Ad Hoc Networks 11 (2013) 383–396

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems

Robin Doss *, Saravanan Sundaresan, Wanlei Zhou

School of Information Technology, Deakin University, Australia

ARTICLE INFO

Article history:
Received 12 February 2012
Received in revised form 29 May 2012
Accepted 20 June 2012
Available online 24 July 2012

Keywords:
RFID systems
Security protocols
Authentication
Privacy

ABSTRACT

In this paper we propose a novel approach to authentication and privacy in mobile RFID systems based on quadratic residues and in conformance to EPC Class-1 Gen-2 specifications. Recently, Chen et al. (2008) [10] and Yeh et al. (2011) [11] have both proposed authentication schemes for RFID systems based on quadratic residues. However, these schemes are not suitable for implementation on low-cost passive RFID tags as they require the implementation of hash functions on the tags. Consequently, both of these current methods do not conform to the EPC Class-1 Gen-2 standard for passive RFID tags which from a security perspective requires tags to only implement cyclic redundancy checks (CRC) and pseudo-random number generators (PRNG) leaving about 2.5k–5k gates available for any other security operations. Further, due to secure channel assumptions both schemes are not suited for mobile/wireless reader applications. We present the collaborative authentication scheme suitable for mobile/wireless reader RFID systems where the security of the server–reader channel cannot be guaranteed. Our schemes achieves authentication of the tag, reader and back-end server in the RFID system and protects the privacy of the communication without the need for tags to implement expensive hash functions. Our scheme is the first quadratic residues based scheme to achieve compliance to EPC Class-1 Gen-2 specifications. Through detailed security analysis we show that the collaborative authentication scheme achieves the required security properties of tag anonymity, reader anonymity, reader privacy, tag untraceability and forward secrecy. In addition, it is resistant to replay, impersonation and desynchronisation attacks. We also show through strand space analysis that the proposed approach achieves the required properties of agreement, originality and secrecy between the tag and the server.

1. Introduction

Radio Frequency Identification (RFID) is a technology that enables the non-contact, automatic and unique identification of objects using radio waves [1]. RFID technology was first used in the IFF (Identify Friend or Foe) aircraft system during World War II. However, its use for commercial applications has recently become attractive with RFID technology seen as the replacement for the optical barcode system that is currently in widespread use [2]. RFID has many advantages over the traditional barcode. It can be applied to different objects (optical barcodes must have a flat surface), it provides read/write capability (optical barcodes are read only), it does not require line-of-sight contact with readers (optical barcodes do) and more than one tag can be read at the same time (optical barcodes can only be read one at a time) [2,3]. These advantages have the potential to significantly increase the efficiency of decentralised business environments such as logistics and supply chain management particularly in the fields of inventory control, distribution and transportation [4].

It is estimated that the the RFID market in 2008 was worth USD 5.2 billion [5]. However, a major proportion

* Corresponding author. Tel.: +61 3 92517305; fax: +61 3 92517604.
E-mail address: robin.doss@deakin.edu.au (R. Doss).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.06.015

of this value was due to large national RFID schemes such as the national ID (in China) and asset tracking (as in the US Dept. of Defense [3]). The demand for such traditional RFID applications is nearing saturation requiring the development of novel applications to achieve the projected growth of more than USD 25 billion in 2018 [5].

The attractiveness of RFID technology as a replacement for the traditional barcode system has necessitated the need for securing RFID systems. An important aspect of RFID security is mutual authentication of the tag, reader and back-end server [6,7]. Mutual authentication is required to ensure that tag information is made available to only valid reader and server systems and that readers and servers are communicating with legitimate tags. Additionally, privacy of communication also needs to be achieved. Further, for any scheme to be practical it needs to achieve compliance with industry standards and specifications.

The EPC Class-1 Gen-2 standard [8] has evolved as the industry standard for RFID tags. From a security perspective it requires tags to only implement cyclic redundancy checks (CRCs) and pseudo random number generators (PRNGs). Based on this specification and with the aim of keeping the cost of tags low, EPC Class-1 Gen-2 tags have limited number of gates available for additional security purposes. The limited processing and storage capability of the RFID tags limits the effective use of cryptographic techniques as there are roughly $2.5k$–$5k$ equivalent gates available for security purposes on a standard chip [9]. This is insufficient for standard cryptographic techniques such as RSA [9]. Further, the use of established security primitives such as one-way hash functions is not possible. As noted by Chen et al. [10] established hash functions such as SHA-1 and MD5 require between $16k$ and $20k$ gates for implementation. This is clearly infeasible for low-cost RFID tags. However, quadratic residues based on modular squaring operations require only a few hundred gates for implementation making them an attractive option for securing low cost EPC Class-1 Gen-2 tags [10,11].

We also note that while cheaper cryptographic alternatives such as Elliptic Curve Cryptography (ECC) exist and authentication schemes such as ERAP [12] based on ECC have been proposed for RFID systems. However, as demonstrated by Batina et al. [13], implementation of ECC would require between $8.2k$ and $15k$ equivalent gates which is beyond the capabilities of low cost RFID tags – the efficient implementation of ECC for RFID tags is still an open research problem.

Many RFID applications use fixed RFID readers, where the channel between the RFID reader and the server is assumed to be secure. However, emerging applications of RFID such as the "Green Taxi" service and the fraudulent wine produce detection in Korea involve mobile RFID readers [14]. In the green taxi service, a passenger is able to retrieve the details regarding the taxi that they are traveling in based on the in-taxi RFID tag using a RFID-enabled mobile device (such as a smartphone). They can then transmit these details to friends and family, who are then able to track their location. However, insecure transmission of information over the wireless channel between the mobile reader and the back-end server can cause reader/owner privacy disclosure.

While there has been considerable work on authentication and privacy in RFID systems, these are concentrated on achieving security properties only between the RFID reader and the RFID tag [3,15–17,10,18,11]. Further, most schemes make the assumption of the existence of a secure channel between the reader and the server and are not suited for mobile/wireless RFID readers. Emerging applications with mobile/wireless enabled RFID readers require security and privacy properties to be achieved over both the tag–reader channel and the reader–server channel as both channels are open to compromise. Hence the motivation for our work. In this paper our main contributions can be summarized as:

- A novel approach to authentication and privacy in RFID systems based on quadratic residues and in conformance to EPC Class-1 Gen-2 specifications. Our scheme requires tags to perform modulo squaring, bitwise operations (XOR, multiplications), CRC calculations and pseudo random number generation (e.g., LAMED [19]) . All of these are within the capabilities of low-cost RFID tags [20,21].
- A collaborative authentication scheme suited to RFID systems with mobile/wireless readers where both the tag–reader channel and the reader-server channel are insecure.

The main distinctions between our work and the work of Chen et al. [10] and Yeh et al. [11] are:

- We do not require the tag to compute hash functions. Chen and Yeh require 3 and 4 hash functions to be implemented respectively.
- Our scheme takes into account the insecure nature of the reader-server channel and achieves, reader authentication, reader anonymity and reader location privacy explicitly. Chen and Yeh do not explicitly achieve these properties.
- Our scheme is suited for mobile/wireless reader RFID systems while Chen and Yeh's schemes are not as they make secure channel assumptions with regards to the server–reader channel.

The required security properties to achieve authentication and privacy in RFID systems can be summarized as follows [18,22–24]:

- *Tag anonymity (P1)*: The protocol should protect against information leakage that can lead to disclosure of a tag's real identifier. This is important as otherwise an attacker may be able to clone a valid tag.
- *Tag location privacy (P2)*: The protocol should ensure that the message contents are sufficiently randomized to ensure that they cannot be used to track the location(s) of the tags and thereby glean social information about the wearer of the tag.
- *Forward secrecy (P3)*: The protocol should ensure that on compromise of the internal secrets of the tag, its previous communications cannot be traced by the attacker. This requires that previous messages are not dependent on current resident data on the tag.

- *Reader anonymity (P4)*: The protocol should protect against information leakage that can lead to disclosure of a reader's real identifier. This is important as otherwise an attacker may be able to clone a valid reader.
- *Reader location privacy (P5)*: The protocol should ensure that the message contents are sufficiently randomized to ensure that they cannot be used to track the location(s) of the readers and thereby glean social information about the owner.
- *Replay attacks (A1)*: The protocol should be able to resist compromise by an attacker through the replay of messages that have been collected by an attacker during previous protocol sequences. This requires that protocol messages in each round of the protocol are unique.
- *Desynchronisation attack (A2)*: The protocol should be able to recover from incomplete protocol sequences that can occur due to an attacker selectively blocking messages. Importantly, such blocking of messages by an attacker should not lead to desynchronisation between the tag and the server/reader.
- *Server impersonation (A3)*: The protocol should ensure that the server cannot be impersonated by an attacker. This requires that the tag/reader challenges a server to prove its legitimacy thereby achieving mutual authentication.

The rest of this paper is organized as follows. In Section 2 we present related work with an overview of the two quadratic residues based schemes proposed by Chen et al. [10] and Yeh et al. [11]. In Section 3 we present our approach based on quadratic residues followed by a detailed security analysis and performance comparison of our scheme in Section 4. Section 5 concludes the work.

2. Related work

The need for security and privacy in RFID systems is well recognized and there has been a significant amount of work in this area [25,24,26,22,23,27]. However, the practical implementation of most schemes are limited by three main factors. Firstly, many schemes do not achieve conformance to EPC Class 1 Gen-2 standards and hence cannot be implemented on low cost tags which cannot support complex computation (such as hash functions). Secondly, schemes that are compliant to EPC Class 1 Gen-2 standards do not provide robust security in terms of authentication and privacy. Thirdly, most schemes assume that the channel between the back-end server and the reader is secure and hence they are not suitable in mobile/wireless reader environments where this assumption does not hold.

Early approaches to deal with the security problem in RFID systems include the use of shared secrets with the use of a pseudorandom function ensemble [28]; hash chains to update a shared random identifier [15]; monotonically increasing session hashes to prevent replay attacks [29]; shared secrets and random nonces [30]; monotonically increasing timestamps [16]; and the use of XOR (exclusive OR), hash chains and a shared secret key between the reader and the back end server for reader tag authentication [17]. Security flaws and protocol vulnerabilities can be identified in all these schemes [31].

In 2004, Juels proposed a "Yoking proof" based on keyed hash functions and message authentication code (MAC) functions for pharmaceutical applications [6]. However, Juels' scheme fails to provide tag anonymity and is not resistant to replay attacks and chosen plain-text attacks [10]. In 2005, Wong et al. [7] proposed the "hash-lock" scheme which was also found to have several security weaknesses. Specifically, it does not provide location privacy and is not resistant to replay and server impersonation attacks [10]. Further, since both schemes require the implementation of hash functions on the tags they are not EPC Class-1 Gen-2 compliant.

In 2007, Chien and Chien [20], proposed a mutual authentication protocol that achieves EPC Class-1 Gen-2 compliance and is based on random nonces and CRC calculations. However, it suffers from significant security drawbacks. Cryptanalysis of Chien's scheme by Peris-Lopez et al. [32], shows that it cannot guarantee the unequivocal identification of tags, forward secrecy and location privacy of tags. It is also observed that it is not robust to resist tag impersonation and auto-desynchronisation attacks. Lo et al. [33] proposed an improvement to Chien's scheme but it still does not address the location privacy concern and can be compromised by collaborating readers [34]. In the scheme by Yeh et al. [34], Chien's and Lo's schemes are improved with the added security property of reader authentication. Reader authentication is based on a hash value calculated over a reader identifier and a random number. The scheme may be susceptible to auto-desynchronisation as it requires synchronization of three different values between the tag and the server. The database index (C_i), the access key (P_i) and the authentication key (K_i) are all updated during each successful authentication. Also, from the tag's computational point of view this can be inefficient. More importantly however, Yeh's scheme does not satisfy the required security properties and is susceptible to server impersonation and data integrity attacks as the server is not challenged by the tag and server data is transmitted in the clear. Similar to Yeh's scheme, Cho et al. [35] proposed a hash-based scheme that does not make secure channel assumptions. However, cryptanalysis of the scheme by Safkhani et al. [36] has shown that the scheme is vulnerable to desynchronisation, tag impersonation and reader impersonation attacks.

Chen and Deng's scheme [37] is based on CRC and PRNG functions and suitable for implementation on EPC Class-1 Gen-2 tags. However, the use of CRC functions makes it possible for attackers to exploit the completely linear property of the CRC function [32] and Kapoor et al. [38] have recently shown that Chen and Deng's scheme is vulnerable to impersonation attacks. Further, each reader and each tag is required to hold in memory n parameters and n key values. While this might be possible for readers, it places severe storage constraints on the tags. We also not that the tag is required to perform $(n + 1)$ CRC calculations each round to verify whether a reader is a legal reader. This is not ideal.

Chien and Laih [18] have proposed a lightweight security scheme based on error correction codes with secret

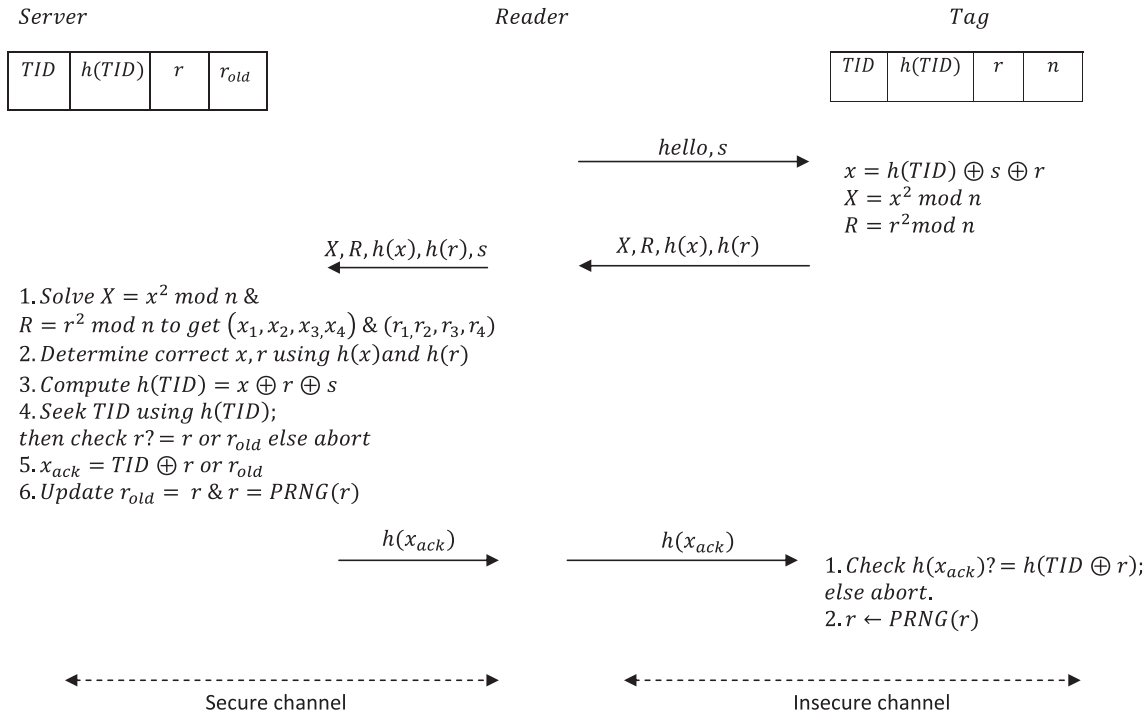


Fig. 1. Chen et al.'s mutual authentication scheme based on quadratic residues.

parameters. Schemes based on error correction codes are attractive as they can be robust to desynchronisation attacks since they do not require regular updating of tag secrets. They work on the principle that the tag introduces random error vectors into the communication with the server which the server is able to remove using the secret generator matrix and secret parity matrix. Thus the communicating tag can be identified uniquely. Chien and Laih's scheme is based on secret linear codes, PRNG and a secret key. The main drawback of the scheme lies in the scalability of the model with respect to storage requirements. With EPC Class-1 Gen-2 tags, with a linear code of length 128, dimension 1024 and distance 22 and with a secret key of 256 bits, if the number of row vectors assigned to each tag is 3 the system will only be able to support 341 tags. More importantly, the storage requirement on each tag to support this many tags would be $3 * 1024 + 256 = 3328$ bits ≈ 416 bytes. As noted by the authors themselves this is clearly not suitable for large scale applications as the storage requirement on each tag would be very large and infeasible.

In [39] Liu and Bailey have proposed the privacy and authentication protocol (PAP) specifically for a retail environment. It is based on a shared key between the reader and the tag, a privacy state and hash value computation by the tag and the reader. Variations of the protocol are proposed for check-out, in-store, out-store and return actions that are common in a retail environment. However, PAP fails to provide tag anonymity as the tag identifier is transmitted in the clear. The authors argue that this is acceptable since the protocol is designed specifically for a controlled environment. In addition, PAP fails to comply with EPC Class-1 Gen-2 standards. Further, vulnerability analysis of PAP by Nasser et al [40] shows that PAP suffers from traceability and impersonation attacks.

In [10], Chen et al. proposed the first mutual authentication scheme based on quadratic residues. The scheme was designed to achieve mutual authentication, tag privacy and resistance to replay and desynchronisation attacks. However, cryptanalysis of this scheme by Cao and Shen [41] shows that the scheme is vulnerable to tag impersonation attacks, replay attacks and tag location disclosure. Chen's scheme was improved by Yeh and Wu [11] by having the tag generate an additional random number. We provide a detailed description of the two quadratic residues based schemes below.

2.1. Review of Chen et al.'s quadratic residue based mutual authentication scheme

Chen et al.'s scheme has two phases: initialization and authentication. It proceeds as follows (Fig. 1).

In the initialisation phase, the server generates two large prime numbers p and q and computes $n = pq$. It proceeds to choose a one-way hash function $h(\cdot)$ and a pseudo-random number generator $PRNG(\cdot)$. The server makes the value of n and $h(\cdot)$ public. The server sets up the tag by choosing a random number r that serves as a shared secret and writes TID, $h(TID)$ and r into the tag's memory. TID includes EPC codes depending on the user's specification. The server maintains a record of the form $\langle h(TID), TID, r, r_{old}\rangle$ for each tag in its database. Initially, $r_{old} = r$ and $h(TID)$ serves as the primary key.

The authentication phase proceeds as follows:

Step 1: Reader → Tag
The reader generates a random challenge s and it broadcasts a "hello" message to the tag along with s.

Step 2: Tag → Reader
On receiving the reader's challenge, the tag proceeds to compute $x = h(TID) \oplus r \oplus s$ using the challenge from the reader and TID, $h(TID)$ and r from its memory. It also computes $X = x^2 \bmod n$ and $R = r^2 \bmod n$. It forwards to the reader $\langle X, R, h(x), h(r) \rangle$.

Step 3: Reader → Tag
Once the reader receives the tag's response $\langle X, R, h(x), h(r) \rangle$it forwards this information along with s to the server over the secure server–reader channel.

Step 4: Server → Tag
When the server receives $\langle X, R, h(x), h(r), s \rangle$, the server solves $X = x^2 \bmod n$ and $R = r^2 \bmod n$ by using the Chinese Reminder Theorem, obtaining four roots (x_1, x_2, x_3, x_4) and (r_1, r_2, r_3, r_4) respectively. It then compares $h(x_i)$ with $h(x)$ and $h(r_i)$ with $h(r)$ where $i = 1$–4 to determine the unique values of x and r. The server then computes $x \oplus r \oplus s$, obtaining $h(TID)$. Using $h(TID)$ the server locates the tag record in the database. If it is not found, the server will abort the session. If found, the server verifies that the solved r is equal to the value of r or r_{old} in the record that it retrieved from the database. If the resulting r is equal to the r in the tag record, the server computes $h(x_{ack}) = h(TID \oplus r)$ and sends it to the reader. It then sets $r_{old} = r$ and $r \leftarrow PRNG(r)$. On the other hand, if the resulting r is equal to r_{old} in the tag record, the server computes $h(x_{ack}) = h(TID \oplus r_{old})$ and sends it to the reader. Neither r nor r_{old} stored in the server is updated.

Step 5: Reader → Tag
Once the tag receives the $\langle h(x_{ack}) \rangle$ from the server via the reader, it verifies if $h(TID \oplus r) = \langle h(x_{ack}) \rangle$. If correct, the tag updates r with $PRNG(r)$; else it aborts.

2.2. Review of Yeh et al.'s improved quadratic residue based mutual authentication scheme

Yeh et al.'s scheme has two phases – initialisation and authentication (Fig. 2). The initialization phase remains the same as in Chen et al's scheme with the authentication phase as follows:

Step 1: Reader → Tag
The reader generates a random challenge s and sends it with a "hello" message to the tag.

Step 2: Tag → Reader
Once the tag receives the challenge s from the reader it generates a random number t and computes $x = h(TID) \oplus r \oplus s \oplus t$, $y = r \oplus t$, $X = x^2 \bmod n$, $R = (r^2 \bmod n) \oplus t$ and $T = t^2 \bmod n$. The tag then sends $\langle X, R, T, h(x), h(y), h(t) \rangle$ to the reader.

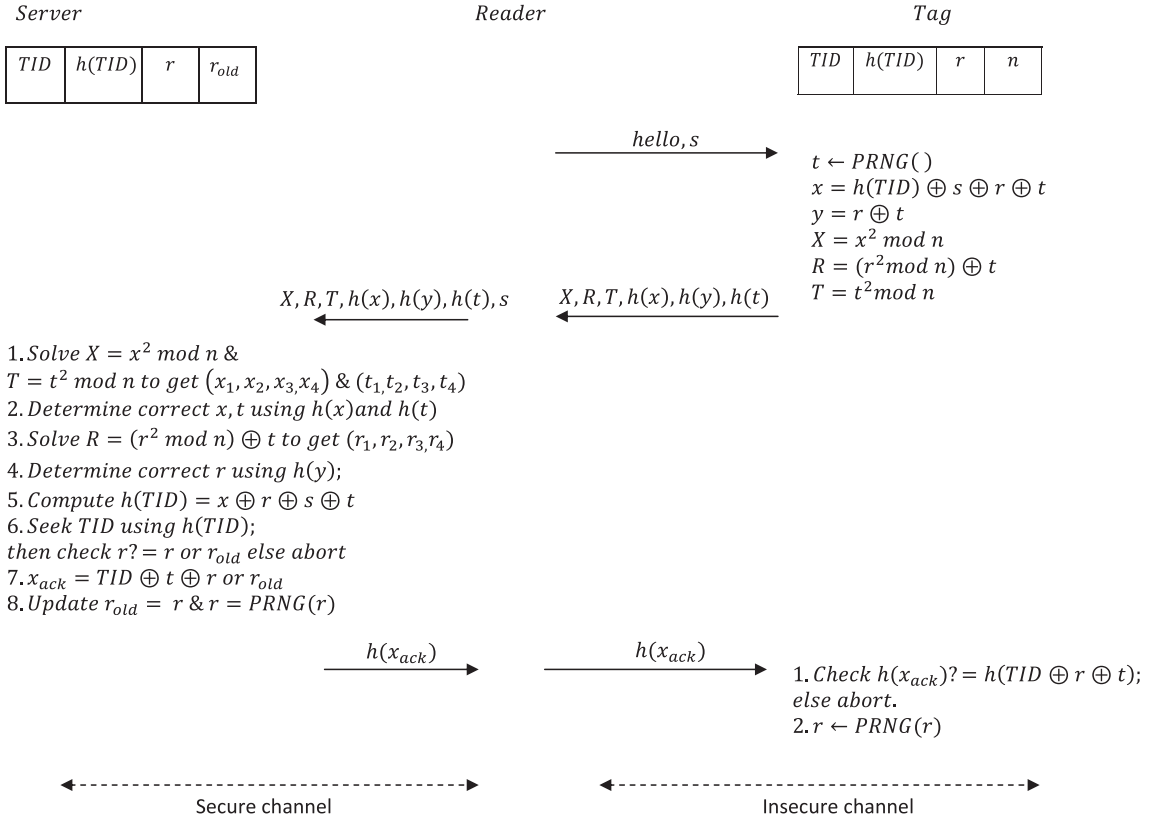


Fig. 2. Yeh et al.'s mutual authentication scheme based on quadratic residues.

Step 3: Tag → Reader
Once the reader receives the tag's response, it forwards this response together with s to the server over the secure reader–server channel.

Step 4: Reader → Server
On receiving $\langle X, R, T, h(x), h(y), h(t), s\rangle$ from the reader, the server solves $X = x^2 \bmod n$ and $T = t^2 \bmod n$ using the Chinese Reminder Theorem and p and q to obtain the roots (x_1, x_2, x_3, x_4) and (t_1, t_2, t_3, t_4) respectively. It then compares $h(x_i)$ with $h(x)$ and $h(t_i)$ with $h(t)$ for $i = 1$–4 to determine the unique values of x and t. The server then proceeds to compute $R \oplus t = (r^2 \bmod n)$ and solves for r using the Chinese Reminder Theorem with p and q to obtain the four roots (r_1, r_2, r_3, r_4). It then compares $h(r_i \oplus t)$ with $h(y)$ where $i = 1$–4 to determine the unique value of r. The server then computes $x \oplus r \oplus s \oplus t$ to get $h(TID)$ and uses it to locate the tag's record on the server. The server aborts if a match is not found. If a match is found the server verifies if the solved r is equal to the stored values of r or r_{old}; else it aborts. If the resulting r is equal to the r in the tag record, the server computes $h(x_{ack}) = h(TID \oplus t \oplus r)$ and sends it to the reader. It then sets $r_{old} = r$ and $r \leftarrow PRNG(r)$. On the other hand, if the resulting r is equal to r_{old} in the tag record, the server computes $h(x_{ack}) = h(TID \oplus t \oplus r_{old})$ and sends it to the reader. Neither r nor r_{old} stored in the server is updated.

Step 5: Reader → Tag
Once the reader receives $h(x_{ack})$ from the server, it forwards it to the tag. The tag verifies if the received $h(x_{ack})$ is equal to $h(TID \oplus t \oplus r)$. If it is then the tag updates r with $PRNG(r)$.

2.3. Analysis of Chen et al.'s and Yeh et al.'s schemes

Chen et al.'s scheme has been shown to be vulnerable to tag impersonation attacks, replay attacks and location privacy compromise [11,41]. In Chen's scheme, the tag does not generate random numbers for each session which makes it vulnerable to tag impersonation. To impersonate a tag, the adversary records R and $h(r)$ in step (2) followed by malicious queries to cheat the tag out of responses three times. The adversary then derives the secret value $h(TID) \oplus r$ allowing it to impersonate the tag using this value and the recorded value of R and $h(r)$. For the detailed attacking steps we refer the reader to [41].

The scheme is also vulnerable to replay attacks. By blocking or modifying step $h(x_{ack})$ in step (5), the adversary can prevent the tag from updating r. Since $h(x_{ack})$ is a function of TID and r, an attacker can simply replay the recorded value of $h(x_{ack})$ from the previous round to achieve successful authentication with the tag.

Finally, Chen's scheme does not achieve location privacy. By blocking or modifying step $h(x_{ack})$ in step (5), the adversary can prevent the tag from updating r. Consequently, in the next reading of the tag, R and $h(r)$ will remain unchanged. Consequently, tracing of the tag becomes trivial for an adversary.

Yeh et al.'s scheme addresses these security vulnerabilities by requiring the tag to generate a random number t for each tag interaction. However as is clear, both Chen's original quadratic residue based scheme and Yeh's improved version require the tag to compute multiple hash functions. Hence both schemes are not suitable for EPC Class-1 Gen-2 tags. Further, both schemes assume the existence of a secure server-reader channel. Hence they are not applicable in environments where this cannot be guaranteed such as in wireless/mobile reader applications.

We finally note that though the EPC Class-1 Gen-2 tags are severely resource constrained, hash functions such as SQUASH by Shamir [21] for implementation on low-cost RFID tags have been proposed. Shamir's scheme is based on the Rabin Cryptosystem and is designed to serve as a message authentication code (MAC). It is therefore not protected against information leakage [21] and so not suited for environments such as RFID systems that need to ensure that the privacy of the tag is also preserved. In addition, Shamir's scheme was proven to be not provably secure by Ouafi and Vaudenay [42]. It was also shown by Gosset et al that implementation of SQUASH would require up to 6000 gates [43]. While this is certainly an improvement on methods such as SHA-1, that require close to 10000 gates, it is still not suited to the computational constraints of EPC Class-1 Gen-2 tags. This further highlights the difficulty of implementing secure hash functions on low-cost RFID tags.

3. The proposed scheme

In this section we present our proposed approach based on the quadratic residue property that can achieve the security requirements of current and emerging RFID systems/applications. Our scheme is designed to be in conformance with EPC Class-1 Gen-2 standards [8] as we do not employ encryption functions or hash functions. We firstly describe the quadratic residue property followed by the details of our collaborative authentication scheme.

3.1. The quadratic residue property

If n is a positive integer, then R is said to be the quadratic residue of n if $(n, R) = 1$ and the congruence $x^2 \equiv R \bmod n$ has a solution. Suppose that $n = pq$ where $p \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$ are distinct large primes and that the congruence $x^2 \equiv R \bmod n$ has a solution $x = x_o$. From the Chinese Remainder Theorem there are exactly four incongruent solutions of the congruence $x^2 \equiv R \bmod n$ (i.e., R has four incongruent square roots modulo n). However, in order to be able to compute these solutions, knowledge of p and q is required. Due to the difficulty of factoring n it is computationally infeasible to find x satisfying $x^2 \equiv R \bmod n$ without knowing p and q [10,44]. Without loss of generality, if x is replaced with x^2, and if a solution exists for $(x^2)^2 \equiv R \bmod n$, it is clear that the solution is required to be a perfect square (x^2). However, of the four possible solutions (obtained using the Chinese Remainder theorem) only one of those would be a

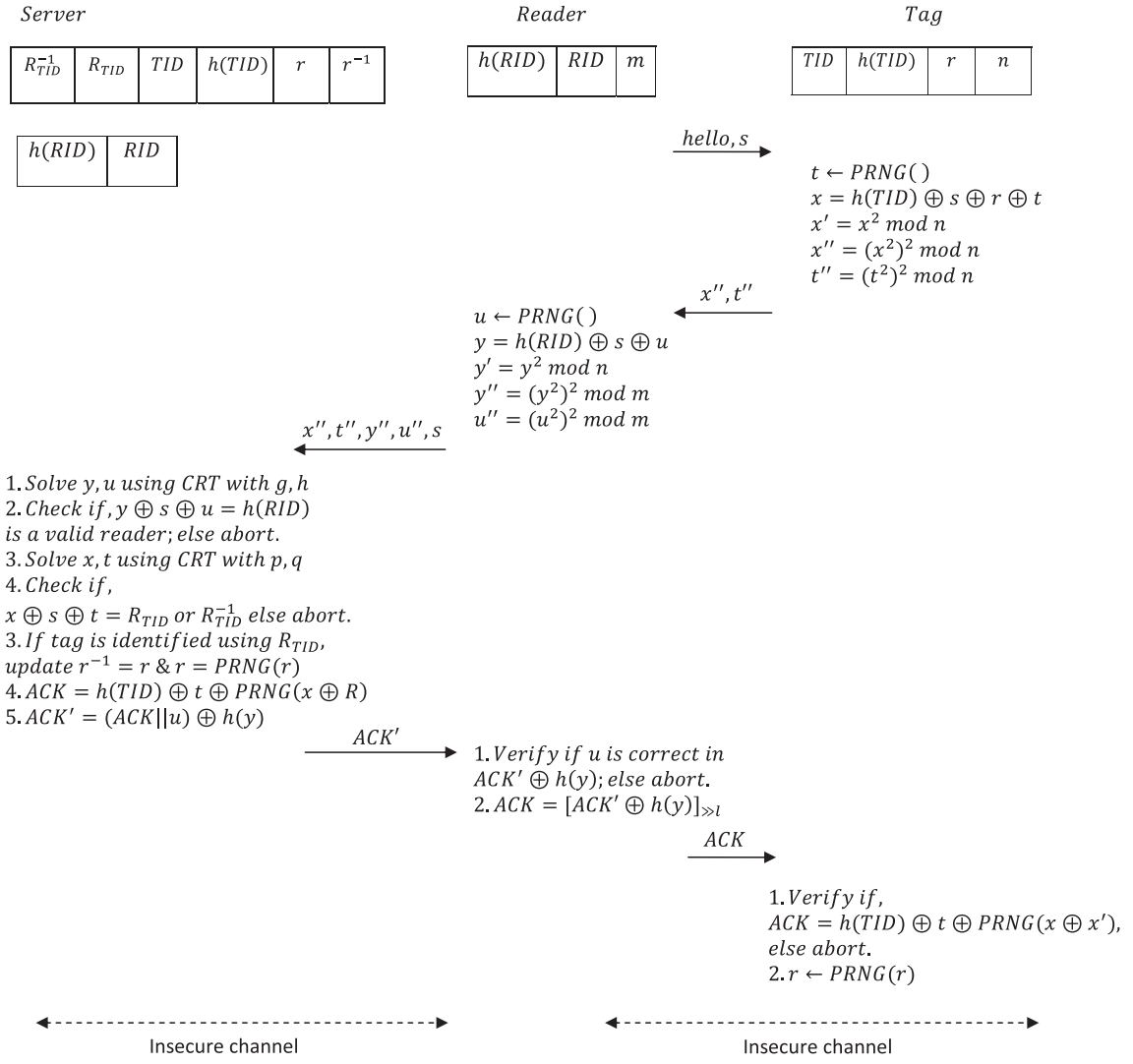


Fig. 3. The collaborative authentication scheme based on unique quadratic residues.

quadratic residue modulo n satisfying $x^2 \equiv R \bmod n$ [44] (see pp. 421–427). Our proposed scheme is based on this uniqueness property of the quadratic residue while the schemes by Chen et al. [10] and Yeh et al. [11] are not. As a result we are able to eliminate the need for the use of hash-functions by the tag. The details of our proposed scheme are presented below.

3.2. Collaborative authentication scheme based on unique quadratic residues

In our collaborative authentication scheme (Fig. 3) we do not assume the existence of a secure channel between the back-end server and the reader. Hence security properties need to be achieved over both the reader–tag and the reader–server channels. The collaborative authentication scheme has two phases: an initialization phase and an authentication phase. We describe the two phases below.

3.2.1. The initialization phase

The server generates four large prime numbers p, q, g and h and computes $n = pq$ and $m = gh$. It also decides upon a hash function $h(\cdot)$ and a $PRNG(\cdot)$. Each valid reader and tag in the system is uniquely identified with *RID* and *TID* respectively. For each valid tag in the system the server computes $R_{TID} = h(TID) \oplus r$ and $R_{TID}^{-1} = h(TID) \oplus r^{-1}$ where r is a random number and r^{-1} is the previous value of r. Initially $r = r^{-1}$. For each valid tag in the system the server stores a record of the form $\langle R_{TID}, R_{TID}^{-1}, TID, h(TID), r, r^{-1} \rangle$. Each tag is initialized with $\langle TID, h(TID), n, r \rangle$. For each valid reader in the system the server stores a record of the form $\langle RID, h(RID) \rangle$ and each reader is initialized with $\langle RID, h(RID), m \rangle$.

3.2.2. The collaborative authentication phase

The authentication phase in our scheme proceeds as follows.

Table 2
Performance comparison.

Scheme	Rounds	Tag	Reader	Server	Security assumption	EPCC1G2 compliance	Database loading (worst case)
Juels [6]	6	3Hash	None	4Hash	Yes	No	$O(1)$
Wong et al. [7]	5	1Hash	None	1Hash	Yes	No	$O(n)$
Chien and Chien [20]	5	1CRC 2PRNG	1PRNG	n+1CRC 2PRNG	Yes	Yes	$O(n)$
Chen et al. [10]	5	3Hash 2modulo squaring 1PRNG	1PRNG	10Hash 1PRNG 2Square root solving	Yes	No	$O(1)$
Yeh et al. [11]	5	4Hash 3modulo squaring 2PRNG	1PRNG	14Hash 3Square root solving 1PRNG	Yes	No	$O(1)$
Lo and Yeh [33]	5	7PRNG 3CRC	None	10PRNG 2CRC	Yes	Yes	$O(1)$
Yeh and Wang [34]	5	7PRNG	1PRNG	6PRNG	No	Yes	$O(n)$
Chen and Deng [37]	5	2CRC 1PRNG	2CRC, 1PRNG	Not Involved	Yes	Yes	$O(n)$
Liu and Bailey [39]	4	2Hash 1PRNG	1Hash 1PRNG	Not involved	Yes	No	$O(1)$
Cho et al. [35]	5	2Hash 1PRNG	1PRNG	1Hash 1PRNG	No	No	$O(n)$
Our collaborative authentication scheme	5	3modulo squaring 3PRNG	2PRNG 3modulo squaring 1Hash	2Square root solving 1PRNG	No	Yes	$O(1)$

Step 1: Reader → Tag
The reader sends a "hello" message along with a unique challenge s to the tag.

Step 2: Tag → Reader
On receiving the challenge s, the tag computes $x = h(TID) \oplus r \oplus s \oplus t$ where $t \leftarrow PRNG(\cdot)$ The tag also computes $x' = x^2 \bmod n$, $x'' = (x^2)^2 \bmod n$ and $t'' = (t^2)^2 \bmod n$. The tag sends $\langle x'', t'' \rangle$ to the reader.

Step 3: Reader → Server
On receiving the tag's response $\langle x'', t'' \rangle$, the reader computes $y = h(RID) \oplus s \oplus u$ where $u \leftarrow PRNG(\cdot)$. The reader also computes $y' = y^2 \bmod n$, $y'' = (y^2)^2 \bmod n$ and $u'' = (u^2)^2 \bmod n$. The tag sends $\langle x'', t'', y'', u'', s \rangle$ to the server.

Step 4: Server → Reader
The server on receiving $\langle x'', t'', y'', u'', s \rangle$ from the reader, solves for the least positive residue Y of y^2 modulo m and U of u^2 modulo m using the Chinese Remainder Theorem [44]. The server is capable of doing this due to its knowledge of the factors of m, g and h. Using y'', g and h, the server is able to compute the four square roots of $y^4 \bmod n$ and identify the quadratic residue of $y^2 \bmod n$ and the value of y^2 using the Legendre symbols of these square roots modulo g and h. It is to be noted that without the knowledge of g and h it is infeasible to calculate the value of Y [44]. Similarly, the server is able to determine the value of U using u'', g, h and determine value of u^2 using the Legendre symbols of these square roots modulo g and h. The server then checks to see if $y \oplus s \oplus u = h(RID)$ matches a record on the server. If it does, then the server validates the reader as a valid reader and proceeds to authenticate the tag.
In order to authenticate the tag, the server solves for the least positive residue R of x^2 modulo n and T of t^2 modulo n using the Chinese Remainder Theorem [44]. The new server is capable of doing this due to its knowledge of the factors of n, p and q. Using x'', p and q, the new server is able to compute the four square roots of $x^4 \bmod n$ and identify the quadratic residue of $x^2 \bmod n$ and the value of x^2 using the Legendre symbols of these square roots modulo p and q. It is to be noted that without the knowledge of p and q it is infeasible to calculate the value of R [44]. Similarly, the server is able to determine the value of t using t'', p, q. The server then checks to see if $x \oplus s \oplus t = R_{TID}$ or R_{TID}^{-1}. If it matches a record on the server, the tag is authenticated as valid as it proves that the tag is in possession of the shared secret r or r^{-1}; else the server aborts the authentication request. If the tag is successfully authenticated, the server generates $ACK = h(TID) \oplus t \oplus PRNG(x \oplus R)$. It then computes $ACK' = (ACK \| U) \oplus h(y)$ and sends $\langle ACK' \rangle$ to the reader. Further, if the tag is identified using R_{TID} the server updates $r^{-1} = r$ and $r \leftarrow PRNG(r)$.

Step 5: Reader → Tag
The Reader on receiving $\langle ACK' \rangle$ verifies if u is correct in $ACK' \oplus h(y)$ by comparing with the l least significant bits of $ACK' \oplus h(y)$, where l is the length of u. If u is not matched the reader aborts. However, if correct, it proves to the reader, that the server is in possession of g,h the factors of m and

therefore the server is authenticated by the reader. The reader, then forwards, $\langle ACK \rangle$ to the tag, where $ACK = [ACK' \oplus h(y)]_{\gg l}$.

The tag on receiving *ACK* verifies using its local information if $ACK = h(TID) \oplus t \oplus PRNG(x \oplus x')$. If correct it proves that the server is in possession of p and q and was able to solve for the unique quadratic residues modulo n. The server is therefore authenticated by the tag and by implication it also authenticates the reader as a valid reader. The tag updates $r \leftarrow PRNG(r)$. On the other hand, if the received *ACK* does not match the local values, the tag aborts.

4. Security analysis

In this section we present the security analysis of the proposed protocols. We first prove the security correctness of the proposed approach using strand spaces to show that the scheme achieves the required properties of agreement, uniqueness and originality between the tag and the server [45].

We then present a series of claims and prove that the required security properties are achieved. We follow an approach similar to [10] for the security analysis which is consistent with other research in this area [11,39,34].

4.1. Security correctness

We first consider the security correctness of the proposed protocols. In order to prove the security correctness of the proposed scheme we undertake analysis using strand spaces [45]. As a result of the analysis we show that the proposed approach satisfies the required property of agreement, originality, uniqueness and secrecy between the tag and the server. We use the following notations for this purpose:

$\mathcal{P}$, Σ: penetrated strand space and strand space;
T, T_{name}: set of texts representing atomic messages;
$\mathcal{C}$: bundle;
K_P: set of keys known to the penetrator;
n_i: nodes in the strand space;
$\preceq$: precedence relationship;
$\sqsubset$: subterm relationship;
$\mathcal{S}_{\mathcal{AP}}$: the proposed protocol.

Definition 1. An infiltrated strand space Σ, $\mathcal{P}$ is a $\mathcal{S}_{\mathcal{AP}}$ space if Σ is the union of three kinds of strands:

- Penetrator strands $s \in \mathcal{P}$;
- Initiator strands $s \in Init[Tag_i, S_i, R, x]$ where $x = h(TID) \oplus s \oplus r \oplus t$, with trace: $\langle +\{hello, s\}, -\{x'', t''\}, +\{ACK\}\rangle$ where $Tag_i, S_i \in T_{name}$, $R, x \in T$ but $R \notin T_{name}$.
- Responder strands $s \in Resp[Tag_i, S_i, R, x]$ where $x = h(TID) \oplus s \oplus r \oplus t$, with trace $\langle -\{hello, s\}, +\{x'', t''\}, -\{ACK\}\rangle$ where $Tag_i, S_i \in T_{name}$, $R, x \in T$ but $x \notin T_{name}$.

4.2. The originality and uniqueness of x

Proposition 1.

1. Σ is a $\mathcal{S}_{\mathcal{AP}}$ space, $\mathcal{C}$ is a bundle in Σ and w is a responder strand in $Resp[Tag_i, S_i, R, x]$;
2. $K_s^{-1}(= \langle p, q \rangle) \notin K_P$;
3. $R \neq x$, s and x is uniquely originating in Σ.

Then $\mathcal{C}$ contains an initiator strand $v \in Init[Tag_i, S_i, R, x]$. We will prove this using a sequence of lemmas.

We fix an arbitrary Σ, $\mathcal{C}$, s, Tag_i, S_i, R, x satisfying the hypothesis of Proposition 1. The node $\langle s, 3\rangle$ receives the value $ACK = h(TID) \oplus t \oplus PRNG(x \oplus R)$; for ease of reasoning we will refer to this node as n_3 and to its term as v_3. The node $\langle s, 2\rangle$ outputs the value x'', t''; we will refer to this node as n_0 and its term as v_0.

Lemma 1. *x originates at n_0*

Proof. By the assumptions, $x \sqsubset v_0$ and the sign of n_0 is positive since it originates from Tag_i. Thus we need to show that $x \not\sqsubset n'$ where n' is the node $\langle s, 1\rangle$ preceding n_0 on the same strand. Since $\text{term}(n') = hello, s$ we need to check that $x \neq s$; this is true from the hypothesis since $s \sqsubset x$. Further, $x \neq hello$ from the stipulation that $x \notin T_{name}$. □

We next present the main lemma that establishes that the crucial step of solving for the quadratic residue of x using x'', p, q is performed on a regular strand and not a penetrator strand.

Table 1
Comparison of security and privacy properties.

Scheme	P1	P2	P3	P4	P5	A1	A2	A3
Juels [6]	No	No	✓	§	§	No	No	✓
Wong et al. [7]	✓	No	✓	§	§	No	✓	No
Chien and Chien [20]	✓	No	No	§	§	No	No	✓
Chen et al. [10]	✓	No	✓	§	§	No	✓	✓
Yeh et al [11]	✓	✓	✓	§	§	✓	✓	✓
Lo et al. [33]	✓	No	✓	§	§	✓	No	No
Yeh et al. [34]	✓	✓	✓	✓	✓	✓	No	No
Chen and Deng [37]	No	No	✓	§	§	✓	✓	No
Liu et al. [39]	No	No	No	§	§	No	✠	No
Cho et al. [35]	✓	✓	✓	✓	✓	✓	No	No
Our Collaborative Authentication Scheme	✓	✓	✓	✓	✓	✓	✓	✓

✓: Fully satisfied; §: Not fully satisfied (assumed); ✠: Not applicable. P1: Tag anonymity; P2: Tag location privacy; P3: Forward secrecy; P4: Reader privacy; P5: Reader location privacy; A1: Resistant to replay attacks; A2: Resistant to desynchronisation attacks; A3: Resistant to impersonation attacks.

Lemma 2. *The set* $S = \{n \in \mathcal{C} : x \sqsubset term(n) \wedge v_0 \not\sqsubset term(n)\}$ *has a* $\preccurlyeq$*-minimal node* n_2*. The node* n_2 *is regular and the sign of* n_2 *is positive.*

Proof. Because $n_3 \in \mathcal{C}$, and n_3 contains R (derived from x'', p, q) but not v_0, S is non-empty. Hence S has at least one $\preccurlyeq$-minimal node n_2 that is positive.

We now need to show that this node n_2 cannot lie on a penetrator strand p. We consider the various possible penetrator strands according to the trace of p.

M. The trace $tr(p)$ has the form $\langle +t \rangle$ where $t \in T$; hence we must have $t = x$. In this case x originates on this strand. But this is impossible as x originates uniquely on n_0 (Lemma 1).

K. The trace $tr(p)$ has the form $\langle +K_0 \rangle$ where $K_0 \in K_P$. But $x \not\sqsubset K_0$ and hence this case does not apply.

F. The trace $tr(p)$ has the form $\langle -g \rangle$ and thus lacks any positive nodes. This is not possible since node n_2 is positive (Lemma 2).

T. The trace $tr(p)$ has the form $\langle -g, +g, +g \rangle$ so the positive nodes are not minimal occurrences. Again this does not apply as it contradicts the minimality of n_2 in S.

C. The trace $tr(p)$ has the form $\langle -g, -h, +gh \rangle$, so the positive node is not a minimal occurrence again contradicting the minimality of n_2 in S.

E. The trace $tr(p)$ has the form $\langle -K_0, -h, +\{h\}_{K_0} \rangle$. Suppose $x \sqsubset \{h\}_{K_0} \wedge v_3 \not\sqsubset \{h\}_{K_0}$. Since $x \neq \{h\}_{K_0}, x \sqsubset h$. Moreover, $v_0 \not\sqsubset h$, so the positive node is not minimal in S.

D. The trace $tr(p)$ has the form $\langle -K_0^{-1}, -\{h\}_{K_0}, +h \rangle$. If we assume $K_s^{-1} = K_0^{-1}$, then there exists a node m with $term(m) = K_s^{-1}$. Since by assumption $K_s^{-1} \notin K_P$, we may infer that K_s^{-1} originates on a regular node. However, it is clear that no initiator or responder strand originates K_s^{-1}.

S. The trace $tr(p)$ has the form $\langle -gh, +g, +h \rangle$. Assume $term(n_2) = g$. Because $n_2 \in S, x \sqsubset g$ and $v_0 \not\sqsubset g$. By the minimality of n_2 however, we know that $v_0 \sqsubset gh$, it therefore follows that $v_0 \sqsubset h$.

Let $T = \{m \in \mathcal{C} : m \prec n_2 \wedge gh \sqsubset term(m)\}$. It is clear that every member of T is a penetrator node, because no regular node contains a subterm gh where h contains a subterm v_0.

T is non-empty because $\langle p, 1 \rangle \in T$. Hence T has a minimal member m which is of positive sign. Clearly, m cannot lie on **M, F, T, K** strands.

For the remaining strands, consider:

S. If $gh \sqsubset term(m)$, where m is a positive node on a strand p' of kind **S**, then $gh \sqsubset term(\langle p', 1 \rangle)$. Moreover, minimality of m in T is contradicted by $\langle p', 1 \rangle \prec m$.

E(D.) If $gh \sqsubset term(m)$, where m is a positive node on a strand p' of kind **E**(*or D*) then $gh \sqsubset term(\langle p', 2 \rangle)$. Minimality of m in T is contradicted by $\langle p', 2 \rangle \prec m$.

C. If $gh \sqsubset term(m)$, where m is a positive node on a strand p' of kind **C** and m is minimal in T then $gh = term(m)$ and p' has trace $\langle -g, -h, +gh \rangle$. Hence, $\text{term}(\langle p', 1 \rangle) = \text{term}(n_2)$ and $\langle p', 1 \rangle \prec n_2$ contradicting the minimality of n_2 in S. Therefore, n_2 does not lie on a penetrator strand but must lie on a regular strand instead. □

Definition 2. Fix some n_2 that is $\preceq$-minimal in $S = \{n \in \mathcal{C} : x \sqsubset term(n) \wedge v_0 \not\sqsubset term(n)\}$, and is therefore regular and positive.

Let t be a strand on which n_2 lies. It can be shown that the strand t also has a node in which v_0 occurs.

Lemma 3. *A node* n_1 *precedes* n_2 *on* t *and* $term(n_1) = v_0$.

Proof. We know from Lemma 1 that x originates uniquely at n_0 in Σ. It is clear that $n_2 \neq n_0$, because $v_0 \sqsubset term(n_0)$ while $v_0 \not\sqsubset term(n_2)$. It therefore follows that x does not originate at n_2. Hence there must be a node n_1 preceding n_2 on the same strand such that $x \sqsubset term(n_1)$. By the minimality of n_2, $v_0 \sqsubset term(n_1)$. However, since no regular node contains v_0 as a proper subterm, $v_0 = term(n_1)$. □

Lemma 4. *The regular strand* t *containing* n_1 *and* n_2 *is an initiator strand, and is contained in* $\mathcal{C}$.

Proof. Node n_2 is a positive node and comes after a node (namely n_1) of the form v_0. Hence t is an initiator strand; since if it was a responder strand, it would contain only a negative node after one of that form. Hence n_1 and n_2 are nodes in $t \in \mathcal{C}$. □

Proof of Proposition 1 follows from Lemmas 3 and 4 □

Proposition 2. *If* Σ *is a* $\mathcal{S}_{\mathcal{AP}}$ *space and* R *is uniquely originating in* Σ *then there is at most one strand* $t \in Init[Tag_i, S_i, R, x]$ *for any* Tag_i, S_i, x.

Proof. If $t \in Init[Tag_i, S_i, R, x]$ for any Tag_i, S_i, R then $\langle t, 3 \rangle$ is positive, $R \sqsubset term\langle t, 3 \rangle$ and R cannot occur earlier on t due to dependence on x. Therefore, R originates at node $\langle t, 3 \rangle$. Hence if R originates uniquely in Σ there can be at most one such strand t. □

4.3. The secrecy of x

Proposition 3. *Suppose:*

1. Σ is a $\mathcal{S}_{\mathcal{AP}}$ space, $\mathcal{C}$ is a bundle in Σ and s is a responder strand in $Resp[Tag_i, S_i, R, x]$;
2. $K_s^{-1} (= \langle p, q \rangle) \notin K_P$;
3. $R \neq x$ and x is uniquely originating in Σ.

Then for all nodes $m \in \mathcal{C}$ *such that* $x \sqsubset term(m)$*, either,* $v_0 \sqsubset term(m)$ *or* $ACK \sqsubset term(m)$*. In particular* $x \neq term(m)$.

Proof. Let $\Sigma, \mathcal{C}, s, Tag_i, S_i, x$ and R satisfy the hypothesis as in Proposition 3. Consider,
$S = \{n \in \mathcal{C} : x \sqsubset term(n) \wedge v_0 \notin term(n) \wedge ACK \notin term(n)\}$.
□

If S is non-empty, then there is at least one $\preccurlyeq$-minimal element. We show through the following two lemmas that such nodes are neither regular nor penetrator nodes. Therefore S is empty and the theorem holds.

Lemma 5. *No minimal element of* S *is a regular node.*

Proof. Suppose instead that $m \in S$ is minimal and a regular node. Therefore m is positive.

It is clear the Node m cannot lie in a responder strand s: Only n_0 is positive and $v_0 = term(n_0)$, so n_0 is not in S. Nor, can m lie on a responder's strand $s' \neq s$. In that case, $m = \langle s', 2\rangle$, so $term(m) = \{x'', t''\}$. Since, $x \sqsubset term(m)$ it implies that x originates at m, contradicting the assumption that x originates uniquely on node n_0.

Suppose next that m lies on an initiator strand s'. It is clear that either $m = \langle s', 1\rangle$ or $m = \langle s', 3\rangle$.

If $m = \langle s', 1\rangle$, then since $x' \sqsubset term(m)$, x originates at m contradicting the assumption that x originates uniquely on n_0.

If $m = \langle s', 3\rangle$, then $term(m) = \{ACK\}$. Therefore the second node $\langle s', 2\rangle$ is of the form $\{j'' = j^4 \bmod n,\ t''\}$. However, $x \neq j$ as otherwise $\{ACK\} = term(m)$. Hence $\langle s', 2\rangle$ is in S contradicting the minimality of m. □

Lemma 6. *No minimal member of S is a penetrator node.*

Proof. The proof is similar to Lemma 2. □

4.4. Security properties of the collaborative authentication scheme

We now consider the security properties of the proposed scheme.

1. *Tag anonymity*: In our scheme, steps (2) and (5) implicitly contain the tag identifier *TID*. However, it is enciphered well and cannot be detected by an attacker. Firstly, from (2), $\langle x'', t''\rangle$ in order to obtain *TID* from x'', the attacker would need to solve for x. However in order to do this knowledge of p and q is required by an attacker. In the unlikely event that the attacker is able to guess p and q and obtain x, recall that $x = h(TID) \oplus r \oplus s \oplus t$ where r is secret and t is generated internally by the tag. Therefore $h(TID)$ is well-protected. And from the one-way property of the hash function *TID* will not be revealed to an attacker. Secondly from step(5) $\langle ACK\rangle$, recall that $ACK = h(TID) \oplus t \oplus PRNG(x \oplus R)$. In order to obtain, $h(TID)$, the attacker needs to know p and q in order to solve for t, x, R from step(2). Similar to (2), *TID* is further protected by the one-way property of the hash function. Hence *TID* cannot be obtained by an attacker by compromising the message contents in (2) and/or (5).
2. *Tag location privacy*: In order to prove tag location privacy we will show that the values of the messages that are used in our scheme $\langle x'', t'', ACK\rangle$ cannot be linked to an individual tag.
   Firstly, in step (2) it is clear that x'' is not unique to a specific tag. Since x'' is derived from $x = h(TID) \oplus s \oplus r \oplus t$, where t is generated uniquely for each protocol sequence. Therefore, x is guaranteed to be different each round. Further, it is obvious that two different tags in the system can generate the same $x'' = (h(TID_1) \oplus s_1 \oplus r_1 \oplus t_1)^4 \bmod n = (h(TID_2) \oplus s_2 \oplus\ r_2 \oplus t_2)^4 \bmod n$. Hence a tag cannot be tracked using the value of x''. In a similar fashion in flow(5) $ACK = h(TID) \oplus t \oplus PRNG(x \oplus R)$ is not unique to a specific tag. It is true that $h(TID)$ is a constant for a given tag; however, for each protocol round t, x, R will all vary and hence *ACK* will vary. It is also obvious that two different tags with $h(TID_1)$ and $h(TID_2)$ can both generate identical values for $ACK = h(TID_1) \oplus t_1 \oplus PRNG(x_1 \oplus R_1) = h(TID_2) \oplus t_2 \oplus PRNG(x_2 \oplus R_2)$. Hence, location privacy of a tag cannot be compromised by an attacker through tracking of the message exchanges.
3. *Forward secrecy*: In order to prove forward secrecy we show that even if the tag is compromised and its current resident data is obtained by an attacker, this cannot enable tracing of any previous communication. Assume that the current resident data is $\langle TID, h(TID), n, r\rangle$ and without loss of generality the previous conversation of the tag is denoted by, $\langle s^{-1}, x''^{-1}, t''^{-1}, ACK^{-1}\rangle$. s^{-1} is a random challenge from the reader and hence is not linked to the resident data on the tag. x''^{-1} is derived from $x^{-1} = h(TID) \oplus s^{-1} \oplus r^{-1} \oplus t^{-1}$ where $h(TID)$ is a constant and is the current resident data on the tag; however, $r^{-1} \neq r$ and both s^{-1} and t^{-1} are random and hence not linked to the current resident data. Therefore, x and by implication x'' is not dependent on the current resident data. As noted earlier, since t is random, t''^{-1} is essentially random as well and cannot be linked to the current resident data. Finally, $ACK^{-1} = h(TID) \oplus t^{-1} \oplus PRNG(x^{-1} \oplus R^{-1})$. Only $h(TID)$ is dependent on the current resident data while, t^{-1}, x^{-1}, R^{-1} are all independent of the current resident data. Hence ACK^{-1} cannot be linked to the current resident data. Therefore with knowledge of the current resident data on the tag, an attacker cannot trace previous communications of the tag.
4. *Reader anonymity*: In our scheme steps (3) and (4) implicitly contain the reader ID (*RID*). However, it is enciphered well using a hash function, s and u. Firstly from (3), we see that in order to obtain *RID* from y'' at a minimum knowledge of g, h is required in order to solve for y. In the unlikely event that the attacker is able to solve for y, recall that $y = h(RID) \oplus s \oplus u$; therefore *RID* is further protected by the one-way property of the hash function. Similarly in (4), y and therefore *RID* is protected by the one-way property of the hash function. Hence the scheme provides reader anonymity.
5. *Reader location privacy*: In order to prove reader location privacy we show that the values of the messages used in steps (3) and (4) cannot be traced back to a specific reader. Firstly, in step (3), $\langle x'', t'', y'', u'', s\rangle$, x'' and t'' are both generated independently by the tag and therefore cannot be linked to a reader. Secondly, both y'' and u'' will be different during each protocol sequence as u is a random number and y'' is dependent on $y = h(RID) \oplus s \oplus u$. Since, s and u are generated fresh each protocol round, y is guaranteed to be different each time. Similarly, u'' will also be different each protocol round. Further, we note that two different readers, with RID_1 and RID_2 can generate the same y'' if, $h(RID_1) \oplus s_1 \oplus u_1 = h(RID_2) \oplus s_2 \oplus u_2$. Therefore, linking of the message contents in (3) to a specific reader is not possible. By a similar reasoning (4) cannot be linked to a specific reader since ACK' is dependent on y, which is generated fresh each time and is not specific to a reader. Hence the scheme offers reader location privacy.

6. *Replay attacks*: In order to show resistance to replay attacks we will show that an attacker cannot impersonate a valid reader by replaying previous messages. Assume an attacker records a previous step (3), $\langle x'', t'', y'', u'', s\rangle^{-1}$ and replays it to the server as part of a protocol sequence. By the same reasoning as in the mutual authentication case, the server will abort since $s \neq s^{-1}$. However, an attacker can choose to partially replay the values in (3) as $\langle x'', t'', y''^{-1}, u''^{-1}, s^{-1}\rangle$ or $\langle x'', t'', y''^{-1}, u''^{-1}, s\rangle$ after communication with a legitimate tag in steps (1) and (2). In the former case, when the server solves for y^{-1} and u^{-1} and checks if $y^{-1} \oplus s^{-1} \oplus u^{-1} = h(RID)$, matches a record on the server, it will find a match. The server will therefore proceed to solve for x and t and check if $x \oplus s^{-1} \oplus t = R_{TID}$ or R_{TID}^{-1} However, this cannot hold since $s \neq s^{-1}$. In the latter case, when the server solves for y^{-1} and u^{-1} and checks if $y^{-1} \oplus s \oplus u^{-1} = h(RID)$, matches a record on the server, it will not find a match. Therefore in both cases the server will abort.
   We next show that server impersonation is also not possible through replay by an attacker. Assume an attacker records a previous ACK'^{-1} and replays to the reader in step (4). Recall that $ACK'^{-1} = (ACK^{-1} \| u^{-1}) \oplus h(y)^{-1}$. Since $u \neq u^{-1}$ and $h(y) \neq h(y)^{-1}$ the reader will abort when it compares u with u^{-1} contained in $ACK'^{-1} \oplus h(y)$. Therefore the scheme is resistant to replay attacks.
7. *Desynchronisation attack*: An attacker can cause denial of service (DoS) by causing desynchronisation between the server and the tag by either blocking or successfully forging step (5) $\langle ACK\rangle$. If an attacker succeeds in blocking $\langle ACK\rangle$, the tag will fail to correctly update the value of r. Hence in any subsequent protocol sequence, it will calculate its values using the non-updated value of r (i.e., r^{-1}). However since the server stores both r and r^{-1} it will still be able to correctly identify the tag using R_{TID}^{-1}.
   An attacker can also cause desynchronisation by forging *ACK* and causing the tag to update its value of r independent of the server. If an attacker is successful in forging *ACK* then permanent DoS will result between the tag and the server as the tag will update r to r^{+1} resulting in unrecoverable desynchronisation with the server (since the server only stores r^{-1} and r). However, forging of *ACK* will require at a minimum knowledge of x as noted earlier. By the quadratic residue property it is impossible to compute x without knowledge of p and q. Hence, only the valid server is able to compute the correct value for step (5) such that $ACK = h(TID) \oplus t \oplus PRNG(x \oplus R)$. Thus, an attacker cannot successfully forge *ACK* and hence our scheme is protected against desynchronisation leading to DoS. We note that desynchronisation attacks on the reader do not apply since there is no shared value that is updated each protocol round.
8. *Server impersonation attack*: The scheme is protected against server impersonation which can cause a tag to reveal its information to an attacker. In order to impersonate a server, an attacker should successfully generate *ACK* in order to complete the protocol sequence. Recall, that $ACK = h(TID) \oplus t \oplus PRNG(x \oplus R)$. When, an attacker is challenged by the tag in step (2) $\langle x'', t''\rangle$ in response to an attacker generated query, the attacker firstly would need to solve for the correct values of x, t. Based on the quadratic residue property, this requires knowledge of p and q. In the unlikely event, that the attacker is able to correctly guess p and q and obtain x, t the attacker would still not be able to generate a correct *ACK*. Recall, that $x = h(TID) \oplus s \oplus r \oplus t$. With knowledge of s, t the attacker would be able to generate $x \oplus s \oplus t = h(TID) \oplus r$. However, to correctly generate *ACK* the attacker would need to obtain $h(TID)$ which requires the knowledge of the shared secret r. Hence an attacker will not be able to successfully impersonate a server to the tag.

From the discussion above, we can see that the collaborative authentication scheme provides robust security properties.

4.5. Comparison with other protocols

In Table 1 we compare the security properties of current authentication protocols that have been proposed. We observe that Yeh et al. [34] and Cho et al. [35] aim to achieve all of the required security properties required for mobile/wireless RFID systems. However both schemes suffer from proven vulnerabilities such as desynchronisation and impersonation attacks. All other schemes do not explicitly take into account the security properties of the reader–server channel. Such current schemes also fail to achieve one or more properties – we observe that the schemes by Chien and Chien [20], Chen and Deng [10] and Lo et al. [33] do not achieve location privacy. Chien and Chien's scheme [20] also does not achieve forward secrecy and is not resistant to replay and DoS attacks based on desynchronisation. Lo et al.'s [33] scheme suffers from desynchronisation and server impersonation attacks. Of the two quadratic residue based schemes Chen et al.'s [10] scheme suffers from tag impersonation, location privacy and replay attacks. However, as noted earlier Yeh et al.'s [11] scheme meets all of the required security properties in a fixed reader environment with secure channel assumptions. As noted in the security analysis (Section 4), our collaborative authentication scheme satisfies all of the required security properties without secure channel assumptions.

In Table 2 we compare the performance of our schemes with other schemes. In the schemes proposed by Chien and Chien [20], Chen et al. [10], Yeh et al. [11] and Chen and Deng [37] the channel between the reader and the server is assumed to be secure. Hence there is no reader–server authentication that is built into the schemes and hence they are not suited for mobile/wireless RFID systems. In, [10,35] and [11] tags are required to implement hash functions. Firstly, implementing of hash functions on passive RFID tags is an open research problem [35] and secondly, such assumptions are not in conformance to EPC standards [8]. It is also known that even the cheapest hash function will cost approximately 1.7k gates to implement [10]; however, constructions based on universal hash functions often give away part of their key bits [46] while others such as SQUASH are more expensive(6k gates). In the schemes by Cho [35],

Yeh [34] and our collaborative authentication scheme the server–reader channel is not assumed to be secure. However, as noted earlier, there are security problems with Cho's and Yeh's schemes and both schemes are not EPC Class-1 Gen-2 compliant. Of the two quadratic residue based schemes, both the schemes by Chen et al. [10] and by Yeh et al. [11] are not EPC Class-1 Gen-2 compliant as they both require the tag to implement hash functions. Our collaborative authentication scheme achieves EPC Class-1 Gen-2 compliance as hash functions are required to be implemented only by the reader and the server.

We also observe that most schemes have a worst case database loading of $O(n)$, where n is the number of tags in the system. In order, to protect against desynchronisation attacks most schemes store previous and current key values and/or secrets leading to an increased number of record-by-record operations and verifications. One of the challenges in authentication is to identify a tag unequivocally without information leakage and high database loading. Both quadratic residue based schemes however are able to achieve a worst case database loading of $O(1)$. Chen's scheme [10] achieves a complexity of $O(1)$; however to achieve this, the tag is required to calculate 3 hash values. Further, the server is required to calculate 10 hash values to allow it to identify the tag uniquely. Yeh's scheme [11] also achieves a complexity of $O(1)$. However, the tag and the server are required to now compute 4 and 14 hash values respectively. Therefore, both schemes are not suitable for EPC Class-1 Gen-2 tags. Our collaborative authentication scheme however is able to achieve a complexity of O(1) without using hash functions and without compromising our resistance to desynchronisation attacks. Further, the tag computation is restricted to modulo squaring, bit-wise operations, CRC calculations and random number generation. All of which are within the capabilities of EPC Class-1 Gen-2 tags. Importantly, as noted by Chien and Chien [20], only a few hundred gates are required for implementing modular squaring operations; this is much cheaper than even the simplest hash function. Thus we see that our scheme provides the required security properties while at the same time conforming to EPC Class-1 Gen-2 standards.

In terms of the number of messages and storage requirements we have found that it is comparable across most of the schemes.

5. Conclusion and future work

In this paper we have a proposed a novel approach to authentication and privacy in RFID systems based on unique quadratic residues. The proposed approach addresses the 3 main drawbacks of current schemes – robust security, EPC Class-1 Gen-2 compliance and suitability for mobile/wireless environments. The proposed approach can successfully validate the tag, reader and back-end server in a RFID system as legitimate parties and is cheaper than other quadratic residues based methods. Our collaborative authentication scheme is suitable for mobile/wireless reader environments where secure channel assumptions are invalid. Importantly, our proposed scheme is suited to the computational constraints of EPC Class-1 Gen-2 passive RFID tags as it only uses the modular squaring, CRC and PRNG functions that passive RFID tags are capable of and does not require the implementation of hash functions on RFID tags. This differentiates the proposed approach from the schemes proposed by Chen et al. [10] and Yeh et al. [11].

Security analysis of our proposed scheme shows that it achieves the required properties of tag anonymity, tag location privacy and forward secrecy while being resistant to replay, desynchronisation and server impersonation attacks. In addition to these security properties, the collaborative authentication scheme also achieves reader anonymity and reader location privacy. Performance comparisons show that our scheme is practical and can be implemented on passive tags and achieves a worst case database loading of $O(1)$. In the future we hope to complete a test bed implementation of the proposed scheme.

Acknowledgement

This work is partially supported by an Australian Research Council (ARC) Linkage project grant (LP100100816).

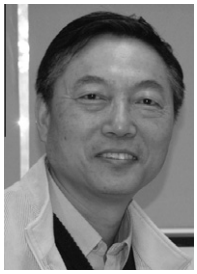
References

[1] A. Juels, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communication 24 (2006) 381–394.
[2] R. Weinstein, RFID: a technical overview and its application to the enterprise, IT Professionals 7 (2005) 27–33.
[3] K. Michael, L. McCathie, The pros and cons of RFID in supply chain management, in: ICMB'05, 2005.
[4] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang, S. Song, An approach to privacy and security of RFID system for supply chain, in: IEEE ICETDE04, 2004.
[5] R. Das, RFID market projections 2008–2018, in: IDTechEx, 2008.
[6] A. Juels, Yoking-proofs for RFID tags, in: First International Workshop on Pervasive Computing and Communication Security, 2004.
[7] K. Wong, P. Hui, A. Chan, Cryptography and authentication on RFID tags for apparels, Computer in Industry 57 (2005) 342–349.
[8] EPCGlobal, Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz–960MHz Version 1.2.0, in: EPC Radio-Frequency Identity Protocols, 2008.
[9] A. Juels, S. Weiss, Authenticating pervasive devices with human protocols, Lecture Notes in Computer Science 3621 (2005) 293–308.
[10] Y. Chen, J.-S. Chou, H.-M. Sun, A novel mutual authentication scheme based on quadratic residues for RFID systems, Computer Networks 52 (2008) 2373–2380.
[11] T.-C. Yeh, C.-H. Wu, Y.-M. Tseng, Improvement of the RFID authentication scheme based on quadratic residues, Computer Communications (34) (2011) 337–341. http://dx.doi.org/10.1016/j.comcom.2010.05.011.
[12] S. Ahamed, F. Rahman, M. Hoque, ERAP: ECC based RFID authentication protocol, in: 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2008.
[13] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, I. Verbauwhede, An elliptic curve processor suitable for RFID-tags, Cryptology ePrint Archive, Report 2006/227.
[14] N. Lo, K.-H. Yeh, C.Y. Yeun, New mutual agreement protocol to secure mobile RFID-enabled devices, Information Security Technical Report 13 (2008) 151–157.
[15] M. Ohkubo, K. Suzuki, S. Kinoshita, A cryptographic approach to a 'privacy-friendly' tags, in: RFID Privacy Workshop, Massachusetts Institute of Technology, 2003.
[16] G. Tsudik, YA-TRAP: yet another trivial RFID authentication protocol, in: 4th IEEE International Conference on Pervasive Computing and Communications, 2006.
[17] S. Lee, T. Asano, K. Kim, RFID mutual authentication scheme based on synchronized secret information, in: Symposium on Cryptography and Information Security, 2006.

[18] H.-Y. Chien, C.-S. Laih, ECC-based lightweight authentication protocol with untraceability for low-cost RFID, Journal of Parallel and Distributed Computing 69 (2009) 848–853.
[19] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, LAMED A PRNG for EPC Class-1 Generation-2 RFID specification, Computer Standards and Interfaces 31 (2009) 88–97.
[20] H.-Y. Chien, C.-H. Chen, Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards, Computer Standards and Interfaces 29 (2007) 254–259.
[21] A. Shamir, SQUASH a new MAC with provable security properties for highly constrained devices such as RFID tags, Lecture Notes in Computer Science 5086 (2008) 144–157.
[22] D. Duc, K. Kim, Defending RFID authentication protocols against DoS attacks, Computer Communications. http://dx.doi.org/10.1016/j.comcom.2010.06.014.
[23] P. Lopez, A. Ofila, J. Castro, J. van der Lubbe, Flaws on RFID grouping proofs. Guidelines for future sound protocols, Journal of Network and Computer Applications. http://dx.doi.org/10.1016/j.jnca.2010.04.008.
[24] R.D. Pietro, R. Molva, An optimal probabilistic solution for information confinement, privacy and security in RFID systems, Journal of Network and Computer Applications. http://dx.doi.org/10.1016/j.jnca.2010.04.015.
[25] T. van Deursen, S. Radomirovic, On a new formal proof for RFID location privacy, Information Processing Letters 110 (2009) 57–61.
[26] E. Choi, D.H. Lee, J.I. Lim, Anti-cloning protocol suitable for EPCglobal Class-1 Generation-2 RFID systems, Computer Standards and Interfaces 31 (2009) 1124–1130.
[27] S.-Y. Kang, D.-G. Lee, I.-Y. Lee, A study on secure RFID authentication scheme in pervasive computing environment, Computer Communications 31 (2008) 4248–4254.
[28] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, Lecture Notes in Computer Science 2802 (2004) 201–212.
[29] D. Henrici, P. Muller, Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, in: 2nd IEEE Annual Conference on Pervasive Computing and Communications, 2004.
[30] D. Molnar, D. Wagner, Privacy and security in library RFID: issues, practices, and architectures, in: 11th ACM Conference on Computer and Communications Security, 2004.
[31] S. Piramuthu, Protocols for RFID tag/reader authentication, Decision Support Systems 43 (2007) 897–914.
[32] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, Cryptanalysis of a novel authentication protocol conforming to epc-c1g2 standard, Computer Standards and Interfaces 31 (2) (2009) 372–380.
[33] N. Lo, K. Yeh, An efficient mutual authentication scheme for EPCglobal Class-1 Generation-2 RFID systems, in: Intenational Conference on Embedded and Ubiquitous Computing, 2007.
[34] T.-C. Yeh, Y.-J. Wang, T.-C. Kuo, S.-S. Wang, Securing RFID systems conforming to EPC Class 1 Generation 2 standards, Expert Systems and Applications 37 (2010) 7678–7683.
[35] J.-S. Cho, S.-S. Yeo, S.-K. Kim, Securing against brute-force attack: a hash based RFID mutual authenication protocol using a secret value, Computer Communications. http://dx.doi.org/10.1016/j.comcom.2010.02.029.
[36] M. Safkhani, P. Peris-Lopez, J.C. Hernandez-Castro, N. Bagheri, M. Naderi, Cryptanalysis of Cho et al.'s protocol, a hash-based mutual authentication protocol for RFID systems, Cryptology ePrint Archive, Report 2011/311, 2011. <http://eprint.iacr.org/2011/331.pdf>.
[37] C.-L. Chen, Y.-Y. Deng, Conformation of EPC Class-1 Generation 2 standards RFID system with mutual authentication and privacy protection, Engineering Applications of Artificial Intelligence 22 (2009) 1284–1291.
[38] G. Kapoor, S. Piramuthu, Vulnerabilities in Chen and Deng's RFID mutual authentication and privacy protection protocol, Engineering Applications of Artificial Intelligence 24 (7) (2011) 1300–1302. <10.1016/j.engappai.2011.06.011>.
[39] A. Liu, L. Bailey, PAP: privacy and authentication protocol for passive RFID tags, Computer Communications 32 (2009) 1194–1199.
[40] M. Nasser, P. Peris-Lopez, P. Rafie, M.J. van der Lubbe, Vulnerability analysis of pap for rfid tags, ArXiv e-printsarXiv:1008.3625. <http://adsabs.harvard.edu/abs/2010arXiv1008.3625N>.
[41] T. Cao, P. Shen, Cryptanalysis of some RFID authentication protocols, Journal of Communications 3 (7) (2008) 20–27.
[42] K. Ouafi, S. Vaudenay, Smashing SQUASH-0, Lecture Notes in Computer Science 5479 (2009) 300–312.
[43] F. Gosset, F.-X. Standaert, J.-J. Quisquater, FPGA implementation of SQUASH, in: 29th Symposium on Information Theory, 2008.
[44] K.H. Rosen, Elementary Number Theory and its Applications, 4th ed., Addison-Wesley, Reading, MA, USA, 1999.
[45] F. Thayer, J. Herzog, J. Guttman, Strand spaces: proving security protocols correct, Journal of Computer Security 7 (2/3) (1999) 191–230.
[46] W. Nevelsteen, B. Preneel, Software Performance of Universal Hash Functions, Advances in Cryptology EUROCRYPT 1999 (LNCS1592) (1999) 24–41.

Robin Doss received the BEng from the University of Madras, India, in 1999, and the MEng and PhD degrees from the Royal Melbourne Institute of Technology (RMIT), Australia, in 2000 and 2004, respectively. He has held professional appointments with Ericsson Australia, RMIT University, and IBM Research, Switzerland. He joined Deakin University, Melbourne, Australia, in 2003, and currently, is a senior lecturer in computing. Since 2003, he has published more than 50 papers in refereed international journals, international conference proceedings and technical reports for industry and government. His current research interests are in the broad areas of communication systems, protocol design, wireless networks, security and privacy. He is a member of the IEEE.

Saravanan Sundaresan received his B.Sc (M) from the University of Madras, India in 1995. He started his career as a programmer in India and took up IT consulting in USA in 1997. He joined HP Inc. as a Senior Database Administrator in 1999 and later joined Caterpillar Inc. in 2004 to become the Team Lead and Senior Database Administrator. In 2006 he took up community work in the villages of South India and received a Social Entrepreneur Reward in 2010. Saravanan joined Deakin University, Victoria, Australia to do his MIT degree in 2010 and has currently submitted his thesis on RFID as part of his course.



Wanlei Zhou received the BEng and MEng degrees from Harbin Institute of Technology, China, in 1982 and 1984, respectively; the PhD degree from the Australian National University, Canberra, in 1991; and the DSc degree from Deakin University, Victoria, Australia, in 2002. He is currently the chair professor of information technology and the head of School of Information Technology, Faculty of Science and Technology, Deakin University, Melbourne, Australia. His research interests include distributed and parallel systems, network security, mobile computing, bioinformatics and e-learning. He has published more than 200 papers in refereed international journals and refereed international conferences proceedings. Since 1997, he has been involved in more than 50 international conferences as general chair, steering committee chair, PC chair, session chair, publication chair, and PC member. He is a senior member of the IEEE.