# Hybrid encryption protocol for RFID Data Security

H.P.T.M. Jayawardana [*], R. L. Dangalla[†]
Department of Computing and Information Systems
Sabaragamuwa University of Sri Lanka
Email: [*]hptmjayawardana@std.appsc.sab.ac.lk, [†]ravindra.dangalla@appsc.sab.ac.lk,

2020 International Conference on Decision Aid Sciences and Application (DASA) | 978-1-7281-9677-0/20/$31.00 ©2020 IEEE | DOI: 10.1109/DASA51403.2020.9317034

*Abstract*—**Radio Frequency Identification (RFID) is an evolving technology. It brings benefits through high productivity and efficiency in applications where artifacts have to be automatically identified. Point of Sale system, library system, and the number of applications available with this RFID technology. As security and privacy challenges are increasing day by day, RFID technology should be improved with its strategies and tactics. Asymmetric key cryptography and symmetric key cryptography separately provided good solutions to such security challenges. The propose hybrid encryption method that is used for encryption and decryption of the RFID data. The hybrid encryption protocol performs both asymmetric and symmetric ciphers. And the proposed an advanced encryption standard (AES) for symmetric cipher as it is proved to be highly secured, fast, and well-standardized, and well supported. The proposed conjoin elliptic curve cryptography (ECC) as asymmetric cipher because it is the latest and best cipher algorithm that uses smaller keys and signatures. It provides a rapid key generation, rapid key agreement, and rapid signatures. This combination will be the best for RFID technology than receiving results from both separately. For security analysis of the hybrid protocol, Automation Validation of Internet Security Protocols and Applications (AVISPA) tool is used. The goal is to propose, hybrid encryption protocol using the AES and ECC algorithms to enhance the RFID data security with the most effective and efficient methods.**

*Keywords*: RFID, AES, ECC, AVISPA

## I. Introduction

Radio Frequency Identification (RFID) technology is an emerging technology in this era. Many Industries use RFID for their tasks. Especially this technology is invaluable in high-level uncertainty demanded by apparel industries. The company can use RFID to record received goods, deduct sold goods by registering them at their Point of Sale (POS) system. There is already a range of applications of RFID technology in the medical field. In Library systems RFID applications are applied as it makes the negotiations more efficient and productive [1].

Most of the previously used RFID technologies had privacy related issues. This emergence of security and privacy challenges for RFID and, is explosively increased and it led to a trend in researches. Widespread RFID implementation can be harmful to privacy since it does not provide a solution. There are some common negative issues of RFID.

*1) Tag cloning :* An RFID tag gives a unique number named the EPC (Electronic Product Code) when asked by an RFID reader. An attacker can create fake tags which emit the same EPCs [2].

*2) Denial / Service interruption :* considerable number of fake tags and malicious readers exploit computer resources and it causes service disruption such as radio communication interference [2].

*3) Eavesdropping:* The Intruder intercepts communication between the RFID reader and Tag. He captures the radio signals and can obtain the transmitted data [3].

*4) Replay attack:* Attacker can gain the identity of an authorized person by creating fake and re-sending the eavesdropped signal again and again [3].

In this paper, our goal is to propose, hybrid encryption protocol using the AES and ECC algorithms to enhance the RFID data security. Most of the previous works have been focused on the symmetric key algorithm or asymmetric key algorithm separately. Also, few works are done by combining both symmetric and asymmetric algorithms. But they required specific hardware for the implementation. Here our strategy is to propose a simple hybrid encryption method with enhanced data security.

The rest of this paper is presented as follows. Section 2 presents related work; Section 3 presents the methodology while section 4 presents the security analysis. Finally, in section 5, we present the conclusion and future works.

## II. LITERATURE REVIEW AND RELATED WORKS

In this section, we present some of the previous works done related to RFID data encryption protocols.

In [4], Mustapha Benssalah, Mustapha Djeddou, and Karim Drouiche proposed a new RFID authentication protocol based on elliptic curves ElGamal encryption schemes. They considered these requirements for their research because RFID tags have several challenging constraint's limitations such as storage capacity, computational resource cost, communication cost, scalability and robustness. This Protocol has been developed and evaluated in C#. This protocol can resist attacks such as man-in-the-middle attack, simple power analysis, and replay attacks.

In [5], Khaled ElMahgoub, introduced a new encryption algorithm for the UHF RFID systems. The algorithm based on the use of a randomizer and encryption of OTP data. Implementation was simple and easy. It is very hard to break because of the usage of two randomly generated keys. Using a real reader's C-API the algorithm was used to write user data for a Higgs 3 tag. The algorithm's efficiency was checked and measured its computational time.

In [6], M. B. Abdelhalim, M. El-Mahallawy, and A. El-hennawy proposed a Modified Tiny Encryption Algorithm

(MTEA) hardware implementation that uses the Linear Feedback Shift Register to overcome the safety vulnerability of the standard TEA algorithm against attacks.

In [7], Yiran Lin and Yue Shi presented AES and ECC based encryption model which can protect users' privacy and implement access controls. They showed the advantage of using both symmetric and asymmetric encryption.

In [8], Thanapol Hongsongkiat and Prabhas Chongstitvatana have proposed 128-bit AES cryptography software program and hardware module. They proposed their AES module with 0.13 um CMOS technology at 1.5 V and use for the high-frequency RFID applications.

In [9], Ravi Kishore Kodali and Ashwitha Naikoti have proposed Elliptic Curve Diffie-Hellman(ECDH) key exchange on NIST P-192 curve. They have discussed and implemented a secured communication using ESP8266 modules. Mesh networks, Smart power meters, Home automation, Wearable devices, Security ID tags and Sensor networks and many other applications were proposed to apply their methodology.

In [10], Srinidhi MB and Romil Roy introduced an attendance monitoring system using RFID and biometric based on multi-tier architecture. A high-frequency RFID reader with frequency ranges from 3 MHz to 30 MHz has been used in the prototype.

In [11], Kyoungyoul Kim, Kyungho Chung, Juseok Shin, Hyunwoo Kang, Sejin Oh, Chunho Han and Kwangseon Ahn have proposed lightweight authentication using AES.The AES was just used for the lightweight authentication here, and the key value could be changed step by step three times. By this, the key exposure could be prevented. The random number which generated by tag, reader and server successively changed the symmetric keys of the tag and server. Therefore, the output of the tag and reader changes. The prevention of eavesdropping, replay attack and location tracking are possible with this key changes.

In [12], Mohammad Tajabadi and Seyed Vahid Azhari have focused on security and performance of RFID systems in traffic management applications. They have proposed a scalable mutual authentication protocol using AES, Rabin and ECC. Both Rabin and ECC are lightweight public key algorithms which are suitable for RFID systems.The slowness of decryption process of Rabin cryptosystem is really a weakness. But it is not a drawback in their system because the backend server performs decryption not the tags. Rabin cryptosystem has another issue. As any of four possible inputs generate the output of its decryption, it is not deterministic.

## III. METHODOLOGY

AES (Advanced Encryption Standard) is the best used symmetrical encryption algorithm in present IT sector. Because it is highly reliable, fast, standardized, and well supported on almost all platforms. AES is named also as the Rijndael. AES can operate with different key lengths such as 128, 160, 192, and 256 bits. But its block size is always 128 bits. But here we combined AES with GCM (Galois/Counter Mode) Block mode operation. Then block size does not fix and can get encrypted data of arbitrary size. Another advantage is GCM block modes which can add the message authentication code (MAC). It gives the advanced security option for protocol security. Finally, our symmetric encryption algorithm is AES-256-GCM.

The Elliptic Curve Cryptography (ECC) is the modern public key cryptosystem in this era. It provides rapid key agreement, rapid signatures and rapid key generation for the implementations. But ECC does not directly provide an encryption mechanism. Therefore, we used a hybrid encryption scheme using the ECDH (Elliptic Curve Diffie–Hellman) key exchange scheme. It helps to obtain a shared secret key to build ECC encryption and decryption. The ECDH is a secret key agreement scheme. It allows two parties to establish an elliptic curve public-private key pair over an insecure channel. ECDH is similar to Diffie Hellman Key Exchange (DHKE). ECDH uses ECC point multiplication. It is defined as follows.
a = A's private Key
b = B's private key
G = elliptic curve with generator point
a*G = public key of A
b*G = public key of B
Then we can derive a shared secret a,
a = (a * G) * b = (b * G) * a

This RFID system has a passive tag, reader, and Server. There is a safe communication channel between the RFID reader and Server. But the communication channel between the reader and the RFID tag is not safe. The server performs the encryption-decryption process using the proposed hybrid cryptography protocol using AES-256-GCM and ECDH. The RFID reader can only write and read the data from the RFID tag. Fig. 1 shows the proposed RFID authentication protocol in this paper. And also, Table I shows the notations of the proposed protocol.

TABLE I
NOTATIONS

| Notation | Content |
|---|---|
| PU | ECC Public Key |
| PR | ECC Private Key |
| PU' | randomly generated ephemeral ECC public Key |
| PR' | randomly generated ephemeral ECC private Key |
| K | Symmetric Key |
| ID | The unique identifier of the tag |
| ID' | Ciphertext of unique identifier of the tag |
| MAC | The message authentication code |

### A. Operation 1

In the beginning, PK and PR are generated by tinyec python library. This pair of keys help for encryption - decryption process through hybrid schema.

### B. Operation 2

In this phase, ECC shared key (K) generates using ECDH. This shared ECC key is used in AES-GCM-256 encryption process as the symmetric key. Then AES-GCM-256 encrypt

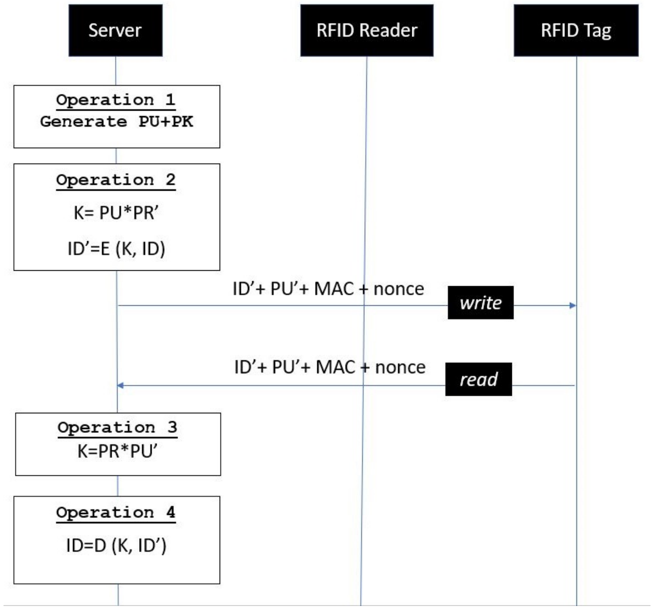

Fig. 1. The proposed protocol

the ID using symmetric key.
K= PU*PR'
ID'=E (K, ID)
Output = ID'+ PU'+ MAC
Finally, RFID reader sends, ID', PU', MAC into the RFID card.

### C. Operation 3

In this phase, RFID Reader reads the RFID card. Then Server checks the MAC code. It should be matched for the successful decryption. Then sever calculates the ECC shared key Using PR and PU'.
Input = ID'+ PU'+ MAC
K=PR*PU'

### D. Operation 4

The final phase is the decryption process. Shared ECC Key is the symmetric key for the AES-GCM-256.
ID=D (K, ID')

## IV. Result of the Comparison

We do security analysis by using AVISPA (Automated Validation of Internet Security Protocols and Applications). It is a push button tool for the vulnerability of internet security of protocols and applications. It offers a formal language that is flexible and concise to define protocols and their security properties. Four various back-ends incorporate a range of automated analysis techniques [13].

1) CL-AtSe - the Constraint-Logic-based Attack Searcher
2) OFMC - the On-the-Fly Model-Checker
3) SATMC - the SAT-based Model-Checker
4) TA4SP - the Tree Automata tool based on Automatic Approximations for the Analysis of Security Protocols

At first, we selected five simple basic protocols which exist inside the AVISPA. These basic protocols are used in practical environment in simple applications. We analyzed this basic protocol and built our hybrid protocol inside the AVISPA tool using the HLPSL (standing for High-Level Protocols Specification Language). Then we compared our hybrid protocol with AVISPA basic protocol using the verification tool.These are the basic protocol inside the AVISPA which we used.

Protocol 1: It is a simple protocol. B sends a secret message (s) to A.
B $\rightarrow A : B, s$

Protocol 2: It is a simple protocol. B sends a secret message (s) to A. Message is encrypted by public key (Kb)
B $\rightarrow A : B, \{s\}Kb - 1$

Protocol 3: It is a simple protocol. B sends a secret message (s) to A. Message is encrypted by public key (Kb) and B is encrypted by public key (Ka).
B $\rightarrow A : \{B, \{s\}\_Kb - 1\}\_Ka$

Protocol 4: It is a key exchange protocol. There are three agents. A, B and the trusted third party (T). A and T share a symmetric key Kat. B and T share symmetric key Kbt. A need to establish a symmetric session key (Kab) with B.
A $\rightarrow T : \{Kab\}\_Kat$
$T \rightarrow B : \{Kab\}\_Kbt$

Protocol 5: It is similar protocol 5.
A $\rightarrow T : \{A, B, Kab\}\_Kat$
$T \rightarrow B : \{B, A, Kab\}\_Kbt$

Table II shows the summary of the comparison results.

TABLE II
Result of the Comparison

| Protocols | OFMC | ATSE | TS4SP |
|---|---|---|---|
| Proposed Protocol | safe | safe | safe |
| Protocol 1 | unsafe | unsafe | inconclusive |
| Protocol 2 | unsafe | unsafe | unsafe |
| Protocol 3 | unsafe | unsafe | safe |
| Protocol 4 | unsafe | unsafe | inconclusive |
| Protocol 5 | unsafe | unsafe | inconclusive |

The existing protocols are viewed as unsafe or inconclusive. It is possible to see that each module, OFMC, CL-Atse, and TA4SP confirmed as safe. Moreover, Tag ID passes after encapsulating with the encryption process. So, it is impossible for eavesdropping. Tag cloning is meaningless because Encrypted ID is available inside the Tag. Although Attacker gets the encrypted ID, it is impossible to decrypt without the decryption keys because it is difficult to guess the decryption process as keys are generated in the hybrid decryption process.

## V. CONCLUSION AND FUTURE WORKS

In this paper a proposed hybrid encryption method using both symmetric and asymmetric algorithms.The AES block cipher (Rijndael) in GCM (Galois/Counter Mode) block mode with 256 bits key lengths were used for the implementation. ECC is the latest and modern public-key cryptography of asymmetric cryptography family.And used a hybrid encryption scheme by using the ECDH (Elliptic Curve Diffie–Hellman) key exchange scheme to derive a shared secret key. It allows two parties to establish the elliptic curve public and private key pair over an insecure channel. Security analysis is done by the AVISPA tool. This security confirmation is resulted by the modules such as OFMC, TS4SP, and CL-Atse which are included in this AVISPA tool. So, safety would be confirmed.

When considering the practical environment, many simple systems do not care about security, as most of the security protocols are complex. And some of them require specific hardware to the implementation. The basic strategy which makes this specified than others, is the safety and simplicity for the general use. It is easy for implementation. We used python language to build encryption and decryption functions. It does not require specific hardware for the RFID reader and the RFID Tag side. As future work suggested to analyse performance in this protocol in the practical environment. Furthermore, to implement the hardware device, propose Raspberry pi module, RFID Passive Tag, and RC522 RFID Reader module for the implementation.

## REFERENCES

[1] Xiaowei Zhu, Samar K. Mukhopadhyay, and Hisashi Kurata. A review of RFID technology and its managerial applications in different industries. *Journal of Engineering and Technology Management - JET-M*, 29(1):152–167, 2012.

[2] Dang Nguyen Duc, Hyunrok Lee, Divyan M. Konidala, and Kwangjo Kim. Open issues in RFID security. *International Conference for Internet Technology and Secured Transactions, ICITST 2009*, 2009.

[3] Gurudatt Kulkarni, Ramesh Sutar, and Sangita Mohite. ”RFID Security Issues & Challenges” Rupa/i Shelke, Lecturer in Marathwada Mitra. 2014.

[4] Mustapha Benssalah, Mustapha Djeddou, and Karim Drouiche. RFID authentication protocols based on ECC encryption schemes. *2012 IEEE International Conference on RFID-Technologies and Applications, RFID-TA 2012*, pages 97–100, 2012.

[5] Khaled Elmahgoub. An Encryption Algorithm for Secured Communication with Passive UHF RFID An Encryption Algorithm for Secured Communication with Passive UHF RFID Systems. (March 2014), 2017.

[6] M. B. Abdelhalim, M. El-Mahallawy, and M. Ayyad A. Elhennawy. Design and Implementation of an Encryption Algorithm for use in RFID System. *International Journal of RFID Security and Cryptography*, 2(1):51–57, 2013.

[7] Yiran Lin, Kaige Kang, and Yue Shi. Research on encryption model based on AES and ECC in RFID. *Proceedings - 2013 International Conference on Computer Sciences and Applications, CSA 2013*, pages 9–13, 2013.

[8] Thanapol Hongsongkiat and Prabhas Chongstitvatana. AES implementation for RFID tags: The hardware and software approaches. *2014 International Computer Science and Engineering Conference, ICSEC 2014*, pages 118–123, 2014.

[9] Ravi Kishore Kodali and Ashwitha Naikoti. ECDH based security model for IoT using ESP8266. *2016 International Conference on Control Instrumentation Communication and Computational Technologies, ICCICCT 2016*, pages 629–633, 2017.

[10] Romil Roy. A web enabled secured system designed for attendance monitoring applying biometric and Radio Frequency Identification (RFID) technology. *2014 International Conference on Signal Propagation and Computer Technology, ICSPCT 2014*, pages 653–657, 2014.

[11] Kyoungyoul Kim, Kyungho Chung, Juseok Shin, Hyunwoo Kang, Sejin Oh, Chunho Han, and Kwangseon Ahn. A lightweight RFID authentication protocol using step by step symmetric key change. *8th IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2009*, pages 853–854, 2009.

[12] Mohammad Tajabadi and Seyed Vahid Azhari. A Hybrid Privacy-Preserving Mutual Authentication Protocol for RFID Traffic Management. *ICEE 2019 - 27th Iranian Conference on Electrical Engineering*, pages 1889–1894, 2019.

[13] Luca Viganò. Automated Security Protocol Analysis With the AVISPA Tool. *Electronic Notes in Theoretical Computer Science*, 155(1 SPEC. ISS.):61–86, 2006.