CRYPTANALYSIS OF TWO ULTRALIGHTWEIGHT MUTUAL AUTHENTICATION PROTOCOLS

Umar Mujahid[1], M.Najam-ul-Islam[1], Qurat-Ul-Ain[1], Rizwan Aamir[2], Muhammad Muzamal[2]
[1]Department of Electrical Engineering, Bahria University Islamabad, Pakistan
[2]Department of Computer Science, Bahria University Islamabad, Pakistan

***ASTRACT**: RFID (Radio Frequency Identification) is one of the most growing technologies in the field of ubiquitous computing. Unique and automatic identification capabilities make RFID systems more prominent than its contended identification schemes. However, RFID systems incorporate wireless channel so there are some allied security risks and apprehensions to the system from malicious adversaries. Numerous ultralightweight authentication protocols have already been proposed to ensure the security of RFID systems in cost effective manner. In this paper, we have performed cryptanalysis of two Ultralightweight Mutual Authentication Protocols (UMAPs): EMAP and R^{2}AP. For EMAP, we propose full disclosure attack and retrieve its concealed secret ID with $\frac{3}{4}$ success rate. For R^{2}AP, we have identified simple traceability and DoS attacks. In order to improve the functionalities of these protocols, we have also suggested some patches for their designs. The performance analysis shows that the (proposed) additional patches in protocol designs do not incorporate intensive operators and successfully conform within EPCC1G2 standard.*

Index Terms— RFID, UMAPs, EMAP, R^{2}AP, Cryptanalysis

I. INTRODUCTION

The last few years have seen the rapid developments and diversifications of designs in the monarchy of pervasive systems. Although, Barcode is leading identification scheme of present era, however the RFID is rapidly capturing the marketplace of barcode in many applications because of its enormous features and functional haste. The RFID systems have two dominant advantages over barcode scheme: unique identification and automation. The barcode schemes mainly identify only the type of the objects while the RFID systems uniquely identify each object among its homogenous set (objects). Moreover, the non-line of sight capability of RFID systems automates the identification process. This automated identification process saves time and resolves the issues of long ques at the billing counters of grocery stores.

The RFID systems mainly comprise of three components: tag, reader and backend database. A tag (electronic chip) acts as transponder and attached to the objects which need to be identified. The reader acts as interrogator and it interacts with all such tags which enter in its vicinity. In addition to querying, the reader also provides power to charge up the passive tags. A backend database manages all the readers and stores the data (information) of all associated readers and the tags.

Since the RFID technology is pervasive, so the privacy and security are the two important aspects which need more attention while designing of such systems. Most of the security and privacy concerns in RFID systems arise because the use of wireless channel for interaction with the tags (which is open for all types of adversaries). The RFID security is becoming very important research area these days as evidenced by the great number of research during last decade (over 1000) [35]. The overall cost of the system has a significant impact in selection and designing of cryptographical solutions for such pervasive systems. From theoretical perspective, it seems that the standard cryptographical solutions (such as AES, ECC etc.) are better approach to address the security issues of RFID systems. However these typical solutions demand more resources in terms of circuitry, memory and power consumption which cannot be afforded by the low cost resources constraint devices. Hence, a new field ultralightweight cryptography has been introduced to ensure the security of low cost RFID tags in recent years. Ultralightweight cryptography avoids the use of costly operations and supports only simple T-functions and some special purpose ultralightweight primitives for security.

After the official release of EPC Class – 1 Generation – 2 standard (targeting the passive low cost tags) [36], many researchers started working on development of lightweight cryptographical solutions to ensure the security and privacy of EPC C1G2 passive tags. In 2003, Vajda et al. [37] proposed the first lightweight security protocol for pervasive systems. In 2006, Peris Lopez et al. [3–5] formally laid down the foundations of extremely lightweight cryptographical solutions for passive low cost RFID systems. Although the security protocols proposed by Peris et al. falls within the scope of ultralightweight cryptography but Chien [1] formally propose the name ultralightweight cryptography for extremely lightweight cryptographical solutions. Afterwards many other Ultralightweight Mutual Authentication Protocols (UMAPs) [1-9, 25, 34] have been proposed but almost all protocols proposed within the framework of EPC C1G2 fall short of the security objectives. Most of the UMAPs are broken within one year (after its introduction). There are two main reasons which shorten the life span of an ultralightweight authentication protocol: Incorporation of weak primitives (similar mistakes) and poor security analysis model.

In this paper, we perform cryptanalysis of two state of the art UMAPs: EMAP [3] and R^{2}AP [5]. We use two-set cryptanalysis to fully disclose secret ID of EMAP. For R^{2}AP, we highlight two simple but effective attacks (DoS and Traceability) and challenge its security claims.

The rest of the paper is organized as follows: Section II details the related work, followed by the description of EMAP and R^{2}AP Ultralightweight Mutual Authentication Protocols (UMAPs) in section III. Section IV and Section V present the cryptanalysis of the both UMAPs and patches for improvement in UMAP designs respectively. Finally, section VI concludes the paper.

II. RELATED WORK

In 2006, Pedro *et al*. [2-4] proposed three Ultralightweight Mutual Authentication Protocols (UMAP family): LMAP, M2AP and EMAP to secure low cost RFID systems. All the three protocols involve simple bitwise logical operations (such as AND, XOR and OR operations) in their designs and avoid traditional cryptographic primitives to reduce the cost of overall cryptographic processor. The authors of UMAP family protocols considered only simple cryptanalysis scenarios to evaluate the security robustness of the protocols against various attack models. Therefore in 2007, Tieyan Li et al. [21, 29, 33] highlighted the pitfalls of UMAP family protocols and proposed multiple desynchronization and full disclosure attacks. They also reported that the combinations of T-functions return another T-function and hence are cryptographically insecure.

Chein [1] improved the designs of ultralightweight protocols and introduced non-triangular primitives in UMAP designs to avoid previously highlighted attacks. The author proposed a new ultralightweight non-triangular primitive "*Rot*" (hamming weight based cyclic left rotation function) and presented a new UMAP to ensure Strong Authentication and Strong Integrity (SASI) using Rotation function. However after one year (2008) of SASI's introduction, it received many attacks including desynchronization [11], traceability [13] and full disclosure [10]. The highlighted attacks raised the question mark on the security claims of the SASI protocol.

In 2008, Peris et al. [8] improved its previous work and used Chein's concept of assimilation of non-triangular primitives in UMAP designs. They introduced a new ultralightweight primitive "MixBits" and proposed a new UMAP: GOASSMER. Although, the GOASSMER protocol provides optimal security but authors have not clarified the hardware requirements of the "MixBits" operator. In 2009, Zeeshan et al. [19] highlighted the weakness in the structure of the GOASSMER protocol and proposed multiple Denial of Service (DoS) attacks. The authors also suggested some additional patches to make GAOSSMER protocol robust against highlighted attacks.

Later David-Prasad [6], Yeh et al. [7] and RAPP [5] protocols were also reported to be vulnerable against various desynchronization, traceability, DoS and full disclosure attacks.

In 2014, Zhuang et al. [34] proposed a Reconstruction based ultralightweight authentication protocol: R^{2}AP. The inclusion of new non-triangular primitive (Reconstruction) makes protocol more resistive against many of the previous full disclosure and desynchronization attacks. However, in this paper we have reported two attacks (traceability and DoS attacks) on R^{2}AP.

In 2015, Umar Mujahid et al. [25] introduced a new hybrid ultralightweight primitive (Recursive hash) and proposed a security protocol to provide Robust Confidentiality, Integrity and Authentication (RCIA). To the best of our knowledge, the RCIA is the most robust and considerably secure UMAP as compare to its contended protocols since none of the attack on RCIA is highlighted to date. However authors have not clarified whether the Recursive hash function falls within the domain of ultralightweight class or not.

From literature presented above, we can observe that the most of the UMAPs are broken within one year (after its introduction). The main reason that shortens the life span of an ultralightweight authentication protocol is that the most of the authors/inventors carry forward the similar mistakes or incorporate weak primitives while designing of UMAPs. Hence the robust and comprehensive security analysis model is the only way to improve UMAP designs.

III. ULTRALIGHTWEIGHT MUTUAL AUTHENTICATION PROTOCOLS

In this section, we describe the basic working of two state of the art UMAPs: EMAP and R^{2}AP. The description of these UMAPs is presented as follows:

A. EMAP

EMAP (Efficient Mutual Authentication Protocol) is one of the pioneer proposals of the UMAP family. The working principles, memory requirements and internal operations of the protocol are quite similar to its preceding protocols [2 - 3]. However in EMAP, Pedro et al. [3] introduced the concept of parity bit F_P: which is defined as a vector built from the parity bits of input (4-bit block). To reduce the computational cost of the tag, EMAP doesn't use modular addition and supports only XOR, AND & OR logical operations at the tag's side.

○ *The Protocol*

Figure-1 shows the basic working of the protocol. The protocol mainly involves following steps:

- **Step – 1**

The reader initiates the protocol by transmitting the "*Hello*" message to the tag.

- **Step – 2**

Upon receiving the reader's query, the tag responds with its current IDS.

- **Step – 3**

The reader initially identifies the tag, if the reader successfully found a match of IDS in its database:

➢ Then the reader generates two pseudorandom numbers (n_1, n_2) and conceals them within messages A, B and C in the following manner:

$$A = IDS \oplus K_1 \oplus n_1 \quad (1)$$

$$B = (IDS \vee K_2) \oplus n_1 \quad (2)$$

$$C = (IDS \oplus K_3) \oplus n_2 \quad (3)$$

➢ Reader ⟶ Tag: $A \parallel B \parallel C$

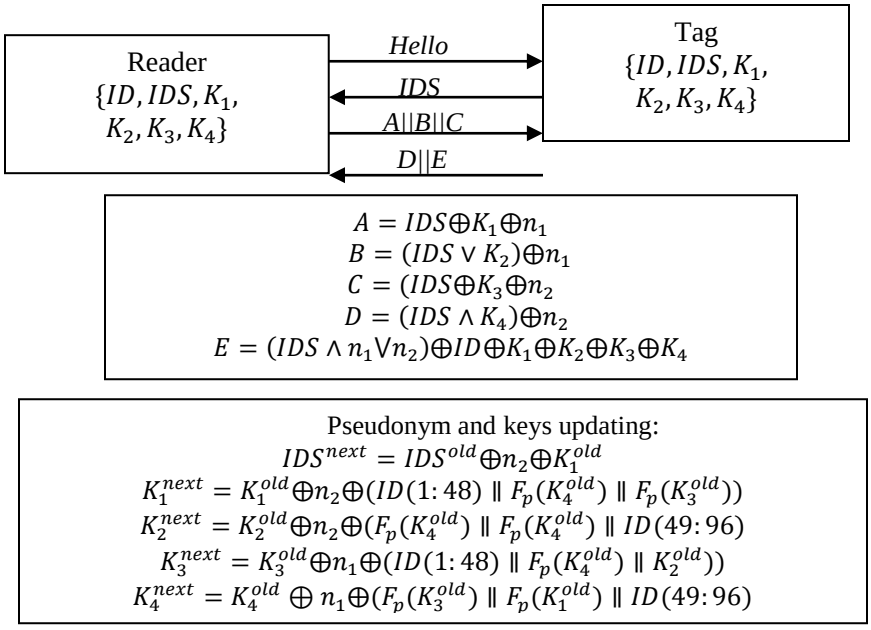

Figure 1: EMAP Protocol

- **Step – 4**

On receiving of $A \| B \| C$ messages, the tag performs following tasks:

- Extracts the pseudorandom number (n_1) from message A:

$$n_1 = A \oplus IDS \oplus K_1 \quad (4)$$

- Uses n_1 to compute a local value of message B:

$$B' = (IDS \vee K_2) \oplus n_1 \quad (5)$$

- Authenticates the reader as follows:

If $B = B'$

the reader is successfully authenticated

else

Protocol is aborted

end if

- After successful authentication of the reader, the tag extracts the pseudorandom number (n_2) from message C:

$$n_2 = C \oplus IDS \oplus K_3$$

- The tag then computes D& E messages:

$$D = (IDS \wedge K_4) \oplus n_2 \quad (6)$$

$$E = (IDS \wedge n_1 \vee n_2) \oplus ID \oplus K_1 \oplus K_2 \oplus K_3 \oplus K_4 \quad (7)$$

- Tag ⟶ Reader: $D \| E$
- The tag updates its pseudonyms and Keys:

$$IDS^{next} = IDS^{old} \oplus n_2 \oplus K_1^{old} \quad (8)$$

$$K_1^{next} = K_1^{old} \oplus n_2 \oplus (ID(1:48) \| F_p(K_4^{old}) \| F_p(K_3^{old})) \quad (9)$$
$$K_2^{next} = K_2^{old} \oplus n_2 \oplus (F_p(K_4^{old}) \| F_p(K_4^{old}) \| ID(49:96) \quad (10)$$
$$K_3^{next} = K_3^{old} \oplus n_1 \oplus (ID(1:48) \| F_p(K_4^{old}) \| K_2^{old})) \quad (11)$$
$$K_4^{next} = K_4^{old} \oplus n_1 \oplus (F_p(K_3^{old}) \| F_p(K_1^{old}) \| ID(49:96) \quad (12)$$

After receiving the $D \| E$ messages, the reader computes the local version of the $D \| E$ messages:

$$D' = (IDS \wedge K_4) \oplus n_2$$
$$E' = (IDS \wedge n_1 \vee n_2) \oplus ID \oplus K_1 \oplus K_2 \oplus K_3 \oplus K_4$$

- Then the reader authenticates the tag in following manner:

If $D = D'$ & $E = E'$

the tag is successfully authenticated

else

Protocol is aborted

end if

- On successful authentication of the tag, the reader uses equations (8 – 12) to update the index – pseudonym (IDS) and keys in its database for future correspondence with the particular tag.

B. R^2AP

Zhuang et al. [34] proposed Reconstruction based RFID Authentication Protocol (R^2AP) in 2014. The inclusion of newly proposed Reconstruction function in protocol design makes hamming weight (hw) unpredictable and resolved many security issues highlighted in previous UMAPs. The definition of the Reconstruction function is as follows:

Assume X and Y are two l −bit strings:

$$X = x_{l-1}x_{l-2} \dots x_0 \quad x_i \in \{0,1\}. \quad i = 0,1, \dots, l-1$$
$$Y = y_{l-1}y_{l-2} \dots y_0 \quad y_i \in \{0,1\}. \quad i = 0,1, \dots, l-1$$

Then Reconstruction of X with Y is:

$Rec(X,Y) = z_{l-1}z_{l-2} \dots z_0$, $z_i = F(x_i, y_i)$,

Where

$$F(x_i, y_i) = \begin{cases} x_{i-1} mod\ l, & x_i > y_i \\ y_{i-1} mod\ l, & x_i < y_i \\ x_i, & x_i = y_i \end{cases}$$

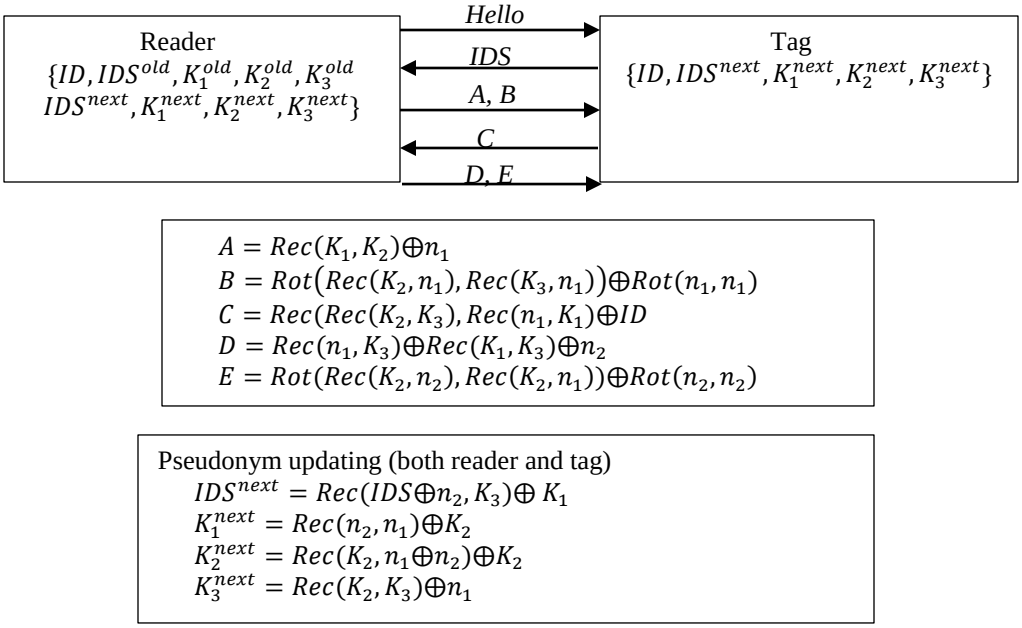

Figure 2: R²AP Protocol

Moreover, to overcome desynchronization attacks, they have adopted denial of old IDS approach. In this approach, the reader stores two copies of the tag's variables (old and new) including pseudorandom numbers $(ID, IDS, K_1, K_2, K_3, IDS^{old}, K_1^{old}, K_2^{old}, K_3^{old})$ while the tag stores only current (updated) variables (ID, IDS, K_1, K_2, K_3) . Upon receiving of old IDS, the reader uses the previous values to compute messages and hence get the same response from tag (previous session) because they use same (previous) pseudorandom numbers. Then the reader rejects the service request of the tag and completes its remaining protocol session to make the tag synchronized. So the next time, the tag will be able to send the IDS^{next}.

- *The Protocol*

Figure 2 shows the basic working of the protocol. The protocol mainly involves the following steps:

- **Step – 1**
  The reader sends a *hello* message towards the tag to initialize a new protocol session.
- **Step – 2**
  Upon receiving of reader's query, the tag responds with its IDS.
- **Step – 3**
  After receiving IDS, the reader uses it as an index to search for a matched entry in its database. If a match does not occur then the reader terminate the protocol session with the particular tag else the reader performs following task:
  - Generates a pseudorandom number (n_1) and computes A and B messages:
  -

$$A = Rec(K_1, K_2) \oplus n_1 \quad (13)$$

$$B = Rot(Rec(K_2, n_1), Rec(K_3, n_1)) \oplus Rot(n_1, n_1) \quad (14)$$

  - Reader ⟶ Tag : A, B
- **Step – 4**
  On receiving of messages (A, B), the tag performs followings:
  - Extracts pseudorandom number $(n_1)$from message A:

$$n_1 = A \oplus Rec(K_1, K_2)$$

  - Computes the local value of message B, B':

$$B' = Rot(Rec(K_2, n_1), Rec(K_3, n_1)) \oplus Rot(n_1, n_1)$$

  - The tag authenticates the reader as follows:
    If $B = B'$
    then the reader is authenticated successfully
    else
    protocol is aborted
    end if
  - The tag computes the message C:
    $C = Rec(Rec(K_2, K_3), Rec(n_1, K_1) \oplus ID$
  - Tag ⟶ Reader: C
- **Step – 5**
  Obtaining message C, the reader computes message local value of message C, C':
  $C' = Rec(Rec(K_2, K_3), Rec(n_1, K_1) \oplus ID$
  - The reader authenticates the tag as follows:
    If $C = C'$
    then the reader is authenticated successfully
    else

protocol is aborted
end if

- Further the reader computes the messages D, E:

$$D = Rec(n_1, K_3) \oplus Rec(K_1, K_3) \oplus n_2$$

$$E = Rot(Rec(K_2, n_2), Rec(K_2, n_1)) \oplus Rot(n_2, n_2)$$

- Reader ⟶ Tag: D, E
- The reader also updates the pseudonym (IDS) and keys (K_1, K_2, K_3) for future correspondence with the tag:

$$IDS^{next} = Rec(IDS \oplus n_2, K_3) \oplus K_1 \quad (16)$$

$$K_1^{next} = Rec(n_2, n_1) \oplus K_2 \quad (17)$$

$$K_2^{next} = Rec(K_2, n_1 \oplus n_2) \oplus K_2 \quad (18)$$

$$K_3^{next} = Rec(K_2, K_3) \oplus n_1 \quad (19)$$

- **Step – 6**

Upon receiving of messages (D, E) the tag extracts the pseudorandom number (n_2) from message D and computes the local value of message E, E':

$$n_2 = D \oplus Rec(n_1, K_3) \oplus Rec(K_1, K_3) \qquad E' = Rot(Rec(K_2, n_2), Rec(K_2, n_1)) \oplus Rot(n_2, n_2)$$

- The tag authenticates the reader as follows:
  If $E = E'$
  the reader is authenticated successfully
  else
  protocol is aborted
  end if
- After successful authentication of the reader the tag uses equations $(16 - 19)$ and updates its pseudonym keys.

IV. CRYPTANALYSIS OF UMAPS

In this section, we perform cryptanalysis of the two ultralightweight mutual authentication protocols (EMAP, and R^2AP) discussed in the section 3. We have proposed full disclosure attacks on EMAP using two set approach. For R^2AP, we have identified two simple traceability and Denial of Service (DoS) attacks. The proposed attacks are described as follows:

A. Cryptanalysis of EMAP

Initially, Tieyan Li and Deng [33] proposed the first full disclosure attack on EMAP which involves complex mathematical computations and requires $n + 1$ authentication sessions with four stages. We simplify their full disclosure attack model and fully disclose the secrets (including secret ID) within only two stages of much easier mathematical computations. Our proposed attack requires only two authentication sessions with the tag with 75% success probability.

- *Attack Description*

Since in EMAP, the tag is considered to be stateless, so we can repeatedly inquire (run sessions) the tag as many times as necessitate. The attack presented here takes the advantage of this weakness of EMAP and retrieve the concealed secrets. The attack involves two stages:

Stage – 1: The main objective of stage – 1 is to derive the pseudorandom number n_2. Initially, an adversary impersonates as an reader and the tag further it also intercepts communication messages $(IDS, A \parallel B \parallel C,\ D \parallel E)$ that are exchanged between legitimate pair of reader and the tag. Now as we know (from equation 6) message, $D = (IDS \wedge K_4) \oplus n_2$, where IDS and D are publically known variables, the attacker can disclose some of bits of n_2 by using two set approach [33] on the particular message. Specifically let $'\theta'$ be the set of bit positions in which corresponding bit values in IDS are 0 and similarly $'\emptyset'$ be the set of bit positions in which corresponding bit values in IDS are 1. Therefore, we have $\theta = \{i | [IDS]_i = 0, \forall\, i \in \{0,1,2, \ldots\ 95\}$ and $\emptyset = \{j | [IDS]_j = 1, \forall\, j \in \{0,1,2, \ldots\ 95\}$. From equation 6, we can easily derive the one half of the n_2:

$$\{D\}_i = [n_2]_i \qquad i \in \theta$$

$$\{D\}_j = [K_4]_j \oplus [n_2]_j \quad j \in \emptyset$$

Similarly, $[n_1]_j$ can be can be derived in the same way from equation 5, since $[B]_j = [\overline{n_1}]_j$.

Now, for the computation of the remaining bits of n_2 ($\emptyset$ set), the adversary toggles the multiple bits of n_1. This can be done by sending the toggled messages $A' \parallel B' \parallel C$ towards the tag and records its response $D \parallel E'$, where A' is toggled as $[A']_\emptyset = [A]_\emptyset \oplus [I]_\emptyset$ and B' is set as $[B']_\emptyset = [B]_\emptyset \oplus [I]_\emptyset$. Since the tag receives n_1' and n_2, that is why it responds with $D \parallel E'$. At this stage, adversary has both the toggled and previous (correct) values of message E (E' and E(previous session)), where the results of E' will be quite different from actual E. Let $result_1 = (IDS \wedge n_1 \vee n_2)$ and (toggled) $result_2 = (IDS \wedge n_1' \vee n_2)$ then if $\{n_2\}_j = 0$ $(j \in \emptyset)$, the toggle operation on $\{n_1\}_j$ also toggles $result_1$ (therefore E_j too). Else if $\{n_2\}_j = 1$ $(j \in \emptyset)$, then toggle operation on $\{n_1\}_j$ does not change the results. Hence bitwise comparison of $result_1$ and $result_2$ or in other words E'_j and E_j derive the bitwise $\{n_2\}_j$ as $\{n_2\}_j = \{0 | [E']_j \neq [E]_j\}, \{n_2\}_j = \{1 | [E']_j = [E]_j\}$. Finally, at this stage we have the complete value of n_2.

Stage – 2: After successful computation of conjecture pseudorandom number n_2, the attacker inquires the tag one more time to retrieve other secrets. Upon receiving of reader's (attacker) query the tag responds with its IDS^{next} (see equation 8). The adversary can easily compute (key) K_1:

$$K_1^{old} = IDS^{next} \oplus IDS^{old} \oplus n_2 \quad (20)$$

The adversary uses the value of K_1^{old} from equation 13 and substitute in equation 3 to compute n_1:

$$n_1 = A \oplus IDS \oplus K_1 \quad (21)$$

Similarly by substituting the value of n_1 in equation 4 computes the K_2:

$$K_2 = B \oplus n_1 \oplus IDS \quad (22)$$

Here for simplicity, we have equated XOR and OR operations, since both operations give identical results with 75% probability.

The value of n_2 further computes the K_3 and K_4:

$$K_3 = C \oplus IDS \oplus n_2 \quad (23)$$

For computation of K_4 , again we use two set approach and by bitwise comparison of E (but now toggling should start from LSB) derives K_4.

Finally, substituting all the conjecture secrets in equation 7 (section-3) computes the secret ID of the tag:

$$ID = (IDS \wedge n_1 \vee n_2) \oplus E \oplus K_1 \oplus K_2 \oplus K_3 \oplus K_4 \quad (24)$$

The overall success probability of the attack is 75%, (which can be improved further by trade – off between success rate and computation time).

B. Cryptanalysis of R²AP Protocol

For R²AP, we have identified two attacks: Traceability and DoS attack. The detailed description of both attacks is as follows:

- *Traceability attack*

Although the R²AP protocol avoids many existing adversarial attacks but the alternative approach for avoidance of desynchronization attacks enforces the both parties (reader and tag) to compute the previously transmitted messages repeatedly. The repetition of same messages opens the horizons for several traceability, replay and Denial of Service (DoS) attacks. For example, if an adversary blocks the messages D and E then the reader updates its pseudonym and keys while the tag keeps the previous values of its pseudonym and keys. Hence by repeatedly blocking $D$and E messages, the adversary can easily identify and track the movement of the tag (because each time the adversary will get the same messages (A, B, C, D and E). The only way to avoid such traceability attacks is to have new pseudorandom number for each new authentication session (The inclusion of new pseudorandom numbers ensures the freshness and anonymity of the messages).

- *Denial of Service attack (DoS)*

In this attack, the adversary sends the "*Hello*" message towards the tag and the tag responds with its IDS. Then attacker randomly generates and sends the messages A and B. The tag extracts n_1 from message A and computes message B to check the correctness of messages. This involves XOR, rotation and reconstructions operations; which incorporates (ALU) excessive computation and registers to store the intermediate values. Now the adversary engages the tag in this computation by repeatedly (with high frequency) sending the random messages to exhaust the tag as shown in the following fig.7. This will finally lead towards the denial of service attack since the tag cannot then communicate with the valid reader during this attack.

This attack can also be extended to exhaust the valid reader as well. In that scenario, attacker pretends to be a valid tag and sends random string of IDS with high frequency. On receiving of invalid 'IDS', the reader will keep on requesting for the older IDS values. And because of high frequency, it will not able to communicate with the valid tags. The concept of the attack is shown in the following fig.8.

The presented attack scenario is applicable to almost all of the previously proposed UMAPs [1-9,25, 38].

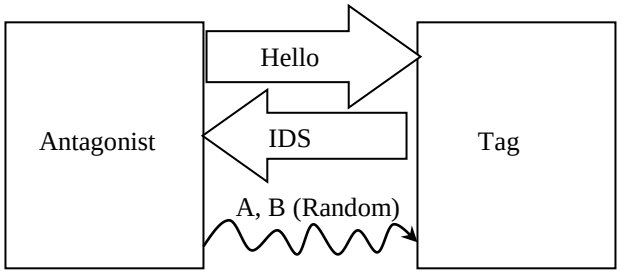

Figure 7: DoS attack towards Tag

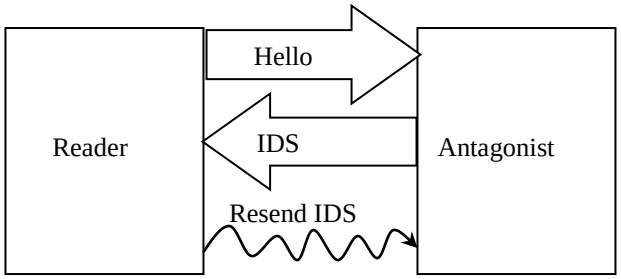

Figure 8: DoS attack towards the reader

V. PATCHES FOR UMAPS

Most of the UMAP developers assume that the avoidance of memory exhaustive DoS attacks is beyond the scope and capabilities of UMAPs. However we can avoid such memory exhaustive DoS attacks by integrating a simple message counter on both sides (reader and the tag). For example in R²AP protocol, the counter based methodology works as follows (assuming that the both parties (reader and the tag) store the values of previous pseudonym and keys):

Two message counters $\mathcal{C}_1$, and $\mathcal{C}_2$ are implanted at the reader and the tag side respectively. The counter ($\mathcal{C}_1$) is basically associated to each particular tag associated with RFID system. After sending "*Hello*" message towards the tag, the reader increments the counter, $\mathcal{C}_1 = 1$. Upon receiving reader's query, the tag responds with its current IDS and increments the counter, $\mathcal{C}_2 = 1$. Now after identifying the tag's IDS, the reader computes and transmits messages $A \parallel B$ towards the tag. The reader also increments the counter, $\mathcal{C}_1 = 2$. Further on successful authentication of the reader, the tag computes and transmits the message C towards the reader. On receiving of message C, the reader computes and transmits messages D and E. The tag also increment the counter, $\mathcal{C}_2 = 2$. The tag also resets the counter, $\mathcal{C}_2 = 0$. The threshold values for both counters are set to $\mathcal{C}_1 \leq 5$ and $\mathcal{C}_2 \leq 2$ and if the counter exceeds its threshold value then the associated device (reader or tag) detects the presence of adversary (DoS attack) and will stop functionality for some particular time. The assigned threshold values for the counters $\mathcal{C}_1 \leq 4$ and $\mathcal{C}_2 \leq 2$ allow only one interruption during the authentication session.

Let's exemplify the statement with the assumption of interruption of messages D and E. If the tag doesn't receive the messages D and E, it will not update its pseudonym and keys while the tag will update its local variables (assuming that reader has received message C). The tag will not reset the

counter C_1(associated with the particular reader) and next time if the same reader interacts with the same tag then counter, C_1 will start from the same value. Now we assume that if the same reader interacts with the same tag then after sending the "*Hello*" message, if the reader receives such IDS which is not present in the database then it will not increment any counter. The reader will send another "*Hello*" message towards the tag and if it receives the old IDS value then it increments the counter $C_1 = 3$. The tag also increments counter $C_2 = 2$. After sending the messages C, the reader further increments the counter $C_1 = 4$. The tag also resets the counter $C_2 = 0$ and sends the message $D||E$ towards the reader. Now next time, if an adversary tries to block message $D||E$ then this will be detected and both devices will stop their functionalities for some particular time.

Moreover the traceability attacks can only be avoided if the tag and the reader both stores the two copies of the *IDS* and Keys . For each new authentication session, the reader and the tag can communicate with new pseudonyms and keys (because of inclusion of new pseudo random number each time).

For improvement in EMAP and SASI protocol, we have to rephrase all the equation and involve some better non – triangular functions such as Recursive hash, MixBits and Reconstruction etc.

The proposed patches don't involve intensive computational operations and either use only protocol defined operators and 4-bit counter. Hence the protocols fall well within ultralightweight class.

VI. CONCLUSION

Security and privacy are two major concerns of RFID base identification systems, which are associated tag's cost. Because of limited computational capabilities only T-function based UMAPs can be used to ensure the security of such low cost systems. In this paper we have cryptanalyzed two UMAPs: EMAP, and R^2AP protocols. For EMAP protocol, we have presented a full disclosure attack, which requires only two authentication session to fully disclose the secret ID. The Success probability of the attack is $\frac{3}{4}$. For R^2AP, we took advantage of its poor structure design and proposed traceability and DoS attack on the protocol. Finally, we suggested some patches to avoid the all possible attacks including proposed ones.

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

[3] 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.

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

[5] 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.

[6] 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, pp172-179, 2009.

[7] Yeh, Kuo-Hui t.al."An efficient ultralightweight authentication protocol for RFID systems."Workshop on RFID Security and Privacy, Turkey, pp 49-60, 2010.

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

[9] Soo.Jeon et.al," A New Ultra-lightweight RFID Authentication Protocol Using Merge and Separation Operations", Int. Journal of Math. Analysis, Vol. 7, No. 52,pp 2583 – 2593, 2013.

[10] Avoine, Gildas, Xavier Carpent, and Benjamin Martin. "Strong authentication and strong integrity (SASI) is not that strong." Workshop on RFID Security and Privacy, Turkey, pp.50-64, 2010.

[11] Sun, Hung-Min, Wei-Chih Ting, and King-Hang Wang. "On the Security of Chien's Ultralightweight RFID Authentication Protocol." IEEE Transactions on Dependable & Secure Computing, Vol.8, No.2, pp.315-317, 2011.

[12] Muhammad Zubair, Umar Mujahid, Najam-ul-Islam and Jameel Ahmed, "Cryptanalysis of RFID Ultra-lightweight Protocols and Comparison between its Solutions Approaches", BUJICT Journal, Vol.5, No. 1, pp. 58-63, 2012.

[13] 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.

[14] Zahra Ahmadian,et al.,"Desynchronization attack on RAPP ultralightweight authentication protocol." Information processing letters, Vol.113, No.7, pp. 205-209, 2013.

[15] 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.

[16] 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.

[17] Hernandez-Castro, Julio Cesar, et.al "Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol." Workshop on RFID Security and Privacy, Turkey, pp. 22-34, 2010.

[18] 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.

[19] 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.

[20] Han, Daewan, "Gröbner Basis Attacks on Lightweight RFID Authentication Protocols." Journal of Information Processing Systems, Vol. 7, No.4, pp.691-706, 2011.

[21] Li, Ticyan, and Guilin Wang. "Security analysis of two ultra-lightweight RFID authentication protocols." International Information Security Conference (SEC), , pp.109-120, South Africa ,2007.

[22] D'Arco, Paolo, and Alfredo De Santis. "On ultralightweight RFID authentication protocols." IEEE Transactions on Dependable and Secure Computing,Vol 8, No.4, pp. 548-563, 2011.

[23] Nawaz, Meena, Jameel Ahmed, and Umar Mujahid. "RFID System: Design Parameters and Security Issues." World Applied Sciences Journal, Vol.23, No.2, pp.236-244,2013.

[24] Umar Mujahid, et.al,"Cryptanalysis of ultralightweight RFID authentication protocol",Cryptology ePrint Archive, Report 2013/385, https://eprint.iacr.org/2013/385 , 2013.

[25] Umar Mujahid, M. Najam-ul-islam, M. Ali shami, "RCIA: A new ultralightweight RFID authentication protocol using Recursive hash," International Journal of Distributed Sensor Networks Volume 2015, Article ID 642180, 8 pages.

[26] 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..

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

[28] 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. http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm, 1999

[29] Tieyan Li and Guilin Wang," Security Analysis of family of Ultra-Lightweight RFID Authentication Protocols", JOURNAL OF SOFTWARE, Vol. 3, No. 3,2008

[30] Wang Shao-hui et.al ," Security Analysis of RAPP: An RFID Authentication Protocol based on Permutation", Cryptology ePrint Archive, Report 2012/327, https://eprint.iacr.org/2012/327 , 2012.

[31] D.Khovratovich et.al ,"Rotational cryptanalysis of ARX",17th international conference on fast software encryption (FSE-2010), pp.333-346, 2010.

[32] Tieyan Li and Robert" Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol", In Second International Conference on Availability, Reliability and Security (AReS}, 2007.

[33] Umar Mujahid, M. Najam–ul-islam,"Ultralightweight cryptography for passive RFID systems" , International Journal of Communication Networks and Information Security (IJCNIS), Vol. 6, No. 3, December 2014.

[34] Xu Zhuang et al."A new ultralightweight RFID protocol for low cost tags": R^2AP", Wireless Personal Communications (2014) Vol 70, pp 1787 – 1802.

[35] Information Security Group, Universit´e catholique de Louvain, Belgium, "Bibliography on Security and Privacy in RFID Systems" Version August, 2015.

[36] GS1 EPCglobal tag data standards version 1.4, Available from; http//www.epcglobalinc.org/standards/.

[37] Istv´an Vajda and Levente Butty´an, "Lightweight Authentication Protocols for Low-Cost RFID Tags", In Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003, Seattle, Washington, USA, October 2003.

[38] Umar Mujahid et al. ," A New Ultralightweight RFID Mutual Authentication Protocol: SASI Using Recursive Hash", International Journal of Distributed Sensor Networks, Volume 2016, Article ID 9648971, 14 pages, 2016.

[39] Umar Mujahid, Atif Raza and M. Najam, "Efficient Hardware Implementation of Ultralightweight RFID Mutual Authentication Protocol", Journal of Circuit Systems and Computers, Vol 25, No.7, 2016.

[40] Kai Fan et al., "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G", SECURITY AND COMMUNICATION NETWORKS, DOI: 10.1002/sec.1314, 2015.