

Design and implementation of a cryptographic algorithm based on the AES advanced encryption standard for UHF RFID systems

Sanae Habibi, Zahra Sahel, Abdelhak Bendali, Abid Reda El Wardi, Samia Zarrik, Mouad El Kobbi, Nazha Cherkaoui, Abdelkader Hadjoudja

Department of Physics, Laboratory of Electronic Systems, Information Processing, Mechanics and Energy, Faculty of Science, Ibn Tofail University, Kenitra, Morocco

Article Info

Article history:

Received Jul 12, 2023

Revised Feb 27, 2024

Accepted Mar 4, 2024

Keywords:

Advanced encryption standard
Cryptographic
Field-programmable gate array
Radio frequency identification
ultra-high-frequency
Security
Xilinx

ABSTRACT

In this paper, a proposal is made for a cryptographic algorithm designed for passive ultra-high-frequency (UHF) radio frequency identification systems. The algorithm relies on the advanced encryption standard (AES) as its fundamental encryption technique, augmented by two supplementary steps: the initial step involves generating a random key and the second is the randomization of data, this introduces an extra level of security to encryption process against attacks. The developed architecture has been optimized to minimize hardware resource consumption with faster execution speed. The algorithm has been simulated, synthesized and implemented in an xtime digital signal processing (DSP) starter kit equipped with xilinx's spartan-3A DSP 1800A edition and it serves the purpose of encrypting and decrypting user data on a radio frequency identification (RFID) passive tag. The main objective is to make it difficult to break the algorithm because of its multiple steps. The experimental results showed that the speed, functionality and cost of encryption and decryption make this a perfectly practical solution, providing a satisfactory level of security for today's communications systems, or other electronic data transfer processes where security is required.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Sanae Habibi

Department of Physics, Laboratory of Electronic Systems, Information Processing

Mechanics and Energy, Faculty of Sciences, Ibn Tofail University

Kenitra, Morocco

Email: sanae.habibi@uit.ac.ma

1. INTRODUCTION

Radio frequency identification (RFID) is a method of storing and retrieving data remotely. The RFID tag comprises an electronic chip and an antenna which detects the radio signal transmitted by the reader. Upon receiving a radio wave by tag from an RFID reader device, it immediately sends digital information to the reader. There are two types of RFID tags: active tags, fitted with a battery, and passive tags, without a battery [1]. Passive RFID systems use backscatter modulation. During communication, the reader emits a modulated signal which is picked up by the tag's antenna. An RF voltage generated at the antenna input is applied to power the chip, which returns the information by modifying its complex RF input impedance [2]. Modulation of the backscattered signal is achieved by varying the impedance between two distinct states: impedance matching and mismatching [2].

In RFID technology, the distribution of information poses a problem in terms of confidentiality and security. An unsecured card can easily be copied to retrieve or modify confidential information. Some research has been carried out to solve the security and confidentiality problems posed by RFID [3]–[5]. Implementing

an authentication process stands out as one of the most effective methods to ensure security and privacy measures.

Although public key algorithms offer enhanced security, their high computing power requirements make them challenging to implement in low-cost RFID systems. Advances in RFID technology and low-power circuits have led to growing acceptance of public-key algorithms in RFID systems. RFID authentication using elliptic curve cryptography is proposed in articles [6], [7]. In [8], the rivest shamir adleman (RSA) electronic signature is used for electronic cards. Because of their cost-effectiveness and low power consumption, ultra-high-frequency (UHF) RFID tags are largely used. Intricate cryptographic processes may not be suitable for chip design in low-cost applications. Efforts are directed towards investigating lightweight security protocols and algorithms to minimize costs while ensuring high security. To diminish computational complexity, the computational resources of the protocols are assumed and extended. An encryption protocol that combines the advanced encryption standard (AES) and elliptic curve cryptography (ECC) algorithms to enhance RFID data security is proposed in paper [9], this approach aims to achieve optimal effectiveness and efficiency in safeguarding the information. In [10], data security is ensured by using peak modulation and backscattering to simultaneously modulate sensor and identification (ID) information. In [11], the authors have developed an algorithm that effectively secures the information stored in RFID tags through the use of triple DES and RSA encryption.

In this paper, a cryptographic algorithm designed for passive UHF radio frequency identification systems. The algorithm relies on the AES as its fundamental encryption technique, augmented by two supplementary steps: the initial step involves generating a random key and the second is the randomization of data, this introduces an extra level of security to encryption process against attacks.

The paper is structured as: first, section 2 describes the method proposed of cryptographic algorithm. Results, discussion and comparative analysis between the proposed algorithm and other circuits produced are featured in section 3. Finally, we conclude the document in the fourth section.

2. METHOD OF THE CRYPTOGRAPHIC ALGORITHM

2.1. Description of the proposed encryption algorithm

Figure 1(a) displays a functional diagram of the encryption process, while Figure 1(b) illustrates the decryption process. The encryption process involves three primary stages. The initial step incorporates a function that generates a random key according to the tag's electronic product code. Subsequently, the AES encryption algorithm is applied. Finally, the encrypted data undergoes a randomization process.

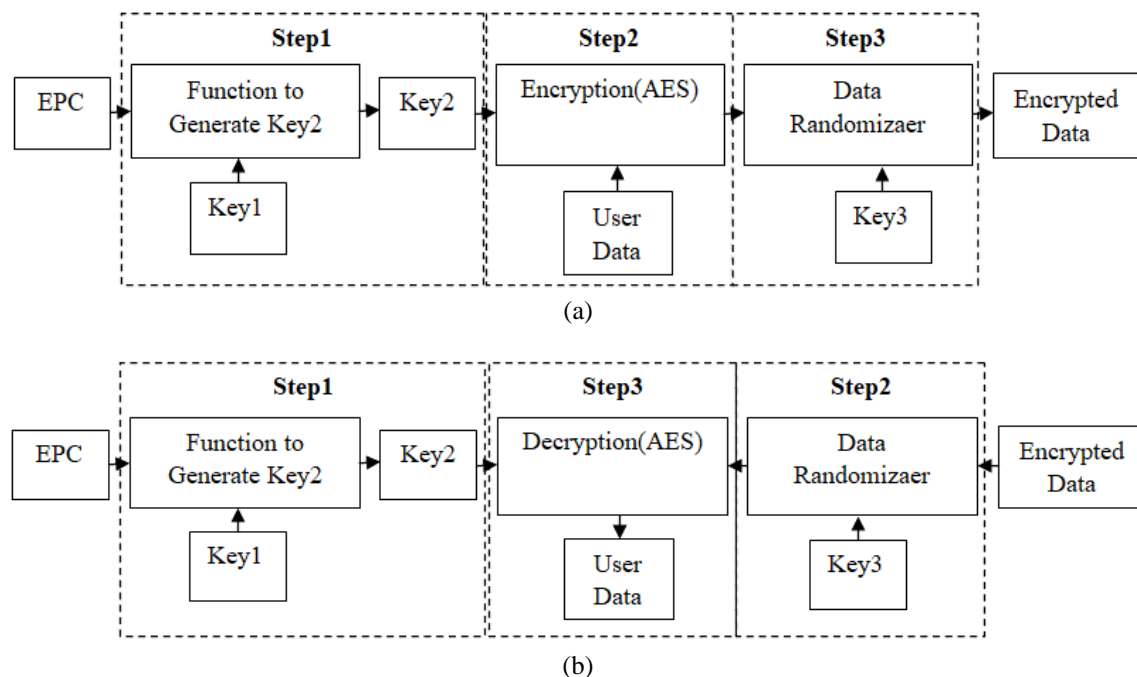


Figure 1. System block diagram: (a) encryption and (b) decryption

2.1.1. Encryption

The algorithm relies on the AES as its fundamental encryption technique. The encryption process comprises three main stages. The initial step includes a function that generates a random key based on the electronic product code (EPC) of the label. Next, the AES encryption algorithm is applied. Finally, the encrypted data is subjected to a randomisation process. In this section, we will describe the different stages of encryption.

a. Step 1: generation of random key

In this step, the tag’s transient ischemic dilation (TID) is fed into a function that generates a unique random key for each tag. The method used in this document is a simplified Exclusively-OR (XOR), i.e., the first 128 bits of the TID are XORed against a randomly generating 128-bit key 1. The 128-bit key 2 is then used in the next step. Note that key 1 must be retained for the decryption process.

b. Step 2: AES encryption

AES is a symmetrical encryption algorithm, where the same key is used for both encrypting and decrypting a text. It works with fixed-size data blocks, each block being an array of 4×4 bytes. Each cell in this array is called a word as shown in Figure 2, with each cell representing a byte in the state [12]. Each round comprises of 4 steps:

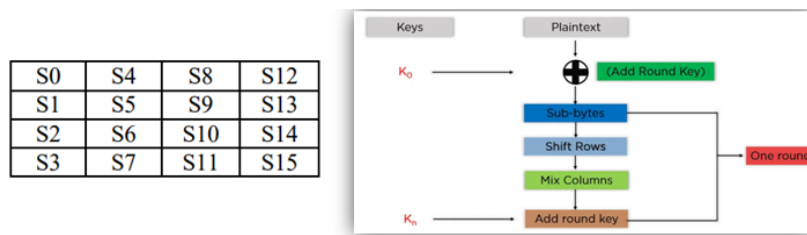


Figure 2. AES data structure [12]

- SubBytes: the SubBytes method is a byte substitution that works independently on each byte. It relies on a look-up table known as the S-Box to replace each byte with another byte [13]. The S-Box table consists of 256 numbers and their respective values [13].
- ShiftRows: in ShiftRows conversion, the report lines are shifted cylindrically to the left. The first line remains unchanged. The second line is shifted circularly to the left by 1 byte. The third and fourth lines are similarly shifted circularly to the left by 2 bytes and 3 bytes respectively [14].
- MixColumns: in MixColumns, columns are treated as polynomials and multiplied modulo x^4+1 with a specified polynomial $c(x)$ [15]. In this process, any byte in a column undergoes conversion to another value, obtained through interaction between the four bytes in the column. This conversion is performed by multiplication of matrix on state. Any element in the product table is the sum of the products of the elements in a row and a column [16].
- AddRoundKey: the AddRoundKey function is very simple. It is based on an exclusive or between the 128 bits of the state and the 128 bits of the round key. The result is a new state value. Figure 3 represents the structure of AES algorithm. AES is modifiable and dependent on key length. The secret key is 128 bits long, hence the version name AES 128. There are two other variants with keys of 192 and 256 bits respectively [17].

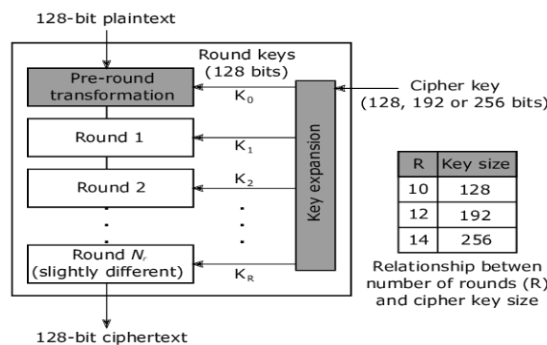


Figure 3. 128, 192 or 256-bit key AES algorithm

c. Step 3: data randomization

Randomization is used in cryptography to add an additional layer of safety to the encryption procedure. It is used to generate random numbers that are used as keys or initialization vectors (IVs) in encryption algorithms such as AES. Randomization helps to prevent attacks such as brute-force attacks and dictionary attacks.

Figure 4 shows a random number generator using 12-stage [18]. Key3 is a 12-byte random vector employed as the starting vector for the 12 stages of the pseudo-random bit sequence (PRBS). Key3 must be kept for use in the decryption procedure.

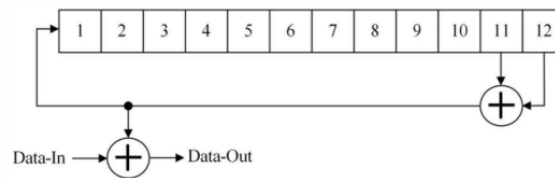


Figure 4. Random number generator using 12-stage

2.1.2. Decryption

The decryption procedure comprises three main stages, as shown in Figure 1(b). Decryption involves reversing the encryption, i.e., reverse conversions are performed in the opposite direction to obtain the original message from an encrypted message, with the same encryption key. Round conversion during decryption involves the successive application of the AddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes functions [19].

2.2. Description of the architecture of the developed circuit

In this part, the description of the architecture of the different modules of the AES encryption/decryption circuit will be presented, as well as the different VHDL models of the whole project. For all the modules of the architecture, the clock signal is used to activate the different operations. The purpose of using the clock is to synchronize the modules and the data bits at the output of each module.

The general principle of operation of the circuit is as follows: the clear or encrypted message is sent from the PC through the RS-232 serial port [20]. This message will pass through the RS-232 interface of the field-programmable gate array (FPGA) board where the message will be composed in frames of 8bits, these frames are stored in a register (Buf8_128) of 128 bits, after the register is filled with 128 bits completely, these bits will be ready to be encrypted/decrypted.

For encryption, the Data_Encryption module receives the 128 bits, and then it applies all the necessary operations concerning the encryption by the AES algorithm. The output of the module is a 128-bit sequence of the encrypted message.

For decryption the Data_Decryption module receives the 128 bits of the encrypted message and applies all the necessary operations concerning decryption by the AES algorithm. The output of the module is a 128-bit sequence of the decrypted message. After the encryption and/or decryption of the message, it will be sent again to the PC through the RS232 interface. Figure 5 represents different modules of the global circuit.

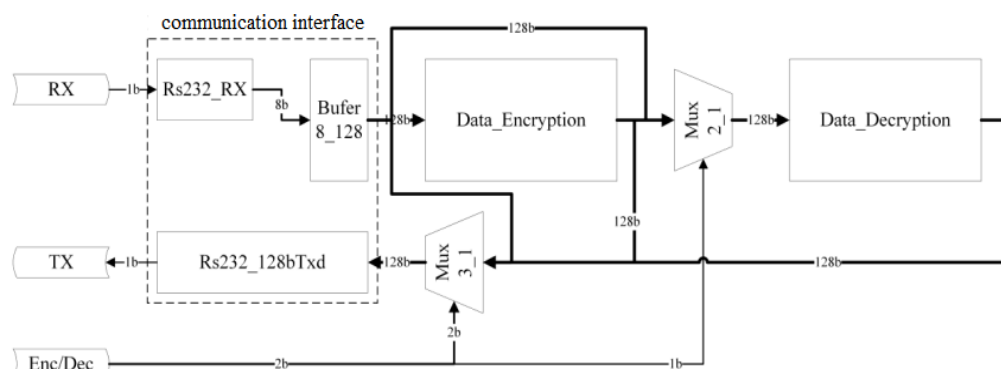


Figure 5. Different modules of the global circuits

3. RESULTS AND DISCUSSION

In this section, the simulation and implementation results of the architectures designed in section 2 on FPGA circuit of xilinx ISE design suite 14.1 of the spartan-3A digital signal processing (DSP) circuit (xc3sd1800a; package fg676; speed -4) are presented. The hardware description language (VHDL) is used to model the proposed architectures. The ISE simulation tool was used to verify their correct operation. At the end, the various obtained results are analysed and compared with those taken from literature. The same examples published on the NIST website are used to verify the accuracy of the results delivered by our architecture. In the following, we will give some examples of simulations of the various blocks of our architecture.

3.1. Key_Gen module

The simulation result of Key_Gen module is shown in Figure 6. Before all ten keys are generated, the invalid signal must be set to 1. After all keys have been generated, the keysvalid signal sends bit 1. The initial key used in this simulation is (0x2b7e151628aed2a6abf7158809cf4f3c). The key for the 10th round is (0xd014f9a8c9ee2589e13f0cc8b6630ca6).

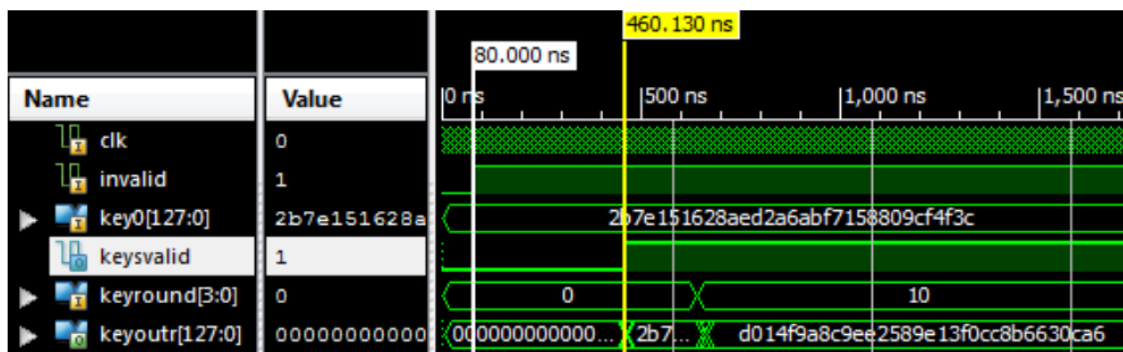


Figure 6. Key_Gen module simulation

3.2. AddRoundKey module

This operation is performed when rst changes to 0 and invalid changes from 0 to 1 as shown in Figure 7. Input data is (0x3243f6a8885a308d313198a2e0370734) and initial key is (0x2b7e151628aed2a6abf7158809cf4f3c). The result of this operation is (0x193de3bea0f4e22b9ac68d2ae9f84808) same value given in [21].

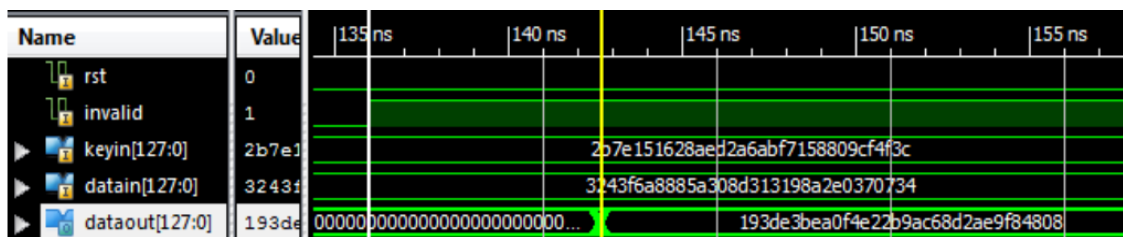


Figure 7. AddRoundKey module simulation

3.3. SubByte and InvSubByte

Figure 8(a) shows the simulation result of SubByte and Figure 8(b) represents the InvSubByte module. The data to be substituted is (0x193de3bea0f4e22b9ac68d2ae9f84808). This operation is performed when rst is set to 0. The output after the four S-Boxes is (0xd42711aee0bf98f1b8b45de51e415230). As opposed to SubByte, at InvSubByte the data input is (0xd42711aee0bf98f1b8b45de51e415230) and the output after four InvS-Boxes is (0x193de3bea0f4e22b9ac68d2ae9f84808). Note that the output of InvSubByte module is the same as the input of the subByte module, which is justified by the fact that this second module is the inverse of the first.

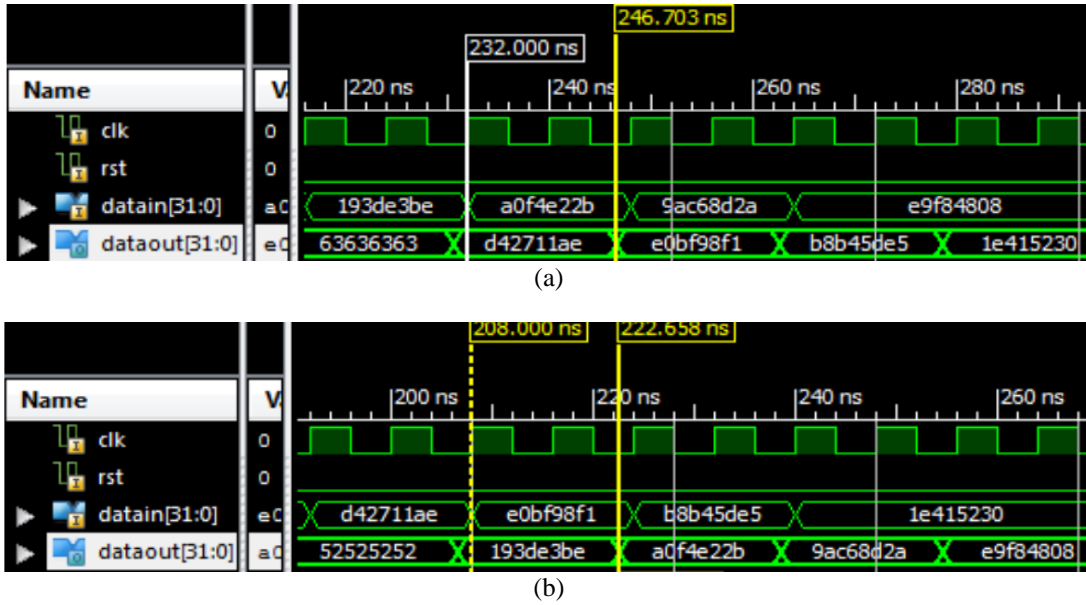


Figure 8. Simulation results of SubByte InvSubByte module: (a) subByte and (b) InvSubByte

3.4. ShiftRows and InvShiftRows

Parameters of simulations performed in this part are given in Figure 9, ShiftRows is illustrated in Figure 9(a) and InvShiftRows simulation is illustrated in Figure 9(b). The operation is performed when *rst* takes 0 and data out is (0xd4bf5d30e0b452aeb84111f11e2798e5). Note that the output of the InvShiftRows simulation is the same as the input of the ShiftRows module.

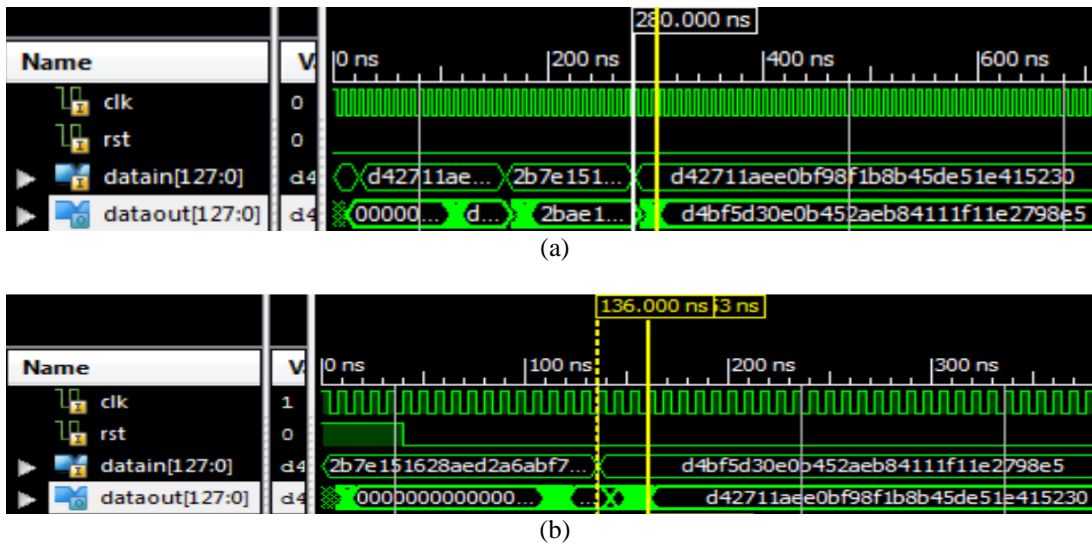


Figure 9. ShiftRows and InvShiftRows simulation: (a) ShiftRows and (b) InvShiftRows

3.5. MixColumns and InvMixColumns

The MixColumns simulation is shown in Figure 10(a) and InvMixColumns module is illustrated in Figure 10(b). These operations are performed on every 32 bits of the 128-bit data. The result of MixColumns simulation is (0x046681e5e0cb199a48f8d37a2806264c). Result of InvMixColumns is (0xd4bf5d30e0b452b84111f11e2798e5).

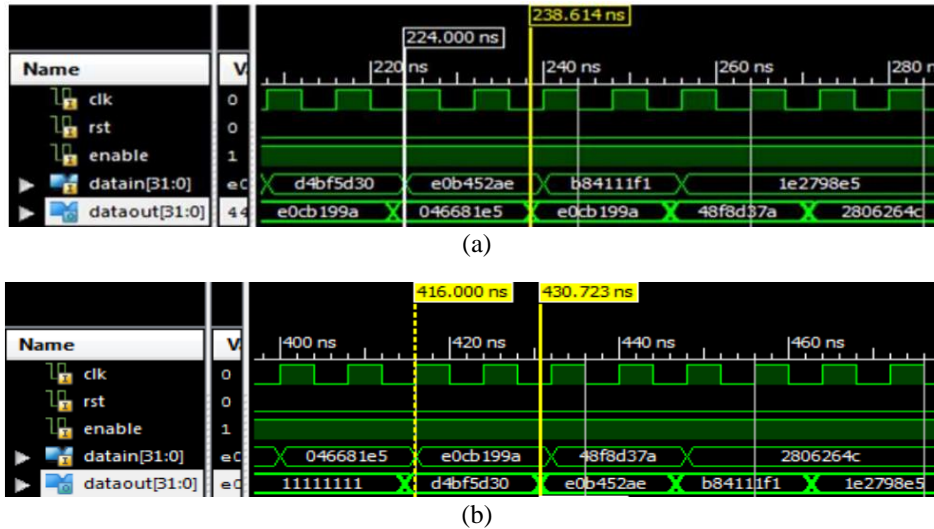


Figure 10. MixColumns and InvMixColumns simulation: (a) MixColumns and (b) InvMixColumns

3.6. Data_Encryption module

The keyinvalid signal takes the value 1, rst the value 0 and datainvalid changes from 0 to 1. As soon as the outvalid signal changes from 0 to 1. The encryption simulation is done as shown in Figure 11. The encrypted message is (0x3925841d02dc09fbdc118597196a0b32).

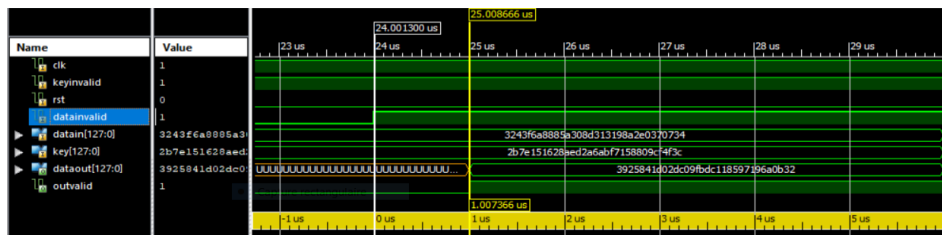


Figure 11. Data_Encryption simulation

3.7. Data randomizer

After encryption, simulation of data randomization is performed in Figure 12. The randomizer data has been illustrated in Figure 12(a) and de-randomized data has been illustrated in Figure 12(b). The input data is (0x3925841d02dc09fbdc118597196a0b32).

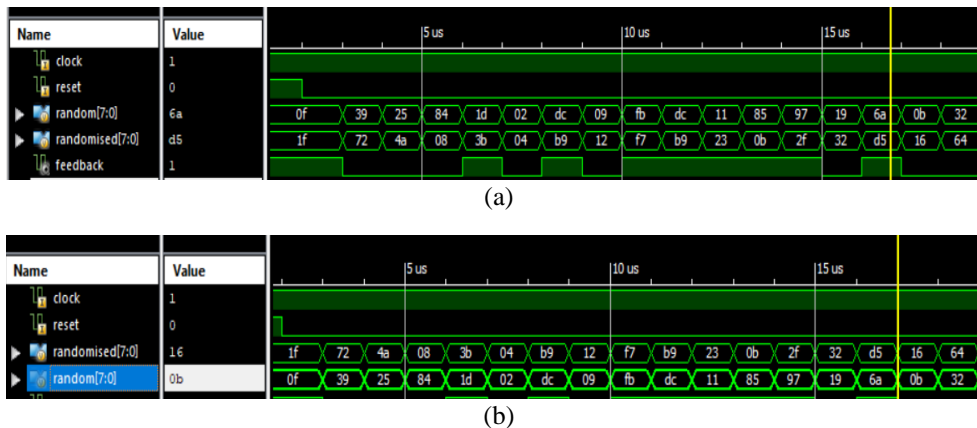


Figure 12. Simulation of data randomizer (a) randomizer data and (b) de-randomized data

3.8. Data_Decryption module

Decryption process involves reversing the encryption. Reverse conversions are performed in the opposite direction to obtain the original message from an encrypted message, with the same encryption key. Figure 13 represents the data decryption simulation.

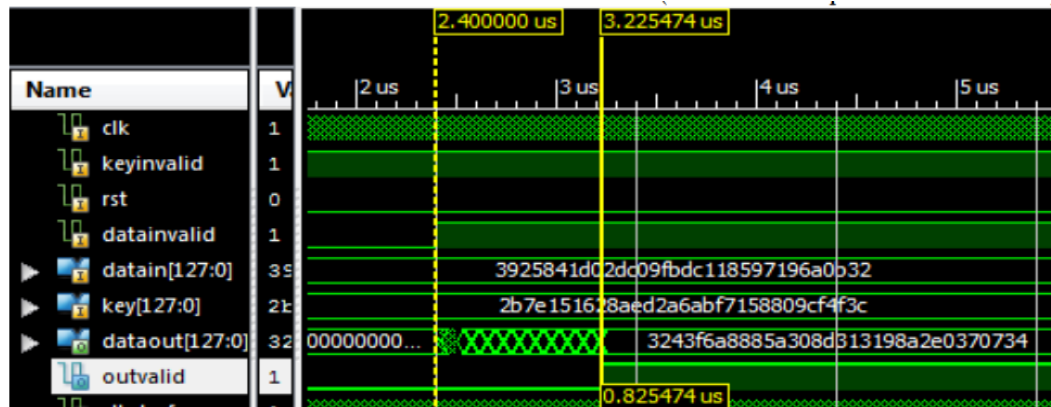


Figure 13. Data_Decryption simulation

3.9. Comparison of the circuit developed with other circuits produced

Table 1 shows a comparison result with previous circuits. The results obtained indicate that our implementation proposal strikes a favorable compromise between material surface utilization and performance design. Using a Spartan 3A dsp and xc3sd1800a-4fg676 with a speed of 151 Mb/s and a speed/slice ratio equal to 0.13.

Table 1. Comparison of our circuit with other circuits produced

	Device	Algo	Key (bits)	Slice	Speed (Mb/s)	Performance (speed/slice)
Our circuit	Spartan-3A DSP	Enc/Dec	128	1173	151	0.13
	xc3sd1800a-4fg676		128	1251	151	0.12
Adib and Raissouni [22]	Spartan 3E XC3S500E -4 FT256	Enc/Dec	128	326	270	0.83
Quynh <i>et al.</i> [23]	Spartan6 XC6SLX150T	Enc/Dec	128	2808	226	0.08
Liu <i>et al.</i> [24]	XC7VX690T	Enc/Dec	128	486	3790	7.8
Hussain and Jamal [25]	Virtex7	Enc/Dec	128	2444	5303	2.17
Wang and Ha [26]	XC6VLX240T	Enc/Dec	128	15,612	1.88	0.12
Zodpe and Sapkal [27]	XC6SLX150	Enc/Dec	128	5566	3005	0.54

4. CONCLUSION

In this paper, a cryptographic algorithm designed for passive UHF radio frequency identification systems. The algorithm relies on the AES as its fundamental encryption technique, augmented by two supplementary steps: the initial step involves generating a random key and the second is the randomization of data. The algorithm has been simulated, synthesized and implemented in an XtremeDSP starter kit equipped with xilinx's spartan-3A DSP 1800A edition (xc3sd1800a, package fg676, and speed -4). The efficiency of the algorithm has been verified and its calculation time measured. Our circuit can encrypt and decrypt data sequences up to 151 Mbps. The speed, functionality and cost of encryption and decryption make this a perfectly practical solution, providing a satisfactory level of security for today's communications systems, or other electronic data transfer processes where security is required.




REFERENCES

- [1] R. Abdulghafor *et al.*, "Recent Advances in Passive UHF-RFID Tag Antenna Design for Improved Read Range in Product Packaging Applications: A Comprehensive Review," *IEEE Access*, vol. 9, pp. 63611–63635, 2021, doi: 10.1109/ACCESS.2021.3074339.
- [2] M. Benbaghdad, B. Fergani, and S. Tedjini, "Backscatter signal model of passive UHF RFID tag. Application to collision detection," *Electronics Letters*, vol. 52, no. 11, pp. 974–976, 2016, doi: 10.1049/el.2015.3974.
- [3] Ö. Aydin, G. Dalkılıç, and C. Kösemen, "A novel grouping proof authentication protocol for lightweight devices: GPAPXR+," *Turkish*




- Journal of Electrical Engineering and Computer Sciences*, vol. 28, no. 5, pp. 3036–3051, 2020, doi: 10.3906/ELK-2004-5.
- [4] C. M. -Ausecha, J. R. -Rosero, and G. R. -Gonzalez, “Rfid applications and security review,” *Computation*, vol. 9, no. 6, p. 69, 2021, doi: 10.3390/computation9060069.
- [5] Y. Naija, V. Beroulle, and M. Machhout, “Security Enhancements of a Mutual Authentication Protocol Used in a HF Full-Fledged RFID Tag,” *Journal of Electronic Testing: Theory and Applications*, vol. 34, no. 3, pp. 291–304, 2018, doi: 10.1007/s10836-018-5725-x.
- [6] L. Zhang and Z. Xiao, “Design and implementation of a RFID security authentication protocol,” in *Proceedings-2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation*, IEEE, pp. 102–105, 2013, doi: 10.1109/IMSNA.2013.6742826.
- [7] A. Ibrahim and G. Dalkiliç, “An Advanced Encryption Standard Powered Mutual Authentication Protocol Based on Elliptic Curve Cryptography for RFID, Proven on WISP,” *Journal of Sensors*, vol. 2017, pp. 1–10, 2017, doi: 10.1155/2017/2367312.
- [8] B. Guihao, Z. Mingguo, L. Jiuwen, and L. Yin, “The design of an RFID security protocol based on RSA signature for E-ticket,” in *2010 2nd IEEE International Conference on Information Management and Engineering*, IEEE, pp. 636–639, 2010, doi: 10.1109/ICIME.2010.5478177.
- [9] H. P. T. M. Jayawardana and R. L. Dangalla, “Hybrid encryption protocol for RFID Data Security,” in *2020 International Conference on Decision Aid Sciences and Application, DASA 2020*, IEEE, pp. 1209–1212, 2020, doi: 10.1109/DASA51403.2020.9317034.
- [10] J. Ambareen, M. Prabhakar, and T. Ara, “Edge Data Security for RFID-based Devices,” in *Proceedings of the International Conference on Smart Technologies in Computing, Electrical and Electronics*, IEEE, pp. 272–277, 2020, doi: 10.1109/ICSTCEE49637.2020.9277007.
- [11] G. C. L. Lim, G. P. Arada, A. C. Abad, and E. R. Magsino, “RFID Tag Data Encryption Using Triple des and RSA Algorithms,” *Journal of Physics: Conference Series*, vol. 1997, no. 1, p. 012028, 2021, doi: 10.1088/1742-6596/1997/1/012028.
- [12] S. Wade, “Description of Image encryption Using AES-256 bits,” *International Journal for Research in Applied Science and Engineering Technology*, vol. 11, no. 5, pp. 7167–7171, 2023, doi: 10.22214/ijraset.2023.53365.
- [13] H. M. Mohammad and A. A. Abdullah, “Enhancement process of AES: a lightweight cryptography algorithm-AES for constrained devices,” *Telecommunication Computing Electronics and Control*, vol. 20, no. 3, pp. 551–560, 2022, doi: 10.12928/TELKOMNIKA.v20i3.23297.
- [14] P. Kumar and S. B. Rana, “Development of modified AES algorithm for data security,” *Optik*, vol. 127, no. 4, pp. 2341–2345, 2016, doi: 10.1016/j.ijleo.2015.11.188.
- [15] P. Katkade and G. M. Phade, “Application of AES algorithm for data security in serial communication,” in *Proceedings of the International Conference on Inventive Computation Technologies*, IEEE, pp. 1–5, 2016, doi: 10.1109/INVENTIVE.2016.7830170.
- [16] F. T. A. Hussien, A. M. S. Rahma, and H. B. A. Wahab, “A Secure Environment Using a New Lightweight AES Encryption Algorithm for E-Commerce Websites,” *Security and Communication Networks*, vol. 2021, pp. 1–15, 2021, doi: 10.1155/2021/9961172.
- [17] K. M. Akhil, M. P. Kumar, and B. R. Pushpa, “Enhanced cloud data security using AES algorithm,” in *Proceedings of 2017 International Conference on Intelligent Computing and Control*, IEEE, pp. 1–5, 2018, doi: 10.1109/I2C2.2017.8321820.
- [18] E. A. Abbood, R. M. Neamah, and S. Abdulkadh, “Text in image hiding using developed LSB and random method,” *International Journal of Electrical and Computer Engineering*, vol. 8, no. 4, pp. 2091–2097, 2018, doi: 10.11591/ijece.v8i4.pp2091-2097.
- [19] S. Oukili and S. Bri, “Hardware Implementation of AES Algorithm with Logic S-box,” *Journal of Circuits, Systems and Computers*, vol. 26, no. 9, p. 1750141, 2017, doi: 10.1142/S0218126617501419.
- [20] M. A. Bibile, G. Khadka, and N. C. Karmakar, “Detection of Chipless RFID Tag Using a Single Antenna RFID Reader System,” in *IEEE Conference on Innovative Technologies in Intelligent Systems and Industrial Applications, Proceedings*, IEEE, pp. 1–6, 2020, doi: 10.1109/CITISIA50690.2020.9371834.
- [21] M. J. Dworkin, “Advanced Encryption Standard (AES).” Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, 2023, doi: <https://doi.org/10.6028/NIST.FIPS.197-upd1>.
- [22] S. E. Adib and N. Raissouni, “AES Encryption Algorithm Hardware Implementation: Throughput and Area Comparison of 128, 192 and 256-bits Key,” *International Journal of Reconfigurable and Embedded Systems*, vol. 1, no. 2, p. 67, 2012, doi: 10.11591/ijres.v1.i2.pp67-74.
- [23] L. N. Quynh, D. V. Son, and M. A. Tuan, “Enhancement of Implementing Cryptographic Algorithm in FPGA built-in RFID Tag Using 128 bit AES and 233 bit kP Multitive Algorithm,” *VNU Journal of Science: Mathematics-Physics*, vol. 33, no. 2, 2017, doi: 10.25073/2588-1124/vnumap.4206.
- [24] Q. Liu, Z. Xu, and Y. Yuan, “High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion,” *IET Computers and Digital Techniques*, vol. 9, no. 3, pp. 175–184, 2015, doi: 10.1049/iet-cdt.2014.0101.
- [25] U. Hussain and H. Jamal, “An efficient high throughput FPGA implementation of AES for multi-gigabit protocols,” in *Proceedings - 10th International Conference on Frontiers of Information Technology*, IEEE, 2012, pp. 215–218, doi: 10.1109/FIT.2012.45.
- [26] Y. Wang and Y. Ha, “FPGA-based 40.9-gbits/s masked AES with area optimization for storage area network,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, no. 1, pp. 36–40, 2013, doi: 10.1109/TCSII.2012.2234891.
- [27] H. Zodpe and A. Sapkal, “An efficient AES implementation using FPGA with enhanced security features,” *Journal of King Saud University - Engineering Sciences*, vol. 32, no. 2, pp. 115–122, 2020, doi: 10.1016/j.jksues.2018.07.002.

BIOGRAPHIES OF AUTHORS






Sanae Habibi    was born in 1992 in Kenitra, Morocco. In 2018, She obtained her master's degree in Embedded Electronics and Telecommunications Systems from the Faculty of Sciences, Department of Physics, Ibn Tofail University, Kenitra, Morocco. She is currently pursuing her doctoral studies at the Laboratory of Electronic Systems, Information Processing, Mechanics, and Energy at the same University, working on security of the front-end of the transmission chain for UHF RFID technologies. She can be contacted at email: sanae.habibi@uit.ac.ma.






Zahra Sahel    earned her Master's degree in Microelectronics from the Faculty of Sciences, Department of Physics, Ibn Tofail University, Kenitra, Morocco in 2009. Currently, she is pursuing her doctoral studies at the Laboratory of Electronic Systems, Information Processing, Mechanics, and Energy at the same University. Her research is centered around the design of the front-end of the transmission chain for UHF RFID technologies, with a specific focus on the design of the energy harvesting block. She can be contacted at email: zahra.sahel@uit.ac.ma.






Abdelhak Bendali    was born in 1982 in Sefrou, Morocco. He obtained his Master's degree in Telecommunication and Microwave Devices at the National School of Applied Sciences of Fez, Morocco, in 2011. He obtained his thesis in Electronics and Telecommunication from the Faculty of Sciences of Kenitra, Morocco, in 2019 member of the Laboratory of Electronic Systems, Information Processing, Mechanics, and Energy since 2017. He is a temporary Professor of Electrical Engineering at Ibn Tofail University, Faculty of Sciences, Department of Physics, Kenitra, Morocco. He works on the Front-End parity of the 5G transmission chain. He can be contacted at email: abdelhak.bendali1@uit.ac.ma.






Abid Reda El Wardi    is a Moroccan Engineer and researcher born in 1986. In 2017, he obtained his Bachelor's degree in the Physical Sciences of Matter. He continued his studies and obtained a Master's degree in Telecommunication Systems in 2019. Currently, he holds the position of quality of service (QoS) optimization engineer at AFD Tech, a company that is part of accenture. In parallel with his professional career, he is pursuing his doctoral studies at Ibn Tofail University, Faculty of Science Kenitra, in the SETIME laboratory. His doctorate focuses on a specific area of telecommunications, contributing to the advancement of knowledge in this constantly evolving field. He can be contacted at email: abidreda.elwardi@uit.ac.ma.






Samia Zarrik    is a Ph.D. at the Laboratory of Telecommunication Systems and Engineering of Ibn Tofail University, Morocco. She got the Master degree in Telecommunications Systems at Ibn Tofail University of kenitra in 2020. She is currently pursuing her doctoral studies at the Laboratory of Electronic Systems, Information Processing, Mechanics, and Energy at the same University, her research interests focus on the design of low noise amplifier. She can be contacted at email: samia.zarrik@uit.ac.ma.






Mouad El Kobbi    obtained a Master degree (Telecommunication and Microwave Device) at the National School of Applied Sciences of Fez, Morocco, in 2011, He is currently pursuing his Ph.D. at the Laboratory of Telecommunication Systems and Engineering of Ibn Tofail University, Faculty of Science, Department of Physics, Kenitra, Morocco, since 2019. His current research focuses on the design of power amplifiers. He can be contacted at email: mouad.elkobbi@uit.ac.ma.



Nazha Cherkaoui    is a Professor in the Faculty of Science in Kenitra (Ibn Tofail University). She holds an engineer and a Ph.D. degree in Electrical Engineering. She is a member of the Laboratory of Electronic Systems, Information Processing, Mechanics, and Energy in the Faculty of Science in Kenitra. Her research interests include renewable energies, smart grids, powers systems, communication data, and smart cities. She can be contacted at email: nazha.cherkaoui@uit.ac.ma.



Abdelkader Hadjoudja    was an Engineer and was awarded a Doctorate in Microelectronics by the National Polytechnic Institute of Grenoble, France, in 1997. He worked for 6 years as PLD Leader Engineer Software in Atmel, Grenoble, France, and as a Consultant within Design and Reuse. Since July 2010, he became a full Professor of Electronics in Ibn Tofail University, Kenitra. He can be contacted at email: abdelkader.hadjoudja@uit.ac.ma.