Journal of Computing and Security

January 2019, Volume 6, Number 1 (pp. 13–23)

http://www.jcomsec.org

Full Secret Disclosure Attack against an EPC- C1 G2 Compliant Authentication Protocol

Masoumeh Safkhani [a,*]

[a] *Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran.*

ARTICLE INFO.

Article history:
Received: 16 March 2018
Revised: 8 August 2018
Accepted: 23 September 2019
Published Online: 25 November 2019

Keywords:
RFID, EPC-C1 G2, Authentication Protocol, Secret Disclosure Attack, GNY Logic.

ABSTRACT

Security analysis of a protocol is an important step toward the public trust on its security. Recently, in 2018, Moradi *et al.* considered the security of the Wei and Zhang RFID EPC-C1 G2 compliant authentication protocol and presented desynchronization attack and also server/reader impersonation attack against it. Then they proposed an improved version of the protocol. However, in this paper as the first third party analysis of this protocol to the best of our knowledge, we present an efficient secret disclosure attack with the complexity of only two runs of protocol and doing $O(2^{16})$ PRNG offline evaluations. We also recommend that designing a secure protocol by using 16-bit CRCs and 16-bit PRNGs in the framework of EPC-C1 G2 may not be possible and changing this standard to allow the use of lightweight cryptographic functions should be inevitable. In this line, we present an improved version of the Moradi *et al.* protocol and also prove its security both informally and formally, through GNY logic.

1 Introduction

Today, the science of designing security protocols has grown well. Perhaps a reason for this progress is the security analyses done on the previous security protocols such as [1–13] which help the designers to learn the errors in the existing protocols and not to repeat them in their design.

Given that RFID tags are very constrained and the passive tags have no internal power resource and should harvest the required energy from the reader, it is not possible to use conventional cryptographic primitives to provide the desired security for their communications. On the other hand, the transferred information should be critical, *e.g.* a patient information or the identity of the tag holder. Hence, the security of the communication of those devices are also important. To address these concrens, many researchers have tried to provide the expected security using lightweight/ultralightweight operations/functions. For example, Tian *et al.*[14] proposed a protocol called RAPP which uses a very lightweight permutation as the security core. However, later analysis showed that it suffers from several flaws [15, 16]. Later, to improve the security of RAPP, Zhuang *et al.* proposed another ultralightweight RFID mutual authentication protocol [17] called R^{2}AP. However, later analysis have shown that it is as insecure as RAPP [18, 19]. Similarly, Haung *et al.* [20] proposed a permutation based lightweight RFID grouping proof protocol for passive tags based on ISO-14443 standard, however later Rostampour *et al.* [21] proposed an efficient secret disclosure attack against this protocol. More recently, Fan *et al.* proposed a new lightweight RFID protocol,

[*] Corresponding author.

Email address: `Safkhani@sru.ac.ir` (M. Safkhani)

https://dx.doi.org/10.22108/jcs.2019.110886

ISSN: 2322-4460 © 2019 JComSec. All rights reserved.

to protect the medical privacy in an IoT system [22]. However, Aghili *et al.* later have shown that it has trivial security flaws [23]. Aghili *et al.* also proposed an improved version of the protocol, based on the similar designing paradigm, called SecLAP. However, recently Safkhani *et al.* in [24] have shown that SecLAP suffers from secret disclosure attacks. On the other hand, given that EPC- C1 G2 standard compliant tags support 16-bit PRNG, several protocols have been proposed based on this component. For example, Jeon and Yoon proposed RAPLT [25] and Pang *et al.* proposed SRP^+ [26] based on this paradigm. However, Wang *et al.* analyzed those two protocols and presented successful attacks with the complexity of $O(2^{16})$ [27] against them. Moreover, Wang *et al.* also proposed a new protocol called SRP^{++}, conforming to the EPC- C1 G2 standard and claimed that their protocol can resist against the disclosure attacks up to the complexity of $O(2^{32})$. However, later it has been shown that it may not be possible to achieve security beyond 2^l using an l-bit PRNG [28].

In the same vein, Moradi *et al.* in [29] cryptanalyzed the Wei and Zhang RFID authentication protocol[30] and presented desynchronization attack and also server and reader impersonation attack against it. Then they proposed an improved version of it and informally and formally, through BAN logic, proved its security against different attacks, including secret disclosure attack. However, in this paper, we present an efficient secret disclosure attack with the complexity of two runs of the protocol and doing $O(2^{16})$ PRNG evaluations.

1.1 Our Contribution

The contribution of this paper has two folds, as follows:

(1) We analyse the security of the improved protocol proposed by Moradi *et al.* in [29] and show that it has some security flaws. More precisely, thanks to the short length PRNG which is used in the structure of this protocol, we demonstrate an attack that retrieves whole secret parameters with the complexity of $O(2^{16})$. Although the used technique is almost similar to the technique used in related papers such as [27–29], however, it is the first third party analysis of Moradi *et al.*'s protocol and we used a non-trivial combination of messages to retrieve the secrets with the complexity of $O(2^{16})$.

(2) Considering the recent advances in the designing of lightweight crypto-primitives for constrained environments, *e.g.*, many lightweight block cipher which have been proposed over the last decade, we improve the Moradi *et al.*'s protocol, mainly by replacing the used PRNG by a block cipher such as SKINNY [31]. In addition, we formally/informally evaluate the security of the proposed protocol and show that it provides desired security against attacks.

1.2 Paper Organization

The rest of the paper is organized as follows: in Section 2, we briefly review the Moradi *et al.* RFID protocol. We present our secret disclosure attack against the Moradi *et al.* protocol in Section 3. We improve the protocol in Section 4 and in Section 5, we prove the security of our proposed protocol both informally and formally through GNY logic. We also compare the proposed protocol with its predecessors in Section 6 from security and computational complexity aspects. Finally, the paper is concluded in Section 7.

2 Description of Moradi *et al.*'s Protocol

The Moradi *et al.*'s protocol, as depicted in Figure 1 using notations represented in Table 1, runs in two phases as below:

Registration Phase :
In this phase of the protocol, any protocol's party saves its related records. More precisely, the tag stores $metaID_i$, K_i^1 and K_i^2. The server stores $(metaID_i)_{old}, (metaID_i)_{new}, (K_i^2)_{old}$ and $(K_i^2)_{new}$. The reader stores K_i^1 which is the same for all the tags.
Authentication Phase :
This phase of the protocol runs as below:

(1) The reader starts this phase of protocol by generating a random number N_r and sending it along with *query* to the tag.

(2) Once the tag receives the message, it does as follows:
- generates another random number N_t;
- computes $M_1 = [PRNG(K_i^2 \oplus N_r) \| PRNG\ (K_i^2 \oplus N_t)] \oplus metaID_i$;
- computes $N = CRC([K_i^1]_R \| N_r) \oplus N_t$;
- and sends M_1 and $N \| (N_t \oplus [K_i^1]_L)$ to the reader.

(3) Upon receipt of the message, the reader:
- retrieves N_t' from $(N_t \oplus [K_i^1]_L)$;
- computes $N' = CRC([K_i^1]_R \| N_r) \oplus N_t'$ and checks whether it equals with the received value of N or not. If it is not, terminates the protocol.
- If it is ok, it sends M_1 along with N_t and N_r to the server;

(4) Once the server receives the message, it does as follows:

Table 1. Notations Used in This Paper.

Category	**Description**
T_i	The i^{th} RFID tag
R	An RFID reader
A	The adversary
$metaID_i$	The pseudonym of the i^{th} RFID tag which is shared between the tag and the server. This is 32-bit in protocol of Moradi *et al.* and 64-bit in our proposed protocol
K_i^2	The secret value of the i^{th} RFID tag which is shared with the server. It is 16-bit in protocol of Moradi *et al.* and in our proposed protocol is 64-bit
K_i^1	The secret value of the i^{th} RFID tag which is shared with the reader and same for all the tags. It is 32-bit in protocol of Moradi *et al.* and in our proposed protocol is 64-bit
K_{SR}	Secret key which is shared between the reader and the server (used only for formal security proof)
N_r, N_t	Random numbers which are generated by the reader and the tag respectively. In the Moradi *et al.* protocol they are 16-bit and in our proposed protocol are 32-bit
$E_K(.)/D_K(.)$	A block cipher with 64-bit inputs, 64-bit outputs and 64-bit keys
PRNG	16-bit output pseudo random number generator
CRC	16-bit output cyclic redundancy code
$[M]_R$, $[M]_L$	The right and the left half of M respectively
$\Vert$	Concatenation operation
$\oplus$	Bit wise exclusive-or operation
$Flag$	Shows the matching record is old or new
$F1: \dfrac{P\vert\equiv\sharp(X)}{P\vert\equiv\sharp(X,Y), P\vert\equiv\sharp(F(X))}$	Means that if P believes the message X is fresh, then it entitled that he believes any combination of X is also fresh
$F2: \dfrac{P\vert\equiv\sharp(X), P\ni K}{P\vert\equiv\sharp(\{X\}_K), P\vert\equiv\sharp(\{X\}_{K^{-1}})}$	Means that if P believes the message X is fresh and P possess K then it entitled that he believes any combination of encryption of X and also decryption of X is also fresh
$R1: \dfrac{P\vert\equiv\phi(X)}{P\vert\equiv\phi(X,Y), P\vert\equiv\phi(F(X))}$	Means that if P believes the message X is recognizable, then it entitled that he believes any combination of X is also recognizable
$I1: \dfrac{A}{B}$, where $A: P\lhd *\{X\}_K, P\ni K, P\vert\equiv P\xleftrightarrow{K}Q, P\vert\equiv\phi(X), P\vert\equiv\sharp(X,K)$ and $B: P\vert\equiv Q\vert\sim X, P\vert\equiv Q\vert\sim\{X\}_K, P\vert\equiv Q\ni X$	Means that if P receives a fresh message X which is encrypted with K, and he possesses K and he believes K is a shared secret between itself and Q, also believes the message X is recognizable and also believes X or K is fresh, then he is entitled that he believes Q conveyed X, and also believes Q conveyed the encrypted message of X with K and also believes Q possess X

   - for each of the database records, *i.e.* $(metaID_i)_{old}$, $(metaID_i)_{new}$, $(K_i^2)_{old}$, $(K_i^2)_{new}$, it calculates M_1' and checks if it is equal to the received value of M_1.This step is repeated so that a record can be found, which indicates the successful authentication of the tag;
   - at the same time, if $Flag = 0$, the matching record is $(metaID_i)_{old}$, $(K_i^2)_{old}$, so, it computes $M_2 = [CRC(K_i^2\|N_t) \|CRC(K_i^2\|N_r)] \oplus metaID_i$ and does not change $(metaID_i)_{old}$ and $(K_i^2)_{old}$ and updates $(metaID_i)_{new}$ as $[PRNG((metaID_i)_{new}) \|CRC((metaID_i)_{new})] \oplus N_t \oplus N_r$ and $(K_i^2)_{new}$ as $PRNG((K_i^2)_{new}) \oplus N_t$;
   - if $Flag = 1$, the matching record is $(metaID_i)_{new}, (K_i^2)_{new}$ so, it computes $M_2 = [CRC((K_i^2)_{new}\|N_t)\|CRC((K_i^2)_{new}\| N_r)]\oplus metaID_i$ and updates $(metaID_i)_{old}$ as $(metaID_i)_{new}$, $(K_i^2)_{old}$ as $(K_i^2)_{new}$, $(K_i^2)_{new}$ as $PRNG((K_i^2)_{new}) \oplus N_t$ and $(metaID_i)_{new}$ as $[PRNG((metaID_i)_{new}) \|CRC((metaID_i)_{new})] \oplus N_t \oplus N_r$;
   - and sends M_2 to the reader;

(5) Once the reader receives the message, it sends M_2 to the tag.

(6) Upon receipt of the message, the tag:
   - computes $M_2' = [CRC(K_i^2\|N_t)\|CRC(K_i^2 \|N_r)] \oplus metaID_i$;
   - checks whether M_2' is equal to the received value of M_2. If it is ok, it authenticates the server and updates K_i^2 and $metaID_i$ as $PRNG(K_i^2) \oplus N_t$ and $[PRNG(metaID_i)\|CRC(metaID_i)] \oplus N_t \oplus N_r$ respectively.

3 Secret Disclosure Attack

Secret disclosure attack is classified among the very strong attacks, because by doing this attack and retrieving one or all of protocol secret values, it may be easy to do other attacks such as impersonating one of the protocol's parties or trace a tag holder.

For the proposed secret disclosure attack, it is enough that the adversary does the following procedure:

Reader Impersonation Phase (Learning Phase): In this phase, the attacker pretends to be a legitimate reader as follows:

(1) The adversary generates a random number N_{r1} and sends it, along with *query*, to the tag.

(2) Once the tag receives the message, it does as follows:
   - generates a random number N_{t1};
   - computes $M_1 = [PRNG(K_i^2 \oplus N_{r1})\| PRNG(K_i^2 \oplus N_{t1})] \oplus metaID_i$;
   - computes $N = CRC([K_i^1]_R\|N_{r1}) \oplus N_{t1}$;
   - and sends M_1 and $N\|(N_{t1} \oplus [K_i^1]_L)$ to the reader, which is impersonated by the adversary.

(3) The attacker receives the messages and stores them. Then, the attacker terminates this session. Up to now, the tag has not updated its secret values yet.

(4) The adversary initiates another session and repeats the above steps once again for this session, where it generates another random number N_{r2} and sends it along with *query* to the tag.

(5) Once the tag receives the message, it does as follows:
   - generates another random number N_{t2};
   - computes $M_1' = [PRNG(K_i^2 \oplus N_{r2})\| PRNG(K_i^2 \oplus N_{t2})] \oplus metaID_i$;
   - computes $N' = CRC([K_i^1]_R\|N_{r2}) \oplus N_{t2}$;
   - and sends M_1' and $N'\|(N_{t2} \oplus [K_i^1]_L)$ to the reader which is the adversary.

Secret Disclosure Attack Phase : In this phase of the attack, using the information which the adversary received in the learning phase of the attack, based on below observation, it does the following computations:

Observation 1 : Given that the message M_1 in the Moradi *et al.*'s protocol is calculated as follows:

$M_1 = [PRNG(K_i^2 \oplus N_r)\|PRNG(K_i^2 \oplus N_t)] \oplus metaID_i$;

If we divide M_1 into two parts, its left and right halves are as follows:
$[M_1]_L = PRNG(K_i^2 \oplus N_r) \oplus [metaID_i]_L$;

$[M_1]_R = PRNG(K_i^2 \oplus N_t) \oplus [metaID_i]_R$;

where $[metaID_i]_L$ and $[metaID_i]_R$ are the left and the right halves of $metalID_i$ respectively.

Based on *Observation 1* and given the stored information from the learning phase of the protocol, to retrieve the secret parameters of the Moradi *et al.*'s protocol, the adversary does as follows:

- given, $N\|(N_{t1} \oplus [K_i^1]_L)$ and $N'\|(N_{t2} \oplus [K_i^1]_L)$, where $N = CRC([K_i^1]_R\|N_{r1}) \oplus N_{t1}$ and $N' = CRC([K_i^1]_R\|N_{r2}) \oplus N_{t2}$, the adversary retrieves $\Delta N_t = N_{t1} \oplus N_{t2}$;
- adversary also calculates $\Delta N_r = N_{r1} \oplus N_{r2}$;
- computes $[M_1]_L \oplus [M_1']_L$ which is equal to $PRNG(K_i^2 \oplus N_{r1}) \oplus PRNG(K_i^2 \oplus N_{r2})$;
- computes $[M_1]_R \oplus [M_1']_R$ which is equal to $PRNG(K_i^2 \oplus N_{t1}) \oplus PRNG(K_i^2 \oplus N_{t2})$;

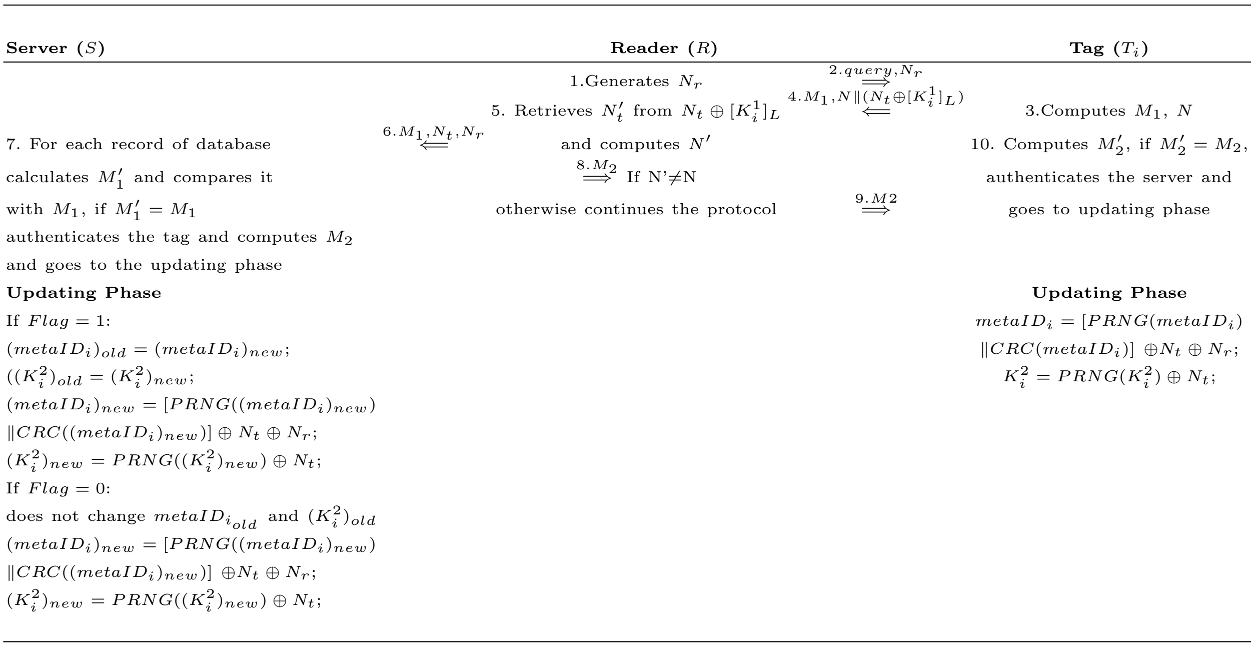
Server (S)
Reader (R)
Tag (T_i)
1.Generates N_r
$\xrightarrow{2.query, N_r}$
3.Computes M_1, N
$\xleftarrow{4.M_1, N\|(N_t \oplus [K_i^1]_L)}$
5. Retrieves N_t' from $N_t \oplus [K_i^1]_L$
and computes N'
$\xleftarrow{6.M_1, N_t, N_r}$
7. For each record of database
calculates M_1' and compares it
with M_1, if $M_1' = M_1$
authenticates the tag and computes M_2
and goes to the updating phase
$\xrightarrow{8.M_2}$ If N'≠N
otherwise continues the protocol
$\xrightarrow{9.M2}$
10. Computes M_2', if $M_2' = M_2$,
authenticates the server and
goes to updating phase
Updating Phase
If $Flag = 1$:
$(metaID_i)_{old} = (metaID_i)_{new}$;
$((K_i^2)_{old} = (K_i^2)_{new}$;
$(metaID_i)_{new} = [PRNG((metaID_i)_{new})$
$\|CRC((metaID_i)_{new})] \oplus N_t \oplus N_r$;
$(K_i^2)_{new} = PRNG((K_i^2)_{new}) \oplus N_t$;
If $Flag = 0$:
does not change $metaID_{i_{old}}$ and $(K_i^2)_{old}$
$(metaID_i)_{new} = [PRNG((metaID_i)_{new})$
$\|CRC((metaID_i)_{new})] \oplus N_t \oplus N_r$;
$(K_i^2)_{new} = PRNG((K_i^2)_{new}) \oplus N_t$;
Updating Phase
$metaID_i = [PRNG(metaID_i)$
$\|CRC(metaID_i)] \oplus N_t \oplus N_r$;
$K_i^2 = PRNG(K_i^2) \oplus N_t$;

Figure 1. Moradi *et Al.*'S Improved Authentication Protocol[29].

- for $j = 0, ..., 2^{16} - 1$:
  - $K_i^2 \oplus N_{r1} \leftarrow j$;
  - if $[M_1]_L \oplus [M_1']_L = PRNG(j) \oplus PRNG(j \oplus \Delta N_r)$, returns j as $K_i^2 \oplus N_{r1}$;
  - returns K_i^2 as $j \oplus N_{r1}$;
- for $j = 0, ..., 2^{16} - 1$:
  - $K_i^2 \oplus N_{t1} \leftarrow j$;
  - if $[M_1]_R \oplus [M_1']_R = PRNG(j) \oplus PRNG(j \oplus \Delta N_t)$, returns j as $K_i^2 \oplus N_{t1}$;
  - returns N_{t1} as $j \oplus K_i^2$;
  - returns $[K_i^1]_L$ as $(N_{t1} \oplus [K_i^1]_L) \oplus N_{t1}$;
- given that $N = CRC([K_i^1]_R \| N_{r1}) \oplus N_{t1}$, for $j = 0, ..., 2^{16} - 1$:
  - $[K_i^1]_R \leftarrow j$;
  - if $N = CRC(j \| N_{r1}) \oplus N_{t1}$, returns j as $[K_i^1]_R$;
- retrieves $metaID_i$ as $M_1 \oplus [PRNG(K_i^2 \oplus N_r) \| PRNG(K_i^2 \oplus N_t)]$;

Hence, all the secret parameters of the protocol, *i.e.* $metaID_i$, K_i^1 and K_i^2, are disclosed. The complexity of the proposed attack is only two times reader impersonation attack and doing only at most $O(2^{16})$ offline computations. Given all secret parameters, applying any other attack on the protocol would be trivial. Hence we exempt them.

4 Recommendation for Improving the Protocol

The current study and previous related studies, *e.g.* [16, 32–35], that compromise security of protocols which have been designed based on EPC- C1 G2, show that it may not be possible to design a new secure protocol based on EPC- C1 G2 standard. The reason is due to this fact that the EPC- C1 G2 standard recommended using 16-bit CRCs and 16-bit PRNGs in designing secure protocols. However, as shown in [28], without EPC- C1 G2 standard change, the design of a secure protocol sounds to be impossible and the standard must be changed, and lightweight block ciphers such as SKINNY [31], SIMON and SPECK [36] should be allowed in the new standard to be employed. If we use lightweight cryptography primitives instead of 16-bit CRCs and 16-bit PRNGs, it should be possible to design a secure protocol. In this section, we propose a secure protocol based on this strategy. It should be noted that K_i^2 and K_i^1 are 64-bit variables in the proposed protocol (despite the protocol of Moradi *et al.*). In addition, the length of the random numbers that are generated by protocol's parties are changed to 32 bits, instead of 16 bits in the predecessor protocols. Similar to the Moradi *et al.*'s protocol, to avoid traceability, both parties update their shared parameters after each successful run of the protocol. We also assume the channel between the reader and the server is secure. Assuming that we are given a lightweight block cipher $E_K(M) : \{0,1\}^{64} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$, *e.g.* SKINNY-64-64 with tweak part considered as blank or identical to the secret key, the proposed protocol proceeds as follows:

(1) The reader starts the protocol by generating a random number N_r and sending it along with *query* to the tag.

(2) Once the tag receives the message, it does as

follows:

- generates a random number N_t;
- computes $M_1 = E_{K_i^2}(([metaID_i]_R \oplus N_r)\|N_t)$;
- computes $N = E_{K_i^1}(([metaID_i]_L \oplus N_t)\|N_r)$;
- sends N_t, M_1 and N to the reader;

(3) Upon receipt of the message, the reader:

- retrieves $([metaID_i]_L \oplus N_t)\|N_r'$ from $D_{K_i^1}(N)$ and compares the extracted N_r' with its record for the generated random number to validate the tag's access to K_i^1; if the comparison is violated, the reader terminates the protocol.
- If it is ok, the reader extracts $[metaID_i]_L$ from $[metaID_i]_L \oplus N_t$ and sends it along with M_1, N_t and N_r through the secure channel to the server;

(4) Once the server receives the message, it does as follows:

- For each of the database records *i.e.* $(metaID_i)_{old}$, $(metaID_i)_{new}$, $(K_i^2)_{old}$, $(K_i^2)_{new}$ that matches the received $[metaID_i]_L$, it calculates M_1' and checks if it is equal to received value of M_1 to authenticate the tag. This step is repeated among the matched records so that a matching can be found, which indicates the successful authentication of the tag.
- At the same time, if the matching record is $(metaID_i)_{old}$, $(K_i^2)_{old}$ so, it computes $M_2 = E_{(K_i^2)_{old}}(N_r\|N_t)$ and does not change $(metaID_i)_{old}$ and $(K_i^2)_{old}$ but updates $(metaID_i)_{new}$ as $E_{(K_i^2)_{old}}((metaID_i)_{old} \oplus (N_r\|N_t))$ and $(K_i^2)_{new}$ as $E_{(K_i^2)_{old}}((K_i^2)_{old} \oplus (N_r\|N_t))$.
- If the matching record is $(metaID_i)_{new}$, $(K_i^2)_{new}$ so, it computes $M_2 = E_{(K_i^2)_{new}}(N_r\|N_t)$ and updates $(metaID_i)_{old}$ and $(K_i^2)_{old}$ respectively with $(metaID_i)_{new}$ and $(K_i^2)_{new}$. Moreover, given the updated values of $(metaID_i)_{old}$ and $(K_i^2)_{old}$, the server updates $(metaID_i)_{new}$ as $E_{(K_i^2)_{old}}((metaID_i)_{old} \oplus (N_r\|N_t))$ and $(K_i^2)_{new}$ as $E_{(K_i^2)_{old}}((K_i^2)_{old} \oplus (N_r\|N_t))$.
- Finally, the server sends M_2 to the reader;

(5) Once the reader receives the message, it sends M_2 to the tag.

(6) Upon receipt of the message, M_2, the tag verifies whether $M_2 \overset{?}{=} E_{K_i^2}(N_r\|N_t)$ to authenticate the server and updates K_i^2 and $metaID_i$ as $E_{K_i^2}(metaID_i \oplus (N_r\|N_t))$ and $E_{K_i^2}(K_i^2 \oplus (N_r\|N_t))$ respectively; otherwise, the tag terminates the session.

5 Security Analysis of the Proposed Protocol

In this section, at the first, we argue about the insecurity of the Moradi *et al.*'s protocol with regard to formal proof and then informally and after that formally prove the security of our proposed protocol.

5.1 In Security of the Moradi *et Al.*'S Protocol With Regard to Formal Proof

Formal security proof methods of protocols are divided into two categories: manual and automated. The logic of BAN [37] and GNY and etc. are among the category of the manual, and AVISPA [38], Proverif [39] and Scyther [40] are among the category of automated tools. Manual security proof methods are based on assumptions and goals, and if there is a wrong assumption or a wrong goal so the protocol is apparently proven to be safe while it is not. Moradi *et al.* in [29] have provided formal security proof for their protocol using BAN logic but, based on the below-mentioned reason, unfortunately, security of their scheme is lost within formal proof. Precisely, in their formal proof, Moradi *et al.* implicitly assumed that 16-bit PRNGs and also 16-bit output CRCs are fully secure. In the formal security proof of their proposed protocol, they explained the messages of protocols for example $M2 = [PRNG(K_i^2 \oplus N_r)\|PRNG(K_i^2 \oplus N_t)] \oplus metaID_i$ as encrypted messages *i.e.* $\{\{N_r\}_{K_i^2}, \{N_t\}_{K_i^2}\}_{metaID_i}$. However, in this paper we showed that such primitives are not enough strong encryption functions and so explanation of protocol messages as encrypted messages are wrong. BAN logic, with the assumption that the cryptographic functions are fully secured based on their own rules, will result protocol's goals. Moradi *et al.* assumed that their protocol messages, which have a secure value in their calculations, are such that they are encrypted with a secret value, and with this assumption and explanations, based on the BAN logic rules, they proved that their protocol is safe. However, in our proposed protocol we actually used cryptographic encryption functions in calculating of messages, and so they are correctly considered as encrypted messages and hence, using the GNY logic's rules, we proved that the proposed protocol is safe.

5.2 Informal Security Analysis

5.2.1 Resistance Against Secret Disclosure Attack

Since most messages of the proposed protocol are computed by using the lightweight block ciphers instead of the 16-bit PRNGs and 16-bit CRCs, the improved protocol resists against the secret disclosure attack presented in this paper.

5.2.2 Resistance Against DoS Attack

Since the proposed protocol has properties such as keeping old and new versions of the secret parameters on the server side and participating both the tag and the reader in randomizing all the messages, the proposed protocol is also safe against DoS attacks.

5.2.3 Resistance Against Impersonation Attacks and Replay Attacks

Since all messages which are exchanged in the protocol are generated using the block ciphers, and also the random numbers that the parties have generated are used in calculating all of the protocol messages, it is not possible for the adversary to be able to generate a valid protocol message or to get the confirmation from protocol parties only by replaying the messages of previous sessions.

5.2.4 Resistance Against Traceability Attacks

Since in the proposed protocol, messages that contain the protocol's parties' identity are encrypted, and the messages of each session are randomized by random numbers generated by the protocol parties, cannot be interconnected to one another, or other session messages. Therefore the constant information that is needed to trace the protocol's parties cannot be obtained from them. So the proposed protocol is secure against the traceability attack.

5.3 Formal Security Analysis

Formal Proof through GNY Logic

In this section by using GNY Logic [41], we formally prove our proposed protocol's security.

The security analysis of protocol by using GNY logic involves four steps:

- **Expression of protocol messages :** in this step, the protocol messages are written using mathematical relationships and also GNY logic relationships as follows. Since we assumed that the channel between the reader and the server is secure, we consider all transferred messages between the reader and the server encrypted using a secret key, *i.e.*, K_{SR}, which is shared between the reader and the server.

  $M1 : R \rightarrow T : N_r, query;$
  $M2 : T \rightarrow R : M_1 = E_{K_i^2}(([metaID_i]_R \oplus N_r)\|N_t),\ N = E_{K_i^1}(([metaID_i]_L \oplus N_t)\| N_r));$
  $M3 : R \rightarrow S : \{[metaID_i]_L\}_{K_{SR}}, \{M_1 = E_{K_i^2}(([metaID_i]_R \oplus N_r)\|N_t)\}_{K_{SR}}, \{N_r\}_{K_{SR}}, \{N_t\}_{K_{SR}};$
  $M4 : S \rightarrow R : \{M_2 = E_{K_i^2}(N_r\|N_t)\}_{K_{SR}};$
  $M5 : R \rightarrow T : M_2 = E_{K_i^2}(N_r\|N_t);$

  which is also written as follows:
  $M1 : T \lhd\ N_r$, queryquery
  $M2 : R \lhd\ \{metaID_i, N_r, N_t\}_{K_i^2}, \{metaID_i, N_r, N_t\}_{K_i^1};$
  $M3 : S \lhd \{[metaID_i]_L\}_{K_{SR}}, \{\{metaID_i, N_r, N_t\}_{K_i^2}\}_{K_{SR}},; \{N_r\}_{K_{SR}}, \{N_t\}_{K_{SR}};$
  $M4 : R \lhd\ \{\{N_r, N_t\}_{K_i^2}\}_{K_{SR}};$
  $M5 : T \lhd \{N_r, N_t\}_{K_i^2};$

- **Idealization of protocol messages:** in this step, the messages that are plain will be deleted as below:

  $IM2 : R \lhd\ \{metaID_i, N_r, N_t\}_{K_i^2}, \{metaID_i, N_r, N_t\}_{K_i^1};$
  $IM3 : S \lhd \{[metaID_i]_L\}_{K_{SR}}, \{\{metaID_i, N_r, N_t\}_{K_i^2}\}_{K_{SR}}, \{N_r\}_{K_{SR}}, \{N_t\}_{K_{SR}};$
  $IM4 : R \lhd \{\{N_r, N_t\}_{K_i^2}\}_{K_{SR}};$
  $IM5 : T \lhd \{N_r, N_t\}_{K_i^2};$

- **Expression of protocol assumptions and security goals:**

  The proposed protocol's assumptions are expressed as:

  $A1 : T| \equiv \sharp N_t;$
  $A2 : T \ni N_t;$
  $A3 : T| \equiv \phi(N_t);$
  $A4 : R| \equiv \sharp N_r;$
  $A5 : R \ni N_r;$
  $A6 : R| \equiv \phi(N_r);$
  $A7 : S| \equiv S \xleftrightarrow{K_i^2} T;$
  $A8 : T| \equiv T \xleftrightarrow{K_i^2} S;$
  $A9 : R| \equiv R \xleftrightarrow{K_i^1} T;$
  $A10 : T| \equiv T \xleftrightarrow{K_i^1} R;$
  $A11 : S| \equiv S \xleftrightarrow{metaID_i} T;$
  $A12 : T| \equiv T \xleftrightarrow{metaID_i} S;$
  $A13 : T \ni K_i^2;$
  $A14 : T \ni K_i^1;$
  $A15 : S \ni K_i^2;$
  $A16 : R \ni K_i^1;$
  $A17 : S| \equiv S \xleftrightarrow{K_{SR}} R;$
  $A18 : R| \equiv R \xleftrightarrow{K_{SR}} S;$

  The security goals of the proposed protocol are as:
  $G1 : T| \equiv S| \sim \sharp\{N_r, N_t\}_{K_i^2};$
  $G2 : R| \equiv T| \sim \sharp\{metaID_i, N_r, N_t\}_{K_i^1};$

  $G1$ and $G2$ shows the adversary does not have any control on encrypted values and also random numbers which are plain and send through insecure channel.

- **Deduction of security goals from protocol messages and assumptions using proper GNY logic rules**:

  Given $A1$ assumption, then based on $F1$ rule of GNY logic, we deduce that $D1 : T| \equiv \sharp(\{N_r, N_t\})$;

  After that we consider $D1$ and $A13$, then based on $F2$ rule of GNY logic, we deduce that $D2 : T| \equiv \sharp\{N_r, N_t\}_{K_i^2}$;
  After that we consider $A3$, then based on $R1$ rule of GNY logic, we deduce that $D3 : T| \equiv \phi(\{N_r, N_t\})$;

  If we consider $IM5$, $A13$, $A8$, $D3$ and $D1$, then based on $I1$ rule of GNY logic, we deduce $D4 : T| \equiv S| \sim \sharp\{N_r, N_t\}_{K_i^2}$ which is same $G1$.
  Given $A4$ assumption, then based on $F1$ rule of GNY logic, we deduce that $D5 : R| \equiv \sharp(\{metaID_i, N_r, N_t\})$;

  After that we consider $D5$ and $A16$, then based on $F2$ rule of GNY logic, we deduce that $D6 : R| \equiv \sharp\{metaID_i, N_r, N_t\}_{K_i^1}$;
  After that we consider $A6$, then based on $R1$ rule of GNY logic, we deduce that $D7 : R| \equiv \phi(\{metaID_i, N_r, N_t\})$;

  If we consider $IM2$, $A9$, $A16$, $D7$ and $D5$, then based on $I1$ rule of GNY logic, we deduce $D8 : T| \equiv R \sim \sharp\{metaID_i, N_r, N_t\}_{K_i^1}$ which is same $G2$.

6 Comparison

In this section, we compare the proposed protocol with its predecessors from security and computational cost aspects. As can be seen in Table 2, the proposed protocol, despite its predecessors, resists different attacks while as depicted in Table 3 our protocol is costly than the others. We used encryption functions with 64-bit inputs, outputs, and keys. There are lightweight block ciphers such as SKINNY-64-64 [31] that requires reasonable resource and suitable for lightweight applications like EPC- C1 G2 standard. Based on the designers report, SKINNY-64-64 [31] can be implemented in round-based implementation mode which provides a trade off between delay and area, using 1223 gates while its delay is $1.77 - ns$, they reported that throughput of the scheme in 100 KHz is 200 Bit/s in this mode. A nibble /bit serial implementations of the scheme also have been provided which require only 988/839 gates and its delay will be $1.03 - ns$. Moreover, Jean *et al.* [42] also presented a bit-serial ASIC implementations of SKINNY, called bit-sliding implementation, which requires 1054 gates for a 64-bit block with 128-bit key version, which could be a good candidate to provide higher security. In this case, the required gates for SKINNY-64-64 is 747 while the delay will be $2.25 - ns$. Hence, SKINNY-64-64 could be a good candidate for lightweight applications like EPC- C1 G2 standard. However, as it also pointed out correctly by an anonymousness reviewer, *"IoT systems have many challenges, and security is only one of them and other criteria such as processing and execution time and transmission overhead should also be considered"*. By the way, we tried to reduce the protocol overhead as much as possible. More precisely, the more constrained side, which is the tag, only requires the encryption function and even not the decryption function. More over it only encrypts 320 bits in total including update phase, in each session, which could be reasonable. Any way we can not achieve desired security without any cost.

Table 2. The Security Comparison of the Improved Protocol With Its Predecessors Where A1: Secret Disclosure Attack; A2: Impersonation Attack and Replay Attack; A3: DoS Attack and A4: Traceability Attack.

Protocols	**A1**	**A2**	**A3**	A4
Wei and Zhang[30]	✓	×	×	✓
Moradi *et al.*[29]	×	×	×	×
The proposed method	✓	✓	✓	✓

Table 3. The Computation Complexity Comparison of the Improved Protocol With Its Predecessors.

Protocols	**♯ of** $\oplus$	**♯ of** $\|$	**♯ of** CRC	**♯ of** $PRNG$	**♯ of** $E_K(.)$ $D_K(.)$	**♯ of transferred bits**
Wei and Zhang[30]	16 × 16	17	12	4	–	10 × 16
Zhang[30] Moradi *et al.*[29]	18 × 16	13	8	8	–	10 × 16
The proposed method method	6 × 64	10	–	–	10	8 × 64

7 Conclusion

In this paper, we have shown that designing a secure protocol in the EPC-C1 G2 standard framework using 16-bit PRNGs and also 16-bit CRCs may not be possible, and in order to achieve a secure protocol, this standard must be changed so that it allows the use of cryptography primitives. In the same vein, we investigated the security of Moradi *et al.* EPC- C1 G2 authentication protocol and showed its vulnerability against secret disclosure attack. The complexity of the proposed attack is only two times reader impersonation and doing almost 3×2^{16} offline computations. We also presented an improved version of the protocol and proved its security against the attack presented in this paper and also other known active and passive attacks.

Acknowledgements

This work was supported by Shahid Rajaee Teacher Training University.

References

[1] C. Wei, C.Yang, M. Hwang, and A. Chin. Cryptanalysis of li–wang authentication protocol for secure and efficient rfid communication. In *Recent Developments in Intelligent Computing, Communication and Devices*, pages 699–705. Springer, Singapore, 2019. ISBN 978-981-10-8943-5. doi:10.1007/978-981-10-8944-2_80.

[2] P. Arulmozhi, J. B. B. Rayappan, and Pethuru Raj. A lightweight memory-based protocol authentication using radio frequency identification (rfid). In *Advances in Big Data and Cloud Computing*, pages 163–172. Springer, Singapore, 2019. ISBN 978-981-13-1881-8. doi:10.1007/978-981-13-1882-5_14.

[3] L. Zhou, X. Li, K. Yeh, C. Su, and W. Chiu. Lightweight iot-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, 91:244–251, 2019. doi:10.1016/j.future.2018.08.038.

[4] Y. Bendavid, N. Bagheri, M. Safkhani, and S. Rostampour. Iot device security: Challenging "a lightweight rfid mutual authentication protocol based on physical unclonable function". *Sensors*, 18(12):4444, 2018. doi:10.3390/s18124444.

[5] F. Moradi, H. Mala, and B. Tork Ladani. Security analysis and strengthening of an rfid lightweight authentication protocol suitable for vanets. *Wireless Personal Communications*, 83(4):2607–2621, 2015. ISSN 0929-6212. doi:10.1007/s11277-015-2558-0.

[6] A. Falahati and H. Jannati. All-or-nothing approach to protect a distance bounding protocol against terrorist fraud attack for low-cost devices. *Electronic Commerce Research*, 15(1):75–95, 2015. ISSN 1389-5753. doi:10.1007/s10660-014-9167-y.

[7] Y. Liu, M. F. Ezerman, and H. Wang. Double verification protocol via secret sharing for low-cost rfid tags. *Future Generation Computer Systems*, 90:118–128, 2019. doi:10.1016/j.future.2018.07.004.

[8] Hoda Jannati. Cryptanalysis and enhancement of two low cost rfid authentication protocols. *arXiv preprint arXiv:1202.1971*, 2012. doi:10.5121/iju.2012.3101.

[9] Y. Liu, X. Yin, Y. Dong, and K. Huang. Lightweight authentication scheme with inverse operation on passive rfid tags. *Journal of the Chinese Institute of Engineers*, 42(1):74–79, 2019. doi:10.1080/02533839.2018.1537811.

[10] S. F. Aghili, M. Ashouri-Talouki, and H. Mala. Dos, impersonation and de-synchronization attacks against an ultra-lightweight rfid mutual authentication protocol for iot. *The Journal of Supercomputing*, 74(1):509–525, 2018. ISSN 0920-8542. doi:10.1007/s11227-017-2139-y.

[11] P. Huang, H. Mu, and C. Zhang. Cryptanalysis and enhancement of a secure group ownership transfer protocol for rfid tags. In *Global Security, Safety and Sustainability & e-Democracy*, pages 186–193. Springer, Berlin, Heidelberg, 2011. ISBN 978-3-642-33447-4. doi:10.1007/978-3-642-33448-1_26.

[12] C. Liu, I. Liu, C. Lin, and J. Li. A novel tag searching protocol with time efficiency and searching accuracy in rfid systems. *Computer Networks*, 150:201–216, 2019. doi:10.1016/j.comnet.2019.01.011.

[13] A. Falahati, H. Azizi, and R. M. Edwards. Rfid light weight server-less search protocol based on nlfsrs. In *2016 8th International Symposium on Telecommunications (IST)*, pages 741–745. IEEE, 2016. ISBN 978-3-540-70543-7. doi:10.1109/ISTEL.2016.7881921.

[14] Y. Tian, G. Chen, and J. Li. A new ultralightweight rfid authentication protocol with permutation. *IEEE Communications Letters*, 16(5):702 – 705, 2012. ISSN 1089-7798. doi:10.1109/LCOMM.2012.031212.120237.

[15] S. h. Wang, Z. Han, S. Liu, and D. w. Chen. Security analysis of rapp an rfid authentication protocol based on permutation. *IACR Cryptology ePrint Archive*, page 327, 2012.

[16] N. Bagheri, M. Safkhani, P. Peris-Lopez, and Juan E. Tapiador. Weaknesses in a new ultralightweight rfid authentication protocol with permutation—rapp. *Security and Communication Networks*, 7(6):945–949, 2014. doi:10.1002/sec.803.

[17] X. Zhuang, Y. Zhu, and C. Chang. A new ultralightweight rfid protocol for low-cost tags: r^2 ap. *Wireless Personal Communications*, 79(3):1787–1802, 2014. ISSN 0929-6212. doi:10.1007/s11277-014-1958-x.

[18] E. Taqieddin, H. Al-Dahoud, and K. Mhaidat. Security analysis and improvement of reconstruction based radio frequency identification authentication protocol. *International Journal on Communications Antenna and Propagation (IRECAP)*, 8(3), 2018. doi:10.15866/irecap.v8i3.13398.

[19] M. Safkhani. Cryptanalysis of r2ap an ultralightweight authentication protocol for rfid. *Journal of Electrical and Computer Engineering Innovations*, 6(1):107–114, 2018. ISSN 2322-3952.

[20] P. Huang, H. Mu, and C. Zhang. A new lightweight rfid grouping proof protocol. In *Advanced Technologies, Embedded and Multimedia for Human-centric Computing*, pages 869–876. Springer, Dordrecht, 2014. ISBN 0-8186-2060-9. doi:978-94-007-7261-8.

[21] S. Rostampour, N. Bagheri, M. Hosseinzadeh, and A. Khademzadeh. On the security of permutation based authentication protocols for internet of things applications: The case of huang et al.'s protocol. *Journal of Computing and Security*, 3 (4):201–209, 2016. ISSN 2322-4460.

[22] K. Fan, W. Jiang, H. Li, and Y. Yang. Lightweight rfid protocol for medical privacy protection in iot. *IEEE Transactions on Industrial Informatics*, 14(4):1656–1665, 2018. ISSN 1551-3203. doi:10.1109/TII.2018.2794996.

[23] S. F. Aghilia, H. Mala, P. Kaliyar, and M. Conti. Seclap: Secure and lightweight rfid authentication protocol for medical iot. *Future Generation Computer Systems*, 101:621 – 634, 2019. doi:10.1007/s11277-014-2189-x.

[24] M. Safkhani, Y. Bendavid, S. Rostampour, and N. Bagheri. On designing lightweight rfid security protocols for medical iot. *IACR Cryptology ePrint Archive*, page 851, 2019.

[25] I. Jeon and E. Yoon. A new ultra-lightweight rfid authentication protocol using merge and separation operations. *International Journal of Mathematical Analysis*, 7(49):2583–2593, 2013. doi:10.12988/ijma.2013.36146.

[26] L. Pang, L. He, Q. Pei, and Y. Wang. Secure and efficient mutual authentication protocol for rfid conforming to the epc c-1 g-2 standard. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pages 1870–1875. IEEE, 2013. ISBN 978-1-4673-5938-2. doi:10.1109/WCNC.2013.6554849.

[27] S. Wang, S. Liu, and D. Chen. Security analysis and improvement on two rfid authentication protocols. *Wireless Personal Communications*, 82(1): 21–33, 2015. ISSN 0929-6212. doi:10.1007/s11277-014-2189-x.

[28] M. Safkhani, M. Hosseinzadeh, M. E. Namin, S. Rostampour, and N. Bagheri. On the (im) possibility of receiving security beyond 2 l using an l-bit prng. *Wireless Personal Communications*, 92(4):1591–1597, 2017. ISSN 0929-6212. doi:10.1007/s11277-016-3623-z.

[29] F. Moradi, H. Mala, B. Tork Ladani, and F. Moradi. Security analysis of an epc class-1 generation-2 compliant rfid authentication protocol. *Journal of Computing and Security*, 3(3): 163–174, 2016.

[30] G. Wei and H. Zhang. A lightweight authentication protocol scheme for rfid security. *Wuhan University Journal of Natural Sciences*, 18(6):504–510, 2013. ISSN 1007-1202. doi:10.1007/s11859-013-0964-2.

[31] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim. The skinny family of block ciphers and its low-latency variant mantis. In *Annual Cryptology Conference*, pages 123–153. Springer, Berlin, Heidelberg, 2016. ISBN 978-3-662-53007-8. doi:10.1007/978-3-662-53008-5_5.

[32] G. Avoine and X. Carpent. Yet another ultralightweight authentication protocol that is broken. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pages 20–30. Springer, Berlin, Heidelberg, 2012. ISBN 978-3-642-36139-5. doi:10.1007/978-3-642-36140-1_2.

[33] P. D'Arco and A. D. Santis. On ultralightweight rfid authentication protocols. *IEEE Transactions on Dependable and Secure Computing*, 8(4):548 – 563, 2011. ISSN 1545-5971. doi:10.1109/TDSC.2010.75.

[34] G. Avoine, X. Carpent, and B. Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *Journal of Network and Computer Applications*, 35(2):826–843, 2012. doi:10.1016/j.jnca.2011.12.001.

[35] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref. Recursive linear and differential cryptanalysis of ultralightweight authentication protocols. *IEEE Transactions on Information Forensics and Security*, 8(7):1140 – 1151, 2013. ISSN 1556-6013. doi:10.1109/TIFS.2013.2263499.

[36] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers. The simon and speck lightweight block ciphers. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2015. ISBN 978-1-4799-8052-9. doi:10.1145/2744769.2747946.

[37] M. Burrows, M. Abadi, and R. Needham. Ban a logic of authentication. *Technical report 39, Digital Equipment Systems Research center, Palo Alto, California*, 1989.

[38] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma,

P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. The avispa tool for the automated validation of internet security protocols and applications. In *International conference on computer aided verification*, pages 281–285. Springer, Berlin, Heidelberg, 2005. ISBN 978-3-540-27231-1. doi:10.1007/11513988_27.

[39] B. Blanchet and A. Chaudhuri. Automated formal analysis of a protocol for secure file sharing on untrusted storage. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 417–431. IEEE, 2008. ISBN 978-0-7695-3168-7. doi:10.1109/SP.2008.12.

[40] Cas J. F. Cremers. The scyther tool: Verification, falsification, and analysis of security protocols. In *International Conference on Computer Aided Verification*, pages 414–418. Springer, Berlin, Heidelberg, 2008. ISBN 978-3-540-70543-7. doi:10.1007/978-3-540-70545-1_38.

[41] L. Gong, R. Needham, and R. Yahalom. Reasoning about belief in cryptographic protocols. In *Proceedings. 1990 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 234–248. IEEE, 1990. ISBN 0-8186-2060-9. doi:10.1109/RISP.1990.63854.

[42] J. Jean, A. Moradi, T. Peyrin, and P. Sasdrich. Bit-sliding: a generic technique for bit-serial implementations of spn-based primitives. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 687–707. Springer, Cham, 2017. ISBN 978-3-319-66786-7. doi:10.1007/978-3-319-66787-4_33.

Masoumeh Safkhani is an assistant professor at Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. She received her Ph.D. from Iran University of Science and Technology. She is the author of over 50 articles in information security and cryptology. A record of her publications is available at google scholar.