# A practical RFID system: with mutual authentication and privacy protection

Chin-Ling Chen[1] and Yong-Yuan Deng[2]

1. Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan 413, ROC. E_mail:clc@mail.cyut.edu.tw
2. Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan 413, ROC. E_mail:s9527625@mail.cyut.edu.tw

## 摘要

無線射頻辨識系統是一項新的科技，近年來大量的應用在我們日常生活當中。無線射頻辨識系統為我們的生活增加了許多的便利，但也帶來了隱憂。由於無線射頻辨識系統是利用無線傳輸的方式，如果在無線環境之中有心人士意圖取得無線射頻辨識標籤內的資訊，對使用者的隱私將造成威脅。雖然目前有許多無線射頻辨識安全上的研究，但都無法兼顧安全性和降低資料庫的負擔。因此，我們提出一個新的認證加密方式，符合電子產品碼第二代第一級(EPC Class1 Generation2)的標準，利用交互認證的概念，確保標籤和讀碼器之間的傳輸是安全的，我們的方法同時也能降低資料庫的負擔。最後利用多種安全觀點來檢視我們所提出的新方法，並提供此方法適用的環境。

**關鍵詞：**無線射頻辨識、電子產品碼、安全、隱私、交互認證

## Abstract

In recent years, a new technology – Radio Frequency Identification (RFID) has involved in our daily life. It brings many conveniences to our life, but it also brings some hidden worries. Due to RFID system uses wireless transmission, there are some malicious people who want to get the information in the RFID tags around the environment, and the user's privacy would be violated. Although there have been many protection methods in RFID's security, many researches still suffered from privacy violation and can not lower database loading. Thus, we propose a new authentication and encryption method that confirms EPC Class1 Generation2 standard and uses the mutual authentication mechanism to make sure the transmission security between tag and reader. By the way, our scheme not only lower database loading, but also ensure user's privacy. Finally, we survey our scheme from several security viewpoints, and prove our scheme is feasible in some situations.

**Keywords:** RFID, EPC, security, privacy, mutual authentication

## 1. INTRODUCTION

### 1.1 Background

Radio frequency identification (RFID) system uses a small device, RFID tag, to receive and send remote command. RFID system contains tag, reader, host and antenna [12]. There is a small and low-cost tag in each RFID object to provide a unique identity of global products – Electric Product Code (EPC). Once RFID reader sends the request signal, and the RFID tag will make a response for reader's reading and writing request.

Many applications which use Bar-code system are replaced by RFID system in the environment. Because the RFID system has many advantages better than Bar-code system. Due to RFID system can identify an object in a large range more than vision, moreover Bar-code system only identify objects in a very closely distance. Besides, RFID system also has bigger storage capacity, so each RFID tag can get a unique identification, Bar-code system can't do it in this way. Thus, RFID system has excellent performance in stock and selling, and also brings many conveniences in market checkout.

By lower RFID tag's cost, there are wider and wider applications about RFID mechanism, and going into our daily life gradually. For example, entrance control, pet identification, highway auto charge, industry control, property management, and home automation etc. Due to lack of common standard, each company uses different operation mechanisms; the consistency of RFID system is not desirable. RFID system will make response to reader's reading request. There exists a potential risk in security problems of RFID system.

For example, RFID system is used in a medicine management system. After a patient gets medicine, there is RFID tag in the medicine. When attacker carries a reader to read the message in the tag of medicine, he/she will know what medicine does the patient get; even know the patient's disease. Moreover someone buys a book with RFID tag in the bookstore, attacker only need carry a reader and near the book, and then he/she can get the book's detail, also knows the user's reading habit.

According to above examples, we can find the touchless read/write characteristic of RFID system, will threaten the user's privacy. In spite of RFID system brings great advantage to us, if it can not protect personal privacy and enhance its security, the public opinion will against this system, and its promotion will not going smoothly. Thus, the concept of mutual authentication on information security is necessary. On the basis of Authentication Processing Framework [6], we therefore design a secure RFID access control system. Both tag and reader must register to server. Tag will know whether reader is legal or not, and reader will also know whether tag had registered or not. Both of the legal tag and reader communicate each other while they have registered. It will protect the user's privacy and the security sufficiently.

## 1.2 Related works

As we known RFID system could be attacked by the unauthorized attackers, and violate the user's privacy. In order to prevent RFID tag leaking message, many scholars had proposed the following schemes:

(1) Tag killing scheme [1, 6, 11]:

The most directly scheme to protect user's privacy is disabled the tag before it handing to user, and tag will not be read forever. The standard operation mode is proposed by AutoID Center. By a special clear command, tag's content can't be read. The disadvantage of this scheme is the tag can only use once. For reducing the tag's cost, we still hope these tags in user's hands can be operated after selling. Thus, tag killing scheme is an impracticable scheme.

(2) Faraday cage scheme [1, 6, 9]:

Using a metal meshed container to cover RFID tag, block reader's request signal, and let RFID tag can not be read by reader. Here is an example, thief put merchandise into a metal bag in the mall, and then this merchandise will not be detected by the sensor when this thief leaves the mall. Although this method solves the attacker illegally read tag, it's very inconvenient and hard to apply in the large target. The other defect is, RFID tag can not be access when it is covered by faraday cage.

(3) Active jamming scheme [1, 6]:

Users use a radio frequency broadcast device to disturb the signal via the RFID reader. When attackers use illegal reader to access the tag information, this device will confused them. Even this scheme block the attack from attackers successfully, the other legal reader can't access RFID tag. By the way, if the broadcast power is too high, it's also illegal. Besides, using this device in some environment is very dangerous. For example, it might affect the other medical equipment in the hospital.

(4) Smart tag scheme [1]:

As mentioned before, which are using an intuitional protecting method. The user must carry an extra device, and these methods have a serious defect. That is, when they block the attacker, they also block the communication between legal RFID reader and legal RFID tag. The other way to prevent attacker attack RFID reader or RFID tag is using encryption transmission method to prevent attacker's attack. Due to its more flexibility in tag and reader management than traditional method, thus smart tag is a future trend.

The following schemes of protect the communication between readers and tags are based on smart tag, which is proposed by other scholars:

(1) Hash lock scheme [10]:

This scheme means that reader sends a read request to tag, tag will return a $metaID$ to reader. The $metaID$ is the coordinated value by tag and reader in advance, which value is generated by the hash function. When reader receives $metaID$, reader will search the entire database, if the corresponding value $K$ has found, reader will return $K$ to tag. Upon receiving the $K$ value, tag will compute $h(K)$, and compare to the original $metaID$ (i.e. $metaID = h(K)$), to verify whether they are equal or not.

However, in this method, when attacker get $metaID$ and $K$ by the communication between tag and reader, attacker can pretend legal tag and legal reader into the communication of original tag and reader, therefore, message hasn't the privacy anymore [2, 15]. Besides, $metaID$ is fixedly sent by tag. Besides, attacker even can't get $K$ value to hold transmission message, it also can rely on multi readers to get same $metaID$ response to know it's sent by the same tag, and can trace the user's location. It will threaten the user's privacy.

(2) Randomized hash lock scheme [10]:

This scheme means that reader sends a read request to tag, tag will select a value randomly. After tag computing $h(ID, RND)$ via hash function $h()$, they will be sent to the reader with random value $RND$. Once reader receives this random value $RND$, it will use $ID'$, which is stored in database, and $RND$ to compute $h(ID', RND)$. After this operation, reader will compare with the hash value $h(ID', RND) = h(ID, RND)$; if they are equal, reader will response a corresponding ID value to tag.

Even a random value $RND$ is used in this scheme; there still exist a security problem [2, 15]. When an attacker pretends a legal reader and sends a reading request to tag; tag will response an unprotected random value. Attacker therefore can intercept this random value, and get a confirmation message from legal reader. At this time, attacker can process illegal access, because of attacker has known the random value and confirmation message. Not only is the data in the tag, but also the user's privacy not secured anymore. This scheme needs plenty of hash operations in database. Thus, it is uneconomic for the whole system in efficiency.

(3) Universal encryption scheme [7, 13]:

This method means that reader sends a reading request to tag, tag will select a random value $RND$, and encrypts with key $k$ which is coordinated with reader in advance; then response the encrypted message $E_k(ID, RND)$ to the reader. After reader receiving the message from the tag, reader will use key $k$ to decrypt it. When reader gets the tag's $ID$ inside the message, it will response an encrypted confirmation message to the tag.

By encryption key and random value to encrypt the message, the security in this scheme is improved. However, that is still a security problem. That is, only use the fixed key in this method. If attacker gets this key, then he/she can decrypt every message in RFID tag of the whole system, and it will threaten the RFID system security.

(4) Karthikeyan-Nesterenko's scheme [14]:

Reader coordinates a value $K$ with tag in register stage, tag and reader also store two matrix $M_1$ and $M_2$. This scheme confirms EPC Class1 Generation2 standard, but can't resist illegal tag access [4]. If the attacker replaces $Z$ with an old one $Z'$ in the above mentioned attack, then the attacker can replay the $Y'$ in the next session to cheat the tag in wrongly accepting the request and access the tag accordingly. Besides, the value $X$ which is stored in tag sent out is fixed, it can not avoid location tracing.

### 1.3 Security requirements

A good RFID system must avoid illegal accessing, protect user's privacy, and protect RFID system. The following security issues are often discussed in general RFID system requirements.

(1) Pretend reader attack tag [5, 8, 15]:

Pretend reader attack tag means attacker's illegal accessing tag. Attacker attempts to get sensitive information from the tag by its illegal reader.

(2) Pretend tag attack reader [5, 8, 15]:

This security threat means attacker attacks legal RFID reader. Attacker owns illegal tag, when legal reader needs to query tag, illegal tag will response fake message to reader. Then reader can't identify the received message, and the whole RFID system would be crashed.

(3) Man-in-the-middle attack [4, 5, 15]:

Attacker attacks the communication between tag and reader. Attacker pretends a transmission role, when reader wants to query tag, attacker will intercept the message from reader, then transfer to tag. When tag wants to response the message to reader, attacker will intercept the message again, and then transfers it to reader. Attacker can hold and modified the all messages to transmit them between tags and readers.

(4) User habit privacy [2, 15]:

Once attacker holds message from user's RFID tag, it will cause the security problem. Because of the EPC code in the tag is not encrypted, when attacker gets the EPC code that tag responses to reader, attacker can query the database, and gets the related information from the tag. Therefore, the tag owner's privacy will be threatened.

(5) User location privacy [2, 15]:

It means attacker knows user's location. The reason that causes this security problem is attacker gets response message from the tag. Although tag transfers the encrypted message to block the attacker, attacker still can get user's location by multi reader at different location querying to RFID tag.

(6) Mutual authentication between tag and reader [4]:

The mutual authentication is a good mechanism to solve the illegal access problem. Through authentication processing framework, both reader and tag are needed to register to the database. Legal reader can verify whether the tag is legal or not, and legal tag also can verify whether the reader is legal or not.

(7) EPC Class1 Generation2 standard [3, 4]:

EPC Class1 Generation2 is established by EPC global, it offers RFID system a general standard. If a RFID protocol can not confirm EPC Class1 Generation2 global standard, which will lower manufacturer's willing. So, a RFID protocol with security and confirm EPC Class1 Generation2 is necessary.

(8) Lower database loading [5, 15]:

In non encrypted RFID system, reader can get tag's EPC easily. But in encrypted RFID system, reader can not get EPC immediately. Reader usually needs to search the entire database, and it can get EPC. It causes lots of time and resources of database. So, lower database loading is necessary.

## 2. OUR SCHEME

Due to the schemes [7, 10, 13] still exist security problems, we therefore propose a new scheme to solve these problems. On the basis of [6], we propose a novel scheme to ask the readers and tags to register to database such that the illegal access can be avoided. Though this scheme, it will achieve mutual authentication, and also protects user's privacy.

### 2.1 Notation

The following notation is used in our scheme:

$N_i$: a nonce word, if tag and reader registered to database, they will get $N_i$ simultaneously.

$K_i$: a key, if tag and reader registered to database, they will get $K_i$ simultaneously.

$CRC(N_i)$: a CRC (Cyclic Redundancy Check) function operates with $N_i$.

$CRC(RND)$ : a CRC function operates with $RND$ .

$EPC_{Ti}$ : the i[th] Electric Product Code which confirms C1G2 standard, to identify the unique global product.

$ID_{Ri}$ : the i[th] reader's identification.

$RND$ : a random value which is generated by reader.

$\oplus$ : exclusive-or operation.

$M_{req}$ : the reader's request message.

$M_{resp}$ : the reader's response message.

## 2.2 Register phase

We divide the register phase into two parts. Tags and readers must register to database separately, and then they can communicate each other. The following steps are described in the register phase.

Step 1: Each RFID tag has a unique EPC. When a tag registered to database, database will issue n parameters $N_1, N_2, \cdots, N_n$ and n keys $K_1, K_2, \cdots, K_n$ for each registered tag respectively. For example, $i^{th}$ tag registered to database, and stored its $EPC_{Ti}$ to database. Then, database will response a corresponding $N_i$ and a $K_i$ . One $N_i$ corresponds to only one $K_i$ . And each reader can read several $N_i$ and $K_i$ . When tag registered to database, this tag can only be read by particular readers.

Step 2: Each RFID reader has a unique identification $ID_{Ri}$ . After registering to database, the reader can only access the particular tags. When a reader registers to database, they will coordinate $N_i$ and $K_i$ . That is, once $i^{th}$ reader registered to database, the database store $ID_{Ri}$ , database will response the corresponding $N_i$ and $K_i$ to the registered reader. Therefore, reader can only read RFID tags that have the same $N_i$ and $K_i$ . Due to the illegal readers have not registered to database, their access ability is excluded.

## 2.3 Communication phase

Through register phase, tag and reader can perform the mutual communication. Our scheme uses mutual authentication mechanism, lightweight encryption–CRC during the communication process, and also confirms EPC Class1 Generation2 standard. The detail scenarios of this new scheme are described in Figure1.

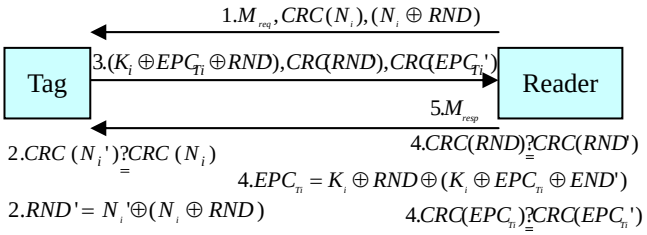


**Figure1. Communication scenarios of the proposed scheme**

Step 1: When reader wants to access tag, it should send a message $M_{req}, CRC(N_i), (N_i \oplus RND)$ , where $M_{req}$ is a reading request, $CRC(N_i)$ is a nonce protected by CRC function, $(N_i \oplus RND)$ is using exclusive-or to operate the nonce $N_i$ and the random value $RND$ .

Step 2: Upon receiving the $CRC(N_i)$ , the tag will verify $CRC(N_i') \stackrel{?}{=} CRC(N_i)$ . It means to use CRC function to calculate several different $N_i'$ which is stored in tag, and checks whether has an equal value $CRC(N_i)$ that is generated from the legal reader. If there is not any equal value, it means this reading request is sent from attacker or from a forbidden list; the tag will not do any further calculation and response. If $CRC(N_i') = CRC(N_i)$ , tag will continue the following calculation. Tag computes $RND' = N_i' \oplus (N_i \oplus RND)$ . Due to $N_i'$ is equal to $N_i$ ; thus $RND'$ is equal to $RND$ which is selected by reader.

Step 3: Tag computes $(K_i \oplus EPC_{Ti} \oplus RND')$ , $CRC(RND')$ , $CRC(EPC_{Ti}')$ , and sends them to reader.

Step 4: Once receiving the tag's response message, reader uses CRC function to operate random value $RND$ that got from its memory, and compares to $CRC(RND')$ that got from tag $CRC(RND) \stackrel{?}{=} CRC(RND')$ . And then reader decrypts the correct EPC by $EPC_{Ti} = K_i \oplus RND \oplus (K_i \oplus EPC \oplus RND')$ . And then reader verifies $CRC(EPC_{Ti}) \stackrel{?}{=} CRC(EPC_{Ti}')$ to make sure the EPC did not modify by attacker.

Step 5: When reader already get tag's $EPC_{Ti}$ , and the legal of tag has been confirmed. Therefore, tag can communicate with reader securely with mutual authentication and response a message

$M_{resp}$.

## 3. SECURITY ANALYSISES

In this session we will survey and analysis security requirements that purposed in session 1.3.

### 3.1 Pretend reader attack tag analysis

The purposed scheme can avoid illegal tag access, because the verification in Step 2 of the communication phase:

$$CRC(N_i') \stackrel{?}{=} CRC(N_i)$$

Tag will use the *CRC* function to operate $N_i'$ which is stored in tag, to compare with each reader's request message $CRC(N_i)$. Thus, any illegal access can be averted.

### 3.2 Pretend tag attack reader analysis

The purposed scheme also can avoid attacker using illegal tag to attack reader. Through the verification in Step 4 of the communication phase:

$$CRC(RND) \stackrel{?}{=} CRC(RND')$$

Reader will calculate $CRC(RND)$, and compare to $CRC(RND')$ that received from tag, to verify whether they are equal or not. If they are the same, they will do further processing. On the contrary, the message, that attacker sends to reader, will not include current random value $RND'$. Thus, the pretend tag attack reader can be averted.

### 3.3 Man-in-the-middle attack analysis

This attack method means attacker attack the communication between tag and reader. However, this attack can't success in our purposed scheme. Through $CRC(N_i)$, $(N_i \oplus RND)$ in Step 1 of the communication phase and $(K_i \oplus EPC_{Ti} \oplus RND')$ in Step 3 of the communication phase, we can verify the critical transmission messages between tag and reader via CRC function, exclusive-or calculation and key to protect. Attacker can not get the inside messages. Besides, we add random value *RND* in transmission process. When reader finishes a query it will change a random value *RND* every time. Therefore, attacker will hard to decrypt. Even attacker gets a key $K_i$, the attacker still can not crash the whole system, and our scheme can decrease the system damage.

### 3.4 User habit privacy analysis

To protect the user habit privacy, our scheme can get this goal clearly. With many protections, attacker can not get tag's EPC. Through the verification in Step 2 of the communication phase:

$$CRC(N_i') \stackrel{?}{=} CRC(N_i)$$

Attacker can not send $CRC(N_i)$ that in tag's permission list, and then tag will have no response to illegal reader. Besides, through the protection method $(K_i \oplus EPC_{Ti} \oplus RND')$, $CRC(RND')$ and $CRC(EPC_{Ti}')$ in Step 3 of the communication phase, we can see even attacker want to get tag send to legal reader's response message, it only can get the above encrypted message, can not know the real $EPC_{Ti}$. Thus, the user's habit privacy can be ensured.

### 3.5 User location privacy analysis

Although attacker can't get message in tag, attacker still can trace user's location. However, it will fail in our purposed scheme. We use CRC function $CRC(N_i)$ and exclusive-or $(N_i \oplus RND)$ to protect transmission message in Step 1 of the communication phase. When tag and reader finished a transmission every time, reader will change a random value *RND*. So, even attacker intercepts the message that tag response to legal reader, reader will use different random value *RND* in next transmission. Then attacker will think that is different tag, so attacker can't lock user's location.

### 3.6 Mutual authentication between tag and reader analysis

The purposed scheme can satisfy mutual authentication mechanism between tag and reader. Through the verification in Step 2 of the communication phase:

$$CRC(N_i') \stackrel{?}{=} CRC(N_i)$$

Tag can confirm if it can read by legal reader.

Besides, if reader has not registered to database, it can not read tag. By the verification in Step 4 of the communication phase:

$$CRC(RND) \stackrel{?}{=} CRC(RND')$$

Reader can confirm the response message if it is a legal tag or not. Thus, tag verifies reader, and reader also verifies tag. It gets mutual authentication between tag and reader.

### 3.7 EPC Class1 Generation2 standard analysis

In EPC Class1 Generation2 standard, tag is limited with hardware and cost, which can only do CRC and exclusive-or operation, and generates random number. Other complex operation, like hash function, symmetric encryption, and asymmetric encryption can not confirm this standard, but our proposed scheme

uses only CRC, random number generator, and exclusive-or calculation, so it can satisfy with EPC Class1 Generation2 standard.

### 3.8 Lower database loading analysis

In the proposed scheme, we use random value $RND$ to decrease reader's searching range. Reader takes $RND$ from its memory that used before, and it can use the corresponding $K_i$ to decrypt tag's EPC without search the entire database. It surely can lower database loading.

## 4. CONCLUSIONS

In sum, the proposed scheme confirms EPC Class1 Generation2 global standard, it is practical. It also lower database loading and achieves many security requirements, such as avoid pretending attack, avoid man-in-the-middle attack, and mutual authentication etc. After tags and readers register to database separately, they can communicate in off-line mode. So, it is suitable for mobile RFID environment.

The purposed scheme can be applied in airport's security management. For example, each electric passport has a RFID tag, and each airline's service area and boarding gate have RFID reader. When Bob buys a plane ticket from "A" airline, the airline will write related information into Bob's electric passport. If Bob's flight number needs to board at boarding gate "one", but Bob goes to boarding gate "two"; when the reader of boarding gate "two" checks the RFID tag's in Bob's electric passport, and find Bob should board at boarding gate "one", then the system will send message to tell Bob the right boarding gate.

Here is another example, sickrooms are separated in different floor in the hospital, and patients on the same floor are separated in different doctors to diagnose. Now, we hypothesis every doctor and nurse have RFID reader in the hospital, and every patient's hand ring or patient card has RFID tag. The assigned doctor or designated nurse can only read the patient's EMR (Electronic Medical Record). The other doctor or nurse can't access unrelated EMR. Through this management, we can protect the patient's privacy. The proposed scheme can solve many security problems in practical applications.

## REFERENCES


[1] A. Juels, R.L. Rivest, M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy", 8th ACM Conference on Computer and Communications Security, pp. 103-111, ACM Press, New York, 2003.

[2] D. M. Konidala, K. Kim, "Mobile RFID Security Issues", SCIS 2006 on Hiroshima, Japan, 2006.

[3] EPC (Electronic Product Code) Class1 Generation2 standard by EPCglobal, description at http://www.epcglobalinc.org/

[4] H. Y. Chien, C. H. Chen, "Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards", Computer Standards and Interfaces, pp. 254-259, 2007.

[5] I. Vajda and L. Butty'an, "Lightweight authentication protocols for low-cost RFID tags," 2nd Workshop on Security in Ubiquitous Computing, Seattle, Washington, USA October 12, 2003.

[6] J. Ayoade, "Security implications in RFID and authentication processing framework", Security Advancement Group, National Institute of Information and Communications Technology, Japan, ELSEVIER Computers & Security, Vol. 25, No. 3, pp. 207-212, 2006.

[7] J. Saito, J.C. Ryou, and K. Sakurai, "Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags", EUC 2004, LNCS Vol.3207, pp. 879-890, 2004.

[8] M. Ohkubo, K. Suzuki and S. Kinoshita, "Cryptographic Approach to Privacy-friendly Tags", in RFID Privacy Workshop, Bartos Theatre, MIT Media Lab, MIT, November 15, 2003.

[9] mCloak: Personal / corporate management of wireless devices and technology, 2003. Product description at http://www.mobilecloak.com/

[10] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in 1st Intern. Conference on Security in Pervasive Computing (SPC), Boppard, Germany, March 12-14, 2003.

[11] S.E. Sarma, S.A. Weis, and D.W. Engels. "Radio-frequency identification systems". In Burton S. Kaliski Jr., Cetin Kaya Koc, and Christof Paar, editors,
CHES '02, Springer-Verlag, LNCS Vol. 2523, pp. 454-469, 2002.

[12] S.L. Garfinkel, A. Juels, R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security & Privacy, the Claremont Resort, Berkeley/Oakland, California, pp. 34-43, 2005.

[13] S.A. Weis, S.E. Sanma, R.L. Rivest, and Daniel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing, LNCS, Vol. 2802, pp. 201-212, 2004.

[14] S. Karthikeyan, M. Nesterenko, "RFID security without extensive cryptography", Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 63-67, 2005.

[15] T. Dimitriou, "A Lightweight RFID Protocol to protect against Traceability and Cloning attacks", IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks, SECURECOMM 2005.