The University of Adelaide

AUTO–ID LABS

A Low Cost Solution to Authentication in Passive RFID Systems

Damith C. Ranasinghe, Daihyun Lim, Peter H. Cole and Srinivas Devadas

Auto-ID Labs White Paper WP-HARDWARE-029

Mr. Damith C. Ranasinghe
PhD Student, Auto-ID Lab, ADELAIDE
School of Electrical and Electronics Engineering,
The University of Adelaide

Prof. Peter H. Cole
Research Director, Auto-ID Lab, ADELAIDE
School of Electrical and Electronics Engineering,
The University of Adelaide

Contact:

E-Mail: damith@eleceng.adelaide.edu.au, daihyn@mit.edu, cole@eleceng.adelaide.edu.au, or srinivasd@mit.edu.au

Internet: www.autoidlabs.org

Hardware

Abstract

This paper aims to propose a solution to address the issue of authentication to prevent counterfeiting in a low cost RFID based system based on using Physically Uncloneable Functions.

1. Introduction

In the implementation of Radio Frequency Identification (RFID) systems concerns have been raised regarding security and violations of end-user privacy. Those concerns may be alleviated using cryptographic primitives.

Despite the vast array of RFID systems, those that are at the low cost end pose the greatest threat to security and privacy due to the possibility of wide scale deployment and inherent constraints that place severe limitations on the number of possible solutions.

There is a large collection of literature available on efficient and inexpensive cryptographic engines suitable for smart card applications, but the use of such engines is an extravagant solution for low cost RFID systems that are beginning to proliferate within global supply chains.

A primary concern with current low cost RFID systems is a cloning attack. The following sections will examine the vulnerabilities of low cost RFID systems to cloning attacks and the consequences of such an attack. A simple means of addressing this issue is to implement a security service on the tag that can achieve the security objective of authentication. The issues are elaborated below.

1.1. Cloning

Cloning genuine RFID tags to impersonate tags (imitating the behaviour of a genuine tag) presents a serious threat to an RFID system. Using cloning attacks to impersonate tags will add a new dimension to thieving as attackers are able to write EPC data onto devices that function like RFID tags.

A direct consequence of cloning is 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. The ‘track and trace’ concept outlined in [1] is one possible solution to detecting such a counterfeited product in a supply chain application.

At the time of writing there is no mechanism for a reader to verify that it is communicating with a genuine RFID label and not a fraudulent label. Thus a thief may replace a tag of a valid item with a fake tag or replace the tag of an expensive item with that of a fake tag with data obtained from a cheaper item. Hence the lack of a means for authentication allows an adversary to fool a security system into perceiving that the item is still present or this may

fool automated checkout counters into charging for a cheaper item. Such fake labels may also be used to create imitation items.

Since there is presently no mechanism for a reader to authenticate itself to a label or a label to authenticate itself to a reader, labels and readers are constantly in an un-trusted environment where the integrity of messages is doubtful and there are no means for establishing the legitimacy of a reader by a label or the legitimacy of a label by a reader.

Clearly more expensive RFID system implementations are also not immune from cloning as shown by a more recent cloning attack published in [2] where a cloned tag was used in the purchase of fuel at a service station and to start an automobile locked with a RFID based car immobiliser. A similar example of cloning of proximity cards is given in [3] while the possibility of cloning the VeriChip [4] in a discussion of its possible use to tag employees was outlined in [5].

1.2. Authentication

In an RFID context authentication simplifies to the corroboration of the identity of a tag or a reader. Authentication is an important RFID security measure for preventing counterfeit manufacture or substitution by cloning authentic RFID labels. 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 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. There are a number of possible ways in which a low cost RFID system may be attacked to obtain the necessary information to clone a tag. Present systems based on Class I and Class II tags, passive eavesdropping or a scan of an RFID tag is enough to carry out a cloning attack [6].

1.3. Challenge-and-Response Protocol

Practically all identification schemes or authentication schemes use a challenge and response protocol as illustrated in Fig. 1. Other identification schemes such as the Schnorr Identification Scheme [7] and the Okamoto Identification Scheme [8] are examples of more complex challenge and response mechanisms. The mechanism for authentication using challenge and response is described below [9].

In the context of an RFID system, where there is no secure channel for communication, the security of the mechanism relies on the secure storage of the key k and the inability of an adversary to compute the key k given both the ciphertext and plaintext.

1. Reader choses a challenge, x, which is a random number and transmits it to the reader.
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 know only to the reader and the particular label).
3. The reader then computes $y' = e_K(x)$.
4. Then the reader verifies that $y' = y$.

Fig. 1: Challenge-response protocol.

1.4. Constructing a Challenge-and-Response Protocol

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 suitable candidates. However, in terms of silicon they present expensive solutions, while at the same time the security provided by such schemes remains vulnerable to various invasive and non-invasive physical attacks [10].

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 have been developed over the years to counter such physical attacks they might be considered to be an extravagant solution for RFID applications. Such an example is the tamper sensing technology [10]. Using a sensor based on additional metallization layers allows interruptions and short circuits to be detected in the event of an attempt to tamper with the IC. However, such sensors only work while the IC is powered and such a sensor technology can only cause a degree of difficulty to an adversary attempting to obtain the key while the IC is powered as the key can still be extracted when the IC is powered off.

Alternatives to storing keys on insecure hardware devices have been developed. Such an alternative is the introduction of physical one-way functions (POWFs) in [11] and [12]. The solution presented used a laser beam as an input to a transparent optical medium with 3D microstructure and the output was a quantification of the resulting interference pattern. The resultant output is dependent on the frequency and the angle of the laser beam entering the optical medium and the optical characteristics of the medium.

The concept of using physical unclonable functions (PUFs) was published in [13] and [14]. The ability to construct a PUF on silicon has far reaching implications since such a design can be easily fabricated into an IC using standard CMOS fabrication processes. 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. The PUF circuit is able to uniquely characterise each IC due to manufacturing variations [13]. 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. The observation of PUF results reveals that a string of challenge bit sequences can be used to generate a response string unique to each IC.

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 computations security because a model based on an exhaustive search is impractical. However, the PUF based structure in [13] is sensitive to noise, especially thermal noise, as wire latencies and gate delays depend on operating temperature of the device. This leads to reliability issues when trying to obtain consistent responses for a given challenge.

Unreliability due to such environmental variations have been addressed in a PUF configuration given in [15], where a challenge response pair is created using a PUF circuit that exploit process variation in the silicon fabrication using a differential topology, using only 100s of gates. The design of such a PUF is considered in the following section.

1.5. Physical Unclonable Functions

A secret key extraction technique from the manufacturing variation in ICs [15] provides a suitable solution to create a low cost security engine on an RFID label that is both cost effective and can guard against tampering to extract secret keys stored on the tag to create clones. The technique employs a PUF (Physically Unclonable Function) circuit which has the number of delay path configurations exponentially dependent on challenge input.

1.5.1. Circuit Implementation

The block diagram in Fig. 2 depicts the structure of a PUF circuit which is based on the arbiter-based PUF in [15 and 16]. The circuit accepts a n bit challenge $b_0, b_2, b_3, \ldots, b_n$ to form two delay paths in 2^n different configurations. In order to generate a response bit, two delay paths are excited simultaneously to allow the transitions to race against each other. The arbiter block at the end of the delay paths determines which rising edge arrives first and sets its output to 0 or 1. The actual implementation of arbiter-based PUFs in [15 and 16] uses 64 bit challenges. The details of the switch component are given in Fig. 3.

The switch component indicated in Fig. 2 is implemented using a pair of two-to-one multiplexers (refer to Fig. 3). Depending on the select bit C_i, the switch either allows the signal to travel straight through or swap the delay paths. The arbiter is constructed using a simple transparent latch with an active-low enable input. The arbiter favours the path to output zero since it is preset to zero and requires a setup time constraint to switch to a logic one. Fixing a small number of most significant challenge bits can compensate for this skew by effectively lengthen one delay path. The layout was carefully done to ensure that both paths are symmetrical and arbiter responses are not biased to 0 or 1.

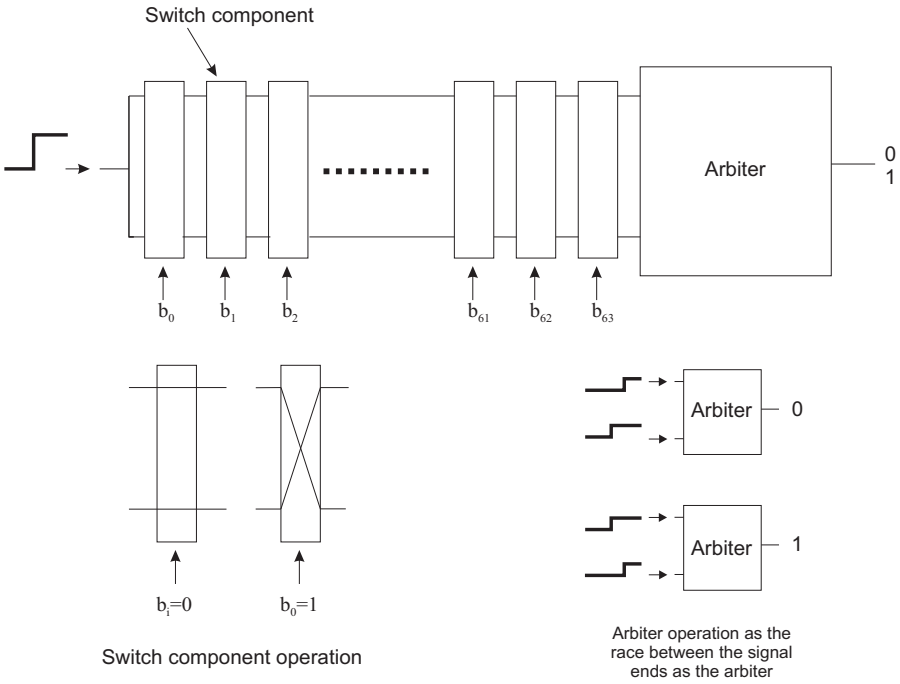

Fig. 2: Arbiter-based PUF circuit implementation.

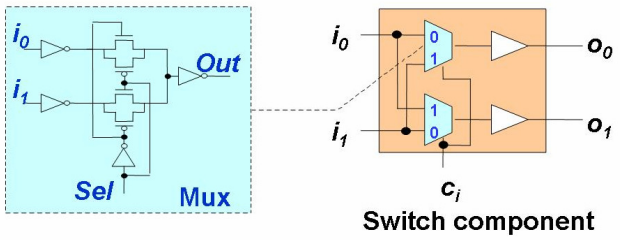

Fig. 3: Switch component implemented using two-to-one multiplexers to swap two delay paths [15].

The chip used in testing was built in TSMC's 0.18 µm, single poly, 6-level metal process with standard cells [16]. The chip contains eight sets of the arbiter-based PUF circuits capable of generating an 8 bit response for a given challenge and a JTAG-like serial interface for communication. The total area of the eight PUF circuits is 1212 µm x 1212 µm and the chip can be operated 100 MHz [15 and 16].

1.5.2. Design Analysis

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. It is estimated in [17] that there is a strong enough variation between chip to chip fabricated from the same silicon wafer 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 [17]. It has been estimated that about 800 challenge response pairs are sufficient to distinguish 10^9 chips with the probability $p \sim 1 - 5\times10^{10}$ [17]. Such an identification scheme can be implemented with less than 1000 gates on an RFID silicon design

The input and output functions of the generator are responsible for most of the power consumption in the PUF and the power consumption of the generator core is relatively small. The total power consumption of a PUF circuit is about 130 µW in our implementation. This is largely because of the external circuits used for feeding input values to the PUF and obtaining results from the PUF, nevertheless it is relatively a small value.

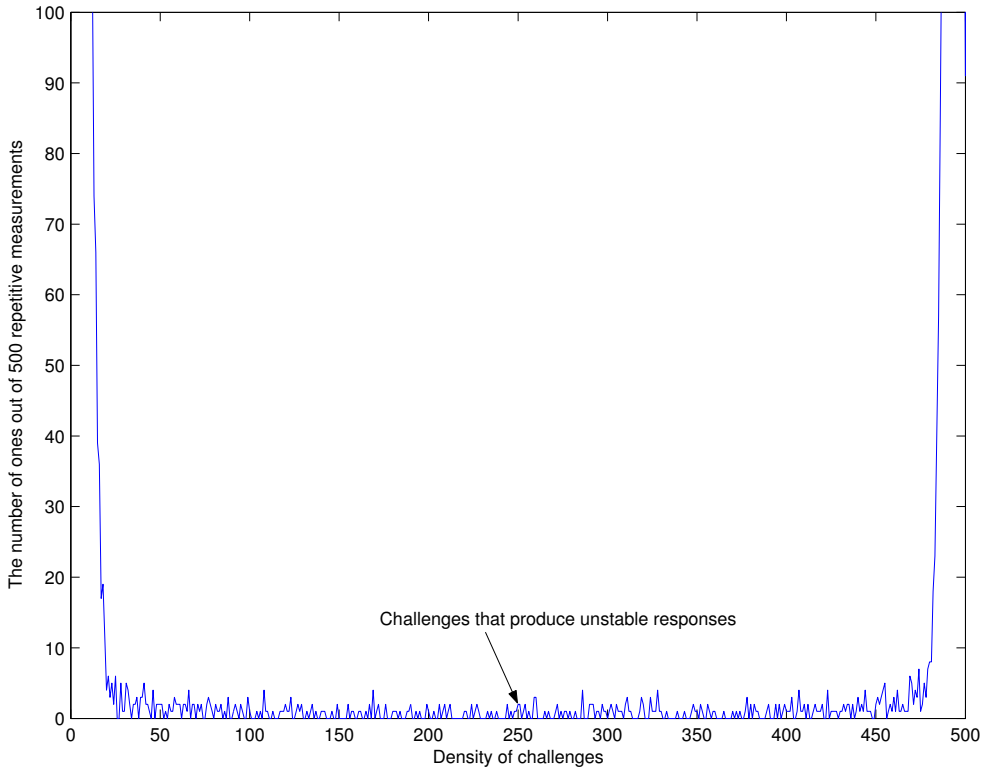

Fig. 4: The density function of the random variable* k*, where* k *is the number of 1's out of 500 repetitive measurements.

1.5.3. Increasing the Dynamic Range of Operation

However, the responses from a PUF are sensitive to environmental conditions such as temperature and power supply voltage. That is a challenge that generates a reliable responses may not generate a reliable responses if environmental conditions change beyond a tolerance level. This issue is highlighted in Fig. 4 where results of 500 repetitive measurements of 1000 challenges are shown. The design in Fig. 2 presented in [15], is used to mitigate the effects of environmental noise based on the fact that noise would affect both signal propagations paths in an identical manner and thus the final results of the circuit are unchanged.

The generator is sensitive to the power supply voltage and the temperature of the surrounding environment [15]. However problems caused by operational voltage changes can be minimised by the fabrication of a voltage regulator on the PUF.

1.5.4. Possible Attacks

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 as discussed in Section 1.5.2 and 1.5.3 of this paper; however this is still an active area of research. The most probable attacks on a PUF based challenge response system are outlined in [15].

The security of the systems based on PUFs will 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.

2. Application to RFID Authentication

2.1. A Low Cost Tag

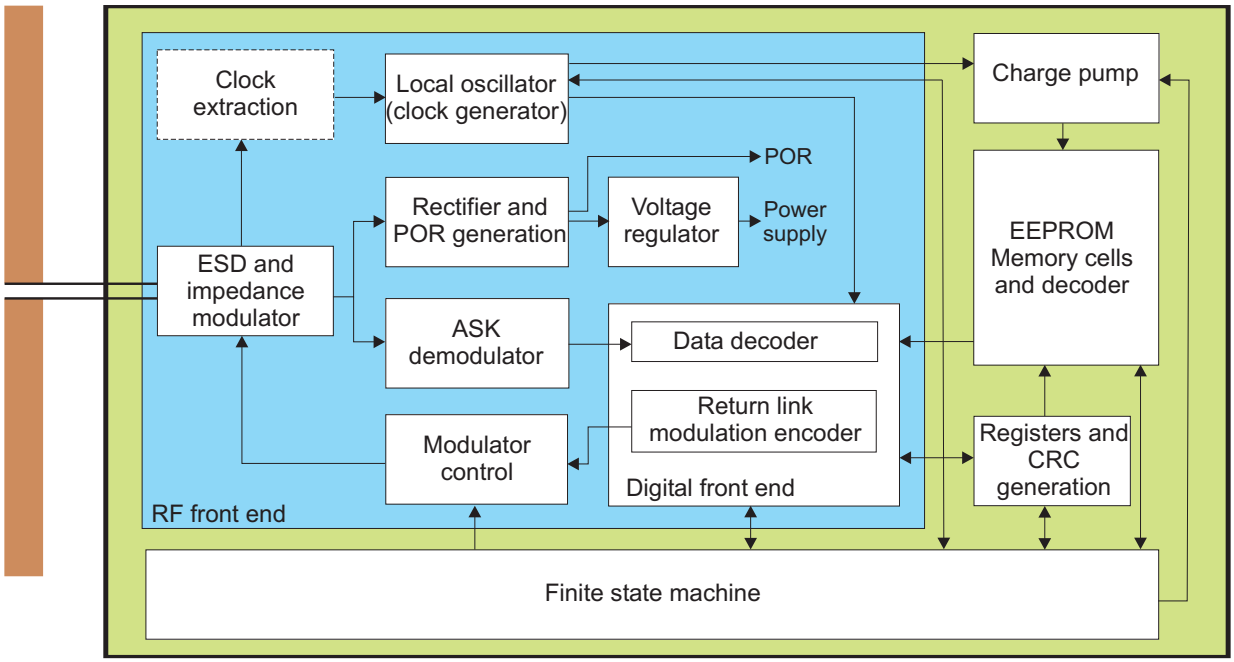

Fig. 5: Block diagram of a passive UHF/HF RFID label.

Fig. 5 is simplified block diagram of a passive RFID label, with the distinction between UHF and HF being the fact the in a HF system the local clock is generated by dividing down the CW frequency while for an UHF chip such a division is not possible and thus a low power local oscillator is used. Current fabrications of Class I labels consist of around 1000 to 4000 logic gates while Class II labels may have several thousand more gates. An RFID microcircuit can be subdivided into three primary sections: RF front-end, Memory circuitry, and Finite State machine (label logic circuitry). Figure 5 is an illustration of a typical low cost RFID transponder (that is a passive label). The block diagram of a HF chip and a UHF chip varies little in that the primary difference being the way in which the local oscillator clock is derived. In a UHF chip there is a dedicated low power oscillator, while in a HF chip the clock signal is derived from the received carrier by dividing down the carrier (at 13.56 MHz) in steps.

2.1.1. RF Front-end

RF front-end consists of antenna pads for attaching the terminal of the antenna to the label IC. The antenna input passes through circuits for ESD (electrostatic discharge) protection. The ASK (Amplitude Shift Keying) demodulation circuits extract the modulation dips from the received signal while the Rectifier, rectifies the received signal to generate power which must be regulated using a voltage regulator to avoid voltage surges due to variations in RF field intensities.

Passive RFID chips consist of a relatively large capacitor following a rectifier for storing charge to power the circuit in the absence of a battery. It is important to note here that the capacitor occupies a relatively large portion of the silicon area and RFID chips consuming larger amounts of power will need higher capacity capacitors and thus will cost more.

2.1.2. Memory Circuitry

The IC has memory capacity in the order of hundreds of bits. Class 1 labels have only read only memory while Class II labels may have some read-write memory. Read write memory, at the time of writing is implemented using EEPROM and thus requires a large voltage before information can be written to memory. Thus a charge pump, consisting of a series of capacitors is required to achieve a voltage of about 17V for writing to the tag's memory.

The CRC circuits are used in the validating the CRC in the received data and commands from an interrogator. The CRC generation unit is also used in the computation of the CRC for data sent from the tag to an interrogator before being encoded for modulation by the Return link modulation encoder.

In the implementation of an EPC tag the EEPROM will store the EPC number of the tag, and the rest of the memory (generally of the order of a few kilobytes) is available to the users.

2.1.3. Finite State Machine (Logic Circuitry)

The logic on board the chip will define the label functionality. Primarily, chip logic will execute reader commands and implement an anti-collision scheme that allows the reading of multiple labels by a reader. These logic circuits are highly specialised and optimised for their tasks.

Furthermore, the logic circuits also control read and write access to the EEPROM memory circuits.

2.2. Challenging Aspects of implementing Authentication on Low Cost Tags

There are a variety of reasons behind the difficulties faced by scientists in implementing existing authentication mechanism on RFID system other than that of tags being insecure environments for long term secret key storage following from the discussion in section 1.4 of this paper. The issue has been addressed in publications such as [18]. Perhaps the most important of all the issues considered and the most relevant to the current discussion on using PUF circuits for authentication is to also consider the fact that the communication between and tag and a reader is constantly exposed to eavesdropping. The aspects of eavesdropping and other vulnerabilities have been dealt with great detail in [6]. This problem is further highlighted by the fact that the current air interface protocol ratified by EPCglobal for Class I tags (C1G2) [18] has provision for establishing a secure communication layer, and it is left up to RFID IC developers to implement such, as perhaps a proprietary solution.

2.3. PUF based RFID IC

The idea of using a PUF in a low cost RFID label was first published in [20]. There are varieties of ways in which such a secret key extraction technique can be incorporated on to a low cost label due to the security it provides to the long term storage of secure keys on a RFID label. The following sections discuss two such schemes proposed.

2.4. Tag Authentication

Fig. 6 depicts a model of an RFID chip with an integrated PUF circuit while Fig. 7 illustrates the use of a PUF based RFID system. The discussion below using PUF security engines will assume using 800 challenge-response pairs as a sufficient number of challenges in a single set, as discussed in Section 1.5.2 of this paper.

Building a symmetric key engine is still not a cost effective solution though certain advances have been made towards the development of hardware optimized encryptions engines in [21, 22] and [23], they still present a performance hindrance to current RFID systems. Hence instead of using the PUF to obtain a secret key, PUF can be directly utilized as illustrated in Fig. 7 and Fig. 8.

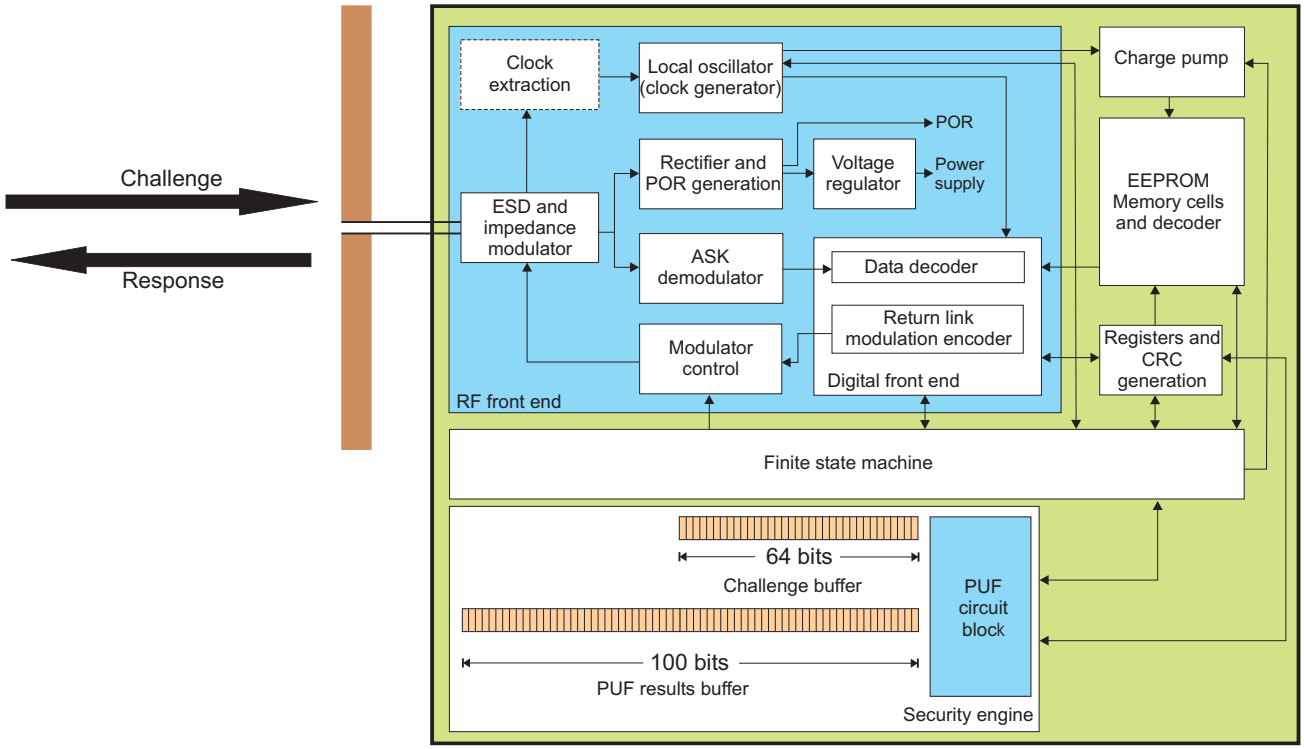

Fig. 6: A PUF based RFID Chip.

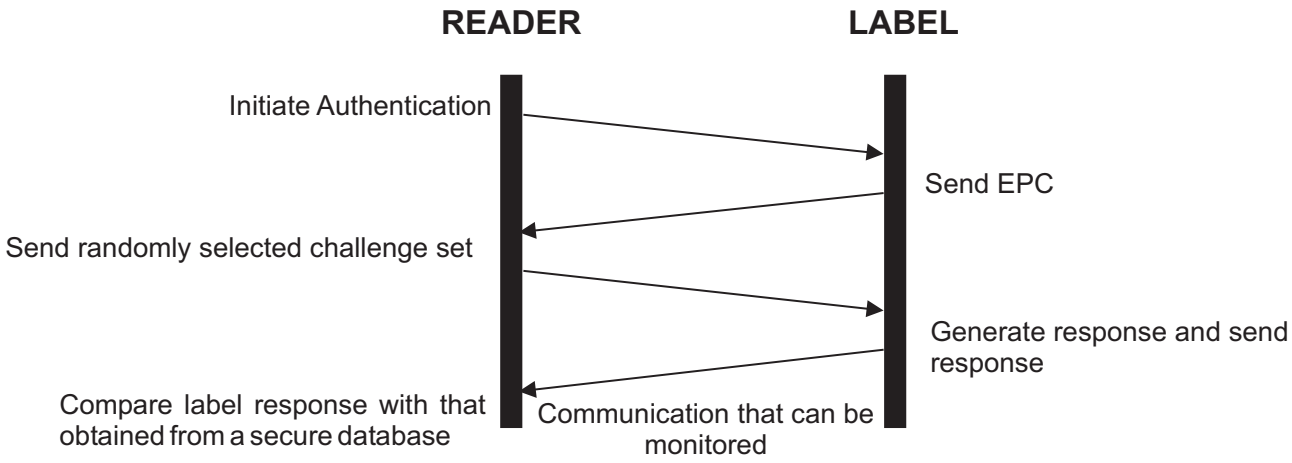

Fig. 7: Message exchange between a reader and an RFID label during an authentication process.

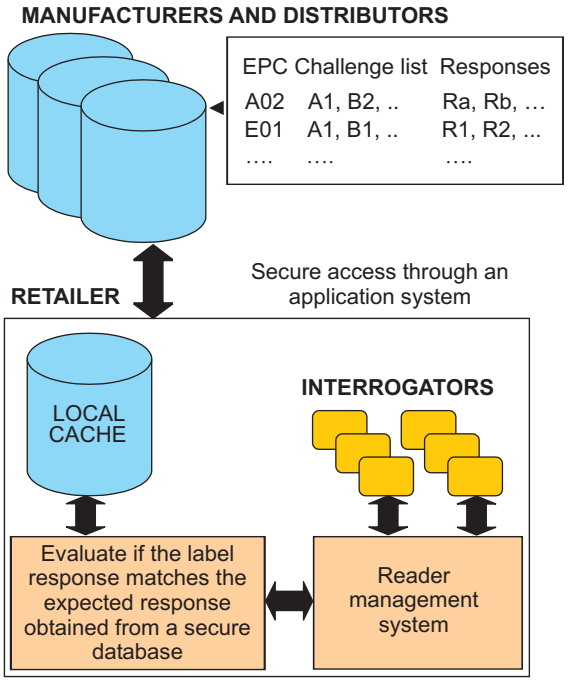

Fig. 8: An overview of an implementation of a PUF based RFID system

It is clear that once a challenge has been used it cannot be used again since an adversary may have observed it. 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. Then there remains the question of delivering a secure communication channel between a reader and the tag. A possible for obtaining such a communication layer encryption scheme is proposed in [20].

However, not all the challenges need to be discarded. A simple alternative to mechanism discussed above requires the reader to randomly alter the order in which challenges are given along with a tag's security engine storing the 800 bit long response and xoring blocks of the response string will allow the challenges to be reused. Thus a third party observing the communication between a tag and reader is unable to formulate the correct challenge response pairs. This random organisation of the challenge string will allow the challenges to be reused even over an insecure communication channel as illustrated in Fig. 9.

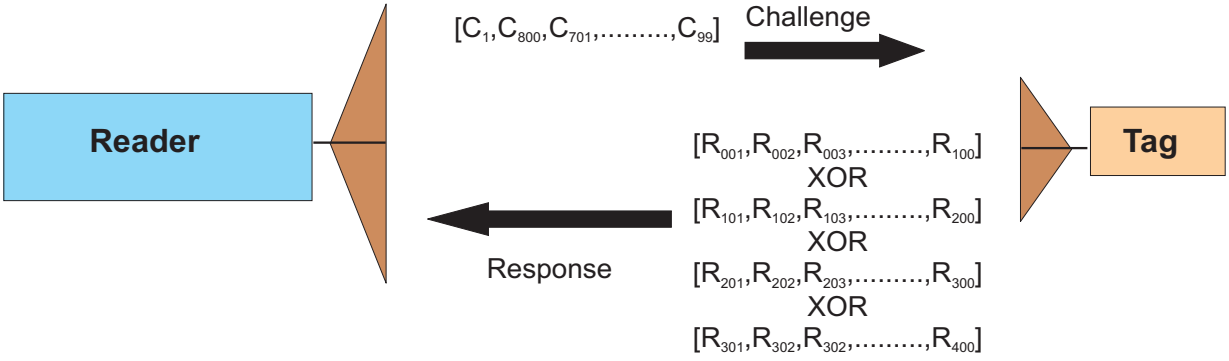

Fig. 9: Using randomised challenges and XORed responses to allow the re-use of challenges.

The above scheme will allow a label to authenticate itself to a reader before any sensitive information passes between the devices, but the fact remains that a reader still needs to identify a tag by requesting its unique identifier (such as the EPC in case of Class I tag implemented using the C1G2 protocol). The scheme also implies that the RFID tags be characterised with a number of challenge response sets. Thus in a supply chain environment a manufacture might have to perform individual tag characterisations using randomly selected challenges in a secure environment such as a Faraday's cage.

2.5. Tag and Reader Authentication (Mutual Authentication)

It is possible to extend the above scheme to enable a tag to authenticate a reader and for a reader to authenticate a tag. This involves sending a select challenge set for which a tag generates a response string. The reply string will uniquely identify the tag, hence the reply can be used to access data related to a tag using a hash table (which will reduce the cost of searching for the response related data, hash tables generally use a hash function such as MD5 [9] and a important characteristic of the function must be that it is collision free). This scheme requires that the tag stores a temporary secret key ***RN*** and ***K*** (refer to Fig. 10) for encryption and that the reader has access to the hash table entries stored on a secure database. The message exchange protocol is outlined in Fig. 11.

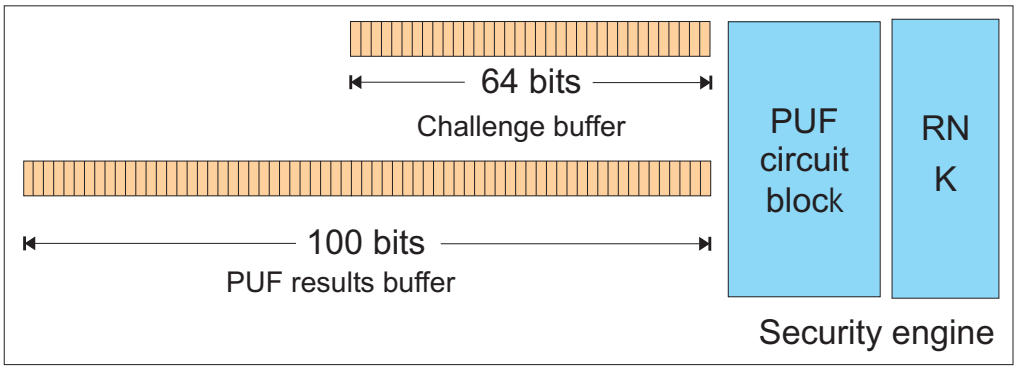

Fig. 10: RFID label with a PUF and extra memory to store secret key **RN.**

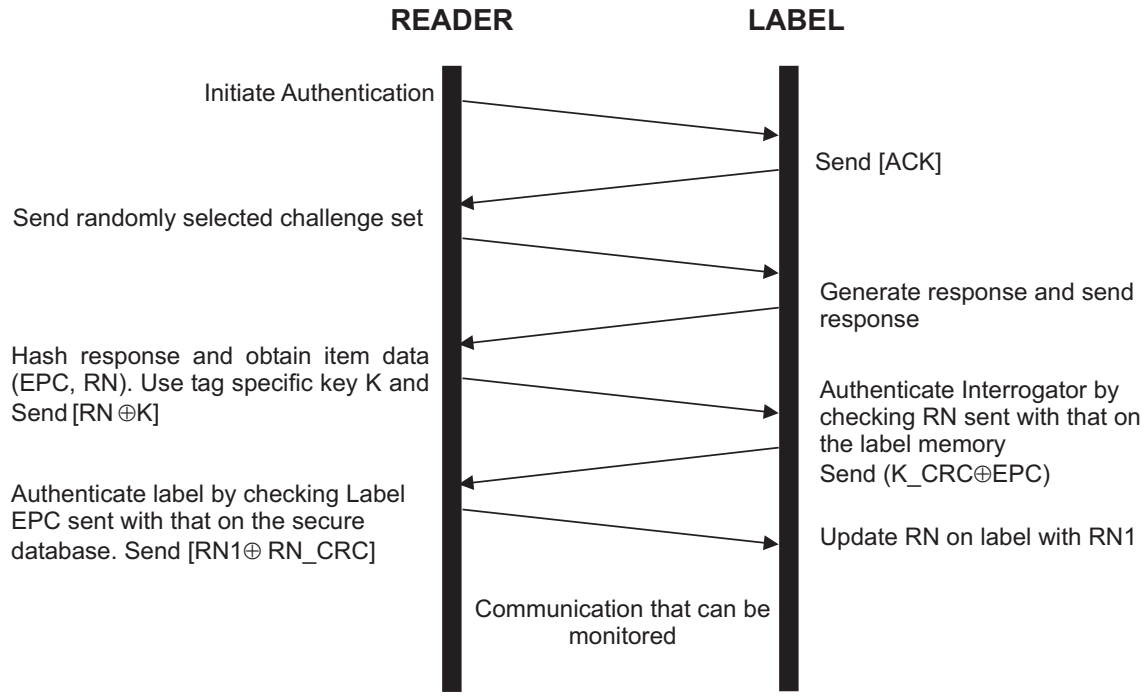

Fig. 11: Protocol for a non identifying label.

The above scheme has the particular advantage that the an RFID label do not need to reveal its unique identifier, such as an EPC, and hence a third party is unable to obtain any useful information pointed to by the unique identifier, such as any information about the object to which the item is attached.

3. 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-thresholds CMOS design can be utilized to reduce the power consumption to make it suitable for use in devices sensitive to low power consumption.

The effects of environmental conditions on the measurements obtained from a PUF are documented in [20], and the symmetrical nature of the circuit counter acts to reduce much of the variation provided otherwise

However, effects of power supply voltage still need to be investigated to discover practical performance boundaries such that the PUF can operate reliably. Nevertheless it is possible to fabricate a voltage regulator onboard the PUF to prevent effects from higher voltage variations, but it will not be able to counteract conditions induced by voltages below a calibrated power supply voltage.

Future work will also involve the investigations into the effects of voltage on the performance of the PUF. It is also left to investigate whether the generator throughput can be improved to reduce the time take for the execution of a challenge response protocol.

Future work should also focus on elaborating the protocols used and investigating the possibility of designing commands and responses based on the current C1G2 protocol ratified by EPCglobal while at the same time performance 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 to further analyse performance issues related to using a PUF security engine on current Class I or Class II tags.

References

[1] D. C. Ranasinghe, K. S. Leong, M. L. Ng, D. W. Engels, P. H. Cole (2005): A distributed architecture for a ubiquitous item identification network in: Seventh International Conference on Ubiquitous computing, Tokyo, Japan, Sept 2005.

[2] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin and M. Szydlo (2005): “Security analysis of a cryptographically-enabled RFID Device”, Proceedings of 14th USENIX Security Symposium, pp 1-16.

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

[4] Verichip corporation home page, accessed June 2006. http://www.4verichip.com/.

[5] K. Albrecht (2006): Chipping workers poses huge security risks in: Freemarketnews, accessed February 2006, http://www.freemarketnews.com/Analysis/139/3812/2006-02-15.asp?wid=139&nid=3812.

[6] D. C. Ranasinghe and P.H. Cole (2006): Security of Low Cost RFID perspective on fixing security and privacy holes in low cost RFID, in: submission to Auto-ID Labs white paper series, June 2006.

[7] Schnorr, C. P (1991): Efficient signature generation by smart cards in: Journal of Cryptology, vol 4, pg 161-174, 1991.

[8] Okamoto, T(1993): Provably secure and practical identification schemes and corresponding signature schemes in: Lecture Notes in Computer Science, vol 196, 1993.

[9] Menezes, P. van Oorschot and S. Vanstone (1996): Handbook of Applied Cryptography, CRC Press, 1996.

[10] O. Kommerling and M.G. Kuhn (1999): Design principles for tamper-resistance smartcard processors in proceedings of USENIX Workshop Smartcard Technology, 1999, pp. 9-20.

[11] P. S. Ravikanth (2001): Physical one-way functions in PhD dissertation, Department of Media and Art Science, Massachusetts Institute of Technology, Cambridge, 2001.

[12] R. Pappu, B. Recht, J. Taylor, and N Gershen-Feld (2002): Physical one-way functions in Science, vol. 297, pp. 2026-2030, 2002.

[13] B. Gassend (2003): Physical random functions in M.S. thesis, Department of Electrical Engineering Computer Science, Massachusetts Institute of Technology, Cambridge, Jan. 2003.

[14] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas (2002): Silicon physical random functions in Proceedings of Computer Communications Security Conf. Nov. 2002. pp. 148-160.

[15] D. Lim (2004): Extracting Secret Keys from Integrated Circuits in Master thesis, Massachusetts Institute of Technology, May 2004.

[16] D. Lim, J. W. Lee, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas (2005): Extracting Secret Keys from Integrated Circuits in IEEE Transactions on VLSI Systems, vol. 13, No. 10, 2005.

[17] J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas (2004): A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications in 2004 Symposium on VLSI circuits, pp 176-179, 2004.

[18] D. C. Ranasinghe, D. W. Engels and P. H. Cole (2005): Low cost RFID systems: confronting security and privacy in Auto-ID Labs White Paper Journal Volume 1, Sept 2005.

[19] EPCglobal UHF Class I Generation II Air Interface Protocol v1.0.0 (2006): Accessed June 2006, http://www.epcglobalinc.org/standards_technology/.

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

[21] M. Aigner, and M. Feldhofer (2005): Secure Symmetric Authentication for RFID Tags, Telecommunications and Mobile Computing TCMC2005, March 8th-9th, 2005.

[22] Feldhofer M., Dominikus S., Wolkerstorfer J (2004): Strong Authentication for RFID in Systems using the AES Algorithm Lecture Notes in Computer Science (LNCS), vol. 3156, pp. 357-370, 2004.

[23] J.Wolkerstorfer (2005): Is Elliptic-Curve Cryptography. Suitable to Secure RFID Tags, in Workshop on RFID and Light-Weight Cryptography, Graz (Austria), 2005.

