Confronting Security and Privacy Threats in Modern RFID Systems

#Damith C. Ranasinghe[1], Peter H. Cole[1]
[1]*School of Electrical and Electronic Engineering, The University of Adelaide*
Auto-ID Lab, Adelaide SA 5005, Australia, damith@eleceng.adelaide.edu.au
cole@eleceng.adelaide.edu.au

Abstract*-*The modern form of RFID technology that is set to dominate is that enabled by low cost RFID technology. This paper presents an overview of the technological aspects vital to illuminating associated security and privacy threats. The paper also describes a simple security model and briefly considers some of the vulnerabilities faced by such low cost RFID systems. Finally the authors would like to extend preliminary work published on a minimalist encryption method first published in [26] and [27].

I. INTRODUCTION

A simple illustration of the concept of a Radio Frequency Identification (RFID) system is provided in Fig. 1. Here a transmitter of interrogation signals which is contained within an interrogator communicates via electromagnetic waves with an electronically coded label to elicit from the label a reply signal containing useful data characteristic of the object to which the label is attached. The reply signal is detected by a receiver in the interrogator and made available to a control system.

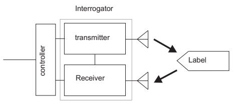

Fig. 1. Illustration of an RFID system.

One of the inhibitors to wide-scale adoption of RFID technology is the cost of a label. Thus low cost RFID refers to an RFID system based on inexpensive RFID tags, and is rapidly becoming the enabling technology of modern RFID systems.

Low cost RFID labels are passive transponders. The most common operating principle of labels in the category of passive technology is that of RF backscatter or load modulation [1] in which a powering signal or communication carrier supplies power or command signals via an HF or UHF link. However the circuits within the label operate at the carrier frequency or at a lower frequency, and reply via sidebands generated by modulation, within the label, of a portion of the powering carrier. This approach combines the benefits of relatively good propagation of signals at HF and UHF and the low power operation of microcircuits at RF or lower. Powering at UHF is employed when a longer interrogation range (several metres) is required, and HF powering is employed when electromagnetic fields, which exhibit good material penetration and sharp spatial field confinement, is required, or sometimes when a very low cost RFID system implementation is desired.

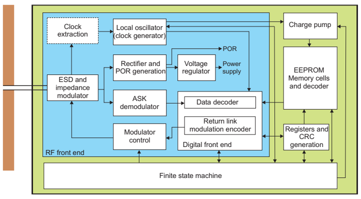
Clock extraction
Local oscillator (clock generator)
Charge pump
POR
Rectifier and POR generation
Voltage regulator
Power supply
ESD and impedance modulator
EEPROM Memory cells and decoder
ASK demodulator
Data decoder
Return link modulation encoder
Modulator control
Digital front end
Registers and CRC generation
RF front end
Finite state machine

Fig. 2. Block diagram of a passive UHF/HF RFID label.

The following section provides a quantitative characterisation of low cost RFID systems prior to highlighting their vulnerabilities.

II. SYSTEM CHARACTERISATION

Fig. 2 is an illustration of a typical low cost transponder [12]. The block diagram of an HF and a UHF chip varies little. In a UHF chip there is a dedicated low power oscillator, while in an HF chip the clock signal is derived from the received carrier by dividing down the carrier in steps. TABLE 1 provides a summary of operational considerations and parameters that define a low cost RFID system.

TABLE 1
LOW COST RFID SYSTEM OPERATIONAL CONSIDERATIONS

RFID labels	Class I and II type of labels
Unique Identifier	EPC (Electronic Product Code) of 96 – 256 bits. Defined in by EPCglobal[2] in the tag data specification standard.
Read range	3 m – 5 m for UHF and 200 – 500 mm for HF operation under FCC regulations.
Label reads/s	200 – 1500 (demanded by end users).
Logic	7000 – 10000 gates for a Class I Generation 2 air interface protocol (CIG2) implementation [3].
Power consumption	10s of microwatts, and should not exceed that required for E^2PROM operation, so the tag read range requirements can be maintained.
Expected Security	Class I labels carry a 'kill password' which must be sent to the tag prior to label destruction. Class II labels are expected to provide services to implement a secure communication link.
Standards	The most prevalent standard for UHF tags is the CIG2 protocol [3]. The multi-part ISO 18000 air interface standard defines protocols for a number of different frequencies; LF, HF and UHF. ISO 18000 Part 3 Mode 1 is possibly the most prevalent standard as of yet. The most commonly used HF standard, other than the ISO 18000, is ISO 14443 (types A and B).

III. SECURITY MODEL

Thus far, the focus has been on considering the various aspects of low cost RFID technology. This section presents a simple security model to aid in the illumination of various vulnerabilities identified in Section IV.

A. *Authorized Readers and Legitimate Tags*

The term “authorized” will be used in relation to readers or interrogators who are registered in a given RFID system’s database and are equipped with the necessary security mechanism to access secure resources of that system. The term “legitimate” will be used in relation to tags that are registered in a given RFID system’s database as verified by an authorized reader. Then a reader that is not authorized will be referred to as an “unauthorised” reader while a tag that is not legitimate will be referred to as a “fraudulent” tag. When a legitimate tag is copied to produce a copy that may for all purposes of identification be verified as a legitimate tag, it will be called a “cloned” tag.

B. *Tamper Proof*

The long-term security of label contents cannot be guaranteed since these contents are vulnerable to physical attacks. Hence, labels cannot be trusted to store long-term secrets such as secret keys that apply to a range of RFID labels, but storage of secrets pertinent to an individual label that are unrelated to another label are considered acceptable as long as the information obtained is unhelpful in defeating the security mechanism of another tag.

C. *System Model*

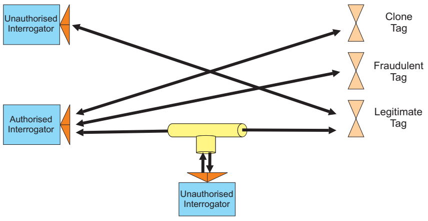

Fig. 3. Possible interaction between communication participants.

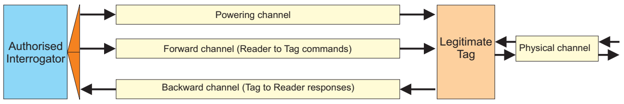
Authorised Interrogator
Powering channel
Forward channel (Reader to Tag commands)
Backward channel (Tag to Reader responses)
Legitimate Tag
Physical channel

Fig. 4. System model describing the information channels.

While RFID systems consist of various components, a system model need only be concerned with interrogators, tags, and the communication channels between them, since other components of the system are not confronted with any constraints with regards to implementing necessary cryptosystems to secure information. Hence it is possible to consider an interrogator and the rest of the back end system as a single entity, which can be referred to as an authorised interrogator. Now it is possible to outline the communication participants; authorized interrogators, legitimate tags, fraudulent tags, clone tags and unauthorised interrogators. Fig. 3 shows the possible ways in which the various communication participants can interact.

A communication model describing the various information channels is shown in Fig. 4. The sources of information available to an adversary in a low cost RFID system are that which can be obtained over the insecure communication channels, the contents of the tag memory by way of the memory channel, power analysis of the powering channel, and from the forward channel and the backward channels as shown in Fig. 3.

The adversary may read or write to the forward and, or the backward channel, depending on the frequency of operation and the nature of the adversary being modelled, as in the case of a man-in-the-middle attack. The physical channel is considered to be read once only as the process of extracting memory contents is destructive to the legitimate tag. However, it may then be possible for the adversary to create a clone of the tag using the information obtained, but creating many clones of the same tag is considered to be not possible in supply chain applications due to the availability of a track and trace facility [4]. However for a general application such as an access control system, such an assumption is not valid.

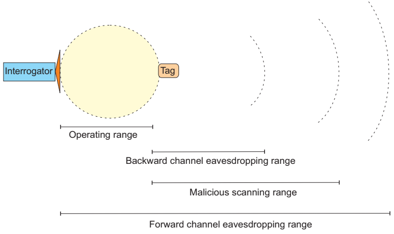
Interrogator
Tag
Operating range
Backward channel eavesdropping range
Malicious scanning range
Forward channel eavesdropping range

Fig. 5. Tag reading range classification.

Considering the possible distances at which a third party can listen to a conversation between a tag and an interrogator allows the general ideas of an adversary’s behaviour to be categorised as shown in Fig. 5. There are generally two forms of eavesdropping possible with low cost RFID systems; passive eavesdropping and scanning (active eavesdropping).

Passive eavesdropping: This form relates to the observation and or recording of communication between a reader and a tag by an unintended recipient. Passive eavesdropping may be performed by a third party in either the operating range, backward channel eavesdropping range or the forward channel eaves dropping range.

Scanning (Active eavesdropping): In this situation a third party or an adversary is actively attempting to read the contents of a tag without the authority of the tag owner. In a scanning scenario with respect to a low cost RFID system an adversary is using a rogue reader to power the tag and an active eavesdropper will have a working range within the malicious scanning range outlined in Fig. 5.

The complete set of data stored on a legitimate tag will be unique, and not dependent on other tags. This assumes that a tag’s complete set of memory contents is unique (such as secret keys, unique tag identifiers and passwords) and it is not identical to any other legitimate tag.

IV. Vulnerabilities of Low Cost RFID Systems

Using the security model outlined in the previous sections it is clear that low cost RFID systems generate significant security risks, mainly due to their cost constrained implementations and insecure communication channels over which tags and readers communicate. The security risks that arise as a result are outlined below.

A. Cloning

Devices designed to impersonate tags or readers (imitating the behaviour of a genuine label or a reader). Direct consequences of cloning are the possibility for counterfeiting, where a genuine article tagged with an RFID label, may be reproduced as a cheap counterfeit and tagged with a clone of the authentic RFID label. Examples of cloning attacks can be found in [5] and [6].

The EPC Class I tags have no mechanism for preventing cloning as the tags are simple bit storage devices that transmit a string of bits on request from any valid reader. While track and trace capability solves the problem of confirming the existence of an illegal clone it may not be possible to distinguish the original tag from its illegal duplicates.

B. Man-in-the-Middle

An RFID system is constantly under threat from man-in-the-middle attacks resulting from eavesdropping on reader and tag transmissions.

C. Denial of Service

An adversary may initiate a denial of service (DoS) attack to bypass or avoid security systems. For instance a DoS attack is easily carried out by placing a large number of fake labels for identification by a reader. In addition tags may be prevented from being read by using the simple concept of a Faraday cage or by jamming the RFID interrogator signals, for instance by intentionally creating noise in the frequency band in use. For critical applications, a DoS attack may pose devastating effects.

D. Communication Layer Weaknesses

Recently ratified EPCglobal C1G2 air interface protocol [2] has a number of security features based on the use of tag specific passwords. A recent publication in [7] has shown how the ‘kill password’ of a tag can be deduced by the careful analysis of the tag power consumption to a series of well constructed test passwords. This highlights a particular vulnerability of low cost tags to power analysis attacks and the vulnerabilities of storing long term secret information on a tag.

While power analysis attacks may be prevented in the future albeit at a higher cost, the fact that each RFID tag has at least two unique passwords will create both potential security and logistical nightmares if the problem of careful key management is not considered. It is not difficult to imagine a scenario in the future where a list of kill passwords is uploaded to a public web site.

The recently ratified C1G2 protocol also relies on the tag generating a random number to be used as an input to an exclusive-or operation. The risks associated with inefficient or inadequate random number generation in RFID tags (that is a high correlation between the random numbers, in a pseudo-random number sequence) is emphasized in [8].

E. Physical Attacks

In addition, the labels themselves are exposed to physical attacks due to the absence of tamper proofing as dictated by cost limitations of low cost tags. Physical attacks are possible irrespective of whether measures are in place to protect labels. However, the ability to gain useful information from a protected label is a much more difficult problem. An insight into to possibilities of physical attacks can be gleaned from an increasing body of work in the area of smart cards. A complete overview of possible physical attacks and countermeasures are outlined in [9] while specific lower cost physical attacks are presented in [10].

The majority of physical attacks possible on devices in general are either non-invasive attacks (timing analysis, power analysis, analysis of certain glitches, radio finger printing, and exploitation of data remnance) or they may be invasive attacks (microprobing, Focus Ion Beam editing, or altering information stored in memory using a laser cutter microscopes) [10, 11].

F. Privacy violations: Profiling

It is possible to imagine various scenarios of privacy violations and most of them are already existing concerns from technologies such as credit cards, browser cookies or Bluetooth devices. However RFID, due to its artefacts resulting from cost constraints, presence of a unique identifier readable by anyone, and the encoding of product information on the unique numbering scheme such as the EPC [4] create two possible scenarios; profiling, and tracking and surveillance, where privacy of people as well as corporations may be infringed.

An individual with a number of labelled items may be scanned by a third party to identify individual possessions or “taste”, and specific EPC numbers on products may then be associated with an individual. The data obtained can be misused to violate an individual’s wishes to remain anonymous. For instance persons carrying religious material, material related to a certain political affiliation may no longer be able to pursue their beliefs or interests in their own privacy and apart from their reading material becoming public knowledge, their beliefs and opinions may be used in acts of persecution, jealousy, or hatred.

G. Tracking and Surveillance

A further privacy concern resulting from the association of human identification information to object identification information and the unobtrusive scanning of RFID labelled items carried by an individual is posed by the possibility of tracking, albeit with technical difficulty. Correlating data from readers obtained from multiple locations can reveal the movement, social interactions or financial transactions of an individual once an association is made between a unique tag identifier and a person. In response to such concerns there have been suggestions to remove the unique identifier in an EPC to prevent a specific EPC from being associated with individuals. Even if such a scheme is implemented, individuals may be tracked through a “constellation” of predictable label responses. Hence, a person’s unique taste in items may betray their location, movements, or identity.

V. ADDRESSING SECURITY ISSUES

RFID tags can not support the computing burden of the usual systems that are supported by significant computing resources at both ends of a communication link. There is a need for simple yet effective solutions. One of the primary vulnerabilities leading many of the problems outlined in section IV above is as a result of the insecure communication channel. Hence tags and readers need to provide a security service to achieve the security objective of confidentiality to overcome the vulnerabilities posed by eavesdroppers. The proposed Class II labels aim to address this issue, but cost effective solutions are not forth coming.

The term ‘confidentiality’ can be used to describe a mechanism to keep information from all but those that are authorized to see it [13]. In an RFID system the communicated information between a reader and a tag needs to be confidential when sensitive data such as secret keys or other such information, which must not be collected by an eavesdropper, is communicated between a reader and a tag. Currently there is no secure means of establishing a secure communication link between a tag and tamper proofing a tag has cost implications that will hinder the economics of low cost RFID technology.

The fact that tags and readers have no method of stating a claim to their legitimacy has lead to problems of cloning and counterfeiting. Addressing these issues require providing a security service to provide authentication.

The goal of an authentication scheme in RFID is to prevent an adversary from creating a clone of a tag to misrepresent the legitimate tag (and hence the authenticity of the object associated with the tag) by a carefully planned attack on the RFID system. In supply chain applications authenticating the tag will allow the prevention and detection of counterfeit goods.

A. *Notation*

It is appropriate to discuss a number of notational aspects to improve the clarity of the discussions below.

Encryption function performed using a key *K* will be indicated by the expression e_K(<*plaintext*>) while a decryption function using the same key will be given by d_K(<*ciphertext*>). If the pair of keys used are public and private they will be distinguished as $k_{private}$ and k_{public}. However a hash function operation on a string of plaintext using key *K* will in particular be expressed as $hash_K$(<*plaintext*>). However where a key stream is used, as the case with a stream cipher, a unique sequence of the key stream will be indicated using italic roman character such as *Ks*.

The exclusive or operator will be notated using the ‘$\oplus$’ symbol through out this paper while its usage in a sentence will be termed as XOR.

A random number or a nonce will be denoted by *RN* where there is a series of random numbers used it will be denoted as *RN1*, *RN2*, *RN3*, … , *RNn*, while the notation *RN(i)* will note the ith random number chosen or used. The CRC (cycling redundancy check) of a number will be noted by preceding the number with the string *CRC*. For instance the CRC of a random number *RN* will be denoted as *CRC_RN*.

B. *Related Work*

The following sections provides a familiarisation with various technologies and concepts discussed in the security proposals, and also highlight the significance of these in the context of low cost RFID.

C. *XOR operation*

The ‘exclusive or’ operation (XOR) is one operation that requires minimal hardware to implement. The XOR operator is both commutative and associative, and it satisfies the following properties outlined in TABLE 2 below for a Boolean variable identified by the symbol ‘A’. The XOR operation will be used extensively in the following security proposals.

TABLE 2
XOR PROPERTIES

$A \oplus A = 0$	$A \oplus \overline{A} = 1$	$A \oplus 0 = A$	$A \oplus 1 = \overline{A}$

D. *Physically Uncloneable Functions*

Attacks such as micro-probing, laser cutting, glitch attacks and power analysis attacks along with reverse engineering techniques used to reconstruct the layout of circuits have enabled adversaries to extract digital keys stored in the memory of integrated circuits. Security systems based on keeping a key a secret have thus been broken as a result. While various tamper-proofing methods [14] have been developed over the years to counter such physical attacks they are too extravagant for RFID applications.

Alternatives to storing keys on insecure hardware devices have been developed. Such an alternative is the introduction of physical one-way functions (POWFs) in [15] and [16]. The concept of using physical uncloneable functions (PUFs) is published in [17] and is a result of the early work on POWFs. Below is a general definition of a PUF.

Definition 1.2. A Physical Uncloneable Function (PUF) maps a set of challenge inputs to a set of responses utilizing some physical characteristic incorporated in an object. A PUF should also satisfy properties listed below.

Easy to compute: The time taken to generating the response set should be acceptable or be computable in polynomial time.

Difficult to model: The amount of information that can be obtained about the response to a randomly chosen challenge by an attacker without access to the physical device based on a polynomial number of measurements conducted previously using only a polynomial amount of resources, such as time, is negligible [16].

The ability to construct a PUF on silicon was outlined in [17] and [18]. A PUF structure that can be easily fabricated into an IC using standard CMOS fabrication processes has far reaching consequences. Below is a definition of a silicon physically uncloneable function.

Definition 1.2. A Silicon Physical Uncloneable Function (SPUF) is a PUF as identified in Definition 1.2 and also satisfies the following properties.

Inseparability: An SPUF is integrated and fabricated as part of an ASIC design such that any physical attack would lead to the destruction of the SPUF.

Secure communication: It is not possible to tamper with the measurement data from an SPUF.

The idea is based on using process variations, which are beyond a manufacturer's control, in wires and transistors on an IC to obtain a characteristic response from each IC when given a certain input [18].

The particular advantage in this technique lies in the fact that an adversary can not construct a model or a device to clone a PUF as there can be a number of possible challenge-response pairs, exponentially dependant on the number of challenges. Hence the system has computational security because a model based on an exhaustive search is impractical.

E. *Shrinking generator*

This generator is a more recent proposal that utilizes two LFSRs, *R1* of length L_1 and *R2* of length L_2 clocked in parallel. At any given transition of the clock the output of the generator is that of R1 given that the output of *R2* is a logical one. If *R2* output is a logical zero then nothing is output from the generator. Hence the output from *R1* is shrunk to produce an irregularly decimated subsequence [13] as shown in Fig. 6.

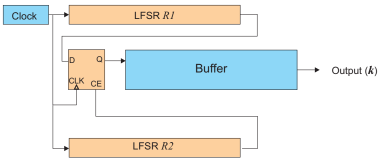

Fig. 6. Configuration of a shrinking generator.

An outline of the properties of the shrinking generator can be found in [13]. The security of the generator has survived many known attacks on LFSR based systems especially due to the very long period of the generator. The order of complexity of known attacks has exponential time complexity as they are a function of the length of both LFSRs. The complexities of known attacks are summarised in [13] and [19].

Nevertheless there have been a number of attempts at breaking the shrinking generator [20], [21], [22], [23], and more recently [24]. Despite all of the above attacks shrinking generators are still considered resistant against efficient cryptanalysis attacks due to the difficulty of the attack scenarios and the time order complexity of the attacking algorithms. It should however be stated here that for maximum security the following implementation consideration should be satisfied.

- Use secret connection polynomials that are not sparse
- Use maximum length LFSRs for *R1* and *R2*
- The lengths of LFSR should be such that gcd(L_1,L_2) = 1

One draw back of this generator is the irregular output from the generator but this may be solved by buffering the key stream prior to its use [25]. The probability of not having a byte of key stream data decreases exponentially with buffer size and the rate at which *R1* and *R2* are running with respect to the required throughput [25].

VI. Confidentiality and Authentication

The following sections will consider mechanisms for providing a service to deliver confidentiality and authentication to low cost RFID systems. This is a difficult task due to the relative ease with which an adversary can obtain an EPC from a low cost tag and the ease with which an eavesdropper can record or participate in a conversation between a tag and a reader. Achieving confidentiality involves creating a secure communication channel in an untrusted environment over an insecure channel. This is not a novel problem [13] but the solution space has little offerings for a resource intensive environment.

A. *Secure forward link*

Achieving a secure communication channel between a tag and an interrogator using a SPUF for the secure storage of a secret key and a stream cipher as a fast and efficient source of a key stream is discussed below.

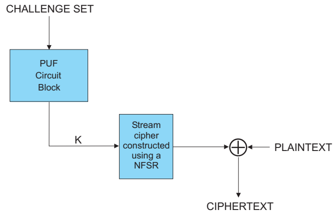

Fig. 7. Tag implementation of a stream cipher performing an encryption operation.

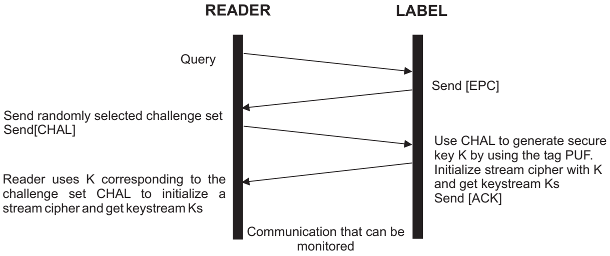
READER
LABEL
Query
Send [EPC]
Send randomly selected challenge set
Send[CHAL]
Use CHAL to generate secure key K by using the tag PUF. Initialize stream cipher with K and get keystream Ks
Send [ACK]
Reader uses K corresponding to the challenge set CHAL to initialize a stream cipher and get keystream Ks
Communication that can be monitored

Fig. 8. Communication protocol to achieve a secure communication channel between a reader and a tag.

The method assumes that an interrogator has uniquely identified the tag using its EPC and obtained a *CHAL* list (a series of bit strings forming a set of challenges) from a secure database corresponding to the tag EPC. The interrogator then initiates the establishment of a secure channel by signalling to the tag and once the tag acknowledges the interrogator's request, the interrogator transmits the *CHAL* list. The tag then uses the *CHAL* list to generate a key *K* which is used to initialize the stream cipher, thus obtaining a key stream *Ks* which can be used to encrypt the forward link as illustrated in Fig. 7. The interrogator is able to generate the same key stream for decryption as the reader can obtain the secret key *K* corresponding to the *CHAL* as the tag's PUF was characterised using the *CHAL* list prior to its deployment. An outlined of the communication protocol is given in Fig. 8.

B. Tag and Reader Authentication (Mutual Authentication)

The section above discussed a mechanism for achieving confidentiality by allowing the establishment of a secure channel. A simple extension to the communication protocol using the existing hardware required for achieving a secure channel can provide mutual authentication of a tag and a reader.

The mutual authentication algorithm is based on using the stream cipher as a means of generating a message authentication code. In the method outlined in Fig. 9 an interrogator initiates the authentication after the establishment of a secure communication channel. Once the tag acknowledges the request, the interrogator sends a randomly generated number *RN1* encrypted using a subsequence *Ks1* of the key stream *Ks* generated previously. A legitimate tag is able to obtain *RN1* and then use it to reinitialize the stream cipher. In order to make the scheme more efficient the tag uses the previously generated key stream bits *Ks1* and encrypts them with the key stream *Ks2* generated from the reinitialized stream cipher to generate the authentication code. The interrogator is then able to authenticate the tag since only a genuine tag could have been able to produce the key stream *Ka1* to produce *Ka2*.

If the tag is legitimate, the reader transmits an encrypted random number *RN2* to the tag. In the event the tag is not authentic the reader will pretend to complete the authentication by transmitting a nonce (number used only once) to the tags. Thus an adversary who does not have access to the reader output has no indication of whether the authentication attempt was successful.

The tag then reinitializes the stream cipher using *RN2* and sends an acknowledgement to the reader. The reader then uses the previously generated *Ka2* and encrypts it with the key stream *Ka3* generated from the reinitialized stream cipher to create the authentication code.

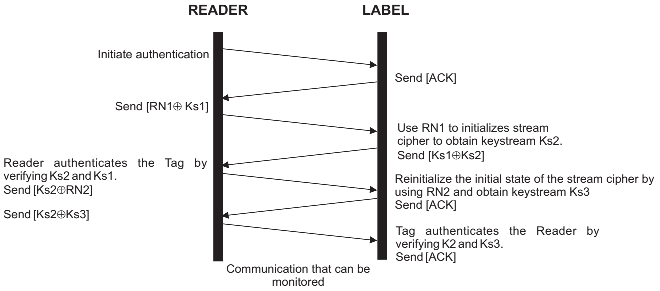
READER
LABEL
Initiate authentication
Send [ACK]
Send [RN1⊕ Ks1]
Use RN1 to initializes stream cipher to obtain keystream Ks2.
Send [Ks1⊕Ks2]
Reader authenticates the Tag by verifying Ks2 and Ks1.
Send [Ks2⊕RN2]
Reinitialize the initial state of the stream cipher by using RN2 and obtain keystream Ks3
Send [ACK]
Send [Ks2⊕Ks3]
Tag authenticates the Reader by verifying K2 and Ks3.
Send [ACK]
Communication that can be monitored

Fig. 9. Protocol for mutual authentication after establishing a secure communication channel.

C. Practical Issues

The first instance use of NLFSR is in the form of a synchronous stream cipher as the key stream is generated by initializing the NLFSR with the response from the PUF and thus has the advantage that a single bit error will only cause a single bit of the plaintext to be corrupted after decryption. However, subsequent use of RNs transmitted from the tag to initialize the stream cipher may cause a failure in the authentication process due to undetected errors in the transmission from the reader.

There is the added overhead of requesting and obtaining the *CHAL* list from a secure database and transmitting the challenges to the RFID IC and. This could be avoided by storing the *CHAL* set on the tag, since a physical attack to discover the *CHAL* list can not reveal the responses of a SPUF circuit on an IC. The tags prior to their deployment also require being subjected to an identification phase.

Identification phase: The SPUF is subjected to a *CHAL* set and the responses, *RES* are measured. Then the CRP (challenge-response) set [EPC, *CHAL*, *RES*] is stored in a secure CRP database, indexed by the EPC. It may also be necessary to store a fourth data item, *A* containing redundant information based on the measured *RES* in the CRP database as well as the tag's memory to aid the tag to distil the correct response to a *CHAL* as noise can effect the accuracy of the *RES* measurements on a tag.

D. Possible Attacks

The security of the above system relies on a PUF to securely store a unique secret key in the form of delay variations. The PUF based security systems are susceptible to reliability issues; however this is still an active area of research [18]. The most probable attacks on a PUF based challenge response system are outlined in [10]. 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.

The mutual authentication mechanism is vulnerable to a replay attack (or a session hijacking) by a third party able to record a complete communication between a legitimate tag and an authorised reader. Such an attack may be used to fool a tag to accept that an unauthorised reader is indeed an authorised reader. However, without the knowledge of the key stream such an authentication to a tag is of little use, since the tag expects encrypted data and write access to tags are protected by an access password [3].

VII. Conclusion

The PUF provides a cost effective solution to low cost RFID Systems. This security engine can be easily constructed using standard digital gates and layout tools and fabricated using standard CMOS technology. A 64-stage PUF circuit costs less than 1000 gates. Additionally, various kinds of low power techniques such as sub-threshold logic design and multi-threshold CMOS design can be utilized to reduce the power consumption to make it suitable for use in devices sensitive to low power consumption.

Future work will focus on elaborating the protocols used and investigating the possibility of designing commands and responses based on the current C1G2 protocol ratified by EPCglobal. It is also left to analyse the hardware and time complexity of the schemes outlined above to evaluate their performance and their cost. Performance evaluations will deal with issues related to the large amounts of data that needs to be transmitted to the tag and from the tag, and the time taken in memory storage and retrieval will also need to be investigated.

Acknowledgment

The authors would like to thank Alf Grasso for his help in improving the clarity of this work and Braden Phillips for his many inputs and my dear colleague Raja Gohosal for all his support.

References

[1] K. Finkenzeller, *RFID Handbook: Radio Frequency Identification Fundamentals and Applications*. John Wiley & Sons, New York, 1999.

[2] EPCglobal Inc. home page, http://www.epcglobalinc.org.

[3] EPCglobal Inc., Specification for RFID air interface, http://www.epcglobalinc.org/standards_technology/EPCglobal2UHFRFIDProtocolV109122005

[4] D. C Ranasinghe, K. Seong, M. Leng, D. W. Engels, and P. H. Cole, “A Distributed Architecture for a Ubiquitous Item Identification Network”, *Smart Object Systems Workshop*, Japan, September 2005.

[5] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin and M. Szydlo, “Security analysis of a cryptographically-enabled RFID Device”, *Proceedings of 14th USENIX Secuirty Symposium*, pp. 1-16.

[6] J. Westhues. “Hacking the prox card”, *RFID: Applications, Security and Privacy,* Addison-Wesley, 2005, pp. 291-300.

[7] Y. Oren, and A. Shamir, “Power analysis of RFID Tags”, unpublished, accessed on March 2006, http://www.wisdom.weizmann.ac.il/~yossio/rfid/.

[8] G. Avoine and P.Oeschlin, “RFID Traceability: A Multilayer Problem”, *Financial Cryptography*, 2005.

[9] Weigart, S.H., “Physical security devices for computer subsystems: A Survey of Attacks and Defences”. *Workshop on Cryptographic Hardware and Embedded Systems, LNCS*, vol. 1965, pages 302-317.

[10] Andreson, R, and Kuhn, M., “Low cost attacks on tamper resistant devices”, *International Workshop on Security Protocols, LNCS*, 1997.

[11] E Bovenlander, invited talk on smartcard security, *Eurocrypt 97*, 1997.

[12] D. C. Ranasinghe, P.H. Cole “A perspective on fixing security and privacy holes in low cost RFID”, *Auto-ID Labs Anti-counterfeiting paper series*, June 2006.

[13] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[14] O. Kommerling and M.G. Kuhn, “Design principles for tamper-resistance smartcard processors”, *proc. of USENIX Workshop Smartcard Technology*, 1999, pp. 9-20.

[15] P. S. Ravikanth “Physical one-way functions”, Ph.D dissertation, Department of Media and Art Science, Massachusetts Institute of Technology, Cambridge, 2001.

[16] R. Pappu, B. Recht, J. Taylor, and N Gershen-Feld, “Physical one-way functions,” *Science*, vol. 297, pp. 2026-2030, 2002.

[17] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, “Silicon physical random functions”, *proc. of computer communications security conf.*, Nov. 2002. pp. 148-160.

[18] D. Lim, J. W. Lee, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas, “Extracting Secret Keys from Integrated Circuits”, *IEEE Transactions on VLSI Sytems*, vol. 13, No. 10, 2005.

[19] Coppersmith, H. Krawczyk, and Y. Mansour, “The shrinking generator”, D.R. Stinson, editor, *Advances in Crytplogy – Crypto ’93*, pp 22-39, Springer-Verlag, New York, 1994.

[20] L. Simpson, J.D. Golic, and E. Dawson, “A probabilistic correlation attack on the shrinking generator,” *Proc. ACISP ’98*, *LNCS* vol. 1438, pp. 147-158, Springer Verlat, 1998.

[21] J. D. Golic and L. O’Connor, “A cryptanalysis of clock-controlled shift registers with multiple steps”, *Cryptography: Policy and Algorithms*, pp.174-184, 1995.

[22] T. Johansson, “Reduces complexity correlation attacks on two clock-controlled generators,” *Proc. Asiacrypt’98, LNCS*, vol 1541, pp. 342-356, Springer-Verlag, 1998.

[23] P. Ekdahl, W. Meier, and T. Johansson, “Predicting the shrinking generator with fixed connections,” *proc. Eurocrypt’03, LNCS*, vol. 2656, pp. 345-359, Springer Verlag, 2004.

[24] P. Caballero-Gil, and A. Fuster-Sabater, “Using linear hybrid cellular automata to attack the shrinking generator”, *IEICE Trans. Fundamentals*, vol. E90-A, no. 5, pp. 1166-1172, May 2006.

[25] I. Kessler, and H. Krawczyk, “Buffer length and clock rate for the shrinking generator”, *IBM Research Report*, RC 19938 (88322), 1995.

[26] D. Ranasinghe, D. W. Engels, P. H. Cole, “Security and Privacy Solutions for Low Cost RFID Systems”, *Proc. of the 2004 Intelligent Sensors, Sensor Networks & Information Processing Conference*, Melbourne, Australia. pp. 337-342, 14-17 December, 2004.

[27] D. C. Ranasinghe, D. Lim, S. Devadas, and P.H. Cole “A low cost solution to authentication in passive RFID technology”, *Auto-ID Labs Anti-counterfeiting paper series*, June 2006.