Journal of the Institute of Industrial Applications Engineers Vol.9, No.2, pp.33–39, (2021.4.25)
DOI: 10.12792/JIIAE.9.33 Online edition: ISSN 2187-8811 Print edition: ISSN 2188-1758

Paper

MUMAP: Modified Ultralightweight Mutual Authentication protocol for RFID enabled IoT networks

Mehedi Hasan Raju[*][†] Non-member, Mosabber Uddin Ahmed[‡] Non-member
Md Atiqur Rahman Ahad[‡] Member

(Received May 15, 2020, revised January 24, 2021)

Abstract: Flawed authentication protocols led to the need for a secured protocol for radio frequency identification (RFID) techniques. In this paper, an authentication protocol named Modified ultralightweight mutual authentication protocol (MUMAP) has been proposed and cryptanalysed by Juel-Weis challenge. The proposed protocol aimed to reduce memory requirements in the authentication process for low-cost RFID tags with limited resources. Lightweight operations like XOR and Left Rotation, are used to circumvent the flaws made in the other protocols. Proposed protocol has three-phase of authentication. Security analysis of proposed protocol proves its resistivity against attacks like desynchronization, disclosure, tracking, and replay attack. On the other hand, performance analysis indicates that it is an effective protocol to use in low-cost RFID tags. Juel-Weis challenge verifies the proposed protocol where it shows insusceptibility against modular operations.

Keywords: Radio Frequency, IoT, Ultralightweight, Mutual Authentication, MUMAP, Security

1. Introduction

The network which connects various electronic devices with distinct identities among each other and creates an internetworking infrastructure through different communication protocols is known as Internet of Things (IoT). IoT network utilizes RFID technology for the identification process because it is lightweight, enables high-speed communication, and ensures no line of sight scanning. RFID is a fast-growing recognition mechanism which identifies the distinct identities effectively [1]. The non-line of sight scanning feature makes RFID a promising technology. Besides, the miniature size and the cost-effectiveness of RFID tags also increase its demand not only in IoT but also in other fields of research. Unlike barcodes, in every RFID object, there is an integrated circuit (IC). But because it identifies/traces the object with radio waves and no physical contact is needed, it will shortly replace the other identification strategies if its reliability concerns can be solved.

RFID system consists mainly of three parts: reader, tag, and back-end server (database). A protected channel connects the back-end server and reader, while the link between the reader and the tag is considered poorly secured. Due to this issue, privacy and protection became one of RFID's indispensable security concerns. Generally, the connection between reader and tag is critical and unattended as the channel is wireless, which is vulnerable to various cyber-attacks. This system is endangered to various kinds of security attacks such as Denial of Service (DoS), man in the middle (MIM), spoofing, eavesdropping, traceability, desynchronization, and probabilistic disclosure attack. Researchers suggested various authentication protocols for the RFID tag and reader, based on the purpose of protecting the communications channel.

Chien [2] classified these protocols into four groups based on the complexity of computation, operations, and function used. These are i) Full-fledged protocols, ii) Simple protocols, iii) Lightweight protocols, and iv) Ultralightweight protocols. Full-fledged protocols include traditional cryptographic techniques, hash functions, etc. The protocols of this class require adequate on-chip resources [3]. For this purpose, costly RFID tags are needed for these protocols. Simple protocols contain only a pseudo-random number generator (PRNG) and hash function. Lightweight protocols carry a cyclic redundancy check (CRC) and a lightweight PRNG check. Low-cost RFID tags have an insubstantial number of resources and drawbacks for advanced computation. There is an ultralightweight class of protocols for this reason. These protocols use only bit-wise logical operations and ultra-light primitives such as rotation, recursive hash, etc. PRNG is used because it was on the server-side.

To strengthen the security of a RFID system from the vulnerabilities and lessening the intricacy in the calculation, a methodical authentication protocol is required which can ensure security for the vulnerable channel mentioned earlier. As of late, numerous ultralightweight mutual authentication protocols have been put forward and practically every one of them demonstrated poor performance against various security attacks. In this paper, we come up with a novel protocol for ultralightweight class. We have titled it

[*] Corresponding: 0.mehedihasanraju@gmail.com
[†] Dept. of ICT, Bangladesh University of Professionals, Bangladesh
[‡] Dept. of EEE, University of Dhaka, Bangladesh
(mosabber.ahmed@du.ac.bd, atiqahad@du.ac.bd)

as, MUMAP: Modified ultralightweight mutual authentication protocol.

2. Related Works

Lopez et al. proposed three RFID protocols named UMAP (Ultralightweight Mutual Authentication Protocol): LMAP (Lightweight Mutual Authentication Protocol) [4], M^{2}AP (Minimalist Mutual Authentication protocol) [5] and EMAP (Efficient Mutual Authentication protocol) [6] which belong to ultralightweight group. In this family of protocols very simple bitwise operations took place. For reducing computational complexity and the cost, these protocols were quite effective for RFID tags of low prices. However, later on, it was found that these protocols were susceptible to different attacks like desynchronization, full disclosure attack, etc.

Chien [2] proposed a new authentication protocol for RFID communication named Strong Authentication and Strong Integrity (SASI) protocol. Authors claimed that SASI offered solid authentication and secure communication and improved data integrity, which can resist all potential attacks that breach the protection of prior techniques. Unfortunately, cryptanalysis of the protocol pointed out its vulnerability to attacks like DoS, desynchronization, anonymity tracing, and full disclosure attack [7]. Gossamer protocol [8] is quite similar to SASI's scheme, but due to the use of dual rotation and the MixBits feature Gossamer tends to be considerably more stable. Gossamer protocol claimed that it was designed to solve the security issues of the SASI protocol but the gossamer protocol also failed to prove its strong authentication.

Tian et al. [9] came with a new ultralightweight protocol named RFID authentication protocol with permutation, which used a new bitwise operation called permutations. But afterward, Avoine et al. [10] described its vulnerability in their paper. Jeon and Yoon proposed RFID authentication protocol for low-cost tags (RAPLT) [11] where merge and separation operations were used. It solves EURFID's [12] *IDS* collision problem. But Wang et al. [13] proved that RAPLT was not secured at all. It was also vulnerable to desynchronization attack.

In the same year, Bassil et al. [14] proposed a novel approach to achieve mutual authentication for ultralightweight tags using physically unclonable functions (PUF). It was claimed that it provided robust security as well as good performance. Umar Mujahid [1] proposed a RFID authentication protocol of similar class in 2014 by using a recursive hash. It was claimed that this protocol would provide security, probity, and authentication cost-effectively. For this reason, it was named robust confidentiality, integrity, and authentication (RCIA) protocol. RCIA introduced a new recursive hash function, which detected the tempered message, and avoided all possible attacks.

A protocol for ultralightweight mutual authentication called Succinct and Lightweight Authentication Protocol (SLAP) was introduced in 2016. Bitwise basic operations, rotations, and conversion have been used in this protocol. Hanguang [15] claimed to withstand numerous attacks including a desynchronization attack, a replay attack and, traceability attack.

Tewari [16] proposed a novel ultralightweight mutual authentication protocol in 2017. Because of using bitwise operations only, this protocol was very efficient in terms of cost. Besides this, it was claimed that the computational overhead was very low and the protocol provided untraceability. But later on, it was found that this protocol was vulnerable to desynchronization attack and full probabilistic disclosure attack [3]. Later, Wang [17] found the vulnerability of the Tewari and Gupta's protocol and proposed a revised version of it. Wang claimed that the revised protocol was able to resist desynchronization and full disclosure attacks. Later in 2016, Umar Mujahid [18] proposed kasami code based mutual authentication protocol: KMAP. A new ultralightweight primitive called pseudo kasami code was introduced. KMAP avoided logical operations like OR, AND because of their unbalanced behavior and the protocol showed resistive nature against all possible attacks.

In 2018 [19], a robust elliptic curve cryptography-based authentication protocol has been suggested to remove the existing issues raised by RFID being an unreliable means of communication between tag and reader. This protocol used elliptic curve Diffie-Hellman as the main agreement protocol to settle on a common message that is used to encrypt the subsequent messages exchanged to secure the tag data. Nevertheless, recently Naeem et al. [20] put forward some scalability and consistency based security concerns. Finally, the paper recommends an update to fix the mentioned problems. Zhu et al. [21] proposed an ultralightweight protocol but incorporates a function which was physically unclonable (PUF). Authors claimed that their proposed protocol was resistant to physical attacks and clone attacks as the tag contains no information and was fitted with a PUF. Rather, enable low-cost tags and large tag implementations.

Therefore, several protocols have been developed over time but none of them developed to be completely covered which is the key impetus for our research. We have addressed the problems generated in the protocol Tewari and Gupta [16] and are proposing a new RFID ultralightweight authentication protocol.

3. Proposed Protocol

In the proposed authentication method, it is presumed that the wireless connection between the reader and the backend database server will be protected while the connection between the reader and the tag will not be secured. The proposed authentication scheme aims to protect the channel. Tag's identity (*ID*), pseudonym (*IDS*) and Key (K_r for reader, K_t for tag) are stored in both reader and tag. K_r and K_t are expected to be the same. Figure 1 depicts the flow diagram of the proposed protocol. There are several steps of authentication in the proposed mechanism which are discussed below:

1. The reader transmits a **Hello** message to all tags at the beginning of the authentication process.

2. After receiving the initialized Hello message, tag re-

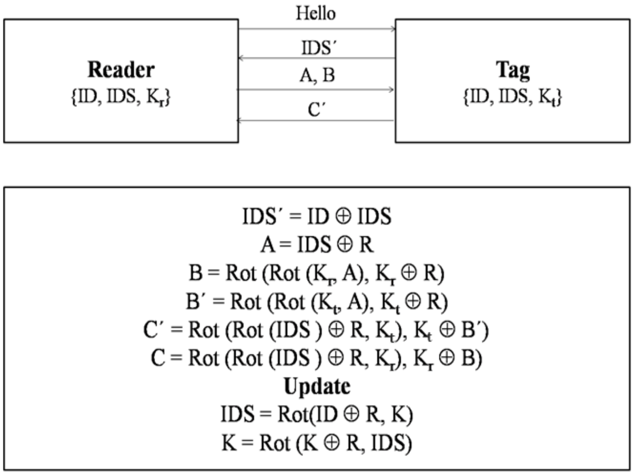
Hello
IDS′
A, B
C′
Reader
{ID, IDS, K_r}
Tag
{ID, IDS, K_t}
IDS′ = ID ⊕ IDS
A = IDS ⊕ R
B = Rot (Rot (K_r, A), K_r ⊕ R)
B′ = Rot (Rot (K_t, A), K_t ⊕ R)
C′ = Rot (Rot (IDS) ⊕ R, K_t), K_t ⊕ B′)
C = Rot (Rot (IDS) ⊕ R, K_r), K_r ⊕ B)
Update
IDS = Rot(ID ⊕ R, K)
K = Rot (K ⊕ R, IDS)

Figure 1: Proposed protocol (MUMAP)

sponses with IDS' where IDS' is used for secure communication.

$$IDS' = ID \oplus IDS \quad (1)$$

3. Upon receiving IDS', reader will dig out ID from IDS' and IDS that saved at reader side ($ID = IDS' \oplus IDS$) and verify ID with the back-end server.

   On receipt of the IDS', reader will dig out ID by IDS' and IDS saved at reader side ($ID = IDS' \oplus IDS$) and verify ID with the back-end server. When the ID is detected on the file, the tag will be accepted as a valid tag, then the tag will be identified as a malicious tag and the link will be terminated automatically along with the first step of the authentication process.

4. If the ID matches in the previous stage, the next authentication step will begin. A random number (R) is generated at the end of the reader at this point, and A is determined.

   $$A = IDS \oplus R \quad (2)$$

   After computing A, the reader computes B using A, K_r, and R. Rotation function, Rot () is used here.

   $$B = \text{Rot}(\text{Rot}(K_r, A), K_r \oplus R) \quad (3)$$

   After that reader calculates A and B and transmits to the tag's end.

5. The tag extracts the random number R with A and IDS stored at the side of the tag after obtaining A, B. Extracting R and the local values that the tag determines B' and comparing it with B.

   $$B' = \text{Rot}(\text{Rot}(K_t, A), K_t \oplus R) \quad (4)$$

   If $B \neq B'$, the connection will be terminated immediately else the protocol will go for next level of authentication.

6. Third authentication stage starts with calculating C' at tag's side with K_t. Tag sends back C' to reader.

   $$C' = \text{Rot}(\text{Rot}(IDS \oplus R, K_t,), K_t \oplus B') \quad (5)$$

7. Reader will compute C using K_r and compare it with C'.

   $$C = \text{Rot}(\text{Rot}(IDS \oplus R, K_r,), K_r \oplus B) \quad (6)$$

   If $C \neq C'$, the connection is terminated immediately and if $C = C'$ found true then the channel will be secured successfully.

Rot (A, B) means rotating the bits of A as per the hamming weight of B. Hamming weight of B means the number of non zero bits in B. For example, A = 10100110 and B = 10111001. The number of non zero bits in B is 5. Therefore, Rot (A, B) = Rot (A, 5) = 11010100.

4. Security Analysis

Our proposed protocol has been analysed in the following section. There are four parts of this security analysis: an analysis using Juels-Weis challenge-response model, vulnerabilities due to modular operations, functionality analysis, and resistivity against different attacks.

4.1 Analysis using Juels-Weis Challenge Juels-Weis challenge [22] involves a one-reader RFID system and a range of RFID tags n. All the legitimate tags in the RFID system contain one discrete secret key and pseudonym which have been altered after every successful authentication period. Three different messages are used to execute the session:

1. **SetKey** message is employed so as to allocate a new key to the tag. Receiving SetKey message, tag replace the existing secret key with a new one.

2. **TagInit** message stacks the session key to another worth evacuating the present session logs and starts with another session key.

3. **ReaderInit** uses this particular message in order to start a new session of authentication.

Adversary Considerations:

1. H is presumed to be an adversary that can generate any of the above messages.
2. H can react to any of the above messages, in light of the information recovered from parameters from the last session.
3. Communication cost will be determined by the number of ReaderInt and TagInt messages generated by H.
4. H is capable of corrupting any tag just by sending SetKey messages to it.
5. H receives and controls every enduring communication between reader and tags.

H can give the following queries:

Execute (*R*, *T*): H controls the channel through which the reader, R, and tag, T communicates in real-time. It is eavesdropping i.e., a passive attack.

Send (E_1, E_2, m): H sends any message m when two entities E_1, E_2 are communicating.

Corrupt (*T*, *K*): Through this query, H manipulates the tag's secret key to K. Contrast to eavesdropping, H has more control and access to the system during this attack as the tag has been compromised.

Test (T_1, T_2, *i*): H has to guess the bit b ∈ {0,1} accurately to be successful depending upon an id ID_b which is chosen from { ID_1, ID_2 }.

According to the OSK scheme [23], in the game played between the system itself and attacker, H looks forward to the original tag. There are a couple of phases are deemed by the OSK in this game [24] [25].

Learning phase: H is competent to send the above queries in order to acquire knowledge about tags and readers. In this context, H initialized an execute query in order that H can eavesdrop to authentication session between R, and T_1 and variables B and C can be disclosed.

Challenge phase: H transmits a Test message to a new session and selects a random bit from {0, 1} by guessing. The fresh tags like T_1, T_2 having individual identifiers ID_1, ID_2 ($ID_1 \equiv 0 \bmod 2$ and $ID_2 \equiv 1 \bmod 2$) has been chosen. After that, H throws a Test query. Consequently, H is given a challenge to test identifier $ID_b = \{ID_1, ID_2\}$. We consider least significant bits (LSB) only. So as per construction, $b = ID_{bLSB}$.

Guessing phase: When H results a bit b, the game terminates and if it accurately guesses the ID of the tag then H will win because it will be capable of differentiating between tags. The accurate guess of H is considered as upper hand for H and denoted as:

$$AdvH(k) = \left| Pr[H\ wins] - \frac{1}{2} \right|$$

The adversary H outputs a guess $b' \equiv B_{LSB} \oplus C_{LSB}$, which can be derived as:

$$\begin{aligned} AdvH(k) &= \left| Pr[H\ wins] - \frac{1}{2} \right| \\ &= \left| Pr[b' = b - \frac{1}{2} \right| \\ &= \left| Pr[B \oplus C = b] - \frac{1}{2} \right| \end{aligned}$$

Considering only the LSBs we have:

$$AdvH(k) = \left| Pr[B_{LSB} \oplus C_{LSB} = b] - \frac{1}{2} \right|$$

Therefore, advantage for the adversary is negligible contrasting to ∈ (k) because here:

$$\begin{aligned} B_{LSB} &= \mathrm{Rot}(\mathrm{Rot}(K_{rLSB}, A_{LSB}) \oplus R_{LSB}, K_{rLSB}) \\ C_{LSB} &= \mathrm{Rot}(\mathrm{Rot}(K_{rLSB}, A_{LSB}) \oplus R_{LSB}, K_{rLSB} \oplus B_{LSB}) \end{aligned}$$

B and C are still uncertain and unpredictable since this is where rotation operation modulo 96 is used. There is a very low likelihood of positive guess. Consequently, during the game, the adversary can not infer the K and IDS values.

4.2 Vulnerabilities due to modular operations:

The study of our protocol was considered here, based on the modular operations. This method of evaluating in SASI was used by Hernandez-Castro et al.[7]. Since we have specifically used rotation operations to measure certain security parameters, another way to evaluate the security of our protocol is to test the conditions where the modular operation is not operating, i.e., the value (wt(B)(mod n)= 0.

Therefore,

$$B = \mathrm{Rot}\ (\mathrm{Rot}\ (K_r, A), K_r \oplus R)\ \text{[Using Eq. 3]}$$

In this case, the probability of ($K_r \oplus R$) mod n = 0 is $\frac{1}{n^2}$. So,

$$B = \mathrm{Rot}\ (\mathrm{Rot}\ (K_r, A), 0) = \mathrm{Rot}\ (K_r, A)\ \text{[Note: n = 96]}.$$

Rotation operation will be executed once again in our protocol and our protocol will not disclose any variable. So, the protocol will remain safe and secured. The probability of A mod n = 0 is $\frac{1}{n}$. The total probability of B compromised will be ($\frac{1}{n^2}$) which is almost negligible and assured resistivity of our protocol. Now, if B is compromised in any case, B would not disclose any key or variable as:

$$B \oplus A = B \oplus IDS \oplus R\ \text{[Using Eq. 2, 3]}$$

Similarly, $B \oplus C$ will not make valid information. Our protocol will also be protected in such a case. Let us examine this situation with other variable C(probability: $1/n^2$), we have: $C = K_r \oplus B$ Now, let us try to find out variables using C, we get:

$$C \oplus A = K_r \oplus B \oplus IDS \oplus R \text{ [Using Eq. 2, 6]}$$

Also, in this case, $C \oplus B$ will not disclose any value. An attacker may have the real value of R. However, with the single R, it is impossible to find out the values of other variables. Consequently, our protocol is not vulnerable because of the modular operation used during rotations.

4.3 Functionality of the protocol

Mutual Authentication: The valid tag and reader should test each other out and interact with each other. The exchanged messages are focused on shared values. Just the true reader and the tags store certain values. In the very first step, the reader authenticates the tag using a legitimate tag *ID*. Likewise, B and C must authenticate the user by name. Therefore, in our protocol only the legitimate tag and the reader will generate legitimate values and authenticate one another.

Confidentiality: The messages exchanged between the device tag and the reader all refer to the shared ID, pseudonym, key, and a number R created randomly. Retrieving the randomly generated number R and the IDS' transmitted between reader and tag without the original tag ID, pseudonym, and key is very nearly impossible. Besides this, it is very difficult to infer the keyword as well as the key, as this value is altered with each authentication step by masking with the previous keys.

Integrity: We can not use a random number generator on both the tag and the user side because of low-cost tags. It is also important to ensure the data validity of randomness on both sides. Modifying any of the exchanged values, like A or B, is quite complicated. But if someone can change any of the values, he/she won't remove the randomly generated number R, B' will be invalid, and the connection will be terminated. Therefore it is difficult for the attackers to change the values because they have to accurately determine B' and C'. Therefore our algorithm implies that a minor change in some value will result in something completely different.

Forward security: Forward authentication requires if the tag is breached, protecting the prior correspondence between the reader and the tag. As the alias, *IDS* and key K changes with the random number and system tags *ID*, if the attacker can know the *ID* somehow but cannot decode the previous communications. So the previous communications stay vigilant.

4.4 Security Attacks

Desynchronization Attack: In our protocol, both the pseudonym and the key have been changed in both the tag and the reader side after each authentication process to keep the tag and reader synchronized. The attacker may take the initiative to desynchronize by changing the exchanged values, A and B. But this is going to lead to an incorrect R and B', which leads to a terminated connection.

Disclosure Attack: In our algorithm, every measured value depends on two or more other values in order to make complex calculations. We use the Rot function twice to calculate the exchanged values. So, if the attack could compromise A and B, it would not be able to obtain any information. Thus, we say that our protocol is resilient to an attempt on disclosure.

Replay Attack: In our protocol, different random number will be generated for each authentication session, and depending on the random value and the local values, different A, B, and C will be determined. So, if the intruder tries to control R, A, B, and C, the communication will be terminated and the replays have no impact on our protocol.

Traceability Attack: As in our protocol, the tag never communicates its ID with others and all sent messages will be masked with the randomly generated number, so accessing the tags ID is very difficult. Besides these, the pseudonym will be replaced with the tags ID after every authentication. It is not possible, therefore, to trace any tag by its ID.

5. Performance Analysis

In this section, we present an analysis of the performance of the proposed protocol. Ultralightweight operators were included, while we introduced an ultralightweight protocol. We have already claimed that RFID tags cannot perform complicated heavyweight operator calculations. In our protocol, tag only involves two basic bitwise logical operations: XOR and Left Rotation based on hamming weight. These operations are very lightweight, simple to execute, and have very low computational costs. In our protocol, tag sent two messages (IDS', C'). So the number of messages tags sent is 2L. If we compare with other protocols, we do need 2L, but ours is more stable as we submit the IDS', which is then XORed of two identical values (*ID*, *IDS*).

Low-cost RFID tags have very poor memory. As far as other protocols are concerned, our proposed protocol needs less memory (4L). Each tag has to save tag ID, pseudonym *IDS*, Key K, and a random generated number R. Each of them is L (where L=96-bits) in size. The total storage requirements are therefore 4L bits, which is comparatively less than other protocols. During the authentication process, the number of messages sent by the tag during the protocol run is the cost of the communication. The cost of communication in our proposed protocol is only 3L. In addition, our protocol demonstrates resistance to various attacks, such as desynchronization, disclosure, and monitoring. Apart from

Table 1: Performance Analysis of our protocol with the other exiting UMAP

	LMAP [4]	SASI [2]	Gosaamer [8]	RAPP [9]	RCIA [1]	Tewari and Gupta [16]	Our MUMAP
Computational operations used	+, ⊕, OR	+, ⊕, OR, AND, Rot	+, ⊕, Rot, MixBits	⊕, Rot, Permutation	Rot, ⊕, AND	⊕, Rot	⊕, Rot
Tag generated messages	2L	2L	2L	2L	2L	2L	2L
Memory requirements	6L	7L	7L	5L	7L	7L	4L
Total number of messages for mutual authentication	4L	4L	4L	5L	5L	3L	3L
Security from De-synchronization attack	No	No	No	No	No	No	Yes
Security from Full disclosure attacks	No	No	Yes	No	No	No	Yes
Untraceability	No	No	No	No	No	No	Yes

this, as in our protocol, there are no AND and OR operations, our protocol is also immune to tango attacks. In Table 1, a comparison of our protocol with other existing protocols has been revealed. It is found that our protocol is working better than other exiting protocols.

6. Conclusion

Radio frequency identification is one of the extensively executed identifying procedures for node revelation in IoT networks. IoT networks lean toward RFID innovation because of top-level examining speed, unmistakable recognizing, and non-view filtering competency. For enhancing the security of RFID tags, many mutual authentication protocols have been proposed. In any case, sadly, none of these is completely made sure about. This paper puts forward a new ultralightweight mutual authentication protocol for IoT networks. The proposed protocol uses two bitwise operations (XOR and left rotation) which are particularly powerful for constrained resourced IoT devices. Contrast with different protocols, MUMAP requires low-cost in storage and communication. As the proposed algorithm is more secure and the protocol is resistive to various attacks, it very well may be the best decision to ease RFID tags utilized for IoT devices. In this paper, we talked about distinctive security attacks on RFID tags. We moreover mean to separate the security of the proposed protocol against DoS attacks. Later on, we likewise intend to perform a further top to bottom cryptanalysis of the proposed protocol.

References

[1] U. Mujahid, M. Najam-ul Islam, and M. A. Shami, "Rcia: A new ultralightweight rfid authentication protocol using recursive hash," *International Journal of Distributed Sensor Networks*, vol. 11, no. 1, p. 642180, 2015.

[2] H.-Y. Chien, "Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity," *IEEE transactions on dependable and secure computing*, vol. 4, no. 4, pp. 337–340, 2007.

[3] M. Khalid, U. Mujahid, and M. Najam-ul Islam, "Cryptanalysis of ultralightweight mutual authentication protocol for radio frequency identification enabled internet of things networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 8, p. 1550147718795120, 2018.

[4] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador, and A. Ribagorda, "Lmap: A real lightweight mutual authentication protocol for low-cost rfid tags," in *Proc. of 2nd Workshop on RFID Security*, p. 06, 2006.

[5] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "M 2 ap: a minimalist mutual-authentication protocol for low-cost rfid tags," in *International conference on ubiquitous intelligence and computing*, pp. 912–923, Springer, 2006.

[6] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "Emap: An efficient mutual-authentication protocol for low-cost rfid tags," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pp. 352–361, Springer, 2006.

[7] J. C. Hernandez-Castro, J. M. Tapiador, P. Peris-Lopez, and J.-J. Quisquater, "Cryptanalysis of the sasi ultralightweight rfid authentication protocol with modular rotations," *arXiv preprint arXiv:0811.4257*, 2008.

[8] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador, and A. Ribagorda, "Advances in ultralightweight cryptography for low-cost rfid tags: Gossamer protocol," in *International Workshop on Information Security Applications*, pp. 56–68, Springer, 2008.

[9] Y. Tian, G. Chen, and J. Li, "A new ultralightweight rfid authentication protocol with permutation," *IEEE Communications Letters*, vol. 16, no. 5, pp. 702–705, 2012.

[10] G. Avoine and X. Carpent, "Yet another ultralightweight authentication protocol that is broken," in *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pp. 20–30, Springer, 2012.

[11] I.-S. Jeon and E.-J. Yoon, "A new ultra-lightweight rfid authentication protocol using merge and separation operations," *International Journal of Mathematical Analysis*, vol. 7, no. 52, pp. 2583–2593, 2013.

[12] W. Shao-hui, H. Zhijie, L. Sujuan, and C. Dan-wei, "Security analysis of rapp an rfid authentication protocol based on permutation," *College of computer, Nanjing University of Posts and Telecommunications, Nanjing*, vol. 210046, pp. 293–308, 2012.

[13] S. Wang, S. Liu, and D. Chen, "Security analysis and improvement on two rfid authentication protocols," *Wireless Personal Communications*, vol. 82, no. 1, pp. 21–33, 2015.

[14] R. Bassil, W. El-Beaino, W. Itani, A. Kayssi, and A. Chehab, "Pumap: A puf-based ultra-lightweight mutual-authentication rfid protocol," *International Journal of RFID Security and Cryptography*, vol. 1, no. 1/2, pp. 58–66, 2012.

[15] H. Luo, G. Wen, J. Su, and Z. Huang, "Slap: Succinct and lightweight authentication protocol for low-cost rfid system," *Wireless Networks*, vol. 24, no. 1, pp. 69–78, 2018.

[16] A. Tewari and B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for iot devices using rfid tags," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1085–1102, 2017.

[17] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, "On the security of a new ultra-lightweight authentication protocol in iot environment for rfid tags," *The Journal of Supercomputing*, vol. 74, no. 1, pp. 65–70, 2018.

[18] U. Mujahid, M. Najam-ul Islam, and S. Sarwar, "A new ultra-lightweight rfid authentication protocol for passive low cost tags: Kmap," *Wireless Personal Communications*, vol. 94, no. 3, pp. 725–744, 2017.

[19] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, "A secure ecc-based rfid mutual authentication protocol for internet of things," *The Journal of Supercomputing*, vol. 74, no. 9, pp. 4281–4294, 2018.

[20] 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*, p. e3906, 2019.

[21] F. Zhu, P. Li, H. Xu, and R. Wang, "A lightweight rfid mutual authentication protocol with puf," *Sensors*, vol. 19, no. 13, p. 2957, 2019.

[22] A. Juels and S. A. Weis, "Defining strong privacy for rfid," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*, pp. 342–347, IEEE, 2007.

[23] M. Ohkubo, K. Suzuki, S. Kinoshita, *et al.*, "Cryptographic approach to "privacy-friendly" tags," in *RFID privacy workshop*, vol. 82, Cambridge, USA, 2003.

[24] K. Ouafi and R. C.-W. Phan, "Privacy of recent rfid authentication protocols," in *International Conference on Information Security Practice and Experience*, pp. 263–277, Springer, 2008.

[25] K. Ouafi and R. C.-W. Phan, "Traceable privacy of recent provably-secure rfid protocols," in *International conference on applied cryptography and network security*, pp. 479–489, Springer, 2008.

Mehedi Hasan Raju (Non-member) graduated from Department of Information and Communication Technology, Bangladesh University of Professionals, Dhaka. His research interests include RFID security, cybersecurity, Biometrics.

Mosabber Uddin Ahmed (Non-member) Ph.D. and Associate Professor in Department of Electrical and Electronic Engineering, University of Dhaka. His research interests include Signal Processing, Brain Signal Modeling, Complexity Analysis, Multiscale Entropy Analysis, and Embedded Systems Design.

Md Atiqur Rahman Ahad (Member) Ph.D. and Professor in Department of Electrical and Electronic Engineering, University of Dhaka. He is Specially Appointed Associate professor in Dept. of Media Intelligent, Osaka University, Japan. His research interests include Computer/Robot vision, Image/Medical-image analysis, Internet of Things (IoT), Robotics, Sensor.