network (WBAN) applications is well described in [20]. The RCIA-based RFID authentication with the logic of events theory (LET) is presented in [21]. The RCIA and LET approaches are incorporated into RFID for mutual authentication between tag and the reader. The multifactor authentication approach with lightweight features for advanced mobile networks is described in [22]. These use ECC–based cipher for multifactor authentication. The processing time, packet overhead, cost, and security analysis with different attacks is performed. The MA with the lightweight approach for smart home applications is presented in [23]. The work analyzes different performance metrics. The ultra-lightweight MA protocol for RFID systems with a maximum distance separable (MDS) coding approach is used in [24]. The security attacks and different costs with different protocols is analysed.

While several literatures have discussed on the security of NFC–enabled devices, it has mainly focused on the validation using software. Additionally, NFC-enabled devices on hardware platforms have not received adequate attention in terms of strengthening security. Incorporating authentication algorithms into the wireless domain has demonstrated its effectiveness, raising the question of their applicability to NFC-enabled devices. However, it is essential to note that advanced and complex authentication algorithms may pose computational challenges, rendering them unsuitable for resource-constrained NFC devices. RFID-tagged objects are susceptible to attacks, potentially leading to the theft of users' private information. Establishing robust authentication mechanisms between NFC-based RFID tags and readers is imperative to ensure secure data communication. Existing research predominantly focuses on lightweight algorithms, primarily in software–based approaches, with limited attention given to hardware–based implementations. Nevertheless, the available hardware-based approaches lack re–configurability and flexibility and may not be suitable for NFC–enabled applications.

Therefore, there is a pressing need for standardized lightweight algorithms that minimize resource utilization in NFC–enabled applications. An efficient and secured authentication approach using LBCs is designed in this manuscript for RFID devices. The proposed technique considers XTEA and HBA as LBCs which provide secured authentication between two devices, i.e., the tag and the reader. The HBA–based MA utilizes lesser resources, consumes low power, and offers better throughput than XTEA–based MA and other approaches. Rest of the manuscript's organization is as follows: Section II discusses the architectures of XTEA and HBA. The authentication of RFID devices using XTEA and HBA is discussed in Section III. The results of the XTEA and HBA and Its MA approaches

Algorithm 1 Extended Tiny Encryption Algorithm

Input: P_T, RF_i, RF_0, m
Output: E_T or D_T
1. Pre-processing Phase:
   I. If $(m = 0)$, then $P_1 = P_0 = P_T[31:0]$ and $P_0 = P_T$ [63:32]; otherwise,
   II. $P_1 = P_T[31:0]$ and $P_0 = P_T[63:32]$;
2. Operation of Rounding Function:
   I. c = 0: $RF_i = P_1$;
   II. c = 1: if $(m = 0)$ then $P_0 = P_0 + RF_0$ else $P_0 = P_0 - RF_0$;
   III. c = 2: $RF_i = P_0$;
   IV. c = 3: if $(m = 0)$ then $P_1 = P_1 + RF_0$ else $P_1 = P_1 - RF_0$;
3. Generation of XTEA output:
   If $(m = 0)$ then $E_T = P_1, P_0$ else $D_T = P_0, P_1$;

are discussed in detail with resource constraint analysis and performance comparison in Section IV followed by conclusion in Section V.

II. LIGHTWEIGHT BLOCK CIPHERS (LBC)

The hardware designs of LBC such as HBA and XTEA are explored in detail in this section. The XTEA design eliminates the flaws of the current LBC methods. Using the HBA, optimization and improved constraint management is accomplished. The XTEA and HBA algorithms are each individually discussed to comprehend the functionality of the encryption/decryption process and create the hardware architectures. The key schedule mechanism for each block cipher module runs concurrently with the encryption/decryption modules. Basic algebraic operations like counters, shifters, adders, registers, and subtractors are used in designing the XTEA and HBA modules.

A. EXTENDED TINY ENCRYPTION ALGORITHM (XTEA)

The drawbacks of the tiny encryption algorithm (TEA) is resolved using XTEA. This improves the security and performance over TEA by incorporating pipelining mechanism. The XTEA has 128-bit key with a 64-bit block size. It contains three main processes: key scheduling, encryption, and decryption. All these three processes are operated based counting (c) mechanism. The encryption and decryption process works based on mode (m) in the proposed XTEA. If the mode 'm' is '0', then it is encryption; else decryption process. The key scheduling operation occurs during the counting operations of '0' and '2'. The key scheduling output (K_o) is obtained for the encryption and decryption process using (1) to (4).

$$Enc: K_0 = K[3\&X_E] + X_E; \quad if(c = 0) \tag{1}$$
$$Enc: K_0 = K[3\&X_E >> 11] + X_E; if(c = 2) \tag{2}$$
$$Dec: K_0 = K[3\&X_D >> 11] + X_D; \quad if(c = 0) \tag{3}$$
$$Dec: K_0 = K[3\&X_D] + X_D; \quad if(c = 2) \tag{4}$$

In these equations, $X_E = \alpha_1 + \delta_1$ during encryption and $X_D = \delta_2 - \delta_2$ during the decryption operation. The 'α' and 'δ' are the constant–coefficient values in the key scheduling process. The '&,' '$\wedge$' '$\ll$,' and '$\gg$' are AND, XOR, Shift–left, and right logical operators respectively. The round function (RF) process is designed based on the Feistel structure and is the same for encryption and decryption processes. The round function (RF) output is generated using key scheduling output, and is represented using (5).

$$RF_0 = ((RF_i \gg 5) \wedge (RF_i \ll 4) + RF_i) \wedge K_0 \tag{5}$$

As shown in Algorithm 1, the XTEA has three operational phases, namely: pre-processing, round function, and output generation phases. The 64-bit input (P_i) is divided into two 32-bit blocks, P_0 and P_1. The round function works based on the counter. When the counter (c) is zero, the second input (P_1) is input to the RF. If the mode 'm' is 0, then the first input (P_0) is added with RF output (RF_0) and stored in P_0 during count $c = 1$. Similarly, if the mode 'm' is '1', then RF_0 is subtracted from the first input and stored in P_0. The operation $c =$ '2' and '3' is the same as '0' and '1', respectively, by replacing P_0 with P_1. Lastly, the XTEA output is generated using P_0 and P_1 data. For encryption ($m = 0$) operation, the cipher text (E_T) is generated by concatenating the P_0 followed by P_1 to form the 64-bit output. Similarly, for the decryption ($m = 1$) operation, the recovered text (D_T) is generated by concatenating the P_1 followed by P_0 to form the 64-bit output.

B. HUMMINGBIRD ALGORITHM (HBA)

The HBA, has both stream and block cipher combinations, which is suitable for ultra–lightweight and low–constrained devices to enhance security features. The HBA supports 16-bit input and 256-bit key for encryption and decryption process. The flow of the HBA for encryption is shown in Algorithm 2. The HBA starts with initialization, followed by the encryption stage. Initially four different initialization vectors or nonces (N_1, N_2, N_3, and N_4) are defined and are used further in the state register initialization process. The random values of four nonces are stored initially in the four registers (R_1, R_2, R_3, and R_4). The linear feedback shift register (LFSR) value is defined during the initialization stage. The encryption stage contains mainly two operations: block encryption (E) operation and internal state updation. The HBA operates with four rounds (r) during the encryption stage.

The block encryption (E) operation contains mainly registers, substitution boxes (S-Box), and linear transformations, followed by add round key (ARK). The 256-bit key is divided into four subkeys $K1$, $K2$, $K3$, and $K4$. Each of the four subkeys is iterated with four operation rounds during block encryption. The first register ($R1$) is XOR with Input data (I_i) and stored in stage output ($T1$). Similarly, the remaining registers ($R2$, $R3$, and $R3$) undergoes XOR operation with previous stage outputs of block encryption. ($T1$, $T2$, and $T3$) generate the stage outputs ($T2$, $T3$, and CT_i). Each

Algorithm 2 Hummingbird Algorithm for Encryption

Input: Nonce Initialization: N_1, N_2, N_3, and N_4; 16-bit input Text (I_i) and 256-bit key (composed into K_1, K_2, K_3, and K_4)

Output: E_T or D_T

- **Initialization Stage**
  1. Register (State) formation $R1$, $R2$, $R3$, and $R4$ using nonces.
     I. $R1 = N_1$;
     II. $R2 = N_2$;
     III. $R3 = N_3$;
     IV. $R4 = N_4$;
  2. Initialization of LFSR:
     I. LFSR = 16'haaaa;
- **Encryption Stage**
  1. Total Rounds r = 0, 1, 2, 3;
  2. Operation of Block Encryption (E):
     I. $T1 = E_{K1}\ (I_i \boxplus R1_r)$;
     II. $T2 = E_{K2}\ (T1_r \boxplus R2_r)$;
     III. $T3 = E_{K3}\ (T2_r \boxplus R3_r)$;
     IV. $CT_i = E_{K4}\ (T3_r \boxplus R4_r)$;
  3. Internal state Updation:
     I. $LFSR_{r+1} = LFSR_r$;
     II. $R1_{r+1} = R1_r \boxplus T3r$;
     III. $R2_{r+1} = R2_r \boxplus T1_r \boxplus R4_{r+1}$;
     IV. $R3_{r+1} = R3_r \boxplus T2_r \boxplus LFSR_{r+1}$;
     V. $R4_{r+1} = R4_r \boxplus T1_r \boxplus R1_{r+1}$;
  4. Return CT_i and loop completes

stage output is operated with four rounds during block encryption. The last stage of operation produces the cipher text (CT_i). The internal state updation is operated parallel to the block encryption process. This internal state updation updates the state registers using stage outputs and an LFSR. The decryption operation is the reverse process of encryption in the HBA.

III. AUTHENTICATION OF RFID DEVICES USING LBC

The RFID-MA module implements the XTEA and HBA block cipher, which are built block-wise using CBC mode. The RFID-MA with XTEA and HBA crypto system for the tag and reader raises security and privacy issues. Two procedures are used to establish MA between the tag and reader: (1) Tag identifying using the encryption scheme (XTEA or HBA), and (2) XTEA or HBA-based tag and reader authentication. In order to establish interaction, the reader requests the tag unit, which then creates random value to use as user identity. Tag recognition is successful when a random value is encrypted using XTEA or HBA. To recover the identical random data later, the decryption operation of XTEA or HBA is performed. Figure 1 depicts the RFID-MA protocol using XTEA or HBA algorithm using CBC Mode.

TABLE 1. Execution process of RFID-MA using HB and XTEA.

Si. No	RFID-MA operation	Using HB (μs)	Using XTEA (μs)
1	Random data Generation (Random_Gen-1,2)	0.155	0.605
2	From Reader to Tag: Challenge Gen. (Reader_Challenge-1,2)	0.25	2.585
3	In Tag: Challenge operation (Tag_Challenge-1,2)	0.25	2.58
4	In Tag: Random Generation (Random_Gen-3)	0.165	0.61
5	In Tag: Reader Authentication successful	0.015	0.02
6	From Tag to Reader: Tag Response Gen. (Tag_Response-1,2)	0.25	2.56
7	In Reader: Reader Response Gen. (Reader_Response-1,2)	0.24	2.58
8	In Reader: Tag Authentication Successful	0.015	0.02
Total Execution Time (µsec)		**1.34**	**11.555**

The two times of encryption and decryption operations using the XTEA or HB methods are performed to establish RFID MA. The 16/64-bit random number generation (RNG1, RNG2, and RNG3), reader challenge (CL), tag challenge (CT), tag response (RP), and reader response (RR) are the primary components of the RFID-MA process. To start the entire RFID-MA operation, the reader issues a request to the tag. The tag then transmits the reader's random number (RNG1). To conduct the XTEA or HB decryption operation utilizing RNG1 and RNG2 in CBC mode, the reader gets RNG1 and creates RNG2, which is then used. The reader challenge (CL1, CL2) denotes that decryption results are transmitted to the tag during authentication. To create the tag challenge, the tag will use CL data to process the XTEA or HB encryption procedure (CT1, CT2). In response to the reader, the tag creates the 16/64-bit Random Number RNG3. The reader authentication process is effective if the tag challenge (CT2) matches RNG1.

The tag uses the tag challenge (CT2) and RNG3 data to encrypt the response data (RP1 and RP2) before providing it to the user. After the reader obtains the tag Response data, it uses XTEA or HB decryption to create the reader response (RR1 and RR2). The tag authentication process is successful if the reader response (RR1) matches the RNG2. The MA is established between the RFID Tag and reader if both the tag and the reader are verified.

IV. RESULTS AND DISCUSSION

The results of LBCs like XTEA and HBA and their MA for RFID devices are discussed in this section. The RFID-based MA using XTEA and HBA architectures is implemented using Xilinx integrated synthesis environment (ISE) environment with Verilog HDL on Artix-7 FPGA. The mutually authenticated outputs are verified using a Modelsim Simulator. The resource constraints like chip area (Slices, LUTs, and LUT-FF pairs), frequency, and power are analyzed after place and route operation on the Xilinx ISE environment.

Figure 2(a) displays the RFID-MA simulation results for XTEA. A global clock (clk) and a reset (rst) signal are both inputs for the design module. There are four output

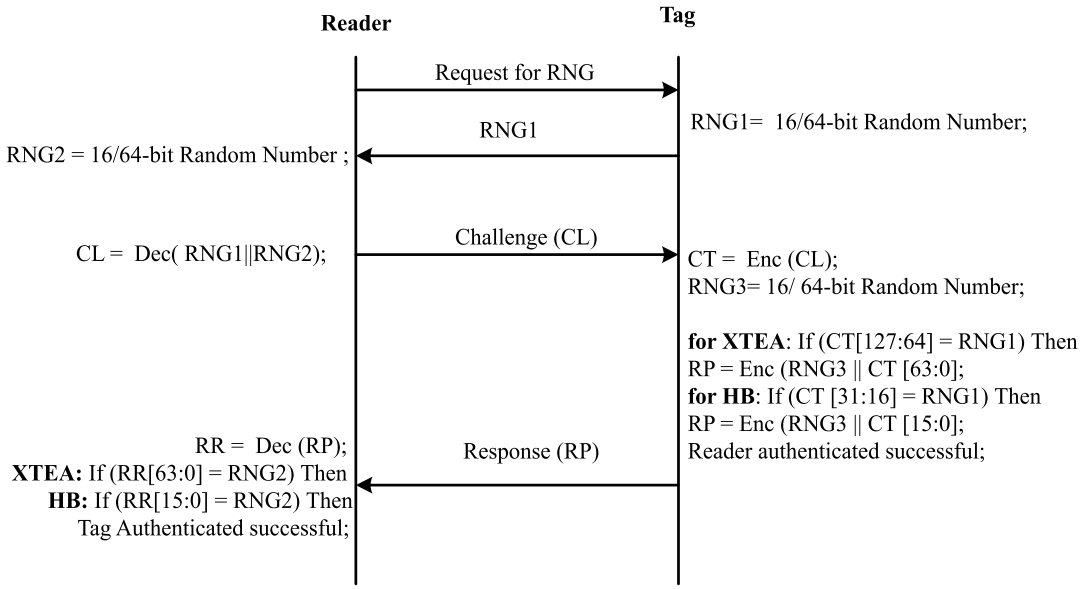
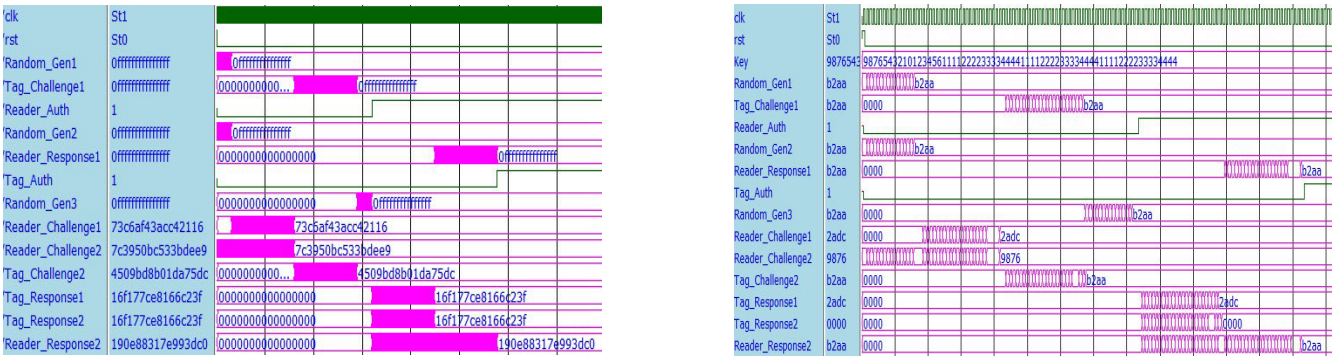


FIGURE 1. RFID-MA protocol using XTEA or HBA cipher.



(a) (b)

FIGURE 2. Simulation results of RFID-MA using (a) XTEA algorithm (b) HB algorithm.

signals: a 1–bit reader authentication signal (Reader_Auth), a 64–bit tag challenge signal (Tag_Challenge1), and a reader response signal (Reader_Response1). On the other hand, for the RFID–MA system employing the HB algorithm, the simulation results are displayed in Figure 2(b). The RFID–MA using HB module takes inputs such as the global clock (clk), reset (rst), and a 256-bit key. Output signals consist of 1-bit reader authentication (Reader_Auth), tag authentication (Tag_Auth), 64-bit tag challenge (Tag_Challenge1), and reader response (Reader_Response1).

During the simulation operation, the global clock (clk) is activated while the reset signal is low. The RFID-MA process initiates with the generation of 64-bit random numbers RN1 and RN2 using LFSR at the tag and reader respectively. The reader challenge data (Reader_ch1 and Reader_ch2) is generated through XTEA or HB decryption operations at the Reader side. Similarly, the new 64-bit random number RN3 is generated using LFSR at the tag side. The tag challenge data (Tag_ch1 and Tag_ch2) is produced by performing XTEA or HB encryption operations at the Tag side. Likewise, the tag response data (Tag_Resp1 and Tag_Resp2) is generated through XTEA or HB encryption operations at the tag side. The reader response data (Reader_Resp1 and Reader_Resp2) is created by performing XTEA or HB decryption operations at the reader side. These simulation operations demonstrate the functioning of RFID-MA using XTEA and HB algorithms, showcasing the generation of various challenge and response data for authentication between the RFID tag and the reader.

Table 1 provides the execution times for each operation or process in RFID–MA using XTEA and HB modules, measured in clock cycles (μs), specifically for NFC applications. It illustrates the efficiency of the RFID-MA using HB and XTEA modules. These times, measured in clock cycles, highlight the time taken to complete authentication stages. In the RFID-MA system, an eight-stage operation is performed using XTEA and HB at CBC code to establish authentication between the RFID tag and reader. To complete the security evaluation of RFID tag and reader in NFC applications, the total execution time required is 11.555 μs for XTEA and 1.34 μs for the HB algorithm. Comparatively, the execution time in RFID-MA using HB is better than

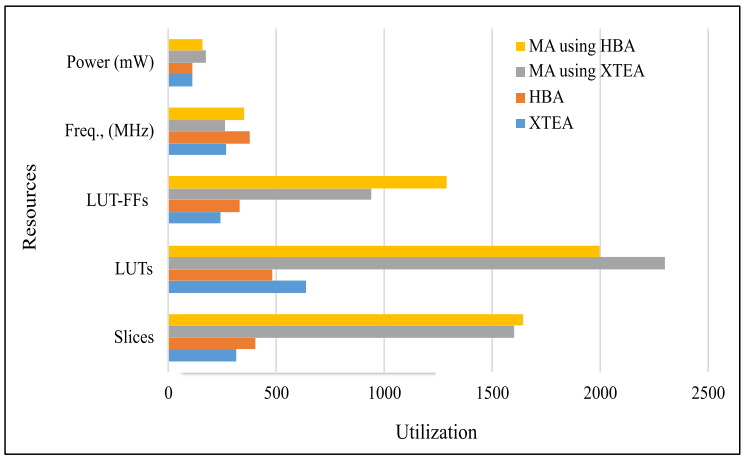


FIGURE 3. Graphical representation of proposed designs.

TABLE 2. Performance analysis of XTEA and HBA on Artix-7 FPGA.

Resources	XTEA	HBA
Slices	312	402
LUTs	638	481
LUT-FFs	240	332
Max. Frequency (MHz)	265	377
Power (mW)	112	108
Latency (CC)	128	12
Throughput (Mbps)	133	503
Efficiency (Slice/Mbps)	0.43	1.25

TABLE 3. Resource constraints analysis of RFID based MA using XTEA and HBA on Artix-7 FPGA.

Resources	MA using XTEA	MA using HBA
Slices	1602	1645
LUTs	2301	1998
LUT-FFs	940	1289
Max. Frequency (MHz)	262	349
Power (mW)	172	155
Execution Time (µs)	11.6	1.34

in RFID–MA using the XTEA process. The significant difference between the execution times of XTEA and HB indicates the superiority of the HB algorithm in terms of speed and efficiency.

The performance analysis of XTEA and HBA on Artix-7 FPGA are tabulated in Table 2. The XTEA cipher utilizes slices of 312 and LUT's of 638 by operating at 265 MHz frequency and consuming power of 112 mW. In contrast, the HBA utilizes 402 slices and LUTs of 481 by operating at 377 MHz frequency and consuming power of 108 mW. The XTEA cipher generates the encrypted output in 128 clock cycles (CC) and achieves a throughput of 133 Mbps with a hardware efficiency of 0.43 Mbps/slice. Similarly, the HBA cipher obtains the encrypted output in 12 CC and achieves a throughput of 503 Mbps with a hardware efficiency of 1.25 Mbps/slice. The differing slice utilization, LUT counts, and operating frequencies provide a basis for understanding their resource utilization and power consumption. The contrast in latency and throughput emphasizes how design choices impact data processing and transmission efficiency.

The resource constraints analysis of RFID–based MA using XTEA and HBA on Artix-7 FPGA are tabulated in Table 3. The RFID–based MA using XTEA utilizes slices of 1602 and LUTs of 2301 by operating 262 MHz frequency and consuming power of 172 mW. In contrast, the RFID-based MA using HBA utilizes slices of 1645 LUTs of 1998 by operating 349 MHz frequency and consuming power of 155 mW. The Tag and Reader are mutually authenticated with an execution time of 11.6 μs and 1.34 μs using RFID-based MA using XTEA and HBA, respectively. The utilization of slices and LUTs alongside operating frequencies and power consumption elucidates the trade–offs between XTEA and HBA. This understanding extends to their execution times and the mutual authentication process, showcasing the efficiency gains made possible by the HB algorithm.

The graphical representation concerning the performance metrics of the RFID–based MA using XTEA and HBA architectures is illustrated in Figure 3. The HBA cipher provides better performance results and is improved by approximately 24.6% in LUTs, 29.7% in frequency, 3.5% in total power, 90.25% in latency, 73.5% in throughput, and 65.6% in efficiency than the XTEA cipher. In contrast, The RFID based MA using HBA provides better performance results and improved by around 13.16% in LUTs, 24.92% in frequency, 12.42% in total power, and 88.36% in execution time than RFID-based MA using XTEA.

The performance comparison of the proposed XTEA and HBA with existing approaches [25], [26], [27], [28] is tabulated in Table 4. The block size, key length, chip area (slices), latency, throughput, and efficiency parameters are considered for comparative study at different FPGAs. The tiny XTEA-1 is designed on Spartan-3 FPGA, utilizes 266 slices, and operates with a throughput of 19 Mbps. The proposed XTEA cipher provides a better chip area of 10.52%, latency of 46.67%, and throughput of 76.55% than the tiny XTEA-1 cipher [25]. The tiny XTEA-3 is designed on Spartan-3 FPGA, utilizes 254 slices, and operates with a throughput of 37 Mbps. The proposed XTEA cipher provides a better chip area of 6.3%, Latency of 3.03%, and

TABLE 4. Performance comparison of proposed XTEA and HBA with existing approaches [25], [26], [27], [28].

Block Ciphers	Block Size	Key size	FPGA	Area (Slices)	Latency (CC)	Throughput (Mbps)	Efficiency (Mbps/Slice)
XTEA Comparison							
Tiny XTEA-1 [25]	64	128	Spartan-3	266	240	19	0.07
Tiny XTEA-3 [25]	64	128	Spartan-3	254	132	37	0.014
XTEA [26]	64	128	Spartan-3	332	128	79	0.24
Proposed XTEA	64	128	Spartan-3	238	128	81	0.34
HB Comparison							
HB-2 [27]	16	256	Spartan-3	485	16	172	0.36
HB [28]	16	256	Cyclone-2	482	16	234	0.49
Proposed HBA	16	256	Spartan-3	408	12	300	0.74

TABLE 5. Performance comparison of RFID based MA with existing approach [29].

Resources	MA using PRESENT [29]	MA using XTEA [29]	MA using HBA [29]	Proposed MA using XTEA	Proposed MA using HBA
FPGA	Spartan-3	Spartan-3	Spartan-3	Spartan-3	Spartan-3
Slices	22.32 K	22.55 K	22.30 K	1.22 K	1.29 K
LUTs	42.85 K	43.32 K	41.9 K	2.23 K	2.03 K
LUT-FFs	2.56 K	2.6 K	2.42 K	1.14 K	1.72 K
Max. Frequency (MHz)	59	61	41	126	195

throughput of 54.33% than the Tiny XTEA-3 cipher [25]. The XTEA cipher [26] is designed on Spartan-3 FPGA, utilizes 332 slices, and operates with a throughput of 79 Mbps. The proposed XTEA cipher provides a better chip area of 28.3% and throughput of 2.4% than the XTEA cipher [26]. In contrast, the HB-2 [27] is designed on Spartan-3 FPGA, utilizes 485 slices, and operates with a throughput of 172 Mbps. The proposed HB cipher provides a better chip area of 15.88%, latency of 25%, and throughput of 42.6% than the HB-2 cipher [27]. The HB [28] is designed on Cyclone -2 FPGA, utilizes 482 slices, and operates with a throughput of 234 Mbps. The proposed HB cipher provides a better chip area of 15.3%, Latency of 25%, and throughput of 22% than the HB cipher [28].

The performance comparison of RFID–based MA using XTEA and HBA with the existing approach [29] using Spartan-3 FPGA is tabulated in Table 5. As seen in the table, the proposed RFID-based MA using XTEA and HBA approaches better chip area (Slices, LUTs, and LUT-FFs) and maximum operating frequency than existing MA using present XTEA, and HBA approaches [29].

V. CONCLUSION

This manuscript presents a comprehensive approach to achieving secured authentication for RFID devices through the utilization of LBCs on the FPGA platform. The detailed discussion on LBCs, specifically the XTEA and HBA algorithms, highlights their significant role in enhancing security and performance. The key focus lies in establishing mutual authentication between RFID tags and readers to ensure a secure communication channel. The individual design and implementation of XTEA and HBA within the Xilinx ISE environment and their successful realization on the Artix–7 FPGA platform mark a critical step in validating the feasibility of our proposed approach. Notably, both XTEA and HBA demonstrate impressive operational characteristics with modest resource utilization. XTEA operates at an average frequency of 321 MHz while consuming 112 mW, exhibiting a latency of 128 clock cycles and a throughput of 133 Mbps. In contrast, HBA showcases even better performance metrics with a latency of 12 clock cycles, a throughput of 503 Mbps, and power consumption of 108 mW. Comparing the proposed RFID-MA using HBA with RFID–MA using XTEA underlines the superiority of the former, as evidenced by superior chip area, power efficiency, and execution time. Future research could delve deeper into the security aspects of LBCs within the context of RFID devices. Exploring their robustness against various attacks and vulnerabilities will provide valuable insights into further fortifying the authentication mechanisms. As the IoT landscape continues to evolve, incorporating the proposed LBC-based authentication approach into emerging technologies such as edge computing, blockchain, and AI will pave the way for even more secure and efficient communication protocols.

REFERENCES

[1] M. Feldhofer and J. Wolkerstorfer, "Hardware implementation of symmetric algorithms for RFID security," in *RFID Security: Techniques, Protocols and System-on-Chip Design*. Boston, MA, USA: Springer, 2008, pp. 373–415.

[2] A. Ibrahim and G. Dalkılıc, "Review of different classes of RFID authentication protocols," *Wireless Netw.*, vol. 25, no. 3, pp. 961–974, Apr. 2019.

[3] Y. S. Kang, E. O'Sullivan, D. Choi, and M. O'Neill, "Security analysis on RFID mutual authentication protocol," in *Proc. Int. Workshop Inf. Secur. Appl.* Cham, Switzerland: Springer, 2016, pp. 65–074.

[4] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues," *J. Netw. Comput. Appl.*, vol. 58, pp. 73–93, Dec. 2015.

[5] I. Bhardwaj, A. Kumar, and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," in *Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Sep. 2017, pp. 504–509.

[6] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *J. Cryptograph. Eng.*, vol. 8, no. 2, pp. 141–184, Jun. 2018.

[7] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for IoT devices," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2018, pp. 1–8.

[8] S. Dutta and S. Chakraborty, "A survey on implementation of lightweight block ciphers for resource constraints devices," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 5, pp. 1377–1398, Jul. 2022.

[9] S. Maitra, D. Richards, A. Abdelgawad, and K. Yelamarthi, "Performance evaluation of IoT encryption algorithms: Memory, timing, and energy," in *Proc. IEEE Sensors Appl. Symp. (SAS)*, Mar. 2019, pp. 1–6.
[10] C. Trinh, B. Huynh, J. Lansky, S. Mildeova, M. Safkhani, N. Bagheri, S. Kumari, and M. Hosseinzadeh, "A novel lightweight block cipher-based mutual authentication protocol for constrained environments," *IEEE Access*, vol. 8, pp. 165536–165550, 2020.
[11] F. Zhu, "SecMAP: A secure RFID mutual authentication protocol for healthcare systems," *IEEE Access*, vol. 8, pp. 192192–192205, 2020.
[12] M. Hosseinzadeh, J. Lansky, A. M. Rahmani, C. Trinh, M. Safkhani, N. Bagheri, and B. Huynh, "A new strong adversary model for RFID authentication protocols," *IEEE Access*, vol. 8, pp. 125029–125045, 2020.
[13] M. Hosseinzadeh, O. H. Ahmed, S. H. Ahmed, C. Trinh, N. Bagheri, S. Kumari, J. Lansky, and B. Huynh, "An enhanced authentication protocol for RFID systems," *IEEE Access*, vol. 8, pp. 126977–126987, 2020.
[14] H. Xu, X. Yin, F. Zhu, and P. Li, "An enhanced secure authentication scheme with one more tag for RFID systems," *IEEE Sensors J.*, vol. 21, no. 15, pp. 17189–17199, Aug. 2021.
[15] S. Gabsi, Y. Kortli, V. Beroulle, Y. Kieffer, A. Alasiry, and B. Hamdi, "Novel ECC-based RFID mutual authentication protocol for emerging IoT applications," *IEEE Access*, vol. 9, pp. 130895–130913, 2021.
[16] T. A. Idriss, H. A. Idriss, and M. A. Bayoumi, "A lightweight PUF-based authentication protocol using secret pattern recognition for constrained IoT devices," *IEEE Access*, vol. 9, pp. 80546–80558, 2021.
[17] S. Sharma, B. Kaushik, M. K. I. Rahmani, and Md. E. Ahmed, "Cryptographic solution-based secure elliptic curve cryptography enabled radio frequency identification mutual authentication protocol for Internet of Vehicles," *IEEE Access*, vol. 9, pp. 147114–147128, 2021.
[18] S. Khan, W.-K. Lee, and S. O. Hwang, "A flexible Gimli hardware implementation in FPGA and its application to RFID authentication protocols," *IEEE Access*, vol. 9, pp. 105327–105340, 2021.
[19] U. Ali, M. Y. I. B. Idris, M. N. B. Ayub, I. Ullah, I. Ali, T. Nandy, M. Yahuza, and N. Khan, "RFID authentication scheme based on hyperelliptic curve signcryption," *IEEE Access*, vol. 9, pp. 49942–49959, 2021.
[20] Z. U. Rehman, S. Altaf, S. Ahmad, S. Huda, A. M. Al-Shayea, and S. Iqbal, "An efficient, hybrid authentication using ECG and lightweight cryptographic scheme for WBAN," *IEEE Access*, vol. 9, pp. 133809–133819, 2021.
[21] X. Zhong, M. Xiao, T. Zhang, K. Yang, and Y. Luo, "Proving mutual authentication property of RCIA protocol in RFID based on logic of events," *Chin. J. Electron.*, vol. 31, no. 1, pp. 79–88, Jan. 2022.
[22] A. S. Khan, Y. Javed, R. M. Saqib, Z. Ahmad, J. Abdullah, K. Zen, I. A. Abbasi, and N. A. Khan, "Lightweight multifactor authentication scheme for NextGen cellular networks," *IEEE Access*, vol. 10, pp. 31273–31288, 2022.
[23] S. U. Jan, I. A. Abbasi, and M. A. Alqarni, "LMAS-SHS: A lightweight mutual authentication scheme for smart home surveillance," *IEEE Access*, vol. 10, pp. 52791–52803, 2022.
[24] P. K. Maurya, H. Ghosh, and S. Bagchi, "MDS code based ultralightweight authentication protocol for RFID system," *IEEE Access*, vol. 11, pp. 10563–10577, 2023.
[25] J. P. Kaps, "Chai-tea, cryptographic hardware implementations of XTEA," in *Proc. Int. Conf. Cryptol. India*. Berlin, Germany: Springer, Dec. 2008, pp. 363–375.
[26] R. Anusha and V. Shastrimath, "FID-MA XTEA: Cost-effective RFID-mutual authentication design using XTEA security on FPGA platform," *Int. J. Electron. Telecommun.*, vol. 67, pp. 1–11, Jan. 2021.
[27] T. Harikrishnan and C. Babu, "Cryptanalysis of hummingbird algorithm with improved security and throughput," in *Proc. Int. Conf. VLSI Syst., Archit., Technol. Appl. (VLSI-SATA)*, Jan. 2015, pp. 1–6.
[28] M. A. Haque and M. L. Ali, "Design of a hummingbird crypto core implementing BIST technique," in *Proc. 9th Int. Conf. Electr. Comput. Eng. (ICECE)*, Dec. 2016, pp. 82–85.
[29] S. Seshabhattar, S. K. Jagannatha, and D. W. Engels, "Security implementation within GEN2 protocol," in *Proc. IEEE Int. Conf. RFID-Technol. Appl.*, Sep. 2011, pp. 402–407.

ANUSHA R received the B.E. degree in electronics and communication engineering and the M.Tech. degree in VLSI and embedded systems from the NMAM Institute of Technology, Nitte, Karnataka, India, in 2012 and 2014, respectively, and the Ph.D. degree from the Department of Electronics and Communication, Visvesvaraya Technological University (VTU), Belagavi, in 2022. She is currently an Assistant Professor with the Department of Electronics and Communication Engineering, NMAM Institute of Technology. Her current research interests include cryptography, NFC security, frontend VLSI, and embedded systems.

RAGHAVENDRA RAO P received the B.E. degree in electrical and electronics engineering and the M.Tech. degree in microelectronics and control systems from the NMAM Institute of Technology, Nitte, Karnataka, India, in 2012 and 2015, respectively, and the Ph.D. degree from the Department of Electrical and Electronics Engineering, National Institute of Technology Karnataka (NITK), Surathkal, India, in 2022. He is currently an Assistant Professor with the Department of Mechatronics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal. His research interests include FPGA, VLSI, application of power electronics in renewable energy systems, and power electronic converters control.

PRATHEKSHA RAI N received the B.E. degree in electronics and communication engineering and the M.Tech. degree in digital electronics from the Sahyadri College of Engineering and Management, Mangalore, India, in 2012 and 2018, respectively. She is currently an Assistant Professor with the Department of Electronics and Communication Engineering, A. J. Institute of Engineering and Technology, Mangalore. Her research interests include cryptography, FPGA, frontend VLSI, and embedded systems.