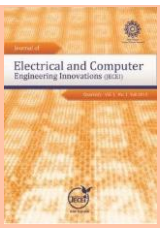
SRTTU

Journal of Electrical and Computer Engineering Innovations

JECEI, Vol. 6, No. 1, 2018



Cryptanalysis of R²AP, an Ultralightweight Authentication Protocol for RFID

Masoumeh Safkhani[1,*]

[1]Faculty of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran.

[*]Corresponding Author's Information: Safkhani@sru.ac.ir

ARTICLE INFO

ARTICLE HISTORY:
Received 07 May 2019
Revised 10 July 2019
Accepted 10 July 2019

KEYWORDS:
RFID
Authentication
R²AP
Linear attack
Traceability attack
Secret disclosure attack
Desynchronization attack

ABSTRACT

To overcome the security flaw of RAPP authentication protocol, Zhuang et al. proposed a novel ultralightweight RFID mutual authentication protocol, called R²AP. In this paper, we first propose a new desynchronization attack against this protocol that succeeds with the probability almost 1 and requires an adversary to initiate 1829 sessions of the protocol with the tag. On the other hand, the protocol updates the tag and the reader secretes to provide the tag holder privacy. However, it is shown that a passive adversary who eavesdrops only two sessions of the protocol can trace the tag with the probability of 0.921. In addition, passive attack for which the adversary can extract the secret *ID* of the tag is presented assuming that the adversary eavesdropped 128 sessions of the protocol, its success probability would be 0.387. To extract the secret *ID*, linear cryptanalysis is used, which is a tool mostly for attack block ciphers.

1. Introduction

Radio Frequency IDentification (RFID) technology is a wireless identification method that uses radio frequency to send and receive data. Most of the RFID systems comprise of tags, reader (s) and a back-end database. While the channel between the reader and the back-end database could be permanent and secure, the channel between the reader and tags is wireless and insecure. On the other hand, a passive tag is a highly constrained microchip with antenna that stores the unique tag identifier and other related information about an object that the tag has been attached to. To provide an acceptable security for such constrained devices, in the last years, several ultralightweight RFID authentication protocols have been proposed, e.g. [1]–[3], but all these schemes have flaws and vulnerabilities to a greater or lesser degree (e.g., [4]-[7]). Zhuang et al. recently proposed an ultralightweight mutual authentication protocol called R²AP [8] which follows a framework already proposed by Tian et al., to design an ultralightweight mutual authentication protocol called RAPP [9]. In R²AP, tags only use three simple operations, bitwise XOR, left rotation and a very lightweight reconstruction function Rec (·), defined as follows:

Deftnition: Let x_i, y_i denote respectively the i[th] bit of x , y ; $x = (x)_1 \,||\, (x)_2 || \ldots ||(x)_l$ and $y = (y)_1 \,||\, (y)_2 || \ldots ||(y)_l$, where $x_i, y_i \in \{0,1\}$ and $||$ denotes concatenation. Then, the reconstruction of x and y, denoted as $Rec(x, y)$, is as follows:

$$\begin{cases} if\ x_i = y_i\ then\ Rec(x,y)_i = x_i \\ if\ x_i \neq y_i\ then\ Rec(x,y)_i = x_i.x_{i-1} + y_i.y_{i-1} \end{cases} \quad (1)$$

where + and . denote bitwise OR and AND, respectively. Compared to the permutation used in RAPP [19], which reveals the Hamming weight of x in the output of $Per(x, y)$, Zhuang et al. claim that the

output of Rec(x, y) is not predictable. In addition, in the case of $Per(x, y)$, given the output and y, it is possible to determine x uniquely. However, it is not the case for *Rec(x, y)*.

In this protocol, the reader and the tag share secret parameters K_1, K_2, K_3 *and* IDS that are updated after each successful run of the protocol. In addition, each tag has a static identifier denoted by ID. The details of the protocol, as depicted in Fig. 1, are as follows:

1. The reader R, sends $Hello$ to the target tag T.
2. T replies with its IDS.
3. R generates a random n_1, computes $A = Rec(K_1, K_2) \oplus n_1$, $B = Rot(Rec(K_2, n_1), Rec(K_3, n_1)) \oplus Rot(n_1, n_1)$ and sends A and B to T .
4. T extracts n_1 from A and evaluates the received value for B to authenticate R. If the reader has been authenticated, the tag computes $C = Rec\big(Rec(K_2, K_3), Rec(n_1, K_1)\big) \oplus ID$ and send it to R.
5. R evaluates the received value for C to authenticate T. If the tag has been authenticated, the reader does as follows:
(a) generates a random number n_2;
(b) computes $D = Rec(n_1, K_3) \oplus Rec(K_1, K_3) \oplus n_2$, $E = Rot\big(Rec(K_2, n_2), Rec(K_2, n_1)\big) \oplus Rot(n_2, n_2)$ and sends D and E to R;
(c) assigns the current values of K_1, K_2, K_3 and IDS^{old} respectively to $K_1^{old}, K_2^{old}, K_3^{old}$ and IDS^{old} and updates the tag's secrets as follows:

$$\begin{aligned} IDS^{new} &= Rec(IDS \oplus n_2, K_3) \oplus K_1 \\ K_1^{new} &= Rec(n_2 \oplus K_1, n_1) \oplus K_2 \\ K_2^{new} &= Rec(K_2, n_1 \oplus n_2) \oplus K_3 \\ K_3^{new} &= Rec(K_2, K_3) \oplus n_1 \end{aligned} \quad (2)$$

6. T extracts n_2 from D and evaluates the received value for E. If E has been confirmed, the tag updates its secrets as step 5c. However, it does not keep a record for the old value of the secrets.

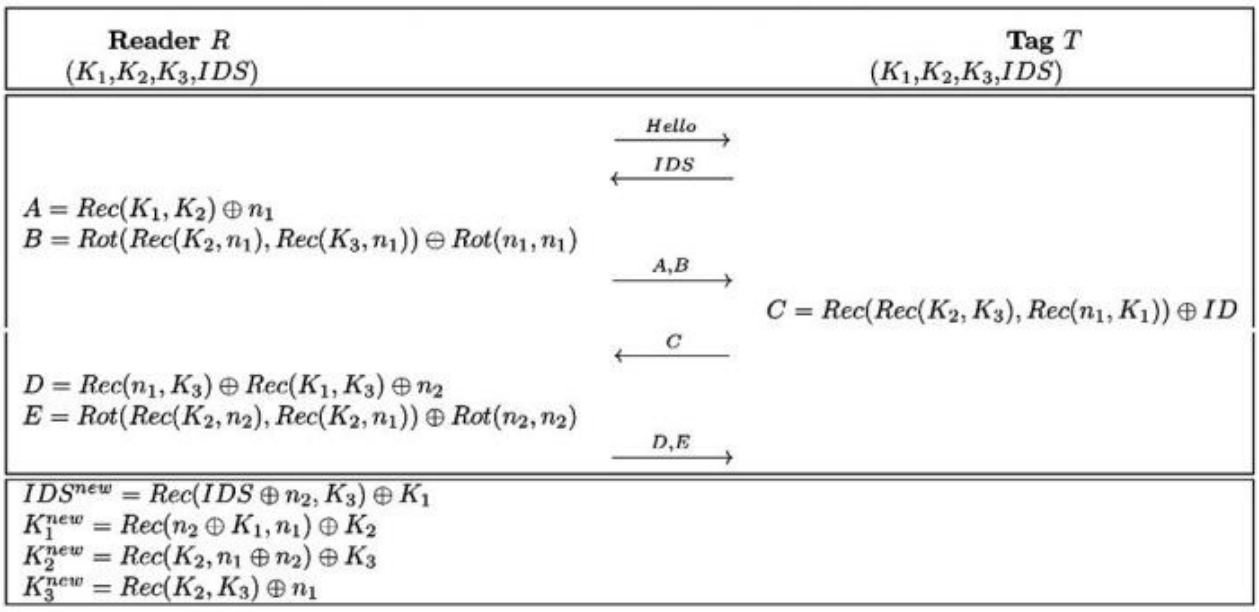


Figure 1: Mutual authentication phase of Zhuang et al. authentication and ownership management protocol [8].

In this protocol, $Rot(x, y)$ denotes a circular left rotate string x by $wt(y)$ bit(s), where $wt(y)$ is the Hamming weight of string $wt(y)$.

The reader keeps two sets of the tuple $\{IDS^x, K_1^x, K_2^x, K_3^x\}$ for $x = old$ (previous values) and $x = new$ (updated values) to prevent desynchronization attacks (e.g., when an active adversary blocks the last message D and E). In addition, it keeps the used random number in the last session n_1 and n_2. Hence, on the next session, if the reader receives IDS^{old}, it will use the same n_1 and n_2 to calculate A, B, D and E. However, it will not give the service access to the tag and is used only to synchronize the tag, it is denoted by synchronization session. To receive service, the tag should participate in another session.

Contributions: R²AP is claimed to be resistant against common attacks, including desynchronization and traceability. In this paper, we first describe a very efficient desynchronization attack with a success probability of almost 1. Secondly, we introduce a traceability attack that exploits the weak properties of $Rec(.)$. In this attack, we disclose a correlation between the transferred messages and bits of the *ID,*

which can be used to trace the tag. The attack can be extended to disclose the whole ID(as in [10]) at the expense of requiring various protocol runs.

In the proposed analysis, The linear cryptanalysis is used which is more common to analyze block ciphers.

2. DESYNCHRONIZATION ATTACK ON R²AP

The designers claim that R²AP scheme resists against common attacks including desynchronization attack [8]. In fact, this property is one of the claimed advantages in comparison to its predecessor (e.g., SASI [1] or RAPP [2]). However, in this section we present an efficient desynchronization attack against R²AP, which contradicts this claim. Before presenting the attack, we prove two lemmas are proved as follows:

Lemma 1: For $y, x \in \{0,1\}^l$, converting any two bits of y does not change the output of $Rot(x,y)$ with the probability of $\frac{1}{2}$.

Proof: Assume that the flipped bits of y are y_i and y_j, for any $i \neq j \in 0,\dots,l-1$. THe new value of y after flipping y_i and y_j is y'. It is clear that $wt(y')= wt(y)- wt(y_i)- wt(y_j) + wt(y_i'), wt(y_j'), y_i' = y_i \oplus 1$ and $y_j' = y_j \oplus 1$. Hence, $y_i||y_j \in \{01,10\}$ gives $wt(y') = wt(y)$, $y_i||y_j = 00$ gives $wt(y') = wt(y) + 2$ and $y_i||y_j = 11$ gives $wt(y') = wt(y) - 2$. So, if $y_i||y_j \in \{01,10\}$ then $wt(y') = wt(y)$ and $Rot(x,y) = Rot(x,y')$, which happens with the probability of $\frac{1}{2}$.

Lemma 2: For $x, y \in \{0,1\}^l$, converting any bit of x or y does not change the output of $Rec(x,y)$ with the probability of $\frac{1}{8}$.

Proof: Assume that the flipped bits of y is y_i, for any $i \in 0,\dots,l-1$. The new value of y after flipping y_i is donated by y'.

It is clear from the definition of $Rec(x,y)$ that $Rec(x,y)_j = x_j.x_{j-1}.\overline{y}_j + \overline{x}_j.y_{j-1}.y_j + x_j.y_j$ in boolean representation. Hence, only $Rec(x,y)_i$ and $Rec(x,y)_{i+1}$ are functions of y_i. Therefore, $Rec(x,y) = Rec(x,y')$ if and only if $Rec(x,y)_i = Rec(x,y')_i$ and $Rec(x,y)_{i+1} = Rec(x,y')_{i+1}$.

Here in, the following equation for all possible values of $x_{i-1}, x_i, x_{i+1}, y_{i-1}, y_i$ and y_{i+1} are evaluated to investigate the correctness of those conditions:

$$\begin{aligned}&(Rec(x,y)_i \oplus Rec(x,y')_i) \cdot (Rec(x,y')_{i+1} \oplus Rec(x,y')_{i+1}) \\ &= \Big(\big((x_i \cdot x_{i-1} \cdot \overline{y}_i) + (\overline{x}_i \cdot y_i \cdot y_{i-1}) + (x_i \cdot y_i)\big) \\ &\quad \oplus \big((x_i \cdot x_{i-1} \cdot y_i) + (\overline{x}_i \cdot \overline{y}_i \cdot y_{i-1}) + (x_i \cdot \overline{y}_i)\big)\Big) \\ &.(((x_{i+1} \cdot x_i \cdot \overline{y}_{i+1} + (\overline{x}_{i+1} \cdot y_{i+1} \cdot y_i) + (x_{i+1} \cdot y_{i+1})) \oplus \\ &\quad \Big(\big(x_{i+1} \cdot x_i \cdot \overline{y}_{i+1} + (\overline{x}_{i+1} \cdot y_{i+1} \cdot \overline{y}_i) + (x_{i+1} \cdot y_{i+1})\big)\Big) \end{aligned} \quad (3)$$

This evaluation shows that the above equation satisfied with the probability of $\frac{1}{8}$. Hence, converting any bit of y does not change the output of $Rec(x,y)$ with the probability of $\frac{1}{8}$. A similar argument holds for the impact of converting any bit of x on the output of $Rec(x,y)$ which completes the proof.

Lemma 3: For randomly selected $x \in \{0,1\}^l$ such that $1 < l \leq 128, pr(wt(x) = \frac{l}{2}) \geq 0.07$

Proof: For randomly selected $x \in \{0,1\}^l$, $pr(x_i = 1) = \frac{1}{2}$ for $0 \leq i \leq l-1$. Hence,

$$pr\left(wt(x) = \frac{l}{2}\right) = \binom{l}{\frac{l}{2}} \times \left(\frac{l}{2}\right)^l \quad (4)$$

Numerical calculation shows that, for $l = 128, pr(wt(x) = 64) = 0.0703860921700151$ and for $i < j, pr(wt(x) = \frac{i}{2}) > pr(wt(j) = \frac{j}{2})$ [11].

Following the above lemmas, the below theorem shows that, despite of the designers claim, an adversary advantage to desynchronize the tag and the reader is not negligible.

Theorem 1: On a session of R²AP between a legitimate tag T and the reader R, the success probability of an adversary which just flips bits $D_i, D_j, E_{i+\frac{l}{2} \mod l}$ and $E_{j+\frac{l}{2} \mod l}$ *to* desynchronize T and R *is* lower bounded by 2^{-11}, for any $i \neq j \in 0,\dots,l-1$.

Proof: On a normal legitimate session between T and R, assume that R sends D and E to T, where $D = Rec(n_1,K_3) \oplus Rec(K_1,K_3) \oplus n_2, E = Rot\big(Rec(K_2,n_2), Rec(K_2,n_1)\big) \oplus Rot(n_2,n_2)$. It is clear that R has already assiged the current values of K_1, K_2, K_3 and IDS^{old} respectively to $K_1^{old}, K_2^{old}, K_3^{old}$ and IDS^{old} and has updated the tag's secrets as follows:

$$\begin{aligned} IDS^{new} &= Rec(IDS \oplus n_2, K_3) \oplus K_1 \\ K_1^{new} &= Rec(n_2 \oplus K_1, n_1) \oplus K_2 \\ K_2^{new} &= Rec(K_2, n_1 \oplus n_2) \oplus K_3 \\ K_3^{new} &= Rec(K_2, K_3) \oplus n_1 \end{aligned} \quad (5)$$

On the other hand, the adversary intercepts D and E and sends to the tag $D' = D \oplus \Delta$ and $E' = E \oplus Rot\left(\Delta, \{1\}^{\frac{l}{2}}\right)$, where $\{1\}^i$ is an string of all 1 of length i-bit. On receiving D' and E', T extracts n_2' as

follows and evaluates the received E' to authenticate the received values and update its secrets:

$$\begin{aligned} n_2' &= D' \oplus Rec(n_1, K_3) \oplus Rec(K_1, K_3) \\ &= Rec(n_1, K_3) \oplus Rec(K_1, K_3) \oplus n_2 \\ &\oplus \Delta \oplus Rec(n_1, K_3) \oplus Rec(K_1, K_3) \\ &= n_2 \oplus \Delta \end{aligned} \quad (6)$$

The above equation shows that n_2' can be considered as n_2 after flipping two bits. Hence, based on Lemma 1 and Lemma 3, it is clear that $Pr\left(Rot(n_2, n_2) = Rot(n_2', n_2') \oplus Rot\left(\Delta, \{1\}^{\frac{l}{2}}\right)\right) \geq 0.07 \times \frac{1}{2}$.

On the other hand, based on Lemma 2, $Pr\left(Rec(K_2, n_2) = Rec(K_2, n_2')\right) = \frac{1}{8}$.

To evaluate E', the tag verifies whether $Rot\left(Rec(K_2, n_2'), Rec(K_2, n_1)\right) \oplus Rot(n_2', n_2') \stackrel{?}{=} E'$ where,

$E' = Rot\left(Rec(K_2, n_2), Rec(K_2, n_1)\right) \oplus \mathrm{Rot}(n_2, n_2) \oplus \mathrm{Rot}\left(\Delta, \{1\}^{\frac{l}{2}}\right)$.

Therefore, T accepts the received D' and E' if $Rec(K_2, n_2) = Rec(K_2, n_2')$ and $Rot(n_2', n_2') = Rot(n_2, n_2) \oplus Rot\left(\Delta, \{1\}^{\frac{l}{2}}\right)$ that respectively are correct with the probability of $\left(\frac{1}{8}\right)^2$ and at least $0.07 \times \frac{1}{2}$ respectively. Hence, the sent D' and E' are accepted by T with the probability not less than $\left(\frac{1}{8}\right)^2 \times 0.07 \times \frac{1}{2} = 0.000546875$.

If the tag accepts D' and E', it will update its secrets as follows:

$$\begin{aligned} IDS^{new} &= Rec(IDS \oplus n_2', K_3) \oplus K1 \\ K_1^{new} &= Rec(n_2' \oplus K_1, n_1) \oplus K_2 \\ K_2^{new} &= Rec(K_2, n_1 \oplus n_2') \oplus K_3 \\ K_3^{new} &= Rec(K_2, K_3) \oplus n_1 \end{aligned} \quad (7)$$

which does not match the reader's records of the new secrets with the probability of $1 - \left(\frac{1}{8}\right)^6 = 0.9999962$. Hence, the lower bound for the success probability of the adversary in its attack is $0.000546875 \times 0.9999962 = 0.000546873 > 2^{-11}$, which completes the proof.

To implement the above attack, an adversary eavesdrops a session of the protocol between the reader and the tag and stores all messages but intercepts D and E and sends D' and E' as mentioned in Theorem 1. Next, it sends a *Hello* command to the tag. If the tag returns the old record of IDS, it means that it has not accepted the sent D' and E' and the adversary can impersonate the reader by sending the stored values of A and B and new values of D' and E'. The adversary repeats this attack up to when the tag accepts D' and E'. Based on Theorem 1, if the tag accepts the sent D' and E', the updated tags records of secrets do not match the reader records with the probability of 0.9999962. The expected complexity of this attack is eavesdropping a session between a legitimate tag T and the reader R and 1829 impersonation of the reader to the tag.

3. Traceability Attack on R²AP

When a reader R sends Hello command to the tag T, the tag returns its IDS which is constant as far as the tag has not participated in a successful run of the protocol and updated its secrets. Hence, the constant value of IDS can be used to mount a trivial traceability attack against the tag holder between any two sessions of the protocol. However, in this section, we present a traceability attack against R²AP that works even after arbitrary updates of the secrets.

The designers claimed that R²AP scheme resists against such traceability attacks [8]. Before presenting the attack, we prove a lemma.

Lemma 4: For $x, y \in \{0,1\}^l$, it is given that $Pr\left(Rec(x,y)_i = Rec(x,y)_{i+1}\right) = \frac{3}{8}$.

Proof : From definition of $Rec(x,y)$, it is clear that

$$Rec(x,y)_i = \left(x_i \cdot x_{i-1} \cdot \overline{y}_i\right) + \left(\overline{x}_i \cdot y_i \cdot y_{i-1}\right) + \left(x_i \cdot y_i\right) \quad (8)$$

$$Rec(x,y)_{i+1} = \left(x_{i+1} \cdot x_i \cdot \overline{y}_{i+1}\right) + \left(\overline{x}_{i+1} \cdot y_{i+1} \cdot y_i\right) + \left(x_{i+1} \cdot y_{i+1}\right) \quad (9)$$

It is clear that both $Rec(x,y)_i$ and $Rec(x,y)_{i+1}$ are functions of x_i and y_i. Hence, a correlation between them is expected. To determine the correlation, $Rec(x,y)_i \oplus Rec(x,y)_{i+1}$ for all possible values of $x_{i-1}, x_i, x_{i+1}, y_{i-1}, y_i$ and y_{i+1} should be evaluated. The evaluation shows that for 40 out of 64 possible cases $Rec(x,y)_i \oplus Rec(x,y)_{i+1} = 0$. Hence, $Pr\left(Rot(x,y)_i = Rot(x,y)_{i+1}\right) = \frac{3}{8}$, which completes the proof.

Following the above lemma, the below theorem shows that, despite of the designers claim, an adversary's advantage to trace the tag holder in R²AP protocol is not negligible.

Theorem 2: Assume that the adversary has eavesdropped a session of the protocol between T and R and the parameter length in the protocol is l, given a session of the protocol T' and R, the adversary's success probability to verify whether $T \stackrel{?}{=} T'$ is 0.977.

Proof: Assume that the adversary has eavesdropped a session of the protocol between T *and* R *and stored* $C = Rec\left(Rec(K_2, K_3), Rec(n_1, K_1)\right) \oplus ID$.

TABLE 1
INTERNAL SECRET VALUES AFTER DESYNCHRONIZATION

Reader (database)	Tag
$IDS^{old} = IDS$ $K_1^{old} = K_1; K_2^{old} = K_2; K_3^{old} = K_3$	$IDS^{new} = Per\ (IDS, n_1 \oplus n_2) \oplus K_1 \oplus K_2 \oplus K_3$ $K_1^{new} = Per\ (K_1, n_1) \oplus K_2$ $K_2^{new} = Per\ (K_2, n_2) \oplus K_1$ $K_3^{new} = Per\ (K_3, n_1 \oplus n_2) \oplus IDS$
$IDS^{new} = Per\ (IDS, n_1' \oplus n_2') \oplus K_1 \oplus K_2 \oplus K_3$ $K_1^{new} = Per\ (K_1, n_1') \oplus K_2; K_2^{new} = Per\ (K_2, n_2') \oplus K_1$ $K_3^{new} = Per\ (K_3, n_1' \oplus n_2') \oplus IDS$	

Based on Lemma 4, for any $0 \le i \le l-1$, it is given that $P\ r((Rec(Rec(K_2, K_3), Rec(n_1, K_1)))_i = \left(Rec\left(Rec(K_2, K_3), Rec(n_1, K_1)\right)\right)_{i+1}) = \frac{3}{8}$

On the other hand, if $\left(Rec\left(Rec(K_2, K_3), Rec(n_1, K_1)\right)\right)_i = \left(Rec\left(Rec(K_2, K_3), Rec(n_1, K_1)\right)\right)_{i+1}$, then $C_i \oplus C_{i+1} = ID_i \oplus ID_{i+1}$, which is constant and independent of the session. Hence, an adversary who eavesdropped a session of the protocol between T and R, computes $C \oplus Rot(C, 1)$ and stores it. Next, given a session of the protocol between T' and R, the adversary computes $WT = wt\left(\left(C \oplus Rot(C, 1)\right) \oplus \left(C' \oplus Rot(C', 1)\right)\right)$ *to decide whether* $T \stackrel{?}{=} T'$. If $T \neq T'$ then $wt((C \oplus Rot(C, 1))$ and $wt(C' \oplus Rot(C', 1)))$ are expected to be independent and:

$$Pr\left(wt\left(\left(C \oplus Rot(C, 1)\right)_i \oplus \left(C' \oplus Rot(C', 1)\right)_i\right) = 0\right) = \frac{1}{2} \quad (10)$$

$$Pr(wt(\left(C \oplus Rot(C, 1)\right)_i \oplus \left(C' \oplus Rot(C', 1)\right)_i) = 1) = \frac{1}{2} \quad (11)$$

and the expected value of WT for each eavesdropped session would be $\frac{l}{2}$. On the other hand, if $T = T'$ and if $C_i \oplus C_{i+1} = ID_i \oplus ID_{i+1}$, then with the probability of 1 it is given that $wt\left(\left(\left(C \oplus Rot(C, 1)\right)_i \oplus \left(C' \oplus Rot(C', 1)\right)_i\right)\right) = 0$, which happens with the probability of $\left(\frac{3}{8}\right)^2$; otherwise the hamming weight of that bit would be 0 with the probability of $\frac{1}{2}$. Hence,

$$Pr\left(wt\left(\left(\left(C \oplus Rot(C, 1)\right)_i \oplus \left(C' \oplus Rot(C', 1)\right)_i\right)\right) = 0\right) = \left(\frac{3}{8}\right)^2 + \left(1 - \left(\frac{3}{8}\right)^2\right) \times \frac{1}{2} = 0.4296875 \quad (12)$$

$$Pr\left(wt\left(\left(\left(C \oplus Rot(C, 1)\right)_i \oplus \left(C' \oplus Rot(C', 1)\right)_i\right)\right) = 1\right) =$$

$$1 - Pr\left(wt\left(\left(\left(C \oplus Rot(C, 1)\right)_i \oplus \left(C' \oplus Rot(C', 1)\right)_i\right)\right) = 0\right) = 0.5703125 \quad (13)$$

Therefore, if $T = T'$, the expected value of WT for each eavesdropped session would be $= 0.5703125 \times l$. To decide whether $T \stackrel{?}{=} T'$, the adversary should distinguish two binomial distribution with $p = \frac{1}{2}$ and $p = 0.5703125$, respectively, where the number of observations are $2l$. Hence, the adversary outputs $T = T'$ if $WT < \frac{l}{2}$ for which the success probability is as follows [12, 13]:

$$\int_{-2\sqrt{2l}\left|p-\frac{1}{2}\right|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \quad (14)$$

When $l = 128$, for an adversary who eavesdrops a session between the tag and the reader the success probability would be 0.921. If the adversary eavesdrops two sessions, then its advantage increases to 0.977 [12].

The above attack contradicts the designers of R²AP claim that it is not possible to link messages over sessions to trace the tag holder. Hence, R²AP compromises the tag holder security.

4. PARTIAL DISCLOSURE ATTACK

In this section, the result of Lemma 4 to extract the ID of the tag is extended which is constant and is expected to be secure. From that Lemma, given the messages of any distinct two sessions of the protocol some linear equations can be found which include bits of parameter C which is known to the attacker and bits of the tag's ID with considerable bias (distance from 0.5). Given this fact and thanks to linear cryptanalysis attack from classical cryptography [12],

the tag's IDcan be extracted. Before presenting the main attack, a Lemma should be presented.

Lemma 5: Assume that the linear equation $\oplus_{i=1}^{m} X_{x_i}^{j} = \oplus_{i=1}^{n} K_{k_i} for \quad 0 \leq x_i^j \leq |X| - 1,$ and $0 \leq k_i \leq |K| - 1$ *where* X^j is a known value and K is a constant secret value, holds with the probability of $q + \varepsilon$. Given ε^{-2} samples of that equation, the adversary can determine $\oplus_{i=1}^{n} K_{k_i}$ with a non-negligible probability.

Proof: The above equation is a special case of classical linear cryptanalysis which is a known plaintext attack that tries to find a high probability linear expressions involving "plaintext" bits, "ciphertext" bits and the "subkey" bits as follows:

$$\oplus_{i=1}^{m} P_{p_i} \oplus_{i=1}^{n} C_{c_i} = \oplus_{i=1}^{z} K_{k_i} \tag{15}$$

where, $0 \leq p_i \leq |P| - 1, 0 \leq c_i \leq |C| - 1$ and $0 \leq k_i \leq K - 1$, and P, C and K represent plaintext, ciphertext and key respectively.

Assuming that the key is fixed, the adversary has N plaintexts and related ciphertexts under that key and the above equation holds with the probability of p, using Algorithm 1 of Matsui [12] the adversary's success probability to determine $\oplus_{i=1}^{m} K_{k_i}$ is as follows:

$$\int_{-2\sqrt{N}\left|p-\frac{1}{2}\right|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \tag{16}$$

for $N = \varepsilon^{-2}$ and $N = 2\varepsilon^{-2}$ the success probabilities are 0.977 and 0.998, respectively. It is clear that the given equation in the Lemma is another representation of the equation for linear cryptanalysis for which $\oplus_{i=1}^{m} P_{p_i} \oplus_{i=1}^{n} C_{c_i}$ has been replaced by $\oplus_{i=1}^{m} X_{x_i}^{j}$as a known parameter. Hence, given $q + \varepsilon$ equations, the success probability of the adversary to determine $\oplus_{i=1}^{n} K_{k_i}$ is 0.977, which completes the proof.

Following the above lemma, the below theorem shows that an adversary can extract the secret ID of the tag in R²AP protocol.

Theorem 3: *Given R²AP, a passive adversary who eavesdrops 128 sessions of the protocol can determine whole tag's ID with the probability of* $\frac{0.998^l}{2}$.

Proof: From Theorem 2, we know that $Pr(C_i \oplus C_{i+1} = ID_i \oplus ID_{i+1}) = \frac{3}{8}$. Hence, we have a linear equation that can be represented in Lemma 5 for which the bias is $\frac{1}{8}$. Hence, given the message C for $2 \times \left(\frac{1}{8}\right)^{-2} = 128$ different sessions of the protocol, the adversary can retrieve $ID_i \oplus ID_{i+1}$ with the probability of 0.998. The success probability of the adversary to determine whole l-equations correctly is 0.998^l.

However, each equation includes two bits of ID which means that the adversary needs to guess a bit of ID which the guess is correct with the probability of 0.5. Therefore, the success probability of the adversary to determine whole ID after eavesdropping 128 sessions of the protocol is $\frac{0.998^l}{2}$ which completes the proof. For $l = 128$, the success probability would be 0.387.

5. Comparison with the Related Works

The described desynchronization attack in this paper benefits from our observations of the structure of the messages that are calculated over R²AP . It should be noted that other desynchronization attacks on this scheme has been reported already, [23,24]. However, they both follow similar attacks on other ultra-lightweight mutual authentication protocols (UMAP) such as SASI [1], RAPP [9], and etc., and are based on the fact that only the reader introduces nonce into the protocol. In [23], Safkhani and Bagheri presented a generalized version of such attacks against UMAP, include R²AP. On the other hand, the proposed attack in this paper is a dedicated attack for R²AP. Although we cannot claim lower complexity for the attack, it provides a new insight behind the designing of R²AP.

It is obvious that after desynchronizing the reader and the tag, either based on the attack provided in this paper or other related desynchronization attacks, it would be possible to trace the tag based on it. However, again it is tried to use the structure of the transferred messages to apply a traceability attack.

In the related work [24], Taqieddin et al. also proposed a secret disclosure attack against R²AP, which extracts whole the secrets with the complexity of 225. The advantage of that attack is to recover whole secrets while here in only ID is recovered. However, the approach of the secret disclosure attack which is presented in this paper is novel, based on linear cryptanalysis and also it has much lower complexity, i.e., 27 sessions of the protocol. In addition, the attack presented in [24] is an active attack, in which the adversary should terminate the messages or manipulate them. In addition, the tag and the reader should not update their shared parameters during the attack process, while the proposed attack is a passive attack and has no restriction on the updating the shared parameters, note that ID is a constant value and will not be updated. This feature makes the proposed attack in this paper more feasible. It should be noted that the main target of this paper is to introduce the application of a technique from cryptanalysis of block ciphers to attack a protocol based on simple operations. In addition, the idea presented in this paper can be used to recover other shared values in an active adversarial model, but it is not the target of this paper.

Finally, it worth nothing Taqieddin et al. [24] also proposed an improved version of R²AP. In the proposed protocol, they kept whole the structure and just changed transferred messages E and B. Given that they have not changed the structure of the transferred message D, an identical disclosure attack can be applied on their protocol also. In addition, given that only the reader introduces nonce into the protocol, following the generalized desynchronization attack of [23], it is possible to desynchronize the tag and the reader also.

6. Conclusions

It was shown that R²AP suffers from desynchronization, traceability, and disclosure attacks, where the two later attacks work in passive adversary model. In the presented secret discloser attack, linear cryptanalysis was used which is a tool to attack block ciphers. This study shows that R²AP is as weak as its predecessor (e.g., SASI [1] or Gossamer [2] and RAPP [9]), and even its successor proposed by Taqieddin et al. [24]. This study along with the past study such as [14]-[16], [4], [17]-[18], [5], [7] show that it may not be possible to design a secure authentication protocol without employing a secure cryptographic primitive. On the other hand, given recent advances in symmetric cryptography and available lightweight block ciphers such as SIMON [19], SIMECK [20] and PRESENT [21] that are very lightweight and can be implemented in the constraint environments, a better direction could be designing a secure authentication protocol using these primitives. Although, using a secure primitive does not guaranty the security of the designed protocol [22].

7. Acknowledgment

This work was supported by Shahid Rajaee Teacher Training University under contract number 9413, 97-05-17.

References

[1] H.-Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Trans. Dependable Sec. Comput.*, vol. 4, no. 4, pp. 337–340, 2007.

[2] P. Peris-Lopez, J. C. H. Castro, J. M. Est´evez-Tapiador, and A. Ribagorda, "Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol," in *Proc. International Workshop on Information Security Applications (WISA)*, pp. 56–68, 2008.

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

[4] G. Avoine, X. Carpent, and B. Martin, "Privacy-friendly synchronized ultralightweight authentication protocols in the storm," J. *Network and Computer Applications*, vol. 35, no. 2, pp. 826–843, 2012.

[5] P. D'Arco and A. D. Santis, "On ultralightweight RFID authentication protocols," *IEEE Trans. Dependable Sec. Comput.*, vol. 8, no. 4, pp. 548–563, 2011.

[6] M. Safkhani and N. Bagheri, "Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things," *The Journal of Supercomputing*, vol. 73, no. 8, pp. 3579– 3585, 2017.

[7] R. C. W. Phan, "Cryptanalysis of a new ultralightweight RFID authentication protocol SASI," *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 4, pp. 316–320, 2009.

[8] X. Zhuang, Y. Zhu, and C. Chang, "A new ultralightweight RFID protocol for low-cost tags: R²AP," *Wireless Personal Communications*, vol. 79, no. 3, pp. 1787–1802, 2014.

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

[10] S. H. Wang, Z. Han, S. Liu, and D. W. Chen, "Security analysis of RAPP an RFID authentication protocol based on permutation," Cryptology ePrint Archive, Report 2012/327, 2012.

[11] L. R. . A. online at: www.faculty.vassar.edu/lowry/ch14a.html. Concepts and applications of inferential statistics. http://www.vassarstats.net/textbook/ch5apx.html, Last accessed 20 June, 2015.

[12] M. Matsui, "Linear cryptoanalysis method for DES cipher," in *Proc. EUROCRYPT: Workshop on the Theory and Application of Cryptographic Techniques*, pp. 386–397, 1994.

[13] K. Nyberg, Linear Cryptanalysis, Icebreak, 2013, http://ice.mat.dtu.dk/ slides/kaisa_1.pdf.

[14] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Desynchronization attack on RAPP ultralightweight authentication protocol," *Inf. Process. Lett.,* vol. 113, no. 7, pp. 205–209, 2013.

[15] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "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] G. Avoine and X. Carpent, "Yet another ultralightweight authentication protocol that is broken," presented at the Workshop on s Security – RFIDSec'12, Nijmegen, Netherlands, June 2012.

[17] N. Bagheri, M. Safkhani, P. Peris-Lopez, and J. E. Tapiador, "Weaknesses in a new ultralightweight RFID authentication protocol with permutation – RAPP," *Security and Communication Networks*, vol. 7, no. 6, pp. 945–949, 2014.

[18] P. D'Arco and A. D. Santis, "Weaknesses in a recent ultra-lightweight RFID authentication protocol," in *Proc. AFRICACRYPT: International Conference on Cryptology in Africa*, pp. 27–39. Springer, 2008.

[19] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," presented at the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 2015.

[20] G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong, "The Simeck family of lightweight block ciphers," presented at the CHES 2015: 17th International Workshop, Saint-Malo, France, 2015.

[21] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: an ultra-lightweight block cipher," in *Proc. International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007)*, pp. 450–466, 2007.

[22] M. Safkhani, N. Bagheri, P. Peris-Lopez, and J. M. E. Tapiador, "Employing a secure cipher does not guarantee the security of RFID protocols," in *Proc. ISCTURKEY 2014*, pp. 1–6, 2014.

[23] M. Safkhani and N. Bagheri, "Generalized desynchronization attack on UMAP: application to RCIA, KMAP, SLAP and SASI+ protocols," *IACR Cryptology*, Available: https://ePrint.iacr.org.2016/905, 2016.

[24] E. Taqieddin, H. Al-Dahoud, and K. Mhaidat, "Security analysis and improvement of reconstruction based radio frequency identification authentication protocol," *International Journal on Communications Antenna and Propagation*, vol. 8, no. 3, p. 206, 2018.

BIOGRAPHIES

Masoumeh Safkhani is an assistant professor at Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. She received her Ph.D. from Iran University of Science and Technology. She is the author of over 50 articles in information security and cryptology. A record of her publications is available at google scholar.

How to cite this paper:
M. Safkhani, "Cryptanalysis of R²AP, an ultralightweight authentication protocol for RFID," *Journal of Electrical and Computer Engineering Innovations*, vol. 6, no. 1, pp. 107-114, 2018.
DOI: 10.22061/JECEI.2018.1103
URL: http://jecei.sru.ac.ir/article_1103.html