

Security and Privacy: Modest Proposals for Low-Cost RFID Systems

#Damith C. Ranasinghe¹, Daniel W. Engels², Peter H. Cole³

¹*Auto-ID Labs, School of Electrical & Electronic Engineering, University of Adelaide
Adelaide SA 5005, damith@eleceng.adelaide.edu.au*

²*Auto-ID Labs, Massachusetts Institute of Technology,
77 Massachusetts Avenue, NE-46, Cambridge, MA 02139 USA, dragon@csail.mit.edu*

³*Auto-ID Labs, School of Electrical & Electronic Engineering, University of Adelaide
Adelaide SA 5005, cole@eleceng.adelaide.edu.au*

Abstract

Low cost Radio Frequency Identification (RFID) systems are increasingly being deployed in industry and commerce. These contactless devices have raised public concern regarding violation of privacy and information security. There is a growing need in the RFID community to discover and develop techniques and methods to overcome several problems posed by the above-mentioned concerns. This paper presents proposals on feasible security mechanisms for low cost RFID systems and analyses them from both security and privacy points of view.

1. INTRODUCTION

Various proposals have been made to address issues regarding information security and end-user privacy. Most of these solutions are outlined in [4, 5]. However, some of these ideas are not applicable because they were based on a particular protocol that will soon be obsolete, with the new generation of low cost RFID systems that are being developed and others are not practicable on account of their demand for circuit size and operation power. We present here a number of practicable proposals that would be suitable for addressing the security and privacy concerns that arise in the widespread use of low-cost RFID labels.

The use of Message Authentication Codes (MACs) has been discussed in previous literature. Takaragi [9] and his team of researchers have been the first to make available commercially an RFID chip (μ -chip) equipped with a MAC. The chip manufactured using a 0.18 micron CMOS technology occupies less than $0.25(\text{mm})^2$ of silicon wafer, placing the IC into the low cost end of the RFID labels.

The MAC implementation takes a very simple approach. The security of the μ -chip relies on a 128bit ID stored permanently on the chip at manufacturing time. This ID is a

concatenation of a previously encrypted MAC and chip data, the MAC being derived by encrypting a portion of the data using a hash function and a secret key, where the secret key is known to the manufacture and the clients. This mechanism does raise the difficulty level for forgers as the process of eavesdropping and creation of fake labels is made more difficult, however it does not provide privacy as the ID code embedded in the chip will breach anonymity and location privacy. There is also the risk of the key, which is common to many labels, becoming known.

The first public key encryption engine to be incorporated into an RFID chip was developed by Atmel. The NTRU GenuID chip uses an 8-bit RISC processor to implement an NTRU public key cryptosystem on the labels [14]. Hence, the NTRU implementation is able to harness all the advantages of a public key cryptosystem. However, the hardware implementation is resource intensive and the RFID label produced from the GenuID chip is an active label that stands at the more expensive end of the RFID label scale.

TEA is an encryption algorithm designed for simplicity and ease of implementation. The encryption algorithm is based on the Feistel cipher [11] and a large number of iterations to gain security without compromising simplicity. A description of the algorithm is provided in [12]. A hardware implementation of the algorithm is stated to have the same complexity as DES [12]. Despite the simplicity and the ease of implementation of the cipher, the level of security or its vulnerability to attacks are still not very clear.

Class I or Class 0 labels, of which the characteristics have been identified in [1] as defined by the AutoID Center, now the AutoID Labs, have only a read only or a write-once memory and are incapable of participating in a complex security mechanism. However, a simple approach to some aspects of privacy and security for Class I and Class 0 labels is suggested in [6]. This involves the destruction of the label

thus rendering it inoperable. Unfortunately the destruction of the label denies the user of the copious benefits that could have been obtained from a “smart object”.

It is the unique identity code, the EPC [7], in articles that allows the label owners to be tracked albeit in practice with difficulty. However, erasing the unique serial number of labels at the point of sale of the item can remove the unique identification aspect of the EPC while retaining the product code information. This does not remove all privacy concerns as tracking is still possible by associating a “constellation” of a label group with an individual. This implies that a particular taste in clothes and shoes may allow an individual’s location privacy or anonymity to be violated. However, it is possible to disable all aspects of a tag permanently in a way that it can not be activated again. Such mechanism may involve the disconnecting of the antenna or the destruction of the rectification circuit.

2. REASONABLE ASSUMPTIONS

It is important to define certain boundaries and assumptions without which it will be impossible to implement a mechanism to address security or privacy. This will also enable the definition of a framework for future research.

A. Framework

The low cost RFID labels taken into consideration will involve Class 0, Class I and Class II labels [1]. The following is a reiteration of those characteristics and certain assumptions to establish a foundation for an RFID security mechanism.

In respect to the cost constraints placed on these labels and the current cost of fabricating a transistor, the low cost labels are expected to have 200-4000 gates available for security purposes, although, the number of gates available is expected to increase over the years as manufacturing techniques and processes improve. Nevertheless, it is important to note that the above range is far below the current requirements for a public key encryption engine.

Furthermore, It is assumed that the time available for a label operation (and thus, any implementation of a security mechanism) is in the range of 5 - 10 milliseconds considering the performance criteria of an RFID system that demand a minimum label reading speed of 100-200 labels per second. A typical passive RFID label data transmission rate of about on the order of 100 kbps will be supposed.

Labels may have a means of communication through a physical contact, such as magnetic strips on smart cards, or close range shielded RF communications, for critical

operations such as “imprinting” secret keys [5]. In addition, it is reasonable to assume that some RFID labelled items may contain “optically encoded information”, in the form of a barcode or another optical encoding system [4,5]. This additional information has the potential to corroborate label identification information. Nevertheless, an RFID label is not required to have a physical contact; neither is an RFID labelled item required to have optically encoded information, but those features may provide a supporting role that can improve the effectiveness of a security mechanism for a low cost RFID system.

The problems involved with securing reader communications with a secure backend database will not be considered; instead, it is assumed that legitimate readers have secure connections to backend databases. The general assumptions on RF communication will be that the forward channel (interrogator to reader) is exposed to undetectable eavesdropping from several hundred meters away, while the backward channel (label to interrogator) is relatively difficult to monitor and can only be monitored from several meters away.

Considering the current electromagnetic compatibility (EMC) regulations, the operating range of low cost labels is limited to a few meters. It is assumed that the labels within reading range have a means of revealing their presence, but not their data, when interrogated by a reader. It is assumed that the labels will reply with a non-identifying signal to an interrogation by using a randomly generated number. It is also assumed that the previously mentioned class of labels implement a ‘kill’ command that will physically render the label unreadable perhaps by setting off a fuse or disconnecting the antenna [4].

The long-term security of label contents cannot be guaranteed since these contents are vulnerable to physical attacks. Hence, it is assumed that labels cannot be trusted to store long-term secrets such as secret keys that apply to a range of RFID labels, but secrets pertinent to an individual label that is unrelated another label seem to be acceptable.

Furthermore, the power utilization of any security related hardware should not exceed the typical tag power consumption of 150 microwatts. The power consumed should be a fraction of this value for the encryption hardware to be viable.

3. SECURITY PROPOSALS

A. Authentication using a challenge-and-response

Practically all identification schemes or authentication schemes use a challenge and response protocol.

Authentication is an important RFID security measure for preventing counterfeit manufacture or substitution. It is also important for controlling access to label contents. Use of authentication may also be required in other applications of RFID technology such as baggage reconciliation or secure entry systems.

The goal of an authentication scheme in RFID is to prevent an adversary from creating a fake label to misrepresent the legitimate article. The mechanism is described below [13].

1. Reader chooses a challenge, x , which is a random number and transmits it to the label.
2. The label computes $y = e_K(x)$ and transmits the value y to the reader (here e is the encryption rule that is publicly known and K is a secret key known only to the reader and the particular label).
3. The reader then computes $y' = e_K(x)$
4. Then the reader verifies that $y' = y$

It is possible to construct a challenge-and-response protocol using a variety of cryptographic tools. Most Symmetric key encryption algorithms, such as AES, are all suitable candidates. However, in terms of silicon they present expensive solutions.

A possible candidate for a cryptographic tool can be found in [8], where a challenge response pair is created using a PUF (Physically Unclonable Functions [10]) circuit that exploit process variation in the silicon fabrication, using only 100s of gates.

The PUF circuit is able to uniquely characterise each IC due to manufacturing variations [8]. These individual characteristics then become similar to the secret keys used in a symmetrical encryption scheme. Thus, it is possible to identify and authenticate each IC reliably by observing the PUF response.

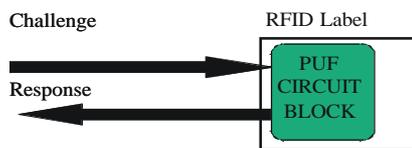


Fig. 2: A model of a PUF based Class I/ Class II RFID label

Manufacturers attempt to control process variations to a great degree however, these variations are largely beyond their control and hence it is not possible for an adversary to fabricate identical PUF circuits. The material presented in [8] suggests that there is a strong enough variation between chip to chip for a sufficient number of random challenges to

identify billions of chips. The probability that the first measured response bits to a given challenge (set of bits) on a chip is different from the measured response for the same set of bits (challenge) on a different chip is estimate to be 23% to 40% depending on the PUF circuit architecture [8]. It has been estimated that about 800 challenge response pairs are sufficient to distinguish 10^9 chips with the probability $p \sim 1 - 5 \times 10^{-10}$ [8]. Such an identification scheme would only involve around hundreds of gates on an RFID silicon design. Figure 2 depicts a model of an RFID chip with an integrated PUF circuit.

The following Figure 3 illustrates the use of a PUF based RFID system. It is clear that once a challenge has been used it can not be used again since it may have been observed by an adversary. However it is possible to have a list of challenges and responses or use an encrypted communication link to deliver challenge and obtain the responses. Such simple encryption schemes are proposed in the following Sections.

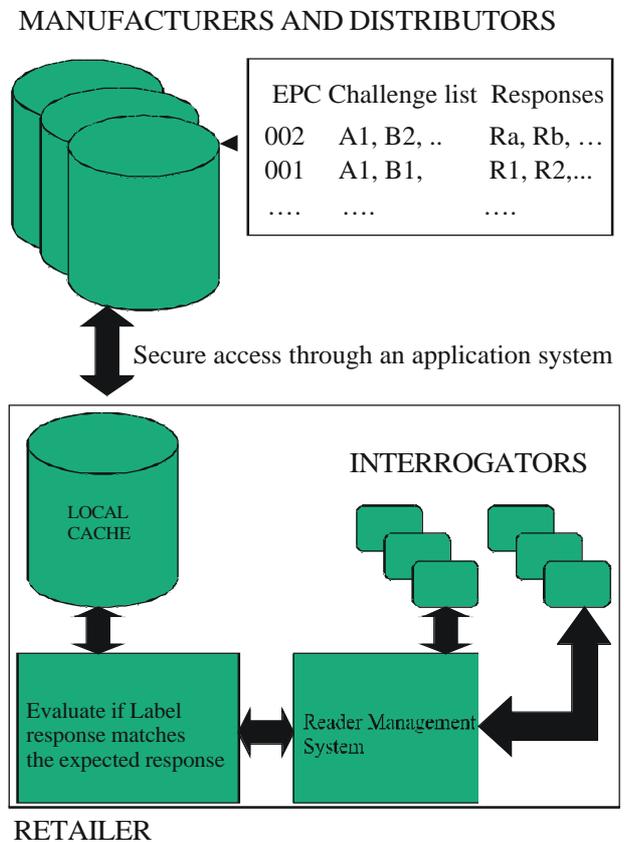


Fig. 3: An overview of an implementation of a PUF based RFID system

The security of the above system relies on a PUF to securely store a unique secret key in the form of fabrication variations. The PUF based security systems are susceptible to reliability issues, however this is still an active area of research. The

most probable attacks on a PUF based challenge response system are outlined in [8]. The above scheme will allow a label to authenticate itself to a reader before any sensitive information passes between the devices. The security of the system depends on the difficulty of replicating a PUF circuit and on the difficulty of modelling the PUF circuit successfully. This is not a simple process and is therefore an adequate deterrent depending on the value of the article being authenticated by the reader.

B. Re-encryption

RFID labels when requested will scroll out their EPC. This unique identity carried by the RFID labels poses a security threat and a privacy threat. Thus, it is important to control access to a label's EPC, or to allow an RFID label to respond with a non-identifying response.

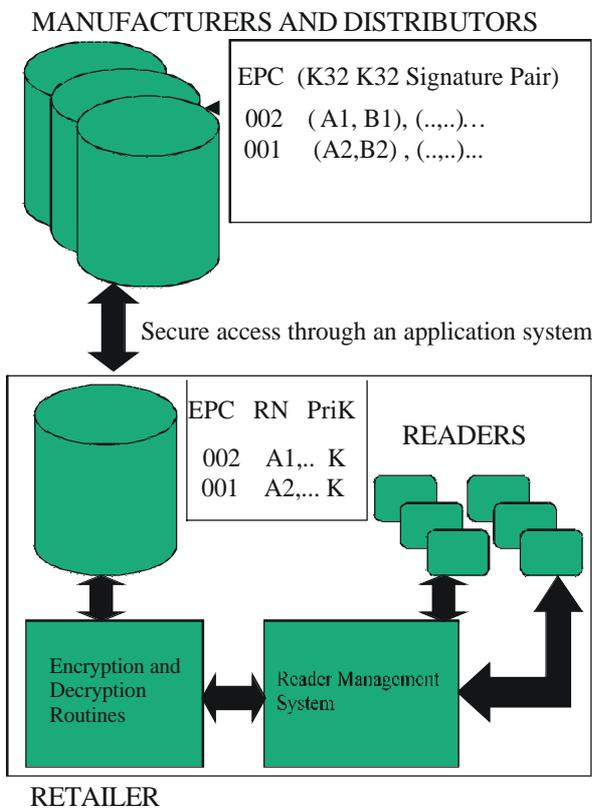


Fig. 4: Re-encryption scheme: After identification, the reader and the label may be authenticated using a two shared secret scheme discussed in the following sections.

Re-encryption offers a novel perspective on achieving these goals. Instead of storing the EPC in a write once format, it is possible, for instance, for a retailer in the supply chain to store an encrypted version of that EPC concatenated with a random number on the tag. This encryption may be performed using a secret key that is known solely to the retailer. Thus,

when a label is requested to scroll out its EPC, it will scroll out an encrypted version of the EPC, which to a third party will appear as a stream of random bits. The scheme is illustrated in Figure 4. This padded random number can then be used as a one-time pad for encrypting the forward link. On identification of the label, the reader has the option of storing back an encrypted version of the EPC padded with a new random number, thus allowing a randomly evolving set of responses from a label. This scheme thus bestows the label owners with the ability to reprogram the label as often as required.

Once an RFID labelled product is sold, the consumer has the opportunity to encrypt the EPC data using a personal public key.

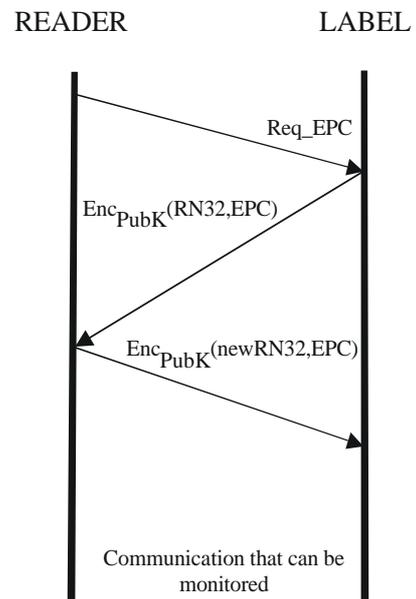


Fig. 5: Re-encryption process: Encryption scheme may be based on a public key encryption or a private key encryption scheme. Use of a public key encryption scheme will allow the encrypted data to be used as a digital signature, thus authenticating the label at the same time.

The above scheme may be further modified by using a public and a private key pair, where the retailer is able to encrypt the EPC and the random number using a public key. Now the decryption of the tag contents using the private key should yield a meaningful EPC and the associated random number. This will allow the RFID label to be authenticated, within a single operation.

An implementation of the re-encryption scheme requires that RFID labelled item be programmed with the encrypted information perhaps in a secure environment. This may be achieved by performing the label programming in a metal cage. This cage may vary in size, such as that of a case or of a

palette. However, it may not be necessary to program the labels in a secure environment, since it is a difficult proposition to trace the evolution of a label contents by an adversary who may have managed to eavesdrop on the first read of an EPC.

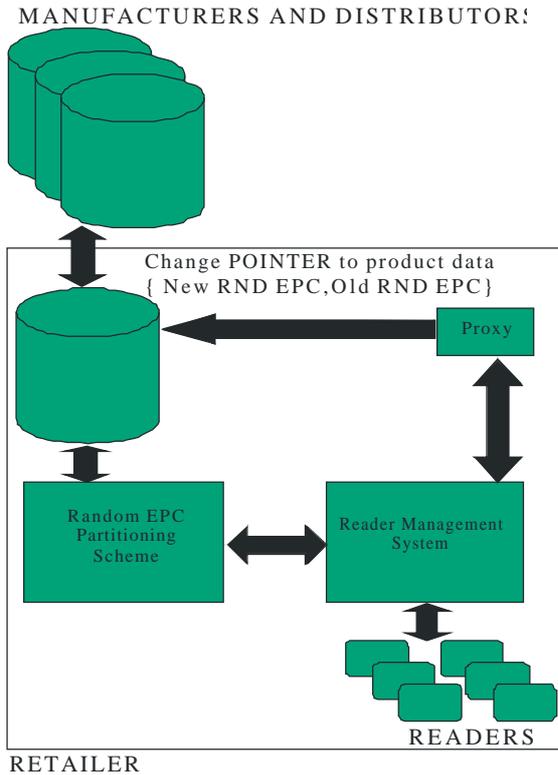


Fig. 6: Random EPC scheme: After reading the encrypted RND EPC the reader forwards the data to a Proxy. The Proxy then decrypts the EPC and generates a new encrypted RND EPC to be stored in the tag. The new encrypted RND EPC is sent to the reader while a change pointer command is issued to the database maintaining pointers to related label data records.

A further modification to the re-encryption scheme is the concept of using a pool of completely random EPC's thus the EPC number will have no longer an information bearing structure. Thus, it is possible for RFID labelled items of sensitive nature (such as that required for military use) to label all of the items with a randomly generated EPC. The labelled items may then contain an encrypted version of the EPC on the label's chip IC. However, scalability is an issue. This can be resolved by partitioning the random number pool into categories based on the ranges of random EPC as depicted in Table 1. It is possible to use an encrypted version of the random EPCs in the re-encryption scheme. This scheme prevents an adversary from obtaining any useful information in the event the encryption scheme is compromised. The security of the scheme relies on the ability of the label owners to keep the encryption key secret (see Figure 6).

TABLE 1: RANDOM EPC PARTITIONING

Partition ranges	Subdivision	Subdivision
0 – 100,000	0 – 50,000	0 – 25,000
	50,001 – 100,000	25,001 – 50,000
		50,001 – 75,000
		75,001 – 100,000
100,001 – 200,000	100,000 – 150,000
	150,001 – 200,000	

Re-encryption provides anonymity by never transmitting a predictable response, an encrypted forward link and also allows the authentication of a reader and a label.

C. Shared Secrets

A simple approach to developing an authentication scheme and providing a secure forward link can be designed by using a single secret (K). Once a reader has uniquely identified a label, a reader may use that information to discover a secret K, and two time stamps (Told, Tnew) associated with that particular label by contacting the distributor/manufacture of that product using a secure mechanism. There may be several keys associated with a single label. The database is then able to provide the reader with a label secret and a cyclic redundancy check (CRC) performed on the key (KCRC). The reader is then able to exclusive-or the KCRC with a reader generated random number (RN1r) to be communicated to the label {RN1r,KCRC}. Upon receipt of the value the label obtains the RN1r. Following which, the label replies to the reader by transmitting the RN1r exclusively or'd with a CRC generated on the RN1r (RNCRC). Thus the reader is able to verify that the label must indeed possess the secret K and therefore is the legitimate label (see Figure 7).

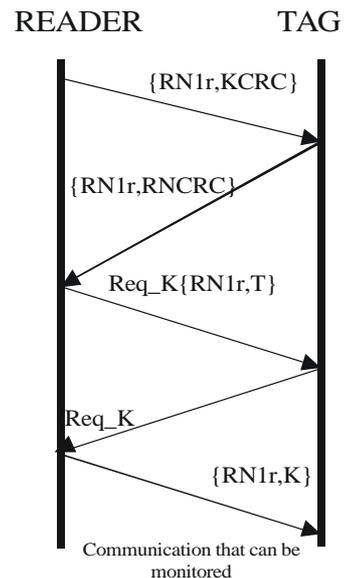


Fig. 7: Single shared secret authentication

However, in order for the label to confirm that it is conversing with a legitimate reader, the reader replies with RN_{r1} exclusively-or'd with the label time stamp (Told and T new). If the old time stamp matches that on the label, the label will store the new time stamp and wait for the reader to transmit the secret key K exclusively-or'd with RN_{r1} . If the key K sent from the reader is that stored in its memory the label grants access to the reader to manipulate its resources. Thus, this simple scheme allows the reader to authenticate a label and a label to authenticate a reader. Instead of time stamps, it is possible to use one time pads to achieve the same authentication procedure. Then the secret key cannot be used again as the mechanism will then be vulnerable to replay attacks.

Similarly authentication of a labelled item may be accomplished by using two shared secrets A and B associated with each label. A reader can communicate key A by exclusive-or'ing it with a randomly generated number RN_{r1} by the reader. The label may then obtain this randomly generated number correctly if it is a legitimate label that has the two secrets imprinted in its memory space. Thus a genuine label will respond with its second secret, B exclusively or'd with its RN_{r1} . The reader can then validate legitimacy of the RFID label by comparing the value B sent from the label with its own value obtained from a secure database. The reader then waits for the label to send a random number generated on the label (RN_{t1}) exclusive or'd with RN_{r1} . The reader then communicate to the label a signature generated using both A and B to the label by encrypting it with RN_{t1} . The label is then able to compare the signature C with that stored in its memory to ascertain that the reader is an authenticated entity that can be trusted. This is however dependent on the label being able to generate a statistically good random number.

E. Many Shared Secrets

A variation on one-time pads can be used in low cost RFID labels. In the novel scheme, labels are equipped with a small rewritable memory. Prior to the release of a label, a set of random numbers (authentication keys) generated by a completely random process is stored into the label along with a label ID. A back end database stores a copy of the random codes and the associated label ID. The number of authentication keys can reflect the lifetime of the product and the number possible times the object may require authentication.

The label ID may be read from the label during an interrogation. The ID provides knowledge of the label being authenticated by the reader by consulting the relevant records in a secure back end database. Thus, the interrogator may

obtain and transmit one or more of the random numbers obtained from a secure database. One of the numbers should match a series of random numbers stored on the label. If a match occurs the label responds with a return authentication code known exclusively to the database and increments a counter to select a new random number for the next authentication procedure. An identical counter that determines which of several authentication numbers is next in force, is incremented at the database (see Figure 8).

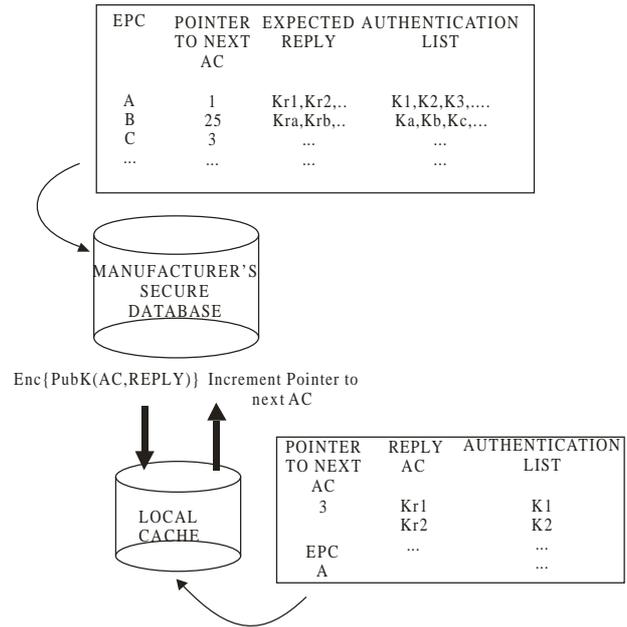


Fig. 8: Many shared secrets: A list of authentication codes (AC) can be used as a one-time pad to authenticate or control access to labels.

Hence, the above mechanism prevents an eavesdropper from obtaining any clue regarding the next correct authentication key, or next label authentication response. The only available information to an eavesdropper is an apparent burst of random numbers. In the event of an unauthorised reader, the label will not respond unless the reader knows the next random number expected by the label or the label may respond with an internally generated almost certainly incorrect random number. In case a counterfeit label is interrogated, the label may respond with a random number, but the interrogator will fail to find a match, and thus detect the counterfeit.

Nevertheless, this scheme still leaves the possibility of a physical attack, where the contents of the label may be discovered. However, in the worst case, this information cannot be used to counterfeit labels in massive quantities as the set of authentication keys and authentication responses are all different, finite, synchronised and completely random on each individual label.

5. CONCLUSION

The severe cost constrains and resulting severe on-label resource constraints for low-cost RFID allow for a range of limited security and privacy features to be added to the labels. Due to the severe constraints, the general concern in these low-cost systems is not to develop an extremely hard to crack security mechanism but is to develop a good enough security mechanism for the expected application.

We have prosed a number of different such useful and simple concepts involving removing label IC complexity, and using the abundant resources available to the reader and application systems of an RFID system to countermeasure the weaknesses in respect to security and privacy. Some of them are nevertheless highly secure.

REFERENCES

- [1] Cole, P. H., "Fundamentals in Radiofrequency Identification", 2003, <http://www.eleceng.adelaide.edu.au/Personal/peter/peter>
- [2] Cole, P. H., and Engels, D. W., "Auto-ID 21st Century Supply Chain Technology", Auto-ID Centre, January 2001. <http://www.autoidlabs.org>
- [3] J. Hoffstein, J. Pipher, and J.H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem", *Proceedings of ANTS III*, Portland, June 1998.
- [4] Weis, S. A., Sarma, E. S., Rivest, R. L., and Engels, D. W., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *Security in Pervasive Computing*, 2003.
- [5] Weis, S. A., Sarma, E. S., Rivest, R. L., and Engels, D. W., "Radio-Frequency Identification: Security Risks and Challenges", *Cryptobytes (RSA Laboratories)*, vol 6, no1, Spring 2003.
- [6] Sarma, S., and Engels, D. W., "RFID Systems, Security & Privacy Implications", Auto-ID center white paper, Feb 2003. <http://www.autoidlabs.org>.
- [7] Brock, D.L., "The electronic product code – a naming scheme for physical objects", Technical Report, AutoID center, January 2001, <http://www.autoidlabs.org>.
- [8] Lee., W. J., Lim, D., Gassend, B., Suh, G. E., Dijk, M. van. And Devadas, S., "A Technique to build a secret key in integrated circuits for identification applications", *VLSI Symposium*, 2003.
- [9] Takaragi, T., Usami, M., Imura, R., Itsuki, R., and Satoh, T., "An Ultra Small Individual Recognition Security Chip", *IEEE Micro*, November-December 2001.
- [10] Gassend, B., Clarke, D., Dijk, M. van, and Devadas, S., "Silicon physical random functions", *Proc. of computer and communication security conference*, May 2002.
- [11] Menezes, A., Van Oorschot, P., and Vanstone, S., *Handbook of Applied Cryptography*, 3rd edition, CRC Press 1996.
- [12] Wheeler, D., and Needham, R., "TEA, a Tiny Encryption Algorithm", Computer Laboratory, Cambridge University, England, 1994.
- [13] Stinson, D. R., *Cryptography Theory and Practice*, CRC Press, 1995.
- [14] Ntru home page, <http://www.ntru.com/products/genuid.html>.