Improved RFID Authentication Protocol Based on Randomized McEliece Cryptosystem

Noureddine Chikouche[1], Foudil Cherif[2], Pierre-Louis Cayrel[3], and Mohamed Benmohammed[4]

(Corresponding author: Noureddine Chikouche)

Computer Science Department, Mohamed Boudiaf University of M'sila[1]

BP 166 ichebilia, 28000 M'sila, Algeria

(Email: chiknour28@univ-msila.dz)

Computer Science Department, LESIA Laboratory, Mohamed Khider University of Biskra[2]

BP 145 RP, 07000 Biskra, Algeria

Laboratoire Hubert Curien, UMR CNRS 5516[3]

Bâtiment F18 rue du professeur Benoît Lauras, 42000 Saint-Etienne, France

LIRE Laboratory, University of Constantine 2[4]

P.O. Box 325, City Ain El Bey 25017 Constantine, Algeria

(Received Dec. 15, 2014; revised and accepted Apr. 2 & Apr. 17, 2015)

Abstract

Among the embedded systems which were quickly developed during the last years and that were used in various domains (e.g. access control, health, ...) we can cite radio frequency identification (RFID). In this paper, we propose an improved mutual authentication protocol in RFID systems based on the randomized McEliece cryptosystem. The McEliece cryptosystem is not only very fast, but it is resistant to quantum computing and it does not require any crypto-processor. Our work includes a comparison between the improved protocol and different existing protocols based on error-correcting codes in terms of security and performance. Security and privacy properties are proved, and the performance of the proposed authentication protocol is analysed in terms of storage requirement, communication cost and computational cost.

Keywords: Authentication protocol, McEliece cryptosystem, RFID

1 Introduction

Among the embedded systems which were quickly developed during the last years and that were used in various domains (e.g. access control, supply chain management,health, ...) we can cite radio frequency identification (RFID). The typical RFID system consists of three entities: tags, readers and server. The tag is a small electronic chip supplemented with an antenna that can transmit and receive data, the reader i.e. a device to communicate with tags by radio waves. The server (or back-end) is a centralized place that hosts all data regarding access permissions and may be consulted by the reader. The use of cryptographic primitives in low-cost RFID tags is limited because the space memory available is restricted, and the computational capabilities are limited. The lowest cost RFID tags are assumed to have the capability of performing bitwise operations (e.g. xor, and, ...), bit shifts (e.g. rotate, logical shift, ...) and random number generator.

The code-based cryptography is a very important research area and it is applied in different schemes. Its advantages are: high-speed encryption and decryption compared to public-key cryptosystems based on number theory. It does not require a crypto-processor and based on difficult problems NP-complete (syndrome decoding, ...). It resists to quantum attacks, and it uses different schemes, such as: public-key cryptosystems, identification schemes, secret sharing and signature [31].

The major problem was the size of public key. Recently, code-based cryptosystems were presented with small key sizes, for example, we quote [3, 22]. In the majority of RFID authentication protocols, the tag does not require a generator matrix or other matrices, but it stores the codeword with the necessary information. RFID authentication protocols based on error-correcting codes use various schemes: error-correcting code with secret parameters [8, 9, 26], randomized Niederreiter cryptosystem [11, 30], Quasi-Dyadic Fix Domain Shrinking [28] and randomized McEliece cryptosystem [19].

In order to have secure authentication protocols, it is important that a RFID authentication protocol own security and privacy properties:

Secrecy. It provides that the identifier of the tag or secret data is never send in clear to air on the interface radio frequency which can be spied.

Mutual Authentication. A RFID authentication protocol achieves mutual authentication that is to say; it achieves the tag's authentication and the reader's authentication. In tag's authentication, the reader has to be capable of verifying a correct tag to authenticate and to identify a tag in complete safety. In reader's authentication, a tag has to be able to confirm that it communicates with the legitimate reader.

Untraceability. the untraceability is one of the privacy properties. The tag is untraceable if an intruder cannot tell whether he has seen the same tag twice or two different tags [12].

Desynchronization Resilience. This property specifies for RFID protocols updating a shared secret before terminating the protocol. The definition of this property is as follows: in session (i), the intruder can block or modify the exchanged messages between the reader and the tag. In the next session, the authentication process is will fail because the tag and the reader are not correlated.

Forward Secrecy. One of the abilities of the intruder is to compromise secrets stored in the tag. The property of forward secrecy signifies to protect the previous communications from a tag even assuming the tag has been compromised.

Resist Replay Attack. The intruder can listen to the message answer of the tag and to the reader. It will broadcast the message listened without modification to the reader later.

We propose in this paper an improved RFID mutual authentication protocol using code-based scheme. Our protocol based on randomized McEliece cryptosystem, uses an efficient decoding/encoding algorithm to generate an error vector of fixed weight. The only datum stored in tag is a dynamic identifier, and it is updated before the end of the session and without the need to do exhaustive search to obtain the identifier from a database. The paper includes a comparison between the new protocol and different protocols based on error-correcting codes in terms of security and performance. Our protocol proves security and privacy properties. Using the AVISPA (Automated Validation of Internet Security Protocols and Applications) tools [1], we prove the security requirements. We use the privacy model of Ouafi and Phan [25] to verify the untraceability property. The performance of the proposed authentication protocol is analysed in terms of storage requirements, communication cost and computational cost.

The rest of this paper is structured as follows: Section 2 presents the basic concepts of code-based cryptography. Section 3 presents related work. We describe our proposed protocol in Section 4. In Section 5, we prove the security and privacy requirements. Section 6 presents the comparative study in terms of performance. Finally, the paper ends with a general conclusion.

2 Code-based Cryptography

$\mathcal{C}[n,k,d]$ is a binary linear code, where n is length and k is dimension which stands a generator matrix $\mathcal{G}'$ (k and n are positive integers and $k < n$). The minimum distance d is the smallest weight of any non-zero codeword in the code. The codeword c of n bits is $m\mathcal{G}$, where m is binary string with length k and $\mathcal{G}$ is a public-key matrix. The encoded codeword is $c' = c \oplus e$, where e is an error vector of length n and weight $t = \mathsf{wt}(e)$, with t is less than or equal to $\lfloor \frac{d-1}{2} \rfloor$.

2.1 McEliece Cryptosystem

The McEliece cryptosystem [20] is the first public key cryptosystem using algebraic coding theory and based on the problem of computational dual decoding syndrome. The idea of McEliece is to hide the corresponding codeword to the message by adding as an error vector while still being able to correct them. If the correction method is kept secret, then only the recipient will be able to recover the original message. We describe this cryptosystem as follows.

Key Generation Algorithm

- choose n, k and d
- randomly generate a generator matrix $\mathcal{G}'$ of an $[n,k,d]$ binary Goppa code $\mathcal{C}$,
- randomly generate a $n \times n$ binary permutation matrix P,
- randomly generate a $k \times k$ binary invertible matrix S',
- compute $\mathcal{G} = S'\mathcal{G}'P$,
- public key is $(\mathcal{G}, t)$, where t integer $< \dfrac{d}{2}$,
- private key is $(S', \mathcal{G}', P, \mathcal{A}(.))$, where $\mathcal{A}(.)$ is a polynomial-time decoding algorithm until $< \dfrac{d}{2}$ errors (like for instance the Patterson algorithm for binary Goppa codes).

Encryption Algorithm

- m message with length k,
- randomly generate e of weight t,
- output $c' = m\mathcal{G} \oplus e$, where $\mathsf{wt}(e) = t$.

Decryption Algorithm

- compute $z = c'P^{-1}$,
- compute $y = \mathcal{A}(z)$,
- output $m = yS'^{-1}$.

2.2 Randomized McEliece Cryptosystem

Nojima et al. [24] prove that padding the plaintext with a random bit-string provides the semantic security against chosen plaintext attack (IND-CPA) for the McEliece cryptosystem with the standard assumptions.

The standard assumptions are: the syndrome decoding (SD) problem is hard and the public-key is indistinguishable.

The randomized McEliece is a probabilistic cryptosystem, whose encryption algorithm of message is as follows:

$$c' = c \oplus e = [r \parallel m]\, \mathcal{G} \oplus e = (r\mathcal{G}_1 \oplus e) \oplus m\mathcal{G}_2 \qquad (1)$$

where:

- $\mathcal{G} = \left[\begin{smallmatrix}\mathcal{G}_1 \\ \mathcal{G}_2\end{smallmatrix}\right]$
- k_1 and k_2: two integers such that $k = k_1 + k_2$ and $k_1 < bk$ where $b < 1$ (e.g. $b = \frac{9}{10}$ [24]),
- $\mathcal{G}_1$ and $\mathcal{G}_2$: matrices with $k_1 \times n$ and $k_2 \times n$, respectively,
- r: random string with length k_1,
- m: message with length k_2.

The encryption algorithm encrypts $[r \| m]$ instead of m itself. The decryption algorithm is almost the same as original McEliece, the difference is that it outputs only the last k_2 bits of the decrypted string.

2.3 Encoding Constant Weight Words

To transform a binary string into error vector (bijective) or encode/decode constant weight words, we have two methods: the enumerative method [10, 27] and the recursive method [29]. We are interested in the enumerative method, which is based on the following bijective application:

$$\begin{array}{rlcl} \phi_{n,t}: & \left[0, \binom{n}{t}\right[& \longrightarrow & \mathcal{W}_{n,t} := \{x \in \mathbb{F}_q^n \mid \mathsf{wt}(x) = t\} \\ & x & \mapsto & (i_1, \cdots, i_t) \end{array}$$

$\mathcal{W}_{n,t}$ is represented by its non-zero positions in increasing order $0 \leq i_1 < i_2 < \cdots < i_t \leq n-1$ and length of x is $\ell = \left\lfloor \log_2 \binom{n}{t} \right\rfloor$.

The inverse application is defined as follows:

$$\begin{array}{rlcl} \phi_{n,t}^{-1}: & \mathcal{W}_{n,t} & \longrightarrow & \left[0, \binom{n}{t}\right[\\ & (i_1, \cdots, i_t) & \mapsto & \binom{i_1}{1} + \binom{i_2}{2} + \ldots + \binom{i_t}{t} \end{array}$$

The cost of a bijective application is $\mathcal{O}(t\ell^2)$ binary operations. The decoding algorithm $\phi_{n,t}$ is proposed by [10, 27] as follows (Algorithm 1).

Algorithm 1 Enumerative decoding

Data $x \in \left[0, \binom{n}{t}\right[$
Result t integers $0 \leq i_1 < i_2 < \cdots < i_t \leq n-1$
$j \leftarrow t$
while $j > 0$ **do**
  $i_j \leftarrow$ invert-binomial (x, j)
  $x \leftarrow x - \binom{i_j}{j}$
  $j \leftarrow j - 1$
end while
where invert-binomial (x, j) returns the integer i such that $\binom{i}{j} \leq x < \binom{i+1}{j}$

3 Related Work

In a survey of design and implementation of authentication protocols on RFID systems, we can find many protocols developed using various algebraic and cryptographic primitives (asymmetric cryptosystems, symmetric cryptosystems, hash function, bitwise operators, ...), such as [5, 7, 17, 23, 32, 33, 34, 35]. Our work is articulated on recent RFID authentication protocols that use error-correcting codes.

Park [26] proposed a one-way authentication protocol to provide untraceability which is based on the secret-key certificate and the algebraic structure of the error-correcting code. This protocol is designed for wireless mobile communication systems. We study this protocol because the computational capabilities of Mobile subscriber is limited like RFID tag. This protocol does not achieve untraceability because the weight of e in session (i) is the same weight as in session (j) with equal t. If the intruder knows d or t, so the intruder can trace of the legitimate tag. Also, this protocol does not resist desynchronization attacks because the tag and the reader store a number of the last session and do not use a secret synchronization value.

In [11], authors proposed an authentication protocol based on the randomized Niederreiter cryptosystem and the amelioration of the protocol [30]. This protocol does not achieve forward secrecy because the data stored in tag is static and does not achieve the reader's authentication.

Chien and Laih [9] proposed a RFID authentication protocol based on error-correcting codes with secret parameters. This protocol uses a confusion scheme to avoid traceability attacks. The data stored in tag is static, therefore, this protocol does not achieve forward secrecy.

Sekino et al. [28] proposed a challenge-response authentication protocol based on Quasi-Dyadic Fix Domain Shrinking that combines Niederreiter personalized public-key cryptosystem (P^2KC) [18] with Quasi-dyadic (Goppa) codes [22]. The authors reduce the size of the public-key matrix stored in tag of protocol [11], but it remains relatively important compared to the resources of low-cost tag. Also, the information stored in tag is static, therefore, this protocol does not achieve forward secrecy.

Malek and Miri [19] proposed a RFID authentication protocol based on randomized McEliece public-key cryptosystem. In this protocol, the tag can communicate with a set of authorised readers. This protocol achieves the untraceability property because the identifier is modified in each session. Concerning the desynchronization attack, if the intruder modifies a last message, then the identifier stored in reader is different to identifier stored in tag. Thus, this protocol does not resist the desynchronisation attacks. In other hand, in the phase of reader's authentication, the tag computes and uses the circulant matrix, this requires a more complex computation and important space in volatile memory.

4 Our Improved Protocol

In this section, we propose an improved mutual protocol based on randomized McEliece cryptosystem. To better describe our proposed protocol, we use the notations given in Section 2 and Table 1.

Table 1: Notations

T, R, S	The tag, the reader and the server
N_R	Random number generated by R
$g(.)$	Pseudo-random function
$\|$	Concatenation of two inputs
t, t'	Integer numbers
x	Random number, with $x \in \left[0, \binom{n}{t'}\right[$
$\phi_{n,t'}(x)$	decoding bijective application (transform x into error vector e)
e	Error vector of length n and weight $t' < t$ where $t = \lfloor(d-1)\rfloor/2$
id	Identifier of tag, with binary length k_2
r, r'	Random numbers with binary length k_1
c_r	Codeword, where $c_r = r\mathcal{G}_1$
$c_{r'}$	Codeword, where $c_{r'} = r'\mathcal{G}_1$
c_{id}	Codeword, where $c_{id} = id\mathcal{G}_2$
DID	Dynamic ID, codeword with length n, where $DID = c_r \oplus c_{id}$
$c_{r_{old}}$,$c_{r_{new}}$	Two secret synchronization codewords, where $c_{r_{old}} = r_{old}\mathcal{G}_1$ and $c_{r_{new}} = r_{new}\mathcal{G}_1$

4.1 System Model

The RFID system consists of three entities: tag T, reader R and server S.

- The tag T is low-cost and passive. It stores the dynamic identity (DID) which is strictly confidential. T implements an application $\phi_{n,t'}$ and pseudo-random numbers generator (PRNG) to generate x and compute $g(.)$. It also supports bitwise operations (xor, and, ...). A tag has a rewritable memory that may not be tamper-resistant.
- The reader R can generate pseudo-random numbers.
- The server S has the sufficient storage space and computational resources. We implement algorithms of $\phi^{-1}_{n,t'}$ and PRNG. Server S can decode the message received from T, then, we implement encryption/decryption of randomized McEliece cryptosystem with public-key matrix $\mathcal{G}$, private-key matrices and a polynomial-time decoding algorithm $\mathcal{A}(.)$. The server contains the database which includes $\{id, c_{id}, c_{r_{old}}, c_{r_{new}}\}$.

In our work, we propose to use $\phi_{n,t'}(x)$ as follows (Algorithm 2).

Algorithm 2 Generation a error vector

1: Randomly choose $x \in \left[0, \binom{n}{t}\right[$
2: **repeat**
3:     determine the largest t' such that $x \in \left[0, \binom{n}{t'}\right[$
4: **until** $t' < t$
5: compute $\phi_{n,t'}(x) = e$ where $\mathsf{wt}(e) = t' < t$

We will choose t' such that the syndrome decoding problem (most efficient algorithm) remains hard.

The communication channel between the server and the reader is assumed to be secure while the wireless channel between the reader and the tag is assumed to be insecure in the authentication phase since it makes it open to attacks on the authentication protocol.

4.2 Description of Our Proposed Protocol

The proposed Protocol is divided into two phases: the initialization phase and the mutual authentication phase.

4.2.1 Initialization Phase

The server generates a random binary Goppa code $\mathcal{C}[n, k, d]$ as specified by the generator matrix $\mathcal{G}'$, where $\mathcal{G} = S'\mathcal{G}'P$ and $\mathcal{G}$ is public-key. The server S generates random values using PRNG, id the unique identifier of tag and the random number r. It computes $c_r = r\mathcal{G}_1$, $c_{id} = id\mathcal{G}_2$ and $DID = c_r \oplus c_{id}$, and initializes $c_{r_{old}}$ and $c_{r_{new}}$ by c_r. Then, the server (registration center) sends DID to the tag through a secure channel, where DID is strictly confidential. S stored in the database $\{id, c_{id}, c_{r_{old}}, c_{r_{new}}\}$ for each tag.

4.2.2 Mutual Authentication Phase

The mutual authentication phase is described as follows (and in Figure 1).

Step 1. ***Tag's Authentication***

Step 1.1. R generates a nonce N_R and sends it as a request to the tag T.

Step 1.2. T generates a random number $x \in \left[0, \log_2\binom{n}{t'}\right[$ and $t' \in [1, t[$, and computes error vector e with $\mathsf{wt}(e) = t'$ from $\phi_{n,t'}(x)$, $c' = DID \oplus e$ and $P = g(N_R \parallel x \parallel DID)$.

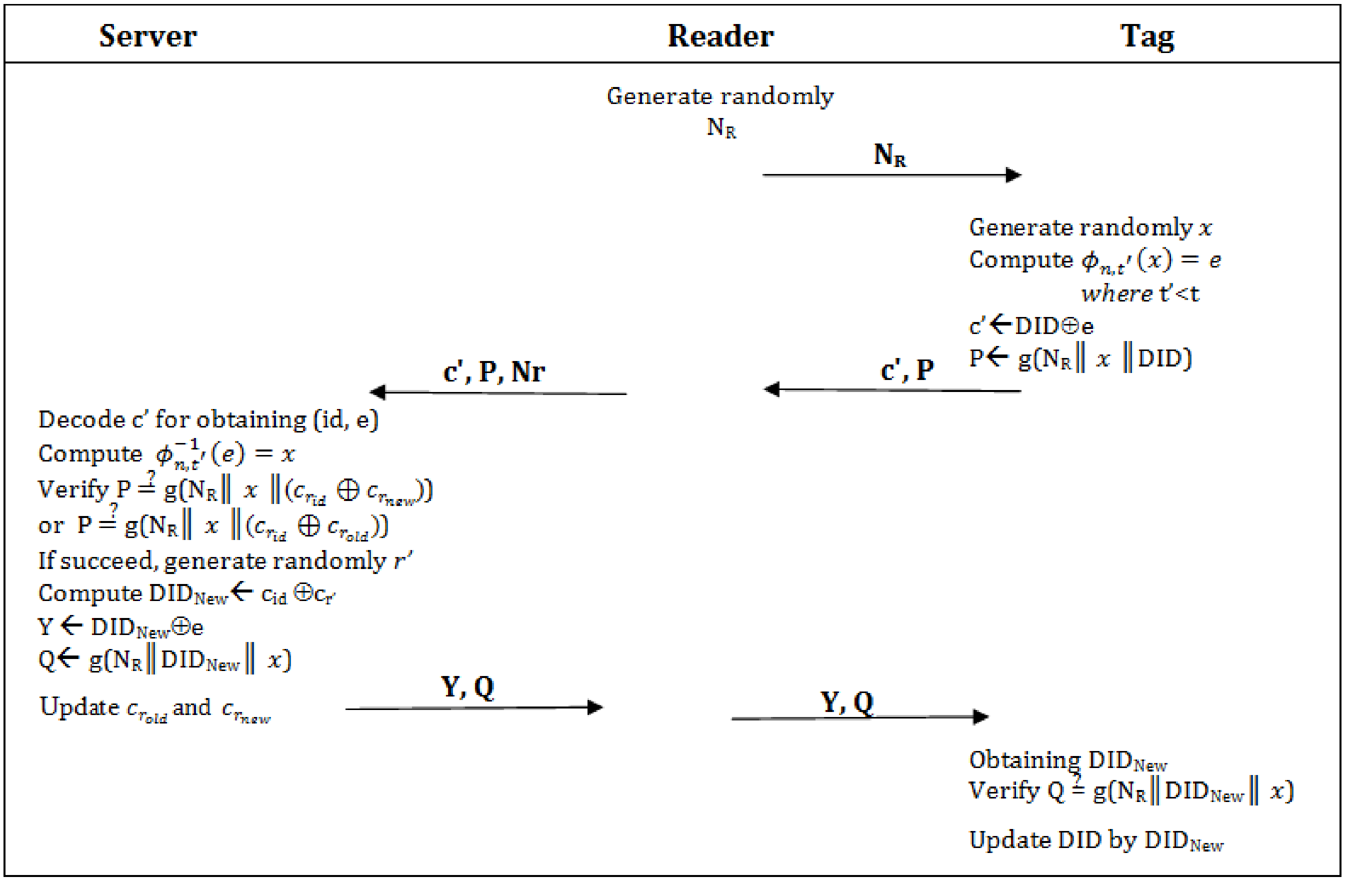

Figure 1: Our proposed protocol

Step 1.3. T sends c' with P to the reader, and resends the received c', message P and nonce N_R to the server S.

Step 1.4. S performs a decoding algorithm $\mathcal{A}(.)$ with private key matrices and identifies the error vector e as well as id and r. From id, in database, the server retrieves the values of $c_{id}, c_{r_{old}}, c_{r_{new}}$ and computes $x = \phi^{-1}_{n,t'}(e)$ and $P_1 = g(N_R \parallel x \parallel (c_{id} \oplus c_r))$ (either $c_{r_{old}}$ or $c_{r_{new}}$). S verifies if $P_1 \stackrel{?}{=} P$, if they are equal, the tag's authentication is successful; otherwise the tag's authentication has failed.

Step 2. ***Reader's Authentication***

Step 2.1. In this case the tag's authentication is successful. The server generates a random number r' and computes $c_{r'} = r'\mathcal{G}_1$ and $DID_{New} = c_{id} \oplus c_{r'}$. It computes $Y = DID_{New} \oplus e$ and $Q = g(N_R \parallel DID_{New} \parallel x)$. It updates $c_{r_{old}} \leftarrow c_{r_{new}}$ and $c_{r_{new}} \leftarrow c_{r'}$, only in case the matched c_r is $c_{r_{new}}$.

Step 2.2. S sends Y and Q to the reader and resends the received message to T.

Step 2.3. T obtains DID_{New} by computing $Y \oplus e$ and calculates $Q_1 = g(N_R \parallel DID_{New} \parallel x)$. T verifies if $Q_1 \stackrel{?}{=} Q$, if they are equal, the reader's authentication is successful; otherwise the authentication of the reader will fail.

Step 2.4. T updates the dynamic identifier by the value of DID_{New}, if reader's authentication is successful.

5 Security and Privacy Analysis

A secure RFID authentication protocol should provide mutual authentication, secrecy, untraceability, desynchronization resilience, forward secrecy and replay attack resisting. In this section, we discuss the security and privacy requirements of proposed protocol and others protocols. Table 2 presents the security comparison between the existing protocols and the proposed protocol.

5.1 Automated Verification

We choose AVISPA tools (Automated Validation of Internet Security Protocols and Applications) [1] to verify the security properties for the following reasons: the tools uses various techniques of validation (Model-checking, automate trees, Solver SAT and resolution of constraints). The AVISPA platform is the analyzer which models a

```
role reader ( R,T: agent, ID,Rold, Rnew: text,
          Fg,Phi : hash_func,
     KG: public_key, Snd,Rec: channel(dy))
   played_by R
   def=
    local  State  : nat,
         Nr, X, RN : text,
         E: hash(text),
         DID,DNew : {text.text}_public_key
    init State := 0
    transition
     1. State = 0
       /\ Rec(start)  =|>  State' := 1 /\ Nr' := new()
       /\ Snd(Nr') /\ witness(R,T,aut_reader,Nr')
% if CR= CRnew
     2. State = 1
       /\ Rec({DID}_E'.Fg(Nr.X'.DID)) =|> State' := 2 /\ RN':=new()
 /\ DNew':={ID.RN'}_KG  /\ Snd(xor(DNew',E').Fg(Nr.DNew'.X'))
      /\ secret({DNew'},sec_did2, {R,T})
      /\ request(R,T,aut_tag,X') /\ Rold':=Rnew /\ Rnew':=RN'
     % if CR= CRold
3. State = 1 /\ Rec({DID}_E'.Fg(Nr.X'.DID)) =|> State' := 2
      /\ DNew':={ID.Rnew}_KG  /\ Snd(xor(DNew',E').Fg(Nr.DNew'.X'))
      /\  secret({DNew'},sec_did2, {R,T}) /\ request(R,T,aut_tag,X')
end role

role tag ( T,R: agent, DID: {text.text}_public_key,
        Fg,Phi : hash_func, Snd,Rec: channel(dy))
   played_by T
   def=
    local  State  : nat,
         Nr, X, RN : text,
         E: hash(text),
         DNew: {text.text}_public_key
   init State := 0
   transition
    1. State = 0 /\ Rec(Nr') =|> State' := 1
      /\ X' := new()  /\ E':=Phi(X')
      /\ Snd({DID}_E'.Fg(Nr'.X'.DID))
      /\ witness(T,R,aut_tag,X') /\ secret({DID},sec_did1, {T,R})
    2. State = 1 /\ Rec(xor(DNew',E).Fg(Nr.DNew'.X'))
       =|> State' := 2
      /\ request(T,R,aut_reader,Nr) /\ DID' := DNew'
end role

role session(R,T: agent,
          ID,Rinit: text,
          Fg, Phi : hash_func,
          KG: public_key)
def=
local Se,Re,Sf,Rf : channel(dy)
const aut_reader, aut_tag, sec_did1, sec_did2 : protocol_id
composition
tag(T,R,{ID.Rinit}_KG,Fg,Phi,Se,Re)
/\ reader(R,T,ID,Rinit,Rinit,Fg,Phi,KG, Sf,Rf)
end role

role environment() def=
const t,r,i : agent,
     id,rinit,idit,idri: text,
     g,phi : hash_func,
     kG,kGti,kGri: public_key

intruder_knowledge = {t,r,i,g,kG,phi,kGti,kGri,idit,idri}
composition

session(r,t,id,rinit,g,phi,kG)
/\ session(r,t,id,rinit,g,phi,kG)
/\ session(i,t,idit,rinit,g,phi,kGti)
/\ session(r,i,idri,rinit,g,phi,kGri)
end role

   goal
 secrecy_of sec_did1 % confidentiality of DID
 secrecy_of sec_did2 % confidentiality of DNew
 authentication_on aut_reader % Reader's authentication
      authentication_on aut_tag % Tag's authentication
   end goal

   environment()
```

Figure 2: Specification of our protocol by HLPSL

Table 2: Comparison of security and privacy properties

	M.A	D.C	Unt	D.R	F.S	R.R
Park [26]	N	Y	N	N	Y	Y
Cui et al. [11]	N	Y	Y	Y	N	Y
Chien-Laih [9]	Y	Y	Y	Y	N	Y
Sekino et al. [28]	N	Y	Y	Y	N	Y
Malek-Miri [19]	Y	Y	Y	N	Y	Y
Our Protocol	Y	Y	Y	Y	Y	Y

M.A: Mutual Authentication, D.C: Data Confidentiality
Unt: Untraceability, D.R: Desynchronization resilience
F.S: Forward secrecy, R.R: Resist replay attacks

big number of cryptographic protocols. These tools can detect passive and active attacks, like replay and man-in-the-middle attacks. AVISPA tools are based on only one specification language named HLPSL language (High-Level Protocol Specification Language) [2].

HLPSL is a formal, expressive, modular and role-based language. Protocol specification consists of two types of roles, basic roles and composed roles. Basic roles serve to describe the actions of one single agent in the run of the protocol. Others instantiate basic roles to model an entire protocol run, a session of the protocol between multiple agents, or the protocol model itself. HLPSL can specify the secrecy and the authentication properties.

The intruder model agreed in HLPSL is Dolev-Yao model [13]. This intruder model is based on two important assumptions that are the perfect encryption and the intruder is the network. *Perfect encryption* ensures in particular that an intruder can decrypt a message m encrypted with key k if it has the opposite of that key. The second hypothesis which is *the intruder is the network* means that, the intruder has complete control over the channel of communication between the reader and the tag. It can intercept any message passing through the network, block or modify messages and it can also derive new messages from its initial knowledge.

Our protocol requires the primitives: PRNG, nonce xor-operator and McEliece cryptosystem. The randomized McEliece cryptosystem requires the primitives: public key, private key, application $\phi_{n,t'}(.)$ and the decoding algorithm $\mathcal{A}(.)$ which is used with a private key to obtain id and e. The application $\phi_{n,t'}(.)$ is bijective, but the intruder cannot find x without knowing the value of t', and the result of this application e does not circulate clearly in the channel, then we can model it by a hash function $Phi(x)$. The intruder will know this function, therefore he will be able to compute the error vector but not invert values of $Phi^{-1}(x)$ (unless he already knows x).

Concerning the message $DID \oplus e$, we cannot specify it in HLPSL by $xor(DID, E)$ because the reader does not use the algebraic properties of or-exclusive operator (e.g. neutral element) to obtain id and e. To retrieve these values, we apply the private decoding algorithm $\mathcal{A}(.)$ and the private key of McEliece. $DID \oplus e$ means the encoding DID by e, where DID is encryption of $[r \parallel id]$ by public key $\mathcal{G}$. The reader (server) obtaining the value DID and e uses the private decoding algorithm $\mathcal{A}(.)$. Therefore, we propose to specify this message in HLPSL by $\{DID\}\_E$. In the other hand, we can specify the message $DID_{New} \oplus e$ by $xor(DNew, E)$ (last message from reader to tag) because the objective of the tag is to retrieve the value of DID_{New} using the algebraic properties of xor operator.

The Figure 2 shows the specification of our protocol by HLPSL. In our protocol, the honest participants are the reader R and the tag T. Then, we have two basic roles, the tag and the reader. We can define a session role which all the basic roles are instanced with concrete arguments. In the *tag*, we initialise the argument DID by {ID.Rinit}_kG. In the *reader*, we initialise the values $Rold$ and $Rnew$ by $Rinit$. We provide a validation of properties: the tag's authentication (*aut_tag*), the reader's authentication (*aut_reader*), the secrecy of current DID (*sec_did*1), and the secrecy of the new DID (*sec_did*2).

The result of verification of our protocol by AVISPA tools is presented in Figure 3. This result clearly means that there is no attack detected (replay or man-in-the-middle attacks). We can thus deduct that the diagnostic of AVISPA tools for our protocol is secure.

5.2 Privacy Verification

In the literature of formal verification of privacy properties, we can find many privacy models. The privacy model proposed by Juels and Weis [16] is based on the notion of indistinguishability. Ouafi and Phan model [25] is based on the Juels-Weis model. Authors added several definitions in the untraceability property.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  UNTYPED_MODEL

PROTOCOL
  /home/avispa/web-interface-computation/./tempdir/workfileEX56ur.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 2543 states
  Reachable  : 325 states
  Translation: 0.04 seconds
  Computation: 0.18 seconds
```

Figure 3: The result of the verification using CL-AtSe tool of our protocol

In Ouafi and Phan model, a protocol party is a tag $T \in Tags$ or a reader $R \in Readers$ interacting in protocol sessions as per the protocol specifications until the end of the session. The adversary is allowed to run the following queries:

• Execute (R, T, i) query. This query models the passive attacks. The adversary A eavesdrops the communication channel between T and R and gets reading access to the exchanged messages in session i of a truthful protocol execution.

• Send (U, V, m, i) query. This query models active attacks by allowing the adversary A to impersonate some reader $U \in Readers$ (respectively tag $V \in Tags$) in some protocol session i and sends a message m of its choice to an instance of some tag $V \in Tags$ (respectively reader U $\in Readers$). Furthermore the adversary A is allowed to block or alert the message m that is sent from U to V (respectively V to U) in session i of a truthful protocol execution.

• Corrupt(T, K') query. This query allows the adversary A to learn the stored secret K of the tag $T \in Tags$, and which further sets the stored secret to *K'*. Corrupt query means that the adversary has physical access to the tag, i.e., the adversary can read and tamper with the tag's permanent memory.

• Test (i, T_0, T_1) query. This query does not correspond to any of A's abilities, but it is necessary to define the untraceability test. When this query is invoked for session i, a random bit $b \in \{0, 1\}$ is generated and then, A is given $T_b \in (T_0, T_1)$. Informally, A wins if he can guess the bit b.

Untraceable privacy (UPriv) is defined using the game played between an adversary A and a collection of the reader and the tag's instances. This game is divided into three phases:

• **Learning phase:** A is able to send any Execute, Send, and Corrupt queries at will.

• **Challenge phase:** A chooses two fresh tags T_0, T_1 to be tested and sends a Test query corresponding to the test session. Depending on a randomly chosen bit $b \in \{0, 1\}$, E is given a tag T_b from the set $\{T_0, T_1\}$. E continues making any Execute, and Send queries at will.

• **Guess phase:** finally, A terminates the game and outputs a bit $b' \in\{0, 1\}$, which is its guess of the value of b.

The success of A in winning the game and thus breaking the notion of UPriv is quantified in terms of A's advantage in distinguishing whether A received T_0 or T_1, in other term, it correctly guessing b. and denoted by $Adv_A^{UPriv}(k)$ where k is the security parameter.

We use the Ouafi-Phan model to verifying the achievement of untraceability property in our proposed protocol. At session (i), by the Execute query, the adversary A eavesdrops a perfect session between T_0 and a legitimate reader. He obtains the values $DID_i \oplus e_i$ and $g(N_{Ri} \parallel x_i \parallel DID_i)$. At next session, an intruder cannot replay a previously used $g(N_R \parallel x \parallel DID)$ and $DID \oplus e$ to a reader, since with high probability, it will not match the N_R value generated by the reader for that session. There are two mechanisms to against the replay. Firstly, by generating an error vector with dynamic length $t' \leq t$ where t' is confidential. Secondly, we accept the principle of dynamic codeword, which is stored in tag in the form of DID. In each session, the transmitted encoding codeword is different from the codeword of the last session because the value of the codeword is updated in the server and in the tag before the end of the session.

In addition, the security of our protocol is based on security of randomized McEliece. Nojima et al. [24] prove that padding the plaintext (in our protocol, identifier of tag id) with a random bit-string (random number r) provides the semantic security against chosen plaintext attack (IND-CPA) for the McEliece cryptosystem with the standard assumptions. So, The randomized McEliece cryptosystem is IND-CPA secure, that means if no probabilistic polynomial-time adversary wins the IND-CPA experiment with an advantage greater than a negligible function of the security parameter.

5.3 Informally Security Analysis

Desynchronization resilience In our protocol the value of the dynamic identifier DID is updated in each session. This implicates a possibility of attack on desynchronization. To achieve this property, we used two secret synchronisation codewords, $c_{r_{old}}$ and $c_{r_{new}}$ stored in the server. In case the last message of the reader's authentication is blocked by the intruder, then the server updates the values of $c_{r_{old}}$ and $c_{r_{new}}$ but the tag does not update DID where $DID = c_{id} \oplus c_r$. In the next session, we mention a problem in the tag's authentication with $c_{r_{new}}$, but the problem is resolved with $c_{r_{old}}$, then the tag's authentication is successful.

Forward secrecy Before terminating a session of protocol, the dynamic identifier DID updated by using error-correcting code. The new DID is $r'\mathcal{G}_1 + id\mathcal{G}_2$, where r' is generated randomly in each session. The intruder could not acquire the previous dynamic identifier DID used in the prior sessions. Thus, the proposed RFID authentication protocol could provide forward secrecy.

6 Performance Analysis

The performance of authentication protocols is mainly measured by storage space on tag, computation cost in tag and server and communications cost between the tag and the reader. Our comparison is articulated on authentication phase for each protocol. Table 3 shows the performance comparison between our protocol and the RFID protocols based on error-correcting codes.

Concerning the storage cost, the tags of protocols [11, 28, 30] require public-key matrix which is of important size compared to resources of low-cost tags. The data stored on tags of protocols [8, 26] are multiple in an agreed number of sessions. Our protocol requires only information which is dynamic identifier DID, thus less space is required than in other protocols.

The communication cost between a tag and a reader consists of: the number of message exchanges, and the total bit size of the transmitted messages, per each communication. Concerning our protocol, the total of the bits of the messages of communication is $2(n + l_p)$.

Concerning the computation cost, the tag requires simple operations: pseudo-random number generator and xor operation. We used the PRNG to generate x and to compute $g(.)$, it is very fast. For optimising the cost of calculation of $g(.)$, we used x in $g(N_R \parallel x \parallel DID)$ because the binary length of x is less binary length of the error vector e. Concerning the server, we store the values of $c_{r_{old}}$ and $c_{r_{new}}$ instead of r_{old} and $_{r_{new}}$ to augment the speed of computation in authentication phases and in the updating of DID. Our protocol does not need an exhaustive search for obtaining the value of id.

With regard to the other protocols and consideration of mutual authentication, the performance of our protocol is effective.

If we select a binary Goppa code $\mathcal{C}[n = 2048, k = 1751, d = 56]$, these parameters agree with the parameters of a secure McEliece cryptosystem for 2^{80} security [4]. We choose the values of k_1= 890 and k_2= 875 which are suitable with condition $k_2 < k_1$. So, the number of tags supported is 2^{875} tags and the space memory required in the tag is 2048 bits for codeword DID and the maximal weight of the error vector is 27 bits. With these parameters, we can implement our protocol in low-cost tags, such as Mifare Classic 1K and Mifare Plus support space memory 1KB to 4 KB [21]. We note here that it is possible to optimize the parameters of the code using the techniques of Quasi-cyclic codes [3] or Quasi-dyadic codes [22]. Using the optimized parameters, we can implement our protocol in Mifare Ultralight EV1 tag support 384 bits to 1024 bits. Though several attacks can be realized against McEliece with Quasi-cyclic codes and Quasi-dyadic codes [14, 15],

Table 3: Performance Evaluation

	Key space	Cost		Communication	
		Tag	Server	$T \rightarrow R$	$R \rightarrow T$
Park [26]	$l_p + n + 2\lvert key\rvert$	$1P$	$iH + 1D + 1ED$	n	-
Chien and Laih [9]	$n + 2\lvert key\rvert$	$8P$	$4P + 2ED$	$2l_p + 2n)$	$2l_p$
Cui et al. [11]	$(n-k) \times (n_2 + 1)$	$2P + 1EC$	$2P + 1ED$	$(n-k) + l_p$	l_p
Sekino et al. [28]	$(n-k) + (n-k) \times (n_1 - (n-k)/t$	$1EC + 2P$	$2P + 1ED$	$(n-k) + l_p$	l_p
Malek and Miri [19]	$(n + k_2 + \lvert key\rvert)$	$2P$+CM	$2P + 1ED$	n	$2n + \lvert key\rvert + lp$
Our Protocol	n	$3P$	$2P + 1ED$	$n + l_p$	$n + l_p$

$|key|$: length of key or id
i: number of authorised sessions
l_p: length of generating random number or hash
P, D and CM: cost of RNG or hash function, decryption operation and generation of circular matrix, respectively
EC and ED: encoding operation and decoding operation, respectively

variants based on binary Goppa codes are secure like [6].

7 Conclusion

In this paper, we have discussed the limitations and vulnerabilities of previous RFID authentication protocols based on error-correcting codes. We have proposed an improved RFID authentication protocol based on randomized McEliece cryptosystem with mutual authentication, untraceability, desychronisation relisience and forward secrecy. Using formal models, the AVISPA tools and Ouafi-Phan model, we have proved security and privacy properties.

With regard to the different existing protocols based on error-correcting codes, the performance of our protocol is effective, required only n bits on the tag, does not need to do exhaustive search, and the tag can perform lightweight cryptographic operations.

References

[1] A. Armando, et al., "The AVISPA tool for the automated validation of internet security protocols and applications," in *Proceedings of 17th International Conference on Computer Aided Verification* (K. Etessami and S. Rajamani, eds.), vol. 3576, pp. 281–285, 2005.

[2] The AVISPA Team, "HLPSL tutorial the Beginner's guide to modelling and analysing internet security protocols," Technical Report, AVISPA project, 2006.

[3] T. P. Berger, P. L. Cayrel, P. Gaborit, and A. Otmani, "Reducing key lengths with QC alternant codes," in *Proceedings of Africacrypt 2009*, vol. 5580, pp. 77–97, 2009.

[4] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *2nd International Workshop on Post-Quantum Cryptography (PQCRYPTO'08)*, LNCS 5299, pp. 31–46, 2008.

[5] T. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols," *International Journal of Network Security*, vol. 9, pp. 95–100, 2009.

[6] P. L. Cayrel, G. Hoffmann, and E. Persichetti, "Efficient implementation of a CCA2-secure variant of McEliece using generalized Srivastava codes," in *Proceedings of PKC'2012*, LNCS 7293, pp. 138–155, 2012.

[7] C. L. Chen, Y. L. Lai, C. C. Chen, Y. Y. Deng, and Y. C. Hwang, "RFID ownership transfer authorization systems conforming EPCglobal class-1 generation-2 standards," *International Journal of Network Security*, vol. 13, pp. 41–48, 2011.

[8] H. Y. Chien, "Secure access control schemes for RFID systems with anonymity," in *Proceedings of the 7th International Conference on Mobile Data Management (MDM'06)*, pp. 96, 2006.

[9] H. Y. Chien and C. S. Laih, "ECC-based lightweight authentication protocol with untraceability for low-cost RFID," *Journal of Parallel and Distributed Computing*, vol. 69, pp. 848–853, 2009.

[10] T. M. Cover, "Enumerative source encoding," *IEEE Transactions on Information Theory*, vol. 19, no. 1, pp. 73–77, 1973.

[11] Y. Cui, K. Kobara, K. Matsuura, and H. Imai, "Lightweight asymmetric privacy-preserving authentication protocols secure against active attack," in *Proceedings of the Fifth Annual IEEE International Conference (PerComW'07)*, pp. 223–228, 2007.

[12] V. Deursen, S. Mauw, and S. Radomirovic, "Untraceability of RFID protocols," *Information Security Theory and Practices, Smart Devices, Convergence and Next Generation Networks*, pp. 1–15, 2008.

[13] D. Dolev and A. C. Yao, "On security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, pp. 198–208, 1983.

[14] J. C. Faugère, A. Otmani, L. Perret, and J. P. Tillich, "Algebraic cryptanalysis of McEliece variants with compact keys," in *Proceedings of the 29th International Conference on Cryptology (EUROCRYPT'10 2010)*, pp. 279-298, 2010.

[15] J. C. Faugère, A. Otmani, L. Perret, and J. P. Tillich, "A distinguisher for high rate McEliece cryptosystems," Technical Report 2010/331, Cryptology ePrint Archive, 2010.

[16] A. Juels and S. A. Weis, "Defining strong privacy for RFID," *ACM Transactions on Information and System Security*, vol. 13, no. 1, Oct. 2009.

[17] W. Khedr, "On the Security of Moessner's and Khan's Authentication Scheme for Passive EPCglobal C1G2 RFID Tags," *International Journal of Network Security*, vol. 16, no. 5, pp. 369–375, 2014.

[18] K. Kobara and H. Imai, "Personalized-public-key cryptosystem (P2KC) - Application where public-key size of Niederreiter PKC can be reduced," in *Workshop on Codes and Lattices in Cryptography (CLC'06)*, pp. 61–68, 2006.

[19] B. Malek and A. Miri, "Lightweight mutual RFID authentication," in *Proceedings of IEEE International Conference on Communications*, pp. 868–872, 2012.

[20] R. J. McEliece, "A public-key system based on algebraic coding theory," Technical Report, DSN Progress Report 44, Jet Propulsion Lab, 1978.

[21] *The Mifar Cards*, 2015. (http://www.mifare.net)

[22] R. Misoczki and P. S. L. M. Barreto, "Compact McEliece keys from Goppa codes," in *Selected Areas in Cryptography (SAC'09)*, LNCS, pp. 376–392, 2009.

[23] M. Naveed, W. Habib, U. Masud, U. Ullah, and G. Ahmad, "Reliable and low cost RFID based authentication system for large scale deployment," *International Journal of Network Security*, vol. 14, pp. 173–170, 2012.

[24] R. Nojima, H. Imai, K. Kobara, and K. Morozov, "Semantic security for the McEliece cryptosystem without random oracles," *Designs, Codes and Cryptography*, vol. 49, no. 1–3, pp. 289–305, 2008.

[25] K. Ouafi and R. C. W. Phan, "Privacy of recent RFID authentication protocols," in *Proceedings of ISPEC'08* (L. Chen, Y. Mu, and W. Susilo, eds.), LNCS 4991, pp. 263–277, 2008.

[26] C. S. Park, "Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems," *Computer Networks*, vol. 44, pp. 267–273, 2004.

[27] P. M. Schalkwijk, "An algorithm for source coding," *IEEE Transactions of Information Theory*, vol. 18, no. 3, pp. 395–399, 1972.

[28] T. Sekino, Y. Cui, K. Kobara, and H. Imai, "Privacy enhanced RFID using Quasi-Dyadic fix domain shrinking," in *Proceedings of Global Telecommunications Conference (GLOBECOM'10)*, pp. 1–5, 2010.

[29] N. Sendrier, "Encoding information into constant weight words," in *IEEE Conference on ISIT'05*, pp. 435–438, 2005.

[30] M. Suzuki, K. Kobara, and H. Imai, "Privacy enhanced and light weight RFID system without tag synchronization and exhaustive search," in *Proceedings of 2006 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 1250–1255, 2006.

[31] P. Véron, "Code based cryptography and steganography," in *Proceedings of CAI'13*, LNCS 8080, pp. 9–46, 2013.

[32] C. H. Wei, M. S. Hwang, and A. Y. H. Chin, "An authentication protocol for low-cost RFID tags," *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.

[33] C. H. Wei, M. S. Hwang, and A. Y. H. Chin, "A mutual authentication protocol for RFID," *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, 2011.

[34] C. H. Wei, M. S. Hwang, and A. Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID," *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.

[35] X. Zhang and B. King, "Security requirements for RFID computing systems," *International Journal of Network Security*, vol. 6, pp. 214–226, 2008.

Noureddine Chikouche, received his B.Sc. (engineer) in computer science from the University of Constantine, Algeria, in 1999. In addition, he received his M.Sc. in computer science from the University of M'sila, Algeria, in 2010. He has been a Ph.D. candidate at University of Biskra, Algeria. He also is assistant professor in computer sciences Department at University of M'sila, from 2011. His research interests include RFID security, formal verification of cryptographic protocols, and code-based cryptography.

Foudil Cherif is an associate professor of computer science at Computer Science Department, Biskra University, Algeria. Dr. Cherif holds Ph.D degree in computer science. The topic of his dissertation is behavioral animation: crowd simulation of virtual humans. He also possesses B.Sc. (engineer) in computer science from Constantine University 1985, and an M.Sc. in computer science from Bristol University, UK in 1989. He is currently the head of LESIA Laboratory. His current research interest is in Artificial intelligence, Artificial life, Crowd simulation, RFID security, formal verification of cryptographic protocols and Software engineering.

Pierre-Louis Cayrel, received his Ph.D. degree in Mathematics from University of Limoges in 2008. He has been a post-doctorate assistant in CASED in Darmstadt, Germany from 2009 to 2011. He is now an Associate Professor in Jean Monnet University, Saint-Etienne since September 2011. His research interests are: coding theory, code-based cryptography, side channel analysis and secure implementations of cryptographic schemes.

Mohamed Benmohammed, received his Ph.D. degree in computer science from University of Sidi Bel Abbès, Algeria in 1997. He is currently a professor in the computer science Department, University of Constantine 2, Algeria. His research interests are Micropocessor Architecture, Embedded systems, and real time applications.