Int. j. inf. tecnol. (June 2021) 13(3):1209–1215
https://doi.org/10.1007/s41870-021-00632-y

ORIGINAL RESEARCH

Mutual authentication protocol for low cost passive tag in RFID system

Atul Kumar[1] · **Ankit Kumar Jain**[1]

Received: 6 May 2020 / Accepted: 13 February 2021 / Published online: 6 March 2021

Abstract Internet of things (IoT) contains a massive number of "things" that are connected to the internet and communicates without human interaction. In these IoT devices, Radio frequency identification is used to detect the location of devices in communication networks. However, the RFID tag contains a low power battery and low memory capacity (i.e., few KB). Hence, it requires a lightweight or ultra-lightweight solutions for these RFID tags. This paper proposes a novel ultra-lightweight authenticate approach for a passive tag that uses XOR and rotate operations. This scheme contains three different phases: tag identification, mutual authentication, and pseudonyms and key updating phases. The first phase comprises the identification of the tag. After that, the second phase performs mutual authentication between the tag and the reader. The last phase involves the updating of the key between the tag and the reader. This scheme also defines the function "MIX" to enhance the security of the protocol. This scheme analyses in terms of communication cost between tag and reader, and storage cost for a passive tag.

Keywords IoT · RFID · Passive tag · Authentication

✉ Atul Kumar
atul.kumar1995@gmail.com

Ankit Kumar Jain
ankitjain@nitkkr.ac.in

[1] Department of Computer Engineering, National Institute of Technology, Kurukshetra, India

1 Introduction

IoT contains various devices like tag, sensor, reader, smart card, actuator. According to Garner's report [1], there are 8.4 billion IoT devices connected to the internet in 2017, and it will grow up to 20.4 billion devices in 2020. These large numbers of devices require a massive amount of power. Hence, the researcher develops various lightweight schemes for these IoT devices. IoT scheme can be applied in many domains such as smart transportation [2], smart grid [3], smart city [4], smart house [5], logistics [6]. However, there are many security issues in terms of authentication, authorization, and privacy [7].

In cryptography, there are various cryptography schemes concerns to IoT that divides into two parts, namely public key cryptography and symmetric key cryptography. Public key cryptography schemes consists of various traditional scheme like RSA, Diffie–Hellman key exchange, Elgamal. However, these schemes require lots of computational capacity and power. An elliptic curve introduces to eliminate these problems that provide less power and fewer communication steps. Symmetric key cryptographic schemes use simple bitwise operation (XOR, OR, AND, rotate), cyclic redundancy checksum, and symmetric encryption. Symmetric key cryptography schemes require less power and communication steps than public-key cryptography.

The radio frequency identification [8] uses to detect the location of devices in communication networks. There are two components in the RFID system, i.e., tags and reader. The tag store identification information (ID), shared key, and other essential information in his memory. There are various tags in an RFID system, such as passive tags, active tags, and semi-passive tags. The passive tags use for lifetime application and having short communication range

applications. The passive tags contain no power battery, but it receives power from an electromagnetic field from the reader. Hence, the passive tag can compute simple bitwise operation, i.e., AND, OR, XOR. The active tag receives power from the battery. Hence, the active tags use for large sensing range applications. Generally, the active tags contain power supply last up to 3–4 years. The active tag can compute symmetric or asymmetric operations like the elliptic curve, recursive checksum. The semi-passive tag consists of a small battery supply. The semi-passive tag outside the range of the reader, it receives power from the battery supply. However, the tag inside the reader's range receives power using the electromagnetic field similar to passive tag.

In RFID security, there are various classes of tags in the RFID system, such as full-fledged, simple, light-weight, and ultra-lightweight classes. The full-fledged class tag can be capable of computing computational costly operations. However, these tags require massive power and computation capacity than other types of tags. Hence, these tags are incredibly costly. The simple class tag capable of computing much lesser computational and power than full-fledged class. The lightweight tag can compute the elliptic curve, hash function. These types of tags are economical in the cost. The ultra-lightweight class consists of simple bitwise operations like OR, XOR, AND, Rot. These class tags require very less computational capacity. Figure 1 shows a general overview of RFID architecture. RFID tags contain a limited amount of power and low computational capacity. Hence, the researcher suggests various light-weight or ultra-lightweight algorithms for computing the authentication.

1.1 Our contribution

This paper creates a new ultra-lightweight authentication scheme for RFID. This scheme comprises of three different phases: tag identification phase, mutual authentication phase, and pseudonyms and key updating phase. This scheme uses Rot operation, "MIX" function, and XOR operation to computes mutual authentication. This paper consists of five sections: the second section involves various existing schemes for mutual authentication for the RFID system. The third section describes the proposed scheme for the RFID system. The fourth section consists of the security and performance analysis of the proposed scheme. The last section includes the overall conclusion of the entire paper

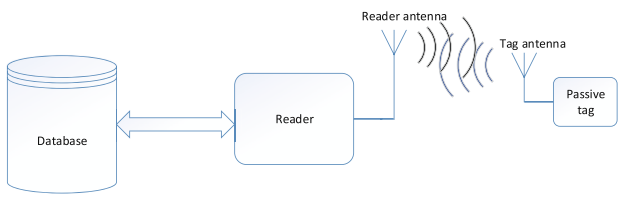

Fig. 1 General overview of RFID architecture

2 Literature review

Chien et al. [9] proposed an authentication scheme for RFID passive tag named as SASI. This scheme uses $\oplus$, $+$, ROT, OR, AND operation during mutual authentication. The researcher found that SASI scheme cannot provide security against various attacks such as de-synchronization attack, disclosure attack, and tracking attack [10, 11]. After that, Peris-Lopez et al. [12] proposed an authentication scheme for RFID system and named as Gossamer. This scheme uses $\oplus$, $+$, AND, MIXBIT, and Rot operations. This scheme address limitation of the SASI scheme using a double rotate function and MIXBIT function. The author uses MIXBIT operation to defend against desynchronization attack. In MIXBIT function consists of addition operation and bitwise right shift operation that is light-weight and easily implements in hardware. However, this scheme provides a low throughput. Later on, Bilal et al. [13] found a desynchronization attack possible on the Gossamer scheme.

He et al. [14] proposed an authentication scheme for the RFID system with an ID verifier transfer protocol. This scheme requires 1440 bits + 480w bits of storage capacity for the server, and tag required 1760 bits of storage capacity. Hence, the total storage requirements of the RFID system is 3200 and 480w bits during the authentication process. RAPP [15] uses XOR, AND, OR, ROT, and Per operations, where Per operation defines as permutation operation. The author suggested that the Per operation is used to improve the security of authentication protocol. This scheme provides resistance from various security flaws such as disclosure attack, tracking, replay attack. Ahmadian [16] performs desynchronization attack on RAPP protocol. Then, Chien et al. [17] proposed a light-weight scheme for RFID in which he uses the elliptic curve and hash function during process of mutual authentication. However, this scheme cannot provide security against various attacks such as tracking, cloning, and replay attacks. Tewari et al. [18] proposed an ultra-lightweight authentication protocol in which it uses Rot and XoR operators to defend against the desynchronization attack. However, Safkhani et al. [19] performs secret disclosure attack on Tiwari and Guptascheme [18].

3 Proposed scheme

Figure 2 shows propose ultra-lightweight authentication scheme for passive RFID tag. In this scheme, there are three different phases to authentication between tag and reader, such as tag identification phase, mutual authentication phase, and pseudo-random and key updating phase. Table 1 represent various notation uses in this paper.

3.1 Tag identification

In this phase, the tag enters in communication range of a reader, then it receives "hello" packet from a reader, and the tag sends its pseudonyms ID (IDS) to the reader.

3.2 Mutual authentication phase

1. After receiving IDS, the reader validates IDS with stored IDS_{new}. If it matches with IDS_{new}, then the reader computes A, B from K_{new} and random number, where A and B compute according to the Eqs. (1) and (2). After that, the reader transmits message packets A and B to the tag.

$$A = Rot(n \oplus K, K) \tag{1}$$

$$B = Rot(n_1 \oplus MIX(n_1', K), n_1 \oplus n_1' \oplus K) \tag{2}$$

where n_1, n', and $n_{1'}$ defined in Eqs. (3), (4) and (5) respectively

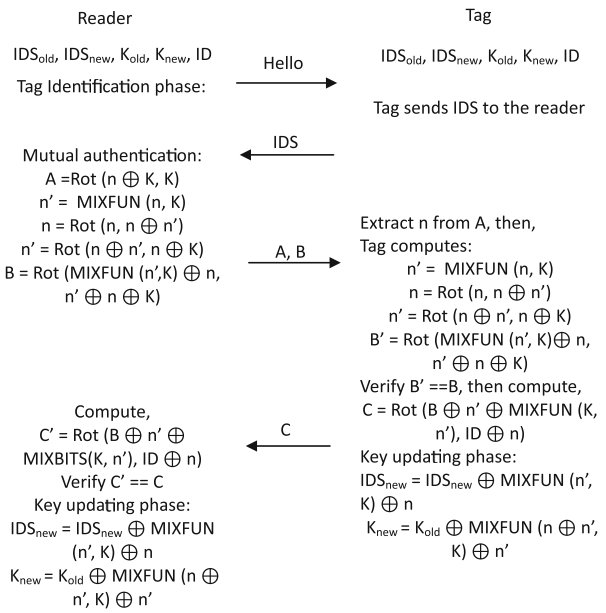

Fig. 2 Proposed authentication scheme for RFID system

Table 1 Notation used in this paper

Symbol	Meaning
IDS	Pseudo-random ID of the tag
ID	Unique identity of the tag
Rot (A, B)	Left rotate the value A by hamming distance of B
$\oplus$	Exclusive or operation
IDS_{new}, IDS_{old}	New and previous pseudo-random ID of the tag
K_{old}, K_{new}	shared key
MIX(A, B)	Function used in this protocol to enhanced security
n, n', n_1', n_1	96-Bit value generated during mutual authentication

$$n_1 = ROT(n, n \oplus n') \tag{3}$$

$$n' = MIX(n, K) \tag{4}$$

$$n_1' = Rot(n' \oplus n_1, K \oplus n_1) \tag{5}$$

2. If the reader cannot validate with IDS_{new}, then the reader match IDS with IDS_{old}, if it matches with IDS_{old}, then the reader computes A, B from K_{old} and a random number in (1) and (2). If both IDS_{new} and IDS_{old} do not match with IDS, then the reader terminates the current authentication session.
3. After receiving message packets A and B from the reader, the tag computes n from A as Eq. (6):

$$n = K \oplus Rot^{-1}(A, K) \tag{6}$$

Then, the tag validating the reader by computing B1 from n and K. If the tag cannot validate the reader, then tag terminates the session. Otherwise, the tag computes C from Eq. (7) and sends back to the reader.

$$C = Rot(B \oplus n_1 \oplus MIX(n_1', n_1 \oplus K), MIX(ID \oplus n_1, K)) \tag{7}$$

4. After receiving C from the tag, the reader computes C′ and matches with C. After the successful validation, the reader verifies the tag and mutual authentication takes place.

3.3 Pseudonyms and key updating phase

In this phase, After successful mutual authentication, both devices updates its key and IDS as Eqs. (8) and (9).

$$IDS_{new} = IDS_{old} \oplus MIX(n_1', K) \oplus n_1 \tag{8}$$

$$K_{new} = K_{old} \oplus MIX(n_1 \oplus n_1', K) \oplus n_1' \tag{9}$$

MIX Function: To computes MIX (X, K) function, there consists of two phases such as:

1. In the first phase, X′ is calculated such as X is left shift by a hamming distance of seed, where seed is calculated as X ⊕ K.
2. In the second phase, XOR the X and X′ to compute the MIX(X, K). The Eq. (10) describe the mathematically formula of the MIX function.

$$MIX(X, K) = X \oplus Rot(X, X \oplus K) \tag{10}$$

4 Security analysis

The paper analyzes this scheme in terms of functionality of protocol i.e., confidentiality, integrity, and mutual authentication.

4.1 Confidentiality

The shared key "K" and random number "n" is used to generate message packets A, B, C as represent in Eqs. (1), (2), (7). However, the shared key is stored in both the tag and reader and it cannot transmit over the communication channel. Also, the shared key (K) and IDS updating using random number "n" after every successful authentication. Therefore, it is difficult for an adversary to guess shared key (K) between tag and reader using eavesdrop message packets. Hence, this scheme provides data confidentiality.

4.2 Integrity

The transmitted packets A, B, C between tag and reader generate using the shared key K. However, the adversary eavesdrops message packets between communication networks. The adversary modifies these message packets A, or B. Hence, if the adversary modifies message packet A, and message packet B remain the same. Then, the adversary transmits A', B message packet to the tag, where A' is modifies message packet of A. The tag computes random number "n_{change}" from Eq. (11).

$$n_{change} = Rot(A', K) \oplus K \tag{11}$$

Therefore, the random number generated by the tag is different from the actual. After that the tag computes B from Eq. (2) with modify random number n_{change}. Due to this, the modify value of message packet B obtained as shown in Eq. (12)

$$\begin{aligned} B_{change} = & Rot(n_{1change} \oplus MIX(n'_{1change}, K), \\ & n_{1change} \oplus n'_{1change} \oplus K) \end{aligned} \tag{12}$$

The n'_{change}, $n_{1change}$ and $n'_{1change}$ computed from Eqs. (13)–(15)

$$n'_{change} = MIX(n_{change}, K) \tag{13}$$

$$n_{1change} = ROT(n_{change}, n_{change} \oplus n'_{change}) \tag{14}$$

$$n'_{1change} = Rot(n'_{change} \oplus n_{1change}, K \oplus n_1) \tag{15}$$

Hence, the tag computes B_{change} that is different from B. Similarly, if adversary change message packet "B" and message packet "A" remain the same. Then also, the tag computes B' that is also different from the original value. In both cases, the tag cannot verify alter message packets and terminates authentication sessions. So, this scheme provides the integrity of the message.

4.3 Mutual authentication

In mutual authentication, both genuine tag and reader authenticate each other. In this protocol, the tag or reader authenticates messages using shared key K_{old} or K_{new}, which generates only by the genuine reader or tag. The shared key cannot transmit over an insecure channel. Therefore, the adversary cannot compute a shared key using eavesdropping messages. Also, the tag validates the reader using the packet *B* and reader validates the tag using packet *c*. In both of the case, the message packet generates using the random number and shared key. Hence, this protocol ensures mutual authentication between RFID devices.

4.4 Resistance from replay attack

In the replay attack, the attacker eavesdrops original packets communicating between RFID devices. Then, the attacker uses these packets to unauthorized access to a communication network. In the proposed scheme, Key and IDS update after the successful mutual authentication. Therefore, the adversary tries to use old genuine packets, the tag tries to verify these packets with new IDS and new shared key. Hence, it discards these modifies packet. Thus, the attacker cannot able to unauthorized access using eavesdrops genuine packet. Therefore, this scheme provides security against a replay attack.

4.5 Resistance from disclosure attack

In the disclosure attack, the adversary guesses secret information such as shared key or identity (ID) of the tag. There are two types of disclosure attacks: full disclosure attack, identity disclosure attack. In full disclosure attack, the adversary computes all stored information of the tag. In an identity disclosure attack, the adversary computes only identity (ID) of the tag. The adversary cannot guess shared key or other information from eavesdropping values A, B,

C, IDS. Also, the combination of T operation (XOR, OR, AND operation) causes a tango attack. The scheme uses only rot and XOR function. So, a tango attack is not possible in this scheme. Hence, this scheme provides resistance from disclosure attacks.

4.6 Resistance from desynchronization attack

In the desynchronization attack, the adversary could disturb synchronization between tag and reader. To perform the desynchronization attack, the adversary eavesdrops "hello", IDS, A, B, C packets between communication channels. Then, the adversary modifies a single bit of A, ands then try to modify B up to when tag validates the reader. In this protocol, a single bit change in bit A, there will be a different value of B, and tag cannot verify the reader. Hence, this protocol provides security against a desynchronization attack.

4.7 Resistance from tracking attack

In tracking attack, the adversary finds the correct ID of the tag. The adversary can guess the correct tag ID if the adversary gives various tag ID of an RFID system. The primary focus of the adversary finds the correct ID of the tag. Juel and weis [21] proposed a model for tracking attack.

4.7.1 Juel and Weis model [21]

This model consists of "n" number of tags and a reader. This model is a challenge-response model in which the adversary modifies pseudonym number and shared key after the execution of the challenge-response model. This model consists of four types of queries that the adversary can use to perform tracking attacks such as execute query, send query, corrupt query, and test query.

- Execute query: In this execute query, the attacker eavesdrops packets between the tag (T) and reader (R) at session i.
- Send query: The adversary impersonates party P_1, where P_1 maybe tag or reader in ith session and sends message m to another party P_2.
- Corrupt query: It is a SetKey query in which the adversary assign a new arbitrary shared key to tag.
- Test query: The adversary is given randomly ID_{b1}, where b1 belongs {0, 1} from ID_0 and ID_1, if the adversary guesses correct tag ID_{b1}, then the adversary succeeds.

There are three phases to compute the identity of the tag, namely the learning phase, challenges phase, and guessing phase.

1. In the first phase, the adversary performs execute query to eavesdrop message packet between tag and reader.
2. The second phase, the challenger given two tags t_1 and t_2 with ID_1 and ID_2 to the adversary.
3. The third phase consists of guessing phase, the adversary guesses tag, and output is bit b1′ of the bit b1.

$$\begin{aligned} Adv_A^{UNT}(k) &= |Pr[A_{wins}] - Pr[random\ coin\ flip]| \\ Adv_A^{UNT}(k) &= |Pr[A_{wins}] - 1/2| \end{aligned} \tag{16}$$

In this challenges-Response model, the adversary wins the game if $Adv_A^{UNT}(k) > \in (k)$, where k is security parameter. In this scheme, the adversary can compute ID of the tag using message packets C as Eq. (7). Then, the probability of guessing correct identity of the tag:

$$Adv_A^{UNT}(k) = |[C' == C] - 1/2| = |1/2 - 1/2| = 0 \tag{17}$$

The advantage of the adversary to compute the identity of a tag is zero. So, the adversary cannot be able to compute the ID of the tag. Hence, this scheme provides security against the tracking attack.

5 Result and comparison

This section analyzes this scheme in terms of communication and storage costs with existing schemes. The MIX function uses XOR and ROT operations. This scheme analyzes in terms of storage cost, the communication cost of the tag for mutual authentication. The scheme uses XOR and ROT operation to mutual authenticate between tag and reader. The tag size 96-bit uses in the protocol. Each tag stores 96 bit length values i.e. IDS_{Old}, IDS_{new}, K_{new}, K_{old}, and ID. Therefore, the storage cost of the tag is 5L = 5 × 96 = 480 bits. During mutual authentication IDS, A, B, C message packets communicate between tag and reader. Hence, the communication cost for mutual authentication of scheme is 4L = 4 × 96 = 384 bits, Where L = 96, which is less than EMAP, RAPP. The tag transmits IDS, C message packets during authentication. So, the tag's communication cost in the scheme is 2L = 2 × 96 = 128 bits. The Table 2 shows the comparison of the various schemes like EMAP, LMAP, SASI, Gossamer, RAPP, Tewari et al. schemes with this scheme.

5.1 Limitation of the study

However, the attacker may transmit a large number of unauthorized message packets to the tag. After that, the tag tries validating these large number of message packets. Thus, the tag cannot be available to the legitimate user

Table 2 Analysis of various authentication schemes for RFID

Analysis	LMAP [20]	SASI [9]	Gossamer [13]	RAPP [15]	Tewari and Gupta [18]	Ours
Operation performed by the tag	+, OR, ⊕	ROT, +, OR, ⊕	MIXBITS, ROT, +, ⊕	PER, RoT, ⊕	ROT, ⊕	⊕, ROT
Communication cost	4L	4L	4L	5L	4L	4L
Storage cost	6L	7L	7L	5L	7L	5L
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes
Desynchronization attack	No	No	No	No	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes	Yes	Yes
Disclosure attack	No	No	Yes	Yes	No	Yes
Tracking attack	No	No	Yes	Yes	Yes	Yes

during this process. Therefore, the denial of service attack can be possible for this authentication scheme. Hence, it is also essential to develop a more secure authentication scheme for the RFID system.

6 Conclusion and future scope

In an RFID system, a passive tag consists of low power capacity. Hence, this paper proposed an ultra-lightweight mutual authentication scheme for a passive tag that uses XOR, ROT, and MIX operation to mutual authenticate between tag and reader. This scheme provides low communication and low memory for the passive tag. In the scheme, the "MIX" function uses to enhance the security of the protocol. The "MIX" function provides irreversibly and low complexity. This scheme requires small memory capacity and less communication between tag and reader. This scheme provides security against various attacks such as tracking, replay, disclosure, and desynchronization attack. Furthermore, it is developing a more secure authentication scheme with low power consumption and less computational cost.

References

1. Gartner (2015) Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. Accessed 23 Feb 2021
2. Greengard S (2015) Smart transportation networks drive gains. Commun ACM 58(1):25. https://doi.org/10.1145/2686742
3. Fang X, Misra S, Xue G, Yang D (2012) Smart grid—the new and improved power grid: a survey. IEEE Commun Surv Tutor 14(4):944. https://doi.org/10.1109/SURV.2011.101911.00087
4. Cocchia A (2014) In: Smart city. Springer, pp 13–43. https://doi.org/10.1007/978-3-319-06160-3_2
5. Ge M, Hong JB, Guttmann W, Kim DS (2017) A framework for automating security analysis of the internet of things. J Netw Comput Appl 83:12. https://doi.org/10.1016/j.jnca.2017.01.033
6. Luqman M, Faridi AR (2018) 2018 4th international conference on computing communication and automation, ICCCA 2018 83, p 326. https://doi.org/10.1109/CCAA.2018.8777560
7. Conti M, Dehghantanha A, Franke K, Watson S (2018). Internet of things security and forensics: challenges and opportunities. https://doi.org/10.1016/j.future.2017.07.060
8. Finkenzeller K, Handbook RFID (2010) Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. Wiley, New York. https://doi.org/10.1002/9780470665121
9. Chien HY (2007) SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Trans Depend Secure Comput 4(4):337. https://doi.org/10.1109/TDSC.2007.70226
10. Avoine G, Carpent X, Hernandez-Castro J (2016) Pitfalls in ultralightweight authentication protocol designs. IEEE Trans Mob Comput 15(9):2317. https://doi.org/10.1109/TMC.2015.2492553
11. Ahmadian Z, Salmasizadeh M, Aref MR (2013) Recursive linear and differential cryptanalysis of ultralightweight authentication protocols. IEEE Trans Inf Forensics Secur 8(7):1140. https://doi.org/10.1109/TIFS.2013.2263499
12. Peris-Lopez P, Hernandez-Castro JC, Tapiador JM, Ribagorda A (2009) In: Lecture notes in computer science, vol. 5379 LNCS. Springer, pp 56–68. https://doi.org/10.1007/978-3-642-00306-6_5
13. Bilal Z, Masood A, Kausar F (2009) In: NBiS 2009—12th international conference on network-based information systems. IEEE, pp 260–267. https://doi.org/10.1109/NBiS.2009.9
14. He D, Kumar N, Chilamkurti N, Lee JH (2014) Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. J Med Syst. https://doi.org/10.1007/s10916-014-0116-z
15. Gao L, Ma M, Shu Y, Wei Y (2014) An ultralightweight RFID authentication protocol with CRC and permutation. J Netw Comput Appl 41(1):37. https://doi.org/10.1016/j.jnca.2013.10.014
16. Ahmadian Z, Salmasizadeh M, Aref MR (2013) Desynchronization attack on RAPP ultralightweight authentication protocol. Inf Process Lett 113(7):205. https://doi.org/10.1016/j.ipl.2013.01.003
17. Chen Y, Chou JS (2015) ECC-based untraceable authentication for large-scale active-tag RFID systems. Electron Commer Res 15(1):97. https://doi.org/10.1007/s10660-014-9165-0
18. Tewari A, Gupta BB (2017) Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using

RFID tags. J Supercomput 73(3):1085. https://doi.org/10.1007/s11227-016-1849-x
19. Safkhani M, Bagheri N (2017) Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. J Supercomput 73(8):3579. https://doi.org/10.1007/s11227-017-1959-0
20. Peris-Lopez P, Hernandez-Castro JC, Estévez-Tapiador JM, Ribagorda A (2006) In: Proceedings of 2nd workshop on RFID security, p 06
21. Juels A, Weis SA (2009) Defining strong privacy for RFID. ACM Trans Inf Syst Secur 13(1):7. https://doi.org/10.1145/1609956.1609963