International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.3 (May-2020)
http://dx.doi.org/10.12785/ijcds/090309

EAP-SRES: An Enhanced Authentication Protocol for Secure Remote Education Systems Using NFC Technology

Noureddine Chikouche[1,2] and Foudil Cherif[2]

[1] *Computer scienceDepartment, University of M'sila, M'sila, Algeria*
[2] *Department of computer science,University of M'sila, M'sila, Algeria*

Received 9 Jun. 2019, Revised 15 Jan. 2020, Accepted 6 Mar. 2020, Published 1 May 2020

Abstract: Radio Frequency Identification (RFID) and Near Field Communication (NFC) are wireless technologies applied in several domains, among which, remote education. The communication between different components of this system is unsecured, which may lead to several security and privacy problems. Designing authentication protocols to protect a remote education system in an open environment (e.g. NFC, RFID, and Internet) is a challenging task. Recently, Yang et al. proposed a mutual authentication protocol based on the hash function for RFID systems to secure this system. Yang et al. showed that their protocol is secure and can resist various attacks. This work proves that Yang et al.'s protocol does not achieve reader authentication, location privacy, and security forward. Furthermore, we propose an enhanced authentication protocol for secure remote education systems (EAP-SRES) using NFC technology. Our protocol is based on post-quantum cryptosystem to resist quantum attacks. Security analysis by using CL-AtSe (Constraint Logic based Attack Searcher) tool and Ouafi-Phan privacy model shows that the EAP-SRES protocol achieves the requirements of mutual authentication, untraceability and resists different possible attacks. In addition, EAP-SRES protocol is very efficient in term of performance.

Keywords: Authentication Protocol, RFID Security, NFC Security, Privacy, Code-Based Cryptography

1. INTRODUCTION

NFC (Near Field Communication) is ubiquitous computing wireless technology. This technology is very important in the world of today; It is applied in different applications and domains of the Internet of Things (IoT) [1, 2], such as access control, payment, library, etc.

The RFID (Radio Frequency Identification) system can identify the objects that carry RFID tags when they pass near an RFID reader according to the used frequency band. NFC like RFID is a wireless technology that allows communication and data sharing between two compatible devices at a short distance. There are three modes in NFC system: reader/writer, card emulation, and peer-to-peer [3].

- In reader/writer mode, NFC mobile can modify and read the information stored in NFC tag.
- In peer-to-peer mode, two NFC devices can share files and transfer data by establishing a bidirectional connection.
- In card emulation mode, NFC mobile communicates with an NFC reader as an RFID tag.

NFC technology is integrated into several devices (e.g. mobile, laptop, and tablet computer) and this will become widespread on all mobile devices in the upcoming years. There are several works in the education domain that support the importance of using RFID/NFC technologies, such as [4, 5].

One of the most important challenges related to IoT technology is privacy and security [6, 7]. Designing authentication protocols to secure different systems in open environments (e.g. NFC, RFID, and Internet) is a challenging area. In the literature, several RFID/NFC security protocols have been proposed in order to ensure privacy and security requirements [8-17]. To evaluate an authentication protocol as a secure one, three conditions must be fulfilled: (1) it uses hardness cryptographic primitives, (2) it is correct and (2) it achieves different security requirements. We can prove these conditions by using formal models and automated tools.

In remote education application, there are two important works [15, 18]. Bai & Huang [18] proposed a security approach to ensure the communications in an interactive remote education system by using a delay tolerant network (DTN). The authors used a hybrid encryption scheme, where they adopt the RSA scheme as

E-mail: noureddine.chikouche@univ-msila.dz

public-key scheme. However, the required RSA scheme is not effective in terms of computation. Recently, Yang et al. [15] proposed an RFID mutual authentication protocol for RFID systems by using hash function. The authors showed that their scheme was resistant to replay, location, and eavesdropping attacks. In addition, the authors proved that the proposed mechanism is safe and applicable.

This paper focuses on privacy and security analysis of the protocol proposed by Yang et al. [15]. The analysis results prove that the Yang et al.'s protocol does not achieve reader authentication, location privacy, and forward secrecy. Moreover, it is not effective for low-cost tags. We give an enhanced authentication protocol based on a lightweight post-quantum cryptosystem to secure remote education systems (EAP-SRES) that use NFC technology. Moreover, we verify the security of EAP-SRES protocol by using CL-AtSe (Constraint Logic based Attack Searcher) tool [19].

The rest of this paper is organized as follows: section 2 shows the adversarial model and the security requirements. Section 3 discusses the lightweight public-key cryptosystems. In section 4, we review and analyze the security of the Yang et al.'s protocol. We present our enhanced protocol in section 5. In section 6, we evaluate the security and the performance of our improved protocol and compare it with other protocols. Finally, the paper terminates with a conclusion.

2. BACKGROUND

This section describes different privacy and security properties to secure an authentication protocol in NFC/RFID technologies. We also provide the adversary model used in the security analysis of the studied protocol and its improvement.

A. Security and privacy requirements

In study, the security of authentication protocols in RES needs to validate privacy and security requirements.

1) Secrecy:

It signifies that secret data (e.g. tag's identifier) can be accessible only to those whose access is allowed. The secret data are not passed on the opening environment without protection; there is a possibility of spying by an attacker.

2) Tag authentication

It signifies that the ability of the RFID/NFC reader to verify that the legitimate RFID/NFC tag is communicating with it.

3) Reader authentication

It signifies that the ability of the RFID/NFC tag to confirm that the legitimate RFID/NFC reader is communicating with it.

4) Location privacy (or untraceability)

The location privacy requirement guarantees that the intruder can neither determine who the RFID/NFC tag is not distinguished whether two sessions are run by the same RFID/NFC tag.

5) Desynchronization resilience

We validate this requirement when the authentication protocol updates shared secrets before ending the scheme. The process goes as follows: in session (*i*), the attacker blocks or modifies the last transmitted message between the reader and the tag. When the process of authentication is failing in the next session, then the authentication protocol does not ensure the desynchronization resilience property where the reader and the tag are not correlated.

6) Replay attack resistance

It consists in replaying previously emitted messages in the different or same in sessions of the protocol.

7) Forward secrecy

When the attacker can disclose the secret data of RFID/NFC tag after hacking the system, it assays to calculate the precedent secret to reveal the data transmitted earlier between the entities. If its try is successful, then this authentication scheme does not ensure the forward secrecy property.

B. Attack model

Before analysis of security protocol, one should define the attack model agreed. In this work, we assume the following capabilities of the adversary:

- The adversary can completely control the exchanged messages between the tag and the reader.
- It can modify or block messages passing through the network.
- It can make new messages and send them to communicate with the legitimate entities.
- It has sufficient processing power and space memory.
- It can apply different cryptographic operations, such as an encryption algorithm, random number generator (PRNG), and hash functions.

3. LIGHTWEIGHT PUBLIC-KEY CRYPTOSYSTEMS

In this section, we present different existing lightweight public-key cryptosystems and justify why we opt for the code-based cryptography in the design of our improved protocol.

To choose a cryptosystem compatible with the capabilities of NFC/RFID devices, one must take into account two important constraints, the performance, and the security. As to the performance, we discuss the effectiveness of implementation of public-key cryptosystems in NFC tags. The server has sufficient computational resources and storage space. The Public-key cryptosystems (PKCs) are divided into three main categories according to the hardness mathematical problem: cryptosystems based on number theory, lattice-based cryptosystems, and code-based cryptosystems.

In the first category, there are an important number of authentication protocols which require the elliptic curve cryptosystem (ECC) [20]. The main advantage of ECC compared to other cryptosystems (e.g., RSA and El Gamal) is the smaller key sizes, where a key size of 160 bits for an ECC is equivalent to an RSA key size of 1024 bits. The main disadvantage of cryptosystems based on number theory is that they are not resistant to quantum computer attacks. P. Shor [21] showed that quantum computers are able to break cryptosystems based on number theory, such as RSA, El Gamal, and ECC.

NTRU cryptosystem [22] is based on the hard problem, the shortest vector in a lattice. It is post-quantum cryptosystem and has relatively small private- and public-key sizes (kilobits). While using this cryptosystem in NFC protocol, we need to implement the encryption algorithm in NFC tags and affects the effectiveness of the protocol. In addition, Albrecht et al. [23] showed vulnerability in the NTRU encryption algorithm by using a larger modulus.

McEliece's cryptosystem [24] is the first cryptosystem adopting the coding theory; it is based on Goppa codes. It is resistant to quantum computer attacks and is high-speed encryption/decryption compared to other PKCs. There exist many variants of McEliece's cryptosystem [25]. Nojima et al. [26] presented the randomized variant of the McEliece cryptosystem which is resistant to semantic security against chosen plaintext attack (IND-CPA). The description of this variant is as follows:

- **Key generation:** Let (n, k, t)-code be a linear code with the parameters: n is the length and k is the demission of the generator matrix G'. This codecan correct up to t errors. Generate a generator matrix $G'^{k\times n}$. Choose randomly two matrices, an invertible matrix $S'^{k\times k}$ and a permutation matrix $P^{n\times n}$. (G', S', P) are private matrices. The public matrix is $G^{k\times n}=S'G'P$.
- **Encryption:** The sender randomly calculates the codeword$c=[r \| m]G$, where $r \in \mathbb{F}_2^{k_1}$ is a random string and $m \in \mathbb{F}_2^{k_2}$ (where $k=k_1+k_2$) is the plaintext vector. Then, it generates an error vector $e \in \mathbb{F}_2^n$ of weight $wt(e)\leq t$ and computes the ciphertext$c' = c\oplus e$.
- **Decryption:** The receiver calculates $z=c'P^{-1}$ where $P^{n\times n}$ is a permutation matrix, calculates the decoding algorithm $y=A(z)$ and then outputs $[r \| m] = yS'^{-1}$ where $S'^{k\times k}$ is an invertible matrix. The plaintext vector m is the last k_2 bits of the decrypted message.

The very important drawback of McEliece's cryptosystem is to need a large public-key matrix size. For example, the public key matrix size is about 2.5 Megabits for 2^{80} security level. Chikouche et al. [23] presented a survey on RFID authentication protocols based on coding theory that adopt different versions of the McEliece cryptosystem. To avoid the mentioned problem, they proposed to store only the codeword where its size is suitable for low-cost tags. To calculate the ciphertext, the tag requires only xor operation between the stored codeword and the generated error vector.

4. REVIEW OF YANG ET AL.'S PROTOCOL

In 2016, Yang et al. [15] invented a hash-based RFID mutual authentication protocol to secure remote education systems. This protocol includes three entities: the server, RFID reader, and RFID tag. The communication reader-tag is unsecured, it use radiofrequency channel. However, Yang et al. supposed that the channel server- reader is protected. Table I presents the notations used throughout the manuscript.

TABLE I. NOTATIONS

Symbol	Meaning
T, R, S	The tag, the reader, and the server, respectively
$\mathcal{A}$	the adversary
N_S	Nonce generated by S
N_T	Nonce generated by T
N_R	Nonce generated by R
ID_T	the tag's identifier
ID_R	the reader's identifier
s_{new}, r_{new}	current session secrets of tag and reader stored in the server
s_{old}, r_{old}	precedent session secrets of reader and tag stored in the server
$g(.)$	PRNG to find a nonce with input
$H(.)$	hash function
e_T, e_R	Error vectors with weight t

In registration phase, the server database stores (ID_T, ID_R), the reader stores ID_R, and the tag stores ID_T. The mutual authentication protocol is as hereafter (see Figure 1):

- The reader R sends a request with a nonce N_R generated by a random number generator to the tag T,
- After receiving request, tag computes $h = H(ID_T \| N_R)$ and sends it to reader as response,
- The reader resends the received $N_R$and h messages to the server,

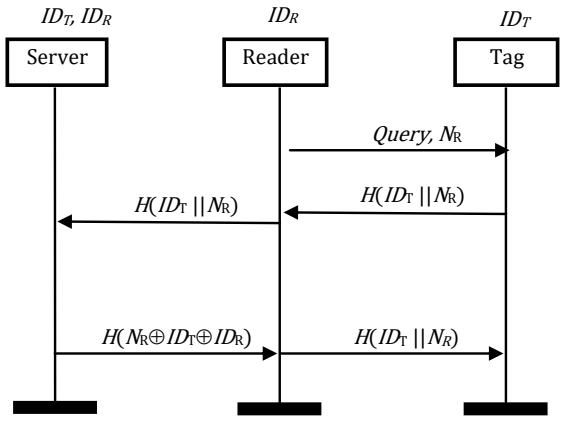

Figure 1. Yang et al.'sauthenticationprotocol

- The server computes $H(ID_T||N_R)$, if outcome equals to received *h*, the tag is legal; Otherwise, tag's authentication fails.
- The server uses (ID_T, ID_R) to compute $H(N_R \oplus ID_T \oplus ID_R)$ and sends it to *R*.
- The reader uses its $ID_R$and $N_R$to compute ID_T, and then calculates $h_1=H(ID_T||N_R)$. the reader sends it to tag.
- The tag verifies the equality between h_1 and *h*. If equal, the reader is legal; otherwise, server's authentication fails.

5. ANALYSIS OF YANG ET AL.'S AUTHENTICATION PROTOCOL

In this section, we will demonstrate that Yang et al.'s protocol does not achieve three important security and privacy requirements: reader authentication, location privacy, and forward secrecy.

A. Attack on reader authentication

In the attack on reader authentication, the adversary plays a reader's role where it communicates with the legitimate tag as a legal reader. The problem posed in this protocol is to use the same message $H(ID_T||N_R)$ to verify tag authentication as well as reader authentication. Figure 2 shows the general structure of this attack on reader authentication.

B. Traceability attack

In session (*i*), the adversary blocks the first message (*Query* and N_R) and replaces N_R by a constant number c, then sends Query with c to tag. The tag computes $h=H(ID_T||c)$ and sends it to the reader. The rest of the protocol concludes normally. In each attack execution, the adversary replaces the value of nonce N_R by *c*, then the hash function keeps the same value of $H(ID_T||c)$.

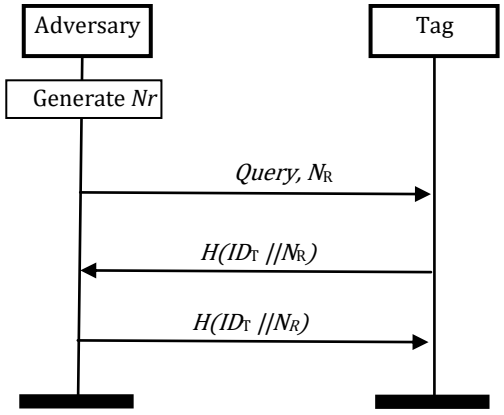

Figure 2.Attack on reader authentication

The adversary is competent to follow the tag's trace by verifying the equality between *h* values. Figure 3 describes how the adversary can track the tag's holder in the studied protocol.

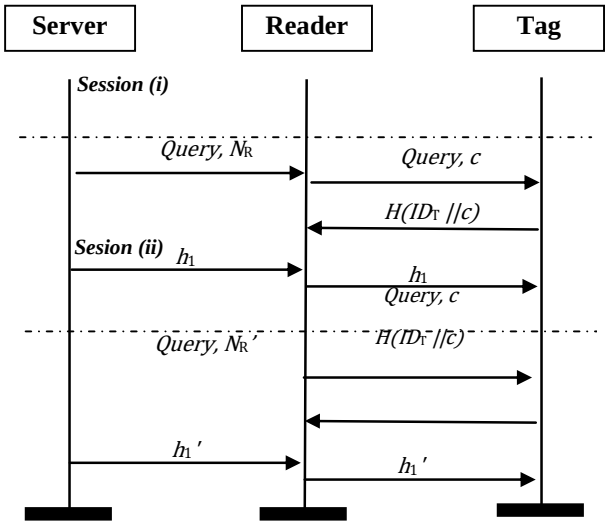

Figure 3.Traceability attack

C. Violating forward secrecy

In the studied protocol, the memory of RFID contains the tag's identifier ID_T only, and which remains constant in all sessions. An adversary breaking into the tag's memory gets the current ID_T. The posed vulnerability is the value of tag's identifier which is static and not alterable. Thus, the studied protocol does not guarantee forward secrecy.

6. EAP-SRES PROTOCOL

This section presents the different components of the remote education system. It also describes an enhanced authentication protocol which is designed to secure remote education systems (EAP-SRES).

A. Model System

In EAP-SRES, the Remote Education System (RES) uses an NFC system to authenticate different components and secure communication between components of the RES. The operating mode used in NFC is of type card emulator. NFC system comprises three main components, the NFC tag (e.g., integrated into mobile), the NFC reader and the server.

- NFC tag is a terminal node in RES system. The most important component of NFC mobile is the NFC tag which consists of a chip and an antenna. The antenna is physically attached to the microchip and it is used to communicate with the reader. NFC mobile is used by teachers and students in proving their identity.
- NFC reader is a device that communicates with the NFC tag via radio waves. It has one or more receptors which can send radio waves and intercept emissions from NFC mobile phones.
- The server provides an information database about items identified by NFC tags. It stores public- and private keys and implements encryption/decryption algorithms of McEliece with random padding. The public-key G is utilized in registering all NFC tags.

The communication between different components of the NFC system (NFC tag, NFC reader, and server) is unsecured. The server and the NFC reader can communicate between them by using the Internet. However, the NFC tag and NFC reader communicate between them through radio frequency channel. Figure 4 depicts our system model.

Figure 4. System Model

B. Description of EAP-SRES Protocol

Our EAP-SRES protocol consists of two procedures: the registration and the authentication.

C. Registration Phase

According to the McEliece's cryptosystem with random padding, the tag's identifier ID_T and reader's identifier ID_R is considered as a plaintext m; and the nonces s and r is considered as a random number where the values of s and r have been updated in each session.

The entities of the NFC system implement a generator of pseudo-random numbers. The NFC tag stores the tag's identifier $ID_T$and the dynamic codeword C_{dyn}^T where $C_{dyn}^T=[r \| ID_T]G$. The NFC reader implements PRNG, it stores the reader's identifier ID_R and the dynamic codeword C_{dyn}^R where $C_{dyn}^R=[s \| ID_R]G$. The server contains a database includes $\{ID_R, s_{old}, s_{new}\}$ and $\{ID_T, ID_R, r_{old}, r_{new}\}$.

To register a new NFC reader R, R sends its reader's identifier ID_R to the server (trusted center) through a secure channel. S generates a nonce s and calculates the dynamic codewordC_{dyn}^R where $C_{dyn}^R=[s \| ID_R]G$. The server stores $\{ID_R, s_{old}, s_{new}\}$ in its database, we initialize the values of s_{old} and s_{new} by s. S sends C_{dyn}^R to R to store it in its memory.

When the NFC tag T wants to obtain service from the server. The T sends its tag's identifier ID_T to the server via the NFC reader that defined by its ID_R through a secure channel. Subsequently, S generates a nonce r and calculates the dynamic codewordC_{dyn}^T where $C_{dyn}^T=[r \| ID_T]G$. The server stores $\{ID_R, ID_T, r_{old}, r_{new}\}$ in its database, we initialize the values of r_{old} and r_{new} by r. S sends C_{dyn}^T to T to store it in its memory. The NFC tag can communicate with a set of authorized NFC readers.

D. Authentication Phase

The different steps of authentication phase are depicted in Figure 5 and are described hereafter:

Setup1. The server sends a query with N_S to the NFC tag via the NFC reader.

Setup2. The NFC tag generates a random number N_T and error vector e_T. It computes $C_T=C_{dyn}^T \oplus e_T$ and $V_T=g(N_R \| N_T \| ID_T)$,

Setup3. The tag T sends N_T, C_T and V_T to the reader R,

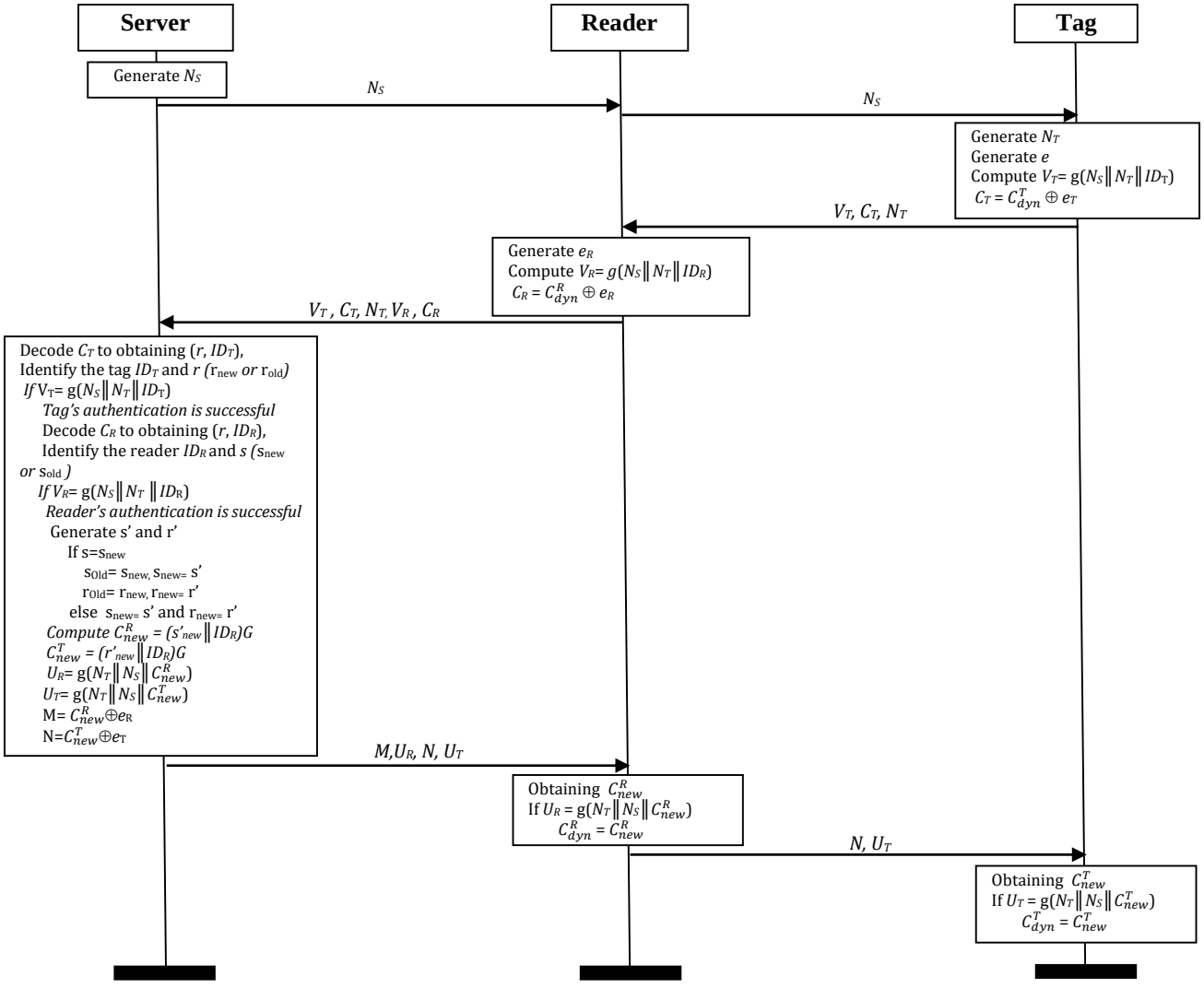

Figure 5. EAP-SRES Protocol

Setup4. The reader generates an error vector e_R. It computes C_R=$C^R_{dyn} \oplus e_R$ and V_R=$g(N_R \| N_T \| ID_R)$. R resends the received N_T, C_T and V_T with C_R and V_R to the server.

Setup5. After receiving $\{N_T, C_T, V_T, C_R, V_R\}$ from the NFC reader, the server decodes C_T to find the values of r and ID_T. The server retrieves database records of ID_T to find if there is a record corresponding to the decrypted ID_T. If it retrieves ID_T, it computes $g(N_S \| N_T \| ID_T)$ and checks it with V_T, if they are equal, the tag's authentication is successful, then the server decodes C_R to find the values of s and ID_R. It retrieves database records of ID_R to find if there is a record corresponding to the decrypted ID_R. If it retrieves ID_R, it computes $g(N_S \| N_T \| ID_R)$ and checks it with V_R,if they are equal, the reader's authentication is successful.After that, the server generates two nonces r' and s'. Depending on the values of s (if s=s_{new} or s= s_{old}) and r (if r=r_{new} or r= r_{old}), the server updates s_{new}, s_{old}, r_{new}, r_{old}. After that the server calculates C^R_{new} = $(s_{new} \| ID_R)G$, C^T_{new} = $(r_{new} \| ID_R)G$, U_R= g($N_T \| N_S \| C^R_{new}$), U_T= g($N_T \| N_S \| C^T_{new}$), M_1= $C^R_{new} \oplus e_R$ and M_2=$C^T_{new} \oplus e_T$. Finally, the server sends $\{M_1, U_R, M_2, U_T\}$ to the reader.

Setup6. After receiving M and U_R from the server, the reader obtains the value of C_{new}^R by calculating $M_1 \oplus e_R$. R calculates $U_R'=g(N_T \| N_S \| C_{new}^R)$ and verifies if $U_R = U_R'$, if they are equal, the reader authenticates the server, after that, it updates $C_{dyn}^R = C_{new}^R$. Then the reader resends $\{M_2, U_T\}$ to T.

Setup7. The NFC tag obtains the value of C_{new}^T by computing $M_2 \oplus e_T$.The reader computes $U_T'=g(N_T \| N_S \| C_{new}^T)$ and checks if $U_T' = U_T$, if they are equal, the NFC tag authenticates the server, the NFC tag then updates $C_{dyn}^T = C_{new}^T$.

7. SECURITY AND PERFORMANCE ANALYSIS OF EAP-SRES PROTOCOL

Table II presents a comparison between recent NFC/RFID protocols and our EAP-SRES protocol in terms of security and performance.

TABLE II. SECURITY COMPARISON BETWEEN EAP-SRES AND EXISTING PROTOCOLS

	[9]	[12]	[13]	[14]	[15]	Ours
M.A	Y	N	N	Y	N	Y
Unt	N	Y	N	Y	N	Y
D.R	Y	Y	Y	Y	Y	Y
F.S	Y	Y	Y	Y	N	Y

M.A: MutualAuthentication
Unt: Untraceability
D.R: Desynchronization resilience
F.S: Forward secrecy

A. Automated analysis

CL-Atse [19] is an automated tool to verify the security of cryptographic services and protocols. It is based on constraint solving and rewriting techniques. It can verify security protocols specified in HLPSL language and requiring cryptographic primitives (public-key encryption algorithm, private-key encryption algorithm, hash function, etc.), PRNG, and algebraic operators like exponentiation and exclusive-or (XOR).

CL-Atse tool can detect attacks of type man-in-the-middle and replaying attacks, if exist, with capabilities of Dolev-Yao adversary.

When a security property of the input specification protocol is not achieved then CL-Atse demonstrates the message *UNSAFE* and the corresponding attack scenario. In another case, when the protocol achieves security properties, CL-Atse demonstrates the message *SAFE*.

Figure 6 shows that the EAP-SRES protocol has been found to be *SAFE* and that no attacks have been detected. Thus this protocol is resistant to the man-in-the-middle attacks and the replaying attacks. It also satisfies mutual authentication and the secrecy of secret data. Therefore, we can deduce that the EAP-SRES protocol is secure.

```
   SUMMARY
   SAFE

   DETAILS
   BOUNDED_NUMBER_OF_SESSIONS
   UNTYPED_MODEL
   PROTOCOL
   /home/span/span/testsuite/results/E
AP_SRES.if

   GOAL
   As Specified

   BACKEND
   CL-AtSe
   STATISTICS
   Analysed   : 887 states
   Reachable  : 187 states
   Translation: 0.18 seconds
    Computation: 0.09 seconds
```

Figure 6. Verification resul

B. Privacy analysis

In the literature, there are several formal models [28] to validate the untraceability property. The model of Ouafi& Phan [29] is one of the well-known models based on the theory of the game. In this model, the protocol entities are reader $R \in Readers$ and tags $T \in Tags$ interacting in the protocol as per the protocol specifications until the end of the session. There are four queries allowed to run by the intruder $\mathcal{A}$: *Execute, Send, Corrupt* and *Test* [29].

Untraceable privacy (UPriv) is presented using the game played between an attacker $\mathcal{A}$ and the instances of the reader and the tag. There are three phases for this game:

- ***Learning phase***: $\mathcal{A}$ is able to send any *Corrupt, Send*,and *Execute* queries at will.
- ***Challenge phase***: $\mathcal{A}$ selects two fresh tags T_0, T_1 to be tested and sends a *Test* query corresponding to the test session. According to a randomly selected bit $b \in \{0, 1\}$, $\mathcal{A}$ is given a tag T_b from the set $\{T_0, T_1\}$. $\mathcal{A}$ continues making any *Send*, and *Execute* queries at will.
- ***Guess phase***: In the end, $\mathcal{A}$ ends the game and outputs a bit $b' \in \{0, 1\}$, which is its guess of the value of b.

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

$$Adv_{\mathcal{A}}^{UPriv}(k) = |\text{pr}(\text{b} = \text{b}') - (\text{random flip coin})| = \left|\text{pr}(\text{b} = \text{b}') - \frac{1}{2}\right|)$$

Where $0 \leq Adv_{\mathcal{A}}^{UPriv}(k) \leq \frac{1}{2}$

About the EAP-SRES protocol, when we run the *Execute* query at a session (i), the attacker $\mathcal{A}$ spies on a perfect session between T_0 and the reader. The adversary $\mathcal{A}$ obtains the values (V_T^{T0},C_T^{T0},N_T^{T0}). It cannot replay a provisionally used C_T=$C_{dyn}^T \oplus e_T$ and V_T=$g(N_R \| N_T \| ID_T)$ to an NFC reader since with high probability, it will not match the N_R value chosen by the reader for that session. In each session, the encoding codeword C_T is different from its value in the previous session because C_{dyn}^T is updated before ending the session.

C. Informally security analysis

1) Secrecy

The secret data in EAP-SRES are ID_T and ID_S. These data are not transmitted clearly in the protocol; they are encrypted by McEliece's cryptosystem with random padding. C_T and C_R are ciphertexts of encrypted ID_T and ID_S, respectively. This encryption algorithm is based on the NP-complete problem and it resists chosen plaintext attacks (IND-CPA), proved by Nojima et al. [24].

2) Data integrity

To guarantee the authentication and the data integrity, we use the messages V_T, V_R, U_R, and U_T. In case the adversary changes the values of N_S and N_T, so the values of last messages are incorrect and the protocol will end. It is difficult for the adversary to change the values such that the values of V_T, V_R, U_R, and U_T are correctly calculated. Then, EAP-SRES protocol achieves data integrity.

3) Forward secrecy

In EAP-SRES, the NFC tag stores data {ID_T, C_{dyn}^T} in its memory. The last process of the protocol is to update the value of C_{dyn}^T in the NFC tag, the new one is C_{new}^T, which is computed by the server. The adversary cannot acquire the last codeword C_{dyn}^T used in the prior sessions. Thus EAP-SRES protocol provides forward secrecy.

4) Desynchronization resilience

To satisfy this requirement, we adopted synchronized numbers, r_{old}, r_{new}, s_{old} and s_{new} in the database of the server. When the intruder blocks the last message transformed from the reader to the NFC tag, so the value of r_{new} that stored in the server and the value of r that stored in the NFC tag are different. In the next session, after receiving V_T, C_T, N_T and decrypting C_T by the server, it finds $r \neq r_{new}$. The proposed solution is to use the old value of r that is r_{old}, this value achieves the equality $r=r_{old}$, then the EAP-SRES guarantees desynchronization resilience requirement. The protocol uses the same technique to avoid the desynchronization attack with values of (s_{new}, s_{old}).

D. Performance Analysis

To evaluate the performance of EAP-SRES authentication protocol, there are three important constraints: storage space, computation cost, and communication cost. Table III presents the performance comparison between EAP-SRES protocol and other studied protocols.

TABLE III. PERFORMANCE COMPARISON BETWEEN EAP-SRES AND EXISTING PROTOCOLS

	[9]	[12]	[13]	[14]	[15]	Ours
S.R	2L	2L	2L	3L	1L	k_2+n
C.C	5L	8L	5L	5L	3L	3L+2n
R.P	H+G	H+G+ Enc	H+G	H+G+ Enc	H+G	G
N.E	N	N	Y	N	N	Y

S.R: Storage requirement in tags
C.C: Communication cost
R.P: Required primitives in tags
N.E: No exhaustive search
L: length of GRN, identifier, ECC point, or hash
H: Hash function
G: PRNG with input
Enc: Encryption function

Concerning the required storage space in the NFC tag, we require only n+k_2 bits where the length of C_{dyn}^T is n, the length of s is k_1, and the length of ID_T is k_2 with k=k_1+k_2. If we choose a Goppa code C[n=2048,k=1751,d=56] which gives a security of level 2^{80}. We also select k_1= 895 and k_2= 856 where (k_2<k_1). Hence the required space is 2904 bits (363 bytes), this value is very compatible with the capabilities of NFC tags. For example, NFC tags of type MIFARE Classic 4K [30] offer 3,440 bytes of net data capacity.

Concerning the computation cost, the NFC tag needs simple operations: xor operation and pseudo-random number generators. In contrast to Yang et al.'s protocol, there is no need to make an exhaustive search to determine the corresponding NFC tag; thus the complexity of time issue performed by the server in tag identification is $O(1)$. Note that we excluded the use of the hash function in the EAP-SRES protocol because it is not supported by low-cost NFC tags.

In EAP-SRES protocol, the messages exchanged between the NFC reader and the NFC tag are to realize the mutual authentication. The length of these messages exchanged is 5l where l is the length of the message.

8. CONCLUSION

Recently, Yang et al. presented an RFID authentication protocol based on the hash function to secure remote education systems. This paper analyzed the security of this protocol. Results of this analysis proved that Yang et al.'s authentication protocol does not ensure the reader's authentication, untraceability, and forward secrecy. This work also proposed an enhanced authentication protocol to secure remote education systems (EAP-SRES) using NFC technology. The proposed EAP-SRES does not require the hash function because the low-cost NFC tags do not support this function, and we adopted a lightweight post-quantum cryptosystem, named, McEliece's cryptosystem with random padding.

The automated security analysis showed that the EAP-SRES protocol resists replay and man-in-the-middle attacks. In addition, it satisfies mutual authentication,

untraceability, forward secrecy, and desynchronization resilience properties. The performance analysis proved that the EAP-SRES is suitable for the memory resources and the constrained computational capacity of the NFC tags. Moreover, it does not require an exhaustive search to determine the corresponding NFC tag.

REFERENCES

[1] K. Kaur, "A Survey on internet of things – architecture, applications, and future trends," 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), 2018, pp. 581-583.

[2] W.M. Abdulkawi and A.F.A. Sheta, "Multi-resonator structure for small size chipless radio frequency identification tag," International Journal of Computing and Digital Systems, vol. 7, no. 01, pp.43-49, 2018.

[3] V. Coskun, B. Ozdenizci and K. Ok."A survey on near field communication (NFC) technology," Wireless personal communications, vol. 71, no. 3, pp. 2259-2294, 2013.

[4] J. Gómez, J.F. Huete, O. Hoyos, L. Perez and D. Grigori, "Interaction system based on internet of things as support for education,". *Procedia Computer Science*, vol. 21, pp. 132-139, 2013.

[5] S.L. Marie-Sainte, S. Alrazgan Muna, F. Bousbahi, S. Ghouzali and W. Abdul, "From mobile to wearable system: A wearable RFID system to enhance teaching and learning conditions," Mobile Information Systems, vol. 2016, no. 10, 2016.

[6] I. Vaccari, E. Cambiaso and M. Aiello, "Evaluating security of low-power internet of things networks," International Journal of Computing and Digital Systems", vol. 8, no. 02, pp. 101-114, 2019.

[7] A. Bashir and A.H. Mir, "Internet of things security issues, threats, attacks and counter measures," International Journal of Computing and Digital Systems, vol. 7, no. 02, pp. 111-120, 2018.

[8] X. Zhang, Z. Zhang and X. Wei."An improved lightweight RFID authentication protocol," In Technological Solutions for Modern Logistics and Supply Chain Management, 2013, pp. 1-9.

[9] M.H. Dehkordi and Y. Farzaneh, "Improvement of the hash-based RFID mutual authentication protocol". Wireless personal communications, vol. 75, no. 1, pp. 219-232, 2014.

[10] P. Książak, W. Farrelly and K. Curran, "A lightweight authentication protocol for secure communications between resource-limited devices and wireless sensor networks, " International Journal of Information Security and Privacy, vol. 8, no. 4, pp. 62-102, 2014.

[11] J. Baek, H.Y. Youm and H. Y, "Secure and lightweight authentication protocol for NFC tag based services". In 10th Asia Joint Conference on Information Security (AsiaJCIS), 2015,pp. 63-68, IEEE, 2015.

[12] D. He, N. Kumar and J.H. Lee, "Secure pseudonym-based near field communication protocol for the consumer internet of things". IEEE Transactions on Consumer Electronics, vol. 61, no. 1, pp. 56-62, 2015.

[13] P. Dass and H. Om."A secure authentication scheme for RFID systems". Procedia Computer Science, vol. 78, pp. 100-106, 2016.

[14] V. Odelu, A.K. Das and A. Goswami, "SEAP: secure and efficient authentication protocol for NFC applications using pseudonyms," IEEE Transactions on Consumer Electronics, vol. 62, no. 1, pp. 30-38, 2016.

[15] L. Yang, Q. Wu, Y.Bai, H. Zheng and S. Lin, "An improved hash-based RFID two-way security authentication protocol and application in remote education," Journal of Intelligent & Fuzzy Systems, vol. 31, no. 5, pp. 2713-2720, 2016.

[16] A. Kumar and H. Om, "Lightweight, ECC based RFID authentication scheme for wLAN," International Journal of Business Data Communications and Networking (IJBDCN), vol. 12, no. 2, pp. 89-103, 2016.

[17] M. H. Alharbi and O. H. Alhazmi, "Prototype: User authentication scheme for IoT using NFC," 2019 International Conference on Computer and Information Sciences (ICCIS), IEEE, 2019, pp. 1-5.

[18] X.-Y. Bai and Y.-J.Huang. "Security mechanism for the interactive satellite remote education system which based on DTN," 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2013, pp. 46-52.

[19] M. Turuani, "The CL-Atse protocol analyser".In International Conference on Rewriting Techniques and Applications, LNCS 4098, Springer, 2006, pp. 277-286.

[20] N. Koblitz, "Elliptic curve cryptosystems". Mathematics of computation, vol. 48, no. 177, pp. 203-209, 1987.

[21] W. Peter Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM review, vol. 41, no. 2, pp. 303-332, 1999.

[22] J. Hoffstein, J. Pipher and J. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic number theory, pp. 267-288, 1998.

[23] M.R. Albrecht, S. Bai and L. Ducas, "A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encodingschemes, " Advances in Cryptology– CRYPTO 2016, LNCS 9814, Springer, 2016, pp. 153–178.

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

[25] P. Véron, "Code based cryptography and steganography," In International Conference on Algebraic Informatics, LNCS 8080, Springer, 2013, pp. 9-46,.

[26] 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, pp. 289-305, 2008.

[27] N. Chikouche, F. Cherif, P-.L. Cayrel and M. Benmohammed, "RFID authentication protocols based on error-correcting codes: A survey," Wireless Personal Communications, vol. 96, no. 1, pp. 509-527, 2017.

[28] J. Hermans, R. Peeters and B. Preneel, "Proper RFID privacy: Model and Protocols," in IEEE Transactions on Mobile Computing, vol. 13, no. 12, pp. 2888-2902, 1 Dec. 2014.

[29] K. Ouafi and R. C. W. Phan, "Privacy of recent RFID authentication protocols," In International Conference on Information Security Practice and Experience, LNC 4991, Springer, 2008, pp. 263-277.

[30] The Mifar cards (2019). [online] available at: http://www.mifare.net.

Dr. Noureddine Chikouche received his Ph.D. degree in computer science from University of Biskra, Algeria, in 2016. He is currently an associate professor in University of M'sila, Algeria. His current research interests include IoT security, RFID security, wireless sensor network security, post quantum cryptography, formal verification of security protocols, image encryption and steganography.

Prof. Foudil Cherif is a full professor in University of Biskra, Algeria. He received his Ph.D. degree in computer science from University of Biskra, Algeria, in 2006. He supervised several Ph.D. and Magister these which have been successfully defended these last years. His current research interest is in Crowd simulation, artificial life, Artificial intelligence, RFID security, software engineering, and formal verification of security protocols.