Wireless Networks
https://doi.org/10.1007/s11276-017-1638-3

Review of different classes of RFID authentication protocols

Alaauldin Ibrahim[1] · Gokhan Dalkılıc[1]

Abstract
Radio-frequency identification (RFID) is an up-and-coming technology. The major limitations of RFID technology are security and privacy concerns. Many methods, including encryption, authentication and hardware techniques, have been presented to overcome security and privacy problems. This paper focuses on authentication protocols. The combination of RFID technology being popular but unsecure has led to an influx of mutual authentication protocols. Authentication protocols are classified as being fully fledged, simple, lightweight or ultra-lightweight. Since 2002, much important research and many protocols have been presented, with some of the protocols requiring further development. The present paper reviews in detail recently proposed RFID mutual authentication protocols, according to the classes of the authentication protocols. The protocols were compared mainly in terms of security, the technique that they are based on, protocols that the presented protocol has been compared with, and finally, the method of verifying the protocol. Important points of the comparisons were collected in two tables.

Keywords Authentication protocols · Radio-frequency identification · Radio-frequency identification attacks · Radio-frequency identification authentication protocols

1 Introduction

Radio-frequency identification (RFID) is being developed to distinguish the correct object with a small tag. This technology has been considered as one of the most substantial technologies of these decades [1]. RFID systems consist of a tag, a tag reader and a back-end database server. The reader reads the RFID tag's identifier and sends the queried identity to the back end server. The information obtained from the tag is mostly an index to a back end database.

The tags are classified into three types according to how they are powered: active, semi-active and passive tags. Active RFID tags need internal batteries to power the electronic components and to create a reply signal to the reader. Semi-active tags or in other words semi-passive use batteries only for powering microchip's circuit and they harvest energy to create a reply signal to the reader by using reader's radio signal. Passive tags harvest their energy from the reader. RFID tags are also grouped into three basic frequency ranges: low frequency (125–134 kHz), high frequency (13.56 MHz) and ultra-high frequency (860–960 MHz) ranges [2]. Passive (low-cost) RFID tags that operate in ultra-high-frequency bands have allowed innovation in several fields of daily application, such as building access control, supply chain management and goods tracking. The Electronic Product Code (EPC) Class1 (C1) Generation2 (Gen2) standard is an example of passive RFID technology [3].

Some experts believe that optical barcodes will be replaced with low-cost RFID tags attached to consumer items [4]. However, owing to the wireless nature of communication between the tag and reader, this technology has major security and privacy threats. Mutual authentication protocols are generally used to overcome security attacks between the reader and tags. Since 2002, much research has been conducted and numerous protocols are proposed but some of these still need to be developed further.

In the proceeding sections, Sect. 2 discusses and explains authentication protocols and their goals. Section 3

✉ Alaauldin Ibrahim
devletaladdin@gmail.com

Gokhan Dalkılıc
dalkilic@cs.deu.edu.tr

[1] Computer Engineering Department, Dokuz Eylul University, Izmir 35160, Turkey

Published online: 30 December 2017

examines and compares protocols according to their class. Section 4 evaluates the comparison. Section 5 presents conclusions drawn from the review of authentication protocols.

2 Authentication protocols

Lopez et al. [5] presented many solutions to overcome the security issues and risks associated with the RFID systems. In this study, we aimed to deepen on authentication protocols. Authentication is the first step in defending against wireless attacks on RFID systems. Once the server validates the identity of the RFID tag, it begins trusting the tag. After authentication, the reader can access the contents of the authenticated tags.

2.1 Classes of authentication protocols

Chein [6] stated that authentication protocols are divided into four classes with accordance to the tag's computational cost and supported operations.

- Fully fledged protocols: Protocols that support symmetric and asymmetric encryption, and a one-way function. Examples are in [7, 8].
- Simple protocols: Protocols that support hash function and random number generator (RNG). Examples of this class are given in [9, 10].
- Lightweight protocols: Protocols that support cyclic redundancy check (CRC) and RNG. Examples are given in [11–14].
- Ultra-lightweight protocols: Protocols that are tailored specially to extremely constrained devices. These protocols involve only simple bitwise operations (like AND, OR, XOR) on tags. Examples are given in [15, 16].

2.2 Goals of authentication protocols

Considering the variety of potential threats, an authentication protocol, whatever the class, should address all or most of the following security threats and services.

Security threats

- Tracking attack: The attacker can track information linked to a given tag.
- Denial-of-service (DoS) attack: It is attempting to crash tags by having malicious readers overload them with more data than they can handle.
- Desynchronization attack: The attacker desynchronizes the reader and tag.
- Man-in-the-middle attack: It is taking control of the message flow.
- Impersonation attack: The attacker forges an authenticated tag and acts as a valid tag.
- Cloning attack: The attacker fools the reader into believing that it receives data from a legitimate tag.
- Full-disclosure attack: The attacker compromises all secret information of the tag.
- Eavesdropping: The attacker eavesdrops on the communication channel.
- Replay attack: The originator or attacker intercepts and retransmits data, possibly as part of a masquerade attack by packet substitution.

Security services

- Mutual authentication: Property that both the tag and server are authenticated to each other.
- Confidentiality: Property that all secret information is securely transmitted.
- Availability: Property that authenticating parties are always available to communicate.
- Forward/backward security: Property that an attacker cannot compromise the previous/current confidential information even if it obtains the current/previous confidential information.
- Ownership transferable: Property that the privacy of the present and new owners is not violated when the existing owner passes necessary data to the new owner.
- Tag anonymity: Property that the attacker cannot trace a tag by listening to the channel.
- Traceability: The tag holder can be traced by using the location privacy information stored in the tag.
- Location privacy: Property that the attacker cannot judge the tracking object from the information of a tag.
- Information privacy: Property that only the legitimate reader can access the information stored in the tag.

3 Examination and comparisons of authentication protocols

Unlike the study of Soos [17] where protocols are categorized according to the services provided and the employed algorithms, this section presents 22 recently proposed RFID authentication protocols with respect to their class; some protocols are examined and explained in detail while others are given in tables because of space limitations. The first column of Table 1 lists the 22 protocols in terms of their class starting from fully fledged protocols and ending with ultra-lightweight protocols. The second column gives the function that the protocol is based on. The third column gives the verification tool used for the

Table 1 Techniques, verifications and classes of authentication protocols (*P* protocol, *C* class, *F* fully fledged, *S* simple, *L* lightweight, *UL* ultra-lightweight)

P	Function based on	Verificated by	EPC	Compared with	C
[31]	ECC	…	X	[27, 28, 30]	F
[37]	Public key cryptography	BAN logic	X	[38–42]	F
[32]	ECC	Random oracle model	X	[25, 28, 30, 43]	F
[33]	ECC & AES	Tested and realized on real devices	X	[25, 28–30]	F
[44]	Increasing key space using nonces	AVISPA	X	[45–47]	F
[48]	Cryptographically supported NFC tags in Medication	Manually as in [49]	X	[49]	F
[50]	One-way hash function and semi randomized encryption keys	Manually as in [51]	X	[9, 10, 36, 51, 52]	F
[53]	Hash based	….	X	[36, 51, 54]	S
[55]	Hash based	Manually	X	[6, 56–61]	S
[62]	Hash and PRNG based	GNY logic [63]	√	[64–66]	S
[67]	Constant-time complexity	Byzantine adversarial model [52]	X	[68]	S
[69]	Hash operation & RNG	GNY logic [63]	X	[10, 70–75]	S
[76]	One-way Hash Function	GNY logic [63]	X	[10, 77, 78]	S
[79]	XOR, PRNG and CRC based	Manually	√	[42, 80]	L
[81]	XOR and PRNG based	Manually as [82]	√	[83–86]	L
[87]	Fast tag indexing, CRC & PRNG	A Simulation Program	√	[10, 73, 77, 88–91]	L
[92]	Learning parity with noise	Manually as in [93]	√	[93–96]	L
[97]	A Pseudo Random Generator Shared Between Readers and Tags	AVISPA	√	[98–103]	L
[104]	CRC and permutation	Simple Promela Interpreter (SPIN)	√	[6, 38, 56, 105]	L
[106]	A security ultralightweight bitwise conversion	Manually	√	[6, 38, 57, 58, 64, 105, 107]	UL
[108]	XOR bitwise rotation based	Manually	√	[6, 38, 56–58, 105]	UL
[109]	Physically Uncloneable Functions PUF	…	√	[110–112]	UL

authentication. The EPC column lists whether the protocol is compatible with EPC Gen2. The 'compared with' column lists the other protocols that the protocol is compared with. The last column gives the class of the authentication protocol. The protocols comparison in terms of security threats and security services in Table 2. Whilst, Table 3 presents the examined paper names and publishing year along with their references.

3.1 Fully fledged protocols

The fully fledged class involves cryptographic algorithms that are divided mainly into two groups: symmetric algorithms and asymmetric algorithms. Asymmetric algorithms based on elliptic curve cryptography (ECC) are strong in terms of security and the services they provide. Compared with the Rivest–Shamir–Adleman (RSA) scheme, ECC-based systems are smaller, faster and consume less power. Hereby, for resource constrained systems, the ECC-based algorithm is a better choice than the RSA algorithm. It is noted that the RSA scheme has an ECC-based variant. Many ECC-based authentication protocols have thus been proposed to satisfy severely constrained tags.

In 2006, Tuyls et al. [7], using the Schnorr identification protocol, proposed an ECC-based RFID identification protocol. They asserted that the protocol is resistant against tag counterfeiting. However, in 2008, Lee et al. [18] showed that the Tuyls et al.'s protocol is defenseless against a location tracking, does not insure forward security nor mutual authentication and lacks scalability. In 2007, Batina et al. [19], based on Okamoto's authentication protocol, proposed an RFID identification protocol based on ECC and mentioned their proposal could avoid active attacks. Yet, Lee et al. [18] stated that the protocol is vulnerable in terms of forward security and location tracking attack and lacks scalability. Lee et al. [18] claimed to have solved these three issues, but studies published in 2008 [20, 21] showed that the Lee et al.'s proposal is defenseless against tracking and forgery attacks and does not provide mutual authentication.

Table 2 Comparison of authentication protocols in terms of security threats and security services (*F* fully fledged, *S* simple, *L* lightweight, *UL* ultra-lightweight)

Protocol	31	37	32	33	44	48	50	53	55	62	67	69	76	79	81	87	92	97	104	106	108	109
Security threats																						
Tracking attack				√			√		√		√	√		√					√	√		
DoS	√	√		√	√	√	√						√	√			√		√			√
De-synchronize	√	√		√	√	√	√	√	√		√	√			√	√	√			√		
Man-in-the-middle	√	√	√	√	√	√	√	√							√		√				√	
Impersonation attack	√		√	√		√	√		√	√		√		√	√		√					√
Cloning attack	√			√		√			√			√	√	√		√						
Full disclosure attack				√		√			√										√	√	√	
Eaves dropping		√		√				√									√	√				
Replay attack	√	√	√	√	√	√		√		√	√	√	√	√	√	√	√		√		√	√
Security services																						
Mutual authentication	√	√	√	√	√	√	√	√			√		√	√	√			√			√	√
Confidentiality	√	√		√	√	√	√			√		√					√		√		√	
Availability	√			√																		
Forward security	√	√	√	√		√	√		√	√	√	√		√		√		√				
Backward security			√	√						√	√					√		√				√
Ownership transferable											√											
Tag anonymity	√			√																	√	
Traceability	√	√	√	√		√		√		√	√	√										
Location privacy			√	√			√									√						√
Information privacy	√			√			√									√		√				
Class																						
Class	F	F	F	F	F	F	F	S	S	S	S	S	S	L	L	L	L	L	L	UL	UL	UL

In 2009, by reconstructing the three components of elliptic curve discrete logarithm problem based randomized access control (EC-RAC) [18]; transfer schemes for secure ID and the secure password, and the server's authentication according to the system requirements and security properties, Lee et al. [22] proposed 6 different protocols to minimize the computation amount on tags.

In 2010, Lee et al. [23] came up with an ECC-based authentication protocol that addressed the existing tracking problems for the protocols presented in [7, 19]. This scheme considers only tag to reader identification and excludes reader to tag authentication. In 2011, Zhang et al. [24] proposed a randomized key protocol based on ECC that is an improvement on the schemes of Lee et al. and Tuyls et al. This protocol is safe against some relevant attacks, but still does not provide mutual authentication.

In 2014, to achieve mutual authentication, Liao et al. [25] proposed a secure authentication protocol based on the strength of ECC with an ID-verifier transfer protocol. However, studies [26–28] showed that the Liao et al.'s proposal suffers from security flaws and lacks performance efficiency. Later in the same year, using ECC, Chou [29] proposed an authentication protocol and informed that their proposal can resist different attacks. Nevertheless, Zhang and Qi [30] showed that Chou's proposal faces problems in terms of tag information privacy and backward and forward traceability. Then, in 2015, Jin et al. [31] suggested a secure mutual authentication protocol for healthcare environments based on ECC and asserted that their proposal can resist different attacks and performs better than schemes presented in [27, 28, 30].

In 2016, Farash et al. [32] showed that Zhang et al.'s [30] scheme does not provide forward privacy. Very recently, in 2017, Ibrahim et al. [33], proposed a strong and powerful mutual authentication protocol based on ECC and proven on the last revision of the wireless identification and sensing platform (WISP5). In the proposal, mutual authentication is proceeded in only two steps and withstands almost all common attacks and fulfills the RFID systems' security requirements.

Asymmetric algorithms are not the only choice for RFID systems because they are time consuming. Moreover, their implementation to RFID systems remains considerably challenging. Some researchers have thus directed their attention towards symmetric schemes, which are divided mainly into two groups: block ciphers and stream ciphers.

Table 3 Examined protocols' reference numbers and names

Refs.	Paper name and publishing year
[31]	A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography (2015)
[37]	A novel mutual RFID authentication protocol with low complexity and high security (2014)
[32]	A provably secure RFID authentication protocol based on elliptic curve for healthcare environments (2016)
[33]	An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for RFID, proven on WISP (2017)
[44]	Increasing key space at little extra cost in RFID authentications (2014)
[48]	Cryptographically supported NFC tags in medication for better inpatient safety (2014)
[50]	HPAP: A novel authentication scheme for RFID systems (2013)
[53]	A hash based mutual RFID tag authentication protocol in telecare medicine information system (2015)
[55]	An efficient RFID authentication protocol providing strong privacy and security (2016)
[62]	Cryptanalysis of the LMAP protocol: A low-cost RFID authentication protocol. (2017)
[67]	An efficient and private RFID authentication protocol supporting ownership transfer (2013)
[69]	RSEL: revocable secure efficient lightweight RFID authentication scheme (2014)
[76]	An one-way hash function based lightweight mutual authentication rfid protocol (2013)
[79]	A novel mutual authentication scheme for low-cost RFID systems (2016)
[81]	An efficient lightweight RFID authentication protocol with strong trajectory privacy protection (2017)
[87]	Secure and efficient lightweight RFID authentication protocol based on fast tag indexing (2014)
[92]	An improvement in HB-family lightweight authentication protocols for practical use of RFID system (2013)
[97]	KEDGEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems (2014)
[104]	An ultralightweight RFID authentication protocol with CRC and permutation (2014)
[106]	SLAP: Succinct and lightweight authentication protocol for low-cost RFID system (2016)
[108]	Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags (2017)
[109]	k-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions (2014)

Stream ciphers are faster and easier to implement but are weaker comparing with block ciphers. Block ciphers are thus preferable, and the most popular block cipher encryption algorithm is the Advance Encryption Standard (AES).

It is worth mentioning that Feldhofer et al. [8] introduced an efficient implementation of AES in 2004. However, in 2008, Kaps [34] noted that the implementation of the Extended Tiny Encryption Algorithm (XTEA) needs less power and fewer resources than that of the AES. Furthermore, searches that use the AES mostly refer to the number of gates rather than the security goals of the authentication protocol, which is the main subject of the present paper.

3.2 Simple protocols

The simple protocol class includes protocols that support RNG and a one-way hash function. Okhubo et al. [35] came up with a strong protocol, as an example of a hash-based protocol, in 2003. However, the tag searching cost by the server is high for this protocol. In the same year, the proposal was updated by Weis et al. [10] under the name of the hash-lock protocol. Although the hash-lock protocol performs well in tag implementation and effectiveness of the server, it performs poorly in terms of security. In 2006, Tsudik claimed that Yet Another Trivial RFID Authentication Protocol (YA-TRAP) [9] resists the tracing attack.

In 2007, however, Tsudik noted the flaws of his previous protocol and proposed a new protocol [36], even though his new protocol does not reflect his original purpose and is vulnerable to a reply attack. In 2011, Chien et al. [113] showed that the scheme presented in [9] is vulnerable to replay attacks and DoS and proposed a secured version. In the same year, Lopez et al. [114] claimed that the proposal of Chien et al. [113] is defenseless against impersonation and replay attacks and proposed a new concept called Inpatient Safety RFID system (IS-RFID).

In 2012, Yen et al. [115] noted that medication evidence generated by an IS-RFID system can be modified by a hospital easily. In 2012, Chen et al. [116] suggested a forge resistant protocol that withstands impersonation, desynchronization and traceability attacks. In 2012, Cho et al. [65] came up with a hash function based mutual authentication protocol that was inspired from his previous work [54]. In the years 2012 and 2013, the scheme of Cho et al. [65] was analyzed by Kim et al. [117, 118] and found to be most vulnerable to a desynchronization attack.

In 2014, Safkhani et al. [119] also analyzed the scheme of Cho et al. [65] and showed that it is vulnerable to desynchronization, tag and reader impersonation. Moreover, the scheme introduced in [117, 118] based on the work presented in [65] was analyzed [119] and found to have the same security faults. In 2015, a new mutual authentication protocol based on hash function proposed by Srivastava et al. [53] was qualitatively compared with protocols proposed in [36, 51, 54] and found to be superior. In 2016, Shen et al. [55] proposed an efficient RFID authentication protocol (ERAP) and claimed that compared with the previous researches, their protocol withstands different types of attacks with low cost, which satisfies the requirement of highly resource constrained RFID tags. Finally, in 2017, Li et al. [62] pointed out that the lightweight mutual authentication protocol (LMAP) [120] is vulnerable to some attacks and data integrity. To enhance the security and the privacy of LMAP, they proposed an improved version of LMAP and claimed that their protocol meets all the requirements of RFID applications and resists common attacks.

Other protocols that may fall into this class and be worthy of mention are the Hopper and Blum (HB) family of protocols. In 2001, Hopper and Blum proposed an extraordinarily lightweight protocol that uses only the AND and XOR operations on binary vectors and a noise bit called the HB bit [94] that can be generated from a physical event. To resist passive attacks, the protocol depends on the computational complexity of the learning parity with the noise problem.

The HB protocol was not designed for RFID or categorized as being lightweight or ultra-lightweight. Afterwards, the lightweight authentication protocol family based on the HB protocol was proposed. As the HB protocol resists passive attacks, Juels and Weis proposed in 2005 a modified protocol, named the HB+ protocol [93], to resist active attacks. They claimed that their protocol is lightweight but may not be directly applied to RFID tags, and their use of a two-round version may not be secure. Also in 2005, Gilbert et al. [14] mentioned that the HB+ protocol is defenseless against a linear time active attack.

In 2006, Bringer et al. [11] modified the HB+ protocol to develop the HB++ protocol, which avoids the attack of Gilbert et al. However, to detect attacks, it requires universal hash functions and additional secret key material. In 2007, Munilla et al. [95] introduced the idea of a round and proposed a new protocol, named as the HB-MP protocol, to resist man-in-the-middle and active attacks that are effective against HB and HB+ protocols.

In 2008, Gilbert et al. [121] revealed that it is possible for a simple passive attack to impersonate a valid tag by eavesdropping on communication. In 2008, the HB# protocol was introduced as an improvement on the Random-HB# protocol that was described in the same work [122]. The HB# protocol is resistant against an extended class of active attacks embracing the Gilbert et al. active attack on HB+ and HB-MP protocols [121] and, unlike the HB++ protocol [11], the HB# protocol does not require additional hardware that would increase the complexity of the HB protocol. Also in 2008, Leng et al. [96] improved on the HB-MP protocol by proposing the HB-MP+ protocol. However, Yoon et al. [123] noted that the HB-MP+ protocol does not have a real function with which to defend against an advanced active attack or strong methods for preventing the tracking problem, and they subsequently proposed the HB-MP++ protocol. Again in 2008, Quafi et al. [124] conducted a man-in-the-middle attack on the HB# protocol and retrieved a secret shared by communicating parties.

In 2009, Halevi et al. [125] indicated that PRF-based protocols, such as HB+ and HB# protocols, are not applicable to low-cost tags, and announced Tree-HB+ and Tree-HB# protocols. In 2012, the GHB# [126] protocol was developed and claimed to resist a man-in-the-middle attack, which is an effective attack on the HB# protocol. With the proposal of the Tree-LSHB+ protocol in 2013 [127], however, Deng et al. claimed that tree-based and regular HB protocols provide only one-way authentication, only tag is authenticated by the reader, and they added mutual authentication. Finally, the Tree-LSHB+ protocol cannot resist disclosure, desynchronization and traceability attacks [128]. In [128], a revised Tree-LSHB+ protocol was developed and claimed to have advantages over the past Tree-LSHB+ protocol. The evolution of the HB family protocols is shown in Fig. 1. Other examined protocols of this class are presented in Tables 1 and 2.

3.3 Lightweight protocols

The lightweight protocol class includes protocols that require simple functions, such as CRC code, and an RNG and broadly involves protocols conforming to the EPC C1 Gen2 standard. Operations supporting EPC C1 Gen2 might not be ideal for security purposes and it is thus important to improve them. Moreover, it is usual to face new problems when trying to solve expected problems. In protocols conforming to the EPC C1 Gen2 standard, the main security problem is CRC-16 (owing to the algebraic weakness of CRC (a $\oplus$ b) = CRC (a) $\oplus$ CRC (b)).

In 2005, Juels [129] was among the first to propose a solution that conforms to the EPC C1 Gen2 and was claimed to resist cloning and spoofing. In the same year, Karthikeyan et al. [130] proposed a protocol and used XOR and matrix operations not to be tracked and used timer and key updating to achieve mutual authentication. However, their protocol is vulnerable to DoS and replay attacks. In

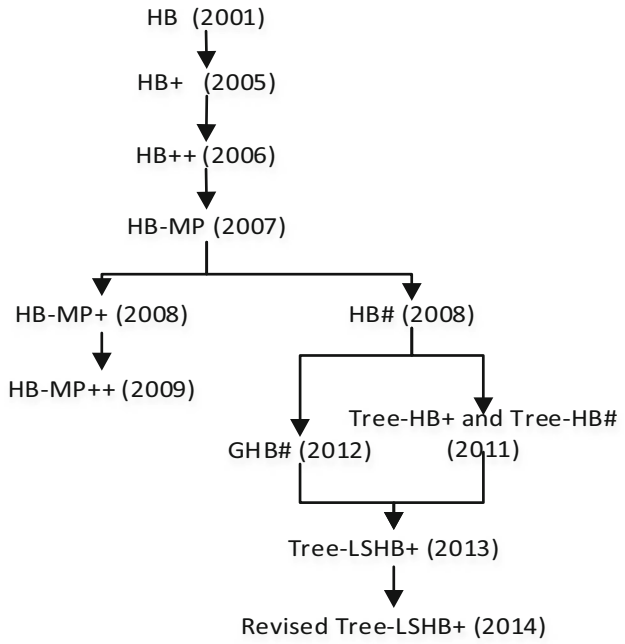

Fig. 1 Evolution of the HB family

2006, Duc et al. [13] showed that Juels' [129] scheme suffers from privacy and information leakage. Moreover, they proposed a new protocol that uses CRC, XOR and a pseudorandom-number generator (PRNG) to guarantee interactive information security, achieving mutual authentication and synchronous updating of the secret key. However, their protocol is vulnerable in terms of a DoS attack and forward security.

In 2007, Chien et al. [12] embellished on both the works of Karthikeyan et al. [130] and Duc et al. [13] in proposing a new protocol called the Chien & Chen (CC) protocol and claimed that they had achieved forward security and resistance against DoS and reply attacks; however, the claimed security objectives were later shown to be false owing to the linear property of the CRC operation used in the protocol. In the same year, Lo et al. [131] improved the CC protocol [12] in terms of data security, privacy and efficiency, but the CC protocol is still vulnerable to eavesdropping and location tracking.

In 2009, Lopez et al. [132] noted the CC protocol cannot hold tag and reader impersonation, desynchronization and tracing attacks. In 2010, Yeh et al. [133] asserted a new protocol, referred to as the secure remote password (SRP) protocol, which is easy and convenient to implement and which they claimed not only resolved the flaws of the CC protocol but also enhanced the overall performance efficiently. However, Habibi et al. [83, 134] noted that the SRP protocol is defenseless to a tracking attack and information leakage and that the complexity of a successful attack is only 2^{16}, and they improved SRP and suggested this new version.

In 2014, Mohammadi et al. [120] studied the scheme proposed in [83] and showed that it is vulnerable to an attack that reveals secret parameters, a tag impersonation attack, a data desynchronization attack and a traceability attack. Additionally, they improved the scheme proposed in [83] and proposed a new protocol called the improved lightweight mutual authentication protocol (ILMAP). Later, in 2014, Alavi et al. [135] investigated the ILMAP protocol and showed that it is vulnerable to an attack that reveals secret parameters, a data integrity attack, a reader forward compromise attack, a traceability attack and backward and forward traceability attacks. Additionally, by altering processes of the ILMAP, they proposed a strengthened version of the ILMAP. In 2013, based on the SRP protocol, Pang et al. [136] suggested an authentication protocol, named SRP+, and they argued that they had overcome the weaknesses of the SRP protocol and increased the complexity of a successful attack to 2^{23}.

In 2015, however, Wang et al. [137] analyzed the SRP+ protocol and showed that it is vulnerable to a desynchronization attack because of the well-known security defect of the CRC function and a passive disclosure attack with a complexity of O (2^{16}). Furthermore, an updated version of the SRP+, called the SRP++, has been proposed and it has been asserted that this proposal can withstand disclosure attack with a complexity reaching O (2^{32}), thus providing better security than its predecessors.

In 2016, Maarof et al. [79] suggested a new mutual authentication scheme that is compliant with EPC C1 Gen2 standard. They demonstrated that their scheme resists against security attacks, is better than the previous schemes and is easy to implement in low cost RFID systems because the simple operators (XOR, CRC and PRNG) are used. Finally in 2017, Zhang et al. [81] proposed a lightweight RFID authentication protocol with strong trajectory privacy protection (LAP-STP). They informed their protocol can withstand different attacks and warrant the strong trajectory privacy. Other examined protocols of this class are given in Tables 1 and 2.

3.4 Ultra-lightweight protocols

Ultra-lightweight protocols are tailored specially to extremely constrained devices in which only simple bit-wise operations (e.g., XOR, AND, OR) are implemented. After Gen-2 was released in 2006, Lopez et al. proposed ultra-lightweight RFID protocols named the ultralightweight mutual authentication protocols (UMAPs) and comprising the minimalist mutual authentication protocol (M^2AP) [56], lightweight mutual authentication protocol (LMAP) [57] and efficient mutual authentication protocol (EMAP) [58], which use only triangular functions ($\vee$, $\wedge$, $\oplus$) and

addition [48]. This family is efficient for low-cost RFID tags in terms of the computation cost and storage cost.

In 2007, however, Li et al. [15, 16] presented several attacks on the M^2AP, LMAP and EMAP. In the same year, Chien [6] pointed out the UMAPs were vulnerable to many attacks, introduced the rotation operation and proposed the strong authentication and strong integrity (SASI) protocol. However, owing to its use of triangular functions ($\vee$, $\oplus$), only a limited number of rotations and addition, SASI protocol is defenseless against various kinds of attacks and this was shown by [138, 139]. Later, in 2009, Lopez et al. [105] used XOR encapsulated in nested rotation functions and addition and produced Gossamer protocol, which is inspired from the SASI protocol.

In 2010, however, Tagra et al. [140] conducted a desynchronization attack on Gossamer. After Gossamer, in 2009, Lopez et al. [141] slightly improved the LMAP and produced the ultra-lightweight authentication protocol (ULAP), which uses only addition and triangular functions, to overcome passive attacks. Meanwhile, in 2010, a passive attack on ULAP was conducted by Wang et al. [142].

In 2012, Tian et al. [38] proposed an interesting ultra-lightweight RFID authentication protocol, named the RFID authentication protocol with permutation (RAPP), which have only three operations as bit-wise XOR, left rotation and permutation. However, because the Hamming weight of rotation and permutation is invariant (i.e., the Hamming weight output of two operations is the same as that of the first parameter) and because of permutation properties, Zhuang et al. [143] in 2013 applied two attacks on the RAPP that can cause a tag to fall into the DoS state in addition to desynchronization and replay attacks.

Also in 2013, Jeon et al. [144] by using merge (merging two bit strings) and separation (inverse of merging) operations suggested a new authentication protocol called the efficient ultra-lightweight RFID authentication protocol (EURFID). In the same year, however, the same authors [66] found that EURFID protocol does not serve correctly in the case of collision between tags and they improved EURFID protocol and proposed the RFID authentication protocol for low-cost tags (RAPLT) that is a new merge and separation operations based ultra-lightweight protocol. Nevertheless, RAPLT is vulnerable in terms of replay and desynchronization attack, and protecting data integrity and user privacy according to Zhuang et al. [145]. In 2015, Wang et al. [137] applied a passive disclosure attack on the RAPLT [66] using the linear property of the merge operation and applied de-synchronization attack on SRP+ [136] using the linearity property of CRC operation. They presented a modified and efficient version of SRP+ protocol that is EPC C1 Gen2 standard compliant, denoted by SRP++. They claimed for this protocol that exhaustive search attack could be resisted.

In 2016, Luo et al. [106] presented a new secure ultra-lightweight bitwise conversion based ultra-lightweight mutual authentication protocol. The aim was to improve the ultra-lightweight authentication against the weak security resistance in recent protocols described in references [107] and [64]. Their protocol employed only three bitwise operations; XOR, left rotation and conversion. They claimed that their protocol is more secure than other compared protocols, can resist various existing attacks and preferable in a low-cost RFID system than other compared protocols. Finally in 2017, Tewari et al. [108] presented an ultra-lightweight mutual authentication protocol that uses bitwise XOR and left-rotation. They pointed out that their protocol ensures data confidentiality, integrity, tag anonymity, and has resistance against tracking and various attacks. Other examined protocols of this class are given in Tables 1 and 2.

3.5 Less traditional forms of authentication

It is worth mentioning that less traditional forms of authentication such as using exhaustive searches to enable privacy-preservation, are also used. The mechanism of randomizing a tag identifier to protect its privacy was firstly proposed in 2003 by Weis et al. [10]. By using a nonce generated by a tag and secret value, they computed the identifier. In the same year, Ohkubo et al. [35] and in 2005 Avoine et al. [146] improved this idea by a different approach; the key that produced the identifier continually changes, where the new key was the message digest of the former.

In 2008, Henrici et al. [147] used the same approach of Ohkubo et al. [35] and Avoine et al. [146], but the new key was triggered by the hash chains of the former. The main problem of randomized tag identifier is on the server side where the identifier has to be searched among a bulk of data. A solution to this problem is a tree search structure approach used by Molnar et al. [70], Molnar et al. [148] and Dimitriou [149]. In this proposal, branches have specific keys and each tag has set of keys. To identify a tag, the keys on each level and on a specific branch are used.

However, in 2010, Avoine et al. [150] mentioned that protocols that use exhaustive searches are vulnerable to a timeful attack. In 2014, Figueiredo et al. [151] proposed a protocol where RFID tags are used on vehicles. The tag, uses the stored secret key with two random values generated by the reader and the tag itself to generate the pseudo-random identifier. The identification application makes an exhaustive search to discover the tag that generated the identifier.

Figueiredo et al. [151] mentioned that approaches of [35, 146, 147] raise critical synchronization matters between identification applications and tags. They also

Table 4 MIFARE products overview

Products	Authentication	Confidentiality
MIFARE Classic EV1	CRYPTO1	CRYPTO1
MIFARE Plus	AES	CRYPTO1 + AES
MIFARE Plus SE	AES	CRYPTO1 + AES (Optional)
MIFARE Plus EV1	AES	AES
MIFARE Ultralight C	3DES	–
MIFARE Ultralight EV1	–	–
MIFARE Ultralight Nano	–	–
MIFARE DESFire EV1	AES + 3DES + DES	AES + 3DES + DES
MIFARE DESFire EV2	AES + 3DES + DES	AES + 3DES + DES

mentioned that the tree search structure approach used by [70, 148, 149], increases the computation within tags and increases the length of the tag's reply. Lastly, they claimed that they solved the above-mentioned issues and informed that the aim of their proposal was not to provide best privacy to tag owners but to reveal the possibility of exhaustive key searches without conveying any direct or clear identifiers during tag authentication.

4 Comparison evaluation

In Table 2, the protocols are compared in terms of security threats and services. Each of the examined protocols has a specific ability to cope with security and privacy issues. When the number of checks counted from the table, the class that overcomes most threats and provides more services is the fully fledged and the class that overcomes least threats and provides least services is the ultra-lightweight. The protocol presented in [33], which provides the best security is fully fledged, and has overcome (9) threats and provides (9) services. The protocol presented in [106], which provides the least security is ultra-lightweight, and has overcome (3) threats and provides (0) service. This is to be expected considering the definitions of authentication classes. In other words, less can be achieved with an authentication protocol when the hardware capability of a tag is low. Not surprisingly, most of the practical RFID-based applications such as building access control [152], e-passports [153], electronic toll collection [154] and electronic ticketing [155] are using fully fledged class. Moreover, the widely-used technology in this field, such as Calypso [156] and most generations of MIFARE [157] (Table 4) are using fully fledged class. When the matter is the life of a person and privacy, this is to be expected. However, the cost must be reduced and a need for more and stronger light and ultra-lightweight authentication protocols is obvious. For the readers who want to deepen on other specific features, please check [158].

5 Conclusion

The use of authentication protocols is the first step in defending against wireless attacks on RFID systems. The present paper reviewed and compared recently proposed RFID authentication protocols. The major points of the comparison were presented in Tables 1 and 2. Table 1 showed that, to deal with attacks and to ensure security and privacy, the examined authentication protocols have adopted different methods, such as ECC, hash functions, random-number generators and merge, separation, mix-bit and rotation operations and different verification methods have been used to verify the proposed protocols. As low-cost RFID tags are severely constrained by their hardware in terms of storage and processing capabilities, most of the examined proposals lie within the fully fledged class and few of the examined proposals lie within the ultra-lightweight class.

Table 2 showed that each of the examined protocols has a specific ability to cope with security and privacy issues. Fully fledged protocols overcome many threats and provide more services than other protocols. Taking into account the authentication classes' definitions and the goals that authentication protocols must achieve, this is to be expected.

The present paper concludes that there is a need for more and stronger authentication protocols, especially ultra-lightweight authentication protocols. It is thus necessary to propose a strong authentication protocol with an integrated approach to deal with all or at least most threats than the protocols mentioned in the present paper in future work.

References

1. Chinese RFID technology policy white paper, 2006. 15 Ministries and Commissions including Ministry of Science and Technology of PRC.

2. Karmakar, N. C. (Ed.). (2011). *Handbook of smart antennas for RFID systems*. New York: Wiley.
3. EPCglobal. (2015). EPC radio frequency identity protocols Class-1 Generation-2 UHF RFID protocol for communications at 860–960 MHz. Technical report, Version 2.0.1. https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf. Accessed 03 Sept 2017.
4. Vajda, I., & Buttyán, L. (2003). Lightweight authentication protocols for low-cost RFID tags. In *Second workshop on security in ubicomp* (Vol. 2003, pp. 1–10).
5. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006). RFID systems: A survey on security threats and proposed solutions. In *IFIP international conference on personal wireless communications* (pp. 159–170). Springer, Berlin, Heidelberg.
6. Chien, H. Y. (2007). Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing, 4*(4), 337–340.
7. Tuyls, P., & Batina, L. (2006). RFID tags for anti-counterfeiting. In D. Pointcheval (Ed.), *Topics in cryptology–CT-RSA 2006* (pp. 115–131). Berlin: Springer.
8. Feldhofer, M., Dominikus, S., & Wolkerstorfer, J. (2004). Strong authentication for RFID systems using the AES algorithm. In M. Joye & J.-J. Quisquater (Eds.), *Cryptographic hardware and embedded systems CHES 2004* (pp. 357–370). Berlin: Springer.
9. Tsudik, G. (2006). YA-TRAP: Yet another trivial RFID authentication protocol. In *Fourth annual IEEE international conference on pervasive computing and communications workshops, PerCom Workshops 2006*. IEEE.
10. Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Müller, W. Stephan, & M. Ullmann (Eds.), *Security in pervasive computing* (pp. 201–212). Berlin, Heidelberg: Springer.
11. Bringer, J., Chabanne, H., & Dottax, E. (2006). HB++: A lightweight authentication protocol secure against some attacks. In *Second international workshop on security, privacy and trust in pervasive and ubiquitous computing, 2006* (pp. 28–33). IEEE.
12. Chien, H. Y., & Chen, C. H. (2007). Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces, 29*(2), 254–259.
13. Duc, D., Park J., & Lee, H. (2006). Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning. In *2006 symposium on cryptography and information security* (pp. 17–20).
14. Gilbert, H., Robshaw, M., & Sibert, H. (2005). Active attack against HB+: A provably secure lightweight authentication protocol. *Electronics Letters, 41*(21), 1169–1170.
15. Li, T., & Deng, R. (2007). Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol. In *The second international conference on availability, reliability and security, 2007, ARES 2007* (pp. 238–245). IEEE.
16. Li, T., & Wang, G. (2007). Security analysis of two ultralightweight RFID authentication protocols. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. von Solms (Eds.), *New approaches for security, privacy and trust in complex environments* (pp. 109–120). New York: Springer.
17. Soos, M. (2009). An overview of RFID security protocols. Ph.D. Thesis. https://www.msoos.org/wordpress/wp-content/uploads/2012/03/soos_thesis_v3.pdf. Accessed 01 Sept 2017.
18. Lee, Y. K., Batina, L., & Verbauwhede, I. (2008). EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In *2008 IEEE international conference on RFID,* (pp. 97–104). IEEE.
19. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007). Public-key cryptography for RFID-tags. In *Fifth annual IEEE international conference on pervasive computing and communications workshops, 2007* (pp. 217–222). IEEE.
20. Van Deursen, T., & Radomirovic, S. (2008). Attacks on RFID Protocols. *IACR Cryptology ePrint Archive, 2008*(310), 1–56.
21. Bringer, J., Chabanne, H., & Icart, T. (2008). Cryptanalysis of EC-RAC, a RFID identification protocol. In *Cryptology and network security* (pp. 149–161). Springer, Berlin, Heidelberg.
22. Lee, Y. K., Batina, L., & Verbauwhede, I. (2009). Untraceable RFID authentication protocols: Revision of EC-RAC. In *2009 IEEE international conference on RFID* (pp. 178–185). IEEE.
23. Lee, Y. K., Batina, L., Singelee, D., Preneel, B., & Verbauwhede, I. (2010). Anti-counterfeiting, untraceability and other security challenges for RFID systems: Public-key-based protocols and hardware. In A.-R. Sadeghi & D. Naccache (Eds.), *Towards hardware intrinsic security* (pp. 237–257). Berlin, Heidelberg: Springer.
24. Zhang, X., Li, J., Wu, Y., & Zhang, Q. (2011). An ECDLP based randomized key RFID authentication protocol. In *2011 international conference on network computing and information security (NCIS)* (Vol. 2, pp. 146–149). IEEE.
25. Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks, 18,* 133–146.
26. Moosavi, S. R., Nigussie, E., Virtanen, S., & Isoaho, J. (2014). An elliptic curve-based mutual authentication scheme for RFID implant systems. *Procedia Computer Science, 32,* 198–206.
27. He, D., Kumar, N., Chilamkurti, N., & Lee, J. H. (2014). Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *Journal of Medical Systems, 38*(10), 1–6.
28. Zhao, Z. (2014). A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. *Journal of Medical Systems, 38*(5), 1–7.
29. Chou, J. S. (2014). A secure RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *The Journal of Supercomputing, 70*(1), 75–94.
30. Zhang, Z., & Qi, Q. (2014). An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *Journal of Medical Systems, 38*(5), 1–7.
31. Jin, C., Xu, C., Zhang, X., & Zhao, J. (2015). A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography. *Journal of Medical Systems, 39*(3), 1–8.
32. Farash, M. S., Nawaz, O., Mahmood, K., Chaudhry, S. A., & Khan, M. K. (2016). A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. *Journal of Medical Systems, 40*(7), 1–7.
33. Ibrahim, A., & Dalkilic, G. (2017). An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for RFID, proven on WISP. *Journal of Sensors*, Article ID 2367312.
34. Kaps, J. P. (2008). Chaitea, cryptographic hardware implementations of xtea. In D. R. Chowdhury, V. Rijmen, & A. Das (Eds.), *Progress in cryptology-INDOCRYPT 2008* (pp. 363–375). Berlin, Heidelberg: Springer.
35. Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003). Cryptographic approach to "privacy-friendly" tags. In *RFID privacy workshop* (Vol. 82).
36. Tsudik, G. (2007). A family of dunces: Trivial RFID identification and authentication protocols. In *Privacy enhancing technologies* (pp. 45–61). Springer, Berlin, Heidelberg.
37. Rostampour, S., Namin, M. E., & Hosseinzadeh, M. (2014). A novel mutual RFID authentication protocol with low complexity

and high security. *International Journal of Modern Education and Computer Science (IJMECS), 6*(1), 17–24.
38. Tian, Y., Chen, G., & Li, J. (2012). A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters, 16*(5), 702–705.
39. Qian, Z., Chen, C., You, I., & Lu, S. (2012). ACSP: A novel security protocol against counting attack for UHF RFID systems. *Computers & Mathematics with Applications, 63*(2), 492–500.
40. Han, S., Potdar, V., & Chang, E. (2007). Mutual authentication protocol for RFID tags based on synchronized secret information with monitor. In *Computational science and its applications–ICCSA 2007* (pp. 227–238). Springer, Berlin, Heidelberg.
41. Qingling, C., Yiju, Z., & Yonghua, W. (2008). A minimalist mutual authentication protocol for RFID system & BAN logic analysis. In *ISECS international colloquium on computing, communication, control, and management* (Vol. 2, pp. 449–453). IEEE.
42. Chen, C. L., & Deng, Y. Y. (2009). Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection. *Engineering Applications of Artificial Intelligence, 22*(8), 1284–1291.
43. Chou, J. S. (2014). An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing, 70*(1), 75–94.
44. Dalkiliç, G., Özcanhan, M. H., & Çakır, H. Ş. (2014). Increasing key space at little extra cost in RFID authentications. *Turkish Journal of Electrical Engineering & Computer Sciences, 22*(1), 155–165.
45. Liu, Y. (2008). An efficient RFID authentication protocol for low-cost tags. In *IEEE/IFIP international conference on embedded and ubiquitous computing* (Vol. 2, pp. 180–185). IEEE.
46. Toiruul, B., & Lee, K. (2006). An advanced mutual authentication algorithm using AES for RFID systems. *International Journal of Computer Science and Network Security, 6*(9), 156–162.
47. Ha, J., Moon, S., Nieto, J. M. G., & Boyd, C. (2007). Low-cost and strong-security RFID authentication protocol. In *Emerging directions in embedded and ubiquitous computing* (pp. 795–807). Springer, Berlin, Heidelberg.
48. Özcanhan, M. H., Dalkılıç, G., & Utku, S. (2014). Cryptographically supported NFC tags in medication for better inpatient safety. *Journal of Medical Systems, 38*(8), 1–15.
49. Peris-Lopez, P., Safkhanim, M., Bagheri, N., & Naderi, M. (2013). RFID in eHealth: How combat medications errors and strengthen patient safety. *Journal of Medical and Biological Engineering, 33,* 363–372.
50. Hakeem, M. J., Raahemifar, K., & Khan, G. N. (2013). HPAP: A novel authentication scheme for RFID systems. In *26th annual ieee canadian conference on electrical and computer engineering* (pp. 1–6). IEEE.
51. Chatmon, C., Le, T. V., & Burmester, M. (2006). Secure anonymous RFID authentication protocols (pp. 1–10). *Technical Report* TR-060112, Florida State Univeristy, Tallahassee.
52. Changqing, O., Jixiong, W., Zhengyan, L., & Shengye, H. (2008). An enhanced security authentication protocol based on hash-lock for low-cost RFID. In *2nd international conference on anti-counterfeiting, security and identification* (pp. 416–419). IEEE.
53. Srivastava, K., Awasthi, A. K., Kaul, S. D., & Mittal, R. C. (2015). A hash based mutual RFID tag authentication protocol in telecare medicine information system. *Journal of Medical Systems, 39*(1), 1–5.
54. Cho, J. S., Yeo, S. S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. *Computer Communications, 34*(3), 391–397.
55. Shen, J., Tan, H., Moh, S., Chung, I., & Wang, J. (2016). An efficient RFID authentication protocol providing strong privacy and security. *Journal of Internet Technology, 17*(3), 443–455.
56. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagor-da, A. (2006). M2AP: A minimalist mutual authentication protocol for low-cost RFID tags. In *Ubiquitous intelligence and computing* (pp. 912–923). Springer, Berlin, Heidelberg.
57. Peris-Lopez, P., Hernandez-Castro, J. C., Estévez-Tapiador, J. M., & Ribagorda, A. (2006). LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In *Workshop on RFID security* (pp. 12–14).
58. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006). EMAP: An efficient mutual-authentication protocol for low-cost RFID tags. In *On the move to meaningful internet systems 2006: OTM 2006 workshops* (pp. 352–361). Springer, Berlin, Heidelberg.
59. Tan, C. C., Sheng, B., & Li, Q. (2008). Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications, 7*(4), 1400–1407.
60. He, L., Jin, S. H., Zhang, T., & Li, N. N. (2009). An enhanced 2-pass optimistic anonymous RFID authentication protocol with forward security. In *5th International conference on wireless communications, networking and mobile computing* (pp. 1–4). IEEE.
61. Rahman, M. S., Soshi, M., & Miyaji, A. (2009). A secure RFID authentication protocol with low communication cost. In *International conference on complex, intelligent and software intensive systems, 2009, CISIS'09* (pp. 559–564). IEEE.
62. Li, J., Zhou, Z., & Wang, P. (2017). Cryptanalysis of the LMAP protocol: A low-cost RFID authentication protocol. In *29th Chinese control and decision conference (CCDC)* (pp. 7292–7297). IEEE.
63. Zhu, S., Yang, B., & Zhang, M. (2007). Research on RFID protocols and security. In *Information security and confidentiality of communications* (pp. 168–170).
64. Mujahid, U., Najam-ul-Islam, M., & Shami, M. A. (2015). RCIA: A new ultralightweight rfid authentication protocol using recursive hash. *International Journal of Distributed Sensor Networks*, *11*(1), Article ID 642180.
65. Cho, J. S., Jeong, Y. S., & Park, S. O. (2015). 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.
66. Jeon, I. S., & Yoon, E. J. (2013). A new ultralightweight RFID authentication protocol using merge and separation operations. *International Journal of Mathematical Analysis, 7*(52), 2583–2593.
67. Kardaş, S., Çelik, S., Arslan, A., & Levi, A. (2013). An efficient and private RFID authentication protocol supporting ownership transfer. In *Lightweight cryptography for security and privacy* (pp. 130–141). Springer, Berlin, Heidelberg.
68. Kardas, S., Levi, A., & Murat, E. (2011). Providing resistance against server information leakage in RFID systems. In *4th IFIP international conference on new technologies, mobility and security* (pp. 1–7). IEEE.
69. Fan, K., Li, J., Li, H., Liang, X., Shen, X. S., & Yang, Y. (2014). RSEL: revocable secure efficient lightweight RFID authentication scheme. *Concurrency and Computation: Practice and Experience, 26*(5), 1084–1096.
70. Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: Issues, practices, and architectures. In

Proceedings of the 11th ACM conference on Computer and Communications Security (pp. 210–219). ACM.
71. Sarma, S. E., Weis, S. A., & Engels, D. W. (2003). RFID systems and security and privacy implications. In *Cryptographic hardware and embedded systems CHES 2002* (pp. 454–469). Springer, Berlin, Heidelberg.
72. Ohkubo, M., Suzuki, K., & Kinoshita, S. (2004). Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In *Proceedings of the SCIS* (Vol. 2004, pp. 719–724).
73. Henrici, D., & Muller, P. (2004). Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers. In *Proceedings of the second IEEE annual conference on pervasive computing and communications workshops* (pp. 149–153). IEEE.
74. Gao, X., Xiang, Z., Wang, H., Shen, J., Huang, J., & Song, S. (2004). An approach to security and privacy of RFID system for supply chain. In *IEEE international conference on e-commerce technology for dynamic e-business* (pp. 164–168). IEEE.
75. Li, Y., & Ding, X. (2007). Protecting RFID communications in supply chains. In *Proceedings of the 2nd ACM symposium on information, computer and communications security* (pp. 234–241). ACM.
76. Ren, X., Xu, X., & Li, Y. (2013). An one-way hash function based lightweight mutual authentication rfid protocol. *Journal of Computers, 8*(9), 2405–2412.
77. Song, B., & Mitchell, C. J. (2008). RFID authentication protocol for low-cost tags. In *Proceedings of the first ACM conference on wireless network security* (pp. 140–147). ACM.
78. Ning, H., Liu, H., Mao, J., & Zhang, Y. (2011). Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. *IET Communications, 5*(12), 1755–1768.
79. Maarof, A., Labbi, Z., Senhadji, M., & Belkasmi, M. (2016). A novel mutual authentication scheme for low-cost RFID systems. In *2016 international conference on wireless networks and mobile communications (WINCOM)* (pp. 240–245). IEEE.
80. Huang, Y. C., & Jiang, J. R. (2012). An ultralightweight mutual authentication protocol for EPC C1G2 RFID tags. In *2012 fifth international symposium on parallel architectures, algorithms and programming (PAAP)* (pp. 133–140). IEEE.
81. Zhang, W., Liu, S., Wang, S., Yi, B., & Wu, L. (2017). An efficient lightweight RFID authentication protocol with strong trajectory privacy protection. *Wireless Personal Communications, 96*(1), 1215–1228.
82. Zhang, W., Wu, L., Liu, S., Huang, T., Guo, Y., & Hsu, C. (2016). A trajectory privacy model for radio-frequency identification system. *Wireless Personal Communications, 90*(3), 1121–1134.
83. Habibi, M. H., Alagheband, M. R., & Aref, M. R. (2011). Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard. In *Information security theory and practice. Security and privacy of mobile devices in wireless communication* (pp. 254–263). Springer, Berlin, Heidelberg.
84. Xiao, F., Zhou, Y. J., Zhou, J. X., & Niu, X. X. (2013). Provable secure mutual authentication protocol for RFID in the standard model. *Journal on Communications, 34*(4), 82–87.
85. Ha, J. C., Ha, J. H., Moon, S. J., & Boyd, C. (2006). LRMAP: Lightweight and resynchronous mutual authentication protocol for RFID system. In *International conference on ubiquitous convergence technology* (Vol. 4412, pp. 80–89). Springer.
86. Alomair, B., Clark, A., Cuellar, J., & Poovendran, R. (2012). Scalable RFID systems: a privacy-preserving protocol with constant-time identification. *IEEE Transactions on Parallel and Distributed Systems, 23*(8), 1536–1550.
87. Pang, L., Li, H., He, L., Alramadhan, A., & Wang, Y. (2014). Secure and efficient lightweight RFID authentication protocol based on fast tag indexing. *International Journal of Communication Systems, 27*(11), 3244–3254.
88. Zhang, Z., Zhou, S., & Luo, Z. (2008). Design and analysis for RFID authentication protocol. In *IEEE international conference on e-business engineering* (pp. 574–577). IEEE.
89. Zhou, S., Zhang, Z., Luo, Z., & Wong, E. C. (2010). A lightweight anti desynchronization RFID authentication protocol. *Information Systems Frontiers, 12*(5), 521–528.
90. Choi, E. Y., Lee, S. M., & Lee, D. H. (2005). Efficient RFID authentication protocol for ubiquitous computing environment. In *Embedded and ubiquitous computing–EUC 2005 workshops* (pp. 945–954). Springer, Berlin, Heidelberg.
91. Dimitriou, T. (2005). A lightweight RFID protocol to protect against traceability and cloning attacks. In *First international conference on security and privacy for emerging areas in communications networks* (pp. 59–66). IEEE.
92. Lin, Z., & Song, J. S. (2013). An improvement in HB-family lightweight authentication protocols for practical use of RFID system. *Journal of Advances in Computer Networks, 1*(1), 61–65.
93. Juels, A., & Weis, S. A. (2005). Authenticating pervasive devices with human protocols. In *Advances in cryptology–CRYPTO 2005* (pp. 293–308). Springer, Berlin, Heidelberg.
94. Hopper, N. J., & Blum, M. (2001). Secure human identification protocols. In *Advances in cryptology—ASIACRYPT 2001* (pp. 52–66). Springer, Berlin, Heidelberg.
95. Munilla, J., & Peinado, A. (2007). HB-MP: A further step in the HB-family of lightweight authentication protocols. *Computer Networks, 51*(9), 2262–2267.
96. Leng, X., Mayes, K., & Markantonakis, K. (2008). HB-MP+ protocol: An improvement on the HB-MP protocol. In *2008 IEEE international conference on RFID* (pp. 118–124). IEEE.
97. Tounsi, W., Cuppens-Boulahia, N., Garcia-Alfaro, J., Chevalier, Y., & Cuppens, F. (2014). KEDGEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems. *Journal of Network and Computer Applications, 39,* 152–166.
98. Van Le, T., Burmester, M., & De Medeiros, B. (2007). Universally composable and forward secure RFID authentication and authenticated key exchange. In *Proceedings of the 2nd ACM symposium on information, computer and communications security* (pp. 242–252). ACM.
99. Burmester, M., & Munilla, J. (2011). Lightweight RFID authentication with forward and backward security. *ACM Transactions on Information and System Security (TISSEC), 14*(1), 11–16.
100. HanataniI, Y., Ohkubo, M., Matsuo, S. I., Sakiyama, K., & Ohta, K. (2012). A study on computational formal verification for practical cryptographic protocol: The case of synchronous RFID authentication. In *Financial cryptography and data security* (pp. 70–87). Springer, Berlin, Heidelberg.
101. Brusó, M., Chatzikokolakis, K., & Den Hartog, J. (2010). Formal verification of privacy for RFID systems. In *23rd IEEE computer security foundations symposium* (pp. 75–88). IEEE.
102. Kim, H. S., Oh, J. H., Kim, J. B., Jeong, Y. O., & Choi, J. Y. (2008). Formal verification of cryptographic protocol for secure RFID system. In *Fourth international conference on networked computing and advanced information management* (Vol. 2, pp. 470–477). IEEE.
103. Asadpour, M., & Dashti, M. T. (2011). A privacy-friendly RFID protocol using reusable anonymous tickets. In *IEEE 10th international conference on trust, security and privacy in computing and communications (TrustCom)* (pp. 206–213). IEEE.
104. Gao, L., Ma, M., Shu, Y., & Wei, Y. (2014). An ultralightweight RFID authentication protocol with CRC and permutation. *Journal of Network and Computer Applications, 41,* 37–46.

105. Peris-Lopez, P., Hernandez-Castro, J. C., Tapiador, J. M., & Ribagorda, A. (2009). Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In *Information security applications* (pp. 56–68). Springer, Berlin, Heidelberg.
106. Luo, H., Wen, G., Su, J., & Huang, Z. (2016). SLAP: Succinct and lightweight authentication protocol for low-cost RFID system. *Wireless Networks, 22,* 1–10.
107. Zhuang, X., Zhu, Y., & Chang, C. C. (2014). A new ultralightweight RFID protocol for low-cost tags: R^2AP. *Wireless Personal Communications, 79*(3), 1787–1802.
108. Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing, 73*(3), 1085–1102.
109. Kardaş, S., Çelik, S., Bingöl, M. A., Kiraz, M. S., Demirci, H., & Levi, A. (2015). K-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions. *Wireless Communications and Mobile Computing, 15*(18), 2150–2166.
110. Ranasinghe, D., Engels, D., & Cole, P. (2004). Security and privacy: Modest proposals for low-cost RFID systems. In *Auto-ID labs research workshop, Zurich, Switzerland.*
111. Tuyls, P., & Batina, L. (2006). RFID-tags for anti-counterfeiting. In *Topics in cryptology–CT-RSA 2006* (pp. 115–131). Springer Berlin Heidelberg.
112. Bassil, R., El-Beaino, W., Itani, W., Kayssi, A., & Chehab, A. (2012). PUMAP: A PUF-based ultra-lightweight mutual authentication RFID protocol. *International Journal of RFID Security and Cryptography, 1*(1/2), 58–66.
113. Chien, H. Y., Yang, C. C., Wu, T. C., & Lee, C. F. (2011). Two RFID-based solutions to enhance inpatient medication safety. *Journal of Medical Systems, 35*(3), 369–375.
114. Peris-Lopez, P., Orfila, A., Mitrokotsa, A., & Van der Lubbe, J. C. (2011). A comprehensive RFID solution to enhance inpatient medication safety. *International Journal of Medical Informatics, 80*(1), 13–24.
115. Yen, Y. C., Lo, N. W., & Wu, T. C. (2012). Two RFID-based solutions for secure inpatient medication administration. *Journal of Medical Systems, 36*(5), 2769–2778.
116. Chen, Y. Y., Huang, D. C., Tsai, M. L., & Jan, J. K. (2012). A design of tamper resistant prescription RFID access control system. *Journal of Medical Systems, 36*(5), 2795–2801.
117. Kim, H. (2012). Enhanced hash-based RFID mutual authentication protocol. In *Computer applications for security, control and system engineering* (pp. 70–77). Springer, Berlin, Heidelberg.
118. Kim, H. (2013). RFID mutual authentication protocol based on synchronized secret. *International Journal of Security and Its Applications, 7*(4), 37–50.
119. Safkhani, M., Peris-Lopez, P., Castro, J. C. H., & Bagheri, N. (2014). Cryptanalysis of Cho et al'.s protocol, A hash-based mutual authentication protocol for RFID systems. *Journal of Computational and Applied Mathematics, 259,* 571–577.
120. Mohammadi, M., Hosseinzadeh, M., & Esmaeildoust, M. (2014). Analysis and improvement of the lightweight mutual authentication protocol under EPC C-1 G-2 standard. *Advances in Computer Science: An International Journal, 3*(2), 10–16.
121. Gilbert, H., Robshaw, M. J., & Seurin, Y. (2008). Good variants of HB+ are hard to find. In *Financial cryptography and data security* (pp. 156–170). Springer, Berlin, Heidelberg.
122. Gilbert, H., Robshaw, M. J., & Seurin, Y. (2008).: HB#: Increasing the security and efficiency of HB+. In *Advances in cryptology–EUROCRYPT 2008* (pp. 361–378). Springer, Berlin, Heidelberg.
123. Yoon, B., Sung, M. Y., Yeon, S., & Oh, H. S. (2009). HB-MP++ protocol: An ultralightweight authentication protocol for RFID system. In *Proceedings of IEEE international conference on RFID* (pp. 186–191). IEEE.
124. Ouafi, K., Overbeck, R., & Vaudenay, S. (2008). On the security of HB# against a man-in-the-middle attack. In *Advances in cryptology-ASIACRYPT 2008* (pp. 108–124). Springer, Berlin, Heidelberg.
125. Halevi, T., Saxena, N., & Halevi, S. (2011). Tree-based HB protocols for privacy-preserving authentication of RFID tags. *Journal of Computer Security, 19*(2), 343–363.
126. Rizomiliotis, P., & Gritzalis, S. (2012). GHB#: A provably secure HB-like lightweight authentication protocol. In *Applied cryptography and network security* (pp. 489–506). Springer, Berlin, Heidelberg.
127. Deng, G., Li, H., Zhang, Y., & Wang, J. (2013). Tree-LSHB+: An LPN-based lightweight mutual authentication RFID protocol. *Wireless Personal Communications, 72*(1), 159–174.
128. Qian, X., Liu, X., Yang, S., & Zuo, C. (2014). Security and privacy analysis of tree-LSHB+ protocol. *Wireless Personal Communications, 77*(4), 3125–3141.
129. Juels, A. (2005). Strengthening EPC tags against cloning. In *Proceedings of the 4th ACM workshop on wireless security* (pp. 67–76). ACM.
130. Karthikeyan, S., & Nesterenko, M. (2005). RFID security without extensive cryptography. In *Proceedings of the 3rd ACM workshop on security of* ad hoc *and sensor networks* (pp. 63–67). ACM.
131. Lo, N. W., & Yeh, K. H. (2007). An efficient mutual authentication scheme for EPCglobal class-1 generation-2 RFID system. In *Emerging directions in embedded and ubiquitous computing* (pp. 43–56). Springer, Berlin, Heidelberg.
132. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2009). Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. *Computer Standards & Interfaces, 31*(2), 372–380.
133. Yeh, T. C., Wang, Y. J., Kuo, T. C., & Wang, S. S. (2010). Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Systems with Applications, 37*(12), 7678–7683.
134. Habibi, M. H., Gardeshi, M., & Alaghband, M. R. (2011). Practical attacks on a RFID authentication protocol conforming to EPC C-1 G-2 standard. *arXiv preprint* arXiv:1102.0763.
135. Alavi, S. M., Baghery, K., & Abdolmaleki, B. (2014). Security and privacy flaws in a recent authentication protocol for EPC C1 G2 RFID tags. *Advances in Computer Science: an International Journal (ACSIJ), 3*(5), 44–52.
136. Pang, L., He, L., Pei, Q., & Wang, Y. (2013). Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 standard. In *2013 IEEE Wireless communications and networking conference (WCNC)* (pp. 1870–1875). IEEE.
137. Wang, S., Liu, S., & Chen, D. (2015). Security analysis and improvement on two RFID authentication protocols. *Wireless Personal Communications, 82*(1), 21–33.
138. Phan, R. C. W. (2009). Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. *IEEE Transactions on Dependable and Secure Computing, 6*(4), 316–320.
139. Hernandez-Castro, J. C., Tapiador, J. M., Peris-Lopez, P., & Quisquater, J. J. (2009). Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations. In *International workshop on coding and cryptography*.
140. Tagra, D., Rahman, M., & Sampalli, S. (2010). Flaws in a recent ultralightweight RFID protocol. In *International conference on software telecommunications and computer networks, Croatia* (pp. 6–10).
141. Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., & Ribagorda, A. (2009). An ultra-light authentication protocol

resistant to passive attacks under the Gen-2 specification. *Journal of Information Science and Engineering, 25*(1), 33–57.
142. Wang, S. H., & Wang, G. L. (2010). Analysis of passive attack on RFID authentication protocol ULAP. *Networks and Communications, 36,* 17–19.
143. Zhuang, X., Wang, Z. H., Chang, C. C., & Zhu, Y. (2013). Security analysis of a new ultralightweight RFID protocol and its improvement. *Journal of Information Hiding and Multimedia Signal Processing, 4*(3), 165–180.
144. Jeon, I. S., & Yoon, E. J. (2013). Cryptanalysis and improvement of a new ultralightweight rfid authentication protocol with permutation. *Applied Mathematical Sciences, 7,* 3433–3444.
145. Zhuang, X., Zhu, Y., & Chang, C.C. (2013). Security analysis of ultralightweight RFID protocols. *Technique Report.*
146. Avoine, G., & Oechslin, P. (2005). A scalable and provably secure hash-based RFID protocol. In *Proceedings of the third IEEE international conference on pervasive computing and communications workshops* (pp. 110–114). IEEE.
147. Henrici, D., & Müller, P. (2008). Providing security and privacy in RFID systems using triggered hash chains. In *Proceedings of the sixth annual IEEE international conference on pervasive computing and communications* (pp. 50–59). IEEE.
148. Molnar, D., Soppera, A., & Wagner, D. (2005). A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In *International workshop on selected areas in cryptography* (pp. 276–290). Springer, Berlin, Heidelberg.
149. Dimitriou, T. (2006). A secure and efficient RFID protocol that could make big brother (partially) obsolete. In *Fourth annual ieee international conference on pervasive computing and communications* (pp. 6). IEEE.
150. Avoine, G., Coisel, I., & Martin, T. (2010). Time measurement threatens privacy-friendly RFID authentication protocols. In *International workshop on radio frequency identification: Security and privacy issues* (pp. 138–157). Springer, Berlin, Heidelberg.
151. Figueiredo, R., Zúquete, A., & e Silva, T. O. (2014). Massively parallel identification of privacy-preserving vehicle RFID tags. In *International workshop on radio frequency identification: Security and privacy issues* (pp. 36–53). Springer International Publishing.
152. Rohr, A., Nohl, K., & Plötz, H. (2010). *Establishing Security Best Practices in Access Control*. Berlin, Germany: Security Research Labs.
153. Kumar, V. N., & Srinivasan, B. (2012). Evolution of electronic passport scheme using cryptographic protocol along with biometrics authentication system. *International Journal of Computer Network and Information Security, 4*(2), 50.
154. Hwang, R. J., Su, F. F., & Tsai, Y. C. (2010). Efficient electronic toll collection protocol for intelligent transport system. *Journal of Computer Science, 21*(3), 18–26.
155. Nair, L. S., Arun, V. S., & Joseph, S. (2015). Secure e-ticketing system based on mutual authentication using RFID. In *Proceedings of the third international symposium on women in computing and informatics* (pp. 673–677). ACM.
156. Calypso Secure (2014). https://www.calypsonet asso.org/secure. Accessed 09 March 2017.
157. Schalk, G. H. (2013). *RFID: MIFARE and contactless cards in application*. Limbricht: Elektor Publishing.
158. UCODE. http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/ucode:MC_50483. Accessed 20 March 2017.

Alaauldin Ibrahim received the B.S. degree in Computer Engineering from University of Mosul, Mosul, Iraq, in 2005, the M.S. degrees in Computer Science from Dokuz Eylul University, Izmir, Turkey, in 2011. He is currently progress his Ph.D. degree in Computer Engineering in Dokuz Eylul University, Izmir, Turkey. His research areas are RFID technology, wireless sensor networks and computer networks.

Gokhan Dalkilic received the B.S. degree in Computer Engineering from Ege University, Izmir, Turkey, in 1997, the M.S. degrees in Computer Science from University of Southern California, Los Angeles, USA, in 1999, and from Ege University International Computing Institute, Izmir, Turkey, in 2001, and Ph.D. degree in Computer Engineering from Dokuz Eylul University, Izmir, Turkey, in 2004. He had been a visiting lecturer in University of Central Florida, Orlando, USA from January 2003 to December 2003. He has been an Assistant Professor of the Department of Computer Engineering of Dokuz Eylul University, Izmir, Turkey since 2004. His research areas are cryptography, statistical language processing and computer networks.