Quantifying cryptographic techniques in radio frequency identification protocols and ways of remedying the security threats

CRISTINA HURJUI, STEFAN HOLBAN, ADRIAN GRAUR
Department of Computers and Automation, Department of Computers
'Stefan cel Mare' University of Suceava, 'Politehnica' University of Timisoara
Str. Universitatii No.13, 720229, Suceava/Vasile Parvan Blvd.2, 300223, Timisoara
ROMANIA
churjui@eed.usv.ro, stefan@aspc.cs.upt.ro, adriang@eed.usv.ro
http://www.eed.usv.ro, http://www.cs.upt.ro

Abstract: - Critical examinations concerning the Radio Frequency Identification security and privacy have determined wide analysis over the time. RFID applications have always assumed two important hierarchies: structures aiming to offer security to RFID systems and structures aiming to offer functionality, with no security issues. A way of creating radio frequency identification systems more secure relies on cryptography. Nine RFID protocols of identification and authentication are examined in this paper, so as to analyze the strong points and to find solutions for the weak or jeopardizing points that threaten the security and privacy of RFID systems. By reaching the best security and privacy solutions, using of RFID systems will bring visibility within developing business strategies or logistics processes, in thoroughly transparency. In many situations, the threatening over RFID structures is the result of designing weak protocols. Presumable attacks on RFID structures are evaluated; important ways of comparison and analysis amongst nine existing protocols are outlined. At the end of each description, solutions of treating the weak points are emphasized.

Key-Words: - Radio frequency identification, protocol of identification, protocol of authentication, security, privacy

1 Introduction

Radio Frequency Identification signifies an implementation of intelligent items [2], so as to track and trace entities or persons, to locate items on various manufacturing lines or to carry out solutions of supply chain management specific to factories or trade companies [10]. RFID will be considered not just simple accomplishment of some research, but an efficient solution for companies or enterprises [2]. The RFID protocol of identification allows a reader to achieve a tag's identity, but without asking any proofs. The basic protocol of identification used nowadays is illustrated in Fig.1.

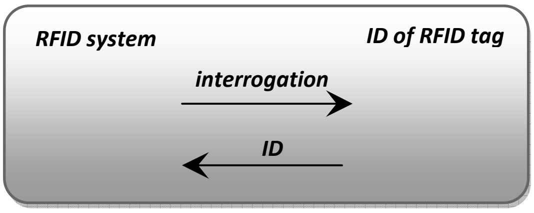

Fig.1 Diagram of RFID tags' identification

This protocol consists in the following: the reader sends a request to a tag and the tag answers the reader, by sending its identification number (*ID*). The RFID system's database contains and will recognize the tag's ID, if the tag is authentic. This protocol seems to be so simple, and of course will need handling of some privacy issues.

The RFID protocol of authentication allows a reader to be sure of tag's identity, tag which is interrogated. The authentication protocol allows a tag to be sure of the reader's identity, which is interrogating that tag. If both features are met, one might talk about the mutual authentication. The authentication protocols provide identification, but the vice-versa situation is not ensured. The basic authentication protocol currently used can be seen in Fig.2.

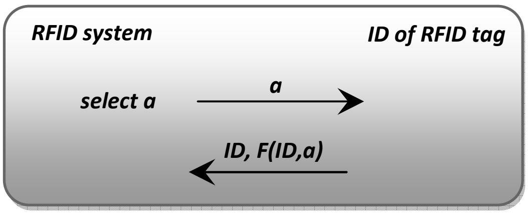

Fig.2 Diagram of RFID authentication and an interrogation-response method

This protocol is under the form of an interrogation-answer mode: the reader sends a request *a* towards tag, and the tag sends its ID and *F(ID, a),* where *F* is a known function (for instance, an encryption function). The threatening of RFID technology can be seen in two classes: the first class, including simple security threatening. The second class refers to privacy, meaning leakage of data and also to traceability, signifying that an adversary is able to recognize a tag, already seen at a past time.

2 Approach on security and privacy of Radio Frequency Identification

Radiofrequency identification brings into analysis, as any other technologies in progress, some security issues. Traceability signifies that an adversary is able to recognize a tag, already seen at a past time or in another location [11]. Some threatening parts against the RFID technology can be brought into mind: relay attack and impersonation, leakage of information or anticipation of traceability. An anti-collision protocol proposed by Philips for ICode1 Label IC tag [5] will be forwards analyzed. The tag uses the frequency 13,56MHz and is formed of an identifier on 64 bits, of which 32 bits are used for the process of singularity, noted by b1...b_{32}.

Although this tag is not using a generator of pseudo-random numbers (abbreviated with *PRNG*) for the process of singularity, the anti-collision protocol implemented is considered probabilistic. Selecting the time periods depends upon tag's identifier and upon data sent by the reader. When a reader interrogates a tag, it sends a request that includes: the number *n* of periods, which can be used by the tag and $n \in \{2^0, 2^1, ..., 2^8\}$ and also a hash value *h,* where $h \in 0,...,25$. Equation (1) illustrates the selection the time periods s_i, carried out as:

$$s_i := CRC8(b_{h+1}...b_{h+8} \oplus prev) \oplus n \qquad (1)$$

CRC8 signifies the *cyclic redundancy check*; *prev* represents the previous CRC8 result, which is initiated with 0x01, when the tag is placed in the reader's area. Therefore, an adversary will easily detect a tag, compliant to the time period chosen by the tag, if this adversary sends always the same *h* and *n* values. An example of such method: an adversary sends a request to a tag, which includes the number *n* of time periods and the hash value *h*. The tag answers during time period $s_{target.}$ When the adversary meets a set of *m* tags, this will wish to find out if its targeted tag is included in that set. In this way, the adversary will send a request of singularity, formed of the same *h* and *n* values. In case no tag answers to this request during the time period s_{target}, it means that tag targeted is not placed within the set of tags interrogated. The probability for a targeted tag to be within a set of *m* tags; (2) proves that at least one tag will answer to interrogation during time period s_{target} is given by

$$P(n, m, p) = \frac{p}{p + (1 - p)\left(1 - \left(\frac{n-1}{n}\right)^m\right)} \qquad (2)$$

and *p* signifies the probability for a targeted tag to exist in that set of *m* tags. As concerns ICode1 Label IC tag, CRC8 is applied on a word of 8 bits, and 8 bits can be recovered from the identifier by sending just one interrogation of singularity. In this way, by sending four requests noted with the following forms $h = 0$, $h = 8$, $h = 16$ and $h = 24$, the adversary will recover those 32 bits of the tag's identifier of singularity.

So as to avoid the detection of a tag's traceability, one might modify the identifier of the tag. In this way, only an authorized part will be able to connect the successive modifications of the identifier. A significant method consists in storing within tag a list of identifiers, named *pseudonyms*, which can be used in sequential and cyclical ways. Another approach assumes the refresh of identifiers specific to tags, by means of deterministic or randomized methods.

In this paper, nine protocols based on identifiers updating by means of RFID readers will be compared, in order to carry out an analysis over endangering points that threaten the security and privacy of RFID structures. The protocols analyzed and compared are: the protocols of Henrici şi Muller [6], of Golle, Jakobsson, Juels and Syverson [13] that is based upon a universal re-encryption scheme, the protocol of Juel based on XOR [1] operations, the protocol of Saito, Ryou and Sakurai [8], of Ohkubo, Suzuki and Kinoshita [11], of Juels and Weis [5], of Weis, Sarma, Rivest and Engels [5], of Feldhofer, Dominikus and Wolkerstorfer [16] and the protocol of Rhee, Kwak, Kim and Won [8].

2.1 The RFID protocol proposed by Henrici and Muller

At this protocol, the RFID transponder needs the storing of an identifier *ID* and two variables *k* şi k_{last}. The transponder contains its current ID, the number *k* of session and k_{last} equal to *k* [4, 6]. As concerns the RFID reader, the database includes and manages 3-items for each tag. Fig.3 depicts the identification of the tag, consisting in: *(a)* the RFID reader sends an interrogation to the RFID tag; *(b)* the RFID tag will increase the number *k* of sessions by one value and will send the answer $h(ID)$, $h(k \oplus ID)$ and $\Delta k := k - k_{last}$. The value $h(ID)$ will allow the database to recover the identifier *ID*. The value Δk allows the database to recover *k*; in this way, $h(k \oplus ID)$ is computed and attacks will no more be activated; the database will check the validity of values, so as to be compliant with its data stored. If this matches, the database will send a random number *r* and the value $h(r \oplus k \oplus ID)$ to the tag, storing the new values. Since the tag knows *k* and *ID* and also receives an *r*, this can check if $h(r \oplus k \oplus ID)$ is correct or not. If this is correct, it will replace its *ID* by $r \oplus ID$ and k_{last} by *k*. Contrariwise, its identifier will not be replaced. Forwards, some potential attacks will be analyzed, so as to determine the strong and weak points of the protocol proposed by Henrici and Muller.

- *Presumable attack based upon avoiding the updating of identifiers.* Such an attack assumes the corruption of hash value sent by the RFID reader. The tag will increase *k*, since it receives the request from adversary [15]. The hash value sent by reader seems to be incorrect, since *k* is now increased. As conclusion, an adversary can always detect a tag between two correct identifications, which are carried out.
- *Presumable attack based upon desynchronizing the system's database.* Such an attack might be severe, since it assumes the desynchronization of both tag and the database. In this way, an adversary might execute the identification process, so that the random value *r* sent by it will represents the neutral value of $\oplus$: the adversary replaces *r* by a string of null bits and will also replace $h(r \oplus k \oplus ID)$ by $h(k \oplus ID)$.

It results $h(0 \oplus k \oplus ID) = h(k \oplus ID)$. In this way, the tag will not be able to detect the potential attack. After this, the tag will replace its ID with $0 \oplus ID$ and updates k_{last}. At the next process of identification, the tag and database will be desynchronized, since the tag calculates a hash value, by means of its previous ID and the new k_{last}, while the database checks the hash value by knowing the previous ID and the previous k_{last}; as result, the identification fails and the tag will be detectable. This attack might be avoided by verifying that $r \neq 0$, but even in this case the desynchronization is still possible. One will assume $h(k_i \oplus ID)$ and $\Delta k_i = k_i - k_{i-1}$ be the data collected. The adversary interrogates again the tag, achieving $h(k_j \oplus ID)$ and the value $\Delta k_j = k_j - k_{j-1}$; the adversary will guess $k_i \oplus k_j$, knowing that:

$$k_i - k_j = \sum_{l-i}^{j-1} \Delta k_l \qquad (3)$$

If one assume $k_i - k_j = 1$, the value $k_i \oplus k_j = 00...01$ will have a value of probability of 50%, as depicted from (3). As in the situation of $r = 0$, the potential attack will desynchronize the database and the tag, which will be detectable.

- *Presumable attack based upon non-random information.* This attack takes into account the detection of tag traceability, by means of information provided by *Δk*. The tag increases its value *k* when receiving an interrogation, but updates k_{last} only when identification occurs. In this way, a potential adversary can interrogate a tag few times, so as to increase too much *k* and to find out Δk. The adversary will be able to recognize its target, in accordance to: if the tag sends a value too high of Δi, the adversary will see that this is its targeted tag.

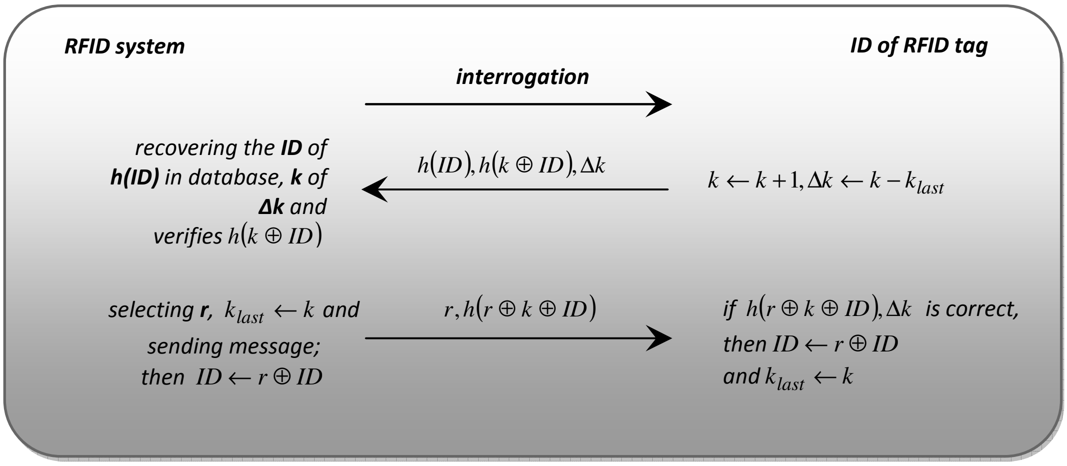
RFID system
ID of RFID tag
interrogation
recovering the ID of h(ID) in database, k of Δk and verifies $h(k \oplus ID)$
$h(ID), h(k \oplus ID), \Delta k$
$k \leftarrow k+1, \Delta k \leftarrow k - k_{last}$
selecting r, $k_{last} \leftarrow k$ and sending message; then $ID \leftarrow r \oplus ID$
$r, h(r \oplus k \oplus ID)$
if $h(r \oplus k \oplus ID), \Delta k$ is correct, then $ID \leftarrow r \oplus ID$ and $k_{last} \leftarrow k$

Fig.3 RFID privacy protocol proposed by Henrici and Muller

2.2 The RFID protocol proposed by Golle, Jakobsson, Juels and Syverson

This protocol is based on the concept of universal re-encryption. The scheme of universal re-encryption assumes that re-encryptions of a message *m* are not accomplished either by interrogation or by achieving the public key's information, under which the message *m* was encrypted at first. The encryption is using ElGamal scheme [8] of a message *m* with the public key *y* and a random number *r* is represented by my^r, g^r; g is the generator of *G*. Given *E* as the scheme of ElGamal encryption and *U* the compliant re-encryption scheme, one might emphasize the result $U(m) := [E(m); E(1_G)]$. Knowing that *q* is the order of *G*, and *g* the generator element of *G*, the re-encryption universal scheme [5] will be defined by four algorithms, as follows:

- *generation of keys:* provides the private key $x \in Z$ and the ElGamal public key $y = g^x$;
- *encryption:* given (r_0, r_1) a random item of $\left(Z / qZ \right)^2$, and the encrypted value for a message *m* will be $U(m) = \left[(\alpha_0, \beta_0); (\alpha_1, \beta_1) \right] = \left[(my^{r0}, g^{r0}); (y^{r1}, g^{r1}) \right]$;
- *decryption*: knowing the ciphertext $[(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ and given that $\alpha_0, \beta_0, \alpha_1, \beta_1 \in G$ and $\alpha_1 / \beta_1^x = 1$, the plaintext will be $\alpha_0 / \beta_0^x = 1$;
- *re-encryption:* $(r_0^{'}, r_1^{'})$ - random item of $\left(Z / qZ \right)^2$.

The re-encrypted value of $\left[(\alpha_0, \beta_0); (\alpha_1, \beta_1) \right]$ ciphertext will be $\left[\left(\alpha_0 \alpha_1^{r_0^{'}}, \beta_0 \beta_1^{r_0^{'}} \right) \right]; \left(\alpha_1^{r_1^{'}}, \beta\beta_1^{r_1^{'}} \right)$.

While initializing a tag, an encrypted identifier is stored in this tag. The steps of the process are illustrated in Fig.4.

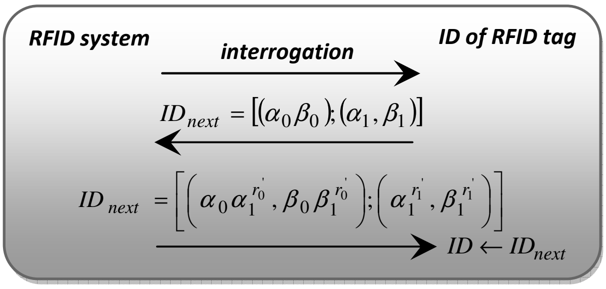
RFID system
ID of RFID tag
interrogation
$ID_{next} = [(\alpha_0 \beta_0); (\alpha_1, \beta_1)]$
$ID_{next} = \left[\left(\alpha_0 \alpha_1^{r_0^{'}}, \beta_0 \beta_1^{r_0^{'}} \right); \left(\alpha_1^{r_1^{'}}, \beta_1^{r_1^{'}} \right) \right]$
$ID \leftarrow ID_{next}$

Fig.4 RFID privacy protocol proposed by Golle, Jakobsson, Juels and Syverson

The identifier encrypted and a secret key related to tag are stored into the database. The reader sends an interrogation towards the tag; the tag sends its identifier just encrypted; the reader re-encrypts the identifier of tag, by the help of universal re-encryption scheme. In the end, the reader will send a new value towards the tag.

If an adversary sends a false re-encrypted identifier to the tag, the database of the system will not be able to identify that tag anymore. Golle, Jakobsson, Juels şi Syverson emphasized that by using their protocol, such an attack will not detect the tag, but yet will affect the operating of the system. Weak points: an adversary can replace a tag identifier, with a value encrypted by the adversary under an own adversary public key. Like this, the potential adversary will be capable of decrypting the tag and detect it. A solution of avoiding such attacks assumes the utilization of cryptographic primitives. A possible attack will be analyzed as following:

- *Presumable attack based upon invariant functions.* Each item of a ciphertext $[(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ meets a uniform distribution scheme, with the assignation that a random function is represented by the discrete logarithm, and these items will not be independent. Let one consider $\left[\left(\alpha_0^{(i)}, \beta_0^{(i)} \right); \left(\alpha_1^{(i)}, \beta_1^{(i)} \right) \right]$ as an answer message sent by tag during identification *i.* In case $\left[\left(\alpha_0^{(i)}, \beta_0^{(i)} \right); \left(\alpha_1^{(i)}, \beta_1^{(i)} \right) \right]$ meets the property *P*, meaning it is an invariant function by re-encryption, then the adversary is about to detect the targeted tag. Such a potential attack looks like: given $\left[\left(\alpha_0^{(i)}, \beta_0^{(i)} \right); \left(\alpha_1^{(i)}, \beta_1^{(i)} \right) \right]$ meets *P* if and only if $\alpha_1 = \beta_1$. In the situation of $\left[\left(\alpha_0^{(i)}, \beta_0^{(i)} \right); \left(\alpha_1^{(i)}, \beta_1^{(i)} \right) \right]$ meets *P,* then $\left[\left(\alpha_0^{(i)}, \beta_0^{(j)} \right); \left(\alpha_1^{(i)}, \beta_1^{(j)} \right) \right]$ will meet *P* in the same way for any $j \geq 1$. This deterministic procedure is applied for α_1 and β_1 while re-encryption, which means that α_1 and β_1 will be raised by a known power order $r_1^{'}$. For detecting a tag, a potential adversary will interrogate this tag and will send the message $ID_{next} = [(a,b); (c,c)]$. Here, *a, b* and *c* might have any values. Next time the adversary interrogates the tag and receives a message under the form of $\left[\left(\alpha_0^{(i)}, \beta_0^{(i)} \right); \left(\alpha_1^{(i)}, \beta_1^{(i)} \right) \right]$, this adversary will also verify if $\alpha_1^{(i)} = \beta_1^{(i)}$. Considering this view, the interrogated tag represents the target of the adversary, in high percentage of probability. One has to see that a tag might be able to detect such an attack, by simply testing that ID_{next} does not meet *P*. There are some invariant functions related to property P', for instance: $\left[\left(\alpha_0^{(i)}, \beta_0^{(i)}\right), \left(\alpha_1^{(i)}, \beta_1^{(i)}\right)\right]$ meets P' if and only if $\alpha_1^{(i)} \cdot \beta_1^{(i)} = 1$ related to *G*.

2.3 The RFID protocol proposed by Juel based upon XOR

Carrying out an evaluation on the second RFID protocol proposed by Saito, Ryou and Sakurai, meaning RFID privacy protocol with one time pad, one might mention that a tag's identifier is updated from a list of values randomized. Updating the list is accomplished by the help of the reader, once in a while. This approach of updating was taken into account by Juel's protocol based upon XOR [1]. The protocol assigns the storing of pseudonyms, denoted as a list under the form $\alpha_{1,\ldots,}\alpha_k$.

Every time a tag is interrogated by a reader, this will use a new pseudonym, by a cyclical method at the beginning of the list and after *k* successive identifications. One might notice that only few pseudonyms can be stored, since the memory of tags is limited. Each pseudonym α_i is assigned with two random values β_i and γ_i, stored within tag. The tag and the system include *k* structures of (α_i , β_i , γ_i) type. A vector of *m* random values is assigned to every *k* values.

Fig.5 illustrates the following scenario: if a reader interrogates a tag while identification (*i+1*), this will send to RFID system a value under the form of $\alpha_{(i \bmod k)+1}$; i is stored into the *c* counter that has zero value, at first. The system will search a value of $\alpha_{(i \bmod k)+1}$ into its database. If this is here, the system will answer by sending $\beta_{(i \bmod k)+1}$. In the next step, the tag will send $\gamma_{(i \bmod k)+1}$ towards the RFID system. This value is checked for validity of expectation, and if it complies, *3k* vectors of *m* new random values will be sent; in this way, the values represented by $\alpha_i s$, $\beta_i s$ and $\gamma_i s$ will be refreshed. In order to update the value Δ_κ, one might consider that *k* is such value, that the vector specific to *k* is represented by $\Delta_\kappa = \left(\delta_\kappa^{(1)}, \ldots \delta_\kappa^{(1)}\right)$, and that the vector sent as answer by the system is $\tilde{\Delta}_\kappa = \left(\tilde{\delta}_\kappa^{(1)}, \ldots \tilde{\delta}_\kappa^{(m)}\right)$ [1]. Equation (4) demonstrates that, knowing that $1 \le i \le m$, the phases of renewal will be:

$$\delta_\kappa^{i} \leftarrow \delta_\kappa^{(i+1)} \oplus \tilde{\delta}_\kappa^{(i)}, \ \delta_\kappa^{m} \leftarrow \tilde{\delta}_\kappa^{(m)}, \ \kappa \leftarrow \kappa \oplus \delta_\kappa^{(1)} \quad (4)$$

This protocol proves more weak points, rather that strong ones. Yet, the protocol can be used only for simple and powerless adversary models, such as: bounded successive interrogations towards the tag or bounded successive interactions intercepted between tags and readers [1]. This paper emphasizes that Juel's protocol based upon XOR proves to be inefficacy. A potential adversary can destroy completely the scheme proposed; the interception procedure will determine tags to be definitively detectable. This potential attack relies on finding the pseudonyms of a tag which might be easily detected. Interrogating at least *k* times the RFID tag, searching of pseudonyms can be accomplished. The threatening exists as long as an adversary is able to carry out a procedure of interception the communications between tags and readers. After that, the RFID system and the tag will be desynchronized, which signifies that system will not be able to search for tag's pseudonyms within its database. As result, the pseudonyms will not be updated anymore, and will become easily detectable.

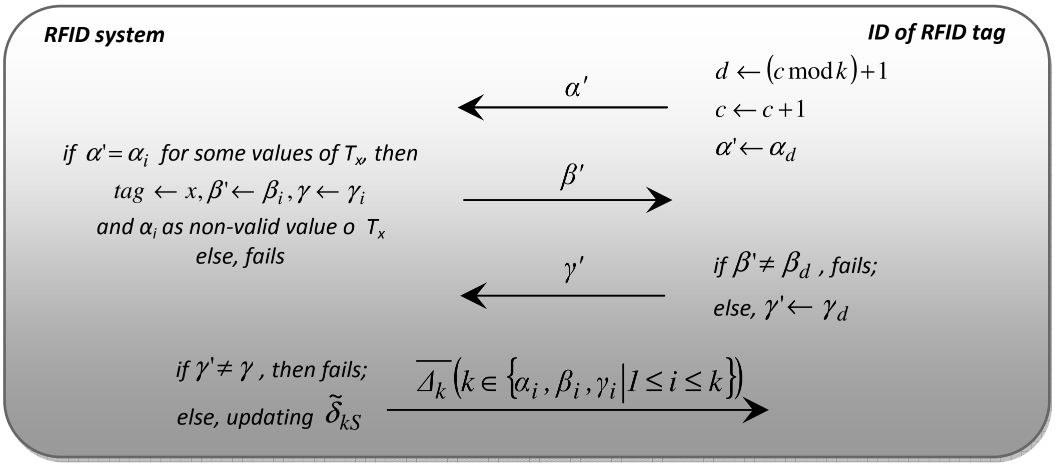
RFID system
ID of RFID tag
$d \leftarrow (c \bmod k) + 1$
$c \leftarrow c + 1$
$\alpha' \leftarrow \alpha_d$
α'
if $\alpha' = \alpha_i$ for some values of T_x, then
$tag \leftarrow x, \beta' \leftarrow \beta_i, \gamma \leftarrow \gamma_i$
and α_i as non-valid value o T_x
else, fails
β'
γ'
if $\beta' \neq \beta_d$, fails;
else, $\gamma' \leftarrow \gamma_d$
if $\gamma' \neq \gamma$, then fails;
else, updating $\tilde{\delta}_{kS}$
$\overline{\Delta_k}\left(k \in \{\alpha_i, \beta_i, \gamma_i \mid 1 \le i \le k\}\right)$

Fig.5 RFID privacy protocol proposed by Juels based on XOR

2.4 The RFID protocol proposed by Saito, Ryou and Sakurai

An evaluation will be accomplished, as concerns a comparison of this protocol with the protocol proposed by Golle, Jakobsson, Juels and Syverson, which proved some weak points. After this comparison, one will emphasize a potential attack against the Golle, Jakobsson, Juels and Syverson's protocol, as seen in Fig.6. Saito, Ryou and Sakurai proposed two RFID protocols, as follows:

- *RFID privacy protocol with one check.* The goal consists in detecting a potential adversary, which might send an erroneous identifier re-encrypted [13]. In this way, when a tag is interrogated, this will send its identifier $[(\alpha_0,\beta_0);(\alpha_1,\beta_1)]$ and will receive a new value, under the form of $\left[\left(\alpha_0^{'},\beta_0^{'}\right);\left(\alpha_1^{'},\beta_1^{'}\right)\right]$. Considering x the private key of the tag, and in the situation of $\left|\alpha_0^{'}\right|,\left|\beta_0^{'}\right| \neq 1$ and $\alpha_0^{'} \big/ \beta_0^{'}{}^{x} = 1$, then the form $\left[\left(\alpha_0^{'},\beta_0^{'}\right);\left(\alpha_1^{'},\beta_1^{'}\right)\right]$ will be calculated as the new identifier. If this is not true, the RFID tag will not update its content.
- *RFID privacy protocol with an algorithm of one time pad encryption (abbreviated OTP).* This protocol also relies on the universal re-encryption scheme. It is assumed that an RFID tag includes an identifier under the form of $ID = [(\alpha_0,\beta_0);(\alpha_1,\beta_1)]$. This includes also a known list of random values $\Delta = \left(\left(\alpha_1^{r1},\beta_1^{r1}\right),\left(\alpha_1^{r2},\beta_1^{r2'}\right),...\right)$. The tag includes a variable *k*, meaning the number of a given session, and a secret, abbreviated by *S*. Two different operations will be carried out by this protocol: the reader sends an interrogation towards the tag; knowing that $\left(\alpha_1^{r_k},\beta_1^{r_k}\right),\left(\alpha_1^{r_{k+1}},\beta_1^{r_{k+1}}\right) \in \Delta$, (5) shows that the tag sends an answer with its ID and will replace the identifier with the following form:

$$ID_{next} := \left[\left(\alpha_0\alpha_1^{r_{k+1}},\beta_0\beta_1^{r_k}\right);\left(\alpha_1\alpha_1^{r_{k+1}},\beta_0\beta_1^{r_{k+1}}\right)\right] \quad (5)$$

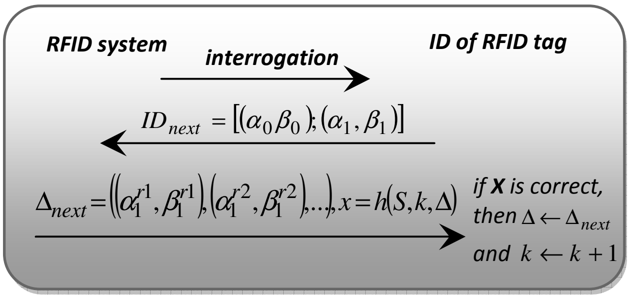
RFID system
ID of RFID tag
interrogation
$ID_{next} = [(\alpha_0\beta_0);(\alpha_1,\beta_1)]$
$\Delta_{next} = \left(\left(\alpha_1^{r1},\beta_1^{r1}\right),\left(\alpha_1^{r2},\beta_1^{r2}\right),...\right), x = h(S,k,\Delta)$
if **X** is correct, then $\Delta \leftarrow \Delta_{next}$ and $k \leftarrow k+1$

Fig.6 RFID privacy protocol proposed by Saito, Ryou and Sakurai

Knowing the *h* (hash function) and in case an update of Δ is required, the reader will send towards the tag a new list Δ_{next} of random values and also key represented by $X = h(S,k,\Delta)$.

The tag will replace Δ with Δ_{next} and will increase the number *k* of the session, if this key is correct.

- *Presumable attack based upon private keys.* An adversary interrogates the tag and achieves an identifier $[(\alpha_0,\beta_0);(\alpha_1,\beta_1)]$. After that, an interrogation will occur: the adversary gets a value $\left[\left(\alpha_0^{'},\beta_0^{'}\right);\left(\alpha_1^{'},\beta_1^{'}\right)\right]$ and sends again to the tag a value under the form of $[(\alpha_0,\beta_0);(\alpha_1,\beta_1)]$, instead of sending the re-encrypted value $\left[\left(\alpha_0^{'},\beta_0^{'}\right);\left(\alpha_1^{'},\beta_1^{'}\right)\right]$ [8].

In this situation, the adversary interrogates again the tag. If the answer received by the adversary is still $\left[\left(\alpha_0^{'},\beta_0^{'}\right);\left(\alpha_1^{'},\beta_1^{'}\right)\right]$, it signifies that the adversary is not targeting the desired tag or the tag did not refresh its identifier. The detected tag would have seen a valid value in $[(\alpha_0,\beta_0);(\alpha_1,\beta_1)]$, encrypted by the public key; in this way, the tag would have used it for its identifier.

- *Presumable attack based upon desynchronizing the database of RFID system.* An adversary can provoke easily a desynchronization process between tags and database. Making a comparison, the protocol proposed by Henrici and Muller described in this paper handles significant methods of avoiding such attacks.

2.5 The RFID protocol proposed by Ohkubo, Suzuki and Kinoshita

The protocol proposed by Ohkubo, Suzuki and Kinoshita [11] uses a hash function. Attacks coming from adversaries that track and trace the identifiers of transponders can be avoided if transponders are updated at the new identifications, by the help of secondary hash functions.

- *Analysis of the Identification Protocol and Its Modification*

This aspect would be able to ensure the privacy of RFID systems. Because the transponders will have to calculate two hash functions at the new identifications, their cost will be increased, also. The protocol proposed by Ohkubo, Suzuki and Kinoshita is illustrated in Fig.7. The two hash functions that will be used are noted with *G* and *H*. Storing a randomized identifier s^1 in the memory of a tag, denoted with T_i, signifies its customization; this identifier is stored under the form of *ID* into the database of RFID system. A set $\{s_i^1 | 1 \leq i \leq n\}$ of random values will be first included within the database.

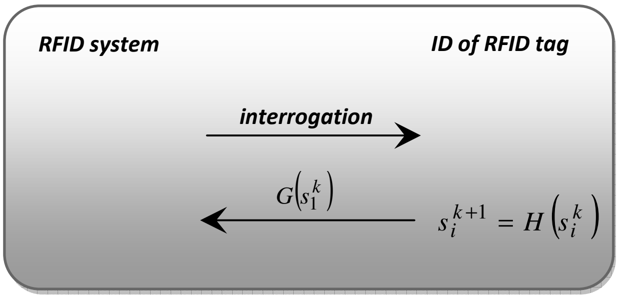

Fig.7 Protocol of identification of Ohkubo, Suzuki and Kinoshita

When the RFID system interrogates the tag T_i, this will receive from tag the form $r^k = G(s^k)$ or $r_i^k := G(s_i^k)$ where s^k or s_i^k signify the tag's identifier. The tag will replace s^k or s_i^k with $s^{k+1} = H(s^k)$ or $s_i^{k+1} := H(s_i^k)$ after is powered by the reader. Starting with r^k or r_i^k , the RFID system will define the tag corresponding to it. In this way, the reader will create hash connections of all initial values noted with *n,* until this will discover the form r^k or r_i^k waited, or will obtain a limited value *m* maximum on the length of the hash connection. The RFID tag's life duration will be restricted to *m* identifications.

If a tag is read by an authentic reader, this tag will be updated in the system's database. In this way, the number of operations read on a single RFID tag between two authentic identifications is represented by the value *m.* As mentioned in [15], the protocol proposed by Ohkubo, Suzuki and Kinoshita can be transformed into a protocol of authentication, as illustrated in Fig.8. One might emphasize the most important strong point of this protocol: it ensures subsequent privacy, but still faces difficulties as concerns the replaying attacks over the RFID system, as depicted in Fig.8.

- *Modifying the Identification Protocol through the Mutual Authentication*

Most of the ordinary methods for facing such attacks are based on clock type synchronization, on new challenges transmitted by system's database and on the incremental number of a sequence. New challenges transmitted by the system's database are forwards emphasized. Authentication of the RFID reader can be ensured by the next method: besides the two messages, another one will be added, under the form of $G(s^{k+1} \oplus w)$; *w* signifies a binary string, fix, public and with no zeros. The explanations are illustrated in Fig.9, where a procedure of mutual authentication is used for modifying the protocol proposed by Ohkubo, Suzuki and Kinoshita.

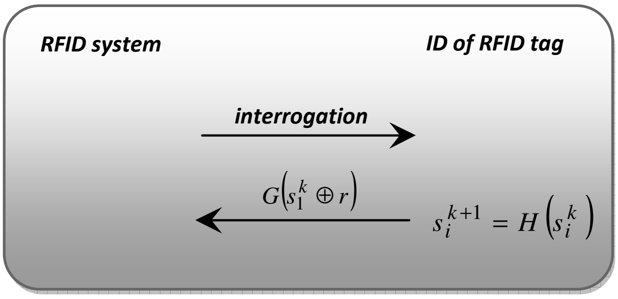

Fig.8 Modifying the identification protocol of Ohkubo, Suzuki and Kinoshita

The authors Ohkubo, Suzuki and Kinoshita outlined a transformation over their proposed scheme [14]. With the aim of reducing the complexity of RFID systems, including the complexity of RFID tags, these authors found two solutions: of using a value *c* (signifying a counter value) and applying *H* (the hash function), in situations when *c* achieves a superior bound; the second solution aimed towards not taking into account and not applying the *H* hash function to all tag's interrogations. One might see that this method brings weak points over the privacy of the RFID system. Potential adversaries can detect *c* values; moreover, when tags are interrogated, the *c* values of the counter will be transmitted to RFID reader and therefore, the tags might be immediately tracked and traced by adversaries.

Some measures of avoiding the replaying attacks over the RFID structures are forwards described. The protocol proposed by authors Ohkubo, Suzuki and Kinoshita can ensure privacy and security at a certain level, when data transmitted towards tags are random. One may outline a strong point of this protocol, as comparing to other protocols of identification and authentication [2]. The protocol of Ohkubo, Suzuki and Kinoshita ensures subsequent privacy of the RFID system, meaning: if presumable adversaries are tampering with RFID tags, the adversaries will not be able to detect the previous events.

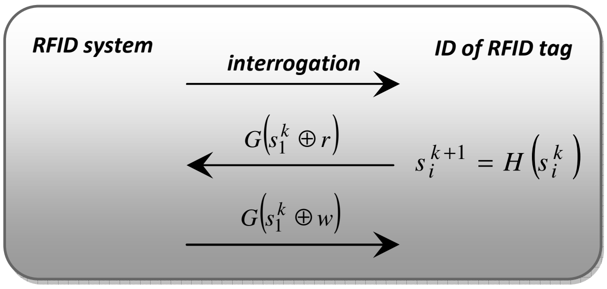

Fig.9 Modifying the identification protocol proposed by Ohkubo, Suzuki and Kinoshita through mutual authentication

A weak point of this protocol consists in the fact that it is not able to avoid or caution against replaying attacks coming from potential adversaries. Another weak point is that this protocol cannot ensure the authentication of RFID readers. Analyzing the efficiency point of view of this protocol, the RFID tags can be interrogated by readers existing outside the initial system taken into account. This aspect will provide avoidance, as regards the synchronization process between tags and systems.

The difficulty brought by hash functions in the view of identifying a tag will rely upon an average value. Considering that two hash operations will be executed of *mn/2* times, one might use for the average value the next formula: $t_{OSK} = mn\theta$. The difficulty assumed in such way would increase up to the value of *2mn*, in situations when RFID readers might read foreign tags; if this is the case, the RFID system will search throughout its entire database in the view of detecting its tags. Thinking of the aspect of synchronization, if the RFID tags and readers are capable of synchronization, solutions of providing higher memory capacity towards the RFID system should be taken into consideration.

2.6 The RFID protocol proposed by Juels and Weis

According to the specialty literature, some authors have proposed RFID protocols that are not based either upon hash functions or upon pseudo-randomized functions. One of these authors is represented by Weis [5], which approached such protocol. The protocol of Weis is based on a protocol of human authentication proposed by Hopper and Blum, denoted with HB [7]; in this way, Weis's protocol is outlined by means of *AND* and *XOR* operations.

- *The protocol proposed by Juels and Weis with a sequence of HB^+*

A device with limited resources is assigned as the RFID tag. Such device is sharing information of an *x* vector on *l* bits with a system's database of the RFID structure. The operations are described as follows: *(a)* the system's database chooses the randomized vector *a*, expressed under the form of $a \in \{0,1\}^l$ and will transfer this vector to the RFID tag; *(b)* the inner binary product will be calculated by the RFID tag; *(c)* the result will be sent to system's database, which verifies the validity of operation.

Weis explained that a correct answer is represented by probability of value 1 (signifying a correct RFID tag) and a wrong answer is represented by a probability lower than ½ (signifying a harmful RFID tag). If this procedure is repeated *k* times, the author outlined that a harmful RFID tag cannot provide a successful probability higher than the value 2^{-k}.

Analyzing all these, one might emphasize that using such protocol, the potential adversaries might be able to intercept authentic communications, denoted by *O(l)*, between tags and system's database; in this way, adversaries might discover the *x* vector. So as to prevent presumable attacks, tags can transmit incorrect results of probability of value η, with $\eta \in [0,1/2]$; therefore, passive adversaries will not be able to discover the secret of *x* vector. The protocol proposed by Hopper and Blum, denoted with *HB*, has proven weak points of resistance as regards the presumable active adversaries. The concept of *active adversaries* refers to adversaries permitted to interrogate RFID tags; only after such interrogation, these adversaries are permitted to communicate with authentic RFID readers. Fig.10 illustrates the procedure applied by protocol HB^+ of Juels and Weis.

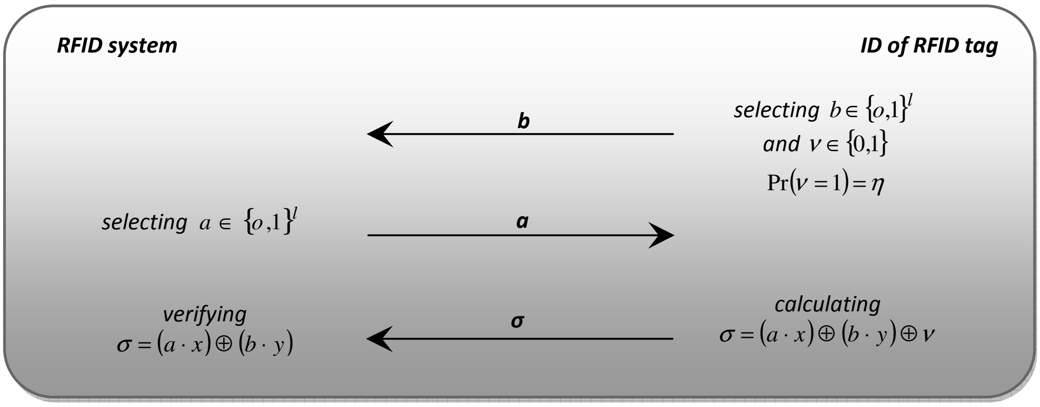
RFID system
ID of RFID tag
b
selecting $b \in \{o,1\}^l$
and $v \in \{0,1\}$
$\Pr(v = 1) = \eta$
selecting $a \in \{o,1\}^l$
a
verifying
$\sigma = (a \cdot x) \oplus (b \cdot y)$
σ
calculating
$\sigma = (a \cdot x) \oplus (b \cdot y) \oplus v$

Fig.10 RFID protocol proposed by Juels and Weis with a sequence of HB^+

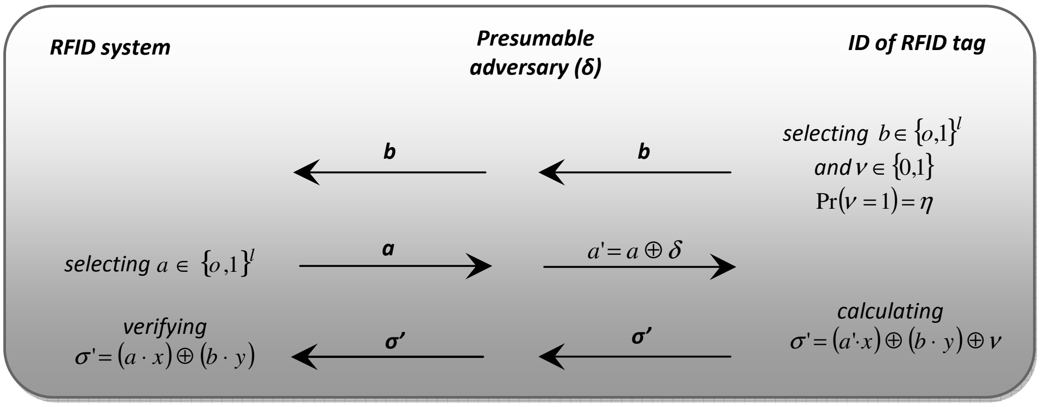
RFID system
Presumable adversary (δ)
ID of RFID tag
selecting $b \in \{o,1\}^l$
and $v \in \{0,1\}$
$\Pr(v=1)=\eta$
b
b
selecting $a \in \{o,1\}^l$
a
$a' = a \oplus \delta$
verifying
$\sigma' = (a \cdot x) \oplus (b \cdot y)$
σ′
σ′
calculating
$\sigma' = (a' \cdot x) \oplus (b \cdot y) \oplus v$

Fig.11 Presumable attacking proposed by Gilbert, Robshaw and Sibert on HB^+ protocol

The storage of the two randomized vectors, assigned as *a* and *b*, in the memory of the tag and within RFID system's database signify the process of RFID tag's customization; it is also assumed that RFID tag comprises a probability of value *η*, with$\eta \in [0,1/2]$. The aim of active adversaries consists in introducing false tags within RFID systems. The authors Juels and Weis [7] proposed a version of the *HB* protocol, assigned under the form of HB^+; this new version proved resistance to active adversaries attacking the RFID system. Here, the tags choose a randomized vector denoted with *b*, which is transmitted towards the system's database. An authentication procedure of sequence *k* will be initialized in the moment of interrogating a tag.

For every separate sequence, the tag will choose and transmit a randomized vector denoted by *b* to the RFID system; then, the tag will receive an answer expressed under the form of a randomized vector denoted by *a*.

Taking into account these two vectors and after the calculations, the tag will transmit to the system a form expressed by$\sigma = (a \cdot x) \oplus (b \cdot y) \oplus \upsilon$; here, *υ* belongs to$\{0,1\}$, so that$\Pr(\upsilon = 1) = \eta$. Forwards, one may observe that a sequence will be fault in the case of$\sigma \neq (a \cdot x) \oplus (b \cdot y)$. After *k* sequences, the procedure of authentication will be correct if less than *ηk* sequences are fault.

- *Outlining presumable attacks on RFID systems that adopt the HB^+ protocol*

Forwards, an analysis over attacks that might endanger the RFID systems using HB^+ protocol will be carried out. Authors Juels and Weis [7] assumed some demonstrations about the security brought by their protocol against active adversaries. Over the time, many authors proposed solutions of attacking RFID systems that use various protocols of privacy and security. Their attacking method is illustrated in Fig.11.

For instance, authors Gilbert, Robshaw and Sibert [5] presented a potential attack that might occur over RFID systems using HB^+ protocol. In this way, weak points of HB^+ protocol will be forwards explained: let one assume a RFID system, and between an authentic tag and an authentic reader, a man-in-the-middle type attack might occur; the assumption that an adversary can see the probability of successfully detecting a tag is also taken into account. Attacking procedure looks in the following way: vector *a* transmitted by the reader will be disturbed by *XOR* operation, using an interference vector *δ* on *l* bits; this vector of interference will be used for all sequences *k*. Two cases might occur: *(a)* the method of authentication is successful, signifying that$\delta \cdot x = 0$; *(b)* the method of authentication is not successful, which means$\delta \cdot x = 1$.

Accomplishing this attacking procedure of many times, for instance *l* times, the secret *x* vector can be discovered, since the vectors denoted by *δ* are linear independent. Such attacking methods over RFID systems can be pretty simple to carry into effect, fact emphasizing weak points of the proposed protocol. RFID protocols face various complexity problems; RFID systems have to search far-reaching the identifiers of its tags, so as to authenticate them. Such methods involve high efforts as regards the time, but also high costs as regards the calculations. Methods proposed in [7] do not prove security as concerns the real attacking patterns.

2.7 The RFID protocol proposed by Weis, Sarma, Rivest and Engels

The protocol of Weis, Sarma, Rivest and Engels [5] outlines the data sent by RFID tags, when they are interrogated. The corresponding data are represented by a randomized value *a* and a hash value represented by $\sigma = h(ID \| a)$ and randomized.

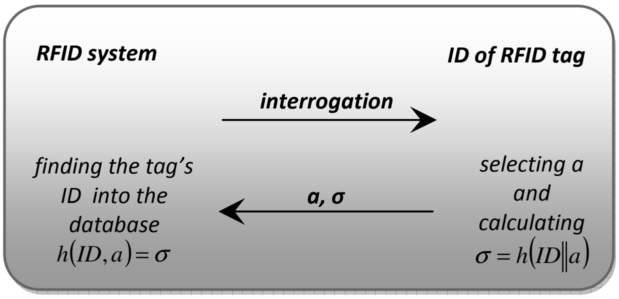
RFID system
ID of RFID tag
interrogation
finding the tag's ID into the database $h(ID,a)=\sigma$
a, σ
selecting a and calculating $\sigma = h(ID\|a)$

Fig.12 RFID privacy protocol proposed by Weis, Sarma, Rivest and Engels applying hash type functions

ID signifies the tag's static identifier. The RFID tag would need a generator of pseudo-randomized numbers in the view of calculating the data sent by the RFID tag, as well as a function of one way hash type, as seen in Fig.12, which will store its related *ID*. Stages proposed by this protocol will be forwards explained: *(a)* the RFID tags will be initialized with *ID* identifiers, selected in a random way. For all tags managed by the RFID system, the identifiers of tags will be stored into the system's database; *(b)* the RFID system will interrogate a tag; then, the tag will select a randomized value *a* and will calculate the form $\sigma = h(ID\|a)$; the values *a* and *σ* are sent by towards RFID system; *(c)* after the stage of receiving values *a* and *σ*, the RFID system will carry out searches into its database; the searching is accomplished by calculating the form $\sigma = h(ID\|a)$ for all identifiers, step by step, until the value *σ* is discovered. Taking into account that hash functions ensure irreversibility, and not privacy, the authors proposing this protocol pointed out that input bits can be anytime discovered. Fig.13 illustrates the modifications approached by the new structure. The authors also proposed another type of structure, based on pseudo-randomized functions; in such structure, the RFID tag will share with the database a secret value denoted by *s*.

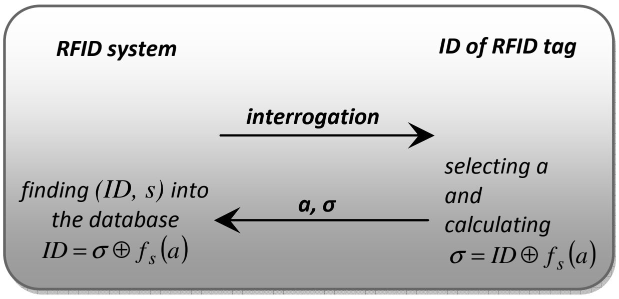
RFID system
ID of RFID tag
interrogation
finding (ID, s) into the database $ID = \sigma \oplus f_s(a)$
a, σ
selecting a and calculating $\sigma = ID \oplus f_s(a)$

Fig.13 RFID privacy protocol proposed by Weis, Sarma, Rivest and Engels applying pseudo-randomized type functions

In this situation, the tag will not send *a* and $h(ID\|a)$, but a value represented by *a* and $ID \oplus f_s(a)$; f_s signifies a pseudo-randomized function, which was selected from a set represented by the form $F = \{f_s\}_{s\in N}$.

2.8 The RFID protocol proposed by Feldhofer, Dominikus and Wolkerstorfer

A RFID privacy protocol based on replacing the pseudo-randomized function by an Advanced Encryption Standard (denoted by *AES*) was proposed by Feldhofer, Dominikus and Wolkerstorfer [16]. The following stages are illustrated in Fig.14: *(a)* all RFID tags are initialized with a value *s,* which represents a secret key, randomly selected and stored together with the tag's ID by the RFID system; *(b)* the RFID system will select a random number, denoted by *a*; then, the system will send an interrogation to the RFID tag; this interrogation contains the value *a*; after receiving this interrogation, the RFID will select a random number, denoted by *b;* the tag will also calculate the value $\sigma = AES_s(a,b)$ that is going to be sent towards the RFID system. The authors also proposed a structure in two stages for this protocol, based on mutual authentication, as Fig.15 illustrates. When the value *s* was discovered to be valid, meaning that tags are identified by the RFID system, the value $\tau = AES(b,a)$ will be calculated and will be sent towards the RFID tag; at this stage, the tag will verify if τ signifies a true encryption of the values *a* and *b*, in other words, if the RFID reader is authentic; *(c)* the RFID system will carry out full searching into its database for all entries denoted by *ID*, after receiving the value *σ*, meaning that the system will calculate the form $AES_s^{-1}(\tau)$, until a valid decryption will be discovered.

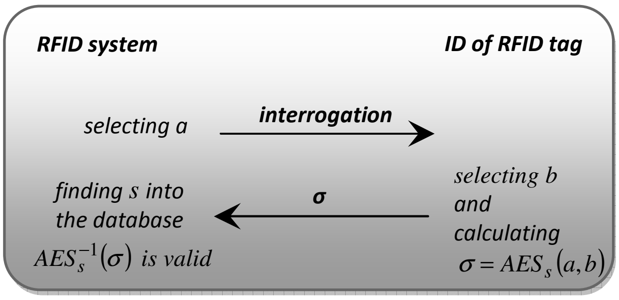
RFID system
ID of RFID tag
selecting a
interrogation
finding s into the database $AES_s^{-1}(\sigma)$ is valid
σ
selecting b and calculating $\sigma = AES_s(a,b)$

Fig.14 RFID protocol of authentication proposed by Feldhofer, Dominikus and Wolkerstorfer

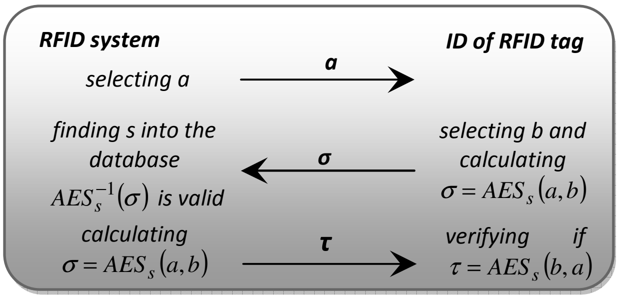

Fig.15 RFID protocol of mutual authentication proposed by Feldhofer, Dominikus and Wolkerstorfer

The following situation should be taken into account: [16] does not outline if the value *s,* which represents a secret key, has been involved into calculations for all RFID tags. In the affirmative situation, the tags will store the corresponding ID, which should be encrypted together with the values denoted by *a* and *b*.

2.9 The RFID protocol proposed by Rhee, Kwak, Kim and Won

A protocol of authentication based upon a hash function was proposed by Rhee, Kwak, Kim and Won [8]. The stages of their protocol can be analyzed in accordance to Fig.16 and are forwards described: *(a)* all RFID tags are initialized by identifiers *ID*, selected in a random way. Complexity problems have proven to be subsistent, as concerns the symmetric cryptographic applications. Identifiers will be stored into the database of the RFID system; *(b)* a value denoted by *a* will be selected and sent by the RFID system towards the tag; the tag will select a value denoted by *b* and will calculate the form $\sigma = h(ID,a,b)$ after receiving the message; then, the tag will transmit the values *b* and σ to the RFID system; when the system identifies a tag, this will calculate $\tau = h(ID,b)$ and will send this value to the tag.

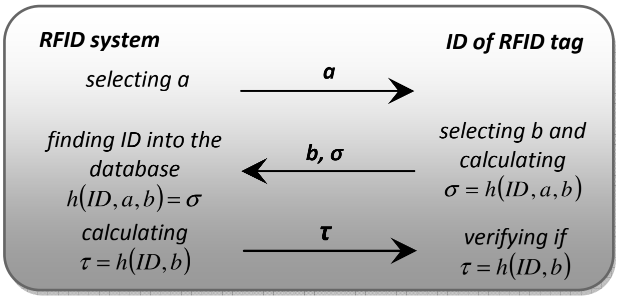

Fig.16 RFID protocol of mutual authentication proposed by Rhee, Kwak, Kim and Won

Knowing the values *ID* and *b,* the RFID tag will verify the validity of τ, meaning the authenticity of the RFID reader. In this way, the mutual authentication can be outlined, as according to [8]; *(c)* the system will carry out searches into its database, after the receiving of σ; meaning that for all entries represented by *ID*, the system will calculate the form signified by $h(ID,b)$, until the value denoted by σ will be discovered. These problems are discussed in [5], taking into account that *AND* and *XOR* operations are preferable towards other types of functions, as hash or pseudo-randomized functions [7, 14, 15].

3 Conclusions

Radio Frequency Identification signifies an advanced wireless technology, which integrates essential solutions within fields of intelligent chips and automation technologies. Analyzing the Radio Frequency Identification applications, one might emphasize two hierarchies: levels aiming to offer security to RFID structures and levels aiming to offer functionality, but no security issues.

In this paper, nine protocols based on updating the tags' identifiers by using RFID readers are compared, so as to accomplish an analysis over the harmful points that are threatening the security and privacy of RFID systems [1, 3]. A chaotic matter is brought into discussion, by the following thoughts: to discover what type of identification and authentication protocols are most appropriate on various RFID structures.

Analyzing these conditions over RFID protocols of security and privacy has carried out wide approach. An essential matter on establishing and designing the RFID protocols consists in defining their aim. Authors that proposed these protocols focused too much over theoretical justifications of the potential adversaries, and not too real patterns. In other situations, the threatening is the result of designing weak protocols.

Within trade area, RFID technology can successfully replace the bar codes, offering additional facilities. An RFID implementation that assigns nowadays high expenses will become approachable in the future [2, 9]. This paper brings into attention an approach over the concepts of security and privacy assumed by feasible RFID systems. Specific ways of comparison and analysis amongst nine already existing protocols are also accomplished. By finding the best security and privacy solutions, the use of RFID systems will determine visibility in developing business or logistics processes [12], in an adequate way and of complete transparency [11]. At the end of each description, solutions of treating the jeopardizing points are emphasized. Working with RFID protocols involves more stages: *(a) stages of installation*: the system's database and the RFID transponders are established and initialized; *(b) stages of communication*: the system's database and the RFID transponders communicate and interact; *(c) stages of searching*: the RFID system searches in its database the identifiers of transponders.

Some threatening parts against the RFID technology can be brought into mind: relay attack and impersonation, leakage of information or anticipation of traceability. The privacy issues cannot be handled by using only the classical theoretical methods, but rather by including the privacy issues within communication methods as an entire, starting with the physical level up to the application level. Radiofrequency identification brings into analysis, as any other technologies in progress, some security issues. In many applications, the high cost of RFID technology will be balanced out by reaching the best solutions and results.

References:

[1] A. Juels, Minimalist cryptography for low-cost RFID tags, *International Conference on Security in communication Networks – SCN 2004,* Volume 3352 of *Lecture Notes in Computer Science*, 2004, pp. 149-164.

[2] C. Hurjui, A. Graur, C.O. Turcu, Monitoring the Shopping Activities from the Supermarkets based on the Intelligent Basket by using the RFID Technology, *The Journal "Electronics and Electrical Engineering"*, Lithuania, No. 3 (83), 2008, pp. 7-10.

[3] X. Huang , Scrutinizing Behavior of a Dynamic Framed Slotted Anti-collision Algorithm for RFID Systems, *7th WSEAS Int. Conference on Applied Computer & Applied Computational Science (ACACOS '08)*, Hangzhou, China, April 6-8, 2008, pp. 112- 115.

[4] S. Srinivasan, Akshai Aggarwal, Anup Kumar, RFID Security and Privacy Concerns, *Proceedings of the 4th WSEAS International Conference on Information Security, Communications and Computers*, Tenerife, Spain, December 16-18, 2005, pp.69-74.

[5] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and privacy aspects of low-cost radio frequency identification systems, *International Conference on Security in Pervasive Computing – SPC 2003,* pp. 454-469.

[6] S. Garfinkel, B. Rosenberg, *RFID: Applications, Security and Privacy,* Addison Wesley Professional, 2005.

[7] A. Juels and S. Weis, Authenticating pervasive devices with human protocols, *Proceedings of Advances in Cryptology,* CRYPTO'05, California, USA, August 2005, pp. 293-308.

[8] I. Ray, In. Ray, An optimistic fair exchange e-commerce protocol with automated dispute resolution*, Electronic Commerce and Web Technologies, EC-Web 2000,* London, United Kingdom, 2000, pp. 84-93.

[9] Z. Hu, Z. Jian, S. Ping Z. Xiaoshuan, M. Weisong, Modeling Method of Traceability System based on Information Flow in Meat Food Supply Chain, *WSEAS Transactions on Information Science and Applications*, Issue 7, Volume 6, July 2009, pp. 1094-1103.

[10] N. Amin, P. Weng Lin, Anti-collision Protocol Development for Passive RFID Tags, *Proceedings of the 7th WSEAS International Conference on Applied Informatics and Communications*, Athens, Greece, August 24-26, 2007, pp. 393-397.

[11] C. Hurjui, C. Turcu, A. Graur, Management system of the products on warranty based on RFID technologies, *Proceedings of the 11th International Conference on Optimization of Electrical and Electronic Equipment – Optim*, 2008, pp. 231-236.

[12] R-S. Chen, C-C. Chen, K.C. Yeh, Y-C. Chen, and C-W Kuo, Using RFID Technology in Food Produce Traceability, *WSEAS Transactions on Information Science and Applications,* Volume 5, Issue 11, 2008, pp. 1551-1560.

[13] P. Golle, M. Jakobsson, A. Juels, P. Syverson. Universal re-encryption for mixnets, *The Cryptographers'Track at RSA Conference-CT-RSA,* California, USA, 2004, pp. 163-178.

[14] D. Molnar, A. Soppera, D. Wagner, A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags, *Handout of the Encrypt Workshop on RFID and Lightweight Crypto*, July 2005.

[15] A. Juels, R. Rivest, M. Szydlo, The blocker tag: Selective blocking of RFID tags for consumer privacy, *Proc. Computer and Communications Security – CCS'03*, Washington, DC, USA, 2003, pp. 103-111.

[16] K. Finkenzeller, *RFID Handbook*, Wiley, England, second edition, 2003.