

Lightweight mutual authentication protocol for resource-constrained radio frequency identification tags with PRINCE cipher

Mahendra Shridhar Naik¹, Desai Karanam Sreekantha², Kanduri V. S. S. S. Sairam³,
Chaitra Soppinahally Nataraju⁴

¹Department of Electronics and Communication Engineering, New Horizon College of Engineering, Bangalore, India

²Department of Computer Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Udupi, India

³Department of Electronics and Communication Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Udupi, India

⁴Department of Information Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Udupi, India

Article Info

Article history:

Received Feb 26, 2024

Revised Apr 8, 2025

Accepted Jun 8, 2025

Keywords:

Cipher

Latency

Mutual authentication

PRINCE

Throughput

ABSTRACT

Radio frequency identification (RFID) is a key technology for the internet of things (IoT), with widespread applications in the commercial, healthcare, enterprise, and community sectors. However, privacy and security concerns remain with RFID systems. This manuscript presents a novel RFID-based mutual authentication protocol (MAP) using the PRINCE cipher to address these concerns. The proposed MAP leverages a PRINCE cipher architecture capable of both encryption and decryption based on a mode signal. It performs five encryption and two decryption processes during tag and reader mutual authentication, with updated seed values ensuring synchronization and secure data communication. The PRINCE cipher implementation utilizes less than 1% of slices, operates at 226 MHz with a latency of 3.5 clock cycles (CC), and has a throughput of 4.125 Gbps. The complete RFID-based MAP consumes 721 mW of power, occupies 2% of the chip area, and achieves a latency of 35.5 CC and a throughput of 262 Mbps. This represents a 25% reduction in latency, a 40% increase in throughput, and a 30% decrease in execution time compared to existing MAP approaches. The findings demonstrate the potential of the proposed MAP to enhance latency, throughput, and execution time, offering a promising solution for secure and efficient RFID authentication.

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



Corresponding Author:

Mahendra Shridhar Naik

Department of Electronics and Communication Engineering, New Horizon College of Engineering

Kadabeesanahalli, Bangalore, Karnataka 560103, India

Email: mahendrasnaik@gmail.com

1. INTRODUCTION

Lightweight and affordable gadgets are needed for the widespread and accessible distributed systems of the future. Smart cards, radio-frequency identification (RFID) technology, and wireless sensor nodes (WSNs) are possible elements of a widespread and accessible network. Smart card readers are employed in RFID-based systems to safeguard private medical data and identify users. Every RFID system must be able to identify objects, track them, generate warnings, and authenticate its users. The three most common RFID technology applications are supply chain management, item recognition, and consumer product surveillance [1]–[3]. Readers (interrogators) and tags (labels) are used in RFID. An antenna and a small, inexpensive chip make up an RFID tag, which is a component of electronic devices that a reader

nearby or even from a distance can recognize. In addition to the electronic product code (EPC), each tag carries additional information about the items and is kept in a central database. RFID tags are the finest choice for various applications, including control of inventory, management of supplies, vehicle verification, fraud detection, animal administration, and environmental monitoring. Therefore, RFID systems are a solid choice to allow pervasive computing because of their possible implementation in various fields [4]–[6].

Numerous privacy and security worries about the communication link between reader and tag limit the widespread adoption of RFID devices. Researchers have suggested several cryptographic approaches to protect this communication link, such as mutual authentication protocols (MAPs) between the two communicating parties. These MAPs are categorized into four classes: simple, full-lightweight, fledged, and ultralightweight, based on the cost of computation and activities permitted by the RFID tags [7]–[9]. The ultra-lightweight class is suggested for the low-cost RFID systems most extensively used and likely to replace bar codes. The different limits on resources are these RFID tags' primary limiting factors. These RFID tags can't afford a cutting-edge CPU, much memory, or much bandwidth because the cost must be kept low [10], [11].

An efficient RFID-based MAP using PRINCE is designed in this manuscript for IoT applications. The proposed work offers high throughput and better execution time with a low-chip area suitable for IoT applications. The contribution of the proposed work is highlighted as follows: the encryption or decryption process of the PRINCE algorithm is working on the same architecture based on the mode, which improves the chip area and power. The proposed RFID-based MAP utilizes less execution time for tag and reader authentication. The updated seed values from tag and the server/reader side provide synchronization and properly secured communication between reader and tag. The performance comparison of proposed designs with recent existing works is discussed with better improvements.

The manuscript's organization is as follows: section 2 discusses the current work of the RFID-based MAP with different approaches and its performance analysis. The working operation of the RFID-based MAP using PRINCE is explained in section 3. The simulation, performance, and comparative results are discussed in detail in section 4. Section 5 concludes the overall work with improvements.

2. RELATED WORKS

The recent works on authentication and security using different approaches for different applications are discussed in this section. Sidorov *et al.* [12] present the ultralightweight mutual authentication-based RFID protocol for blockchain-enabled devices. The mutual authentication-based RFID uses a database to provide a secured blockchain for the supply chain management system. The work discusses the ultralightweight protocol with a collision analysis of the design. The formal and security analyses are discussed in detail. The communication, storage, and computational costs are evaluated in detail. Lu *et al.* [13] describe the linear feedback shift register (LFSR)-based lightweight tripling (LT) MAP with an RFID tag chip. The design uses an analog front-end (AFE) module, a radio-frequency (RF) limiter, a voltage generator, and amplitude shift keying (ASK)-based modulators. The LT MAP uses the LFSR scheme for reader and tag authentication. The work realizes the randomness test to evaluate the pass rate and consumes 117 μ W of power. Hosseinzadeh *et al.* [14] discuss the robust adversary model for RFID MAP. The adversary model is designed and deployed in server-mounted authentication protocol (SMAP) to improve the security features. Hosseinzadeh *et al.* [15] explain the enhanced authentication protocol for the RFID system. The Rabin-based authentication protocol is used to realize the security, formal, and performance analyses.

Zhu [16] describe a secured RFID-based MAP for healthcare applications. The work reviews the existing security, weakness, and scalability issues and solves them with a new MAP approach. The quadratic residue theorem is used for secured MAP and realizes security and performance analysis. The work discusses the communication, storage, and computational costs in detail. Trinh *et al.* [17] present the lightweight block cipher-based MAP for IoT devices. The craft-based lightweight block cipher is used as a security algorithm in MAP. The work realizes the informal and formal security analysis with a cost comparison. Naeem *et al.* [18] explain the RFID MAP using elliptic curve cryptography (ECC) with secured and scalable features for IoT applications. The work discusses the MAP and informal analysis in detail. The security evaluation is validated using the Proverif tool. The work obtains the computation cost for the tag and reader within 6.7114 milliseconds. Sharma *et al.* [19] discuss the ECC-based RFID MAP for the internet of vehicles (IoV). The MAP uses the setup, tag, and server authentication stages. The server and tag authentication, scalability, availability, anonymity, and forward security features are discussed.

Zhong *et al.* [20] explain the MAP of the RCIA protocol in RFID systems based on logic event theory (LET). The LET proof system, including formal foundation theory and the axiom system, is discussed in detail with proofs. The vigorous mutual authentication is provided for tag and reader using the RCIA protocol based on LETs. Wang *et al.* [21] describe the lightweight MAP for edge IoT nodes with physical

unclonable function (PAF). The MAP has setup, registration, and authentication phases to realize the security analysis: the work analysis, security functions, and costs in detail. Cai *et al.* [22] present the RFID tag/mutual authentication one step beyond the process. The work discusses unpredictable-based privacy notations. The storage and communication overheads are discussed with existing works in detail with improvements. Noori *et al.* [23] discuss the ECC-based RFID MAP for IoT in healthcare applications. The work discusses security analyses like men-in-middle, replay, mutual authentication, forward security, and data integrity. The work realizes tag and reader's computational, communication, and storage costs. Wei *et al.* [24] present the improved secured authentication protocol (SAP) for lightweight RFID systems using ECC. The work analyzes different attacks and performance metrics with comparative discussion.

2.1. PRINCE cipher

Borghoff *et al.* [25] initially developed the prince cipher in 2012 for pervasive computing applications. The PRINCE cipher supports a 64-bit data size and a 128-bit key size. The proposed PRINCE cipher can perform encryption and decryption operations by changing the mode. The hardware architecture of PRINCE cipher is illustrated in Figure 1. The cipher contains two add round key (ARK), two round constant (RC) additions, five normal rounds, one middle round, and five inverse round operations. Each normal round performs substitution box (Sbox), followed by linear layer (M), RC addition, and ARK operations. Similarly, each inverse round performs ARK, RC addition, inverse linear layer (M^{-1}), and inverse Sbox operations.

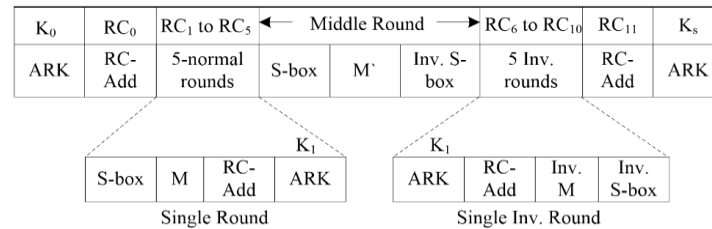


Figure 1. Hardware architecture of PRINCE cipher

The PRINCE cipher performs 11 rounds (normal, middle, and inverse), ARKs, and RC addition operations twice. The 128-bit key (K) is decomposed into two sub-keys (K_0 , K_1) in a concatenation (\parallel) manner ($K=K_0\parallel K_1$). The PRINCE cipher uses an additional whitening key (K_s) in the encryption and decryption processes to create confusion and diffusion. The generation and usage of the key and whitening key for the encryption and decryption processes are represented in (1) and (2) as follows:

$$\text{Mode}=1: \text{Encryption: } K=(K_0\parallel K_1) \text{ and } K_s=(K_0[0]\parallel K_0[63:2]\parallel (K_0[1]\oplus K_0[63])) \quad (1)$$

$$\text{Mode}=0: \text{Decryption: } K=(K_s\parallel (K_1\oplus \alpha)) \text{ and } K_0=(K_s[0]\parallel K_s[63:2]\parallel (K_s[1]\oplus K_s[63])) \quad (2)$$

The encryption process uses key (K_0) for the first ARK operation, key (K_1) for round operations, and whitening key for the last ARK operation. Similarly, the decryption process uses a whitening key for the first ARK operation, a key (K_0) for round operations, and a key ($K_1\oplus \alpha$) for the last ARK operation. The alpha (α) is a 64-bit constant value ($\alpha=c0ac29b7c97c50dd$), and \oplus is an exclusive OR (XOR) operation. The ARK performs a simple XOR operation with a corresponding state input and key. The RC addition performs a simple XOR operation with corresponding state input and RC values. The five normal and inverse rounds use five different RC additions, like RC1 to RC5 and RC6 to RC10, respectively, to perform encryption and decryption operations. The RC values in hexadecimal notation are tabulated in Table 1.

Table 1. RC values for PRINCE cipher

RC number	RC value	rc number	RC value
RC ₀	0000000000000000	RC ₆	7EF84F78FD955CB1
RC ₁	13198A2E03707344	RC ₇	85840851F1AC43AA
RC ₂	A4093822299F31D0	RC ₈	C882D32F25323C54
RC ₃	082EFA98EC4E6E89	RC ₉	64A51195E0E3610D
RC ₄	452821E638D01377	RC ₁₀	D3b5A399CA0C2399
RC ₅	BE5466CF34E90C6C	RC ₁₁	C0AC29B7C97C50DD

The Sbox uses a 4-bit data value as input and is replaced with the corresponding Sbox value in the encryption process. The Sbox operation was repeated 16 times to construct a 64-bit Sbox output. The inverse Sbox output is the same as the Sbox operation and is the decryption process. The Sbox and Inverse Sbox for the encryption and decryption processes are tabulated in Table 2. The linear (M) and M⁻¹ layers contain the 64-bit state input multiplied by the 64×64 matrix M or M⁻¹. The M⁻¹ layer is used only in the middle round and is constructed based on the alpha reflection property. The M layer matrix uses shift rows to generate M and M⁻¹ mapping, as represented in Figure 2. The 16 nibbles are used; each is 4-bit in M and M⁻¹ mapping. The PRINCE cipher produces the encryption output by performing the XOR operation using the 11th round RC addition output with a whitening key in the last ARK operation. Similarly, the PRINCE deciphers the decryption output by performing the XOR operation using the 11th round RC addition output with Key (K0) in the last ARK operation.

Table 2. Sbox and inverse Sbox for PRINCE cipher

In	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Sbox out	B	F	3	2	A	C	9	1	6	7	8	0	E	5	D	4
Inv. Sbox out	B	7	3	2	F	D	8	9	A	6	4	0	5	E	C	1

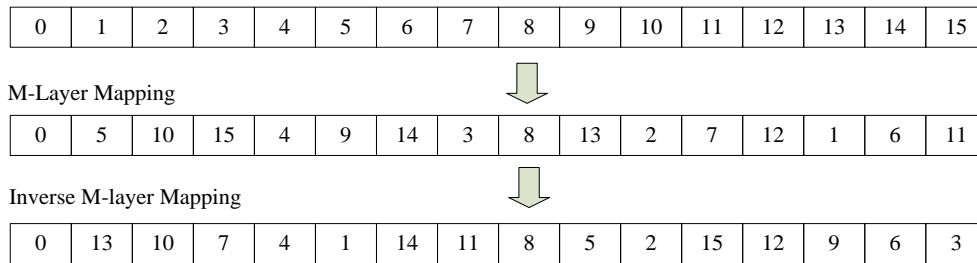


Figure 2. M-layer and inverse M-Layer mapping

3. RFID-BASED MUTUAL AUTHENTICATION PROTOCOL

RFID-based MAP using PRINCE cipher for IoT applications is discussed in this section. The proposed RFID-based MAP contains a server database, a reader, and tag information with multiple encryption and decryption processes. The parameters and descriptions used in RFID-based MAP are tabulated in Table 3. A few of the assumptions are mandatory to perform authentication between tag and reader. The database must know the 128-bit key (K) of the PRINCE cipher, 64-bit seed (S), 64-bit tag identification (IDT), and 64-bit reader ID (IDR). The reader must know the 128-bit key and reader ID. The tag should have information about the 128-bit key, tag identification (IDT), and 64-bit seed (S). The RFID-based MAP process is illustrated in Figure 3. The operation of the RFID-based MAP using PRINCE cipher is discussed as follows:

- Query: the server database sends the query to the tag via reader. First, perform encryption (E) operation using K and IDR to generate server-side cipher-1 (SC1). The SC1 data is passed to reader. The reader performs a decryption (D) operation for SC1 data and generates server-side decipher-1 (SD1). Perform XOR operation between SD1 and IDR to generate the reader cipher (RC) value. The RC data acts as query data to tag.
- Reader to tag authentication process: initially, tag generates tag cipher (TC) data by performing E(S). If the TC matches the received RC, then update the seed value (UST) by performing $(RC \oplus K)$, and reader is authenticated at the tag side. If not, the matches tag has to wait until further query. Respond to reader (TR) by performing E (UST \oplus IDT).
- Tag to reader authentication process: reader receives the tag response (TR) and forwards it to the server database for reader authentication. The database performs E(S) and D(TR) to generate the SC2 and SD2. These values SC2 and SD2 are XOR with a Key to generate the ID at the server side (IDS) and used further to extract the Tag's ID. If the IDS and IDT match, then update the server-side (USS) seed value by performing $(SC2 \oplus K)$, and tag is authenticated on the server side.
- Synchronization between tag and reader: if the updated seed at tag-side (UST) value matches the USS, the synchronization between tag and reader is successful and ready for secured data communication.

Table 3. Parameters and its description used in RFID MA protocol

Parameters	Description	Parameters	Description
K	128-bit Key	S_{C1}, S_{C2}	Server-side ciphers-1,2
E	PRINCE encryption	S_{D1}, S_{D2}	Server-side decipherers-1,2
D	PRINCE decryption	R_C	Reader cipher after encryption
S	Seed Value	T_C	Tag cipher after encryption
ID_T	Tag ID	T_R	Tag response after encryption
ID_R	Reader ID	US_T	Updated seed value at tag- side
ID_S	Server ID	US_S	Updated seed value at server- side

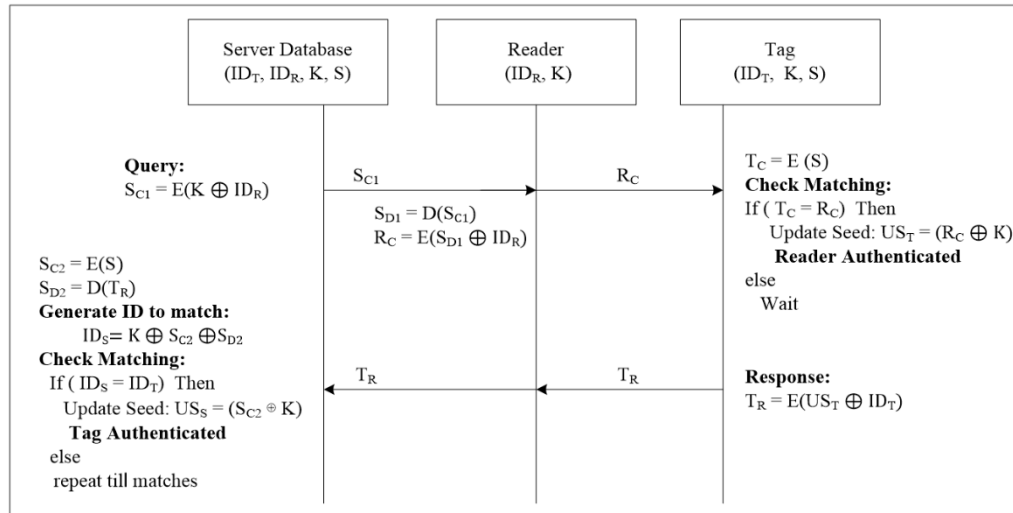


Figure 3. RFID-mutual authentication protocol

4. RESULTS AND DISCUSSION

The detailed results of the PRINCE cipher and RFID-MA protocols using PRINCE are discussed in this section. The design modules are constructed using Verilog HDL on the Xilinx ISE platform and synthesized using the Artix-7 FPGA (Device: XC7A100T-5CSG324). The mentor graphics-based ModelSim simulator verifies and visualizes the simulation waveform. The simulation results of the RFID-MA using the PRINCE cipher are illustrated in Figure 4. The global clock (clk) is activated at 100 MHz with an active low reset (rst) to start the RFID-MA process. Define 128-bit key, 64-bit seed, and ID (tag and reader) values. Based on the RFID-MA protocol, if the values of the reader and tag ciphers match, then the reader is authenticated (Reader_Auth).

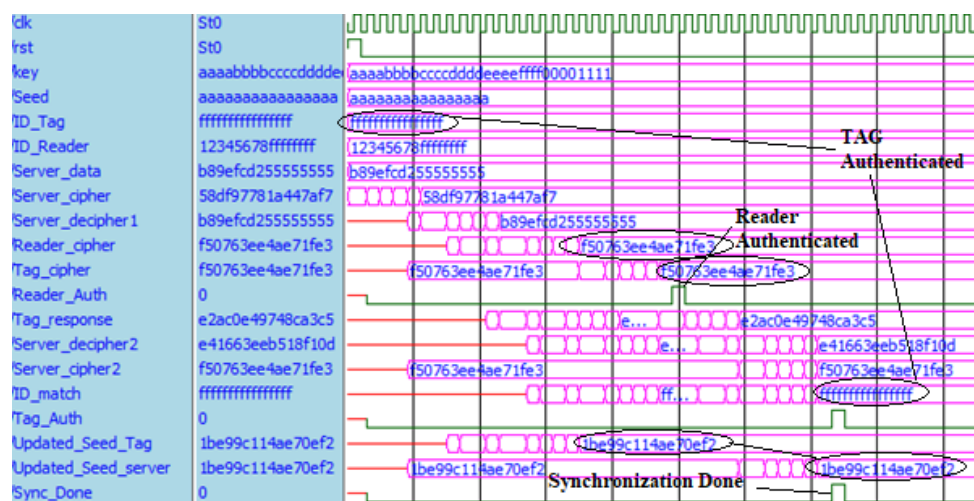


Figure 4. Simulation results of RFID-MA using PRINCE cipher

Similarly, after the encryption and decryption process on the server side, the obtained ID (ID_Match) matches the tag ID (ID_Tag), and the tag is authenticated (Tag_Auth). The synchronization of both tag and reader is achieved only after seed updates. Once the updated seed values match tag and reader, RFID authentication is successful with synchronization. The performance of the PRINCE cipher and RFID-mutual authentication protocol using PRINCE are realized concerning chip area utilization, and performance metrics are tabulated in Table 4. The chip area utilization contains slices, lookup tables (LUTs), LUT-flip-flops (FFs), and power. The parameters like latency in terms of clock cycles (CC), throughput (Gbps), and hardware efficiency (Mbps/slice) are considered for performance realization.

Table 4. Performance summary of proposed designs

Resources	PRINCE cipher	RFID-MA using PRINCE
Slices	197	2727
LUTs	1.420	9295
LUT-FFs	197	1221
Max. frequency (MHz)	226	145.683
Dynamic power (mW)	170	637
Total power (mW)	253	721
Latency (CC)	3.5	35.5
Throughput (Gbps)	4.125	0.262
Efficiency (Mbps/Slices)	20.94	0.097

The PRINCE cipher uses slices of <1%, LUTs of 2%, operates at 226 MHz, and consumes a total power of 253 mW. The PRINCE cipher uses only 3.5 CC as latency, achieving a throughput of 4.125 Gbps, with a hardware efficiency of 20.94 Mbps/Slice. Similarly, the RFID-MA protocol utilizes slices of 2%, and LUTs of 14%, operates at 145.6 MHz, and consumes a total power of 721 mW. The PRFID-MA protocol uses 35.5 CC as latency and achieves a throughput of 262 Mbps, with an efficiency of 0.097 Mbps/Slice. The representation of the resource utilization of PRINCE cipher and RFID-MA protocol is shown in Figure 5.

The performance comparison of the proposed PRINCE cipher with existing PRINCE ciphers is tabulated in Table 5. The FPGA device, chip area (slices), obtained frequency, latency, throughput (Gbps), and hardware efficiency parameters are considered for performance comparison. The Virtex-4 FPGA device is considered for all the PRINCE Cipher designs. The proposed PRINCE improves the slices by 11.7%, frequency by 81%, and throughput by 35.1%, and efficiency by 42% than the existing PRINCE cipher [26]. Similarly, the proposed PRINCE improves the slices by 35%, frequency by 20.4%, latency by 68%, throughput by 50.2%, and efficiency by 45% than the existing PRINCE cipher [27]. The proposed PRINCE cipher performs better by concerning slices by 17%, frequency by 81%, throughput by 35.09%, and efficiency by 46% more than the existing PRINCE cipher [28] on the Virtex-4 FPGA.

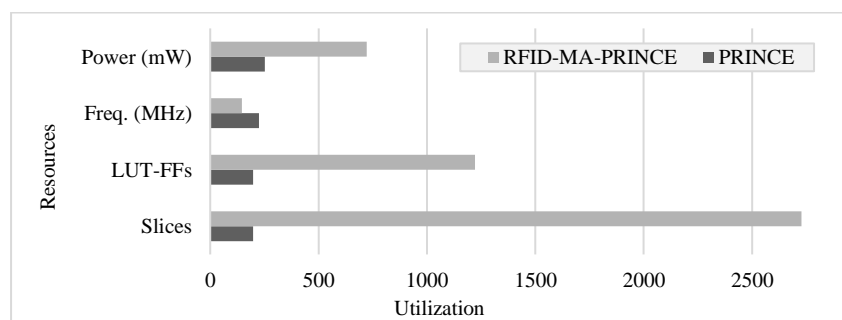


Figure 5. Resource utilization of design-modules

Table 5. Performance comparison of proposed PRINCE cipher with existing PRINCE ciphers

PRINCE designs	Ref [25]	Ref [26]	Ref [27]	Our work
FPGA device	Virtex-4	Virtex-4	Virtex-4	Virtex-4
Slices	956	1305	1026	844
Frequency (MHz)	31.76	136.03	31.72	171
Latency (CC)	1	11	1	3.5
Throughput (Gbps)	2.032	2.081	2.029	3.126
Efficiency (Mbps/Slices)	2.126	2.01	1.978	3.7

The resource comparison of the proposed RFID-MA using PRINCE with other RFID-MA works is tabulated in Table 6. The Spartan-3 FPGA device is used for all the design's resource comparisons. The proposed RFID-MA using PRINCE provides less chip area overhead (Slices and LUTs) of around 70% than RFID-MA Using XTEA, PRESENT, and HB ciphers [28]. The proposed RFID-MA using PRINCE operates at better Frequency by 6%, 8.2%, and 38% than RFID-MA using XTEA, PRESENT, and HB ciphers [28], respectively, on Spartan-3 FPGA. The performance comparison of the proposed RFID-MA using PRINCE with RFID-MA using XTEA [29] on the Spartan-3 FPGA is tabulated in Table 7. The proposed RFID-MA using PRINCE provides better performance of around 90% in latency, throughput, and execution time and 66% by efficiency than RFID-MA using XTEA [29] system.

Table 6. Resource comparison of proposed RFID-MA using PRINCE with other RFID-MA works

Designs	FPGA	Slices	LUTs	Frequency (MHz)
RFID MA - XTEA [28]	Spartan-3	22.55 K	43.32 K	60.6
RFID MA - PRESENT [28]	Spartan-3	22.32 K	42.84 K	59.16
RFID MA - HB [28]	Spartan-3	22.29 K	41.90 K	40.1
Proposed RFID MA -PRINCE	Spartan-3	6.76 K	13.22 K	64.5

Table 7. Performance comparison of proposed RFID-MA using PRINCE with RFID-MA using XTEA [29]

Designs	FPGA	Slices	Latency (CC)	Throughput (Mbps)	Efficiency (Kbps/Slice)	Execution time (us)
[29]	Spartan-3	1212	1155	6.96	5.74	11.55
Our design	Spartan-3	6760	35.5	116.28	17.2	0.355

5. CONCLUSION

This manuscript presents the design and implementation of a secure RFID-based MAP using the PRINCE cipher. The protocol was designed in Verilog-HDL, implemented on an Artix-7 FPGA, and demonstrated significant performance advantages over existing MAP systems. Key findings include: i) efficient PRINCE cipher implementation: the lightweight PRINCE cipher occupied less than 1% of the chip area, operated at 226 MHz with a latency of 3.5 CC, and achieved a throughput of 4.125 Gbps; ii) secure and efficient MAP: the complete RFID-based MAP, utilizing the PRINCE cipher, achieved a latency of 35.5 CC, a throughput of 262 Mbps, and authentication within 0.355 μ s. This represents a 25% reduction in latency, a 40% increase in throughput, and a 30% decrease in execution time compared to existing MAP approaches; and iii) optimized resource utilization: the MAP consumed 721 mW of power and utilized only 2% of the chip area, demonstrating its suitability for resource-constrained RFID systems. Future directions for this research include: i) security analysis: a comprehensive security analysis of the MAP using PRINCE will be conducted to evaluate its resilience against various attacks and ensure its suitability for real-world RFID deployments; ii) performance optimization: further optimization of the MAP's performance metrics, such as latency and throughput, will be explored to enhance its overall efficiency and scalability; and iii) potential applications: the practical applications of the proposed MAP in diverse RFID-based systems will be investigated to demonstrate its real-world impact and potential benefits. The research results show that the suggested RFID-based MAP using PRINCE could be used to make authentication safe and quick in RFID environments with limited resources. It offers a promising solution for enhancing security and performance in various RFID applications, contributing to the advancement of secure IoT systems.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Mahendra Shridhar Naik	✓	✓		✓				✓	✓	✓			✓	
Desai Karanam	✓	✓			✓				✓			✓		
Sreekantha														
Kanduri V. S. S. S.					✓	✓			✓			✓		
Sairam														
Chaitra Soppinahally	✓	✓	✓		✓	✓			✓	✓	✓			
Nataraju														

C : C onceptualization	I : I nterpretation	Vi : V isualization
M : M ethodology	R : R esources	Su : S upervision
So : S oftware	D : D ata Curation	P : P roject administration
Va : V alidation	O : Writing - O riginal Draft	Fu : F unding acquisition
Fo : F ormal analysis	E : Writing - Review & E ditng	

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] A. Jeng, L. I. C. Chang, and H. K. Ho, "Survey and remedy of mutual authentication protocols for RFID system," in *Proceedings of the 7th International Conference on Machine Learning and Cybernetics, ICMLC*, 2008, vol. 6, pp. 3361–3366, doi: 10.1109/ICMLC.2008.4620985.
- [2] S. M. Mohsin, I. A. Khan, S. M. Abrar Akber, S. Shamshirband, and A. T. Chronopoulos, "Exploring the RFID mutual authentication domain," *International Journal of Computers and Applications*, vol. 43, no. 2, pp. 127–141, 2021, doi: 10.1080/1206212X.2018.1533614.
- [3] M. S. Naik, D. K. Sreekantha, and K. V. S. S. S. Sairam, "Comparative study of block ciphers implementation for resource-constrained devices (review)," *Radioelectronics and Communications Systems*, vol. 66, no. 3, pp. 123–137, 2023, doi: 10.3103/S0735272723050011.
- [4] Z. Bilal and K. Martin, "Ultra-lightweight mutual authentication protocols: weaknesses and countermeasures," *2013 International Conference on Availability, Reliability and Security, ARES 2013*, pp. 304–309, 2013, doi: 10.1109/ARES.2013.41.
- [5] S. Leng, M. Tang, X. Jiang, Z. Zhang, and M. H. Lee, "An improved mutual authentication scheme compliant to EPC Class-1 Generation-2 standard," in *2011 International Conference on Consumer Electronics, Communications and Networks, CECNet*, 2011, pp. 3933–3937, doi: 10.1109/CECNET.2011.5768269.
- [6] S. Han, V. Potdar, and E. Chang, "Mutual authentication protocol for RFID tags based on synchronized secret information with monitor," in *Computational Science and Its Applications – ICCSA 2007*, 2007, pp. 227–238, doi: 10.1007/978-3-540-74484-9_20.
- [7] Y. J. Huang, C. H. Jiang, H. H. Wu, Y. H. Hong, and K. J. Liu, "Mutual authentication protocol for RFID system," in *2011 14th IEEE International Conference on Computational Science and Engineering*, 2011, pp. 73–80, doi: 10.1109/CSE.2011.27.
- [8] D. Engels, X. Fan, G. Gong, H. Hu, and E. M. Smith, "Hummingbird: ultra-lightweight cryptography for resource-constrained devices," in *Financial Cryptography and Data Security*, 2010, pp. 3–18, doi: 10.1007/978-3-642-14992-4_2.
- [9] Y. S. Kang, E. O'Sullivan, D. Choi, and M. O'Neill, "Security analysis on RFID mutual authentication protocol," in *16th International Workshop, WISA 2015*, 2016, pp. 65–74, doi: 10.1007/978-3-319-31875-2_6.
- [10] L. Luo and D. Liu, "An improved lightweight RFID mutual-authentication protocol," in *Second International Conference on Mechanics, Materials and Structural Engineering (ICMMSE 2017)*, 2017, pp. 278–284, doi: 10.2991/icmmse-17.2017.45.
- [11] F. Zhu, P. Li, H. Xu, and R. Wang, "A lightweight RFID mutual authentication protocol with PUF," *Sensors*, vol. 19, no. 13, 2019, doi: 10.3390/s19132957.
- [12] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains," *IEEE Access*, vol. 7, pp. 7273–7285, 2019, doi: 10.1109/ACCESS.2018.2890389.
- [13] J. Lu, D. Liu, H. Li, C. Zhang, and X. Zou, "A fully integrated HF RFID tag chip with LFSR-based light-weight tripling mutual authentication protocol," *IEEE Access*, vol. 7, pp. 73285–73294, 2019, doi: 10.1109/ACCESS.2019.2920437.
- [14] M. Hosseinzadeh *et al.*, "A new strong adversary model for RFID authentication protocols," *IEEE Access*, vol. 8, pp. 125029–125045, 2020, doi: 10.1109/ACCESS.2020.3007771.
- [15] M. Hosseinzadeh *et al.*, "An enhanced authentication protocol for RFID systems," *IEEE Access*, vol. 8, pp. 126977–126987, 2020, doi: 10.1109/ACCESS.2020.3008230.
- [16] F. Zhu, "SecMAP: a secure RFID mutual authentication protocol for healthcare systems," *IEEE Access*, vol. 8, pp. 192192–192205, 2020, doi: 10.1109/ACCESS.2020.3032541.
- [17] C. Trinh *et al.*, "A novel lightweight block cipher-based mutual authentication protocol for constrained environments," *IEEE Access*, vol. 8, pp. 165536–165550, 2020, doi: 10.1109/ACCESS.2020.3021701.
- [18] M. Naeem, S. A. Chaudhry, K. Mahmood, M. Karuppiah, and S. Kumari, "A scalable and secure RFID mutual authentication protocol using ECC for internet of things," *International Journal of Communication Systems*, vol. 33, no. 13, 2020, doi: 10.1002/dac.3906.
- [19] S. Sharma, B. Kaushik, M. K. I. Rahmani, and M. 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, doi: 10.1109/ACCESS.2021.3124209.
- [20] 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," *Chinese Journal of Electronics*, vol. 31, no. 1, pp. 79–88, 2022, doi: 10.1049/cje.2021.00.101.
- [21] H. Wang, J. Meng, X. Du, T. Cao, and Y. Xie, "Lightweight and anonymous mutual authentication protocol for edge IoT nodes with physical unclonable function," *Security and Communication Networks*, no. 1, 2022, doi: 10.1155/2022/1203691.
- [22] S. Cai, Y. Li, C. Ma, S. S. M. Chow, and R. H. Deng, "Prove you owned me: one step beyond RFID tag/mutual authentication," *arXiv-Computer Science*, pp. 1–13, 2022.
- [23] D. Noori, H. Shakeri, and M. N. Torshiz, "An elliptic curve cryptosystem-based secure RFID mutual authentication for Internet of things in healthcare environment," *Eurasip Journal on Wireless Communications and Networking*, no. 1, 2022, doi: 10.1186/s13638-022-02146-y.




- [24] G. H. Wei, Y. L. Qin, and W. Fu, "An improved security authentication protocol for lightweight RFID based on ECC," *Journal of Sensors*, vol. 2022, no. 1, 2022, doi: 10.1155/2022/7516010.
- [25] J. Borghoff *et al.*, "PRINCE-a low-latency block cipher for pervasive computing applications," in *18th International Conference on the Theory and Application of Cryptology and Information Security*, 2012, pp. 208–225, doi: 10.1007/978-3-642-34961-4_14.
- [26] Y. A. Abbas, R. Jidin, N. Jamil, M. R. Z'aba, M. E. Rusli, and B. Tariq, "Implementation of PRINCE algorithm in FPGA," in *Proceedings of the 6th International Conference on Information Technology and Multimedia*, 2014, pp. 1–4, doi: 10.1109/ICIMU.2014.7066593.
- [27] B. Rashidi, "Low-cost and two-cycle hardware structures of PRINCE lightweight block cipher," *International Journal of Circuit Theory and Applications*, vol. 48, no. 8, pp. 1227–1243, 2020, doi: 10.1002/cta.2832.
- [28] A. A. Abdullah and N. R. Obeid, "Efficient implementation for PRINCE algorithm in FPGA based on the BB84 protocol," *Journal of Physics: Conference Series*, vol. 1818, no. 1, 2021, doi: 10.1088/1742-6596/1818/1/012216.
- [29] R. Anusha, P. R. Rao, and N. P. Rai, "Secured authentication of RFID Devices using lightweight block ciphers on FPGA platforms," *IEEE Access*, vol. 11, pp. 107472–107479, 2023, doi: 10.1109/ACCESS.2023.3320277.

BIOGRAPHIES OF AUTHORS






Mahendra Shridhar Naik    is a Senior Assistant Professor in the Department of Electronics and Communication Engineering at New Horizon College of Engineering, Bengaluru, Karnataka, India. He holds an M.Tech. in Digital Electronics and Communication Engineering and a Bachelor of Engineering in Electronics and Communication Engineering, both from Visvesvaraya Technological University, Belagavi, Karnataka, India. With over ten years of academic experience, his research interests encompass IoT, wireless sensor networks, communication, VLSI, artificial intelligence, machine learning, and deep learning. He has published extensively in reputable journals and holds multiple patents in the field of intellectual property rights. He can be contacted at email: mahendrasnaik@gmail.com.






Desai Karanam Sreekantha    has been serving as Professor in the Department of Computer Science and Engineering at NMAM Institute of Technology, NITTE, and India since November 2014 and was awarded Ph.D. from Symbiosis International University, Pune, in 2014. He has secured Second Rank at Gulbarga University in B.Sc. (Electronics) degree examinations and National Merit Scholarship. He has 23 years of teaching experience and 6 years of industry experience in the TATA group. He authored about 25 Scopus-indexed papers, i.e., one book, 13 book chapters, and 25 papers in international journals, and he also presented 30 research papers at international/national conferences. He published two Indian patents. He was currently guiding four Ph.D. students. He can be contacted at email: sreekantha@nitte.edu.in.



Kanduri V. S. S. S. Sairam    working as a Professor at Department of Electronics and Communication Engineering and also IEEE student branch Counsellor in NMAMIT, NITTE. He obtained his B.E. (ECE) from Karnataka University Dharwad in 1996, M.Tech. (Industrial Electronics) from SJCE, Mysore University Mysore, 1998, and Ph.D. (ECE) (Optical Communications) JNTUH, Hyderabad in 2013. He has 25 years of experience in teaching and research. He published 54 papers at international, national conferences and workshops. He is guiding four Ph.D. students and 40 M.Tech. Projects and B.E. Projects. His research areas are optical communications, optical networks, and wireless communication. He can be contacted at email: drsairam@nitte.edu.in.



Chaitra Soppinahally Nataraju    is a Senior Assistant Professor in the Department of Electronics and Communication Engineering at GM Institute of Technology, Davangere, Karnataka, India. She earned her M.Tech. in Digital Electronics and Communication Engineering and her Bachelor of Engineering in Telecommunication Engineering, both from Visvesvaraya Technological University, Belagavi, Karnataka, India, where she is currently pursuing her Ph.D. With over a decade of academic experience, her research interests lie in IoT, wireless sensor networks, communication, and VLSI. She has contributed to the field through publications in reputable journals and holds multiple patents in intellectual property rights. She can be contacted at email: chaitrasn48@gmail.com.