REVIEW ARTICLE

inventi Spreading Knowledge

A Survey of RFID Authentication Protocols

Mohammed Issam Younis[1*], Mustafa Hashim Abdulkareem[1]

Abstract: Security and privacy are significant issues in radio frequency identification (RFID) systems. There are many RFID authentication protocols have been proposed to address those issues. Some of these protocols employ way hashing function as a mechanism for addressing security and privacy issues of RFID systems, other protocols employ random number generator (RNG) and simple functions like cyclic redundancy code (CRC) functions as a mechanism for solving security and privacy problems and some proposals employ simple bitwise operations (e.g. XOR, AND, OR) for enhancing security and privacy of RFID systems. Although the proposed protocols have the capability to supply particular solution for RFID security and privacy issues, they cannot supply integrated solution. This paper is a survey to closely study those protocols in terms of their focus and limitations. In doing so, the security and privacy requirements are identified. Moreover, based on these requirements; 28 Secure RFID-based systems are discussed and compared in a form of checklist. Finally, this study is recommended to use heavy-weighted cryptographic techniques on the back-end side instead of lightweight cryptographic techniques to achieve the missed requirements on the studied authentication protocols.

INTRODUCTION

The RFID technology was first employed in the Second World War to recognize and differentiate between the aircraft of friend and foe. Later, in the 1970s, the US Department of Energy investigated the ability of RFID technology to protect materials at nuclear weapons locations. Recently, the RFID technology has been considered as the main driver of the future ubiquitous technology. It is also claimed as the core technology to realize internet of everything (IoE) environment where all the physical objects are connected anytime and anywhere. The RFID technology provides simplicity for an object to object (O2O) and people to object (P2O) communications. It is supposed that it will play an important role for future ubiquitous society, [1] as well as, in the Internet of Every Thing (IoE) era.

Generally, the RFID technology utilizes RF electromagnetic signals to communicate data between an RFID reader and RFID tags. Ordinarily, RFID tags are used for tracking and identifying what they are embedded into, such as a person, object or animal. Since the RFID tags are small, they can be attached to almost anything including money and clothing. Some RFID tags do not have batteries and they are known as "Passive Tags". The energy needed by the passive tag to send data is gained from the RF signals that are transmitted by the RFID reader. The passive tag receives the RF signal and uses its energy to send information. The passive tags have a sending range of a few meters. Other RFID tags have batteries and they are known as "Active Tags". The active tags can broadcast data at all times. They normally have a sending range of hundred meters. Unlike the barcode, RFID depends on RF signals; therefore, it does not need a line of sight to operate. Because of its low power requirements and flexibility, the RFID technology is a considerable method to connect the unconnected physical objects to an IoE solution by supplying data by an RFID tag to an RFID reader. The RFID tags can keep data about persons or physical objects to which they are attached, such as personal information, location tracking history, ownership and date of manufacture. [2] Based on the various industry areas that are featured in the reviewed literature, RFID technology is widely used in many areas such as transportation, access control, supply chain management, manufacturing, libraries, automobile security, healthcare, animal tracking, automatic payment, E-passports, etc.

Therefore, RFID related business experiences many significant advantages. [1] However, every technology has its problems. Security and privacy of RFID technology are very questionable since RFID is a wireless technology and is, therefore, subject to third-party interception unless the signal is secured. RFID systems need to be designed and implemented with adequate security and privacy protection in order to protect the data on the tag and the data transmitted between the tag and the reader to ensure it is accurate and safe from unauthorized access. [3] RFID authentication protocols are considered as a possible solution to secure RFID communications and address the security and privacy issues of RFID systems. [4] One of a growing area in RFID literature is authentication protocols which is deeply discussed in this paper.

The rest of this paper is organized as follows. In the next section, security and privacy issues of RFID systems are reviewed. In Section 3, the identified security and privacy issues are used to set security and privacy requirements. A comparative study of recent RFID authentication protocols is presented in Sections 4. Finally, Section 5 states the conclusion and gives the direction for future research.

SECURITY AND PRIVACY OF RFID SYSTEMS

RFID technology poses exclusive privacy and security concerns since it is a wireless technology and RFID tags can be detected from its range distance and its' contents can be read by anyone with an appropriately equipped RFID reader. [5] As a result, security and privacy issues are considered as the fundamental issue the RFID technology. [6, 7] This section investigates two classes of threats to RFID systems; namely: threats to security and privacy. The examined threats are taken from the existing literature.

Security

The communications between the RFID readers and tags through an insecure wireless communication channel are

[1]Computer Engineering Department, College of Engineering, University of Baghdad, Baghdad, Iraq.
E-mail: younismi@gmail.com
*Corresponding author

subjected to eavesdropping and unauthorized access. [8] Security threats feasible to RFID systems are discussed below:

1. Tag Cloning Attack

In this attack, an adversary creates a copy of an original (genuine) RFID tag. [9] The copied information of the genuine tag is stored into a new (fake) tag owned by the adversary to impersonate the genuine tag and gain the privileges of that tag. [10] The wide availability of rewritable (reprogrammable) RFID tags with rewritable tags' identifiers (IDs) makes the tags cloning feasible and simple. [11]

2. Tag Spoofing Attack

The tag spoofing is a variant of tags cloning that does not physically duplicate RFID tags. In this attack, an attacker impersonates a genuine RFID tag using RFID emulation devices to gain the privileges of the genuine tag. [11]

3. Replay Attack

In this attack, an attacker eavesdrops on the communications between an authorized RFID reader and a genuine RFID tag without being noticed and stores the messages exchanged between them. Later, the attacker can employ these messages and replay them to communicate with an authorized reader or a genuine tag. [12]

4. MitM Attack

In this attack, an adversary can manipulate messages exchanged between an authorized RFID reader and a genuine RFID tag by deletion, insertion or modification without being detected by the system. [8]

5. Desynchronization Attack

In this attack, the shared secret information between a genuine RFID tag and an authorized RFID reader or back-end server is made inconsistent by an adversary. Then, the RFID tag and reader cannot recognize each other in the future and the tag becomes disabled. [13]

Privacy

One of the principal considerations of users of RFID systems is the user privacy. Unprotected communications between an authorized RFID reader and a genuine RFID tag via an unsafe wireless channel may reveal sensitive user's data in the tag. [8]

SECURITY AND PRIVACY REQUIREMENTS

RFID systems should fulfill the following security and privacy requirements to address the security and privacy issues presented in previous section.

Data Confidentiality or Tag's Information Privacy

The confidentiality of an RFID system needs that all of the sensitive data is safely transmitted during all communications between the authorized RFID readers and genuine tags, so the exchanged data is accessed only by authorized entities. If the sensitive data is transmitted without encryption, an attacker can simply violate the privacy of the tag's owner by eavesdropping the communications between the RFID readers and tags and in this case, the confidentiality of the RFID system is breached. Therefore, to supply confidentiality, it is essential to encrypt the sensitive data, exchanged between the RFID readers and tags. In that way, only the authorized entities can access and understand that data. [14]

Resistance to Tags Cloning and Spoofing Attacks

An attacker should not be able to clone or spoof a genuine RFID tag.

Resistance to Replay Attack

An attacker should not have the ability to reuse messages transmitted between an authorized RFID reader and a genuine tag.

Resistance to MitM Attack

An attacker should not have the ability to manipulate messages exchanged between an authorized RFID reader and a genuine tag without detecting the unauthorized modifications by the system.

Resistance to Desynchronization Attack

An attacker should not be able to desynchronize the secret information shared between a genuine RFID tag and an authorized reader.

Data Origin Authentication

The data authentication or data origin authentication allows the receiver of transmitted data to verify its origin. [8]

Data Integrity

The integrity of an RFID system needs that all of the sent data between a genuine RFID tag and an authorized reader is correct and consistent. A breach of integrity takes place when information is inconsistent or incorrect. [15]

Non-Repudiation

The non-repudiation restrains an entity from repudiating having done an action or made a commitment by providing evidence about that action or commitment. [16]

COMPARATIVE STUDY OF RFID AUTHENTICATION PROTOCOLS

Every year, many RFID authentication protocols are proposed by researchers and published in the scientific literature to address the security and privacy threats. The authentication protocols are employed to achieve security and privacy requirements in RFID systems by supplying resistance against different attacks on RFID systems. Some of these protocols are appropriate for only one specific solution, other protocols are found to be incorrect and afterward corrected and lastly some proposals are insignificant and are later disregarded. [17]

With respect to computational capability (computational cost) of RFID tags, The RFID protocols can

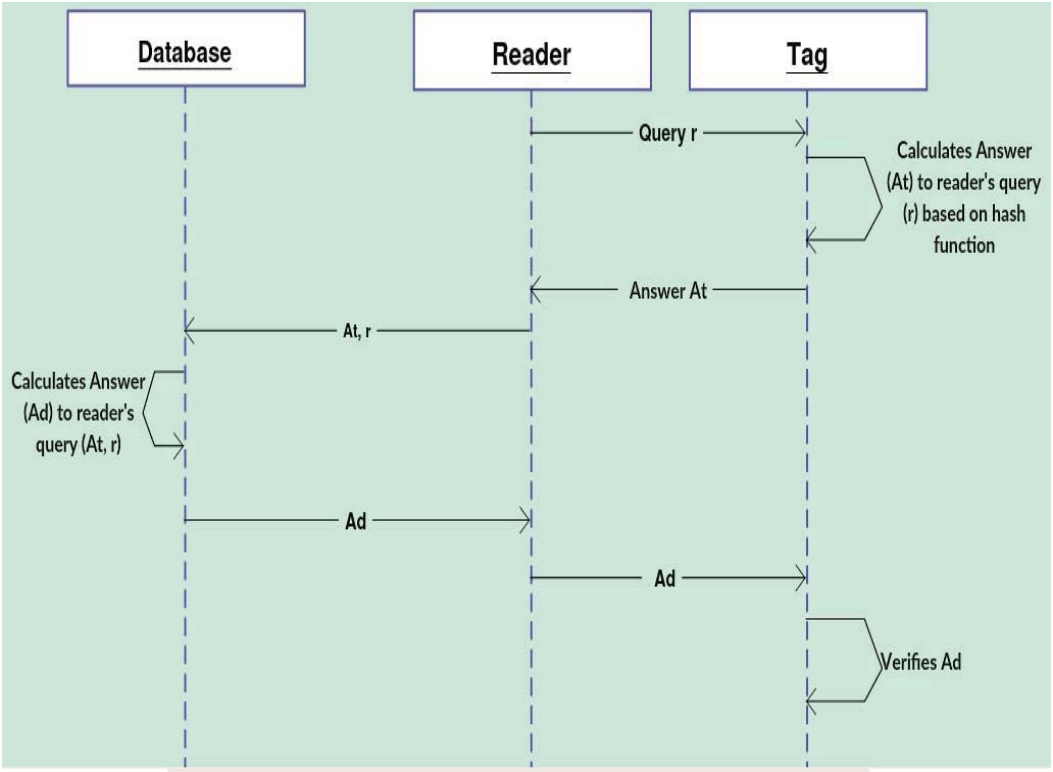

Figure 1: General scheme of hash-based RFID authentication protocols

be classified into three groups; namely: hash based authentication protocols, lightweight authentication protocols and ultra-lightweight authentication protocols.

Hash-Based Authentication Protocols

Several RFID authentication protocols employ one-way hashing function on RFID tags as a mechanism for improving security and privacy of RFID systems. Figure 1 shows the general scheme of hash-based RFID authentication protocols. Nine hash-based RFID authentication protocols are provided below.

Henrici and Muller [18] proposed a hash-based authentication protocol. This proposed protocol needs just a hashing function in the RFID tag and information management at the backend server. The proposed protocol is claimed appropriate to provide resistance against many attacks such as MitM, tag spoofing, tag cloning and replay attacks. Moreover, the communication channel between the RFID reader and tags does not have to be reliable and the third party/reader does not have to be trusted. However, the limitations of this protocol are that it does not give assurances to supply full security and privacy requirements. The proposed protocol is vulnerable to the desynchronization attack because the attacker can desynchronize the secret key, shared between the genuine tag and the authorized reader. [12] Another limitation is that the protocol is vulnerable to the replay attack because the tag's response does not rely on the reader's challenge, so an attacker may query a genuine tag and later replay the tag's response to an authorized reader when challenged thereby spoofing or cloning genuine tags. [12, 19] In addition, the proposed protocol does not provide data integrity, data origin authentication and non-repudiation.

Choi *et al*., [20] proposed One Way Hash-based Low-Cost Authentication Protocol (OHLCAP). The OHLCAP targets at protecting user privacy, particularly for the low-cost RFID systems in ubiquitous computing environments. The proposed protocol demands only one one-way hashing function. Leakage of information is claimed to be prevented in the OHLCAP since an RFID tag transmits its data only after the authentication. The OHLCAP is claimed to be safe against different attacks like tag spoofing, tag cloning and replay attacks. In addition, the OHLCAP protocol is secure against desynchronization attack since an adversary does not have the ability to authenticate to the back-end database without accessing to the secret value that is used for authentication. Yet, the OHLCAP protocol has several security weaknesses. An attacker can read sensitive information stored in a genuine tag by impersonating an authorized reader. [21] Moreover, an adversary can perform MitM attack by modifying the exchanged messages without detecting the unauthorized modifications by the system. [21] In addition, OHLCAP protocol does not provide data integrity, data origin authentication and non-repudiation.

Ha *et al*., [22] offered a strong security and low-cost RFID protocol. The aim of this protocol is to minimize the computational cost of both the tags and the back-end server in an RFID system. In addition, when a desynchronization happens because of attackers or a communication failure, the proposed protocol can recover the synchronization between the back-end database and the RFID tags in the next session. Moreover, the proposed protocol is claimed to supply robustness against the replay attack. However, although the protocol is claimed to supply tag spoofing/cloning resistance, the protocol is still suffered from these attacks. [23] In addition, it is possible to

desynchronize a genuine tag and an authorized reader by employing a MitM attack and forcing the RFID reader and tag to perform different updates to the shared secret key. [23, 24] Moreover, the authors [24] show that the way used by this protocol to recover the synchronization is deficient to prevent desynchronization attack. In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Osaka *et al*., [25] offered a hash-based RFID protocol. In their protocol, several security and privacy requirements are claimed to be achieved such as the replay attack resistance and spoofing and cloning attacks resistance. However, this protocol fails to overcome desynchronization attack since the attacker can desynchronize the secret key, shared between the genuine tag and the authorized reader, making future authentication impossible. [19] Another limitation is that this protocol is vulnerable to the MitM attack because an attacker can modify the exchanged messages without detecting the unauthorized modifications by the system. [19] In addition, the proposed protocol does not provide data integrity, data origin authentication and non-repudiation.

Song and Mitchell [26] proposed a hash-based RFID protocol. The target of the protocol is to supply security and privacy requirements by employing least storage and computational cost in an RFID tag. It needs less tag-side computational cost and storage capacity than other equivalently structured RFID protocols. The authors claim that the proposed protocol resists tag's information leakage, replay attack, spoofing and cloning attack. However, although the protocol is claimed to supply desynchronization resistance, the protocol is still suffered from this attack. [19, 23] In addition, the authors of this protocol claim that their protocol is robust to tag spoofing and cloning, but the authors [23] show its vulnerability to the spoofing and cloning attacks, since an attacker can collect the response messages transmitted by a genuine tag and modify the information and then resend the modified messages to an authorized RFID reader to masquerade as the legal tag. Moreover, an attacker that has no access to the information of a tag, has the capability to impersonate an authorized reader/server [27, 28] thereby reading sensitive information stored in a genuine tag. In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Liu and Bailey [29] introduced a privacy and authentication protocol (PAP) for passive RFID tags. The PAP protocol needs a passive RFID tag that saves a numeric value in which both RFID readers and tags are authenticated using the verification of results of the hashing function. The PAP protocol needs three requirements for each RFID tag. This includes the capability to perform a secure hashing function, the capability to compare two numeric values and the capability to produce a random number. The authors claim that the PAP protocol is both secure and efficient. Yet, the PAP protocol is weakly designed and it is vulnerable to replay spoofing and cloning attacks. [30] An adversary can spoof/clone a genuine tag by replaying answers sent by a legitimate RFID reader after eavesdropping on the ID of the target tag. [30] In addition, the PAP protocol does not supply data integrity, data origin authentication and non-repudiation.

Sadighian and Jalili [31] proposed a hash-based mutual RFID authentication protocol called Anonymous Forward-Secure Mutual Authentication Protocol (AFMAP). The authors claim that their protocol is provably secure and supplies some significant requirements like MitM attack resistance, cloning/spoofing resistance and replay attack resistance. Furthermore, they claim that their protocol provides the most improved security requirements in RFID mutual authentication protocols with respect to the user privacy. However, a desynchronization attack against the AFMAP protocol is presented [32] with small complexity. In addition, the AFMAP protocol does not supply data integrity, data origin authentication and non-repudiation.

Cho *et al*., [33] proposed a hash-based RFID mutual authentication protocol. The aim of this protocol is to address security issues and user privacy infringement in the RFID systems. The basic feature of the proposed protocol is the grouping of random numbers to protect tag data and supply data confidentiality, resulting in the acquisition of the random numbers by adversaries using eavesdropping or other means to access tag's data. In the proposed protocol, the tag executes one random number generation, four modular computations and two hashing computations. The authors of the protocol claim that it provides all the security and privacy requirements for the RFID systems. Yet, the proposed protocol is weakly designed and it is vulnerable to desynchronization, spoofing/cloning attacks. [34] Moreover, the proposed protocol is vulnerable to privacy violation since an attacker can impersonate an authorized reader, then read all information stored in a genuine tag. [34] In addition, the authors [35] show that the protocol is vulnerable to the replay attack. Moreover, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Srivastava *et al*., [36] introduced a hash-based RFID mutual authentication protocol for the medical sector. This protocol requires hashing operation with synchronized secret key shared between RFID tag and the back-end server. The protocol is claimed to supply resistance against different attacks like cloning, spoofing, replay, MitM and desynchronization attacks. Yet, the author [37] proposes a security evaluation which shows several security weaknesses in the protocol's design. He shows that the protocol is vulnerable to the privacy violation and spoofing/cloning attacks since the secrets shared between genuine tags and authorized readers can be revealed by an attacker, thereby passing the authentication protocol by the attacker who reveals the secret keys. Moreover, the proposed protocol is vulnerable to the desynchronization attack which forces the RFID tag and back-end server to be out of synchronization, so the back-end server no longer identifies the genuine tag. [37] In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

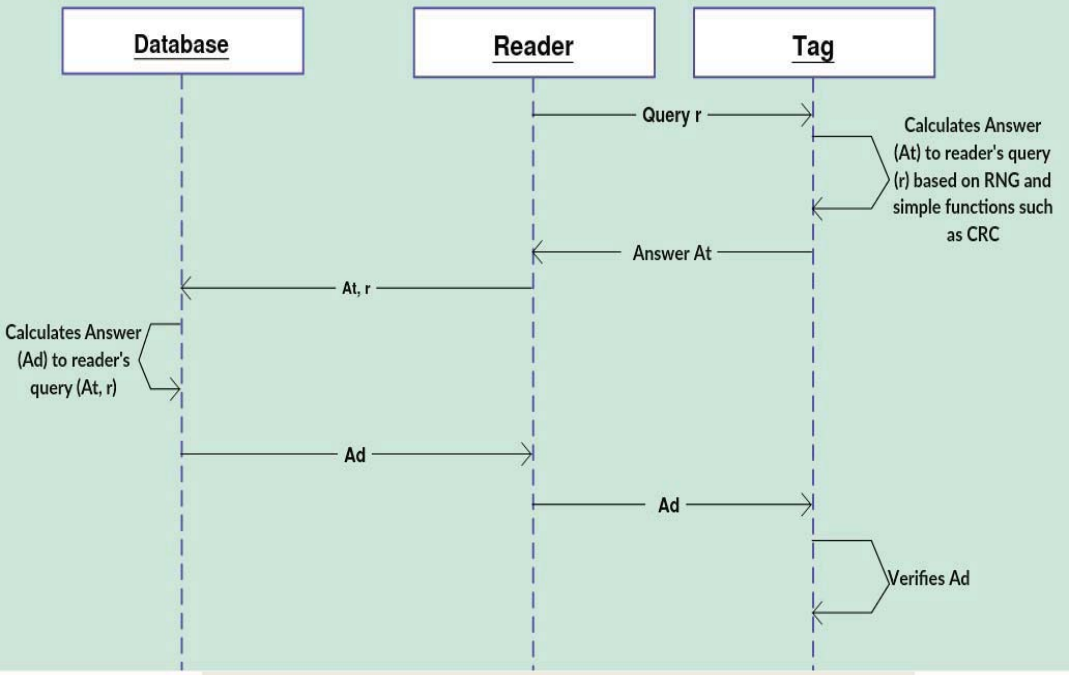

Figure 2: General scheme of lightweight authentication protocols

Lightweight Authentication Protocols

Several RFID authentication protocols employ random number generator (RNG) and simple functions like Cyclic Redundancy Code (CRC) functions as a mechanism for improving security and privacy of RFID systems. Figure 2 shows the general scheme of lightweight authentication protocols. Ten lightweight authentication protocols are listed below.

Kim *et al*., [38] proposed a lightweight privacy protection protocol appropriate to low-cost RFID tags. This protocol needs only approved capabilities of tags in EPCglobal Class 1 Generation 2 (C1G2) specification so it is appropriate to the application using EPCglobal C1G2. In the proposed protocol, the RFID tag employs XOR functions and 32-bit pseudo-random number generator PRNG. The authors claim that their protocol is secure against spoofing, cloning and replay attacks. However, while this protocol is claimed to provide replay resistance, it is still vulnerable to this attack since an attacker can perform a replay attack to impersonate an authorized reader. [19] Thereby, the attacker may use the replay attack to impersonate an authorized reader and read the information stored in a genuine tag, thereby violating the privacy of the tag. In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Chien and Huang [39] proposed a lightweight RFID authentication protocol. The target of the protocol is to enhance the security and performance of the RFID systems. By taking into account that cheap tags are very resource-limited, the tags only requires random number generation, Exclusive-OR (XOR), shifting and substring functions which are efficient and lightweight and they can simply be implemented on the cheap RFID tags. The authors claim that their protocol can resist the replay and desynchronization attacks. However, the proposed protocol fails to overcome replay spoofing and cloning attacks. [19] In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

NXP (formerly Philips) [40] proposed a three pass lightweight authentication protocol for low-cost RFID tags. This protocol requires just the abilities of "MIFARE Classic" tags which are manufactured by NXP. These tags are the most widely used contactless smart tags in the world. Their communication is based on the ISO 14443-A standard. [41] In the proposed protocol, the RFID tag employs only 32-bit PRNG. The proposed protocol provides resistance against the desynchronization attack, since it does not need to synchronize the secret keys shared between the genuine tags and authorized readers because the shared secret keys can be fixed and write-protected. [40] Thereby, the attackers cannot desynchronize the genuine tags and the authorized readers. In addition, the proposed protocol is scalable, since it does not need a database to identify and authenticate the RFID tags, so the identification time to a tag is O(1). However, the proposed protocol is vulnerable to spoofing and cloning attacks since an attacker can use a replay attack to spoof/clone a genuine tag. [41] In addition, the author [41] shows how to get the secret keys shared between the authorized readers and genuine tags. Given the secret keys, it would be simple to launch spoofing/cloning attack to spoof or clone a genuine tag. Moreover, an attacker can employ the disclosed keys to impersonate an authorized reader, then read information stored in a genuine tag, thereby violating the data confidentiality. In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Burmester and Medeiros [42] proposed a lightweight mutual authentication RFID protocol. The aim of this protocol is to supply security and privacy requirements and that conforms to the EPC C1G2 standard. The proposed protocol uses a strong Pseudo Random Function (PRF)

instead of a weak 16-bit RNG to provide the security requirements in the RFID systems. However, this protocol is vulnerable to desynchronization attack since the secret value, shared between the RFID tag and the back-end server, may be out of synchronization by only executing a series of challenge-response operations. [43] Moreover, an adversary can suitably use transmitted messages obtained in previous sessions to spoof/clone a genuine tag and communicate legally with a back-end server or authorized reader. [43] In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Qingling *et al*., [44] offered a lightweight authentication protocol which satisfies the lightweight requirements of the security of RFID systems based on the EPC C1G2 standard. The aim of the proposed protocol is to employ the constrained resources of low-cost RFID systems to implement encryption algorithm, decryption algorithm and mutual authentication between the RFID tags and readers. The proposed protocol uses a CRC function and bitwise operations to supply the security and privacy requirements. The authors claim that their protocol can effectively address the security and privacy issues of RFID systems based on EPC C1G2 standard. Yet, the proposed protocol is weakly designed since the security of the proposed protocol is incorrectly based on the assumption that CRC functions are one-way functions. [45] The proposed protocol is vulnerable to the spoofing/cloning attacks since an attacker may spoof or clone a genuine tag without requiring disclosing any secret parameters. [45] Moreover, an attacker can violate the confidentiality of tag's information by impersonating an authorized reader without requiring knowing any secret values of that target tag. [45] In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Sun and Ting [46] offered a lightweight authentication protocol based on C1G2 specification. It is a several-round protocol that uses PRNG and cyclic redundancy check tools to provide privacy and security requirements and resist different attacks. The proposed protocol uses no cryptographic function and hence, it is appropriate to cheap RFID tags. However, this protocol is vulnerable to replay, spoofing and cloning attacks since an attacker may eavesdrop on the communication between a genuine tag and a legitimate reader and extract the transmitted information. [12] Another limitation is that the proposed protocol is vulnerable to desynchronization attack. [12] In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Yeh *et al*., [47] proposed a lightweight mutual authentication protocol based on EPC C1G2 standard. The proposed protocol is claimed to be secure against different attacks and it can be used in environments with high security needs. Yet, the authors [48] show that the protocol is vulnerable to spoofing and cloning attacks since an adversary may easily obtain the secret parameters of genuine tags by eavesdropping the communications between the authorized readers and the genuine tags and carrying out some computations. In addition, the disclosure of secret values of the target tags makes the protocol also vulnerable to confidentiality violation since the attacker may employ the disclosed secret values to impersonate an authorized reader and read the information stored in the target tag. [48] Moreover, the proposed protocol is vulnerable to desynchronization attack. [48] In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Deng *et al*., [49] introduced a lightweight authentication protocol. The proposed protocol is appropriate to use in the low-cost RFID systems. The proposed protocol needs just the implementation of dot products of binary vectors and a random noise bit, so it is lightweight and appropriate to the cheap RFID tags with limited computation capability. The proposed protocol is claimed to resist the replay, spoofing and cloning attacks and supply data confidentiality. However, the authors [50] prove that the proposed protocol is not secure. They notice that this protocol has security and privacy vulnerabilities. They show how to get all the secret parameters shared between the authorized readers and genuine tags. Given all the secret parameters, it would be simple to launch spoofing/cloning attack to spoof or clone a genuine tag. Moreover, an attacker can employ the disclosed secret values to impersonate an authorized reader, then read information stored in a genuine tag, thereby violating the data confidentiality. In addition, an attacker may perform a MitM attack and cause desynchronization between an authorized reader and a genuine tag. [50] Moreover, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Niu *et al*., [51] introduced a lightweight authentication protocol that is compliant with the EPC C1G2 Version 2 standard. The proposed protocol needs only PRNG function and ultra-lightweight permutation operations. The employing of these simple operations adds a minimal level of computational cost and energy consumption while maintains the objectives of the proposed protocol. The protocol is claimed to resist the spoofing, cloning, replay, MitM and desynchronization attacks. Yet, the authors [52] show that it is feasible to reveal secret values in the protocol efficiently. Thereby, the attackers can use the disclosed secrets to spoof/clone a genuine tag. Moreover, the attackers can use the revealed secret values to impersonate an authorized reader, then read the information stored in a genuine tag, thereby violating the privacy of the tag. In addition, two different desynchronization attacks against the protocol are introduced. [52] Moreover, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Zhou [53] introduced a lightweight RFID protocol. The proposed protocol allows the private identification of RFID tags in the RFID systems with constant-time complexity based on quadratic residue and thereby it solves the issue of tag identification in extensive RFID system. The proposed protocol is appropriate to cheap passive RFID tags since it needs only passive tag abilities of modular

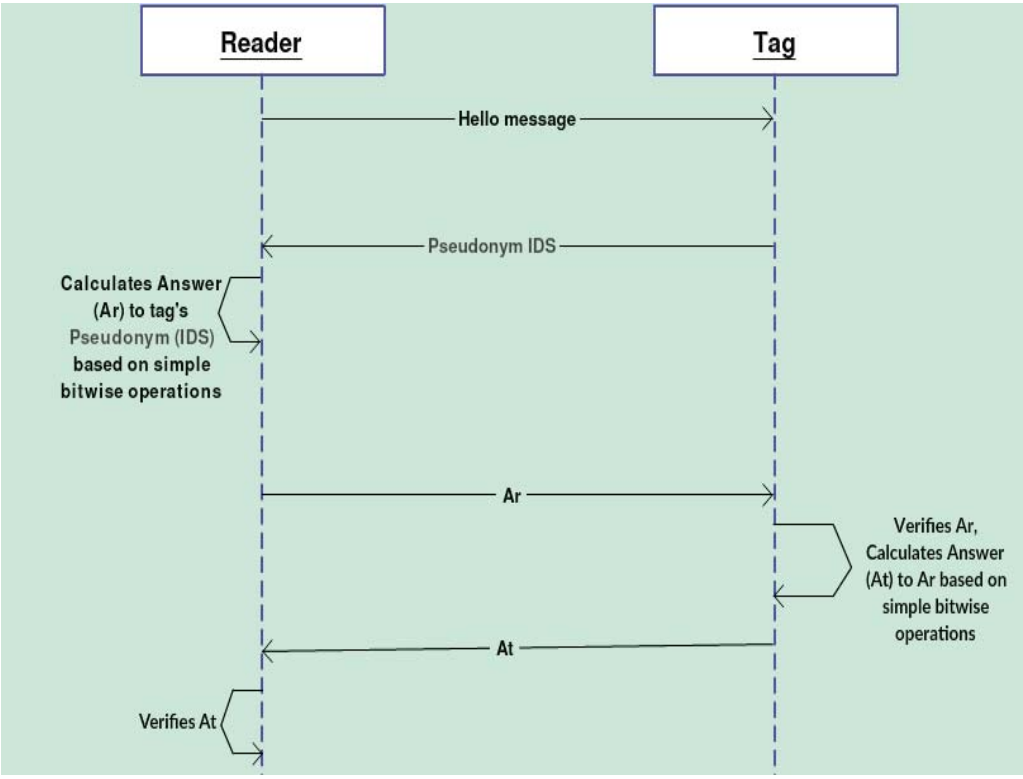

Figure 3: General scheme of ultralightweight authentication protocols

squaring and XOR function to supply security and privacy requirements and does not need implementation of hashing function on RFID tags or readers. However, the author [54] shows that the secret parameters of genuine tags may be exposed and an attacker can employ the exposed secrets to spoof or clone a genuine tag, thereby authenticating with the authorized RFID reader. [54] Moreover, an attacker may violate the confidentiality of tag's data by impersonating an authorized reader and reading the information stored in the target tag. [54] In addition, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Ultra-Lightweight Authentication Protocols

Other RFID authentication protocols employ simple bitwise operations (like XOR, AND, OR, etc.) on RFID tags as a mechanism for improving security and privacy of RFID systems. Figure 3 shows the general scheme of ultra lightweight authentication protocols. Nine ultra-lightweight authentication protocols are listed below.

Peris-Lopez *et al.*, [55] proposed an ultra-lightweight mutual authentication protocol that is appropriate to the low-cost tags. The proposed protocol is called Lightweight Mutual Authentication Protocol (LMAP) and it employs very lightweight operations like bitwise XOR ($\oplus$), bitwise OR ($\vee$), bitwise AND ($\wedge$) and addition mod (+). Heavy operations like multiplication operations and hash functions are not needed at all and the random number generation is only performed by the RFID reader. The authors claim that their protocol has the capability to avoid security and privacy issues and it supplies replay prevention, MitM attacks prevention and cloning/spoofing resistance. In addition, the tag identification by an authorized RFID reader does not need exhaustive search in the back-end server. However, LMAP protocol is suffered from desynchronization attack. [56] Moreover, the authors [56, 57] present attacks resulting the full break of LMAP protocol by disclosing the identification number of a target tag and all secret values shared by a genuine tag and an authorized reader after eavesdropping few authentication rounds of communications between the tag and the reader. Thereby, the attacker can successfully spoof/clone the target tag. In addition, the attacker can successfully violate the data confidentiality by impersonating an authorized reader, then reading all information stored in a target tag. Moreover, LMAP protocol does not supply data integrity, data origin authentication and non-repudiation.

Peris-Lopez *et al.*, [58] proposed an ultra-lightweight mutual authentication protocol called Minimalist Mutual Authentication Protocol (M2AP). The M2AP protocol is used for cheap RFID tags to provide a sufficient security level for particular RFID applications, which may be implemented even in the most restricted cheap RFID tags. The M2AP protocol employs ultra-lightweight functions like bitwise XOR ($\oplus$), bitwise OR ($\vee$) and bitwise AND ($\wedge$). Heavy-weighted operations like hash functions are not needed at all and the random number generation is only executed by the RFID reader. The authors claim that their protocol has the ability to avoid security and privacy problems and it achieves MitM attack prevention, resistance cloning and spoofing resistance. In addition, the tag identification by a legitimate RFID reader does not need exhaustive search in the back-end database. However the M2AP protocol is suffered from desynchronization attack. [56] In addition, the authors [59] introduce a constructive proof that M2AP protocol is weak and breakable. They

show that M2AP is vulnerable to confidentiality violation, spoofing and cloning attacks. Moreover, M2AP protocol does not supply data integrity, data origin authentication and non-repudiation.

Chien [60] offered an ultra-lightweight mutual authentication protocol. The proposed protocol is called Strong Authentication and Strong Integrity (SASI) protocol and its target is to achieve strong authentication and integrity protection of its transmissions and updated information. The SASI protocol needs only ultra-lightweight bitwise operations like AND, OR and left rotation on the RFID tags and it is claimed to resist different attacks like privacy violation, desynchronization and replay attacks. These characteristics make SASI protocol very attractive to the low-cost RFID systems. However, the authors [61-63] propose desynchronization attacks through which, an adversary may break the synchronization between a genuine tag and an authorized reader. In addition the authors [63] show that an adversary can disclose all secret parameters stored in a genuine tag. Thereby, the adversaries can employ the disclosed secrets to spoof/clone the genuine tag. Moreover, the adversaries can use the disclosed secret values to impersonate an authorized reader, thereby violating the data confidentiality by reading all information stored in a genuine tag. In addition, SASI protocol does not supply data integrity, data origin authentication and non-repudiation.

Li [64] proposed an RFID mutual authentication protocol using ultra-lightweight mathematic operations to provide secure RFID tag/reader authentication by employing only simple bitwise operations. The proposed protocol is called Lightweight Mutual Authentication Protocol++ (LMAP++) and it is aimed at supplying MitM attack resistance and cloning/spoofing resistance. Yet the authors [65] show that LMAP++ protocol suffers from a desynchronization attack. In addition, by employing the weakness of LMAP++ protocol structure and the property of simple bitwise operations, the authors [66] show that all the secret values may be disclosed by attackers after eavesdropping around 20 round authentication messages. Thereby, adversaries may employ the disclosed secret parameters to spoof/clone a genuine tag. Moreover, the adversaries can use the secrets to impersonate an authorized reader, thereby reading all information stored in a genuine tag and violating the data confidentiality of that tag. In addition, LMAP++ protocol does not supply data integrity, data origin authentication and non-repudiation.

Peris-Lopez *et al*., [67] introduced a protocol, called "Gossamer" protocol. The main target of this protocol is to supply sufficient security level, which can practically be implemented in the very low-cost RFID systems. The authors of this protocol claim that their protocol can achieve data confidentiality and supply desynchronization attack resistance by employing only ultra-lightweight bitwise operations like XOR, addition mod, left rotation and MixBits function on RFID tags. These bitwise operations are very low-cost and can be efficiently implemented in very cheap tags. However, the Gossamer protocol is vulnerable to desynchronization attack since the secret key, shared between a genuine tag and a back-end server may be out of synchronization by only carrying out a several challenge-response operations [43] or by replaying eavesdropped messages. [68] In addition, an attacker can spoof/clone a genuine tag even if he/she does not obtain the secret values of the genuine tag. [68] Moreover, Gossamer protocol does not supply data integrity, data origin authentication and non-repudiation.

Lee *et al*., [69] proposed an ultra-lightweight RFID authentication protocol. The proposed protocol needs only very lightweight bitwise operations; namely: XOR, AND, OR and rotate operations. The protocol is claimed to protect the user's privacy, prevent desynchronization attack and resist replay attack. Yet, the authors [70] show how an attacker can clone/spoof a genuine tag after obtaining the whole secret values stored in the genuine tag. Moreover, adversaries may employ the revealed secrets to impersonate an authorized reader, thereby violating the data confidentiality of a genuine tag by reading the whole information stored in the genuine tag. In addition, an attacker has the capability to desynchronize a genuine tag and an authorized reader. [70] Moreover, the proposed protocol does not supply data integrity, data origin authentication and non-repudiation.

Kianersi *et al*., [71] introduced an ultra-lightweight mutual authentication protocol. The propose protocol is called Secure Ultra Lightweight Mutual Authentication (SULMA) protocol and it is inspiring the Gossamer and SASI protocols. The aim of SULMA protocol is to achieve strong authentication and integrity of the RFID transmissions and of the updated information. The tag in SULMA needs only very lightweight functions like AND, OR, XOR and rotation functions. These characteristics make SULMA very suitable to the low-cost RFID systems. The authors of this protocol claim that it can resist desynchronization attack and it can achieve data confidentiality. However, SULMA protocol is vulnerable to confidentiality violation since an adversary can impersonate a legitimate reader, then read all information stored in a genuine tag by performing a replay attack. [72] In addition, the SULMA protocol does not supply data integrity, data origin authentication and non-repudiation.

Lee [73] proposed two ultra-lightweight authentication protocols for low-cost RFID systems. The first protocol is called Ultra-lightweight RFID Protocol with Dynamic Identity (DIDRFID) and the second one is called Ultra-lightweight RFID Protocol with Static Identity (SIDRFID). Both DIDRFID and SIDRFID protocols need low computational cost. Furthermore, the DIDRFID and SIDRFID protocols are claimed to supply data confidentiality and resistance against replay, spoofing, cloning and desynchronization attacks. However, the authors [74, 75] show that both DIDRFID and SIDRFID protocols are vulnerable to confidentiality violation and spoofing/cloning attacks after revealing the secret values of a genuine tag. In addition, an adversary can simply launch a desynchronization attack on "DIDRFID" Protocol and desynchronize a genuine tag and an authorized reader successfully after revealing the secret parameters. [75] In

Table 1: Comparison of All RFID Authentication Protocols

Implemented requirement (√) Not supported requirement (X)	Requirements								
RFID authentication protocols	**Desynchronization resistance**	**Spoofing/Cloning resistance**	**Replay attack resistance**	**MitM attack resistance**	**Data confidentiality**	**Non-repudiation**	**Data origin authentication**	**Data integrity**	**Computational cost**
Henrici-Muller [18]	x	x	x	x	x	x	x	x	Hash
OHLCAP [20]	√	√	x	x	x	x	x	x	Hash
Osaka [25]	x	√	x	x	√	x	x	x	Hash
Ha [22]	x	x	x	x	√	x	x	x	Hash
Song-Mitchell [26]	x	x	x	x	x	x	x	x	Hash
PAP [29]	√	x	x	√	√	x	x	x	Hash
AFMAP [31]	x	√	√	√	√	x	x	x	Hash
Cho [33]	x	x	x	x	x	x	x	x	Hash
Srivastava [36]	x	x	√	√	x	x	x	x	Hash
Chien-Huang [39]	√	x	x	√	√	x	x	x	PRNG
NXP [40]	√	x	x	x	x	x	x	x	PRNG
Kim [38]	√	√	x	√	x	x	x	x	PRNG
Sun-Ting [46]	x	x	x	√	√	x	x	x	PRNG
Niu [51]	x	x	x	x	x	x	x	x	PRNG
Burmester-Medeiros [42]	x	x	x	√	√	x	x	x	PRNG
Qingling [44]	√	x	x	x	x	x	x	x	PRNG
Yeh [47]	x	x	x	x	x	x	x	x	PRNG
Deng [49]	x	x	x	x	x	x	x	x	PRNG
Zhou [53]	√	x	x	x	x	x	x	x	PRNG
LMAP [55]	x	x	x	x	x	x	x	x	Bitwise Operations
M2AP [58]	x	x	x	x	x	x	x	x	Bitwise Operations
SASI [60]	x	x	x	x	x	x	x	x	Bitwise Operations
LMAP++ [64]	x	x	x	x	x	x	x	x	Bitwise Operations
Gossamer [67]	x	x	x	x	√	x	x	x	Bitwise Operations
Lee [69]	x	x	x	x	x	x	x	x	Bitwise Operations
SULMA [71]	√	√	x	x	x	x	x	x	Bitwise Operations
DIDRFID-SIDRFID [73]	x	x	x	x	x	x	x	x	Bitwise Operations
RAPP [76]	x	x	x	x	x	x	x	x	Bitwise Operations

addition, both DIDRFID and SIDRFID protocols do not supply data integrity, data origin authentication non-repudiation.

Tian *et al*., [76] (2012) offered an RFID Authentication Protocol with Permutation (RAPP). The RAPP protocol avoids using the "OR" and "AND" operations and introduces a new simple operation called "permutation". The tags in RAPP protocol only need three operations; namely: bitwise "XOR", left rotation and permutation operation. In addition, unlike other existing ultra-lightweight protocols, the last messages in RAPP protocol are transmitted by the RFID reader. The authors of this protocol claim that RAPP protocol achieves data confidentiality and integrity and resistance to the desynchronization attack since the last messages of the protocol are transmitted by an authorized reader and not by a genuine tag. However, the authors [77] present a replay attack which can lead to desynchronization between a genuine tag and a back-end server, which means that the genuine tag can no longer be authenticated by any legitimate reader. Moreover, the authors [78] show that the bad properties of the used permutation function may be employed by an attacker to reveal the secret parameters of genuine tags. Then, the adversaries can employ the revealed secret values to spoof/clone the genuine tags. Moreover, the adversaries can use the revealed secrets to impersonate an authorized reader, thereby violating the data confidentiality of genuine tags by reading all information of these tags. In addition, the RAPP protocol does not supply data integrity, data origin authentication and non-repudiation.

CONCLUSION

From the survey of the existing RFID authentication protocols; it is clear that all RFID protocols being studied are different in terms of the way of employing a method to improve the security and privacy of RFID systems but they focus on the same aim that is achieving better mechanisms against different attacks and providing security and privacy requirements. As tabulated in Table 1, while security and privacy problems can be solved, security and privacy requirements can be provided and implemented using RFID authentication protocols, other problems are arising and other requirements are missed and not implemented. Therefore, it can be concluded that the recent RFID authentication protocols failed to achieve integrated security and privacy requirements for RFID systems.

Based on the findings, we recommend future study in this area to focus on using heavy-weighted cryptographic techniques on the back-end server side instead of lightweight cryptographic techniques to achieve the missed requirements in the previous authentication protocols.

REFERENCES

1. Syamsuddin I, Dillon T, Chang E and Han S. A survey of RFID authentication protocols based on hash-chain method. Third International Conference on Convergence and Hybrid Information Technology, 2:559-564, 2008.
2. Chaouchi H. The internet of things: connecting objects. Wiley-ISTE, 2010.
3. Muhic I and Hodzic M. Internet of things: current technological review and new low power wireless sensor network protocol proposal. Southeast Europe Journal of Soft Computing, 3(2):46–57, 2014.
4. Bilal Z. Addressing security and privacy issues in low-cost RFID systems. PhD Thesis, University of London, England, 2015.
5. Yu D. Implementation of RFID technology in library systems case study: Turku City Library. Msc. Thesis, Lahti University of Applied Sciences, United Kingdom, 2011.
6. D Molnar and D Wagner. Privacy and security in library RFID issues, Practices and Architectures. ACM Conference on Computer and Communication Security, 2004.
7. S Han, T S Dhillon and E Chang. Anonymous mutual authentication protocol for RFID tag without back-end database. MSN, 4864:623-632, 2007.
8. Song B. RFID authentication protocols using symmetric cryptography. PhD Thesis, University of London, England, 2009.
9. Singh G, Kaur R and Sharma H. Various attacks and their countermeasure on all layers of RFID system. International Journal of Emerging Science and Engineering, 1(5):38–42, 2013.
10. Spruit M and Wester W. RFID Security and privacy: threats and countermeasures. Technical report UU-CS- 2013-001, Department of Information and Computing Sciences, Utrecht University, Netherlands, 2013.
11. Mitrokotsa A, Rieback M R and Tanenbaum A S. Classification of RFID Attacks. Journal of Information Systems Frontiers, 12(5):491–505, 2008.
12. Vahedi E, Ward R K and Blake I F. Security analysis and complexity comparison of some recent lightweight RFID protocols. Lecture Notes in Computer Science, 6694:92–99, 2011.
13. Habibi M H, Gardeshi M and Alaghband M R. Practical attacks on a RFID authentication protocol conforming to EPC C-1 G-2 standard. International Journal of UbiComp, 2(1):1–13, 2011.
14. Cho J, Yeo S and Kim S K. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer Communications, 34(3):391–397, 2011.
15. Schaberreiter T, Wieser C, Sanchez I, Riekki J and Roning J. An enumeration of RFID related threats. Second IEEE International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 381–389, October 2008.
16. Menezes A J, Oorschot P C and Vanstone S A. Handbook of Applied Cryptography. CRC Press, NY, 1997.
17. Yousuf Y and Potdar V. A survey of RFID authentication protocols. 22nd International Conference on Advanced Information Networking and Applications, 1346–1350, 2008.
18. Henrici D and Muller P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 149–153, 2004.
19. Deursen T and Radomirovic S. Attacks on RFID protocols. Cryptology ePrint Archive, Report 2008/310, 2008.
20. Choi E Y, Lee S M and Lee D H. Efficient RFID authentication protocol for ubiquitous computing environment. Lecture Notes in Computer Science, 3823:945–954, 2005.
21. Ha J, Moon S, Nieto J M G and Boyd C. Security analysis and enhancement of one-way hash based low-cost authentication protocol (OHLCAP). International Workshops on Emerging Technologies in Knowledge Discovery and Data Mining, 4819:574–583, 2007.
22. Ha J, Moon S, Nieto J M G and Boyd C. Low-cost and strong-security RFID authentication protocol. Lecture Notes in Computer Science, 4809:795–807, 2007.
23. Cao T and Shen P. Cryptanalysis of some RFID authentication protocols. Journal of Communications, 3(7):20–27, 2008.
24. Deursen T and Radomirovic S. Security of RFID protocols – A case study. Electronic Notes in Theoretical Computer Science, 244:41–52, 2009.
25. Osaka K, Takagi T, Yamazaki K and Takahashi O. An efficient and secure RFID security method with ownership transfer. IEEE International Conference on Computational Intelligence and Security, 4456:778–787, 2007.
26. Song B and Mitchell C J. RFID authentication protocol for low-cost tags. First ACM Conference on Wireless Network Security, 140–147, Alexandria, Virginia, USA, 2008.
27. Rizomiliotis P, Rekleitis E and Gritzalis S. Security analysis of the song-mitchell authentication protocol for low-cost RFID Tags. IEEE Communications Letters, 13(4):274–276, 2009.
28. Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, Li T and Li Y. Vulnerability analysis of RFID protocols for tag ownership transfer. Computer Networks, 54(9):1502–1508, 2010.
29. Liu A X and Bailey L A. PAP: A privacy and authentication protocol for passive RFID tags. Computer Communications, 32(7):1194–1199, 2009.
30. Naser M, Peris-Lopez P, Budiarto R and Alvarez B R. A Note on the security of PAP. Computer Communications, 34(18):2248–2249, 2011.
31. Sadighian A and Jalili R. AFMAP: Anonymous forward-secure mutual authentication protocols for RFID Systems. Third International Conference on Emerging Security Information, Systems and Technologies, 31–36, 2009.
32. Safkhani M, Naderi M and Bagheri N. Cryptanalysis of AFMAP. IEICE Electronics Express, 7(17):1240–1245, 2010.
33. Cho J, Jeong Y and Park S O. Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol. Computers & Mathematics with Applications, 69(1):58–65, 2012.
34. Safkhania M, Peris-Lopezb P, Hernandez-Castroc J and Bagherid N. Cryptanalysis of the Cho et al. Protocol: A Hash-Based RFID Tag Mutual Authentication Protocol. Journal of Computational and Applied Mathematics, 259(1):571–577, 2014.
35. Chang C, Chen W and Cheng T. A Secure RFID Mutual Authentication Protocol Conforming to EPC Class 1 Generation 2 Standard. Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 642–645, August 2014.
36. Srivastava K, Awasthi A K, Kaul S D and Mittal R C. A Hash Based Mutual RFID Tag Authentication Protocol in Telecare Medicine Information System. Journal of Medical Systems, 39(1):1–5, 2015.

37. Ozcanhan M H. Analysis of a recent hash based RFID authentication protocol intended for telecare medicine. International Research Journal of Engineering and Technology, 2(4):1520–1524, 2015.
38. Kim K H, Choi E Y, Lee S M and Lee D H. Secure EPCglobal Class-1 Gen-2 RFID system against security and privacy problems. Lecture Notes in Computer Science, 4277:362–371, 2006.
39. Chien H and Huang C. A Lightweight RFID Protocol Using Substring. Lecture Notes in Computer Science, 4808:422–431, 2007.
40. NXP Semiconductors. MIFARE Standard 4kByte Card IC Functional Specification, 2007.
41. Tan W H. Practical Attacks on the MIFARE Classic. MSc Thesis, Imperial College London, United Kingdom, 2009.
42. Burmester M and Medeiros B. The Security of EPC Gen2 Compliant RFID Protocols. Lecture Notes in Computer Science, 5037:490–506, 2008.
43. Yeh K and Lo N W. Improvement of two lightweight RFID authentication protocols. Information Assurance and Security Letters, 1:6–11, 2010.
44. Qingling C, Yiju Z, Yonghua W. A minimalist mutual authentication protocol for RFID System and BAN logic analysis. ISECS International Colloquium on Computing, Communication, Control and Management, 2:449–453, 2008.
45. Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, Li T and van der Lubbe J C A. Weaknesses in two recent lightweight RFID authentication protocols. Lecture Notes in Computer Science, 6151:383–392, 2010.
46. Sun H and Ting W. A Gen2-Based RFID Authentication protocol for security and privacy. IEEE Transactions on Mobile Computing, 8(8):1052–1062, 2009.
47. Yeh T, Wang Y, Kuo T and Wang S. Securing RFID systems conforming to EPC class 1 generation 2 standard. Expert Systems with Applications, 8(12):7678–7683, 2010.
48. Habibi M H, Alagheband M R and Aref M R. Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard. Lecture Notes in Computer Science, 6633:254–263, 2010.
49. Deng G, Li H, Zhang Y and Wang J. Tree-LSHB+: An LPN-Based lightweight mutual authentication RFID protocol. Wireless Personal Communications, 72(1):159–174, 2013.
50. Qian X, Liu X, Yang S and Zuo C. Security and privacy analysis of tree-LSHB+ Protocol. Wireless Personal Communications, 77(4):3125–3141, 2014.
51. Niu H, Taqieddin E and Jagannathan S. EPC Gen2v2 RFID standard authentication and ownership management protocol. IEEE Transactions on Mobile Computing, 15(1):137–149, 2015.
52. Bagheri N, Safkhani M and Jannati H. Security analysis of Niu et al. authentication and ownership management protocol. Cryptology ePrint Archive, Report 2015/615, 2015.
53. Zhou J. A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification. Journal of Communications, 10(2):117–123, 2015.
54. Ozcanhan M H. Analysis of a recent quadratic residue based authentication protocol for low-cost RFID tags. International Journal of Novel Research in Engineering and Science, 2(1):7–13, 2015.
55. Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M and Ribagorda A. LMAP: A real lightweight mutual authentication protocol for low-Cost RFID tags. Second Workshop on RFID Security, July 2006.
56. Li T and Wang G. Security analysis of two ultra-lightweight RFID authentication protocols. IFIP International Federation for Information Processing, 232:109–120, 2007.
57. Barasz M, Boros B, Ligeti P, Loja K and Nagy D A. Breaking LMAP. Workshop on RFID Security, July 2007.
58. Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M and Ribagorda A. M2AP: A minimalist mutual-authentication protocol for low-cost RFID Tags. Lecture Notes in Computer Science, 4159:912–923, 2006.
59. Barasz M, Boros B, Ligeti P, Loja K and Nagy D A. Passive attack against the M2AP mutual authentication protocol for RFID Tags. First International EURASIP Workshop on RFID Technology, Vienna, Austria, September 2007.
60. Chien H. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Transactions on Dependable and Secure Computing, 4(4):337–340, 2007.
61. Cao T, Bertino E and Lei H. Security analysis of the SASI protocol. IEEE Transactions on Dependable and Secure Computing, 6(1):73–77, 2009.
62. Sun H, Ting W and Wang K. On the security of chien's ultralightweight RFID authentication protocol. Cryptology ePrint Archive, Report 2008/083, 2008.
63. D'Arco P and De Santis A. From weaknesses to secret disclosure in a recent ultra-lightweight RFID authentication protocol. Cryptology ePrint Archive, Report 2008/470, 2008.
64. Li T. Employing lightweight primitives on low-cost RFID tags for authentication. IEEE Vehicular Technology Conference, 1–5, September 2008.
65. Bagheri N, Safkhani M, Naderi M and Sanadhya S K. Security analysis of LMAP++, an RFID authentication protocol. International Conference for Internet Technology and Secured Transactions, 689–694, December 2011.
66. Shao-hui W, Sujuan L and Danwei C. Efficient passive full-disclosure Attack on RFID lightweight authentication protocols LMAP++ and SUAP. Indonesian Journal of Electrical Engineering and Computer Science, 10(6):1458–1464, 2012.
67. Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M and Ribagorda A. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer Protocol. Lecture Notes in Computer Science, 5379:56–68, 2009.
68. Bilal Z, Masood A and Kausar F. Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID Tags: Gossamer Protocol. International Conference on Network-Based Information Systems, 260–267, August 2009.
69. Lee Y, Hsieh Y, You P and Chen T. A new ultralightweight RFID protocol with mutual authentication. WASE International Conference on Information Engineering, 2:58–61, 2009.
70. Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, Li T and Van der Lubbe J C A. Security flaws in a recent ultralightweight RFID protocol. Workshop on RFID Security, Cryptology and Information Security Series, 4:83–94, 2010.
71. Kianersi M, Gardeshi M and Arjmand M. SULMA: A secure ultra light-weight mutual authentication protocol for low cost RFID tags. International Journal of Ubi Comp, 2(2):17–24, 2011.
72. Azizi M and Bagheri N. Cryptanalysis of SULMA, an ultralightweight mutual authentication protocol for low-cost RFID Tags. International Journal of Ubi Comp, 2(4):15–25, 2011.
73. Lee Y. Two ultralightweight authentication protocols for low-cost RFID Tags. Applied Mathematics and Information Sciences, 6:425–431, 2012.
74. Bilal Z, Martin K and Saeed Q. Multiple attacks on authentication protocols for low-Cost RFID Tags. Applied Mathematics and Information Sciences, 9(2):561–569, 2015.
75. Farzaneh Y, Azizi M, Dehkordi M and Mirghadri A. Vulnerability analysis of two ultra lightweight RFID authentication protocols. The International Arab Journal of Information Technology, 12(4):340–345, 2015.

76. Tian Y. A new ultralightweight RFID authentication protocol with permutation. IEEE Communications Letters, 16(5):702–705, 2012.
77. Zhuang X, Wang Z, Chang C and Zhu Y. Security analysis of a new ultra-lightweight RFID protocol and its improvement. Journal of Information Hiding and Multimedia Signal Processing, 4(3):166–177, 2013.
78. Bagheri N, Safkhani M, Peris-Lopez P and Tapiador J E. Weaknesses in a new ultralightweight RFID authentication protocol with permutation—RAPP. Security and Communication Networks, 7(6):945–949, 2014.

Cite this article as: Mohammed Issam Younis, Mustafa Hashim Abdulkareem. A Survey of RFID Authentication Protocols. Inventi Impact: Information Security, 2017(1):1-12, 2017.