Wireless Pers Commun
DOI 10.1007/s11277-017-4181-8

RFID Authentication Protocols Based on Error-Correcting Codes: A Survey

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

Abstract Code-based cryptography is a very promising research area. It allows the construction of different cryptographic mechanisms (e.g. identification protocol, public-key cryptosystem, etc.). McEliece cryptosystem is the first code-based public-key cryptosystem; several variants of this cryptosystem were proposed to design various security protocols in different systems. In this paper, we present a survey on various and recent authentication protocols in radio frequency identification systems which use diverse variants of the McEliece cryptosystem. Moreover, we discuss the security and the performance of each presented protocol.

Keywords RFID · Error-correcting codes · Authentication protocols · Vulnerabilities

✉ Noureddine Chikouche
noureddine.chikouche@univ-msila.dz

Foudil Cherif
foud_cherif@yahoo.fr

Pierre-Louis Cayrel
pierre.louis.cayrel@univ-st-etienne.fr

Mohamed Benmohammed
ben_moh123@yahoo.com

[1] Computer Science Department, University of M'sila, BP. 166, Ichebilia, 28000 M'sila, Algeria

[2] LESIA Laboratory, Computer Science Department, University of Biskra, BP 145, RP, 07000 Biskra, Algeria

[3] Laboratoire Hubert Curien, UMR CNRS 5516, Bâtiment F18 rue du prof. Benoît Lauras, 42000 Saint-Étienne, France

[4] LIRE Laboratory, University of Constantine 2, P.O. Box 325, City Ain El Bey, 25017 Constantine, Algeria

Published online: 16 May 2017

1 Introduction

The Internet of Things (IoT) is an up to date technology paradigm envisioned as an internet network of physical objects (i.e. devices and machines) capable of interacting with each other without requiring human-to-human or human-to-computer interaction. One of the most important technologies of the IoT is radio frequency identification (RFID). This technology enables the automatic identification of objects using radio waves. It is applied in different applications including healthcare, credit card, passport, logistics, access control, library, location tracking, etc. A typical RFID system involves three parties: the RFID tag, the RFID reader, and the back-end server. The RFID tag consists of a microchip (with an antenna) which has a memory that can store tag's identifier and other information. The RFID reader is a device which communicates with RFID tags via radio waves; It can be employed to write the data received from server into RFID tags. The back-end server provides the database of the items identified by tags.

Security is a main issue in RFID systems. The communication between the RFID tag and the RFID reader is unsecured as it is based on radio waves. To cope with this issue, there is an important number of authentication protocols for RFID systems in the literature, they adopt several cryptographic mechanisms, such as hash functions [1, 3, 14, 20], private-key cryptosystems [35, 39], public-key cryptosystems (PKC) [16, 17, 23, 42], and algebraic primitives [2, 19, 40, 43].

The code-based cryptographic schemes adopt error-correcting codes to produce public-keys out of private matrices. They are used in several RFID protocols [10–13, 26, 27, 37]. Despite the large size of the public keys, code-based cryptosystems provide fast and secure encryption and decryption schemes. Furthermore, code-based scheme produce very short signature and very efficient hash-functions and stream ciphers. One major domain where code-based cryptography can prove its efficiently is resistance to quantum computer attacks. In February 2016, the NIST (National Institute of Standards and Technology) [9] outlined plans to "initiate a standardisation effort in post-quantum cryptography". It's crucial to re-evaluate the cryptographic schemes used to protect information in different communications (e.g Internet, mobile, IoT, etc.) and also to improve quantum-safe cryptography. For further information about the quantum cryptography trends, the reader is redirected to the survey [33].

In this paper, we are interested in RFID protocols based on error-correcting codes. The first code-based cryptosystem was proposed by McEliece [28] in 1978. Since its proposal, many outstanding variants of this cryptosystem were designed, such as Niederreiter cryptosystem [31], randomized McEliece and Niederreiter cryptosystems [32], CCA2-secure variant of McEliece cryptosystem [8, 21], McEliece cryptosystem based on quasi-dyadic Goppa codes [29], Quasi-Dyadic Fix Domain Shrinking [37], and McEliece cryptosystem based on Quasi Cyclic-Moderate Density Parity Check code (QC-MDPC) [30]. Each variant has specific characteristics in terms of security (e.g. semantic security) and in terms of performance (e.g. length of public key).

In this paper, we present a survey of various and recent RFID authentication protocols which use diverse code-based encryption schemes. We identify some weaknesses of the studied protocols. Furthermore, we discuss the security and evaluate the performance of each protocol.

The remainder of this paper is structured as follows: Sect. 2 introduces concepts of code-based cryptography. Section 3 presents the security requirements and the adversarial

model. In Sect. 4, we study code-based RFID authentication protocols. A brief discussion is presented in Sect. 5. Section 6 concludes our work.

2 Code-Based Cryptography

Code-based cryptography has high-speed encryption and decryption algorithms compared to public-key schemes based on number theory (e.g. RSA scheme and El Gamal scheme). It is easy to implement as it does not need any cryptographic processor. It is employed in the construction of various cryptographic mechanisms (e.g. digital signature, public-key cryptosystem, secret sharing, identification schemes, etc.). Moreover, its computational complexity is NP-complete problems.

Let $\mathcal{C}[n, k, d]$ be a binary linear code, where n is length, k is dimension which stands as a generator matrix G (with k and n as positive integers and $k < n$), and $\mathcal{C}$ can correct up to t errors.

2.1 McEliece Cryptosystem

The first public key cryptosystem (PKC) based on algebraic coding theory was invented by McEliece [28], and it was named after him. The security of McEliece scheme is based on two distinct problems: the public-key is indistinguishable, the syndrome decoding (SD) problem is hard. This cryptosystem has the following components:

- *Key generation* Generates three private matrices, a generator matrix $G' \in \mathbb{F}_2^{k\times n}$ of a binary Goppa code $\mathcal{C}$, a permutation matrix $P \in \mathbb{F}_2^{n\times n}$ and an invertible matrix $S' \in \mathbb{F}_2^{k\times k}$. Then computes $G = S'G'P$, which is another valid generator matrix. The private-key is $(S', G', P, \mathcal{A}(.))$, where $\mathcal{A}(.)$ is a polynomial-time decoding algorithm and the public-key is (G, t).
- *Encryption* Generates an error vector $e \in \mathbb{F}_2^n$ of weight $\mathsf{wt}(e) \leq t$, computes the cryptogram $c' \in \mathbb{F}_2^n$ where $c' = c \oplus e$. The codeword $c \in \mathbb{F}_2^n$ is mG and the plaintext is $m \in \mathbb{F}_2^k$.
- *Decryption* Given a cryptogram c', computes $z = c'P^{-1}$, $y = \mathcal{A}(z)$ and outputs $m = yS'^{-1}$.

2.2 Niederreiter Cryptosystem

Niederreiter cryptosystem [31] proposed the dual version of McEliece cryptosystem. It is based on the syndrome decoding problem using the parity check matrix. In key generation phase, it uses a parity check matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ instead of a generator matrix G'. The main advantage of this cryptosystem compared to McEliece is reduction of the public-key size from $k \times n$ to $n \times (n-k)$ and length of the cryptogram from n to $(n-k)$. This cryptosystem has the following components:

- *Key generation* Generates a parity check matrix $H' \in \mathbb{F}_2^{(n-k)\times n}$ of a binary linear $\mathcal{C}$, a permutation matrix $P \in \mathbb{F}_2^{n\times n}$, an invertible matrix $Q \in \mathbb{F}_2^{(n-k)\times(n-k)}$. The private-key is $(Q, H', P, \mathcal{A}(.))$ with $\mathcal{A}(.)$ a decoding algorithm until $\frac{d}{2}$ errors. The public-key is $H \in \mathbb{F}_2^{(n-k)\times n} = QH'P$ and t integer $< \frac{d}{2}$.

- *Encryption* Decodes message m to error vector $e \in \mathbb{F}_2^n$ with $\mathsf{wt}(e) = t$, then calculates the ciphertext $S = H^T e$.
- *Decryption* Computes $Q^{-1}S = Q^{-1}QH'(Pe)$, and $P^{-1}(Pe)$, then encodes e into message m.

2.3 Randomized Niederreiter and McEliece Cryptosystems

Nojima et al. [32] proposed a new version of McEliece scheme (and its dual, the Niederreiter PKC), it is named randomized McEliece cryptosystem. They proved formally that padding the plaintext with a random bit-string provides semantic security against chosen plaintext attack (IND-CPA) under standard assumptions.

2.3.1 Randomized McEliece Cryptosystem

Let k_1, k_2 be two integers such that $k = k_1 + k_2$ and $k_1 < bk$ where $b < 1$ is a positive rational number (e.g. $\frac{9}{10}$). The encryption algorithm works as follows:

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

where $r \in \mathbb{F}_2^{k_1}$ is a random string, $m \in \mathbb{F}_2^{k_2}$ is the message. $G_1 \in \mathbb{F}_2^{k_1 \times n}$ and $G_2 \in \mathbb{F}_2^{k_2 \times n}$ are sub-matrices of G.

The decryption algorithm is almost the same as McEliece, the difference is that it outputs only the last k_2 bits of the decrypted plaintext.

2.3.2 Randomized Niederreiter Cryptosystem

Let n_1 and n_2 be two integers with $n = n_1 + n_2$ and $n_1 = bn$ for some positive rational number b. The encryption algorithm is as follows:

$$c' = [r \parallel m]H = r\mathcal{H}_1 \oplus m\mathcal{H}_2 \tag{2}$$

where $r \in \mathbb{F}_2^{n_1}$ is a random string with weight $t_1 = \lfloor \frac{n_1 \times t}{n_1 + n_2} \rfloor$ and $m \in \mathbb{F}_2^{n_2}$ is the message with weight $t_2 = \lfloor \frac{n_2 \times t}{n_1 + n_2} \rfloor$. $H_1 \in \mathbb{F}_2^{n_1 \times (n-k)}$ and $H_2 \in \mathbb{F}_2^{n_2 \times (n-k)}$ are sub-matrices of H. The decryption algorithm is the same as Niederreiter except that it outputs only the last n_2 bits of the decrypted plaintext.

2.4 McEliece Cryptosystem Based on QC-MDPC Codes

Misoczki et al. [30] defined in 2013 a modified version of McEliece cryptosystem which is based on Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) code. QC-MDPC code is a linear block code with quasi-cyclic construction. Use this code allows to reduce the size of the public-key. This cryptosystem has the following components:

- *Key Generation*: Generates a $\mathcal{C}(n, k, w)$-QC-MDPC code. Chooses a vector $h' \in \mathbb{F}_2^n$,of row weight w uniformly at random, as the initialization factor of generating $H \in \mathbb{F}_2^{k \times n}$. The parity check matrix H is obtained from $k - 1$ cyclic shifts by h'. The matrix has the form $H = [H_0|H_1|\cdots|H_{n_0-1}]$, 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 is $G \in \mathbb{F}_2^{(n-k)\times n}$ and the private key is H.

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

- *Encryption*: To encrypt the plaintext $m \in \mathbb{F}_2^{n-k}$, generates $e \in \mathbb{F}_2^n$ of $\mathsf{wt}(e) \leq t$. The cryptogram $c' \in \mathbb{F}_2^n$ is $c' = mG \oplus e$.
- *Decryption*: To decrypt c' into m, computes $mG = \mathcal{A}_H(mG \oplus e)$, where $\mathcal{A}_H$ is a t-error-correcting (QC-)MDPC decoding algorithm, then extracts the plaintext m from the first $n - k$ positions of mG.

2.5 Message-Resend Attack

The message-resend attack [5] is a major critical attack on McEliece cryptosystem. This attack is based on the use of structural weaknesses of the protocol. Detecting this attack in RFID authentication protocol implies that the adversary can track the tag as run in different sessions. Therefore, we mention that this protocol does not provide untraceability property. The message-resend attack is described as follows:

We assume that the adversary intercepts the transmitted cryptograms in different sessions, $c_1 = mG \oplus e_1$ and $c_2 = mG \oplus e_2$ where $e_1 \neq e_2$. The adversary can easily recover the plaintext m from the system of c_i with $i = 2$. Note that $c_1 \oplus c_2 = e_1 \oplus e_2 \bmod 2$.

Observing the Hamming weight of the sum of two cryptograms, the resend of message can be detected easily. The plaintext m identical in different runs and the weight of the sum cannot exceed $2t$. With these conditions, Heiman [18] showed that the resend of message can be detected.

3 Security Requirements and Adversarial Model

3.1 Security Requirements

The basic requirements for security and privacy in RFID authentication protocols include:

- *Secrecy* It means that secrets like tag's identifier and shared key can only be read by the authorized entities, the legitimate tag and the legitimate reader.
- *Mutual authentication* The authentication is a mechanism permitting to identify the tag or the reader (or the server) and to certify their identity. The mutual authentication is provided if the protocol achieves both tag's authentication and reader's authentication.
- *Untraceability* The tag is untraceable if an adversary cannot tell whether it has seen the same tag twice, or two different tags [44]. This property is one of the important privacy properties.
- *Desynchronization resilience* When the active intruder blocks or modifies messages before ending the session of RFID protocol (update's phase) and if the protocol is run successfully in the next session, then this protocol achieves desynchronization

resilience property. This property is specific for RFID protocols updating a tag's identifier or a shared secret in each run.

- *Forward secrecy* The adversary compromises the secret shared by the reader and the tag and then tries to compute the previous secret to reveal the information exchanged earlier between the reader and the tag. If the trials of the adversary are successful then we say that this protocol cannot provide security against forward secrecy attack.
- *Active attacks resistance* The adversary can interfere with messages transmitted between an authentic tag and reader by insertion, modification, interruption, or suppression, in order to impersonate it later.
- *Replay attacks resistance* They consist in replaying precedent emitted messages in the same or in different sessions of the RFID authentication protocol.
- *Critical attacks resistance* These attacks are based on the use of structural weaknesses of the protocol. A description of all possible critical attacks against code-based encryption schemes are listed in [7].

3.2 Adversarial Model

In the RFID systems, the communication between the tag and the reader is based on radio frequency waves. This permits to the adversary $\mathcal{A}$ to completely control the exchanged messages. However, the communication between the server and the reader is assumed secure.

Authors of [36] proposed a classification of adversaries depending on their objectives, level of interference, presence, and available resources. In our model, we assume that the adversary is active which means that it can eavesdrop on messages passing through the channel of communication reader-tag, interrupt, or modify messages. $\mathcal{A}$ can also create new messages from its initial knowledge. The adversary can communicate with the honest entities (i.e. the tag and the reader) and can compromise the secret information stored in a legitimate tag. $\mathcal{A}$ can launch replay attacks, active attacks, and critical attacks. Moreover, the adversary possesses sufficient memory to store all messages transmitted between an authentic tag and reader. $\mathcal{A}$ can employ different cryptographic and algebraic primitives, like hash functions, bitwise operators, and pseudo-random numbers generators (PRNG).

4 Code-Based RFID Authentication Protocols

Code-based RFID authentication protocols apply different code-based cryptosystems: randomized McEliece cryptosystem [12, 27], QC-MDPC McEliece cryptosystem [13, 25, 26], Quasi-Dyadic Fix Domain Shrinking [37], combination between two variants of McEliece cryptosystem [10], and combination with cryptosystem based on number theory [11].

To perform a description and analysis of each protocol, we provide only a sketch to facilitate description and discussion. For detailed descriptions of these protocols, the reader is redirected to the original publications. We note that the public matrix and private matrices are stored in back-end server (or reader).

We use the following notations (also, we use the notation from Sect. 2:

T, R	The tag and the reader
id	Identifier of T
K	Symmetric-key between T and R

u	Number of authorized readers
e_R, e, p	Error vector, length n and weight t
c_T	Codeword, where $c_T = idG$
$h(.)$	Hash function
$g(.)$	Pseudo-random generator function (PRNG)
r, r'	Secret random vectors
N_R, N_T	Random vectors generated by reader and tag, respectively
A_p	Circulant matrix $(n \times n)$
r_{old}, r_{new}	Secret synchronization values stored in the reader R
$\phi_{n,t'}(m)$	Decoding bijective application (transform m into error vector e)
$Right(x)$	The rightmost l bits of x
$Left(x)$	The leftmost l bits of x.

4.1 Sekino et al. [37]

Sekino et al. proposed an RFID authentication protocol based on Niederreiter scheme. The authors combine the Quasi-dyadic (Goppa) codes [29] and Fix Domain Shrinking of Niederreiter personalized public-key cryptosystem (P^2KC) [22]. The aim of this approach is to reduce the size of public-key matrix of Niederreiter cryptosystem so as to permit storing it in RFID tags. P^2KC is a technique to produce a public key individually used by certain *id*, called Personalized Public Key (PPK). The reader can determine the tag's identifier by decrypting the cryptogram with PPK.

In this challenge-response protocol, the data stored in tag's memory are $\{H_1, c_2\}$ where c_2 is a vector of length $(n-k)$ and H_1 is a matrix of length $(n-k) \times (n_1 - (n-k))/t$. The authentication protocol is depicted in Fig. 1.

The protocol of Sekino et al. does not achieve reader's authentication, it is one-way authentication. In this protocol, the adversary can derive the c_2 and matrix H_1 from a

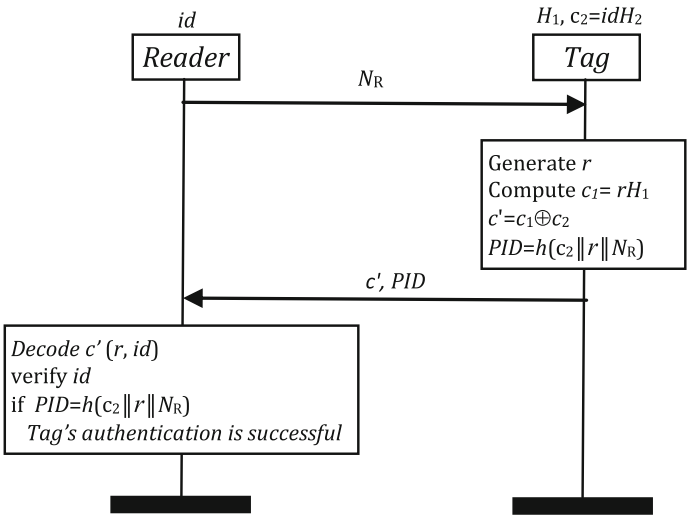

Fig. 1 Protocol of Sekino et al. [37]

compromised tag. These data stored inside the legitimate tag are static during its life. Therefore, this protocol does not achieve the forward secrecy.

About performance, this protocol is not suitable with low-cost tags because it requires an important memory space to store the matrix H_1 and it needs the implementation of hash function.

4.2 Malek and Miri [27]

This protocol is based on randomized McEliece public-key cryptosystem. The RFID tag can communicate with a set of readers. It stores $\{r\mathcal{G}_1 \oplus id\mathcal{G}_2, id\}$ for each authorized reader id_R, where id_R is the reader's identifier. On the other hand, the database of the reader (server) is composed of $\{id_R, r, id\}$. The authentication phase is shown in Fig. 2.

When the adversary interrupts the last message y', the new nonce r updated in database is r', however in RFID tag, there is no modification for $\{rG_1 \oplus idG_2\}$. In the next session and after decrypting y, the received id, r is different from id, r'. Thus, the tag's authentication has failed. Consequentially, this protocol does not resist the desynchronization attack.

The required space in tag's memory is depending on the number of authorized readers, when it is considerable then one requires $u \times (n + k_2)$ bits. Another important constraint,

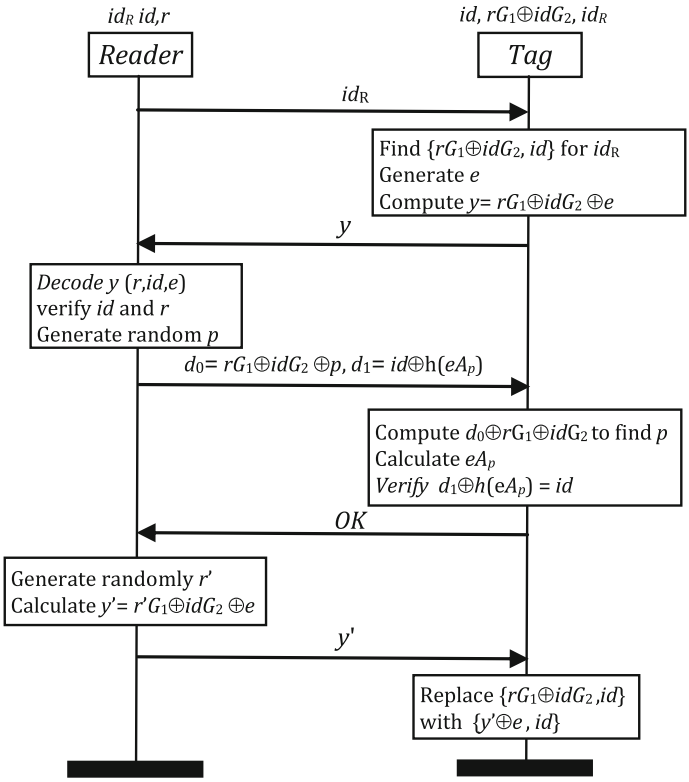

Fig. 2 Protocol of Malek and Miri [27]

the circulate matrix A_p, where the RFID tag needs an important space in volatile memory $n \times n$ bits to compute eA_p.

4.3 Chien [11]

Using the combination of Rabin cryptosystem and the error-correcting codes, Chien [11] has proposed an RFID authentication protocol, where the designer of this protocol claimed that the used of this combination achieved privacy properties including untraceability and anonymity. The server keeps $\{id, K, c_T, r_{old}, r_{new}\}$ for each RFID tag, and stores two large primes p and q as private key of Rabin cryptosystem. The tag's memory contains $\{id, K, c_T, r\}$ and the public-key of Rabin cryptosystem N where $N = p \times q$.

The principal idea of Chien's protocol is that the tag randomly adds an error vector e to its pre-assigned codeword c_T to have $c' = c_T \oplus e$, and computes $V_T = g(e \oplus g(N_R \oplus K \oplus r))$. Then it applies encryption algorithm of Rabin cryptosystem to compute $M = m^2 mod N$, where m is $c' \parallel V_T$. Upon receiving M,the reader which knows the private-key p and q, can apply the Chinese reminder theory to get the four possible answers $\{m_1, m_2, m_3, m_4\}$, uses the secret parity matrix to identify the error vector e and derives the corresponding codeword c_T for each m_i,and then verifies which one satisfies the verification equation. All steps of Chien's authentication protocol are depicted in Fig. 3.

The Rabin cryptosystem (especially of RSA) is based on number theory, the author selects $N = 512$ as size of public-key, but the size key 512-bit number is factored in 1999 by the Number Field Sieve factoring method (NFS). If the adversary determinates the private-key p and q, this implicates a privacy problem in Chien's protocol because the

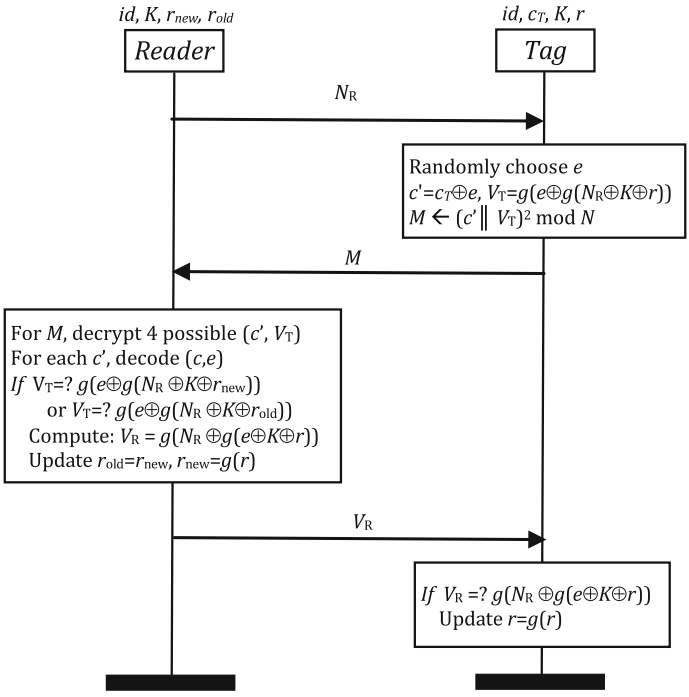

Fig. 3 Protocol of Chien [11]

codeword c_T is static and the parameters t or d are known by the adversary. With this condition, this protocol does not resist message-resend attack and consequently untraceability attack too.

Concerning the performance of Chien's protocol, the Rabin cryptosystem is relatively not fast to code-based cryptosystems. Using this Rabin cryptosystem implicates adding a space memory and other computational operations (square modular and square root modular). Among techniques used to resolve the problem of modular square root to determine the correct plaintext (4 plaintexts possible), one can cite redundancy scheme. But the author of [11] did not use this scheme, this implicates the decoding of codeword and computation of g four times.

4.4 Li et al. [25]

This mutual RFID authentication is based on the McEliece cryptosystem with QC-MDPC codes. The tag's memory contains the identifier id and the vector h' which is used to generate the public-key matrix. Li et al.'s protocol requires pseudo-random generator, hash function and bit-wise operators. The steps of authentication phase are summarized in Fig. 4.

In [13], authors demonstrated that the adversary can attempt to trace the tag with the following scenario: the adversary intercepts the cryptogram $(c'_i = id\mathcal{G} \oplus e_i)$ and saves it. In the next run of the protocol, the adversary intercepts other cryptogram $(c'_j = id\mathcal{G} \oplus e_j)$. $\mathcal{A}$ calculates $c'_i \oplus c'_j = id\mathcal{G} \oplus e_i \oplus id\mathcal{G} \oplus e_j$. The tag's identifier id is fixed, then the codeword $id\mathcal{G}$ is static for all sessions and leads to message-resend attack. Therefore, this protocol does not resist tracing attack.

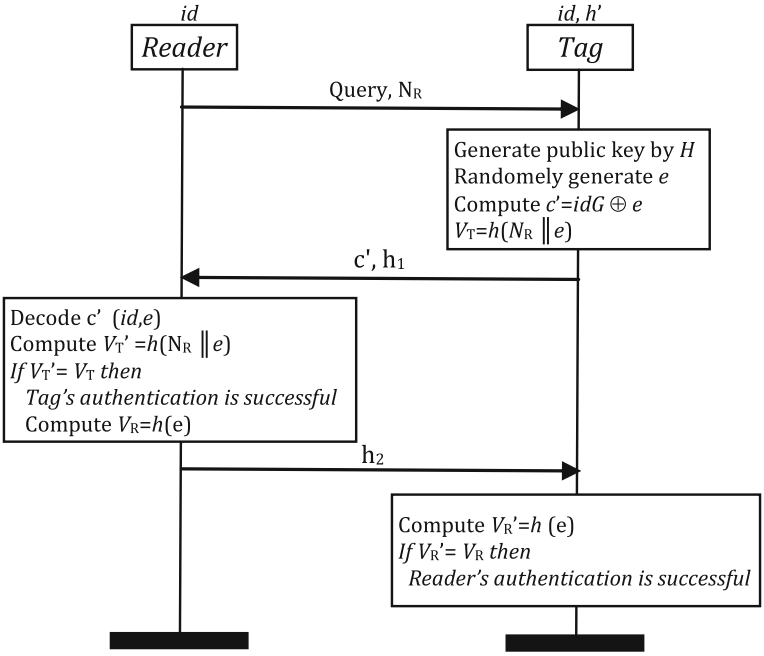

Fig. 4 Protocol of Li et al. [25]

Another vulnerability in this protocol is that it does not achieve forward secrecy; The data stored in the tag's memory are $\{id, h\}$. These data remain their values in different runs of the protocol. Therefore, the adversary can obtain the previous tag's identifier used in the prior sessions.

The Li et al.'s protocol is not compatible with low-cost RFID tags because it needs implementation of hash function.

4.5 Chen et al. [10]

This protocol adopts error-correcting code for RFID systems. The main objective of this protocol is a specific target tag among a large group of tags. Since the RFID reader may receive a substantial number of tags' responses for a single query, the protocol adds a filtering mechanism to prevent the reader from having to check every responding message. The reader (server) keeps $\{id, K, sp\}$ where sp is syndrome pattern. The server writes $\{id, K, sp, G', H\}$ into the storage memory of the tag. The required primitives in Chen et al.'s protocol and implemented in different entities of the system are $g(.)$, $h(.)$, and bit-wise operators. The steps of authentication phase are summarized in Fig. 5.

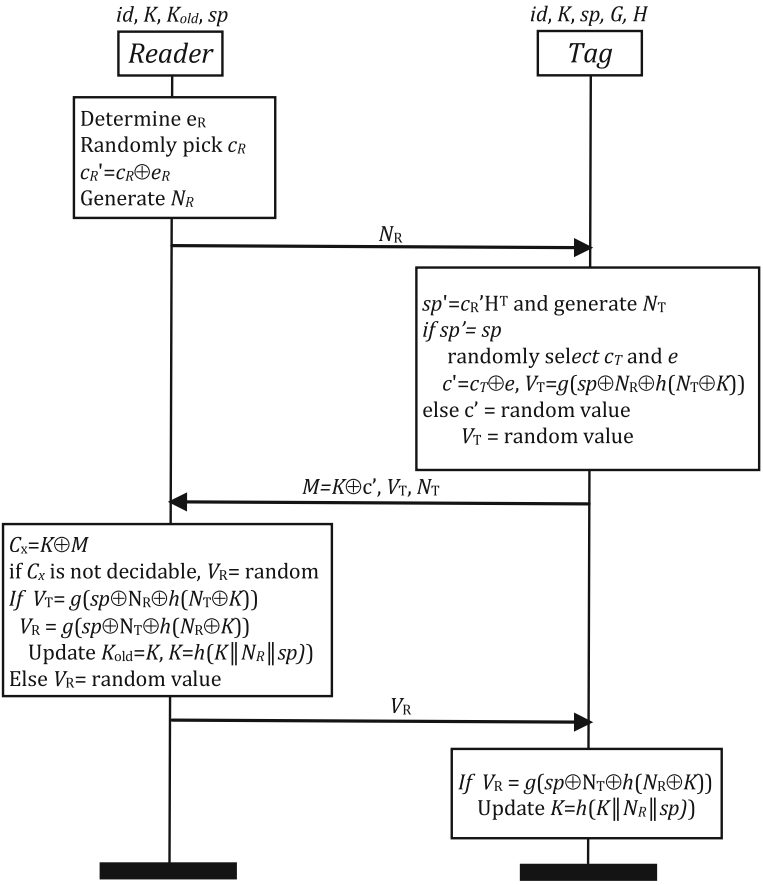

Fig. 5 Protocol of Chen et al. [10]

Chen et al. claimed that their protocol is a realisable scheme fulfilling security and privacy requirements. However, the work of Ergular [15] proved that this protocol does not resist tracing attack. In addition, he discovered another attack which is a key recovery where an adversary can compromise tag's secret key in practical time by only querying this tag for several times.

We point out another problem that is the space requirement in tag's memory. The tag requires an important space to store the parity matrix H with length of $(n-k) \times n$ and the generator matrix G' with length $k \times n$. For example, in case of security level is 2^{80}, the parameters of Goppa code are $C[\mathrm{n} = 2048, \mathrm{k} = 1751, \mathrm{d} = 56]$, the space required to store the two matrices H and G' is 501.23 KB. And this is not suitable for low-cost tags.

4.6 Chikouche et al. [12, 13]

Chikouche et al. have proposed two improved RFID authentication protocols using two different code-based schemes. The authentication phases of these protocols [12, 13] are summarized in Fig. 6.

In the first paper [12], the authors have proposed an RFID protocol based on the randomized McEliece cryptosystem. It adopts an efficient decoding/encoding algorithm to produce an error vector with fixed weight. The only datum stored in the tag's memory is the dynamic identifier (*DID*) of length n and which is updated in each run. The authors verified the untraceability property using the privacy model of Ouafi–Phan [34].

In the second paper [13], the authors analysed a recent protocol proposed by Li et al. [25] and proved that this protocol does not satisfy forward secrecy and untraceability properties. The authors proposed a revised version to avoid the detected attacks. The improved protocol is based on the combination of randomized McEliece cryptosystem with QC-MDPC codes. This protocol requires execute matrix operations compared with the first protocol.

We cite here that the authors of these protocols [12, 13] agreed an automated tool to validate the security properties, namely AVISPA tool (Automated Verification Internet

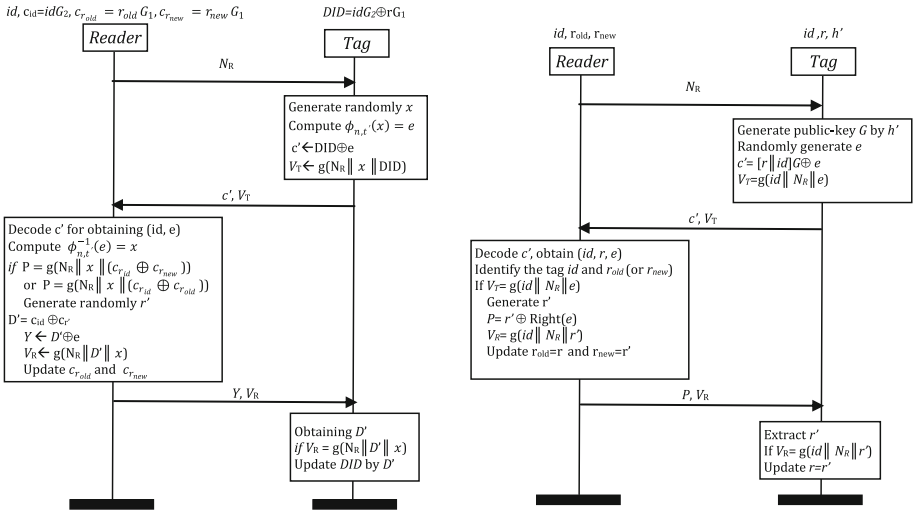

Fig. 6 Protocols of Chikouche et al. [12] (*left*) and [13] (*right*)

Protocol and its Applications) [4]. The security analysis demonstrated that these protocols are secured.

Concerning the computational cost of these protocols, we note that the first protocol [12] requires only PRNG and bitwise operators. However, the second protocol [13] needs the latter cited operations and also matrix operations which may affect the efficiency of the protocol.

4.7 Liu et al. [26]

Liu et al. [26] have proposed a recent lightweight mutual authentication protocol based on QC-MDPC McEliece scheme for RFID systems. The tag's memory contains two items of information $\{id, h'\}$, where the length of id is k bits and the length of vector h' is n bits. The tag uses this vector to generate the public-key so as to calculate the codeword $(N_R \oplus N_T)G$. Figure 7 shown authentication phase of Liu et al.'s protocol.

Liu et al. claimed that their protocol is efficient against essential attacks of RFID systems including location privacy, tag anonymity, forward security, resistance to de-synchronization attack and replay attack.

Concerning the security of this protocol, we noticed that the data stored in the memory of RFID tag have been maintained the same values in different sessions. This characteristic

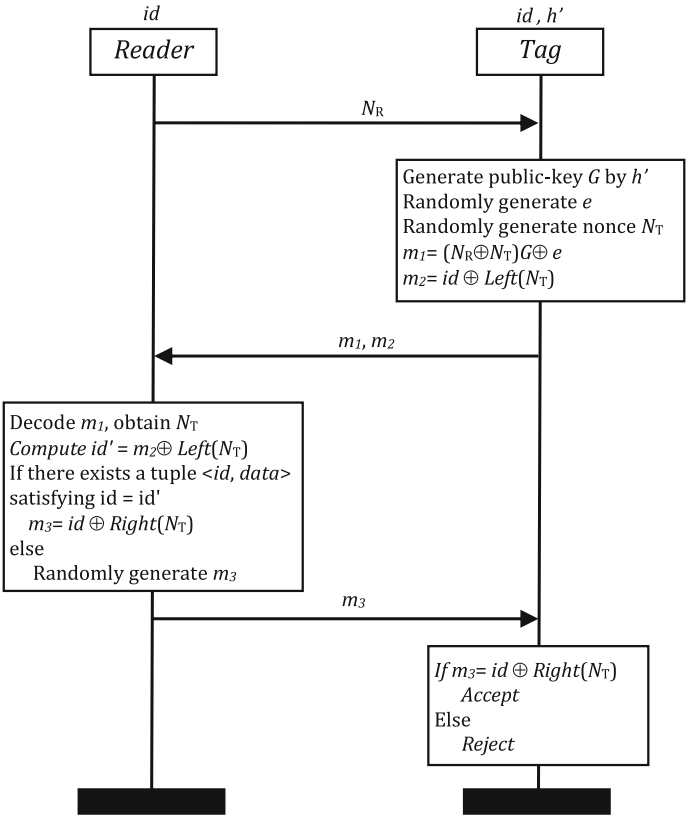

Fig. 7 Protocol of Liu et al. [26]

allows the adversary to break into the memory of the targeted tag with the static *id*. Thus, the Liu et al.'s protocol does not achieve the forward secrecy.

5 Discussion

The design and implementation of authentication protocols in RFID systems depend on three constraints: firstly, it is necessary to achieve the different security properties and particularly secrecy and mutual authentication. To achieve these properties, one specifies the protocol by a specification language and uses formal tools to determine the result of automatic validation (for more details see [6, 41]). Secondly, the protocol must validate the privacy properties and particularly untraceability (for more details see [24, 38]). Finally, the limitation of tag's resources. It is necessary to improve the performance of the protocol: minimize the required memory and the calculation cost.

The Table 1 provides a summary of the security analysis on the existing code-based RFID authentication protocols. The considered security and privacy requirements are: mutual authentication (M.A), untraceability (Unt), desynchronization resilience (D.R), forward secrecy (F.S), and replay attack resistance (R.R).

The main reason of tracing attack in code-based RFID protocols is articulated on the nature of the codeword, in other terms: when the tag's identifier value is static in all sessions as in [11, 25] and the adversary knows the parameters d or t, then it can follow the trace of the tag. To avoid this attack, one agrees the approach of dynamic codeword where the value of the encoded codeword is different from one session to another. There are two methods to realise this approach, the tag stores the codeword in its memory and updates it before finishing the session as in [12, 27]. The second method is padding the tag's identifier with a random vector to compute the codeword as in [13, 26, 37].

The adversary can compromise secrets stored in the tag when the data stored in tag's memory remain the same in all runs, then the protocol cannot resist the forward secrecy attack as in [10, 26, 37]. One can agree the same approach used for avoiding tracing attack where one stores the updated codeword or random vector in memory of tag at the end of each session.

With the described approach, we have avoided the cited attacks, but one concludes another attack which is desynchronization attack as in [27]. The adversary can block (or modify) the transmitted messages between the entities of RFID systems to create a disturbance in the communication reader-tag. Therefore the authentication process of the next session will fail because these entities (tag/reader) are no more correlated. The solution is to adopt two secret synchronization vectors (codeword or random vector), the old value

Table 1 Comparison of security and privacy properties

	M.A	Unt	D.R	F.S	R.R
Sekino et al. [37]	N	Y	Y	N	Y
Malek and Miri [27]	Y	Y	N	Y	Y
Chien [11]	Y	N[a]	Y	Y	Y
Li et al. [25]	Y	N	Y	Y	Y
Chen et al. [10]	Y	N	Y	N	Y
Chikouche et al. [12, 13]	Y	Y	Y	Y	Y
Liu et al. [26]	Y	Y	Y	N	Y

[a] If the adversary breaks the Rabin scheme

and the new value as [11, 12]. These vectors are stored in the database of the server. In case of any problem in the authentication process with the new value, the server uses the old value to complete the authentication process. Therefore, this approach permits to avoid the desynchronization attack.

A number of code-based protocols require hash function as [10, 25, 37] this primitive is not compatible with the capabilities of low-cost tags, a great number of gates is required for its implementation. The primitives used in the lowest cost RFID tags are bit-wise operations (e.g. or-exclusive, bit-wise and, etc.), random number generator (PRNG), and bit shifts (e.g. logical shift, rotate, etc.).

The main advantage of adopting error-correcting codes in RFID protocols is that they do not need to do exhaustive search to obtain the identifier from a database contrary to other categories such as hash-based RFID protocols. On the other hand, the big disadvantage is the size of public-key matrix. We find that some protocols stored this matrix or a part of it in their tag's memory such as [10, 37] which is not compatible with storage requirement in low-cost tags. There are other protocols adopting the mechanism of QC-MDPC to generate a public-key as [13, 25, 26] where the tag stores a vector of length n bits. In the paper [45], the authors have presented a lightweight implementation of the McEliece scheme with QC-MDPC codes for embedded devices, as Xilinx FPGAs. Despite that the generation of a public-key has been needed execute matrix operations and to store the large matrix in a volatile memory. The best approach to avoid the problems posed in the two described approaches—storing matrix or using QC-MDPC codes—is storing only the codeword as [11, 12, 27]. This is suitable with the capabilities of low-cost tags where the RFID tag requires only bitwise operators and needs small memory space compared to other approaches.

6 Conclusion

This paper has shown and analysed the recent RFID authentication protocols based on error-correcting codes. These protocols adopt different variants of the McEliece PKC (e.g. randomized McEliece, McEliece based on QC-MDPC codes, etc.). We have shown that there are several protocols that cannot provide security and privacy against major RFID attacks. Moreover, we have discussed their performances in terms of computation cost and storage requirements.

CCA2-secure variants of McEliece cryptosystem are not adopted in previously proposed code-based RFID protocols because they require important resources, memory and computation. The proposition of a new variant of CCA2-secure compatibles with the capabilities of low-cost RFID tags will be our future work.

References

1. Agudo, I., Ruben, R., & Lopez, J. (2013). A privacy-aware continuous authentication scheme for proximity-based access control. *Computers & Security*, *39*, 117–126.
2. Alavi, S. M., Baghery, K., Abdolmaleki, B., & Aref, M. R. (2015). Traceability analysis of recent RFID authentication protocols. *Wireless Personal Communications*, *83*(3), 1663–1682.
3. Alqarnia, A., Alabdulhafitha, M., & Sampalli, S. (2014). A proposed RFID authentication protocol based on two stages of authentication. In *Proceedings of international workshop on privacy and security*

in healthcare (PSCare14), Procedia Computer Science (Vol. 37, pp. 503–510). Amsterdam: Elsevier B.V.
4. Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., et al. (2005). The AVISPA tool for the automated validation of internet security protocols and applications. In *International conference on computer aided verification, Lecture Notes in Computer Science* (Vol. 3576, pp. 281–285). Berlin: Springer.
5. Berson, T. A. (1997). Failure of the McEliece public-key cryptosystem under message-resend and related-message attack. In *Advances in cryptology—CRYPTO '97, Lecture Notes in Computer Science* (Vol. 1294, pp. 213–220). Berlin: Springer.
6. Blanchet, B. (2012). Security protocol verification: Symbolic and computational models. In *Principles of security and trust post 2012, Lecture Notes in Computer Science* (Vol. 7215, pp. 3–29). Berlin: Springer.
7. Cayrel, P. L., Gueye, C. T., Ndiaye, O., & Niebuhr, R. (2015). Critical attacks in code-based cryptography. *International Journal of Information and Coding Theory*, *3*(2), 158–176.
8. Cayrel, P.L., Hoffmann, G., & Persichetti, E. (2012). Efficient implementation of a CCA2-secure variant of McEliece using generalized Srivastava codes. In *Public key cryptography—PKC 2012, Lecture Notes in Computer Science* (Vol. 7293, pp. 138–155). Berlin: Springer.
9. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., et al. (2016). Report on post-quantum cryptography. NISTIR8105. DRAFT.
10. Chen, C. M., Chen, S. M., Zheng, X., Chen, P. Y., & Sun, H. M. (2014). A secure RFID authentication protocol adopting error correction code. *The Scientific World Journal*. doi:10.1155/2014/704623.
11. Chien, H. Y. (2013). Combining Rabin cryptosystem and error correction codes to facilitate anonymous authentication with un-traceability for low-end devices. *Computer Networks*, *57*, 2705–2717.
12. Chikouche, N., Cherif, F., Cayrel, P. L., & Benmohammed, M. (2015). Improved RFID authentication protocol based on randomized McEliece cryptosystem. *International Journal of Network Security*, *17*(4), 413–422.
13. Chikouche, N., Cherif, F., Cayrel, P. L., & Benmohammed, M. (2015). A secure code-based authentication scheme for RFID systems. *IJ Computer Network and Information Security*, *7*(9), 1–9.
14. Dehkordi, M. H., & Farzaneh, Y. (2014). Improvement of the hash-based RFID mutual authentication protocol. *Wireless Personal Communications*, *75*(1), 219–232.
15. Erguler, I. (2014). A key recovery attack on error correcting code based a lightweight security protocol. *IACR Cryptology*. ePrint Archive 475. http://eprint.iacr.org/2014/475
16. Farash, M. S., Nawaz, O., Mahmood, K., Chaudhry, S. A., & Khan, M. K. (2016). A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. *Journal of Medical Systems*, *40*(7), 165.
17. He, D., Kumar, N., Chilamkurti, N., & Lee, J. H. (2014). Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *Journal of Medical Systems*, *38*(10), 116.
18. Heiman, R. (1987). On the security of cryptosystems based on linear error-correcting codes. Master's Thesis, Feinberg Graduate School of the Weizman Institute of Science.
19. Huang, P., Mu, H., & Zhang, C. (2014). A new lightweight RFID grouping proof protocol. In *Advanced technologies, embedded and multimedia for human-centric computing: HumanCom and EMC 2013, Lecture Notes in Electrical Engineering* (Vol. 260, pp. 869–876). Berlin: Springer.
20. Kaul, S. D., & Awasthi, A. K. (2013). RFID authentication protocol to enhance patient medication safety. *Journal of Medical Systems*, *37*(6), 9979.
21. Kobara, K., & Imai, H. (2001). Semantically secure McEliece public-key cryptosystems—conversions for mceliece PKC. In *Public key cryptography, PKC 2001, Lecture Notes in Computer Science* (Vol. 1992, pp. 19–35). Berlin: Springer.
22. Kobara, K., & Imai, H. (2006). Personalized-public-key cryptosystem(P2KC)-application where public-key size of Niederreiter PKC can be reduced. In *Workshop on codes and lattices in cryptography (CLC2006)* (pp. 61–68)
23. Kumar, A., Gopal, K., & Alok, A. (2015). A novel trusted hierarchy construction for RFID-sensor based MANETs using ECC. *ETRI Journal*, *37*(1), 186–196.
24. Lee, K. (2013). Privacy of RFID models and protocols. PhD Thesis, Queensland University of Technology, Brisbane, Australia.
25. Li, Z., Zhang, R., Yang, Y., & Li, Z. (2014). 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* (pp. 73–78). IEEE.
26. Liu, Z., Zhang, W., & Wu, C. (2015). A lightweight code-based authentication protocol for RFID systems. In *Applications and Techniques in Information Security, ATIS 2015*

27. Malek, B., & Miri, A. (2012). Lightweight mutual RFID authentication. In *Proceedings of IEEE international conference on communications* (pp. 868–872). IEEE.
28. McEliece, R. J. (1978). A public-key system based on algebraic coding theory. Tech. Rep. DSN Progress Report 44, Jet Propulsion Lab.
29. Misoczki, R., & Barreto, P. S. L. M. (2009). Compact McEliece keys from goppa codes. In*Selected areas in cryptography, SAC 2009, Lecture Notes in Computer Science* (Vol. 5867, pp. 376–392). Berlin: Springer.
30. Misoczki, R., Tillich, J. P., Sendrier, N., & Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *Proceedings of IEEE international symposium on information theory (ISIT)* (pp. 2069–2073). IEEE.
31. Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. *Problems Control Information Theory*, *15*(2), 159–166.
32. Nojima, R., Imai, H., Kobara, K., & Morozov, K. (2008). Semantic security for the McEliece cryptosystem without random oracles. *Designs, Codes and Cryptography*, *49*(1), 289–305.
33. Noor-ul Ain, W., Atta-ur Rahman, M., Nadeem, M., & Abbasi, A. G. (2016). Quantum cryptography trends: A milestone in information security. In *Advances in intelligent systems and computing* (Vol. 420, pp. 25–39). Berlin: Springer.
34. Ouafi, K., & Phan, R. C. W. (2008). Privacy of recent RFID authentication protocols. In *Information security practice and experience, ISPEC 2008, Lecture Notes in Computer Science* (Vol. 4991, pp. 263–277). Berlin: Springer.
35. Pham, T., Hasan, M., & Yu, H. (2012). A RFID mutual authentication protocol based on AES algorithm. In *UKACC international conference on control (CONTROL 2012)* (pp. 997–1002). IEEE.
36. Ranasinghe, D. C., & Cole, P. H. (2008). *An evaluation framework* (pp. 157–167). Berlin: Springer.
37. Sekino, T., Cui, Y., Kobara, K., & Imai, H. (2010). Privacy enhanced RFID using quasi-dyadic fix domain shrinking. In *Proceedings of global telecommunications conference (GLOBECOM 2010)* (pp. 1–5). IEEE.
38. Vaudenay, S. (2010). Privacy models for rfid schemes. In *Radio frequency identification: Security and privacy issues, RFIDSec 2010, Lecture Notes in Computer Science* (Vol. 6370, pp. 65–65). Berlin: Springer.
39. Wang, J., Floerkemeier, C., & Sarma, S. E. (2014). Session-based security enhancement of RFID systems for emerging open-loop applications. *Personal and Ubiquitous Computing*, *18*(8), 1881–1891.
40. Wang, S., Liu, S., & Chen, D. (2015). Security analysis and improvement on two RFID authentication protocols. *Wireless Personal Communications*, *82*(1), 21–33.
41. Woo-Sik, B. (2014). Formal verification of an RFID authentication protocol based on hash function and secret code. *Wireless Personal Communications*, *79*(4), 2595–2609.
42. Xin, H., Pin, Y., & Kun, L. (2014). NTRU-based RFID tripartite authentication protocol. *Computer Engineering Applications*, *50*(3), 63–66.
43. Zhuang, X., Zhu, Y., & Chang, C. C. (2014). A new ultralightweight RFID protocol for low-cost tags: R^2AP. *Wireless Personal Communications*, *79*(3), 1787–1802.
44. van Deursen, T., Mauw, S., & Radomirović, S. (2008). Untraceability of RFID protocols. In: *Information security theory and practices. Smart devices, convergence and next generation networks, WISTP 2008, Lecture Notes in Computer Science* (Vol. 5019, pp. 1–15). Berlin: Springer.
45. von Maurich, I., & Güneysu, T. (2014). Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices. In *Proceedings of the conference on design, automation & test in Europe (DATE'14)* (pp. 1–6)

Noureddine Chikouche is an associate professor in computer science department, at University of M'sila; He received his Ph.D. degree in computer science from the University of Biskra, Algeria, in 2016. He also received his master's degree in computer science from the University of M'sila, in 2010 and his engineer degree in computer science from the University of Constantine, in 1999. His research interests include formal verification of cryptographic protocols, RFID security , 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 these 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 microprocessor architecture, embedded systems, and real time applications.