I. J. Computer Network and Information Security, **2015, 9, 1-9**
Published Online August 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.09.01

A Secure Code-Based Authentication Scheme for RFID Systems

Noureddine Chikouche
Computer Science Department, University of M'sila, BP. 166 Ichebilia, 28000 M'sila, Algeria
Email: chiknour28@yahoo.fr

Foudil Cherif
Computer Science Department, LESIA Laboratory, University of Biskra, BP 145 RP, 07000 Biskra, Algeria
Email: foudil.cherif@yahoo.fr

Pierre-Louis Cayrel and Mohamed Benmohammed
Laboratoire Hubert Curien, UMR CNRS 5516, B âtiment F18 rue du prof. Benoit Lauras, 42000 Saint-Etienne, France
LIRE Laboratory, University of Constantine, P.O. Box 325, City Ain El Bey 25017 Constantine, Algeria
Email: {pierre.louis.cayrel@univ-st-etienne.fr, ben_moh123@yahoo.com}

Abstract—Two essential problems are still posed in terms of Radio Frequency Identification (RFID) systems, including: security and limitation of resources. Recently, Li et al.'s proposed a mutual authentication scheme for RFID systems in 2014, it is based on Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) McEliece cryptosystem. This cryptosystem is designed to reducing the key sizes. In this paper, we found that this scheme does not provide untraceability and forward secrecy properties. Furthermore, we propose an improved version of this scheme to eliminate existing vulnerabilities of studied scheme. It is based on the QC-MDPC McEliece cryptosystem with padding the plaintext by a random bit-string. Our work also includes a security comparison between our improved scheme and different code-based RFID authentication schemes. We prove secrecy and mutual authentication properties by AVISPA (Automated Validation of Internet Security Protocols and Applications) tools. Concerning the performance, our scheme is suitable for low-cost tags with resource limitation.

Index Terms—RFID, Security, McEliece cryptosystem, authentication scheme, QC-MDPC codes.

I. Introduction

The Radio Frequency Identification (RFID) is a technology without contact making possible the identification of an object, and applied in various domains (e.g. e-passport, access control, supply chain management, health, etc.). The typical RFID systems are comprised of three main components: the tag, the reader, and the server. The communication channel between the reader and the tag is based on communication by radio waves. Therefore, it is insecure, which makes it open in front of passive and active attacks.

In order to have secure authentication schemes, it is important that a RFID authentication scheme requires privacy and security proprieties, such as:

- ***Secrecy*** the verification that the identity of the tag or secret shared data is never passed on the interface radio frequency which can be spied.
- ***Mutual authentication:*** A RFID authentication scheme achieves mutual authentication, that is to say, it achieves reader's authentication and the tag's authentication.
- ***Untraceability*** The tag is untraceable if an intruder cannot tell whether he has seen the same tag twice or two different tags [1].
- ***Desynchronization resilience:*** We can define this property as follows: at session (*i*), the intruder can modify or block the transmitted messages between the tag and the reader. In the next session, if the authentication process fails, then the tag and the reader are not correlated and this protocol does not achieve desynchronization resilience. We note that this property specifies for RFID schemes that update a shared secret in each scheme run.
- ***Forward secrecy:*** One of abilities of intruder, 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.
- ***Replay attack resisting:*** It consists in replay precedent emitted messages in the same session of protocol or in various sessions of this same protocol.

In RFID system, two essential problems posed are security and limitation of resources. In the literature on design of RFID authentication schemes, we can find several schemes according to various primitives requirements: hash function, public-key cryptosystems, private-key cryptosystems, bitwise operators, and code-based cryptosystems, such as [2][3][4][5][6][7][8][9][10]. Several RFID authentication schemes based on error-correcting codes exist in the literature, like [3][11][4][12]

[13][14][15][25][26].

Recently, Li et al. [15] proposed a mutual authentication scheme for RFID systems, based on Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) **(**QC-MDPC) McEliece cryptosystem. This cryptosystem permits to reduce the key sizes [24]. In this paper, we found that this scheme does not provide untraceability and forward secrecy properties. To eliminate existing vulnerabilities of studied scheme, we propose an improved scheme, based on the QC-MDPC McEliece cryptosystem with padding the plaintext by a random bit-string. We provide security properties using AVISPA (Automated Validation of Internet Security Protocols and Applications) tools [16]. Our work also includes a comparison between the improved scheme and different code-based RFID authentication protocols in terms of security and performance.

The rest of this paper is organized as follows: section II presents code-based cryptography. Section III presents related work and analyzes the Li et al.'s scheme. In section IV, we give an improved version of Li et al. scheme. The section V presents a formal verification of the improved scheme and analyses the security properties. Section VI evaluates the performance of the improved scheme. Finally, the paper terminates with a conclusion.

II. Preliminaries

A. Code-based cryptography

Code-based cryptography allows the construction of different schemes (like public-key encryption scheme, identification scheme, etc.). It is based on difficult problems NP-complete and resists to quantum attacks. The encryption and decryption are high-speed and do not require any crypto-processor (for more information see [17]). Let $\mathcal{C}(n,k,t)$ be a binary linear code, where n is length, k is dimension which stands a generator matrix $\mathcal{G}$ (with k and n are positive integers and $k<n$). $\mathcal{C}$ is a t-error correcting linear code.

The first code-based cryptosystem is McEliece cryptosystem [18]. The security of this cryptosystem is based on two standard computational assumptions: the public-key is indistinguishable, and the syndrome decoding (SD) problem is hard.

B. McEliece cryptosystem based on QC-MDPC codes

Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) code is a linear block code with quasi-cyclic construction (see [13]) which permits to reduce the public key size.

- **Quasi-cyclic code**: An $C(n,r)$-code of length $n=\ell n_0$ is a quasi-cyclic code of order ℓ (and index n_0) if C is generated by a parity-check matrix $H=[H_{i,j}]$ where each $H_{i,j}$ is an $\ell\times\ell$ circulant matrix.
- **MDPC codes**: An $C(n,r,w)$-MDPC code is a linear code of length n and co-dimension r which stands a parity-check matrix of row weight w.

The McEliece cryptosystem based on QC-MDPC codes works as follows:

- **Key Generation**: generate $C(n,r,w)$-QC-MDPC code, with $n=\ell n_0$ and $r=\ell$. Select a vector F_2^n, of row weight w uniformly at random, as the initialization factor of generating $H\in F_n^{r\times n}$. The parity check matrix H is obtained from r-1 cyclic shifts by h. The matrix has the form $H=[H_0|H_1|...|H_{n_0-1}]$, where row weight of H_i is w_i and $w=\sum_{i=0}^{n_0-1} w_i$. A generator matrix $G=(I|Q)$ can be derived from the H. Note that the public key for encryption is $G\in F_2^{(n-r)\times n}$ and the private key is H.

$$Q=\begin{pmatrix} \left(H_{n_0-1}^{-1}.H_0\right)^T \\ \left(H_{n_0-1}^{-1}.H_1\right)^T \\ \cdots \\ \left(H_{n_0-1}^{-1}.H_{n_0-2}\right)^T \end{pmatrix}$$

- **Encryption**: To encrypt the message $m\in F_2^k$, where $k=n-r$, randomly generate $e\in F_2^n$ of $wt(e)\le t$. The ciphertext $c'\in F_2^n$ is $c'=mG\oplus e$.
- D**ecryption**: Let A_H a decoding algorithm equipped with the sparse parity check matrix H. To decrypt c' into m, compute $mG=A_H(mG\oplus e)$, and extract the plaintext m from the first k positions of mG.

C. Randomized McEliece cryptosystem

Nojima et al. in [19] 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 randomized McEliece is a probabilistic cryptosystem, whose encryption algorithm of message is as follows:

$$c'=c\oplus e=[rand\,//\,m]G\oplus e$$

Where $rand\in F_2^{k_1}$ is a random string and $m\in F_2^{k_2}$ is the plaintext. The dimension k is equal to k_1+k_2, with $k_1<bk$ and $b<1$.

D. Notations

Throughout the paper, we use the following notations:

T, R, S	The tag, the reader and the server
id	Identifier of tag
$\mathcal{G}$, *H*	Public-key and private-key matrices

v	Random vector generated by R
h	initialization vector shared between T and R
rand, *rand*'	Secret random vectors
hash(.)	One-way hash function
g(.)	Pseudo-random function
‖	Concatenation of two inputs
t	Integer numbers
e	Error vector of length n and weight $wt(e)$
$Right(e,k_1)$	Extract a substring from e, starting from the right-most bit, with length k_1
N_R	Nonce generated by reader
$rand_{old}$, $rand_{new}$	Two secret synchronization keys

III. Related Works

RFID authentication schemes based on error-correcting codes use various schemes: error-correcting code with secret parameters [11][3], randomized McEliece cryptosystem [4][26], randomized Niederreiter cryptosystem [12][13], Quasi-Dyadic Fix Domain Shrinking [14] and Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) McEliece cryptosystem [15].

The scheme proposed by Chien [11] and the scheme proposed by Malek and Miri [4] do not resist desynchronization attack. Cui et al's protocol [13] and Suzuki et al's scheme [12] do not achieve reader's authentication. The scheme proposed by Chien and Laih [3] does not achieve the forward secrecy.

In the next subsections, we discus the security of Li et al.'s protocol [15]. This protocol is based on Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) McEliece cryptosystem.

A. Review of the Li et al.'s scheme

Li et al. proposed in [15] a mutual RFID authentication based on the QC-MDPC McEliece cryptosystem. It was designed to secure mutual authentication and to resist replay attack.

In the initialization phase, the trusted center (e.g. server) generates the initialization vector $h \in F_2^n$, saves it in the tag T and the reader of R with identifier $id \in F_2^k$. The scheme works as follows (see Fig. 1):

- The reader R generates a random vector v and queries the tag T.
- After receiving the vector v, T randomly generates an error vector e, and then utilizes the vector h to create public-key matrix G for encryption. Then, it computes $c'=idG \oplus e$ and $h_1=hash(p // e)$, and sends c' and h_1 back to the reader.
- After receiving authentication message from R and transmitting them to back-end database, R performs a decoding algorithm with private key matrices and identifies the error vector e as well as id. From id, the server retrieves the corresponding value of id. It computes $hash(p // e)$ and compares it with h_1. If they are equal, R computes $h_2=hash(e)$ and sends it to T.
- T would compute $hash(e)$, if $hash(e)=h_2$, then the object of mutual authentication is achieved, authentication is successful, otherwise, the reader's authentication has failed.

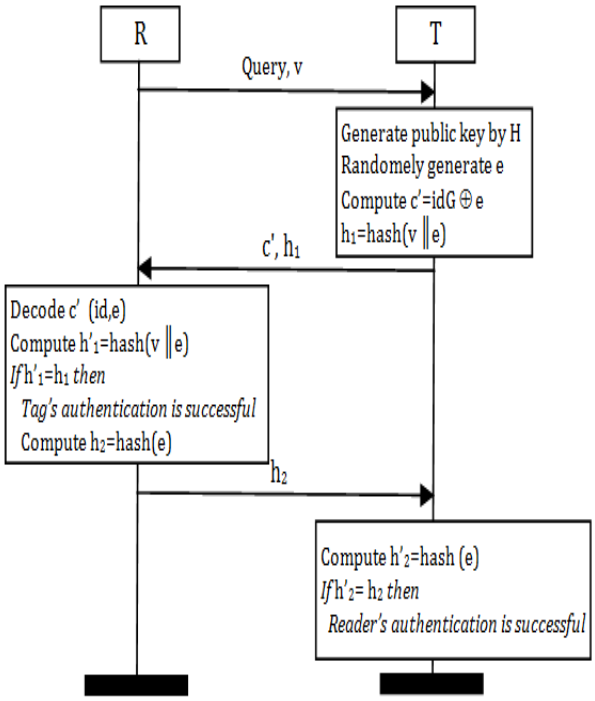

Fig.1. Li et al.'s Scheme [15].

B. Traceability attack

In the McEliece cryptosystem, the parameters (n,k,t) are public. With these information, and particularly, the minimum distance d and the Hamming weight t; the adversary can attempt to trace the tag with the following scenario:

- At session (i), the adversary intercepts ($c'_i=idG \oplus e_i$) and saves it.
- At session (j), it intercepts ($c'_j=idG \oplus e_j$).
- The intruder computes: $c'_i \oplus c'_j=idG \oplus e_i \oplus idG \oplus e_j$

We have $e_i \neq e_j$ and the identifier of the tag id is static in all sessions, this implicates: $c'_i \oplus c'_j=e_i \oplus e_j$. The Hamming weight of $(c'_i \oplus c'_j)$ is less than $2t+1$, and the codeword idG is fixed for all sessions leads to message-resend attack, and implicates, that this protocol does not provide untraceability.

C. Violate forward secrecy

If an intruder compromises a tag, then it might be able to derive previous secret data to track old transactions

involving that tag, thus violate forward secrecy. In Li et al.'s scheme, the data stored in the tag's memory are {*id*, *h*}, which remain constant in all the runs of scheme. An intruder breaking into the memory of tag gets the current *id*. The problem posed is the value of identifier is static and not dynamic. Therefore, this scheme does not achieve forward secrecy.

IV. The Improved Scheme

A. System framework

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

- The **tag** *T* is a small electronic device, supplemented with an antenna that can transmit and receive data via radio frequency. In our context, it is passive and stores {*id*, *rand*, *h*} which are strictly confidential. *T* implements key generation algorithm and encryption algorithm of QC-MDPC cryptosystem. It also implements pseudo-random number generator and supports bitwise operations (xor, and, ...).
- The **reader** is a device for reading and writing RFID tags by radio waves. In our scheme, *R* can generate the pseudo-random numbers.
- The **server** (or backend, database) is a centralized place that hosts all data regarding access permissions and may be consulted by reader. *S* has the sufficient storage space and computational resources. In our context, we implement decryption algorithm of QC-MDPC cryptosystem and PRNG (Pseudo Random Number Generator). It contains the private-key and the database which includes {*id*, $rand_{old}$, $rand_{new}$}.

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.

B. Threat Model

In our context, we use the Dolev-Yao model [20]. The intruder can be either passive (e.g. eavesdropper) or active (e.g. impersonator). It has complete control over the channel of communication between the tag and the reader. It can intercept any message passing through the wireless network, modify or block messages and it can also create new messages from its initial knowledge.

C. Description of the improved scheme

The proposed scheme is divided into two phases: the setup phase and the authentication phase.

Setup phase:

In this phase, the tags and the database server are initialized for authentication process to be performed in future. The server generates a random binary QC-MDPC code $\mathcal{C}(n,r,w)$. The server (trusted center) generates the initialization vector $h \in F_2^n$, the unique identifier of tag $id \in F_2^{k_2}$ and shared secret $rand \in F_2^{k_1}$. Then, the server sends {*id*, *rand*, *h*} to the tag through a secure channel. It stores in your database {*id*, *rand*} for each tag and *h*, where $rand=rand_{old}=rand_{new}$.

Authentication phase:

The mutual authentication phase takes place as follows (to see Fig. 2):

1) *R* generates a nonce N_R and sends it then as a request to the tag *T*.
2) *T* generates an error vector *e* with $wt(e) \le t$, and computes $c'=[rand \| id]\mathcal{G} \oplus e$. It also computes $U=g(id \| N_R \| e)$.
3) *T* sends *c*' with *U* to the reader, it resends the received *c*' and message *U* and nonce N_R to the server.
4) The server (reader) runs decryption algorithm to find *id*, *rand* and *e*. From *id*, in database, the server obtains the values of $\{rand_{old}, rand_{new}\}$. if $rand=rand_{old}$ or $rand=rand_{new}$ then the tag computes $U_1=g(id \| N_R \| e)$ (either $rand_{old}$ or $rand_{new}$) and verifies if $U_1 \stackrel{?}{=} U$. If they are equal, authentication of tag is successful; otherwise the authentication of tag has failed.
5. In this case the authentication of tag is successful. The server generates a random number $rand' \in F_2^{k_1}$ and computes $V=g(id \| N_R \| rand')$ and $P = rand' \oplus Right(e, k_1)$. It updates $rand_{old} \leftarrow rand_{new}$ and $rand_{new} \leftarrow rand'$, only in case the matched *rand* is $rand_{new}$.
6. *S* sends *P* and *V* to the tag.
7. *T* obtains *rand*' by computing $P \oplus Right(e, k_1)$. It computes $V_1=g(id \| N_R \| rand')$ and checking if $V_1 \stackrel{?}{=} V$. If they are equal, the authentication of reader is successful; otherwise the authentication of the reader will fail.
8. *T* updates the secret *rand* by the value of *rand*', in case of reader's authentication is successful.

V. Analysis of the Improved Scheme

A secure RFID authentication scheme should provide secrecy, mutual authentication and untraceability. It assures desynchronization resilience and forward secrecy. It also resists man-in-the-middle attack and replay attack. In this section, we discuss the security and privacy requirements of proposed scheme. The Table 1 shows the security comparison between the existing schemes and our improved scheme.

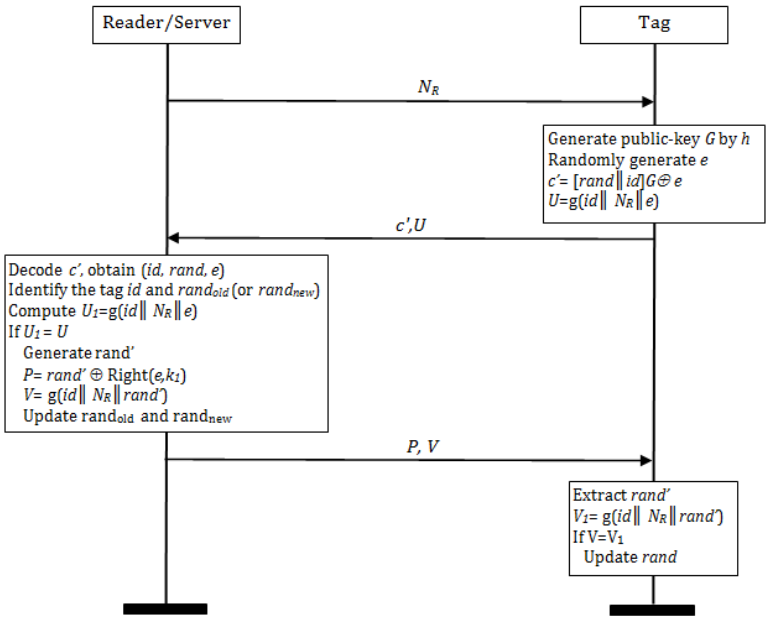

Fig.2. The Improved Scheme

Table 1. Security comparison

Properties	[13]	[14]	[4]	[15]	Our scheme
Secrecy	Y	Y	Y	Y	Y
Mutual Authentication	N	N	Y	Y	Y
Untraceability	Y	Y	Y	N	Y
Desynchronization resilience	Y	Y	N	Y	Y
Resist replay attacks	Y	Y	Y	Y	Y
Forward secrecy	N	N	Y	N	Y

A. Formal verification

To provide the security properties of our proposed scheme, we select AVISPA tools (Automated Validation of Internet Security Protocols and Applications) [16] for the following reasons: these tools are based on only one specification language named HLPSL language (High-Level Protocol Specification Language) [21]. These tools use different techniques of formal verification: automate trees, Solver SAT, Model-checking, and resolution of constraints. They can model a big number of security protocols (more than 90 protocols). AVISPA tools can detect active and passive attacks. Glouche et al. [28] developed a SPAN (Security Protocol ANimator) tool to animate the security protocols which are specified by HLPSL and verified by AVISPA tools. The threat model agrees in HLPSL is Dolev-Yao model [20] which is described in subsection III.B.

HLPSL is role-based language, formal, a modular and expressive. Protocol specification consists in two parties: basic roles and composition roles. The first part presents honest participants and the second part describes scenarios of basic roles. The composition roles consist in three parts: session, environment and goal. The session role defines the initial state of the system. The environment role shows sessions of protocol between honest participants. Before terminating the specification, we determine the security properties we want to verify. HLPSL can specify the secrecy and the authentication properties.

Our scheme requires the primitives: PRNG, nonce, xor-operator, public-key, private-key and encryption/ decryption of Randomized McEliece cryptosystem based on QC-MDPC codes. We have two honest agents tag and reader. We can present the ciphertext $c'=[id \| rand]\mathcal{G} \oplus e$ as $F_{Encry}([id, rand], PKG, E)$ that means encryption $[id \| rand]$ by public-key PKG (is matrix $\mathcal{G}$), then encoding the result by the private error vector E (is e). To obtain the value of E, one uses the decoding algorithm $\mathcal{A}_H$ So, The specification of this ciphertext by HLPSL is *{{Rand.ID}_PKG}_E*. We specify the functions *g*(.) and *Right*(.) by hash function. Other primitives are defined in HLPSL.

We define a ***session role*** where all the basic roles are instanced with concrete arguments. In the *reader*, we initialize the values $Rand_{old}$ and $Rand_{new}$ by *rand*.

The top-level role ***environment role*** contains global constants and a composition of one or more sessions, where the adversary may play some roles as legitimate participant. We use four parallel sessions to detect a replay and man-in-the-middle attacks. We provide a validation of properties: authentication of tag (*auth_tag*), authentication of reader (*auth_reader*), the secrecy of identifier of tag *id* (*sec_id*), and the secrecy of secret random number *rand* and the new random number *rand*' (*sec_rand* and *sec_randp*). These properties are specified in ***goal***. We also provide that our scheme resists to replay attack and man-in-the-middle attack.

HLPSL specification of our improved scheme is shown in Appendix A.

Running the AVISPA & SPAN tools on the improved scheme returns as follows in Fig.3. The tool output (CL-ATSE) shows that the scheme has been found to be safe and that no attacks has been found. We can thus deduct

that the diagnostic of AVISPA tools for our scheme is secure.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  UNTYPED_MODEL

PROTOCOL

C:\progra~1\SPAN\testsuite\results\S
pec_ImprLi.if

GOAL
  As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 2750 states
 Reachable  : 1696 states
 Translation: 0.01 seconds
 Computation: 0.39 seconds
```

Fig.3. Verification result

B. Security analysis

Untraceability To against the traceability attack, we agreed two mechanisms, (1) generate an error vector with dynamic length where wt(e)≤t, and we accept the principle of padding the plaintext with a random bit-string. This principle is applied in randomised McEliece cryptosystem, where the transmitted encoding codeword is different in each session.

In our scheme, we have two messages in two different sessions:

$$c'_i=c_i \oplus e_i, \text{ where } c_i=[rand_i // id]G$$

and

$$c'_j=c_j \oplus e_j, \text{ where } c_j=[rand_j // id]G$$

where $c_i \neq c_j$ and $e_i \neq e_j$. The intruder intercepts c'_i and c'_j as follows:

$$c'_i \oplus c'_j=c_i \oplus c_j \oplus e_i \oplus e_j,$$

In case $wt(e_i)=wt(e_j)=t$ and $c_1=c_2$ or the adversary knows the linear relation between the messages m_i of c_1 and c_2 then this protocol does not resist traceability attack.

Concerning our scheme, the vector $rand_i$, which is used in session i is different from $rand_j$ which is used in session j, and there is no linear relation between them, $rand_i$ and $rand_j$ are randomly generated. We note that $wt(e_i)$ and $wt(e_j)$ are secret and different. Then, our scheme resists traceability attack.

Desynchronization resilience To achieve this property, we used two secret synchronization vectors, $rand_{old}$ and $rand_{new}$ stored in the server. In case the last message of scheme is blocked by the adversary, then in the next run, when the server received N_R,c' and decrypts c', then the tag mentions a problem in the authentication of tag because the secret vector stored in the server and the vector received from the tag are different. In our scheme, we do not found this problem because we use the old vector *rand_old* to resolve this problem, then the authentication of tag is successful.

Forward secrecy {*id*, *rand*, *h*} are data stored in the tag's memory. Before terminate run of session, the tag updates the value of *rand*, the new one is *rand*', is generated randomly by the server. The adversary could not acquire the previous random vector *rand* used in the prior sessions. So, the proposed RFID authentication scheme could provide forward secrecy.

VI. Performance Evaluation

The performance of authentication protocols is mainly measured by storage space on tag and computation cost in tag and server and communications cost between the tag and the reader.

The storage cost, the scheme proposed by [13] [14] requires public-key matrix which is of important size compared to available space in low-cost tags. The improved scheme requires {*id*, *rand*, *h*} with size $k+n$, is same space required to [15]. The QC-MDPC code $\mathcal{C}[n=9602,r=4801,w=90]$, $n_0=2$ and $t=84$ are parameters proposed by Misoczki et al. [24] for a 2^{80} security. Using these parameters, the space requires in the tag are 14403 bits ($n+r$). If we choose $k_1=4300$ and $k_2=501$ which is suitable with condition $k_1<bk$ and $b=9/10$. Then, the number of tags which can use in our scheme is 2^{501} tags. Thus, we can implement our scheme in low-cost tags, such as Mifare Classic 1K and Mifare Plus support space memory 1KB to 4 KB [27].

The calculation cost, our scheme requires QC-MDPC McEliece cryptosystem with padding the plaintext by a random bit-string, PRNG and xor operation. The McEliece cryptosystem is high-speed encryption and decryption compared to asymmetric cryptosystems based on number theory, such as Elliptic Cube Cryptosystem (ECC). The QC-MDPC McEliece cryptosystem is designed to reducing the key sizes [24]. The works of [22][23] presents a very lightweight implementation of the QC-MDPC McEliece cryptosystem for embedded devices. We used the PRNG to generate $\{N_R, e\}$ and compute $g(.)$, which is very fast. We also cite that, the server does not need an exhaustive search for obtaining the value of *id*. When the server decrypts the encoded codeword, it can obtain the value of tag's identifier.

The communication cost between a reader and a tag consists of: the total bit size of the transmitted messages. Concerning our scheme, the total of the bits of the messages of communication in authentication process is $3l_p+n+k_1$), where l_p is the length of the generated random number.

VII. Conclusion

Recently, Li et al. proposed a RFID authentication scheme based in QC-MDPC McEliece cryptosystem. In this paper, we have discussed the weaknesses of this scheme. The results of security analysis showed that this scheme does not provide untraceability and forward secrecy.

We also proposed an improved scheme which is based on the QC-MDPC McEliece cryptosystem with padding the plaintext by a random bit-string. We have proved secrecy and mutual authentication properties by AVISPA tools. The careful security analysis shows that the improved scheme achieves untraceability, desynchronization resilience, and forward secrecy. It also resists man-in-the-middle attack and replay attack. Moreover, the performance evaluation shows that the new scheme is compatible with the constrained computational and memory resources of the RFID tags.

References

[1] 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.

[2] H.-Y. Chien, "Tree-based matched RFID yoking making it more practical and efficient," *I.J.Computer Network and Information Security*, vol. 1, no. 1, pp. 1–7, 2009.

[3] 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.

[4] B. Malek and A. Miri, "Lightweight mutual RFID authentication," in *Proceedings of IEEE ICC'12*, 2012, pp. 868–872.

[5] V. N. Kumar and B. Srinivasan, "Biometric passport validation scheme using radio frequency identification," *I.J.Computer Network and Information Security*, vol. 5, no. 4, pp. 30–39, 2013.

[6] S. Rostampour, M. E. Namin, and M. Hosseinzadeh, "A novel mutual RFID authentication protocol with low complexity and high security," *I.J. Modern Education and Computer Science*, vol. 6, no. 1, pp. 17–24, 2014.

[7] M. Benssalah, M. Djeddou, and K. Drouiche, "Security enhancement of the authenticated RFID security mechanism based on chaotic maps," *Security and Communication Networks*, vol. 7, no. 1, 2014.

[8] Q. L. Cai, Y. J. Zhan, and J. Yang, "The improvement of RFID authentication protocols based on R-RAPSE," *Journal of Networks*, vol. 9, no. 1, pp. 28–35, 2014.

[9] M. Pourpouneh, R. Ramezanian, and F. Salahi, "An improvement over a server-less RFID authentication protocol," *I.J.Computer Network and Information Security*, vol. 7, no. 1, pp. 31–37, 2015.

[10] S. Dhal and I. S. Gupta, "Object authentication using RFID technology: A multi-tag approach," *I.J.Computer Network and Information Security*, vol. 7, no. 4, pp. 44–53, 2015.

[11] H.-Y. Chien, "Secure access control schemes for RFID systems with anonymity," in *Proceedings of MDM'06*. IEEE, 2006, p. 96.

[12] M. Suzuki, K. Kobara, and H. Imai, "Privacy enhanced and light weight RFID system without tag synchronization and exhaustive search," in *Proceedings of IEEE ICSMC'2006*. IEEE, 2006, pp. 1250–1255.

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

[14] 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 2010)*. IEEE, 2010, pp. 1–5.

[15] Z. Li, R. Zhang, Y. Yang, and Z. Li, "A provable secure mutual RFID authentication protocol based on error-correct code," in *Proceedings of 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. IEEE, 2014, pp. 73–78.

[16] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, , L. Compagna, J. Cuellar, P. Drielsma, P.-C. Heam, J. Mantovani, S. Mödersheim, , D. von Oheimb, M. Rusinowitch, J. S. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "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, 2005, pp. 281–285.

[17] R. Overbeck and N. Sendrier, *Code-based cryptography*. Springer, 2009, Post-Quantum Cryptography, pp. 95–145.

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

[19] 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.

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

[21] T. A. team, "HLPSL tutorial the Beginner's guide to modelling and analysing internet security protocols," AVISPA project, Tech. Rep., 2006.

[22] I. von Maurich and T. Güneysu, "Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices," in *Proceedings of the Conference on Design, Automation & Test in Europe, DATE '14*. IEEE, 2014, pp. 1–6.

[23] S. Heyse, I. von Maurich, and T. Güneysu, "Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices," in *Cryptographic Hardware and Embedded Systems - CHES 2013*, G. Bertoni and J.-S. Coron, Eds.

[24] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes," in *Cryptology ePrint Archive, Report 2012/409*, 2012.

[25] N. Chikouche, F. Cherif, P-.L. Cayrel, M. Benmohammed "Weaknesses in Two RFID Authentication Protocols," i*n Proceedings of C2SI 2015* (S. El Hajji et al. Eds.), LNCS 9084, pp. 162–172, Springer, 2015.

[26] N. Chikouche, F. Cherif, P-.L. Cayrel, M. Benmohammed "Improved RFID Authentication Protocol Based on Randomized McEliece Cryptosystem," *International Journal of Network Security*, vol. 17, no. 4, pp. 413–422, 2015.

[27] The Mifar cards, http://www.mifare.net, 2015.

[28] Y. Glouche, T. Genet, O. Heen, E. Houssay and R. Saillard, "SPAN - a Security Protocol ANimator for AVISPA," version 1.6, Manual Report, http://www.irisa.fr/celtique/genet/span/, 2009.

Authors' Profiles

Noureddine Chikouche, received his the engineer degree in computer science from the University of Constantine, Algeria, in 1999. In addition, he received his master's degree 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. He supervised several Ph.D. and Magister theses which have been successfully defended these last years.

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, where he is also a head of group in the LIRE laboratory. His research interests are micropocessor architecture, embeded systems, and real time applications.

APPENDIX A

HLPSL SPECIFICATION FOR OUR SCHEME

```
role tag (T,R: agent, ID,Rand: text,
          Fg,Right: hash_func,
          PKG: public_key,
          Snd,Rec: channel(dy))
    played_by T
    def=
      local State: nat,
            Nr, E, Randp: text
    init State:= 0
    transition
1. State = 0 /\ Rec(Nr') =|> State':= 1
  /\ E':= new()
  /\ Snd({{ID.Rand}_PKG}_E'.Fg(ID.Nr'.E'))
  /\ witness(T,R,tag_auth,E')
  /\ secret({ID},sec_id, {T,R})
  /\ secret({Rand},sec_rand, {T,R})
2. State = 1 /\
 Rec(xor(Randp',Right(E)).Fg(ID.Nr.Randp'))
   =|> State' := 2
   /\ request(T,R,reader_auth,Nr)
   /\  Rand':=Randp'
end role

role reader ( R,T: agent,
              ID,Rnew,Rold: text,
              Fg,Right : hash_func,
              PKG: public_key,
              Snd,Rec: channel(dy))
    played_by R
    def=
      local State: nat,
            Nr, E, Randp: text
      init State:= 0
      transition
1. State = 0 /\ Rec(start) =|>
   State':= 1 /\ Nr':= new() /\ Snd(Nr')
   /\ witness(R,T,reader_auth,Nr')

2. State = 1 /\
   Rec({{ID.Rnew}_PKG}_E'.Fg(ID.Nr.E'))
   =|> State': = 2 /\ Randp':= new()
   /\ request(R,T,tag_auth,E') /\
Snd(xor(Randp',Right(E')).Fg(ID.Nr.Randp'))
   /\ Rold':=Rnew /\ Rnew':=Randp'
   /\ secret({Randp'},sec_randp, {R,T})

2. State = 1 /\
    Rec({{ID.Rold}_PKG}_E'.Fg(ID.Nr.E'))
    =|> State': = 2 /\ Randp':= Rnew
    /\ request(R,T,tag_auth,E') /\
Snd(xor(Randp',Right(E')).Fg(ID.Nr.Randp'))
    /\ secret({Randp'},sec_randp, {R,T})
end role

role session(R,T: agent, ID,Rand: text,
             Fg,Right: hash_func,
             PKG: public_key)
  def=
  local Se,Re,Sf,Rf: channel(dy)
  const reader_auth, tag_auth, sec_id,
  sec_rand,sec_randp: protocol_id
  composition
  tag(T,R,ID,Rand,Fg,Right,PKG, Se,Re)
  /\ reader(R,T,ID,Rand,Rand,Fg,Right,PKG,
```

```
     Sf,Rf)
end role

role environment() def=
  const t,r,i: agent, id,rand: text,
       g,right: hash_func,
       pkG: public_key

  intruder_knowledge = {t,r,i,g,right,pkG}
  composition
     session(r,t,id,rand,g,right,pkG)
  /\ session(r,t,id,rand,g,right,pkG)
end role

goal
   secrecy_of sec_id
   secrecy_of sec_rand
   secrecy_of sec_randp
   authentication_on reader_auth
   authentication_on tag_auth
end goal

    environment()
```

How to cite this paper: Noureddine Chikouche, Foudil Cherif, Pierre-Louis Cayrel, Mohamed Benmohammed,"A Secure Code-Based Authentication Scheme for RFID Systems", IJCNIS, vol.7, no.9, pp.1-9, 2015.DOI: 10.5815/ijcnis.2015.09.01

