


Cryptanalysis of ultralightweight mutual authentication protocol for radio frequency identification enabled Internet of Things networks

International Journal of Distributed
Sensor Networks
2018, Vol. 14(8)
© The Author(s) 2018
DOI: 10.1177/1550147718795120
journals.sagepub.com/home/dsn


Madiha Khalid¹ , Umar Mujahid² and Muhammad Najam-ul-Islam¹

Abstract

Internet of Things is one of the most important components of modern technological systems. It allows the real time synchronization and connectivity of devices with each other and with the rest of the world. The radio frequency identification system is used as node identification mechanism in the Internet of Thing networks. Since Internet of Things involve wireless channel for communication that is open for all types of malicious adversaries, therefore many security protocols have been proposed to ensure encryption over wireless channel. To reduce the overall cost of radio frequency identification enabled Internet of Thing network security, the researchers use simple bitwise logical operations such as XOR, AND, OR, and Rot and have proposed many ultralightweight mutual authentication protocols. However, almost all the previously proposed protocols were later found to be vulnerable against several attack models. Recently, a new ultralightweight mutual authentication protocol has been proposed which involves only XOR and Rotation functions in its design and claimed to be robust against all possible attack models. In this article, we have performed cryptanalysis of this recently proposed ultralightweight mutual authentication protocol and found many pitfalls and vulnerabilities in the protocol design. We have exploited weak structure of the protocol messages and proposed three attacks against the said protocol: one desynchronization and two full disclosure attacks.

Keywords

Radio frequency identification, ultralightweight, authentication, Internet of Things

Date received: 17 April 2018; accepted: 26 July 2018

Handling Editor: Paolo Bellavista

Introduction

The Internet of Thing (IoT) network refers to the Internet enabled devices which can be accessed globally on real time basis. These globally connected devices are being used in large number of applications such as smart grids, autonomous vehicles, and wearables. To communicate with the IoT nodes, object identification is a primary requirement. The identification techniques that are being used for node discovery are radio frequency identification (RFID) system, barcodes, quick response (QR) codes, and so on. The RFID system is preferred by the IoT networks due to high scan speed,

unique identification, and non-line of sight scanning capabilities. The applications that use radio frequency

¹Department of Electrical Engineering, Bahria University, Islamabad, Pakistan

²Department of Information Technology, Georgia Gwinnett College, Lawrenceville, GA, USA

Corresponding author:

Umar Mujahid, Department of Information Technology, Georgia Gwinnett College, 1000 University Center Lane, Lawrenceville, GA 30043-7409, USA.

Email: umarkhokhar1@hotmail.com



system for node management are termed as RFID-enabled IoT networks. The identity management system for such platforms mainly involves three components: the tag (\mathcal{T}), the reader (\mathcal{R}), and the backend database (\mathcal{D}). The \mathcal{T} is attached to the device which needs to be identified and the \mathcal{R} is connected to the \mathcal{D} which contains detail information of all the associated tags.

Since the \mathcal{R} communicates with the \mathcal{T} over a wireless channel which is open for all types of adversaries (\mathcal{A}), therefore some cryptographic suites must be incorporated to secure this channel. The traditional cryptographic methods are not suitable to ensure the security because of resources constraints at tag's side. Pedro Peris-Lopez et al.¹ proposed an ultralightweight category of authentication protocols for extremely low-cost computational systems, that is, the passive RFID tags. The protocols from this class involves simple bitwise logical operations in their designs to conform to the Electronic Product Code (EPC) C1G2 standards. According to the EPC C1G2 standard, a low-cost passive tag contains 10K gates out of which only 4K gates are allocated for the security-related tasks.

Since 2006, several ultralightweight mutual authentication protocols (UMAPs) have been presented. Some of the prominent authentication protocols are lightweight mutual authentication protocol (LMAP),¹ efficient mutual authentication protocol (EMAP),² strong authentication strong integrity (SASI) protocol,³ robust confidentiality integrity and authentication (RCIA) protocol,⁴ and pseudo-Kasami code based mutual authentication protocol (KMAP).⁵ However, to the best of our knowledge, almost all the previously proposed UMAPs were reported to be vulnerable against multiple denial-of-service (DoS), desynchronization, and full disclosure attacks. Recently, Tewari and Gupta proposed a new UMAP using only *XOR* and *Rot* functions.⁶ The authors have used several formal and structural security analysis tools to prove the robustness of the proposed UMAP against all possible attacks. In this article, we have performed cryptanalysis of their UMAP and highlighted some structural weaknesses. We have proposed three attack models against Tewari and Gupta protocol: one desynchronization and two full disclosure attacks.

The rest of the paper is organized as follows: Section "Related work" presents the literature review. Section "Tewari and Gupta protocol" introduces the authentication algorithm followed by detail security analysis in section "Security analysis of Tewari and Gupta protocol." Section "Comparison" analyzes our cryptanalysis approach and some recent attack models. Finally, section "Conclusion" concludes the paper.

Related work

The RFID system is one of the widely deployed identification schemes in the field of ubiquitous computing. The system uses radio frequency for unique and automatic identification of the objects. The RFID system mainly comprises three components: the tag (\mathcal{T}), the reader (\mathcal{R}), and the backend database (\mathcal{D}). The \mathcal{T} is a low-cost electronic chip that communicates with the \mathcal{R} over the wireless channel for basic identification and authentication. The \mathcal{D} stores the detailed information about all the tags and the reader. Usually, the channel between the \mathcal{R} and the \mathcal{D} is considered to be secure since there is no power constraint at the database side and traditional cryptographic algorithms (advanced encryption standard (AES), international data encryption algorithm (IDEA), elliptic curve cryptography (ECC), etc.) can be used to ensure the security and privacy. Because of limited computational capability at the tag's side, these traditional cryptographic algorithms cannot be used to secure the channel between the \mathcal{T} and the \mathcal{R} . The level of the security and the privacy of an RFID system is directly associated with the cost of the \mathcal{T} . The high-cost tags can support greater on-chip resources and therefore can support standardized encryption algorithms. While the low-cost passive RFID tags can support only bitwise logical operators to secure the wireless channel between the \mathcal{R} and the \mathcal{T} . In 2007, Chien classified the cryptographic protocols in four major categories:³

1. Full-fledged protocols: These protocols include classical cryptographic techniques such as the symmetric cryptography, the asymmetric cryptography, and the hash function. Because of adequate on-chip resources, active high cost RFID tags are capable to support security protocols under the umbrella of full-fledge class.
2. Simple protocol: This class of protocols can incorporate only pseudorandom number generator (PRNG) and the one-way hash function.
3. Lightweight protocols: The protocols fall under this class can support lightweight PRNG and cyclic redundancy check (CRC) and are suitable for many IoT applications.
4. Ultralightweight protocol: According to the EPC C1G2 standard, the protocols can support only 4K gate equivalents and therefore, only bitwise logical operators and ultralightweight primitives (*Rotation*, *Recursive hash*, etc.) can be used to perform security-related tasks.

In this research paper, our focus will be on ultralightweight protocols. Over the last decade, the researchers have proposed many (over 1000 protocols) UMAPs. Unfortunately, most of the previously proposed

UMAPs were reported to be vulnerable against simple DoS and full disclosure attacks. A comprehensive survey of the UMAPs and their weaknesses is presented as follows.

The foundation of UMAPs was laid by Pedro Peris-Lopez in 2006. Pedro Peris proposed three ultralight-weight authentication protocols, that is, LMAP,¹ EMAP,² and M²AP (minimalistic mutual authentication protocol).⁷ All these protocols use triangular functions (*T-functions*), that is, *AND*, *OR*, and *XOR*. The computational cost of LMAP and M²AP was 300 gate equivalents whereas EMAP used only 150 gates for implementation. The security standards of these protocols were ensured via randomness test suits: Diehard,⁸ ENT,⁹ and NIST.¹⁰ In 2007, detail cryptanalysis of these protocols was preformed.^{11,12} The researchers exploited inherent weak diffusion property of *T-functions* to perform probabilistic and deterministic full disclosure attacks. Multiple successful desynchronization attack models were also proposed by blocking tag authentication challenge message.

In 2007, Chien proposed the SASI protocol.³ Chien introduced a non-triangular function, that is, *Rot(x, y)* that performs left rotation of x by the hamming weight (HW) or modular weight of y . The basic requirements for implementation of the rotation function were two L bit registers (L refers to number of bits of session key) and a clock. Since single-bit left rotation requires one clock cycle, introduction of non-triangular function (*nonT-function*) increased the strength of SASI at the cost of elevated execution time and gate equivalents. The cryptanalysis of the SASI protocol presented multiple desynchronization attack schemes.¹³ Successful full disclosure and traceability attacks were also launched by exploiting the weakness of modular operation used in rotation function.^{14,15}

Later, Gossamer,¹⁶ Yeh et al.,¹⁷ and David-Parsad¹⁸ protocols were proposed. These protocols used single *nonT-function* to enhance the confusion and diffusion abilities of the public messages. The security analysis of these protocols demonstrated their lack of robustness against multiple structured and non-structured attack models.

After 2011, the strength of UMAPs was enhanced using multiple *nontriangular* primitives. One of the initial protocols that belonged to this category was the RFID authentication protocol using permutation (RAPP).¹⁹ The RAPP provided tag-reader authentication assurance using two *nonT-functions*, that is, rotation (*Rot(x, y)*) and permutation (*Per(x, y)*). The permutation function increased the efficiency of the protocol at the cost of increased memory requirement and execution time. In Shao-hui et al.²⁰ and Ahmadian et al.,²¹ the authors exploited the weakness of permutation function to reveal the HW of the operands. This

limitation became the basis of full disclosure and desynchronization attacks on the RAPP.

In 2016, H Luo et al.²² proposed a new ultralight-weight primitive, that is, the conversion function (*Conv(x, y)*) for succinct and lightweight authentication protocol (SLAP). The conversion function was composed of three non-triangular functions, that is, grouping, rearranging, and composition. All these subfunctions were bitwise shuffling techniques; therefore, conversion function did not require excessive hardware and was suitable for low-cost RFID tags. M Sakhani and N Bagheri²³ presented security analysis of SLAP and identified a very simple desynchronization attack which required only five authentication sessions between the \mathcal{R} and the \mathcal{T} to make them permanently desynchronized.

From above discussion, we can conclude that since last decade numerous UMAPs have been proposed^{1-5,7,16-18,20,22} but the cryptanalysis models highlighted their weakness and made these protocols unsuitable for practical tags^{11-13,15,20,21,23} Therefore, there is an immense need of new ultralightweight primitives and the UMAPs that could ensure the security of the systems optimally.

Tewari and Gupta protocol

To provide robust authentication solution to IoT node authentication problem, Tewari and Gupta came up with a *non-triangular* UMAP. For the completeness, they have used some formal security analysis models to verify the robustness of the protocol.

The protocol assumes that the channel between the \mathcal{R} and the \mathcal{T} is open for \mathcal{A} . Each \mathcal{T} stores an L bit identification number (ID) (L can be 32, 64 and 96 bits depending on the size of identification system) and two latest values of dynamic variables, which are, pseudonym and key $[(IDS^{new}, IDS^{old}), (K^{new}, K^{old})]$. The reader's memory also stores above-mentioned five L bit numbers associated with each tag. The memory architecture of the \mathcal{T} and the \mathcal{R} implementing Tewari and Gupta protocol is given in Table 1.

The detail explanation regarding execution of the protocol is described as follows:

1. The \mathcal{R} transmits *Hello* message to the \mathcal{T} . The \mathcal{T} sends a pair of latest pseudonyms (IDS^{new}, IDS^{old}) as a response.
2. The values received by the \mathcal{R} are searched in the memory. The outcome of the search can be divided into two categories.

CASE I: The \mathcal{T} and the \mathcal{R} are in complete synchronization and the received pair of pseudonyms is present in reader's memory. In this case, the \mathcal{R} will replace value of old pseudonym with latest index

Table 1. Memory architecture of Tewari and Gupta protocol.

Storage location: tag and reader					
Variable	ID	IDS^{new}	IDS^{old}	Key(K^{new})	Key(K^{old})
Size	96 bits	96 bits	96 bits	96 bits	96 bits
Nature	Static	Dynamic	Dynamic	Dynamic	Dynamic

pseudonym present in reader's memory

$$Reader\ IDS^{old} = Reader\ IDS^{new} \quad (1)$$

$$Reader\ K^{old} = Reader\ K^{new} \quad (2)$$

Case II: The tag's IDS^{new} is not found at reader's side and tag's IDS^{old} is equal to reader's IDS^{new} . This case arises due to unsuccessful tag's authentication in previous session. As a result, the pair of pseudonyms and keys at reader's side assumes latest values transmitted by the tag

$$Reader\ IDS^{old} = Reader\ IDS^{new} = Tag\ IDS^{new} \quad (3)$$

$$Reader\ K^{old} = Reader\ K^{new} = Tag\ K^{new} \quad (4)$$

Once the tag is identified, the authentication at both ends is performed on the basis of latest dynamic variable.

After successful tag identification, the \mathcal{R} generates two L bit random numbers m and n . The \mathcal{R} also calculates and transmits message $P||Q||R$

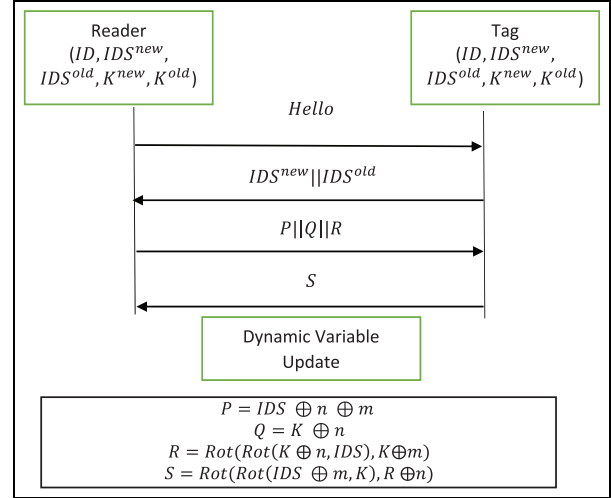
$$P = IDS \oplus n \oplus m \quad (5)$$

$$Q = K \oplus n \quad (6)$$

$$R = Rot(Rot(K \oplus n, IDS), K \oplus m) \quad (7)$$

- The message P and Q are used for extraction of random numbers m and n , respectively. Message R is used for the \mathcal{R} authentication. For reader verification, the \mathcal{T} calculates local value of R and compares it with the received value. The \mathcal{R} is successfully authenticated if both the values match.
- In this step, the \mathcal{T} calculates and transmits message S . After transmitting tag authentication challenge message S , the dynamic memory at tag's side is updated using equations (9)–(12)

$$S = Rot(Rot(IDS \oplus n, K), R \oplus m) \quad (8a)$$

**Figure 1.** Block diagram of Tewari and Gupta protocol.

A variant of the protocol uses another expression of the message S which is defined as follows

$$S = Rot(Rot(IDS \oplus m, K), R \oplus n) \quad (8b)$$

- The \mathcal{R} calculates the response of the \mathcal{T} authentication challenge S' . If both challenge and response messages are equal, the \mathcal{T} gets successfully authenticated. After mutual authentication, dynamic variables of reader's memory are updated using following equations

$$IDS^{old} = IDS^{new} \quad (9)$$

$$K^{old} = K^{new} \quad (10)$$

$$IDS^{new} = Rot(Rot(IDS \oplus n, K \oplus n), IDS \oplus m) \quad (11)$$

$$K^{new} = Rot(R \oplus n, IDS \oplus m) \quad (12)$$

The block diagram for representation of Tewari and Gupta protocol is presented in Figure 1.

Security analysis of Tewari and Gupta protocol

The Tewari and Gupta protocol⁶ is a *non-triangular* UMAP which incorporates two ultralightweight primitives, that is, *XOR* and *Rot*(x, y). Instead of using traditional HW-based rotations, the protocol uses the modular rotation (MR) function to increase the computational complexity of the protocol's equations. However, in our cryptanalysis models, we have shown that how this novel idea results in calamity of the protocol. We have proposed one simple desynchronization and two full disclosure attack models on the protocol. The detailed description of the attacks is presented as follows.

Desynchronization attack

In the desynchronization attack model, the \mathcal{A} disconnects an authentic \mathcal{T} from the RFID system. The objective of this cryptanalysis model is to tamper the dynamic memory of the \mathcal{R} and as a result, the protocol terminates at the identification stage.

Two design properties of the Tewari and Gupta protocol form the basis of successful desynchronization attack on the \mathcal{T} . These properties are described as follows:

- The tag's static identification number (*ID*) is never used for public message calculation.
- The \mathcal{R} overwrites the dynamic memory associated with the \mathcal{T} without formal verification of the tag's identity.

The above-mentioned attributes of the protocol lead to the desynchronization attack. The description of proposed attack model is described as follows.

As discussed in section "Tewari and Gupta protocol" (step b), if the tag and the reader's index pseudonyms are not in complete synchronization, the \mathcal{R} updates its dynamic memory with the latest value of *IDS* received from the \mathcal{T} as a response to the *Hello* message. Our proposed attack model exploits this feature of the protocol to execute deterministic desynchronization attack. The model requires two consecutive identification sessions on a completely synchronized tag–reader pair:

Session 1: In the first session, the \mathcal{A} eavesdrop the response of the reader's *Hello* message [IDS^i, IDS^{i-1}] and blocks the tag authentication challenge message *S*. As a result, the identity pseudonyms in tag's memory are updated, that is, [IDS^{i+1}, IDS^i] whereas the reader's dynamic memory remains same, that is, [IDS^i, IDS^{i-1}].

Table 2. Memory status of tag–reader pair during desynchronization attack.

Session	Reader memory status		Tag memory status	
Initial state	IDS^i	IDS^{i-1}	IDS^i	IDS^{i-1}
Session i	IDS^i	IDS^i	IDS^{i+1}	IDS^i
Session $i + 1$	IDS^i	IDS^i	IDS^{i+1}	IDS^i

Session 2: In this session, the \mathcal{A} impersonates as an authentic \mathcal{T} and responds to the reader's *Hello* message with the string [IDS', IDS^i]. The IDS' is a L bit random number whereas IDS^i was recorded by the \mathcal{A} in earlier session. The reader's memory search concludes partial synchronization between the \mathcal{T} and the \mathcal{R} and the protocol updates the reader's dynamic memory using equation (13)

$$Reader\ IDS^{new} = Reader\ IDS^{old} = IDS' \quad (13)$$

At the end of this session, the identity pseudonyms on reader's side assume an invalid value, that is, (IDS') whereas the values of *IDS* stored at the tag's side are (IDS^{i+1}, IDS^i). After the successful execution of desynchronization attack, the protocol will always terminate in the identification phase. Table 2 elaborates the memory status of tag–reader pair subjected to desynchronization attack.

Probabilistic full disclosure attack

We have used Hernandez-Castro et al.¹⁵ lemma in order to simplify the MR function. Our proposed probabilistic attack model is active in nature since we need to block one authentication message and it requires only one authentication session to retrieve all of the secrets. The attack executes as follows:

Step 1: After receiving the *Hello* message, the legitimate \mathcal{T} responds with two values of *IDS* (IDS^{new}, IDS^{old}). Since the channel is wireless therefore, the \mathcal{A} can listen their conversation and hence stores both values.

Step 2: Upon receiving of *IDS* (both new and old), the legitimate \mathcal{R} sends *P*, *Q*, and *R* messages to the legitimate \mathcal{T} . The \mathcal{A} again intercepts these messages, stores them, and performs following operations to fully disclose the concealed secrets.

The intercepted messages are

$$P = IDS \oplus m \oplus n \quad (14)$$

$$Q = K \oplus n \quad (15)$$

$$R = Rot(Rot(K \oplus n, IDS), K \oplus m) \quad (16)$$

Since the authors have used the MR functions, and according to lemma,¹⁵ equation (16) can be simplified as follows with $1/L$ probability (where L denotes the size of ID)

$$R = Rot(Rot(K \oplus n, IDS), 0) \quad (17)$$

Further simplification of equation (17) will result in

$$R = Rot(K \oplus n, IDS) \quad (18)$$

$$R = K \oplus n \quad (19)$$

The success rate of equation (19) is $1/L^2$.

Step 3: Upon successful authentication, the \mathcal{T} calculates and transmits message S (equation (8a)) toward legitimate reader; however, the \mathcal{A} first intercepts this message and then blocks this message from reaching at the reader's side so it may not update its pseudonyms. The \mathcal{A} performs following computations in order to retrieve the concealed secrets.

The \mathcal{A} uses the same lemma¹⁵ to simplify message S as well and after simplification, the message S calculated will become

$$S = IDS \oplus n \quad (20)$$

Now, take XOR between equations (19) and (20)

$$S \oplus R = IDS \oplus n \oplus K \oplus n \quad (21)$$

$$S \oplus R = IDS \oplus K \quad (22)$$

$$K = S \oplus R \oplus IDS \quad (23)$$

Since all of the variables in equation (23) are publicly known (S, R , and IDS) therefore we can easily extract the value of secret key (K). Furthermore, by substituting the value of K in publicly known equations, the remaining secrets can be disclosed as well.

Since $Q = K \oplus n$ and $P = IDS \oplus m \oplus n$, we can calculate the remaining concealed values

$$n = Q \oplus K \quad (24)$$

$$m = P \oplus IDS \oplus n \quad (25)$$

The success rate of the proposed attack model is $1/L^2$ and it can be further improved using recursive differential cryptanalysis (RDC) for simplification for the MR-based equations.

Guess and determine attack

This attack model exploits the poor composition of the protocol messages design and shows that the plain use of double rotation function can make the protocol a soft target for the adversaries. The guess and determine

attack is a passive model with the success probability of $1/2^{2L}$, that is, for a 96-bit system the probability will become $1/2^{192}$. In this attack model, the \mathcal{A} first collects and stores all publicly exchanged messages (P, Q, R , and S) of the protocol. Then \mathcal{A} performs following steps to retrieve the concealed secrets (m, n and K):

1. Take XOR between message P and Q

$$P \oplus Q = IDS \oplus K \oplus m \oplus K \oplus n \quad (26)$$

$$P \oplus Q = IDS \oplus K \oplus m \quad (27)$$

2. All of the variables in equation (27) are public, except K and m ; however, \mathcal{A} knows the output of $J = P \oplus Q$ that will be used as a seed for guess and determine model. The equations (28)–(30) will be used to execute the guess and determine attack

$$J = P \oplus Q \quad (28)$$

$$A = J \oplus IDS \quad (29)$$

$$A = K \oplus m \quad (30)$$

In order to compute these secrets, the \mathcal{A} applies the guess and determines model in following manner: \mathcal{A} generates all the possible combinations (strings of L bit) of K and m that can yield A in a sequential manner using equation (30). For example, if (starting from most significant bit (MSB)) i th bit value of $A_i = 1$, then (for one conjecture combination) i th bit of $K_i = 1$ while $m_i = 0$ and if $i + 1$ bit or any succeeding bit of $A_{i+1} = 1$, then $K_{i+1} = 0$ while $m_{i+1} = 1$ and similar method will be used $A_i = 0$ as well.

3. Use all conjecture sets of m to calculate conjecture n sets

$$n = P \oplus IDS \oplus m \quad (31)$$

All sets of conjecture n will have the error on the same position as that of m .

4. Now, shortlist only those combinations of conjecture secrets n and K which satisfy equation (15) and discard the remaining conjecture sets.
5. Since all of the variables (IDS, K, m , and n) are basically computed from pseudo random number generators (PRNGs) which actually hold the balance and run properties and hence computed random sequences contain equal number

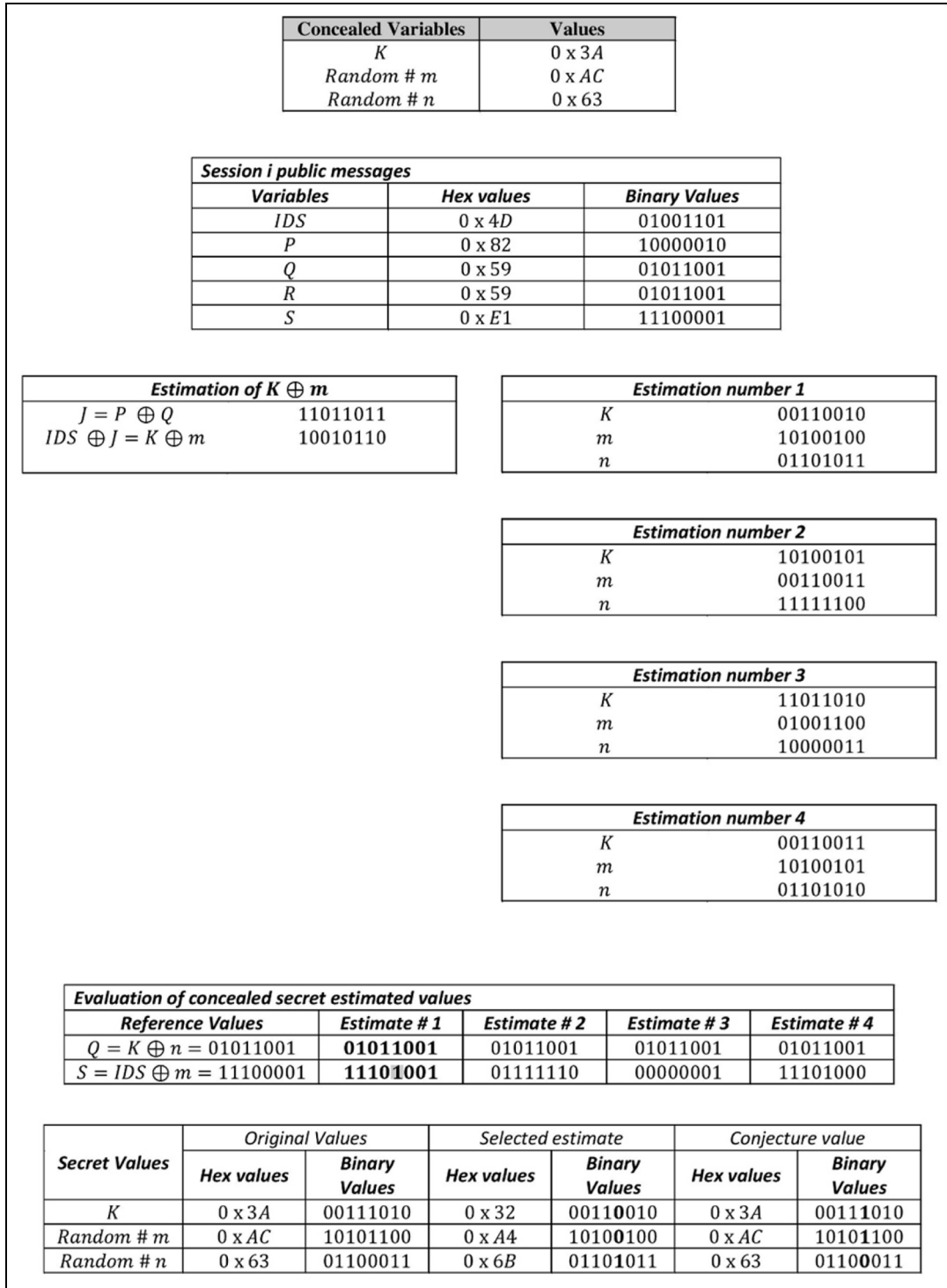


Figure 2. Example of guess and determine attack model.

of 0s and 1s. Because of this fact, use of double rotation function can be dangerous since it can get back the original operands (internal secrets). Therefore, the following lemma has been proposed

Lemma 1

$$W = Rot(Rot(X, Y), Z)$$

$$\text{If } hw(Y) = hw(Z) \text{ then } W = X$$

Table 3. Comparison of full disclosure attack models.

	Proposed attack	Passive attack #1 ²⁴	Passive attack #2 ²⁵
Requirements of adversary	Eavesdrop single authentication session	Eavesdrop single authentication session	Eavesdrop single authentication session
Basics of full disclosure attack	Utilization of structural weakness of modular rotation to estimate $IDS \oplus m$	Brute force attack to estimate $IDS \oplus m$	Brute force attack to estimate $IDS \oplus m$
Probability of full disclosure attack	$P \left(\begin{array}{l} \text{Probabilistic} \\ \text{attack} \end{array} \right) = 1/L^2$ $P \left(\begin{array}{l} \text{Guess and} \\ \text{determine} \\ \text{attack} \end{array} \right) = 1/2^{2L}$	$P = 1$	$P = 1$
Basics of full desynchronization attack	Utilization of protocols ability to update readers dynamic memory without authentication	–	–
Probability of desynchronization attack	$P = 1$	–	–

6. Now, let us apply Lemma 1 on equation (16) and if $R = Q$ only then this attack will work; otherwise, attacker will wait for the next authentication session. However, if the protocol messages have been computed using PRNGs, then because of poor message compositions this will happen all the times (verified over 10,000 sessions).
7. Similarly, after validating $R = Q$, the message S from equation (8b) will become $S = IDS \oplus m$. Now, there are two ways to compute to retrieve conjecture m :
 - Take XOR between the IDS and shortlisted combinations of m (step d). Then compare the result with S and select that string which satisfies received S . If there is a disagreement at a single bit position, conjecture m can be calculated by flipping the bit at position of disagreement. After retrieval of m , rest of the secrets can be easily calculated from equations (14) and (15).
 - Taking XOR between IDS and S can also give the same results.

Figure 2 shows the working of the attack model with 8-bit variable length. Although the proposed model uses the brute force technique but the possible combinations of K and m are shortlisted with the success probability of $1/2^{2L}$ using string A .

Comparison

In this section, we have compared our cryptanalysis model with existing attacks on the said protocol. As of today, two passive full disclosure attacks were reported in Safkhani and Bagheri²⁴ and Wang et al.²⁵ Unlike the existing attacks, our proposed cryptanalysis model exploits the structural weakness of MR primitive;

therefore, our cryptanalysis model can be applied to a wide range of protocols that use *Rotation* function. Moreover, we have also highlighted the desynchronization attack for the said protocol which shows the structural weakness of the protocol. Table 3 shows a comparison of the cryptanalysis models.

Conclusion

Recently, a new UMAP has been proposed by Tewari and Gupta⁶ and they have used only $Rot(x, y)$ and XOR operations in their design. The protocol was claimed to be robust against all possible adversarial models. In this article, we have challenged their claim of being robust against desynchronization and full disclosure attack. We have proposed three attack models and highlighted the vulnerabilities of the protocol. The utmost pitfall in mutual authentication protocol is that the tag's ID is not at all used throughout the authentication session which eventually leads toward desynchronization, denial of service, and even full disclosure attacks.


Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Bahria University, Pakistan provided financial support for publication of this article.

ORCID iD

Madiha Khalid  <https://orcid.org/0000-0001-9069-7865>

References

- Peris-Lopez P, Hernandez-Castro JC, Estévez-Tapiador JM, et al. LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags. In: *Proceedings of the 2nd workshop on RFID security*, Graz, 12–14 July 2006, p.6.
- Peris-Lopez P, Hernandez-Castro JC, Estévez-Tapiador JM, et al. EMAP: an efficient mutual-authentication protocol for low-cost RFID tags. In: *Proceedings of the OTM confederated international conferences: "On the move to meaningful internet systems,"* Montpellier, 29 October–3 November 2006. Berlin: Springer.
- Chien HY. SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE T Depend Secure* 2007; 4(4): 337–340.
- Mujahid U, Najam-ul-Islam M and Shami MA. RCIA: a new ultralightweight RFID authentication protocol using recursive hash. *Int J Distrib Sens N* 2015; 11(1): 642180.
- Mujahid U, Najam-ul-islam M and Sarwar S. A new ultralightweight RFID authentication protocol for passive low cost tags: KMAP. *Wirel Pers Commun* 2017; 94(3): 725–744.
- Tewari A and Gupta B. Cryptanalysis of a novel ultralightweight mutual authentication protocol for IoT devices using RFID tags. *J Supercomput* 2017; 73(3): 1085–1102.
- Peris-Lopez P, Hernandez-Castro JC, Estévez-Tapiador JM, et al. M²AP: a minimalist mutual-authentication protocol for low-cost RFID tags. In: *Proceedings of the international conference on ubiquitous intelligence and computing*, Wuhan, China, 3–6 September 2006. Berlin: Springer.
- Marsaglia G and Tsang WW. Some difficult-to-pass tests of randomness. *J Stat Softw* 2002; 7(3): 1–9.
- Woodcock N and Naylor MA. Randomness testing in three-dimensional orientation data. *J Struct Geol* 1983; 5(5): 539–548.
- Chari S, Jutla C, Rao JR, et al. A cautionary note regarding evaluation of AES candidates on smart-cards. In: *Proceedings of the second advanced encryption standard candidate conference*, Rome, Italy, 22–23 March 1999. State College, PA: CiteSeerx.
- Li T and Deng R. Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol. In: *Proceedings of the second international conference on availability, reliability and security*, Vienna, 10–13 April 2007. New York: IEEE.
- Li T, Wang G and Deng RH. Security analysis on a family of ultra-lightweight RFID authentication protocols. *J Softw* 2008; 3(3): 1–10.
- Sun HM, Ting WC and Wang KH. On the security of Chien's ultralightweight RFID authentication protocol. *IEEE T Depend Secure* 2011; 8(2): 315–317.
- Jeon IS and Yoon EJ. A new ultra-lightweight RFID authentication protocol using merge and separation operations. *Int J Math Anal* 2013; 7(52): 2583–2593.
- Hernandez-Castro JC, Tapiador JM, et al. *Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations*. Technical report arXiv: 0811.4257, 2008, <https://arxiv.org/abs/0811.4257>
- Peris-Lopez P, Hernandez-Castro JC, Tapiador JM, et al. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In: *Proceedings of the international workshop on information security applications*, Jeju Island, Korea, 23–25 September 2008. Berlin: Springer.
- Yeh KH, Lo N and Winata E. An efficient ultralightweight authentication protocol for RFID systems. *Cryptol Inform Secur Ser* 2010; 10: 49–60.
- David M and Prasad NR. Providing strong security and high privacy in low-cost RFID networks. In: *Proceedings of the international conference on security and privacy in mobile information and communication systems*, Turin, 3–5 June 2009. Berlin: Springer.
- Tian Y, Chen G and Li J. A new ultralightweight RFID authentication protocol with permutation. *IEEE Commun Lett* 2012; 16(5): 702–705.
- Shao-hui W, Zhijie H, Sujuan L, et al. *Security analysis of RAPP an RFID authentication protocol based on permutation*. Nanjing, China: College of Computer, Nanjing University of Posts and Telecommunications, 2012, p.210046.
- Ahmadian Z, Salmasizadeh M and Aref MR. Desynchronization attack on RAPP ultralightweight authentication protocol. *Inform Process Lett* 2013; 113(7): 205–209.
- Luo H, Wen G, Su J, et al. SLAP: succinct and lightweight authentication protocol for low-cost RFID system. *Wirel Netw* 2018; 24(1): 69–78.
- Safkhani M and Bagheri N. Generalized desynchronization attack on UMAP: application to RCIA, KMAP, SLAP and SASI + protocols. *IACR Cryptol ePrint Arch* 2016; 2016: 905.
- Safkhani M and Bagheri N. Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. *J Supercomput* 2017; 73(8): 3579–3585.
- Wang KH, Chen CM, Fang W, et al. On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *J Supercomput* 2018; 74(1): 65–70.