Pak. J. Engg. & Appl. Sci. Vol. 19 July, 2016 (*p.* 14–25)

Probabilistic Recursive Cryptanalysis of Ultralightweight Mutual Authentication Protocols for Passive RFID Systems

Umar Mujahid[1] and M.Najam-ul-islam[2]

1. Department of Electrical Engineering, Bahria University Islamabad, Pakistan
2. High Speed Digital Design Research Group, Bahria University Islamabad, Pakistan

* **Corresponding Author:** E-mail: umarmujahid.bahria@gmail.com

Abstract

Security and privacy are the fundamental concerns of RFID systems. Several ultralightweight mutual authentication protocols have been proposed to ensure the security of RFID systems in cost effective manner. These protocols usually involve simple bitwise logical operations such as XOR, AND, OR and some special purpose ultralightweight primitives. In this paper, we identify the vulnerabilities of the two recently proposed ultralightweight mutual authentication protocols: SASI and Yeh. et al. We have used Recursive Linear Cryptanalysis (RLC) for security analysis of SASI protocol, which requires only two authentication sessions to reveal concealed secret ID of the tags. For Yeh et al. protocol, we have proposed an active Quasi-Linear attack, which requires approximately 2^{13} *authentication sessions to disclose the tag's secret ID.*

Key Words: Security, RFID, Synchronization, Ultralightweight mutual authentication protocols, SASI

1. Introduction

RFID (Radio Frequency Identification) is one of the most growing systems in the field of ubiquitous computing. RFID systems automatically identify the objects with non-line of sight capability. This feature makes RFID systems more exclusive than its contending systems. However as RFID systems incorporate wireless channel, so there are some allied security risks and apprehensions from malicious adversaries.

A typical RFID system comprises of three components: tags, readers and back-end database. In normal scenario, the reader enquiries such tags, which enter in the vicinity of the reader. Upon receiving of reader's query, the tag responds with its identity *ID*. After receiving *ID*, the reader uses it as an index to search a matched entry in the database. If both values coincide, only then the tag can have access to the RFID associated particular systems. Usually, it is assumed that the channel between reader and back-end database is secure, as we can incorporate traditional cryptographic algorithms to ensure security. However, the channel between reader and tag needs more attention as limited computational capabilities at tag's side restrict us to use simple bitwise logical operations (*T-functions.* [27]) to secure the systems.

Chein [1] categorized the RFID mutual authentication protocols into four classes: Full-fledged, Simple, Lightweight and Ultralightweight.

Full-fledged protocols support traditional encryption schemes (such as AES, DES, hash functions etc.) while Simple protocols can only support pseudo-random number generators and one-way hash functions. Lightweight protocols incorporate lightweight pseudo-random number generators and low cost operations like CRC (Cyclic Redundancy Check), however one-way hash functions cannot be used in this class. Ultralightweight protocols support only simple bitwise logical operations (such as XOR, AND, OR etc.) to provide the security and privacy in cost effective manner. Usually in ultralightweight authentication protocols, tag supports maximum 250 – 3K logic gates for security related tasks. Since 2006, numerous ultralightweight authentication protocols have been proposed; section II highlights the various previously proposed authentication protocols. In this paper, we have highlighted the vulnerabilities of two ultralightweight authentication protocols: SASI (Strong Authentication and Strong Integrity) and Yeh. et al. [23].

The rest of the paper is organized as follows: Section II describes the literature review. Section III

highlights the generic structure of ultralightweight authentication protocols. In section IV, we present the novel attacks on SASI and Yeh et al. [23] protocols and finally section V concludes the paper.

2. Literature Review

In 2006, Peris Lopez et al. proposed a family of Ultralightweight RFID Mutual Authentication Protocols (UMAP): LMAP [4] (Lightweight Mutual Authentication Protocol), M^2AP [7] (Minimalist Mutual Authentication Protocol) and EMAP [6] (Efficient Mutual Authentication Protocol). UMAP family protocols involve only simple bitwise logical operations (such as XOR, AND, OR etc.) on tags to provide the optimal security with minimal cost. These protocols mainly involve three steps: tag identification, mutual authentication, pseudonym and keys updating. The randomness of the protocols messages is ensured with three randomness test suites: DIEHARD [33], ENT [34] and NIST [35]. However in 2007, Tieyan Li and Guilin Wang [40] highlighted the security vulnerabilities of UMAP family protocols. They exploit the poor diffusion properties of the *T – functions* used in protocols messages and proposed two attacks: desynchronization and full disclosure attack. Desynchronization attack abolishes the potential relation between reader and tag while full disclosure attack reveals all the concealed secrets.

In 2007, Chein [1] proposed a new ultralightweight authentication protocol: Strong Integrity and Strong Authentication (SASI). In addition to simple bitwise logical operations, a new ultralightweight primitive *Rot* (Left Rotation) has been integrated in the protocol messages to enhance the diffusion properties of the protocol. However, Sun et al.[3], Avoine et al.[26] and Hernandez-Castro et al. [25] showed that the *Rot* function is also a linear function, therefore inherits all the pitfalls of *T-Functions*. Hence SASI is also vulnerable to various desynchronization, DoS and full disclosure attacks.

In 2008, Peris Lopez et al.[9] proposed a quite interesting ultralightweight authentication protocol: GOASSMER. A new ultralightweight non-triangular primitive "*MixBits*" (using genetic programming) has been integrated in the protocol messages to provide the optimal security. To the best of our knowledge, the *MixBits* function is the most powerful nonlinear primitive used in such protocols; however authors have not clarified whether *MixBits* function falls in the domain of ultralightweight. In 2009, Yeh et al.[10] and Zeeshan et al.[11] found the weakness in GOASMMER protocol's structure. They highlighted the Denial of Service (DoS) and desynchronization attacks on GOASSMER protocol. Zubair et al.[12] incorporated the counter based methodology in GOASSMER protocol to avoid highlighted attacks.

Later, David-Prasad [13] and Lee et al. [36] proposed authentication protocols using simple *T – functions* and *Rot* function respectively. However, both protocols were also reported [14,37] to be vulnerable against various desynchronization and full disclosure attacks.

In 2012, Tian et al. [15] introduced a new ultralightweight primitive *"Permutation (Per)"* and proposed a novel protocol: RAPP (RFID Authentication Protocol using Permutation). RAPP excessively uses permutation operation in protocol messages to enhance the computational complexity for adversaries. Initially, like *Rot* function, *Per* function also seemed to be nonlinear function; however later on it was shown that permutation operation reveals the information of hamming weight (*hw*) of the first parameter (operand) [32]. In the same year, Bagheri et al. [16] and Wang et al.[38] proposed a desynchronization and full disclosure attack on RAPP respectively. However the requirement of massive authentication sessions makes full disclosure attack less feasible.

In all [1, 2, 4, 6, 7, 9, 13, 15, 18, 19, 23, 28, 36] ultralightweight authentication protocols have been proposed, but most of these protocols have similar flaws such as use of *T – function*, Linear functions (*Rot, Per* etc.) and poor messages composition etc. So, these parameters should be taken into account while designing a privacy friendly authentication protocols.

3. Ultralightweight Mutual Authentication Protocols (UMAP)

In this section, we describe the general structure of the ultralightweight authentication protocols. Since

2006, numerous ultralightweight authentication protocols have been proposed; however the basic structure (working) of the protocols is quite similar. Fig.1 shows the generic structure of the ultralightweight authentication protocols.

In all ultralightweight protocols, each tag pre-shares its identity pseudonym (*IDS*), key (*K*) and static identity (*ID*) with the readers. Reader uses *IDS* for initial identification of the tag instead of the tag's original *ID*. A normal authentication protocol involves following five steps:

1. Reader initiates the protocol session by sending a message *"Hello"* towards tag.
2. Upon receiving the reader's query, tag responds with its *IDS*.
3. After receiving *IDS*, the reader uses it as an index to search a matched entry in the database. If a matchoccurs, then the reader computes a pseudorandom number *'n'* conceals *'n'* in message M_R using bitwise logical operations ($M_R=f_t^*$ (IDS, n, K)) and finally transmits M_R towards the tag. If reader does not find a suitable match of *IDS* in the database, then it either terminates protocol session with the particular tag or asks for old *IDS*.
4. Upon receiving of M_S message, the tag performs following four tasks:
   i) Extracts pseudorandom number *'n'*.
   ii) Authenticates reader, as only legitimate reader (with prior knowledge of tag's secret information) can compute a valid message, $MR = f_i$ (*IDS, n, K*) which will be acceptable for the tag.
   iii) Computes the message M_T ($M_T = f_2$ (*IDS, n, K, ID*)) by concealing its original *ID* in the message and then transmits M_T towards the reader.
   iv) Finally, the tag updates its pseudonym (*IDS*) and key (*K*):

   $$IDS_{next} = f_3 (IDS)\ t \qquad K_{next} = f_4 (K)$$

5. Reader computes the local value of message M_T and compares it with the received M_T, if both the values are same then the reader successfully authenticates the tag. Now, reader will also update the pseudonyms and keys of the particular tag in its database for future correspondence with the tag.

   $$IDS_{next} = f_3 (IDS);\ K_{\text{next}} = f_4 (K)$$

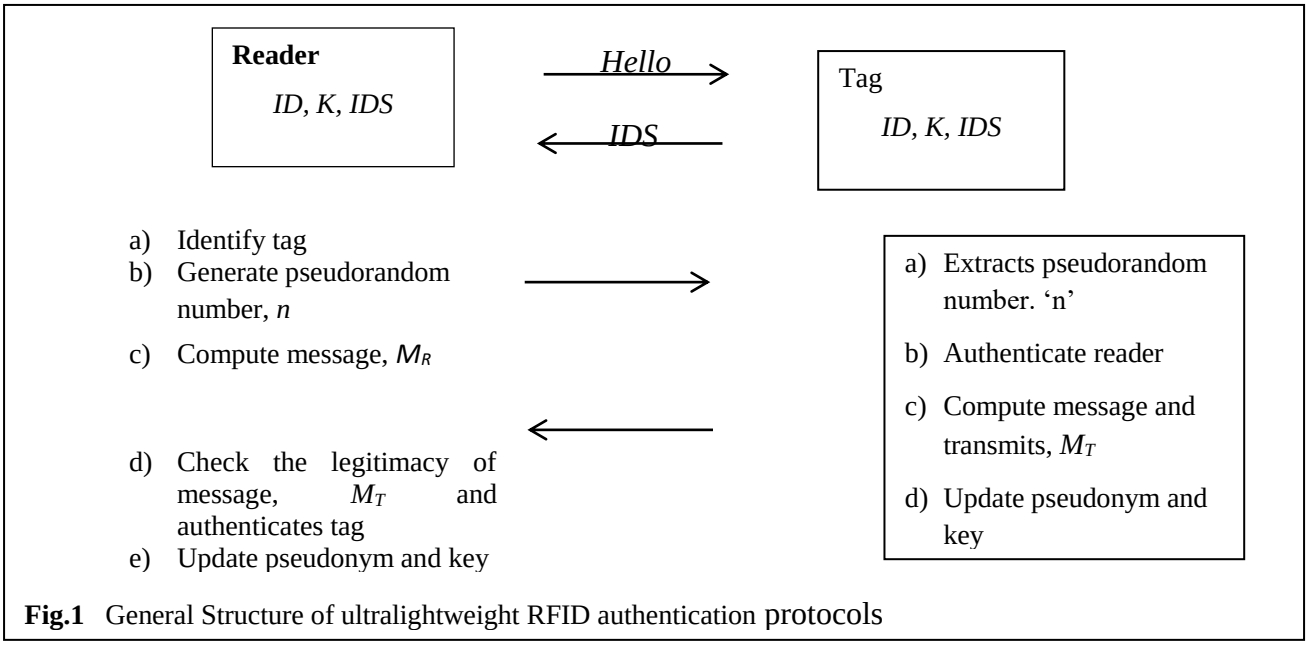

Fig.1 General Structure of ultralightweight RFID authentication protocols

* *where f_t represents the protocol specific function to compute/update messages.*

Security analysis of the ultralightweight authentication protocols is performed in two main aspects: the basic functionality of the protocol (privacy & authentication) and resistance against various known attacks. Most of the attacks (desynchronization, replay, full disclosure etc.) proposed for ultralightweight authentication protocols are based on ad-hoc based methods, which are not extensible to a larger class of ultralightweight protocols. The basic description of these ad-hoc attacks is as follows:

a) Desynchronization attack mainly disrupts the synchronization between the reader and the tag. After each successful authentication session, both the reader and the tag update their pseudonym and key for future correspondence. If an adversary blocks the message M_T from reaching at the reader, then the tag will update its variables while the reader keeps the previous values of variables. Next time, when the reader sends the "*Hello*" message towards the tag, it will respond with its updated IDS_{new}, which will not be acceptable to the reader. Hence the reader will terminate its protocol session with a legitimate tag. In order to avoid desynchronization attack, the object that first updates its pseudonym and key must maintain a backup of its preceding state as well.

b) In Replay attacks, the attacker may impersonate as a legitimate reader or tag and replays the previously captured messages of the genuine protocol session to launch a Denial of Service (DoS) attack. Replay attack can also be used to desynchronize both the reader and the tag [3].

c) In Full disclosure attacks, the attacker tries various modified combinations of the messages to find the suitable approximation of the tag's internal secrets. Most of the full disclosure attacks are ad-hoc based, which are protocol specific, however some structural (formal) cryptanalysis frameworks such as Tango, Recursive linear and differential cryptanalysis etc. also exist to validate the security claims of the protocols.

We will also use Recursive Linear Cryptanalysis to highlight the vulnerabilities of SASI protocol in Section IV.

4. Cryptanalysis of Ultralightweight Mutual Authentication Protocols

In this section, cryptanalysis of two ultralightweight authentication protocols (SASI and Yeh et al.) has been performed. We have applied Recursive Linear Cryptanalysis RLC [24] on SASI, which requires only two authentication sessions to reveal concealed secret *ID* of the tags. For Yeh et al. protocol [23] we have proposed an active Quasi-Linear attack: which requires approximately 2^{12} authentication sessions to retrieve tag's *ID*.

The basic working and the cryptanalysis of both the protocols are given below:

4.1 Strong Authentication and Strong Integrity (SASI) protocol

In 2007, Chein proposed an ultralightweight authentication protocol: SASI. A new ultralightweight non-triangular function *Rot* (Left rotation) has been extensively used in protocol messages to enhance the diffusion properties of the messages. Rotation, *Rot* (*X*, *Y*) is basically circular left shifting of *X* according to the hamming-weight of *Y*. Rotation function is extremely lightweight as it requires only two registers for its operation, however it is a clock cycle consuming operation (since for each rotation, *'l'* clock cycles are required; where *l* is the number of bits in both strings).

In SASI, each tag has a static *l - bit* unique identity *ID* and pre-shares its pseudonym (*IDS*) and keys (K_1, K_2) with reader. The tag also keeps the set of previous values of *IDS* and keys to overcome the desynchronization attacks. Fig. 2 illustrates the specification of SASI protocol.

The working of the protocol is as follows:

1. The reader sends *"Hello"* message towards tag to initiate the protocol session.
2. The tag responds with its currently updated *IDS.*
3. After receiving *IDS*, the reader uses it as an index to search a matched entry in the database. If a match occurs then the reader generates two pseudorandom numbers (n_1, n_2), computes and transmits *A*, *B* and *C* messages. *A* and *B* messages are used to transmit pseudorandom numbers (n_1, n_2), while *C* message is used to authenticate the reader. However if a match

doesn't occur, then the reader asks for old *IDS* from the tag.

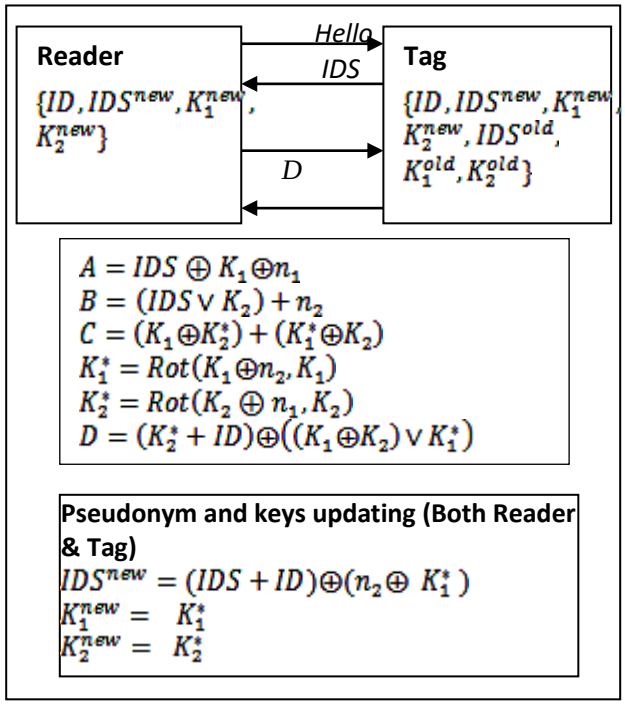

Fig.2 SASI Protocol

4. Tag extracts the pseudorandom numbers (n_1, n_2) from *A* and *B* messages respectively. The tag further computes the local value of *C* message. If the locally computed value of *C* matches with the received *C*, then the tag will perform two tasks:
   a) Updates its pseudonym (*IDS*) and keys (K_1, K_2).
   b) Computes and transmits message *D*.
5. After receiving *D* message, the reader computes a local value of *D* and if local value of *D* equals to the received *D*, only then the reader authenticates the tag. The reader also updates the pseudonym and keys for the particular tag.

4.2 Cryptanalysis of SASI Protocol

SASI protocol received numerous attacks (desynchronization attack, replay attack, traceability attack etc.) right after it was proposed. Hernandez Castro et al. [25] proposed first passive full disclosure attack on SASI protocol. Initially only $log_2[96]$ bits of the *ID* has been disclosed, however attack is extensible to retrieve $log_2[l–1]$. Least Significant Bits (LSB) of the *ID* after eavesdropping $\theta(l–1)$ authentication sessions. In 2011, Avoine et al. [39] also proposed a sequential passive full disclosure attack on SASI, but attack requires 2^{17} authentication sessions to disclose *l – bit* of the *ID*.

We have used RLC (Recursive Linear Cryptanalysis) and disclosed *l – bits* of tag's *ID* with almost 3/4 success probability. RLC is a formal structural cryptanalysis; which directly exploits the weak diffusion properties of the protocol messages and discloses the secrets bitwise. The basic working of RLC is as follows:

4.2.1 Recursive Linear Cryptanalysis (RLC)

In 2013, Zahra Ahmadian et al. [24] introduced a new passive and deterministic framework (Recursive Linear Cryptanalysis) for security analysis of ultralightweight RFID authentication protocols. In RLC, adversary constructs a system of linear equations and then solves these equations recursively for each particular secret. RLC mainly involves three steps: which are as follows:

i) Identify all unknown secret variables (*ID*, pseudorandom numbers and keys).

ii) Write equations in terms of i^{th} location for each i^{th} bit of the variables. We may use transitional variables such as carries (*Car*) and borrows (*Bar*) for modular additions and subtractions respectively for computation of equations.

iii) Solve these equations recursively to retrieve the desired secret variable, starting from LSB.

4.2.2 Recursive Linear Cryptanalysis of SASI protocol

Here we apply three stages of RLC on SASI protocol.

i) For a single authentication session, all the secret unknown variables are *ID*, K_1, K_2, n_1 and n_2.

ii) Each message in SASI protocol (*A, B, C, D* and IDS^{new}) provides linear equation which is sufficient in constructing a system of independent linear equations (as number of equations and number of unknown variables are same). Usually RLC requires only one protocol session for its execution; however for SASI we need at least two authentication sessions. Since, XOR and OR operations coincide with ¾ probability, so we have used this probabilistic analogy of both operations for construction of our equations. To elaborate this probabilistic analogy of logical operations, table 1 shows bitwise truth tables of XOR and OR operations.

Table 1 XOR Vs OR Operation

a	b	$a \oplus b$	$a \vee b$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1

Table 2 enlists the notations used in SASI attack. For bit $I = 0, \quad l - 1$ of the messages (*A, B, C, D* and IDS^{new}) we have:

$$A_i = IDS_i \oplus K_{1i} \oplus n_{1i} \tag{1}$$

Using probabilistic analogy of logical operations can be represented as:

$$B_i = IDS_i \oplus K_{2i} \oplus n_{2i} \oplus car1_i \tag{2}$$

$$C_i = (K_{1i} \oplus K_{2i}^*) + (K_{2i} \oplus K_{1i}^*) \tag{3}$$

Tianjie et al. [8] and Hernandez et al. [25] showed when *K mod n*= then $Rot(A \oplus K, A) = A \in$ hence:

$$Rot(K_2 \oplus X, K_2) = K_2 \oplus X;$$

When K_2 *mod* $n = 0$

$$K_{2i}^* = Rot(K_{2i} \oplus n_{1i}.K_{2i})$$

$$= K_{2i} \oplus n_{1i} \tag{4}$$

$$K_{1i}^* = Rot(K_{1i} \oplus n_{2i}, K_{1i}) = K_{1i} \oplus n_{2i} \tag{5}$$

Substituting (4) & (5) in (3):

$$C_i = (K_{1i} \oplus K_{2i} \oplus n_{1i} \oplus K_{2i} \oplus K_{1i} \oplus n_{2i} \oplus car2_i)$$

$$C_i = n_{1i} \oplus n_{2i} \oplus car2_i \tag{6}$$

Now, for next session adversary pretends to be valid reader and asks for IDS from the tag. The tag responds with *IDS*, adversary uses this information for computation of new equations for attack as follows:

$$IDS_{next\,i} = (IDS_i + ID_i) \oplus (n_{2i} \oplus K_{li}^*) \tag{7}$$

Substituting the value of K_{li}^* from (5) in (7)

$$IDS_{next\,i} = (IDS_i \oplus ID_i \oplus n_{2i} \oplus K_{1i} \oplus n_{2i} \oplus car3_i$$

$$IDS_{next\,i} = IDS_i \oplus ID_i K_{1i} \oplus car3 \tag{8}$$

Where;

$$car1_o = car2_o = ... = car8_o = 0$$

for $i = 1, \ldots, l-1.$

$$car1_i = Maj(IDS_{i-1} \oplus K_{2(i-1)}, n_{2(i-1)}, car1_{i-1})$$

$$car2_i = Maj(K_{1(i-1)} \oplus n_{1(i-1)}, K_{2(i-1)} \oplus K_{1(i-1)} \oplus n_{2(i-1)}, car2_{(i-1)})$$

$$car3_i = Maj(IDS_{i-1}, ID_{i-1}, car3_{i-1})$$

$$D_i = (K_{2i}^* + ID_i) \oplus (K_{1i} \oplus K_{2i})v \tag{9}$$

Substituting variables of (4) & (5) in (9):

$$D_i = K_{2i} \oplus n_{1i} \oplus ID_i \oplus K_{1i} \oplus K_{2i} \oplus K_{1i} \oplus n_{2i}$$

$$D_i = n_{1i} \oplus n_{2i} \oplus \tag{10}$$

iii) Variables of (1), (2), (6), (8) & (10) compute the system of linear equations with the following matrix depiction:

$$U \cdot \begin{bmatrix} K_{1i} \\ K_{2i} \\ n_{1i} \\ n_{2i} \\ ID_i \end{bmatrix} = v$$

Where,

$$U = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$v = \begin{pmatrix} A_i \oplus IDS_i \\ B_i \oplus IDS_i \oplus car1_i \\ C_i \oplus car2_i \\ IDS_{next\,i} \oplus IDS_i \oplus car3_i \\ D_i \end{pmatrix}$$

The above matrix is a non-singular matrix, in each step i ; one can easily extract all the concealed values one after another.

Table 2 Notations Used in SASI Attack (RLC)

Symbol	Definition
V	*OR* operation
·	*AND* operation
⊕	*XOR* operation
||	Concatenation
L	Length of all variables, l = 96.
+	Addition in *modulo – 2*
Maj	Majority function $Maj(a,b,c) = a,b \oplus a, c \oplus b,c$
Car	Carry function for modular additions $Z = X + Y (mod\,2^l) \Rightarrow X_i \oplus Y_i \oplus Car_i$ $Car_0 = 0,\ Car_i = Maj(X_{i-1}, Y_{i-1}, car_{i-1})$
Bar	Barrow function for modular subtraction $Z = X - Y (mod\,2^l) \Rightarrow X_i \oplus Y_i \oplus bar_i$ $bar_i = Y_{i-1} \oplus bar_{i-1} \oplus Maj(X_{i-1}, Y_{i-1}, bar_{i-1})$

4.3 Yeh et al. Protocol

In 2010, Yeh et al.[23] proposed a process oriented ultralightweight authentication protocol. The protocol is quite similar to SASI protocol except that the reader stores two copies of pseudonym and keys *(old and new)* instead of the tag.

In Yeh et al. protocol, each tag stores a unique *l – bit* identity *ID* and pre-shares its IDS and key (*K*) with the reader. Fig. 3 shows the specification of the Yeh et al. protocol.

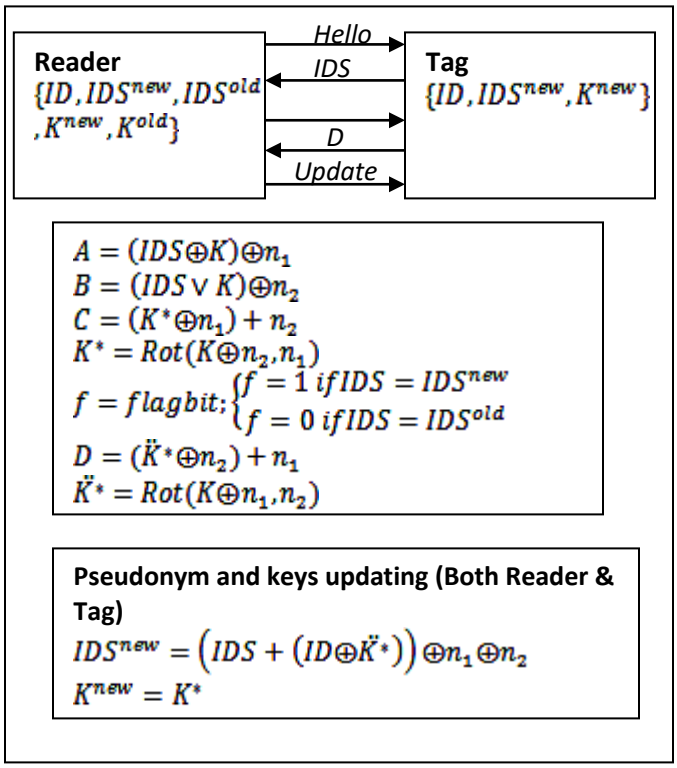

Fig. 3 Yeh et al. Protocol

The working of the protocol is as follows:

1. The reader sends *"Hello"* message towards the tag to initiate the protocol session.
2. The tag responds with its *IDS.*
3. After receiving *IDS*, the reader uses it as an index to search a matched entry in the database. If *IDS* = *IDS* ^{new}, then the reader generates two pseudorandom numbers (n_1, n_2), uses key *K* (K=K^{new}) to compute *A* || *B* || *C* messages and sets flag bit *f*=0. If *IDS* = *IDS* ^{new}, then the reader uses key *K*(*K*=*ID*) to compute *A* || *B* || *C* messages and sets flag bit *f* = 1

4. Upon receiving of $A \,||\, B \,||\, C \,||\, f$ message, the tag first checks the flag bit (f):.

$$\begin{cases} iff = 0 & K = K^{new} \\ iff = 1 & K = ID \end{cases}$$

5. Tag then performs two tasks:
   a) Extracts pseudorandom numbers (n_1, n_1) from A and B messages.
   b) Compute a local value of message C and compares it with received C. If both values equate, then the tag computes and transmits message D.
6. Reader computes a local value of message D and compares it with received D. If both values are equal then the reader updates its variables (IDS, K) and transmits an update command towards the tag.
7. Upon receiving the update command, the tag will also update its internal secrets (IDS, K).

4.4 Cryptanalysis of Yeh et al. Protocol

Yeh et al. protocol uses two pseudorandom numbers (n_1, n_2) to ensure the freshness of each authentication session. However, we analyze that in Yeh et al. protocol, there are some serious threats to the system [22] when two pseudorandom numbers have the same value *mod M* i.e.

$$n_1 \bmod M = n_2 \bmod M \tag{14}$$

We shall provide the guidelines for selection of optimal M later in this section. Assuming that equation (14) holds, we can then probabilistically (using analogy of *XOR* and *OR* operations) simplify the publically transmitted messages to disclose the concealed secrets as follows:

$$A = IDS \oplus K \oplus n_1 \tag{15}$$

$$B = (IDS \, v \, K) \oplus n_2 \tag{16}$$

By taking XOR between equation (15) & (16):

$$\begin{aligned} A \oplus B &= [IDS \oplus n_1] \oplus [(IDSvK) \oplus n_2] \\ &\cong n_1 \oplus n_2 \end{aligned} \tag{17}$$

For the next session, adversary pretends to be legitimate reader and asks for IDS from the tag. Upon receiving *"Hello"* message, tag will respond with IDS_{new}. The adversary then takes *XOR* between IDS_{new} and (17):

$$\begin{aligned} IDS_{new} \oplus (A \oplus B) &= [(IDS \\ &\quad + (ID \oplus K^*)) \oplus n_1 \oplus n_2][n_1 \oplus n_2] \\ &= IDS + (ID \oplus K^*) \end{aligned} \tag{18}$$

Where;

$$K^* = Rot(K \oplus n_1, n_2) = K \oplus n_1; K \bmod M = 0$$

So:

$$IDS_{new} \oplus (A \oplus B) = IDS+)ID \oplus K \oplus n_1) \tag{19}$$

Now, we have to verify the correctness of (17) for each session. Further, we use the same approximation in messages C and D to correlate the both conditions:

$$\begin{aligned} C \bmod L &\simeq (K^* \oplus n_1) \oplus n_2 \bmod M \\ &\simeq (K \oplus n_2 \oplus n_1 \oplus n_2) \simeq (K \oplus n_1) \end{aligned} \tag{20}$$

$$\begin{aligned} D \bmod L &\simeq (K^* \oplus n_2) \oplus n_1 \bmod M \\ &\cong K \oplus n_1 \oplus n_2 \oplus n_1 \cong K \oplus n_2 \end{aligned} \tag{21}$$

By taking XOR of equations (20) & (21)

$$C \oplus D - (K \oplus n_1) \oplus (K \oplus n_2) = n_1 \oplus n_2 \tag{22}$$

By comparing (17) and (22); we can probabilistically detect the condition that leads towards full disclosure of the concealed secrets.

We know if $IDS = IDS_{old}$ (means adversary has blocked the update command) then $K = ID$ & $f = 1$. Hence (20) can be simplified as follows:

$$IDS + (ID \oplus K \oplus n_1) = IDS + n_2 \tag{23}$$

From (23), we can retrieve n_1 which can be used further for computation of secret $ID_{Conjucture}$ of the tag. As if $f = 1$ then $K = ID$, so (16) can be simplified as follows:

$$ID = A \oplus IDS \oplus n_1 \tag{24}$$

Where *A* & *IDS* are publically known variables.

Hence, after validating the attack feasibility condition (comparison of (17) and (22)), we have to filter the results to obtain the maximum likelihood value of *UD*. We enlist the steps of the proposed attack below:

1. For $l = 0$ to M
2. Observations $[i] = 0$
3. Observe *IDS*, *A*, *B*, *C*, *D* and *f* (flag) messages of a valid authentication sessions to construct the system of probabilistic (quasi) equations.
4. Compare (17) and (22): if both equations do not coincide, then go to step number 3; otherwise go to the next step.
5. Allow both the reader and the tag to communicate and block the 'update command'.
6. Send a *"Hello"* message to obtain previously updated IDS_{new}.
7. Calculate the concealed conjecture secrets from (24) and (25).

The proposed attack is active and quasi linear, which is inspired from Norwegian attack [22]. Norwegian attack requires approximately 10^5 authentication sessions to retrieve the $ID_{conjecture}$, while our proposed attack model requires only 2^{13} authentication sessions to retrieve conjecture *ID*.

Fig. 4 presents the example of observations and results (histogram of $ID_{conjecture}$ candidates) for M=96 and N=2^{13} sessions. We can clearly observe a peak and correctly conjecture the targeted value ($ID_{conjecture}$ = 37) for the particular example. Although the attack can be run independently for any value of *M* it is highly recommended to select one which is a power of 2, in order to have a higher success probability.

The success probability of the attack mainly depends upon the number of eavesdropped sessions. Fig. 5 shows the success probability of the proposed attack for M = 96. We can observe from the figure that only 213 sessions are required to retrieve the IDConjecture with 3/4 probability.

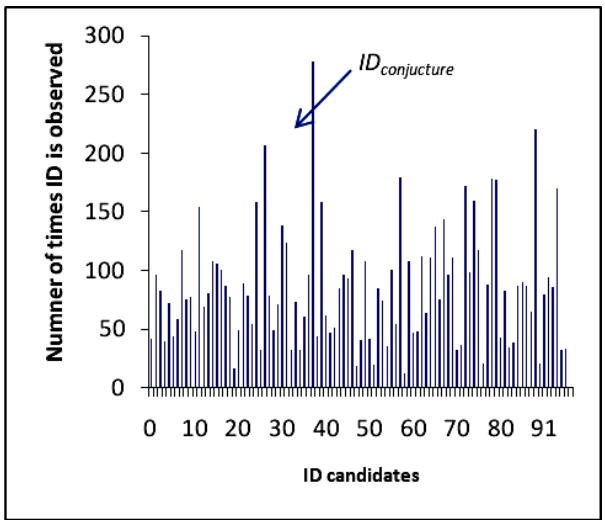

Fig. 4 Histogram of $ID_{conjecture}$ candidates (M = 96, N = 2^{13})

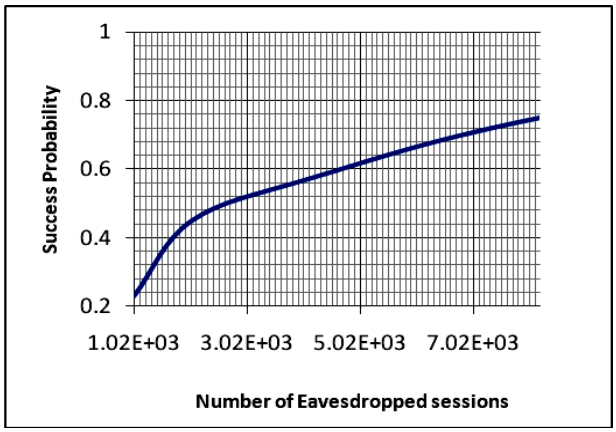

Fig. 5 Success Probability of the proposed attack (M = 96, N = 2^{13})

6. Conclusions

In this paper, we have highlighted that a good degree of randomness in publically exchanged messages doesn't guarantee the security countermeasures. We have firstly described the need of ultralightweight mutual authentication protocols for low cost passive RFID systems, and then we have proposed two full disclosure attacks on SASI and Yeh et al. ultralightweight mutual authentication protocols. We have used Recursive Linear Cryptanalysis (RLC) to analyze the security vulnerabilities of SASI protocol and for Yeh et al. protocol an active quasi linear cryptanalysis has been proposed; which discloses the secret ID of the tag

with 3/4 probability. The success probability of the attack can further be improved by increasing the number of eavesdropped sessions.

6. References

[1] Hung-Yu Chien," *SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity*", IEEE Transaction on Dependable and Secure Computing, Vol. 4, No. 4, pp. 337 – 340, 2007.

[2] Umar Mujahid, M. Najam-ul-Islam, and M. Ali Shami, *"RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash*," International Journal of Distributed Sensor Networks, vol. 2015, Article ID 642180, 8 pages, 2015. doi:10.1155/2015/642180

[3] Hung-Min Sun, Wei-Chih Tiang et al.,"*On the Security of Chein's Ultralightweight RFID Authentication Protocol*", IEEE Transactions on Dependable and Secure Computing, Vol.8, No.2, pp.315-317, 2011.

[4] Pedro Peris-Lopez, Julio Hernandez-Castro et al. "*LMAP: A real lightweight mutual authentication protocol for low-cost RFID tag*.", Proceedings of 2nd Workshop on RFID Security, Austria, pp.100-112, 2006.

[5] Tieyan Li et.al," *Security Analysis of family of Ultra-Lightweight RFID Authentication Protocols*", Journal of Software, Vol. 3, No. 3, pp. 1-10, 2008.

[6] Peris-Lopez, Pedro, Julio Cesar Hernandez et.al. "*EMAP: An efficient mutual-authentication protocol for low-cost RFID tags*.", The 1st International Workshop on Information security (OTM-2006), France, pp. 352-361, 2006.

[7] Peris-Lopez, J.C. Hernandez-Castro, J.M.E. Tapiador, A.Ribagorda,"M2AP: a minimalist mutual-authentication protocol for low cost RFID tags", International Conference on Ubiquitous Intelligence and Computing, pp.912-923, 2006.

[8] Tianjie, Elisa Bertin et al. "*Security analysis of the SASI protocol*", IEEE Transactions on Dependable and Secure Computing, Vol.6, No. 1, pp. 73 – 77, 2009.

[9] Peris-Lopez,Hernandez-Castro et al. "*Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protoco*l.", The 9th International Workshop on Information Security Applications, pp. 56-68, 2009.

[10] Yeh, Kuo-Hui, and N. W. Lo. "*Improvement of two lightweight RFID authentication protocol*s", Information Assurance and Security Letters Vol.1, No.1, pp 6-11, 2010.

[11] Bilal, Zeeshan, Ashraf Masood, and Firdous Kausar. "*Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol*", The 12th International Conference on Network-Based Information Systems, Indianapolis, USA, pp. 260-267, 2009.

[12] Muhammad Zubair, Umar Mujahid et.al," *Cryptanalysis of RFID Ultralightweight protocols and comparison between its solution approaches*", Bahria University Journal of information & communication technology (BUJICT), Vol.5, No. 1, pp. 58-63, 2012.

[13] David, Mathieu, and Neeli R. Prasad. "*Providing strong security and high privacy in low-cost RFID networks*", International conference on Security and privacy in mobile information and communication systems, Italy, pp.172-179, 2009.

[14] Barrero, David F.et.al. "*A genetic tango attack against the David–Prasad RFID ultra‐lightweight authentication protocol*", Expert Systems (Journal) Vol. 31, no. 1, pp. 9-19, 2014.

[15] Tian, Yun, Gongliang Chen, and Jianhua Li. "*A new ultralightweight RFID authentication protocol with permutation*", IEEE Communications Letters, Vol.16, no. 5, pp.702-705, 2012.

[16] Bagheri, Nasour, Masoumeh Safkhani et al. "*Cryptanalysis of RAPP, an RFID Authentication Protocol*", Cryptology ePrint

Archive, Report 2012/702, https://eprint.iacr.org/2012/702, 2012.

[17] Tingyuan, and Teng Zhang. "*A study of DES and Blowfish encryption algorithm.*", IEEE Region 10 Conference, TENCON-2009, Singapore, pp. 1-4, 2009.

[18] Engels, Daniel, et al. "*Hummingbird: ultra-lightweight cryptography for resource-constrained device.*" The 14th International Conference on Financial Cryptography and Data Security, Spain, pp.3-18, 2010.

[19] Boyeon song and Chris J. Mitchell. "*RFID authentication protocol for low-cost tags*" The 1st ACM conference on Wireless network security, USA, pp. 140-147, 2008.

[20] Rizomiliotis, Panagiotise et.al."*Security analysis of the Song-Mitchell authentication protocol for low-cost RFID tag.*", IEEE Communications Letters, Vol.13, No. 4, pp. 274-276, 2009.

[21] Peris-López," Lightweight Cryptography in Radio Frequency Identification (RFID) Systems", PhD thesis, UNIVERSIDAD CARLOS III DE MADRID, 2008.

[22] Pedro Peris-Lopez, et.al "*Quasi-linear cryptanalysis of a secure RFID ultralightweight authentication protocol* ", The 6th International Conference on Information Security and Cryptology, China, pp. 427-442, 2011.

[23] Yeh, Kuo-Hui, N. W. Lo, and Enrico Winata. "*An efficient ultralightweight authentication protocol for RFID systems*", Workshop on RFID Security and Privacy, Turkey, pp 49-60, 2010.

[24] Zahra Ahmadian, Mahmoud. et.al "*Recursive linear and differential cryptanalysis of ultralightweight authentication protocols*", IEEE Transactions on Information Forensics and Security, Vol.8. No.7, pp.1140–1151, 2013.

[25] Julio C. Hernandez. et.al "*Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations.*", ArXiv, Cryptography and Security, Report; 0811.4257, http://arxiv.org/abs/0811.4257, 2008.

[26] Avoine, Gildas, Xavier Carpent, and Benjamin Martin. "*Privacy-friendly synchronized ultralightweight authentication protocols in the storm*", Journal of Network and Computer Applications, Vol.35, No. 2, pp. 826-843, 2012.

[27] A. Klimov and A. Shamir. "*New Applications of T-functions in Block Ciphers and hash functions"*. Proc. of FSE'05, LNCS vol. 3557, pp. 18–31. Springer-Verlag,2005.

[28] Xu Zhuang, Yan Zhu and Chin-Chen Chang," *A New Ultralightweight RFID Protocol for Low-Cost Tags: R^{2}AP"*, Wireless Personal Communications, Vol. 79, No.3, pp 1787-1802, 2014.

[29] Zeeshan Bilal, Keith Martin and Qasim Saeed, "*Multiple Attacks on Authentication Protocols for Low-Cost RFID Tags*", Applied Mathematics & Information Sciences, Vol.9, No.2, pp-561-569, 2015.

[30] Soo Jeon and Eun-Jun Yoon," *Cryptanalysis and Improvement of a New Ultra-lightweight RFID Authentication Protocol with Permutation*" Applied Mathematical Sciences, Vol. 7, 2013, No. 69, pp. 3433 – 3444, 2013.

[31] Umar Mujahid, M.Najam-ul-Islam," *Ultralightweight Cryptography for Passive RFID systems*", International Journal of Communication Networks and Information Security, Vol.6, No.3, pp.173-181, 2014.

[32] Zahra Ahmadian, Mahmoud Salmasizadeh and Mohammad Reza Aref, "*Desynchronization attack on RAPP ultralightweight authentication protocol.*" Information processing letters, Vol.113, No.7, pp. 205-209, 2013.

[33] G. Marsaglia and W.W. Tsang. "*Some difficult-to-pass tests of randomness*", Journal of Statistical Software, Vol. 7, No. 3, pp.37–51, 2002.

[34] J. Walker. ENT Randomness Test. http://www.fourmilab.ch/random/, 1998.

[35] C. Suresh, Charanjit J., J.R. Rao, and P. Rohatgi,"*A cautionary note regarding*

evaluation of AES candidates on smart-cards". In Second Advanced Encryption Standard (AES) Candidate Conference, 1999.

[36] Lee. Y.C., Hsieh.Y.C., et al.,"*A new ultralightweight RFID authentication protocol with mutual authentication* ", International Conference on Information Engineering, Vol. 1, pp.55-61, 2009.

[37] Peris-Lopez, Hernandez Castro, J.C., Tapiador and Van der Lubbe," *Security flaws in a recent ultralightweight RFID authentication protocol*", Workshop on RFID security- RFIDSec Asia'10, Singapore, 2010.

[38] Wang, S., Han, Z., Lui, S. and chen,D," *Security analysis of RAPP: an RFID authentication protocol based on permutation*", Cryptology ePrint Archive, Report 2012/327.

[39] Gildas Avoine, Xavier Carpent and Benjamin Martin," *Strong Authentication and Strong Integrity (SASI) is not that strong",* RFID Security and Privacy Issues, LNCS, Vol.6370, pp-50-64, 2010.

[40] Li. T and Wang.G, "*Security analysis of two ultralightweight RFID authentication protocols*" The second information security conference, Sandton, Ganteng, South Africa, 2007.