Journal of Medical Systems manuscript No.
(will be inserted by the editor)

Two RFID Standard-based Security Protocols for Healthcare Environments

Pablo Picazo-Sanchez · Nasour Bagheri · Pedro Peris-Lopez · Juan E. Tapiador

Received: date / Accepted: date

Abstract Radio Frequency Identification (RFID) systems are widely used in access control, transportation, real-time inventory and asset management, automated payment systems, etc. Nevertheless, the use of this technology is almost unexplored in healthcare environments, where potential applications include patient monitoring, asset traceability and drug administration systems, to mention just a few. RFID technology can offer more intelligent systems and applications, but privacy and security issues have to be addressed before its adoption. This is even more dramatical in healthcare applications where very sensitive information is at stake and patient safety is paramount. In [43], Wu *et al.* recently proposed a new RFID authentication protocol for healthcare environments. In this paper we show that this protocol puts location privacy of tag holders at risk, which is a matter of gravest concern and ruins the security of this proposal. To facilitate the implementation of secure RFID-based solutions in the medical sector, we suggest two new applications (authentication and secure messaging) and propose solutions that, in contrast to previous proposals in this field, are fully based on ISO Standards and NIST Security Recommendations.

Keywords RFID · Healthcare · Privacy · Standards

Pablo Picazo-Sanchez
Department of Applied Mathematics, University School of Computer Science (UPM) of Madrid. E-mail: ppicazo@eui.upm.es

Nasour Bagheri
Department of Electrical Engineering, Shahid Rajaee Teachers Training University, Tehran, Iran. E-mail: nbagheri@srttu.edu

Pedro Peris-Lopez and Juan E. Tapiador
Department of Computer Science, Universidad Carlos III de Madrid, Spain. E-mail: {pperis, jestevez}@inf.uc3m.es

1 Introduction

Radio Frequency Identification (RFID) is a technology for remote identification using radio waves. An RFID system is composed of tags, readers and a database for access and authentication management procedures. There are three different types of tags according to their source of power. Active tags –the most expensive– are equipped with a battery and can start a connection with a reader by themselves. Passive tags are the cheapest ones, do not have any on-board source of power and harvest energy from the reader signal. Semi-passive tags lie somewhere in between both classes, as they use their own battery for computations but collect energy from the reader signal for communication purposes.

Tying up RFID technology and healthcare environments has been the focus of much research recently due to the potential benefits that this technology could offer, both in terms of savings in operational costs and as enablers of novel applications [42,49]. As shown in Table 1, the range of healthcare problems where RFID could be successfully applied is significant, in some cases with important benefits. For example, the theft of newborn children is a worldwide problem that has recently made the news. It is claimed that in the last 50 years more than 300,000 newborns were abducted in Spain [27]. Similar cases have been reported in Australia [15], while in the US the National Center for Missing & Exploited Children has published some statistics about this alarming problem [31]. To address this problem, several hospitals in different countries have adopted a new –and controversial– RFID-based solution [3,25,44].

Security and privacy concerns associated with the widespread adoption of RFID systems in healthcare environments have been a major deterrent for the penetration of this technology in key application areas. In

Patient Traceability	[30,46]
Asset Management	[35,40]
Medication Administration	[2,50]
Handling Errors	[9,36]
Ownership Transfer Procedures	[45,51]
Efficiency Management	[36,48]
Cost Savings	[7,47]

Table 1 Some healthcare applications of RFID technology.

the last five years, many works have addressed some of these issues by proposing different schemes that facilitate a secure execution of certain healthcare functions. The majority of such schemes have been soon proved insecure despite the claims made in their original proposals. For example, in 2009 Huang and Ku proposed a grouping proof to guarantee medication safety of inpatients [21]. Soon after it was shown that the scheme was vulnerable to Denial-of-Service (DoS) and replay attacks [13]. Chien *et al.* suggested a more secure version, but unfortunately an adversary can still conduct impersonation and replay attacks with a high success probability [37]. In this direction, the IS-RFID system proposed in [37] seems an interesting proposal to combat medication errors, but the system does not guarantee that the proofs cannot be manipulated by the hospital [50], which can be crucial in case of dispute due to malpractice. In 2012, Chen *et al.* [10] proposed a novel RFID-based tamper-resistant prescription access control protocol for different authorized readers. Yet again, the protocol was proved to suffer from impersonation, traceability and de-synchronization attacks [41].

1.1 Contributions and organization

Wu *et al.* have recently proposed a new RFID authentication protocol for healthcare environments [43]. Apart from guaranteeing some essential security properties, the protocol claims to solve the trade-off between location privacy and scalability in healthcare environments. A description of Wu *et al.*'s protocol is provided later in Section 2. In this paper, we first show that this protocol is vulnerable to a traceability attack that allows an adversary to compromise the location privacy of the tag's holder (e.g. a patient, doctor or nurse). The detailed description and analysis of this attack is provided in Section 3. Subsequently in Section 4 we propose authentication and secure messaging protocols based on established ISO standard and well-known security recommendations. In particular, we adapt an entity authentication protocol from ISO/IEC 9798 Part 2 and a secure messaging protocol from ISO/IEC 11770 Part 2 similar to that used in electronic passports. In addition, we discuss some implementation aspects and suggest specific primitives based on NIST 800-38A, NIST 800-38B, and NIST 800-108 recommendations. Finally, Section 5 concludes the paper by summarizing our main results.

2 Wu *et al.'s* Protocol

Wu *et al.* introduce in [43] a novel authentication protocol to be used in open environments such as academic medical centers or metropolitan and local community hospitals. The authors claim that the proposal solves the trade-off between location privacy and scalability in healthcare environments. Figure 1 shows the main steps involved in the scheme using the notation provided by Table 2.

The protocol consists of two different phases: setup and execution. In the setup phase, the server generates three $d \times d$ binary matrices (Key_1, Key_2, Key_3), where Key_1 is a nonsingular matrix and Key_3 is a singular one. After that, the server generates two matrices for each tag: $K_{T1} = Key_1 Key_3 S_T$ and $K_{T2} = Key_2 Key_3 S_T$, where S_T is a random matrix of size $d \times d$. The execution phase of the protocol is described below:

Step 1: The reader ($\mathbb{R}$) sends a query signal and a random value N_R to the tag.
Step 2: The tag ($\mathbb{T}$) generates a random value N_T and computes $c_1 = K_{T1} N_T$, $c_2 = K_{T2} N_T \oplus ID$, and $c_3 = h(c_1, K_{T2} N_R)$. Finally, the tag sends c_1, c_2, and c_3 to the reader.
Step 3: $\mathbb{R}$ appends N_R to the received messages c_1, c_2, and c_3 and forwards them to the server.
Step 4: The server computes $c_4 = Key_2 Key_1^{-1} \times c_1$ and recovers the ID by computing $c_4 \oplus c_2$. Then, the server checks if the calculated matrix key K_{T2} matches the received c_3. To do this, a local version of c_3 is computed as $c_3' = h(c_1, K_{T2}' n_R)$. If both are equal the reader authenticates the tag; otherwise the server informs the reader to restart the communication or simply reject it.
Step 5: The server computes $c_5 = h(c_4)$ and sends it to the tag.
Step 6: Finally, $\mathbb{T}$ checks if c_5 is equal to $h(K_{T2}' n_T)$. If so, the tag believes that this message comes from a valid reader (reader authentication).

3 Location Attack against Wu *et al.*'s Protocol

In this section, we show that the Wu *et al.*'s protocol fails to preserve the location privacy of a tag's holder. In

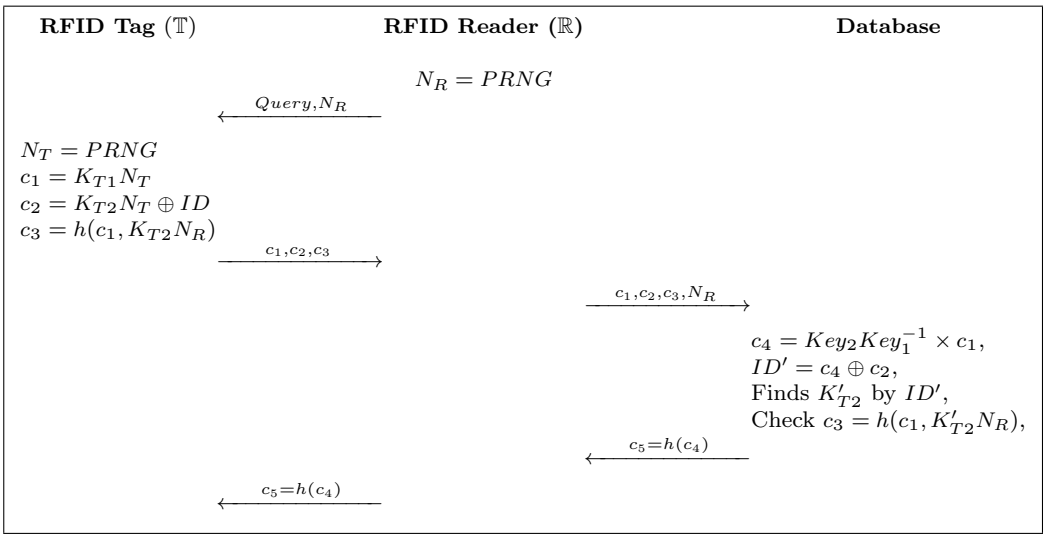


Fig. 1 Wu *et al.'s* Authentication Protocol [43].

K_T	Secret key of tag T
Key	Secret key of the server
ID	Identification number of the tag
N_R, N_T	Nonces chosen by the reader and the tag, respectively
$h(.)$	A hash function
$\oplus$	Bit-wise exclusive OR operation.
A^{-1}	Inverse of matrix A.
AB	Multiplication of matrices A and B

Table 2 Notation used in Wu *et al.'s* protocol [43].

fact, an adversary $\mathbb{A}$ can execute a successful traceability attack that requires to eavesdrop only a few authentication sessions. The details of the proposed attack are given below.

Wu *et al.* analyze extensively their protocol to prove that the proposed scheme provides location privacy. They claim that the adversary advantage to trace a given tag after q queries[1] is upper bounded by $\frac{q^2}{2^{l+1}}$, where l is the output length of the hash function used in the protocol. Nevertheless, we show how an active adversary can efficiently trace any given tag in this protocol with an advantage significantly higher than that. The presented attack is based on the following observation, which was missed by the designers:

Observation 1
Assume that $(A)_i$ denotes the i-th column of matrix A. Let X and X' be random binary matrices of size $d \times d$, and Y and Y' fixed binary matrices of size $d \times r$.

1. *If $(X)_i = (X')_j$ and $Y = Y'$, then $(Y \times X)_i = (Y' \times X')_j$ with probability 1.*
2. *If $(X)_i = (X')_j$ and $Y \neq Y'$, then $(Y \times X)_j = (Y' \times X')_j$ with probability 2^{-d}.*

Recall that in Wu *et al.*'s protocol, we have $c_1 = K_{T1}N_T$ and $c_2 = K_{T2}N_T \oplus ID$, where K_{T1} is a non-singular matrix. Thus, if $(N_T)_i = (N'_T)_j$ then:

$$(K_{T1}N_T)_i = (K_{T1}N'_T)_j$$

and

$$(K_{T2}N_T \oplus ID)_i = (K_{T2}N'_T \oplus ID)_j$$

Based on the above observation, an adversary $\mathbb{A}$ can perform the following steps to trace a target tag $\mathbb{T}$:

Phase 1 (Learning): $\mathbb{A}$ creates a table Tab with N rows and runs N sessions with the tag $\mathbb{T}$ as follows. At each run $1 \leq j \leq N$:

1. $\mathbb{A}$ sends $N_R^j \in \{0,1\}^l$ to the tag.
2. $\mathbb{T}$ generates a random value N_T^j and computes $c_1^j = K_{T1}N_T^j$, $c_2^j = K_{T2}N_T^j \oplus ID$ and $c_3^j = h(c_1^j, K_{T2}N_R^j)$. Finally, $\mathbb{T}$ sends c_1^j, c_2^j, and c_3^j to $\mathbb{A}$ (since he is acting as a reader).
3. $\mathbb{A}$ stores c_1^j and c_2^j in the j-th row of Tab.

[1] In the location-privacy game used in [43] a query represents the hash query of $\mathbb{T}$ or an anonymous query sent to $\mathbb{T}$.

Phase 2 (Execution): Given a tag $\mathbb{T}'$, the adversary proceeds exactly as in the learning phase, creating a table Tab' with N' columns and running N' sessions with $\mathbb{T}'$ as follows. At each run $1 \leq f \leq N$:

1. $\mathbb{A}$ sends $N_R^f \in \{0,1\}^l$ to the tag.
2. $\mathbb{T}'$ generates a random value N_T^f and computes $c_1^f = K_{T1}N_T^f$, $c_2^f = K_{T2}N_T^f \oplus ID$ and $c_3^f = h(c_1^f, K_{T2}N_R^f)$. Finally, $\mathbb{T}'$ sends c_1^f, c_2^f, and c_3^f to $\mathbb{A}$ (who, again, is acting as a reader).
3. $\mathbb{A}$ stores c_1^f and c_2^f in the f-th row of Tab.

Phase 3 (Decision): To decide whether $\mathbb{T}'$ is the target tag $\mathbb{T}$, the adversary checks:

- $\mathbb{T} \neq \mathbb{T}'$ if $\exists\ (c_1^j, c_2^j) \in Tab$ and $(c_1^f, c_2^f) \in Tab'$ such that $(c_1^j)_m = (c_1^f)_n$ but $(c_2^j)_m \neq (c_2^f)_n$, for all $0 \leq j \leq N$, $0 \leq f \leq N'$ and $0 \leq m, n \leq r-1$.
- Otherwise $\mathbb{T} = \mathbb{T}'$.

The total complexity of the given attack is N sessions in the learning phase plus N' sessions in the execution phase. The adversary's advantage, Adv_A, to make the correct decision in the third phase of the attack is defined as:

$$Adv_A = \left| Pr[A^{\mathbb{T}=\mathbb{T}'} \Rightarrow 1] - Pr[A^{\mathbb{T}\neq\mathbb{T}'} \Rightarrow 1] \right| \quad (1)$$

In order to determine Adv_A, we have to take into account the following considerations:

1. There are N entries in Tab, each of which includes a value for c_1 with r columns. There are, therefore, $N \times r$ columns in total. Similarly, there are $N' \times r$ columns for the values of c_1 in Tab'.
2. For each $(c_1^j)_m \in Tab$ and $(c_1^f)_n \in Tab'$ we have $(c_1^j)_m = (c_1^f)_n$ with probability 2^{-d}. Consequently, the expected number of matching columns for c_1 in Tab with those in Tab' is $(N \times r) \times (N' \times r) \times 2^{-d}$.
3. Given that $(c_1^j)_m = K_{T1}(N_T^j)_m$ and K_{T1} is a nonsingular, if $(c_1^j)_m = (c_1^f)_n$ and $\mathbb{T} = \mathbb{T}'$, then with probability 1 we have $(N_T^j)_m = (N_T^f)_n$ and $(c_2^j)_m = (c_2^f)_n$. However, if $(c_1^j)_m = (c_1^f)_n$ and $\mathbb{T} \neq \mathbb{T}'$, then with probability 2^{-d} we have $(c_2^j)_m = (c_2^f)_n$. Therefore, the probability of incorrectly believing that $\mathbb{T} = \mathbb{T}'$ when in fact $\mathbb{T} \neq \mathbb{T}'$ is given by:

$$Pr[A^{\mathbb{T}\neq\mathbb{T}'} \Rightarrow 1] = \left(2^{-d}\right)^{(N\times r)\times(N'\times r)\times 2^{-d}} \quad (2)$$

In summary, the adversary's advantage to successfully trace the target tag is:

$$\begin{aligned} Adv_A &= |Pr[A^{\mathbb{T}=\mathbb{T}'} \Rightarrow 1] - Pr[A^{\mathbb{T}\neq\mathbb{T}'} \Rightarrow 1] \\ &= 1 - \left(2^{-d}\right)^{(N\times r)\times(N'\times r)\times 2^{-d}} \end{aligned} \quad (3)$$

The probability of success given by (3) is considerably high for a sufficient number of eavesdropped sessions (N and N'), allowing an attacker to successfully trace a tag with probability $>> 1/2$. (Note that the value $1/2$ would be the advantage in the ideal case when location privacy location is guaranteed.) Assume, for instance, that 256-bit keys are chosen (e.g., by using 16×16 matrices, i.e., $d = 16$), and that random numbers have size 128 bits through 16×8 matrices and, therefore, $r = 8$. In this case, if the attacker is able to eavesdropped just $N = 32$ sessions during the learning phase of the attack, and another $N' = 32$ sessions during the execution phase, he will succeed with a probability $Adv_A \geq 1 - 2^{-16}$, which is almost equal to 1. Figure 2 shows the probability of success of the attack for the most common values of $l = d^2$ in current RFID tags.

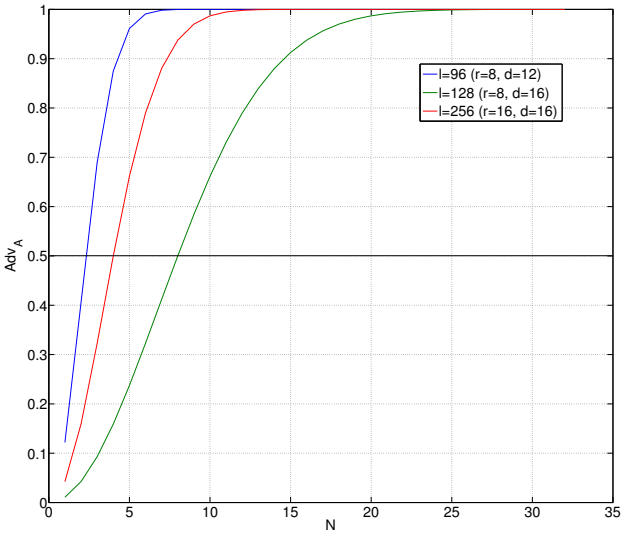


Fig. 2 Probability of success of the location attack as a function of the number of eavesdropped sessions.

Finally, an interesting point of the proposed attack is that the adversary could even be run passively. In this case, instead of sending the queries to tags $\mathbb{T}$ and $\mathbb{T}'$, the adversary would wait for interation with these tags and then eavesdrops their communications with the legitimate reader $\mathbb{R}$.

4 Standard-based RFID Health Protocols

There is currently a significant number of proposals on RFID authentication protocols (see, e.g., [14,18,39]), some of which have a clear focus on health applications, such as for example [26,41,50]). Nevertheless, the vast of majority of these schemes, like the one in [43] analyzed in this paper, suffer from various flaws and have been proven to be insecure [10,13,21,37]. This is mainly caused by the usage of non-standard approaches that ignore prudent practices and well-established principles in the design of security protocols, as well as a

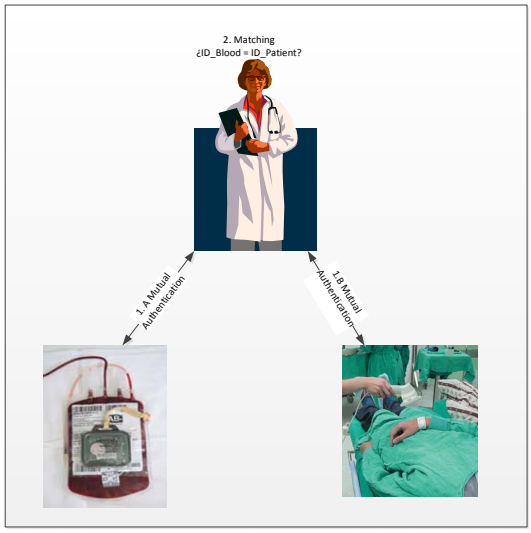


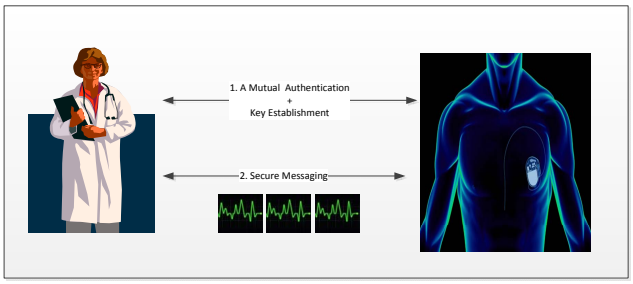
Fig. 3 Blood-handling scenario.

lack of rigorous security analysis. In particular, Wu *et al.*'s scheme offers a rather standard gaming-based security analysis, but the authors miscalculate probabilities. One major weakness of this proposal lies in using a matrix multiplication-based classical cipher (Hill) as cryptographic primitive for encryption. This is an old and largely insecure mechanism [12,19] that open doors to attacks like the one presented in this paper.

Even though current passive RFID tags have rather limited on-chip capabilities, they support some cryptographic functions, especially lightweight ones that have been recently developed for this type of applications. Later on Section 4.3 we will discuss implementation aspects and suggest specific algorithms to carry out this functions. Building upon this assumption, in this section we introduce two RFID security mechanisms based on existing standard designs adapted to healthcare environments. As a motivating examples, we will use two practical scenarios sketched in Figures 3 and 4. The first case illustrates a typical application where mutual authentication between two medical entities (e.g., a doctor and a patient, or a doctor and a blood container) is required. The second scenario motivates the need for secure channels to access an Implantable Medical Device (IMD) –a pacemaker, in this case–, which requires mutual authentication, key establishment and secure messaging. Note that the security core running on-chip of the implant is functional and computational equivalent to the one supported on a RFID tag.

The notation used throughout this section is summarized in Table 3.

Fig. 4 Secure messaging scenario.



4.1 Entity Authentication

There is a wide variety of applications in a hospital where secure and efficient authentication mechanisms are demanded. For instance, RFID technology may be used to prune blood-handling errors. This process consists of two phases. First the identities of the patients and blood bags are confirmed (authentication protocol) and then the matching between both entities is checked (verification step). The process is sketched in Fig. 3 and an authentication protocol is at the core of this application.

ISO/IEC 9798 Part 2 [23] specifies six schemes based on symmetric encryption algorithms. Four of these protocols provide entity authentication alone, while the last two ones provide also key establishment. Our proposed scheme is based on the fourth protocol of this standard and guarantees mutual authentication. Furthermore, the peculiarities of RFID systems like the anonymous identification through the insecure radio channel have been taken into account in our design.

The entities involved are the tag ($\mathbb{T}$), the reader ($\mathbb{R}$) and the database ($\mathbb{DB}$). $\mathbb{T}$ and $\mathbb{DB}$ share an authentication key (K_{ENC_TB}), a message authentication key (K_{MAC_TB}), and their identifiers are ID_T and ID_{DB}, respectively. Tags are anonymously identified by the use of pseudonyms (IDS_T), which are updated once the authentication process has been successfully completed. On the other hand, a copy of the old and current values (IDS_T^{new}, IDS_T^{old}) are held in the database to avoid de-synchronization attacks. The database keeps a table in which each row stores the information of a particular tag: $\{IDS_T^{\{new,old\}}, K_{ENC\_TB}, K_{MAC\_TB}\}$. The pseudonym is used as a search index in the database to retrieve the information linked to the interrogated tag (K_{ENC_TB}, K_{MAC_TB}). The protocol makes use of four cryptographic primitives: an encryption algorithm, a Message Authentication Code (MAC) algorithm, a one-way compression function and a pseudo-random number generator. The exchanged messages, shown in Fig-

$\mathbb{T}$ and $\mathbb{IMD}$:	Tag and Implantable Medical Device (IMD)
$\mathbb{DB}$:	Back-end Server (database)
ID_X:	Identification number of entity X
SSC:	Send Sequence Counter
F_{XY} :	Keying material sent from X to Y
ACK	Acknowledge message
ERR:	Error message
K_{ENC_XY}:	Authentication key shared between entities X and Y
K_{MAC_XY}:	Message authentication key shared between entities X and Y
KS_{ENC_XY}:	Authentication session key shared between entities X and Y
KS_{MAC_XY}:	Message authentication session key shared between entities X and Y
$[[M]]_K$	Encryption of message M with key K to provide confidentiality
$\{M\}_K$	Message Authentication Code (MAC) of message M with key K to provide integrity
$h(\cdot)$	One-way compression function
$f(\cdot)$	Key Derivation Function (KDF)

Table 3 Notation used in the proposed authentication and secure messaging schemes for health applications.

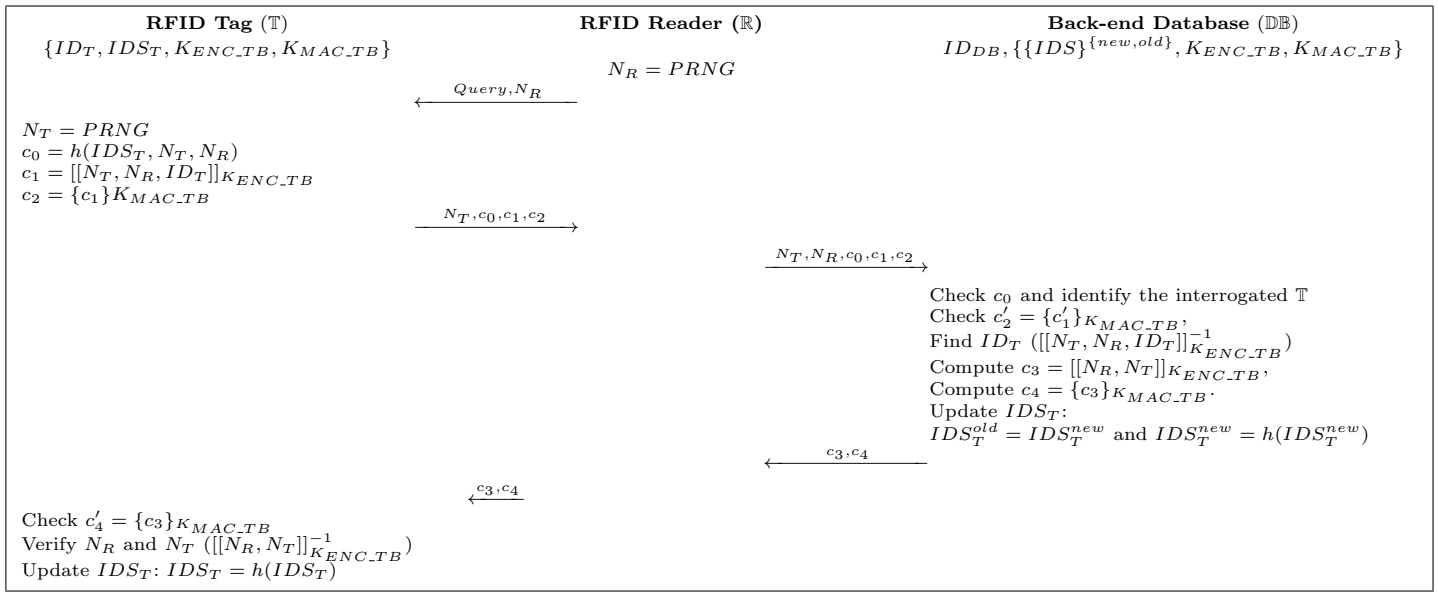


Fig. 5 Entity Authentication Protocol

ure 5, in our three-pass mutual authentication protocol are described bellow:

Step 1: $\mathbb{R} \rightarrow \mathbb{T}$: N_R. The reader sends a query signal and a random value N_R to the tag.

Step 2: $\mathbb{T} \rightarrow \mathbb{R}$: N_T, c_0, c_1, c_2. The tag generates a random number N_T and computes a fresh version of its pseudonym ($c_0 = h(IDS_T, N_T, N_R)$) that facilitates its anonymous identification. Then $\mathbb{T}$ computes an encrypted message that includes both the random number received and the one generated on-board, and its static identifier ($c_1 = [[N_T, N_R, ID_T]]_{K_{ENC\_TB}}$). Finally a MAC is computed ($c_2 = \{c_1\}_{K_{MAC\_TB}}$) and all these aforementioned values (i.e. $\{c_0, c_1, c_2\}$) together with the nonce N_T are sent to the reader and finally forwarded to the database.

Step 3: $\mathbb{DB} \rightarrow \mathbb{T}$: $\{c_3, c_4\}$. The back-end searches in its table the entry that satisfies the value c_0. More precisely, at the n-row it retrieves the new and old index-pseudonyms and computes a local version of c_0 (i.e., c_0^{new} and c_0^{old}). Then $\mathbb{DB}$ checks whether one of the above values fits with the received one. If yes, the tag is identified and its associated values are retrieved $\{K_{ENC\_TB}, K_{MAC\_TB}\}$. Otherwise, the above process is executed with the next entry (n+1-row) in the table. The process is repeated until a match is found or the end of the table is reached. The protocol is interrupted at this step if no matching occurred and all the entries were checked. If not, once the tag is identified, the database computes a local version of the MAC ($(c_2' = \{c_1'\}_{K_{MAC\_TB}})$) and checks its equality with the received value. The protocol is aborted whether the above checking fails.

Otherwise, $\mathbb{DB}$ decrypts c_1 and obtains the identifier of the target tag (ID_T). At this step the tag is authenticated (one-side authentication). Then, the database encrypts the random numbers linked to the session ($c_3 = [[N_R, N_T]]_{K_{ENC\_TB}}$), computes a MAC ($c_4 = \{c_3\}_{K_{MAC\_TB}}$), and both values are sent to the tag. Finally the current pseudonym is held and the new pseudonym is updated using the one-way compression function: $IDS_T^{old} = IDS_T^{new}$ and $IDS_T^{new} = h(IDS_T^{new})$.

Step 4: $\mathbb{T}$: The tag calculates a local version of the MAC ($c_4' = \{c_3'\}_{K_{MAC\_TB}}$) and decrypts message c_3. If the MAC is correct and the nonces obtained match with the nonces associated with the current session, the server is authenticated. Therefore both sides are authenticated at this point and the mutual authentication process finishes successfully. Finally, the tag updates its pseudonym ($IDS_T = h(IDS_T)$). On the contrary, if some of the above checkings were wrong, the tag sends an error message and an alarm is triggered in the protocol – the pseudonym updating is not executed in this case.

4.2 Secure Messaging

Apart from authentication, there are many medical applications that demand the exchange of private information. For instance, nowadays the new generation of medical implants possess wireless connectivity. Imagine a doctor equipped with a reader aims to access the records of vital signals stored on the memory of an implant. In this scenario, the doctor (reader) and the patient (implant) are first mutually authenticated and then a secure exchange of data can be performed. The process is displayed in Figure 4 and the details are given below.

Thirteen protocols using symmetric encryption algorithms are specified in ISO/IEC 11770 Part 2. Six of them are server-less, while the other seven require a trusted server. As in electronic passports [22], we opt for ISO-IEC 11770 Mechanism 6. Moreover, the special characteristics of wireless-medical systems like the anonymous identification through an insecure (radio) channel or its energy restrictions have been considered.

The entities involved in the protocol are the implant ($\mathbb{I}$), the reader ($\mathbb{R}$) and the database ($\mathbb{DB}$). $\mathbb{I}$ and $\mathbb{DB}$ share an authentication key (K_{ENC_IB}), a message authentication key (K_{MAC_IB}), and its identifiers are ID_I and ID_{DB}, respectively. The anonymous identification of implants is guaranteed by the use of pseudonyms (IDS_I), which are updated once the authentication process has been successfully completed. At the same time, a copy of the old and current values (IDS_I^{new}, IDS_I^{old}) are held in the database to avoid de-synchronization attacks. The database keeps a table in which each row stores the information of a particular implant: $\{IDS_I^{\{new,old\}}, K_{ENC\_IB}, K_{MAC\_IB}\}$. The pseudonym is used as a search index in the database to retrieve the information linked to the interrogated implant (K_{ENC_IB}, K_{MAC_IB}). The scheme requires an encryption algorithm, a MAC algorithm, a one-way compression function, a pseudo-random number generator, and a Key Derivation Function (KDF). The exchanged messages, shown in Figure 6, in our three-pass mutual authentication protocol plus two-pass secure messaging scheme are described bellow:

Step 1: $\mathbb{R} \rightarrow \mathbb{I}$: N_R. The reader sends a query signal and a random value N_R to the implant.

Step 2: $\mathbb{I} \rightarrow \mathbb{R}$: N_I, c_0, c_1, c_2. The implant generates a random number (N_I) and keying material (F_{IB}) and computes a fresh version of its pseudonym ($c_0 = h(IDS_I, N_I, N_R)$) that facilitates its anonymous identification. Then $\mathbb{I}$ computes an encrypted message that includes the random number received and the one generated on-board, keying material, and its static identifier ($c_1 = [[N_I, N_R, ID_I, F_{IB}]]_{K_{ENC\_IB}}$). Then a MAC is computed ($c_2 = \{c_1\}_{K_{MAC\_IB}}$) and the aforementioned values (i.e., $\{c_0, c_1, c_2\}$) together with the nonce N_I are sent to the reader and finally forwarded to the database.

Step 3: $\mathbb{DB} \rightarrow \mathbb{T}$: $\{c_3, c_4\}$. The back-end searches in its table the entry that satisfies the value c_0. In detail, at the n-row it retrieves the new and old index-pseudonyms and computes a local version of c_0 (i.e., c_0^{new} and c_0^{old}). Then $\mathbb{DB}$ checks whether one of these computed values fits with the received one. If yes, the implant is identified and its associated values are retrieved $\{K_{ENC\_IB}, K_{MAC\_IB}\}$. Otherwise, the above process is executed with the next entry (n+1-row) in the table. The process is repeated until a match is found or the end of the table is reached. The protocol is interrupted at this step if no matching occurred and all the entries were checked. If not, once the implant is identified, the database computes a local version of the MAC ($c_2' = \{c_1'\}_{K_{MAC\_IB}}$) and checks its equality with the received value. If the above checking fails, the protocol is aborted. Otherwise, $\mathbb{DB}$ decrypts c_1 and obtains the identifier of the implant (ID_I) and the keying material generated by the other side (F_{IB}). At this step, the implant is authenticated (one-side authentication). Next, the database generates keying material (F_{BI}) and encrypts this value together with the nonces linked to the session ($c_3 = [[N_R, N_I, F_{BI}]]_{K_{ENC\_IB}}$) and computes a MAC ($c4 = \{c_3\}_{K_{MAC\_IB}}$). After that, both values are sent to the implant. Finally the

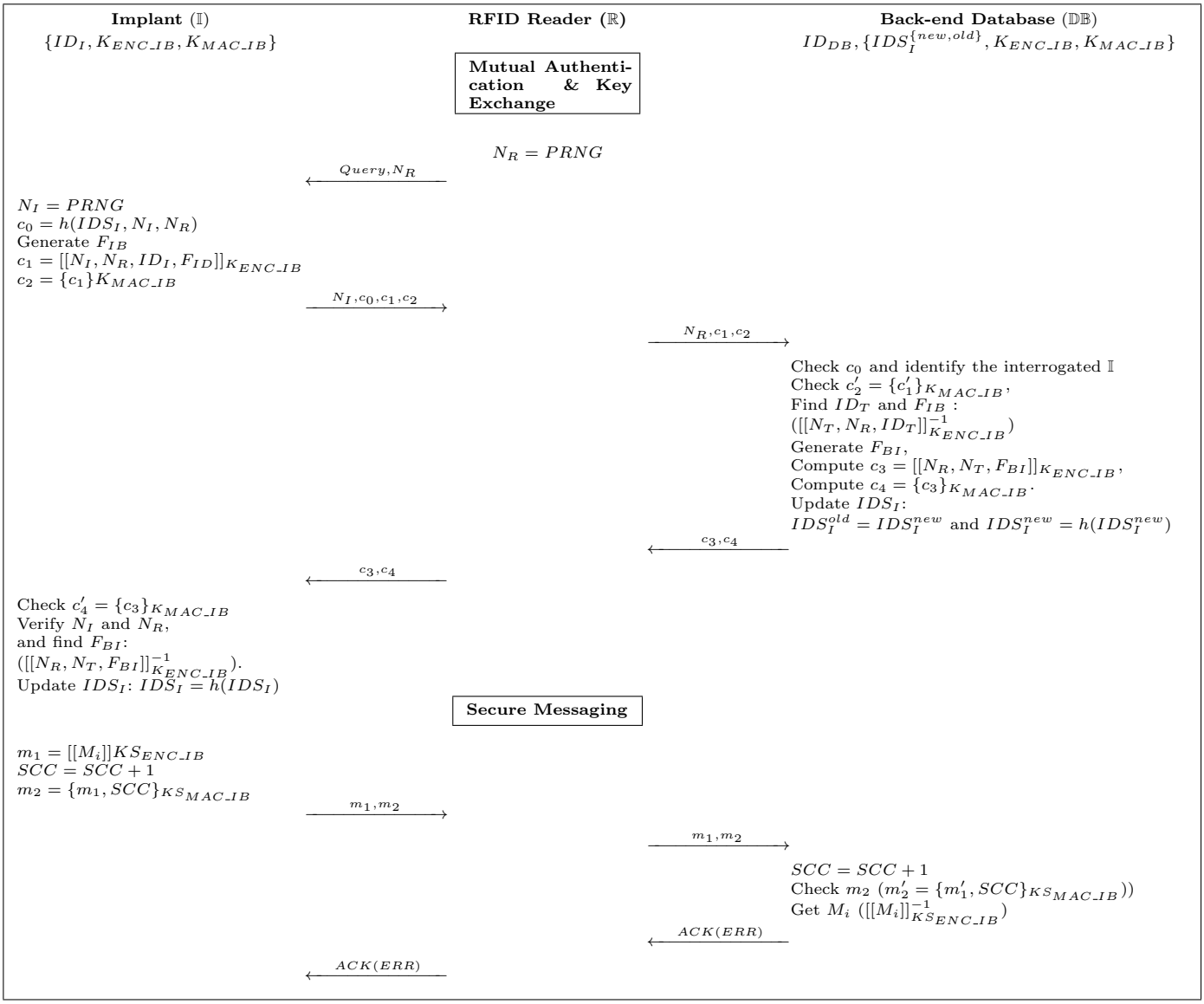


Fig. 6 Secure Messaging Scheme

current pseudonym is held and the new pseudonym is updated using the one-way compression function: $IDS_I^{old} = IDS_I^{new}$ and $IDS_I^{new} = h(IDS_I^{new})$.

Step 4: 𝕀: The implant calculates a local version of the MAC ($c4' = \{c_3'\}_{K_{MAC\_IB}}$) and decrypts message c_3. If the MAC is correct and the nonces obtained match the nonces associated with the current session, the server is authenticated. Thus, both sides are authenticated at this step, the mutual authentication process finishes successfully and the implant updates its pseudonym ($IDS_I = h(IDS_I)$) . If some of the above checkings were wrong, the implant sends an error message, an alarm is triggered in the protocol, and the pseudonym updating is not executed. Note that, apart from authentication, the implant also received the keying material from the database (F_{BI}).

Step 5: Session Key Derivation: Once authentication is completed, the implant and the database calculate the session keys. We use a Key Derivation Function (KDF; $f(\cdot)$) with two inputs (F_{IB} and F_{BI}). In particular, we follow the KDF in counter mode specified in NIST 800-108 recommendation (see Sect. 5.1 in [34] for details). Following this algorithm, two fresh keys KS_{ENC_IB} and KS_{MAC_IB} are shared between both entities. Furthermore, as in [22] specification (see page IV-40; Section A.5.4.2) a Send Sequence Counter (SSC) is computed from the two random numbers linked to the session: e.g., $SSC = N_I$ (2 least significant bytes), N_B (2 least significant

bytes).

After that, a secure exchange of data can be accomplished. For each data block (M_i) the following procedure is followed:

Step 6: $\mathbb{I} \rightarrow \mathbb{DB}$: m_1, m_2. First the implant encrypts M_i with KS_{ENC_IB} ($m_1 = [[M_i]]_{KS_{ENC\_IB}}$). Then the MAC of m_1 is computed following three steps: 1) SSC is incremented with 1; 2) SCC is padded to m_1, and 3) the MAC with KS_{ENC_IB} is calculated (i.e., $\{m_1, SCC\}_{KS_{ENC\_IB}}$). Next these two values ($\{m_1, m_2\}$) are sent to the reader and finally forwarded to the database.

Step 7: $\mathbb{I} \rightarrow \mathbb{DB}$: ACK or ERR: The database computes a local version of the MAC. More precisely, SCC is incremented with one and padded to the received m'_1 and finally the MAC is computed (i.e. $m'_2 = \{m'_1, SCC\}_{KS_{ENC\_IB}}$). If both values match, the data block is decrypted ($[[M_i]]^{-1}_{KS_{ENC\_IB}}$) and an acknowledge message (ACK) is sent to the implant. Otherwise, an error message (ERR) is sent to the implant.

4.3 Implementation Aspects

The two applications presented in this paper rely on the use of several cryptographic primitives: encryption, one-way compression, MAC, PRNG, and key derivation functions. As we next discuss, the proposed primitives use a block cipher as the core component of each algorithm. RFID tags can be classified regarding its operating frequency or its source of power as described in Section 1. On the other hand, price is a crucial factor that determines tag capabilities (e.g., memory and power computation). Low-cost and high-cost tags are the two main classes with respect to this parameter. The size of the chip –and, consequently, its capabilities– is directly linked to its price. Low-cost tags have a price that varies from 10 to 30 cents, with around 3000-5000 gates equivalents that can be devoted to security purposes [1]. Adequate implementations of standard block ciphers like AES, or modern designs like PRESENT, can be used in such tags [5,24]. Even though in our proposal all primitives are based on a block cipher, the tag must support several algorithms and it does not seem plausible that all of them would fit in a low-cost tag. Consequently, we recommend the usage of high-cost tags. These have a market price of 1-2 dollars, which is reasonable for medical environemnts. In this sort of tags, more than 7000 gates equivalents are available for security issues [4,16], and the overprice is justified by the high security level demanded in medical applications, particularly when the safety of patients is a vital factor in these environments [11,38].

We next discuss in detail the cryptographic building blocks used in our proposal. As in the case of the protocols presented above, all constructions are based on ISO/IEC standards and NIST recommendations.

4.3.1 Encryption Algorithm

The first key aspect is the adoption of symmetric or asymmetric cryptographic approaches. We discard public cryptography due to the current scarcity of resources in constrained devices like low-cost RFID tags or IMDs. Our two proposals described above use a lightweight and secure cipher. We can opt for standard approaches, such as for example the tiny implementation of AES [17] or more recent lightweight block ciphers like PRESENT [6] or KATAN family [8]. Stream ciphers like Grain [20] or Trivium [29] could also be used, but we discard this option since the MAC algorithm will be based on the cipher and stream-cipher-based MAC algorithm are not standardized.

4.3.2 One-way Compression Function

A one-way compression function is a function that transforms a fixed-length input into a fixed-length output, being difficult to compute an input given a particular output. This sort of functions are often build using block ciphers like the mentioned in the previous section. In detail, these make use of the following components: 1) a block cipher with block size L, called CIPH and parametrized by a symmetric key K; 2) a function g with maps L-bit inputs to keys K suitable for CIPH; and 3) a fixed L-bit initial value. In the literature, there are several proposed algorithms: Davies-Meyer, Matyas-Meyer-Oseas and Miyaguchi-Preneel [28]. This latter is described below. The input M (i.e., $h(M)$) is divided into L-bit blocks and padded, if necessary, to completed the last block M_m: $M_1||M_2||\cdots||M_m$, where $m = |M|/L$ and $||$ symbolizes concatenation. Then the algorithm is executed as follows:

Hash Algorithm (Miyaguchi-Preneel construction)
1. $H_0 = IV$
2. For $i = 1$ to m
3. $\quad H_i = CIPH_{g(H_{i-1})}(M_i) \oplus M_i \oplus H_{i-1}$.
4. $T = H_m$
5. Return T

4.3.3 MAC Algorithm

We propose the use of a MAC algorithm based on a symmetric-key block cipher, since this primitive is already used in the protocol and we can easily reuse it. This cipher-based MAC is abbreviated as CMAC. Our algorithm follows the NIST 800-38B Recommendation [33]. We assume that we have a block cipher with block size L, called CIPH, and a shared key (K). Moreover, for sub-key generation we follow the guidelines dictated in [33] (NIST 800-38B, pages 7-8); the sub-keys (K_1 and K_2) are generated and stored in the memory of entities involved (i.e., tag and database) at the key distribution phase. To compute the MAC of message M (i.e., $\{M\}_K$), M is divided into blocks of L bits: $M_1||M_2||\cdots M_m$, where $m = |M|/L$ and $||$ denotes concatenation. As specified in [33], the last block is XORed with $K2$ or $K1$, depending if padding is needed or not.The CMAC algorithm is described below:

CMAC Algorithm (compliant with NIST 800-38B)
1. $C_0 = 0^L$
2. For $i = 1$ to m
3. $\quad C_i = CIPH_K(C_{i-1} \oplus M_i)$.
4. $T = C_m$
5. Return T

4.3.4 Pseudo-random Number Generator

Apart from the Hash and MAC algorithms, random numbers are used in the protocol. We opt for an standard approach again. As specified in NIST 800-38A [32] (recommendation for block ciphers modes of operation), we propose the use of a block cipher in counter mode, denoted CTR. The current value of the counter is called T_j and R_N represents the resulting $L/2$-bits random number, L being the block size for the used block-cipher. The initial value of the counter is set at the key distribution phase, i.e., $T_0 = random\_seed$. After each nonce generation, the counter value is updated to T_{j+1}. The algorithm is described below:

PRNG: Block cipher in CTR Mode (compliant with NIST 800-38A)
1. $O_j = CIPH_k(T_j)$
2. $R_N = \|O_j\|_{0\cdots(L/2-1)}$
3. $T_{j+1} = \|O_j\|_{L/2\cdots L}$

4.3.5 Key Derivation Function

As specified in NIST 800-108 [34], we propose the use of a KDF in counter mode and the $CMAC$ primitive is used as the Pseudo-Random Function (PRF). The key derivation function is calculated by xoring the keying materials exchanged in the first phase of the protocol ($K_l = F_{ID} \oplus F_{DI}$). Next, the session keys KS_{ENC_IB} and KS_{MAC_IB} are generated. In the following, we assume that the bit length of these keys are r times the length of the used block-cipher with block size L. Depending on whether the key is used for encryption or MAC, the Fixed Input Data (FID) take one of these values: (0x 00 00 00 00 00 01 || 0x 00 || ID_I) or (0x 00 00 00 00 00 02 || $0x$ 00 || ID_I).

Key Derivation Function – CTR Mode (compliant with NIST 800-108)
1. $result = []$;
2. For $i = 1$ to r, do
3. $\quad K(i) = CMAC_{K_l}(i, FID)$
4. $\quad result(i) = result(i-1) \;||\; K(i)$
5. Return $KS =$ leftmost $(r \cdot L)$ bits of $result$.

5 Conclusions

In the last years, several RFID-based solutions have been proposed to solve a variety of problems in healthcare environments. These proposals deal with interesting applications, such as monitoring of Alzheimer patients or intelligent drug administration systems. Unfortunately, the majority of such schemes, like the one by Wu *et al.* [43] analyzed in this article, have resulted poor from the security point of view [10,13,21,37]. In general, such a lack of security is due to two main reasons: (i) the use of non-standard constructions that do not follow prudent design practices and established recommendations; and (ii) informal and/or non-rigorous security analysis.

With the aim of avoiding these common mistakes, we have proposed two new RFID protocols for healthcare environments based on standards and recommendations. More precisely, the security schemes proposed conform to ISO/IEC 9798 and 11770. The security of the mechanisms included in these specifications has been deeply studied. This provides, in our opinion, more confidence than ad hoc designs. Furthermore, we provide details about implementation aspects by following NIST Security Recommendations. Finally, we hope that schemes such as those here proposed can give support to additional RFID-based healthcare applications and stimulate further research in the area.

References

1. Arbit, A., Oren, Y., Wool, A.: Toward practical public key anti-counterfeiting for low-cost epc tags. In: IEEE

International Conference on RFID, pp. 184–191 (2011)
2. Aronson, J.: Medication errors: what they are, how they happen, and how to avoid them. QJM: An International Journal of Medicine **102**(8), 513–521 (2009)
3. Azevedo, S.G., Ferreira, J.J.: Radio frequency identification: a case study of healthcare organisations. Int. J. Secur. Netw. **5**(2/3), 147–155 (2010)
4. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: Public-key cryptography for RFID-Tags. In: Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 217–222 (2007)
5. Biryukov, A.: Block ciphers and stream ciphers: The state of the art. Cryptology ePrint Archive, Report 2004/094 (2004). Http://eprint.iacr.org/
6. Bogdanov, A., Knudsen, L., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: Present: An ultra-lightweight block cipher. In: Cryptographic Hardware and Embedded Systems - CHES 2007, *Lecture Notes in Computer Science*, vol. 4727, pp. 450–466. Springer Berlin Heidelberg (2007)
7. Bunduchi, R., Weisshaar, C., Smart, A.U.: Mapping the benefits and costs associated with process innovation: The case of rfid adoption. Technovation **31**(9), 505 – 521 (2011)
8. Cannire, C., Dunkelman, O., Kneevi, M.: KATAN and KTANTAN A family of small and efficient hardware-oriented block ciphers. In: Cryptographic Hardware and Embedded Systems - CHES 2009, *Lecture Notes in Computer Science*, vol. 5747, pp. 272–288. Springer Berlin Heidelberg (2009)
9. Chan, H.L., Choi, T.M., Hui, C.L.: Rfid versus bar-coding systems: Transactions errors in health care apparel inventory control. Decision Support Systems **54**(1), 803 – 811 (2012)
10. Chen, Y.Y., Huang, D.C., Tsai, M.L., Jan, J.K.: A design of tamper resistant prescription rfid access control system. Journal of Medical Systems **36**(5), 2795–2801 (2012). DOI 10.1007/s10916-011-9758-2. URL http://dx.doi.org/10.1007/s10916-011-9758-2
11. Chen, Y.Y., Wang, Y.J., Jan, J.K.: A secure 2G-RFID-Sys mechanism for applying to the medical emergency system. Journal of Medical Systems **37**(3), 1–10 (2013)
12. Chien, H.Y., Chen, C.H.: Mutual authentication protocol for rfid conforming to epc class 1 generation 2 standards. Computer Standards & Interfaces **29**(2), 254 – 259 (2007)
13. Chien, H.Y., Yang, C.C., Wu, T.C., Lee, C.F.: Two rfid-based solutions to enhance inpatient medication safety. Journal of Medical Systems **35**(3), 369–375 (2011). DOI 10.1007/s10916-009-9373-7. URL http://dx.doi.org/10.1007/s10916-009-9373-7
14. Duc, D.N., Kim, K.: Defending rfid authentication protocols against dos attacks. Computer Communications **34**(3), 384 – 390 (2011)
15. Dunbar, P.: 300,000 babies stolen from their parents - and sold for adoption: Haunting bbc documentary exposes 50-year scandal of baby trafficking by the catholic church in spain. Daily Mail (2011). URL http://www.dailymail.co.uk/news/article-2049647/BBC-documentary-exposes-50-year-scandal-baby-trafficking-Catholic-church-Spain.html
16. Feldhofer, M., Rechberger, C.: A case against currently used hash functions in rfid protocols. In: Proceedings of the 2006 international conference on On the Move to Meaningful Internet Systems - Workshops - Volume Part I, OTM'06, pp. 372–381. Springer-Verlag (2006)
17. Feldhofer, M., Wolkerstorfer, J., Rijmen, V.: Aes implementation on a grain of sand. IEE Proceedings Information Security **152**(1), 13–20 (2005)
18. Fu, X., Guo, Y.: A lightweight rfid mutual authentication protocol with ownership transfer. In: Advances in Wireless Sensor Networks, *Communications in Computer and Information Science*, vol. 334, pp. 68–74. Springer Berlin Heidelberg (2013)
19. Gmez Pardo, J.: Classical ciphers and their cryptanalysis. In: Introduction to Cryptography with Maple, pp. 1–33. Springer Berlin Heidelberg (2013)
20. Hell, M., Johansson, T., Maximov, A., Meier, W.: A stream cipher proposal: Grain-128. In: IEEE International Symposium on Information Theory, pp. 1614–1618. IEEE (2006)
21. Huang, H.H., Ku, C.Y.: A rfid grouping proof protocol for medication safety of inpatient. Journal of Medical Systems **33**(6), 467–474 (2009). DOI 10.1007/s10916-008-9207-z
22. ICAO: Machine readable travel documents – part 3. International Civil Aviation Organization (2009)
23. ISO: Information technology – security techniques – entity authentication – part 2: Mechanisms using symmetric encipherment algorithms, iso/iec 9798-2:2008. International Standard (2nd ed., 1999)
24. Kitsos, P., Sklavos, N., Parousi, M., Skodras, A.N.: A comparative study of hardware architectures for lightweight block ciphers. Computers & Electrical Engineering **38**(1), 148 – 160 (2012)
25. Lin, L., Yu, N., Wang, T., Zhan, C.: Active rfid based infant security system. In: M. Ma (ed.) Communication Systems and Information Technology, *Lecture Notes in Electrical Engineering*, vol. 100, pp. 203–209. Springer Berlin Heidelberg (2011)
26. Lin, Q., Zhang, F.: Ecc-based grouping-proof rfid for inpatient medication safety. Journal of Medical Systems **36**(6), 3527–3531 (2012)
27. Malkin, B.: 300,000 babies stolen from their parents - and sold for adoption: Haunting bbc documentary exposes 50-year scandal of baby trafficking by the catholic church in spain. The Telegraph p. 1 (2011). URL http://www.telegraph.co.uk/news/religion/8660249/Australias-Roman-Catholic-Church-apologises-for-forced-adoptions.html
28. Menezes, A.J., Vanstone, S.A., Oorschot, P.C.V.: Handbook of Applied Cryptography, 1st edn. CRC Press, Inc. (1996)
29. Mora-Gutirrez, J., Jimnez-Fernndez, C., Valencia-Barrero, M.: In: Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation, *Lecture Notes in Computer Science*, vol. 7606, pp. 113–120. Springer Berlin Heidelberg (2013)
30. Najera, P., Lopez, J., Roman, R.: Real-time location and inpatient care systems based on passive rfid. Journal of Network and Computer Applications **34**(3), 980 – 989 (2011)
31. NCMEC: Newborn/infant abductions. National Center for Missing & Exploited Children p. 1 (2012). URL http://www.ncmec.org/en_US/documents/InfantAbductionStats.pdf
32. NIST: Recommendation for block cipher modes of operation. methods and techniques, NIST special publication 800-38a. National Institute of Standards and Technology (2001)
33. NIST: Recommendation for block cipher modes of operation: The CMAC mode for authentication, NIST special

publication 800-38b. National Institute of Standards and Technology (2005)
34. NIST: Recommendation for key derivation using pseudorandom functions (revised), NIST special publication 800-108. National Institute of Standards and Technology (2009)
35. Oztekin, A., Pajouh, F.M., Delen, D., Swim, L.K.: An rfid network design methodology for asset tracking in healthcare. Decision Support Systems **49**(1), 100 – 109 (2010). DOI 10.1016/j.dss.2010.01.007
36. Parlak, S., Sarcevic, A., Marsic, I., Burd, R.S.: Introducing rfid technology in dynamic and time-critical medical settings: Requirements and challenges. Journal of Biomedical Informatics **45**(5), 958 – 974 (2012)
37. Peris-Lopez, P., Orfila, A., Mitrokotsa, A., van der Lubbe, J.C.: A comprehensive rfid solution to enhance inpatient medication safety. International Journal of Medical Informatics **80**(1), 13 – 24 (2011). DOI 10.1016/j.ijmedinf.2010.10.008
38. Peris-Lopez, P., Orfila, A., Mitrokotsa, A., van der Lubbe, J.C.A.: A comprehensive rfid solution to enhance inpatient medication safety. International Journal Medical Informatics **80**(1), 13–24 (2011)
39. Piramuthu, S.: Rfid mutual authentication protocols. Decision Support Systems **50**(2), 387 – 393 (2011)
40. Qu, X., Simpson, L.T., Stanfield, P.: A model for quantifying the value of rfid-enabled equipment tracking in hospitals. Advanced Engineering Informatics **25**(1), 23 – 31 (2011)
41. Safkhani, M., Bagheri, N., Naderi, M.: On the designing of a tamper resistant prescription rfid access control system. Journal of Medical Systems **36**(6), 3995–4004 (2012). DOI 10.1007/s10916-012-9872-9. URL http://dx.doi.org/10.1007/s10916-012-9872-9
42. Sun, P.R., Wang, B.H., Wu, F.: A new method to guard inpatient medication safety by the implementation of rfid. J. Med. Syst. **32**(4), 327–332 (2008)
43. Wu, Z.Y., Chen, L., Wu, J.C.: A reliable rfid mutual authentication scheme for healthcare environments. Journal of Medical Systems **37**, 1–9 (2013)
44. Wyld, D.: Preventing the worst case scenario: An analysis of rfid technology and infant protection in hospitals. The Internet Journal of Healthcare Administration **7**(1) (2010)
45. Yang, M.H.: Secure multiple group ownership transfer protocol for mobile rfid. Electronic Commerce Research and Applications **11**(4), 361 – 373 (2012)
46. Yao, W., Chu, C.H., Li, Z.: The use of rfid in healthcare: Benefits and barriers. In: RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on, pp. 128 –134 (2010)
47. Yao, W., Chu, C.H., Li, Z.: The use of rfid in healthcare: Benefits and barriers. In: IEEE International Conference on RFID-Technology and Applications (RFID-TA), pp. 128–134. IEEE Society (2010)
48. Yao, W., Chu, C.H., Li, Z.: Leveraging complex event processing for smart hospitals using rfid. Journal of Network and Computer Applications **34**(3), 799 – 810 (2011)
49. Yao, W., Chu, C.H., Li, Z.: The adoption and implementation of rfid technologies in healthcare: A literature review. Journal of Medical Systems **36**(6), 3507–3525 (2012)
50. Yen, Y.C., Lo, N.W., Wu, T.C.: Two rfid-based solutions for secure inpatient medication administration. Journal of Medical Systems **36**(5), 2769–2778 (2012). DOI 10.1007/s10916-011-9753-7
51. Zhou, W., Yoon, E.J., Piramuthu, S.: Simultaneous multi-level rfid tag ownership & transfer in health care environments. Decision Support Systems **54**(1), 98 – 108 (2012)