Tampering in RFID: A Survey on Risks and Defenses

Noname manuscript No.
(will be inserted by the editor)

Tampering in RFID: A Survey on Risks and Defenses

Filippo Gandino · Bartolomeo Montrucchio · Maurizio Rebaudengo

Received: date / Accepted: date

Abstract RFID is a well-known pervasive technology, which provides promising opportunities for the implementation of new services and for the improvement of traditional ones. However, pervasive environments require strong efforts on all the aspects of information security. Notably, RFID passive tags are exposed to attacks, since strict limitations affect the security techniques for this technology. A critical threat for RFID-based information systems is represented by data tampering, which corresponds to the malicious alteration of data recorded in the tag memory. The aim of this paper is to describe the characteristics and the effects of data tampering in RFID-based information systems, and to survey the approaches proposed by the research community to protect against it. The most important recent studies on privacy and security for RFID-based systems are examined, and the protection given against tampering is evaluated. This paper provides readers with an exhaustive overview on risks and defenses against data tampering, highlighting RFID weak spots and open issues.

Keywords Data Tampering · RFID · Security · Ubiquitous Computing

F. Gandino · M. Rebaudengo · B. Montrucchio
Dipartimento di Automatica ed Informatica, Politecnico di Torino
Tel.: +39-011-0907068
Fax: +39-011-0907099
E-mail: filippo.gandino@polito.it

1 Introduction

A widely employed pervasive technology is represented by Radio Frequency Identification (RFID), which is used in various sectors, e.g. supply chain management [1] and internal traceability management [2]. A typical RFID system [3] is made up of a *reader*, which generates an electromagnetic field, and some *passive tags* without an own voltage supply. They can be read only if they are in the reading range of a reader which supplies the power required through a coupling unit. The RFID tags hold a memory that stores an unambiguous identification code (ID) and potentially a rewritable user memory. RFID technology is mainly used in order to identify objects by matching them with tags. The Automatic Identification and Data Capture (AIDC) based on RFID provides many benefits, such as time saving and great accuracy, at a reduced cost [4]. However, RFID tags are also used for other kinds of operations, such as localization, data storing, and personal identification.

Although RFIDs provide relevant opportunities, they involve also considerable information security threats [5], such as cloning of original tags and privacy violation. A critical threat is represented by data *tampering*, which consists in the malicious changing of data recorded in the tag memory. The tampering has many dangerous effects, such as incoherence in the information system, exposure to opponent attacks, and mistakes in the production flow. This malicious action has been studied in various fields, e.g. software source protection [6], and many approaches, addressing it, have been proposed.

Nowadays, the application of RFID is rapidly growing and, according to the strict security requirements for RFID-based systems, several research studies on RFID security problems have been proposed (e.g. [5, 7]). According to [8] in 2007, 58 papers on security and privacy in RFID systems, and 39 papers on controlling the information flow between tags and readers have been proposed. Both specialized approaches [9–12] and some more general ones [13–15] address the tampering problem. Several solutions to various security issues in mobile [16] and pervasive technologies have been provided, but problems as tampering in RFID still represent a critical threat for data security.

Although various books [17, 18] and survey-based journal papers [5, 8, 19, 20] present the state-of-the-art in RFID security, these studies are mainly focused on privacy protection, authentication features, and cryptographic hardware implementations, which represent the most frequently analyzed RFID security issues. Therefore, this paper aims at filling the gap in RFID security study, analyzing the characteristics of data tampering in RFID-based information systems, and surveying the state-of-the-art of RFID tampering protection, in order to provide readers with an exhaustive overview on risks and on proposed defenses against tampering. The characteristics of RFID technology are described, highlighting security weak spots. This survey is specially focused on tampering with data in tag memories, since this threat represents a critical open issue. Furthermore, the most recent and effective general purpose security approaches for RFID tags are analyzed, evaluating their ability to effectively protect against tampering.

The remaining of the paper is organized as follows: in Section 2 background about RFID is briefly introduced, while in Section 3 the characteristics of data tampering are presented with special regard to general pervasive environments and in particular to RFID-based systems. The state-of-the-art of security approaches is described in Section 4 and in Section 5, divided according to the adopted protection features (i.e. tamper-evidence and tamper-resistance, respectively) provided by the protocols. Finally, in Section 6 the analyzed approaches are compared and in Section 7 some conclusions are drawn.

2 RFID

In this section a brief introduction on RFID technology is presented, highlighting weak spots and special requirements for RFID security techniques.

An RFID system [3], which is shown in Figure 1, typically includes an RFID *reader* and some RFID *tags*. The reader is able to access tags by a wireless communication, which is managed by a radio frequency interface. Furthermore, the reader communi-

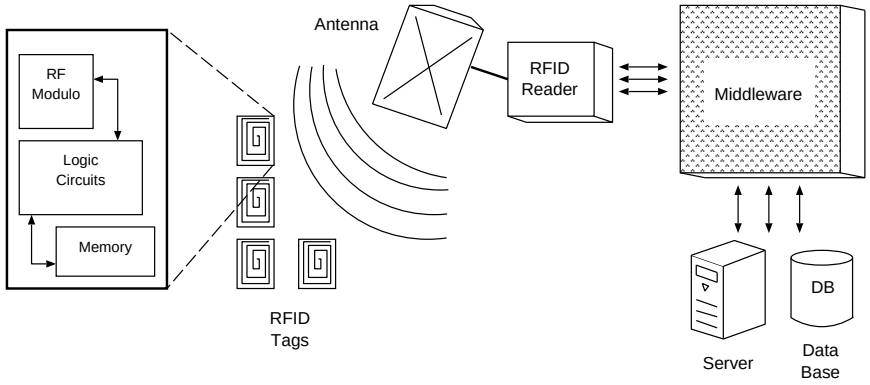

Fig. 1 RFID System

cates the collected data to a *middleware*, which is the software layer that allows the interconnection between the reader and the information system.

A tag is composed by a radio frequency interface block, a memory component and a logic element. There are two kinds of tags: *passive* and *active*. Passive tags have no battery, and they acquire the power supply from the electromagnetic field of the reader. Instead, active tags have their own power supply. Passive tags are cheaper than active ones, but they present a shorter range of transmission. The active tag life depends on the battery duration and use, while the rewritable passive tag life is typically measured in number of read/write cycles. The passive tags are more largely employed, thanks to their low cost. Active tags present performance similar to other pervasive technologies, and they are able to provide more advanced security features than passive ones, since their own power can supply more hardware modules. Therefore, security techniques designed for other wireless devices, such as wireless sensor networks and smart phones, can be applied to these devices. Instead, according to the strict limitations that affect passive tags, they require ad-hoc security techniques. The same techniques used for passive tags could be applied also to active ones, but they have stricter limitations than general purpose ones. Therefore, this paper is specifically focused on passive tags, and in the following, if not differently reported, the word 'tag' is referred to passive tags.

The most important standardization organizations for RFID are represented by International Organization for Standardization (ISO) and EPCglobal, which define the physical and logical requirements and interfaces for tags and readers. Furthermore, EPC standards define the structure and content of data. Operational frequency used in RFID systems vary according to the country. The frequency bands are:

- Low Frequency (LF) between 125 and 134 KHz;
- High Frequency (HF) at 13.56 MHz (e.g. ISO 14443 and ISO 15693, both defined for identification cards);
- Ultra High Frequencies (UHF) between 866 and 868 MHz in EU, between 902 and 928 MHz in USA (e.g. EPC Class I Gen 2 [21], defined for item management);
- Microwave at 2.45 GHz in EU, between 2.4 and 2.4835 GHz and between 5.725 and 5.85 GHz in USA.

A limitation to the use of RFIDs is represented by the presence of metal or liquid that can create noise to the electromagnetic field, disturbing or stopping the transmission. Lowest frequencies assure a major noise tolerance, but involve a shorter transmission range. Another factor that affects the transmission is the antenna shape and size. Typically, LF requires larger antennas. A reader compliant with EPC Class I Gen 2 can read RFID passive tags in a range over 4 meters. On the other hand, a small reader for Personal Digital Assistant (PDA) compliant with ISO 14443 can read RFID passive tags only in a range shorter than 10 cm. The RFID transmissions are characterized by two ranges:

- the *reading range*, corresponding to the area where the electromagnetic field of the reader induces enough voltage in the tag antenna in order to correctly receive tag data;
- the *transmission range*, corresponding to the area where the data can be received, but the supplied voltage could be not enough for passive tags; the reader transmission range is larger than the tag transmission range, according to the higher power, and than the reading range.

Commonly, computational capacities are extremely limited in a tag. The major concern of an RFID reader consists in accessing the tag memory. Memory plays an important role in the tag architecture; it contains the unique identification number and may have up to several kilobits of storage capacity. However, the presence of a larger memory increases significantly the tag cost. Tags can have read-only or read and write memory. The rewritable memories open many application opportunities, but they are exposed to malicious writing actions. The widely used EPC Class I Gen 2 tags typically have a 96-bit memory bank that contains a code for the identification of the tagged object and a 64-bit bank of reserved memory that contains passwords. On the other hand, some ISO 14443 tags is equipped with memories larger than 8 Kbits.

The hardware or software computation of cryptographic operations requires too computational effort for RFID tags. An RFID tag compliant with EPC Class I standard requires between 1000 and 4000 gates, while a commercial implementation of Advanced Encryption Standard (AES) requires between 20000 and 30000 gates [22]. Since the number of gates for security is strictly limited, usually tags implement only simple security operations. For example, EPC Class I Gen 2 requires the use of password and bitwise XOR operations. However, some RFID tags with cryptographic capability have been designed, such as DEFfire from Philips [23], which owns a crypto co-processor for DES/AES operations, compliant with ISO/IEC 14443A for HF.

Each type of application requires an RFID system with specific technological characteristics. In the following a list of RFID applications and their specifications are presented.

- Supply chain management [1]. A basic application can match each item with a tag. The tags can have small read-only memory with a unique code. Their frequency is UHF, in order to have a long reading range, and they are typically compliant with EPC standards.
- Internal traceability management based on reusable containers [2]. Each tag is matched to a container and the data about the products, written in the tag memory, are repeatedly updated. These applications require tags with rewritable memory in

order to update the information. The frequency of the tag is HF, normally matched to a large memory, or UHF, providing a larger reading range.

– RFID applications for libraries [24]. Each tag is matched to a book, and it contains information about the book and its location. These systems are often based on tags with rewritable memories, so the stored data can be updated and new ones can be added. The tags are normally read by a PDA, so the short reading range provided by HF does not represent a limitation.

The pervasive nature of RFID technology exposes tags to two kinds of possible accesses:

– *physical access*, when an entity gets in touch with the tag;
– *RF communication access*, by means of the tag communication protocol, potentially without knowledge of the owner of the tag.

The first case seems more dangerous, since adversaries have time and means to perform strong attacks. However, the possible damages due to tampering actions are limited, since hardly they can be performed without knowledge of the tag owner. Instead, RF attacks can generate troubles, since adversaries could alter data on rewritable memory tags that will be reused, generating possible mistakes.

As a conclusion, the main elements that affect RFID security techniques for tags are:

– low computational effort;
– limited memory;
– exposure to RF access by hidden readers.

The strict limitations related to tags do not affect the reader and the middleware, which can implement normal security techniques.

3 Tampering in Pervasive Information Systems

The definition of tampering changes according to the context. It can be defined as a malicious action that alters something (e.g. objects or data). Several fields in Informa-

tion Technology are subject to the tampering problem, so many effective defenses have been proposed [25–31]. There are two kinds of protections against tampering.

- *Tamper-evidence*. The feature of a process, device, or software, to detect the existence of tampering.
- *Tamper-resistance*. The ability to resist to tampering.

The effects of tampering can be divided in two main groups:

- *damage*, when tampering makes something unusable;
- *alteration*, when the target seems correct, but according to the malicious alteration, it is faulty and it will generate possible mistakes.

Although tamper-resistance solutions aim at preventing all tampering effects, tamper-evidence aims at preventing only mistakes due to an alteration, reduced to a damage. In the following the main tampering effects and tamper-protection schemes from several fields are introduced, describing their relation with RFID.

One field in information technology, where the tampering problem has been widely studied, is the *software protection*. A tamper attack could *alter* a program in some ways. An adopted solution is adding tamper-evident features, by inserting into the program tamper-proofing code, which can detect if the program was tampered with, stopping the program when tampering effects are detected [6]. This kind of attack could be very dangerous for pervasive devices, since they are often deployed into hostile areas. However, low cost RFID tags are very simple devices and most of them do not present a microprocessor, so software tampering does not represent a relevant threat.

A considerable tampering subject is the *hardware tampering*. Tampering actions may aim at *damaging* the device or at *altering* the system accessing to the code in order to reprogram it with a malicious one able to execute insider attacks. The tamper-resistant hardware may avoid unauthorized access to the running code and it may resist to malicious actions such as physical penetration, and temperature manipulation. Various applications employ tamper-resistant hardware, among which several approaches for authentication and integrity checking in mobile systems [25]. However, the use of

tamper-resistant hardware requires high costs, which are often too expensive for pervasive environments. In wireless sensor networks a tampered node with a malicious running program is a critical threat. Hardware tampering attacks to RFID tags have not been reported, and it is not yet directly handled by RFID security approaches for low cost RFID tags. The main motivation is that tags are often vulnerable to simpler and faster RF attacks, which can be applied also without physical access.

In *wireless communications*, tamper attacks could modify in-transit packets, so received data are *altered* and differ from the transmitted ones. This malicious action is recognized as really dangerous especially in mobile fields, such as Vehicular [26], and Mobile [27] Ad-Hoc Networks.

The greatest threat for RFID Information System is represented by *data tampering*. The most well-known data tampering attacks control data, and the main defense against it is the control flow monitoring for reaching tamper-evidence. However, tampering with other kinds of data such as user identity data, configuration data, user input data, and decision-making data, is also dangerous [28]. Some solutions were proposed, such as a tamper-evident compiler and micro-architecture collaboration framework to detect memory tampering [29]. A further threat is the tampering with application data, involving mistakes in the production flow, denial of service, incoherence in the information system, and exposure to opponent attacks. This kind of attack is especially dangerous for RFID systems, since one of the main RFID applications is the automatic identification for database real-time updating. The main data tampering actions are:

- *data impairing*, some bits of digital information are changed, in order to *damage* it making data unreadable or to *alterate* its value;
- *wrong data insertion*, data are *altered* replacing them with new data with erroneous values; this action requires the ability to compose new data consistent with the original data encoding;
- *data copying*, original data are *altered* deleting and replacing them with other data copied from a different location; this action does not require an encoding process.

In a RFID-based system, data tampering is very dangerous, since it could generate serious mistakes, e.g. in a company with AIDC the production flow could be stopped, and in pharmaceutical industry [30], drugs with wrong data may be delivered to a wrong destination, causing troubles for patients.

Data tampering can be performed on RFID tags with a rewritable memory, by means of a RF communication. According to the pervasive deployment of tags, an attack can be performed moving the adversary RFID reader for few seconds inside the reading range of the tag, or viceversa waiting until the tag is moved in the reading range of the hidden adversary RFID reader. For tags with a read-only memory, tampering attacks cannot be performed by means of a RF communication, so the physical access to the tag is required in order to perform the more costly hardware tampering.

An evaluation of threats on RFID systems compliant with EPC standards has been presented in [32]. This study, partially based on an evaluation framework proposed by ETSI [33], determines the *likelihood* of a threat, which represents the probability that an attack is performed, according to the *motivation*, which is evaluated according to the provided benefits, and the required *difficulty* for attackers. Finally the evaluation method ranks the *risk* of a threat as "critical", "major" or "possible", according to the computed likelihood and the *impact*, which represents the relevance of the attack effects. This study has been extended in [34], where the threats contained in the STRIDE model [35], which is used to define threat types for the design of secure software systems, are evaluated according to the proposed method. However, only a limited part of the study is focused on tampering, and the analysis deals only with systems compliant with EPC standards, which are designed for item management. The motivation for tampering with RFID data has been ranked medium, since adversaries do not reach clear benefits. The difficulty has been ranked high, since adversaries have to bypass 32-bit passwords, according to EPC Class I Gen 2 [21]. The impact has been ranked low, since the tampering effects are evaluated temporary. The resulting likelihood and risk have been evaluated low. However, according to our analysis, when the motivation is to damage a competitor it can be ranked high. Moreover, tampering actions can be

performed for economic purposes, e.g. changing the price of a good in a shop. Many RFID tags are not protected by passwords, and often eavesdropping the passwords could be simple, as detailed in Section 5.3, so the difficulty is medium. When the effect is an *alteration* the impact could be medium or high. The likelihood in our analysis is considered medium and the risk is evaluated medium/high.

4 Tamper-evident approaches

In this section the approaches that aim at detecting tampering are detailed. These schemes aim at reducing the *alteration* effects of tampering to a *damage*. According to the evaluation method presented in [32], the result is the reduction of the impact and of the risk from medium/high to low. Even if data tampering can be performed not only on the data stored in the tag memory, it represents the weak spot of RFID systems, so this section is focused on tampering with data on tags. Other attacks conducted beyond the RFID reader, such as tampering with database or messages between the RFID reader and servers, can be managed by well-known security techniques (e.g. Tamper-Evident Database [31] and Message Authentication Code (MAC) [36]). The described approaches are shown in Figure 2.

4.1 Fragile watermarking for RFID data tamper detection

The watermarking consists in embedding information into original data. It is defined fragile when a minimal change of the original data generates incoherence between the data and the embedded information.

A tamper detection system based on fragile watermarking was proposed in [9]. This system aims at detecting tampering on RFID tag with a writable memory compliant with EPC96 standard, as shown in Fig 3. The tag memory is composed by the following fields:

- the Header that defines the EPC version,
- the EPC Manager that identifies the manufacturer,

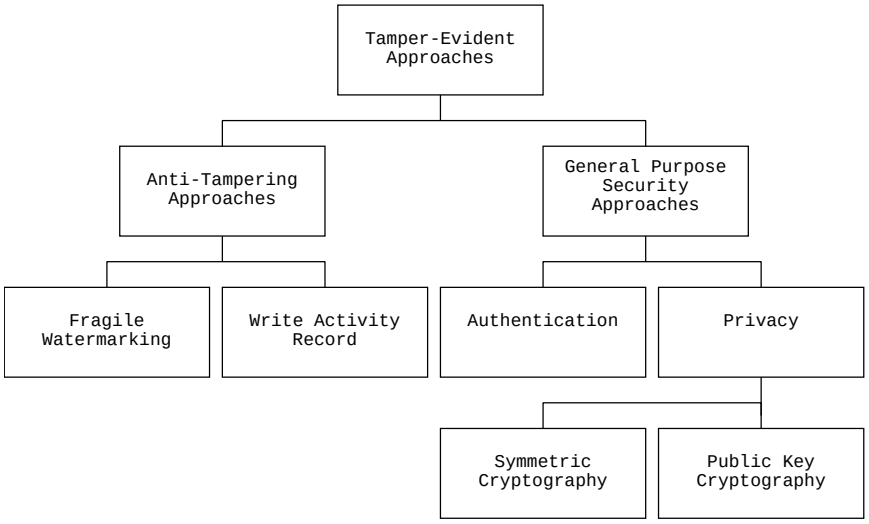

Fig. 2 Tamper-evident approaches

- the Object Class that identifies the kind of object,
- the Serial Number that is used by the manufacturer to unambiguously identify the tagged item.

Since the format of the first three data fields is set by the standard but the serial number is directly managed by the companies, the authors propose to embed the watermark into the serial number. The fragile watermark is reached by performing 3 one-way functions respectively on the EPC Manager, the Object Class, and the original Serial Number. The check of the watermark requires the knowledge of its location inside the EPC, and the adopted one-way functions, so these data shall be shared by the partners that aim to guarantee the authenticity of the information by adopting the described approach. This system allows detecting tampering on the EPC Manager, the Object Class, and the original Serial Number. When tampering actions are detected, the system detects the tampered area with a discrimination of one among the three data, and the watermark.

In [10], an implementation of the system described in [9] is proposed. The watermark requires 8 bits out of the 32 bits of the Serial Number, and it is generated as a hash number by the EPC Manager, and the Object Class, through a pseudo random

Header	EPC Manager	Object Class	Serial Number
8-bit	28-bit	24-bit	36-bit

Fig. 3 Standard EPC96: Tag Memory Organization

number generator. The function is not applied on the Serial Number, since tampering actions on it are not considered dangerous by the authors. One additional bit from the Serial Number is required as parity bit of the watermark.

The authors conclude that the short length of the watermark could affect the robustness of the tamper detection system, but this problem could be avoided by adding an additional memory area for the watermark.

A drawback of this implementation is that the watermarking is based on a secret function. Therefore, when an opponent obtains the function a huge modification of the system is required.

This system can be applied only to RFID tags that hold data compliant with EPC96. However, it could be easily extended to other standards. The RFID tags do not require special features. The communication protocols between the reader and tags have no special requirements. When the reader receives a writing request, it shall be able to generate the watermark and to embed it into the original data. The middleware is in charge of managing the checking protocol. The time required by the tamper check corresponds to the reading of 96 bits, and to the computation of the watermarking function.

The robustness of the system is based on the secrecy of the adopted function, and of the location of the watermark. However, this information shall be shared by all the entities involved in the trade of the tagged products, so the application of this system requires strong trust among participants. The system does not involve participants with limited permissions, e.g. the only tamper checking ability, so the method is vulnerable to insider attack, since a malicious participant can sabotage the

whole system. Furthermore, external companies or customers that want to buy the products cannot directly use the system in order to detect tampering.

According to the implementation proposed in [10], data impairing performed by an opponent that does not know the secret function and the location of the watermark is undetected only if performed on the bits of the original Serial Number. When the opponent knows the location of the watermark, it can impair all the bits of the original Serial Number. This action, else if limited to the Serial Number, can seriously *damage* some services, such as traceability management. As data impairing, also wrong data insertion can be performed only on the bits of the original Serial Number. However, the knowledge of the Serial Number format adopted by a company makes easier to find the location of the watermark. This malicious action can more effectively damage services, since its consequences are deterministic. The data copying can be performed on the whole tag memory also without knowledge on the functions and on the location of the watermark, since by copying both the original data and the watermark no incoherence is generated. This action triggers critical troubles, since all the data can be *altered*, and when performed on RFID tags for item management, it can generate various mistakes.

This scheme can be used both to detect tampering with tag memories that do not present any other protections (e.g. password), and as additional protection. The application of the system, according to the restriction to EPC compliant tags, is almost limited to item management systems. The extension to other tag types and RFID systems is also possible. The strength of this scheme is that it is compliant with RFID tag limitations, because no additional computation effort is charged on tags, and no additional memory is required. However, the provided protection against tampering is limited. The introduction of watermarking can defend against random tampering attacks performed to the purpose of impair generic tags, but it is weak against an adversary with proper means.

4.2 Write activity record for RFID data tamper detection

Yamamoto et al. have proposed a method for tamper detection based on write activity record [11]. In this approach the RFID tag has a special memory area that RFID readers can only read, and that the tag itself can read and write. When a writing operation is performed on the tag memory by a reader, the tag writes a record that describes the operation in the special memory area. A writing operation is described by the offset of the written memory area, and by the length of the written data. The first information in the special memory area represents the pointer to the area for the next insertion, and the number of recorded writing operations.

The tamper detection method requires the check of the records in the special memory area, in order to check if some data have been overwritten on previous data. If there is no overlap, then the memory has not been tampered. Otherwise if some memory areas have been overwritten, then data could be tampered.

The authors have proposed and tested an implementation that requires 2 bytes for each record of the special memory area. Therefore, the special memory area shall be very large, in order to hold more than one record for each memory bank. Furthermore, the protocol should be able to manage effectively a number of writing operations greater than the number of records in the special memory area, in order to avoid that several writing operations on the same bank could hide tampering on other banks.

The tamper detection can be performed without special permissions, so every company or customer can check if tags have been tampered.

This system can be applied to RFID tags, regardless of their data organization and format. The RFID tags require an additional special memory area, and a special writing protocol. The middleware shall manage the checking protocol; while, the communication protocol and the RFID reader do not present special requirements. The time required by the tamper check corresponds mainly to the reading of memory slots of 2 bytes for each performed writing. This overhead corresponds to a drawback in many critical and real-time applications.

This approach allows detecting all the tampering actions, but it detects as possible tampering also each rewriting operation. Therefore, it is not suitable for an Information System that uses the same memory area more than once, e.g. internal traceability systems based on reusable containers [4]. Furthermore, applications that allow operators to correct writing operations of wrong data, by writing the correct information on the same memory bank, will generate several false tamper detections, according to the error rate of human operators. The suitability of the system requires that the number of false detections should be very small. Another drawback of the system is that only tampering with written memory banks can be detected, but wrong data insertion and data copying on unused banks cannot be detected.

This approach requires the design of new tags, currently not available, which would be compliant with existing standards. The main drawbacks of this approach are the large memory requirement, the long transmission time for tamper checking, and the limited applicability. However for some applications where a high cost per tag is acceptable, it can provide a good security against data tampering attacks performed by RF channel.

4.3 Public key cryptography for authentication

Various protocols for authentication employ cryptography and RFID tags without cryptographic capability. In these approaches the cryptographic operations are not performed by the tag, which only contains the encrypted data. Typically, a critical code is encrypted using a secret key and a public key cryptosystem in order to get a signature. The public key is given to all the entities that have to check the authenticity of the product matched with the tag. The authenticity checking requires the decryption of the signature, and the comparison with the original code.

An authentication approach based on RSA was proposed in [13]. In this approach the ID of the tag is encrypted and written in the user memory. The authenticity checking corresponds to the decryption of the number in the user memory. When

the result does not correspond to the ID, the tag and the corresponding product are considered false.

An authenticity check on a tag, where some bits of the signature have been impaired, recognizes the tag and the product as false. An opponent cannot insert wrong data, since this action requires the knowledge of the secret key. The copying of the signature from other tags generates false tags, so it is equivalent to the data impairing. The tamper detection can be performed only by the authenticity check, but this operation cannot distinguish between a not authentic tag written by an adversary and an original tag written by the competent entity and tampered by an attacker.

Authentication protocols can provide tamper-evidence, but they require tags with a large memory and long data transmissions. Furthermore, it is not possible to distinguish if a tag is not original or it has been tampered, and the tamper-evidence is not extended to other information contained by the tag. Therefore, authentication schemes based on public key cryptography for RFID tags without cryptographic capability are not effective tamper-evident approaches. The *damaging* effects due to false positives generates a medium/high impact according to the importance of the authentication, so tags with additional tamper-resistant features are required in order to reach a high difficulty for attackers and to reduce the risk from medium/high to low.

4.4 Cryptography for privacy protection

Many applications uses secret or private information, employing RFID tags without cryptographic capability that contain secret or private information. A possible solution to avoid unauthorized readings of the recorded data is represented by the encryption.

In a symmetric cryptosystem, all the participants own the key, so they can perform both encryption and decryption. However, this system requires a strong trust among the participants, since the robustness of the system is based on the secrecy of the key.

Another approach is to employ Public key cryptography. Two alternative methods have been presented in [15]. These methods aim at providing food traceability with privacy protection. They involve a competent authority (i.e. the same authority

that monitors food traceability) that supervises the security mechanism. In the former method, the information are reserved to the competent authority, which generates the keys employed in the system. Each company encrypts its data by using a public key deployed by the authority. In order to improve the security, the ciphertexts are nested. Each company attaches its information to the encrypted data written by the previous company on the RFID tag, and it encrypts the resulting text by using a key with the same length of the new plaintext (corresponding to the length of the previous key increased by the length of the new data). Only the authority owns the secret keys, so companies and customers cannot read the data. In the latter method, also the companies generate a couple of keys, and they give the public key to the authorities. The information is encrypted by companies using both the authority-public key and the company-private key, in order to guarantee both the privacy and the authenticity of the information.

Another interesting protocol is Insubvertible Encryption [14], which aims at protecting privacy, and employs a public-key cryptosystem based on ElGamal encryption [37] for privacy protection. In this scheme the data written in the tag memory are encrypted and can be re-encrypted by an authorized user without knowledge on the keys previously used. The scope of the re-encryption is to change the context of the tag in order to avoid tracking. This scheme is tamper-evident, since the entity that performs the re-encryption can identify if the ciphertext has been tampered.

In cryptosystems that manage also the authenticity, as described in Section 4.3, the tamper detection can be performed only by the authenticity check, but this operation cannot normally distinguish between a not authentic tag and a tampered one. Instead, in cryptosystems that encrypt information only for privacy, data impairing is detected by decryption, so only authorized entities can check it. Wrong data insertion is possible only for opponents with the secret key. The data copying of the whole memory can be performed avoiding detection only when the protocol does not encrypt a reference information, that unambiguously identifies the item or the tag. However, only systems where tags are not suspected to be not authentic are effectively tamper-evident.

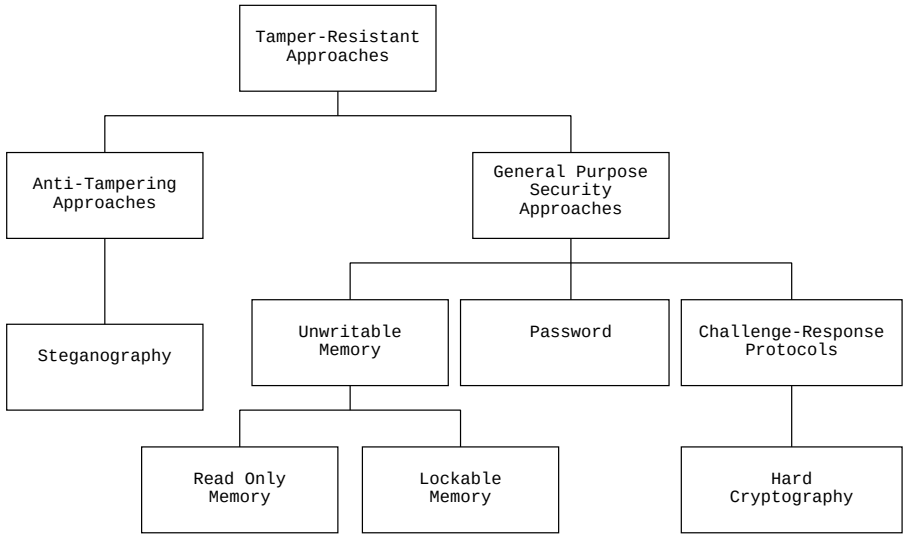

Fig. 4 Tamper-resistant approaches

5 Tamper-resistant approaches

In this section one approach specifically designed for tamper-resistant RFID tag is detailed. Furthermore, some security tamper-resistant general purpose approaches are described. A classification of tamper-resistant approaches is shown in Figure 4. According to the evaluation method presented in [32], these schemes aim at increasing the difficulty for adversaries to tamper with data in tag memories.

5.1 Steganography for RFID tag data recovery

The steganography is the ability to hide information. In [12] an approach based on steganography that aims at recovering tampered data on RFID tag memories compliant with EPC96 is presented.

According to the approaches described in Sec. 4.1, the approach proposed in [12] is based on the statement that opponents could get benefits only by tampering with the EPC Manager and Object Class, and that the Serial Number is the best area to embed security bits.

Authors propose to select a group of products of the same consignment that are characterized by the same EPC Manager and Object Class, to split in groups of bits the secret pattern generated from the EPC Manager and the Object Class of the tags, and to embed each group of bits in the Serial Number of a tag. The secret pattern is computed using error correction codes, and its length is equal to the sum of the lengths of the EPC Manager, the Object Class, and some bits required by the formula. Error correction codes help to recover data, when also the Serial Number has been tampered. Authors propose an implementation where the length of the pattern is 66 bits. Therefore, these 66 bits are devised in groups, and each group is embedded in a tag memory. Then for each group it calculates the parity bit, which is embedded in the Serial Number of the subsequent tag. The tamper detection and recover procedure consists in checking the parity bit, and performing the error correction coding. The parity bit aims at detecting tamper with the Serial Number, and the secret pattern is used to generate the original EPC Manager and Object Class. Also when few bits of the secret pattern have been tampered, the error correction coding can calculate the right original data.

This system can be applied only to RFID tags that hold data compliant with EPC96. The RFID tags do not require special features. The protocols of communication between the reader and tags are compliant with standards. Writing operation shall be managed according to the group division of the tags, in order to embed correctly the security bits. The middleware is in charge of the checking protocol. The time required by the tamper checking and recovery, which may be performed on a whole group of tags, corresponds to the reading of 96 bits for each tag, and to the computation of the error correction coding.

The system can be applied only to indivisible set of products, since the lack of some tags makes the recovery system unusable, and the tamper detection possible only when both a tag and the subsequent one are available. The robustness of the system is based on the secrecy of the location of the secret information and on the error correction coding. However, this information shall be shared by all the entities that are

involved in the trade of the tagged products; so the application of this system requires strong trust among participants. The system does not involve participants with limited permissions, so a malicious participant can sabotage the whole system. Furthermore, external companies and customers that want to buy the products cannot directly use the system in order to detect tampering.

As for tamper detection approaches described in Sec. 4.1, data impairing performed by an opponent that does not know the secret function and the location of the secret pattern is undetectable only if performed on the bits of the original Serial Number. When the opponent knows the location of the secret pattern, he/she can impair all the bits of the original Serial Number. When the data impairing alters too many bits of the secret pattern, the recovery cannot be performed. As data impairing, also wrong data insertion can be performed avoiding detection only when performed on the bits of the original Serial Number. However, opponents that know the meaning of data in the Serial Number can easily find the secret pattern. Since the system shall be applied to groups of products of the same set, the data copying of the whole tag memory can be easily detected. However, the copy of all the data of a group of tags, on a different group cannot be detected by this approach.

This scheme can be used to recover tampered data on tag memories that have no other protections (e.g. access password), or as additional protection. The application of the system, according to the restriction to EPC compliant tags, is generally limited to item management systems. The application restriction to indivisible groups of items and the low protection level strictly limits the applicability of this scheme.

5.2 Unwritable Memory

RFID tags with unwritable memory are tamper-resistant. They can be divided in two groups according to the memory characteristics:

- read-only memory, as the memories that hold only the ID;
- permanently lockable memory, such as in the EPC Class I Gen 2 Standard [21], where after being locked with a password the memory becomes unlockable.

A great benefit of systems that employ these kinds of tags is the strong tamper-resistance. Although these RFID tags cannot be used for applications which require the ability to record information on the tags (e.g. internal tracking with reusable containers [2,38]), when they are applicable (e.g. supply chain management [1]) they represent the strongest solution. Also for authentication systems, unwritable memory are an effective solution, especially when the tag memory contains a signature. Tags with a permanently lockable memory are more versatile than tags with a read only memory, and if the locking is correctly managed, they provide the same tamper-resistant level.

5.3 Passwords

A basic protocol that authenticates readers can employ passwords. In this case a reader needs the correct password in order to access to the tag memory. However, an eavesdropper can listen the password and use it for unauthorized accesses to the tag. The optional use of 32-bit passwords is required by EPC Class I Gen 2 [21]. When a password is used to write into memory area, the tag sends a random number to the reader, which performs a bitwise XOR operation between the password and the random number, and then it sends the result to the tag. An adversary that can only eavesdrop reader to tag communication, but not the other direction, is not able to find the password. However, an adversary that can eavesdrop both the directions of the communication can easily find it.

The strength of passwords is that they are easy to implement, and they are also managed by low cost tags. However, the simple use of password increases the difficulty for adversaries to tamper with RFID data, since this action requires eavesdropping, but does not stop it. Furthermore, the use of password cannot be applied to systems where generic users have the writing privilege.

5.4 Challenge-Response Protocols

In a challenge-response authentication protocol an entity presents a question, and a second entity properly answers. When the answer is incorrect the second entity is considered not valid. The authentication can be unilateral or mutual. Several methods that implement challenge-response authentication can be applied to RFID technology.

Advanced protocols employ cryptography [39]. An example that employs symmetric key encryption, unilateral authentication, and random number, can be based on ISO/IEC 9798-2 [40]. Both the tag and the reader own the secret key. The tag sends a random number to the reader, which encrypts it using the secret key and which sends back the ciphertext. The described protocol requires tags with enough computation capacity to perform symmetric-key encryption and to generate random or suitable pseudo-random numbers. The robustness of the protocol is related to the difficulty to predict the pseudo-random number and to the length and the security of the employed keys. An example of RFID tags with cryptographic capability is DEFfire from Philips [23], which can perform AES/DES operations.

The only ways to tamper with data on a tag that employs a challenge-response authentication protocol based on symmetric key encryption are breaking the encryption scheme, finding the secret keys or predicting/altering the pseudo-random number generation. When the employed cryptosystem is strong enough, challenge-response protocols represent a strong solution. Moreover, they can be employed for applications that require rewritable memories, provided that only authorized users have to write on the tags. However, the main drawback is the additional cryptographic modulo required by tags, which increases the cost per tag, and can reduce the reading range, according to the higher power supply required by the tag.

6 Discussion

During the last years, many approaches have been proposed for security problems aiming at protecting from tampering, and in particular various tamper-evident and

Table 1 Requirements Comparison of Anti-Tampering Approaches respect to EPC Class I Gen 2 Standard

Approach	Requirements		
	tags	readers/ middleware	communication
Watermarking [10]	standard (EPC96)	watermark generation	standard
Write activity [11]	special memory area special writing protocol	standard	standard
Authentication [13]	standard (large user memory)	standard/ encryption	standard
Privacy protection [15]	standard (large user memory)	standard/ encryption	standard
Steganography [12]	standard (EPC96)	standard	standard
Permanently lockable memory [21]	standard (lockable)	standard	standard
Password [21]	standard (password)	standard	standard
Challenge-Response Authentication [23]	encryption	standard/ encryption	Challenge-Response

tamper-resistant approaches have been proposed for RFID tags. These approaches are characterized by different properties, requirements, and applications. Furthermore, each approach has specific benefits and drawbacks.

In order to analyze the feasibility of anti-tampering approaches, their requirements have to be considered. Table 1 shows the main characteristics of RFID tags, readers and communications protocols that are required by anti-tampering approaches. The compared authentication and privacy protection approaches are based on messages encrypted with public key cryptography and embedded in the tag memory. The requirements for the readers and the middleware are the easiest to satisfy, adding additional software modules to the middleware, or implementing their functionalities directly on the reader, also when these modules require relevant computational effort. Requirements that modify the communication standards often involve longer communication sessions and generate incompatibility with standard devices. However, the only approach that has special requirements for communication is the Challenge-Response Authentication, which is naturally limited to authorized tags and readers. Each approach presents some requirements for RFID tags, which are the most difficult to

Table 2 Protection Comparison of Anti-Tampering Approaches

Approach	Tampering Threats		
	data impairing	wrong data insertion	data copying
Watermarking [10]	tamper-evident[1]	tamper-evident[1]	possible
Write activity [11]	tamper-evident[2]	tamper-evident[2]	tamper-evident[2]
Authentication [13]	possible	possible	possible
Privacy protection [15]	tamper-evident	tamper-evident	possible
Steganography [12]	tamper-evident[1] light resistance	tamper-evident[1] light resistance	possible light resistance
Permanently lockable memory [21]	tamper-resistant	tamper-resistant	tamper-resistant
Password [21]	tamper-resistant	tamper-resistant	tamper-resistant
Challenge-Response Authentication [23]	tamper-resistant	tamper-resistant	tamper-resistant

[1] According to the analyzed implementation tampering with the original Serial Number cannot be detected.
[2] Tampering with blank memory banks cannot be detected.

satisfy. The Challenge-Response Authentication and the Write activity scheme present requirements not addressed by the standards, which involve high cost tags with additional hardware modules. Authentication and privacy protection approaches require large user memories, increasing the cost. The tag requirements of the other schemes can be accomplished without excessive effort.

Table 2 compares the protection against data-tampering threats of both approaches designed for tampering, and general security approaches. One implementation for each approach is used as reference in the table. A tamper threat is defined as "possible" when the requirements of the approach are satisfied and it can still be performed. The definition "light resistance" is used when tampering can be performed, and the data recovery could be possible. Observing Table 2, we can find that only one method is tamper-evident against data copying, but only for tampering with written memory banks, so the protection from this attack represents a relevant open issue for RFID tamper-evident research studies. Examining the general purpose security techniques, we can find that although tag authentication protocols do not provide any effective pro-

Table 3 Robustness Comparison of Anti-Tampering Approaches

Approach	Robustness Factors	RFID Drawbacks
Watermarking [10]	length of the watermark function secrecy watermark location secrecy participant trust	area in the EPC code difficult updating insider vulnerable
Write activity [11]	no rewritings special memory length	tampering and rewriting unnoticeable memory area
Privacy protection [15]	length of the keys key secrecy	memory area and transmission time
Steganography [12]	length of the code error correction coding watermark location secrecy participant trust	area in the EPC code multiple tags insider vulnerable
Permanently lockable memory [21]	hardware	
Password [21]	password secrecy password length password number	eavesdropper vulnerable memory area memory area
Challenge-Response Authentication [23]	length of the keys key secrecy	tag computation

tection against tampering, privacy protection systems present effective tamper-evident features.

A critical characteristic for the evaluation of an approach is represented by its robustness, since a protocol that protects against all tamper threats but can be easily broken is not acceptable. Table 3 shows the main factors that affect the robustness of a method, and the related drawbacks due to RFID technology, such as additional memory area, which increases the cost, and additional computation, which increases the time and consumption. The most robust tamper-evident approach is represented by the Write activity scheme. However, it requires a large memory to store the writing activities. The tamper-evidence provided by the privacy protection approach is quite high, but it does not address data copying, and it requires a large memory. The robustness of the Watermarking scheme is lower, mainly because it is based on several factors, such as the length of the watermark and the trust among participants, which are not easy to fully satisfy. The most robust tamper-evident approach is the Permanently lockable

Table 4 Tamper Checking Comparison of Tamper-evident Approaches

Approach	Detection Ability Owner	Checking Time
Watermarking [10]	participants	96-bit reading watermarking function
Write activity [11]	public	reading of 2 bytes for performed writing
Privacy protection [15]	authority	whole ciphertext reading decryption

memory, since it is protected against RF attacks. Also the Challenge-Response Authentication is robust, but it requires relevant tag computation capability. The Password approach is exposed to brute force attacks, which are addressed by long passwords, and to eavesdropping attacks, which represents the weak spot of this approach. The Steganography approach does not provide high robustness, since tampering with the watermark location prevents data recovery.

Table 4 shows the characteristics of tamper checking. The number of entities that can check the tamper presence affects the usefulness of the system, since a restricted number of possible users lead to difficulties to detect tampering. Also the number and the kind of operations is important, since they affect the performance of the system. However, as shown in Table 4, the RFID-specific tamper-evident approaches do not require too long operations, so they are quite fast; instead, the general privacy protection approach, which involves cryptography, requires more computation time.

Table 5 shows the tamper-evident approaches sorted according to their robustness, and the restrictions to their applicability. According to the decrease of the robustness, the schemes can be more widely applied. The *Write activity* scheme can be used only for applications that do not require more than one writing operation per memory bank (e.g. supply chain management). *Privacy protection* can be used for every type of application, but it requires that all the participants own the keys. The *Watermarking* scheme can be used for applications that employ tags compliant with EPC96 standard, which is normally used for item management.

For applications that do not require rewriting the *Write activity* approach is the best solution. However, it requires expensive tags. For applications that require rewrit-

Table 5 Applicability Comparison of Tamper-evident Approaches

#	Approach	Applicability Restrictions
1	Write activity [11]	No corrections or updates
2	Privacy protection [15]	Participants with keys
3	Watermarking [10]	EPC96 data format

ing, and only authorized users have to access tags, a good tamper-evident solution is represented by the *Privacy protection* approach. However, also this approach requires quite expensive tags. For the other applications where data are compliant with EPC96, or when the tag cost is a critical parameter, the *Watermarking* approach can represent a good solution. However, the provided tamper-evidence is limited.

Although tamper-evident approaches reduce the *alteration* effects of tampering to *damage*, according to Section 3, tamper-resistant approaches can provide better protection against both *alteration* and *damage*. Table 6 shows the tamper-resistant approaches sorted according to their robustness, and the restrictions to their applicability. As for tamper-evident schemes, according to the decrease of the robustness, they can be more widely applied. The *Permanently lockable memory* approach can be used only for applications that do not require rewriting, similarly to the *Write activity* approach. The *Challenge-Response Authentication* and the *Password* schemes can be used for every type of application, but they require that the participants with writing privilege own the keys or passwords. The *Steganography* approach can be used for applications that employ tags compliant with EPC96 standard, as the *Watermarking* approach.

For applications that do not require rewriting the Permanently lockable memory approach is the best solution. Moreover, it can be implemented with low cost tags. Therefore, for these application the *Permanently lockable memory* approach is better than the *Write activity* scheme. For applications that require rewriting, and where only authorized users have to write tags, the *Challenge-Response Authentication* can be a good solution. However, this approach requires very expensive tags. When low cost tags are required, the same kind of applications managed with the *Challenge-Response Authentication* can employ the *Password* approach, but they provide less security, being exposed to eavesdropping. In order to reach a higher security the *Password*

Table 6 Applicability Comparison of Tamper-resistant Approaches

#	Approach	Applicability Restrictions
1	Permanently lockable memory [21]	No corrections or updates
2	Challenge-Response Authentication [23]	Participants with keys
3	Password [21]	Participants with password
4	Steganography [12]	EPC96 format, Inseparble tags

approach can be used together with *Privacy protection*. For the other applications where data are compliant with EPC96, or when the tag cost is a critical parameter, the *Steganography* scheme can represent a solution, but only if inseparable set of tags are used. This approach provides low tamper-resistance, but it provides also limited tamper-evidence.

The main open issues for tamper-resistant solutions are represented by the lack of cheap and robust schemes applicable to tags with rewritable memory. Tamper-evident approaches lack of robust schemes based on low cost tags, and the lack of schemes usable for a generic application. Especially data copying requires to be carefully managed by future tamper-evident approaches. Watermarking-based schemes seem a quite effective low cost solution, but it should be extended to tags with different memory organizations.

7 Conclusion

Tampering is one of the most dangerous threats for RFID systems, especially data-tampering, which cannot easily be addressed with standard methods. In this paper the characteristics and the effects of tampering have been described. The peculiarities of tampering with RFIDs and in general with pervasive technologies have been detailed. Tamper-evident and tamper-resistant approaches for RFID have been surveyed and classified. Furthermore, other general purpose RFID security techniques have been described, analyzing their protection against tampering attacks.

The comparison of the described approaches highlighted their benefits and drawbacks. Among the various approaches the main protection is given by the tamper-

resistant general purpose ones, but these methods involve either strict limitations to RFID applications, or RFID tag computational capacity. The RFID-specific tamper-evident approaches do not require relevant computational capacity, but either their robustness is limited or their applicability is narrow. The main open issue is represented by the lack of tamper-evident approaches that are able to effectively manage data copying.

Acknowledgements This work has been partially supported by the grant "Nano-materials and -technologies for intelligent monitoring of safety, quality and traceability in confectionery products (NAMATECH)" from Regione Piemonte.

References

1. Atock, C.: Where's my stuff? Manufacturing Engineer **82**(2), 24–27 (2003)
2. Gandino, F., Montrucchio, B., Rebaudengo, M., Sanchez, E.: Analysis of an RFID-based information system for tracking and tracing in an agri-food chain. In: RFID Eurasia, 2007 1st Annual, pp. 1–6 (2007)
3. Finkenzeller, K.: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley & Sons, Inc., New York, NY, USA (2003)
4. Gandino, F., Montrucchio, B., Rebaudengo, M., Sanchez, E.: On improving automation by integrating RFID in the traceability management of the agri-food sector. Industrial Electronics, IEEE Transactions on **56**(7), 2357–2365 (2009)
5. Juels, A.: RFID security and privacy: a research survey. Selected Areas in Communications, IEEE Journal on **24**(2), 381–394 (2006)
6. Collberg, C., Thomborson, C.: Watermarking, tamper-proofing, and obfuscation - tools for software protection. Software Engineering, IEEE Transactions on **28**(8), 735–746 (2002)
7. Spiekermann, S.: RFID and privacy: what consumers really want and fear. Personal and Ubiquitous Computing **13**(6), 423–434 (2009)
8. Spiekermann, S., Evdokimov, S.: Critical RFID privacy-enhancing technologies. Security & Privacy, IEEE **7**(2), 56–62 (2009)
9. Potdar, V., Wu, C., Chang, E.: Tamper detection for ubiquitous RFID-enabled supply chain. In: Computational Intelligence and Security - CIS 2005, LNCS, pp. 273–278. Springer Berlin / Heidelberg (2005)
10. Potdar, V., Chang, E.: Tamper detection in RFID tags using fragile watermarking. In: Industrial Technology, 2006. ICIT 2006. IEEE International Conference on, pp. 2846–2852 (2006)

11. Yamamoto, A., Suzuki, S., Hada, H., Mitsugi, J., Teraoka, F., Nakamura, O.: A tamper detection method for RFID tag data. In: RFID, 2008 IEEE International Conference on, pp. 51–57 (2008)
12. Mohan, M., Potdar, V., Chang, E.: Recovering and restoring tampered RFID data using steganographic principles. In: Industrial Technology, 2006. ICIT 2006. IEEE International Conference on, pp. 2853–2859 (2006)
13. Bernardi, P., Gandino, F., Lamberti, F., Montrucchio, B., Rebaudengo, M., Sanchez, E.: An anti-counterfeit mechanism for the application layer in low-cost RFID devices. In: Circuits and Systems for Communications, 2008. ECCSC 2008. 4th European Conference on, pp. 227–231 (2008)
14. Ateniese, G., Camenisch, J., de Medeiros, B.: Untraceable RFID tags via insubvertible encryption. In: CCS '05: Proceedings of the 12th ACM conference on Computer and communications security, pp. 92–101. ACM, New York, NY, USA (2005)
15. Bernardi, P., Demartini, C., Gandino, F., Montrucchio, B., Rebaudengo, M., Sanchez, E.: Agri-food traceability management using a RFID system with privacy protection. In: Advanced Information Networking and Applications, 2007. AINA '07. 21st International Conference on, pp. 68–75 (2007)
16. Zhong, S., Yang, Y.R.: Verifiable distributed oblivious transfer and mobile agent security. Mobile Networks and Applications **11**(2), 201–210 (2006)
17. Kitsos, P., Zhang, Y. (eds.): RFID Security: Techniques, Protocols and System-On-Chip Design. Springer Publishing Company, Incorporated (2008)
18. Ahson, S.A., Ilyas, M. (eds.): RFID Handbook : Applications, Technology, Security, and Privacy. CRC Press (2008)
19. Garfinkel, S., Juels, A., Pappu, R.: RFID privacy: an overview of problems and proposed solutions. Security & Privacy, IEEE **3**(3), 34–43 (2005)
20. Sheng, Q., Li, X., Zeadally, S.: Enabling next-generation RFID applications: Solutions and challenges. Computer **41**(9), 21–28 (2008)
21. EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz 960 MHz (2004)
22. Ranasinghe, D.C., Engels, D.W., Cole, P.H.: Low-cost RFID systems: Confronting security and privacy. In: Auto-ID Labs Research Workshop (2005)
23. MF3ICD21, MF3ICD41, MF3ICD81 - MIFARE DESFire EV1 contactless multi-application IC. Product short data sheet (2009). Rev. 02
24. Boss, R.W.: RFID technology for libraries. Library Technology Reports **39**(6) (2003)
25. Zachary, J., Brooks, R.: Bidirectional mobile code trust management using tamper resistant hardware. Mobile Networks and Applications **8**(2), 137–143 (2003)

26. Hartenstein, H., Laberteaux, K.: Topics in ad hoc and sensor networks - a tutorial survey on vehicular ad hoc networks. Communications Magazine, IEEE **46**(6), 164–171 (2008)
27. Obowoware, O.: Security issues in mobile ad-hoc networks: A survey. The 17th White House Papers Graduate Research In Informatics at Sussex pp. 40–44 (2004)
28. Chen, S., Xu, J., Sezer, E.C., Gauriar, P., Iyer, R.K.: Non-control-data attacks are realistic threats. In: SSYM'05: Proceedings of the 14th conference on USENIX Security Symposium, pp. 12–12. USENIX Association, Berkeley, CA, USA (2005)
29. Zhang, K., Zhang, T., Pande, S.: Memory protection through dynamic access control. In: Microarchitecture, 2006. MICRO-39. 39th Annual IEEE/ACM International Symposium on, pp. 123–134 (2006)
30. Potdar, M., Chang, E., Potdar, V.: Applications of RFID in pharmaceutical industry. In: Industrial Technology, 2006. ICIT 2006. IEEE International Conference on, pp. 2860–2865 (2006)
31. Miklau, G., Suciu, D.: Implementing a tamper-evident database system. In: Advances in Computer Science ASIAN 2005, LNCS, pp. 28–48. Springer Berlin / Heidelberg (2005)
32. Garcia-Alfaro, J., Barbeau, M., Kranakis, E.: Analysis of threats to the security of EPC networks. In: Communication Networks and Services Research Conference, 2008. CNSR 2008. 6th Annual, pp. 67–74 (2008)
33. ETSI 4.2.1-Telecommunications and internet converged services and protocols for advanced networking (TISPAN); methods and protocols; part 1: Method and proforma for threat, risk, vulnerability analysis (2006). Technical Specification
34. Garcia-Alfaro, J., Barbeau, M., Kranakis, E.: Security threats on EPC based RFID systems. In: Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on, pp. 1242–1244 (2008)
35. Howard, M., Leblanc, D.: Writing Secure Code. Microsoft Press, Redmond, WA, USA (2001). Foreword By-Valentine,, Brian
36. Bellare, M., Canetti, R., Krawczyk, H.: Keying hash functions for message authentication. In: Advances in Cryptology CRYPTO 96, LNCS, pp. 1–15. Springer Berlin / Heidelberg (2005)
37. Elgamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. Information Theory, IEEE Transactions on **31**(4), 469–472 (1985)
38. Karkkainen, M.: Increasing efficiency in the supply chain for short shelf life goods using RFID tagging. International Journal of Retail & Distribution Management **31**(10), 529 – 536 (2003)
39. Menezes, A.J., Vanstone, S.A., Oorschot, P.C.V.: Handbook of Applied Cryptography. CRC Press, Inc., Boca Raton, FL, USA (1996)

40. International Organization for Standardization, Geneva, Switzerland: ISO/IEC 9798-2 - Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms (1994)