
Article:
Good, T. and Benaissa, M. (2013) A holistic approach examining RFID design for security and privacy. Journal of Supercomputing, 64 (3). pp. 664-684. ISSN: 0920-8542

https://doi.org/10.1007/s11227-010-0497-9

A holistic approach examining RFID design for security and privacy

Tim Good[2], Mohammed Benaissa[1]

[1] *Dept. Electronic & Electrical Engineering, University of Sheffield, Mappin Street, Sheffield, S1 3JD*

[2] *now with Dept of Medical Physics, Royal Hallamshire Hospital, Sheffield Teaching Hospitals NHS Foundation Trust, Sheffield, S10 2JF*

timothy.good@sth.nhs.uk m.benaissa@sheffield.ac.uk

Abstract. This paper adopts a holistic approach to Radio Frequency Identification (RFID) security that considers security and privacy under resource constraints concurrently. In this context, a practical realization of a secure passive (battery-less) RFID tag is presented. The tag consists of an off the shelf front end combined with a bespoke 0.18µm Application Specific Integrated Circuit (ASIC) assembled as a credit card sized prototype. The ASIC integrates the authors' ultra low power novel Advanced Encryption Standard (AES) design together with a novel random number generator and a novel protocol which provides both security and privacy. The analysis presented shows a security of 64-bits against many attack methods. Both modelled and measured power results are presented. The measured average core power consumed during continuous normal operation is 1.36µW.

Keywords: *RFID, challenge-response, security, privacy, low power, AES, RNG*

1 Introduction

Radio Frequency Identification (RFID) systems usage has seen a dramatic surge in recent years. Such systems, as illustrated typically in Fig. 1, have three principal components, a radio tag or transponder, a reader and a database [1]. The tags comprise small integrated circuits typically connected to a small wire coil antenna and attached to an item or carried by a person to facilitate electronic identification. This can be in terms of an electronic product code (EPC) [2] or a unique serial number. The reader emits a radio signal which provides the challenge to tag and in the case of passive tags also provides the source of energy for the tags operation. The RFID process is non-contact, does not require line of sight and depending on the selected RF band and antenna design can be carried out at ranges from several millimetres to several meters. Typically a database is then queried using the tag's identifier to provide further details.

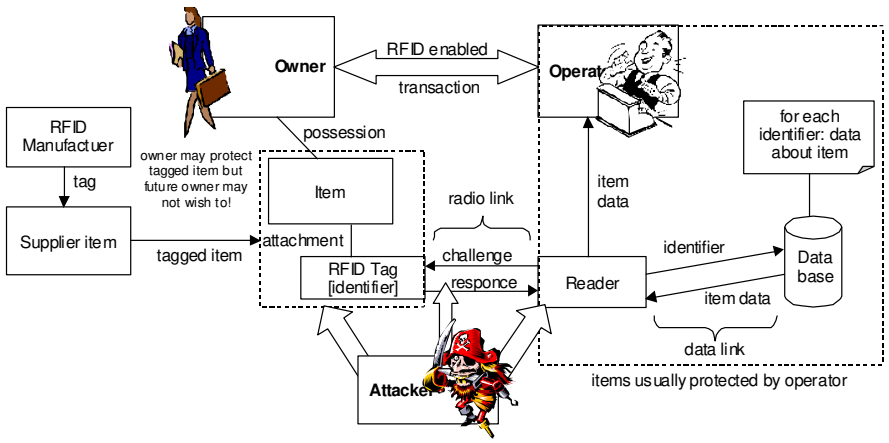

Fig. 1. Typical RFID System

RFID technology already pervades our daily lives from management of the supply chain (attached to goods in retail stores, car tires, etc) through to the chip in you car key which operates the immobilizer [3]. RFID already offers very many benefits to society however there have been a number of privacy and security concerns raised regarding the proliferation and standardization of RFID together with real world examples of exploitation of the negative aspects [4-8].

The privacy concern arises from the ability to remotely interrogate an RFID at a distance to ascertain some information about the individual or individual's property [9]. One particular concern is the association of particular tag response(s) with a specific individual disclosing their location, often referred to as location privacy [10].

Security issues for RFID centre around the ability to forge the credentials embodied by the device. This may be in terms of cloning the RFID or mimicking it's responses to a reader.

The majority of the population of tags form part of the supply chain and are removed or disabled (killed) at a point of sale [11]. It has been argued [12] that if the disposition of tags is tracked by so called smart shelves during shopping then the individuals shopping habits can be ascertained. However, there is a second class of RFID, where as part of its normal lifecycle remains active whilst in the possession of an individual, thus posing far greater privacy and security concerns. Examples include: identity cards, car keys, car tyres, medicine packaging and some higher value retail products.

Economics plays a large role in the design of RFID tags: they must be fundamentally low cost as they are frequently attached to low value items. The deployers of RFID are normally interested in issues such as product

authentication, counterfeit detection and supply chain efficiency. It has been stated that to be economic any tag-borne security measures must fit within an area of 250-3000 gate equivalents [8,10,11]. It is expected that the economic limit of area will increase year-on-year in line with Moore's law.

Research in RFID technology, and in particular RFID security, is currently very active and is summarized in two recent review papers [8,13]. The challenge is to develop secure protocols for RFID which do not leak sufficient information (i.e. an identifier) which in turn may be used to derive personal information about its owner / bearer. Previous attempts have focused exclusively on privacy at the expense of security, and vice-versa. Even the best previous attempts at such protocols [10,14-18] have vulnerability to either Denial of Service (DoS) attacks, radio-relay attack [19] or allow user tracking via a unique constellation of non-unique identifiers [10].

Modelled results for the baseband part of a UHF RFID tag using the AES were reported in [20]. However, the design is rather large (approx. 3 times larger than this work) with only simulated power results and with unknown duty cycle. Further, a Tausworthe PRNG [21] is used which may initialize to a known state facilitating a number of attacks. The on-tag storage of a long-term secret-key shared between a large set of tags and readers makes a tempting target for reverse engineering or side channel analysis of a tag.

Typically passive tags are powered by rectifying the applied RF field and use this same field as the clock source. This constrains the design to operate on very tight energy / power budgets and effectively fixes the clock rate. The limited power also limits the available area in terms of static power consumption together with economic factors. This has a disadvantage for cryptographic protocols, in that the tag is not powered between interrogations thus cannot have its own sense of time.

The challenge-response model, adopted in the majority of RFID systems, requires two-way communication; however, a passive tag derives its clock from the reader's transmission thus cannot discern time/phase changes, hence the only suitable modulation for reader-to-tag communication is basic on-off keying. Conversely the tag-to-reader channel may select a more efficient modulation.

There are a number of protocols which have been proposed which require the tag to update its NVRAM; such write operations are typically expensive in

terms of power and time and also raise data integrity issues (due to loss of power) which must be addressed by additional complexity. Further, if there is a requirement to write to the NVRAM this opens up a set of DoS attacks with a high degree of permanence.

If a tag can keep a static identifier internally, then One Time Programmable (OTP) memory may be used which represents considerable savings over NVRAM. However, to maintain security or privacy such an identifier cannot be transmitted in the clear.

Tags typically operate in a fundamentally insecure environment in which an attacker may seek to counterfeit them (in order to copy the item they protect). It is assumed that they may be subject to side channel analysis and reverse engineering. This places a limit on the value and longevity of any key which such a tag attempts to store securely.

In this paper, a holistic approach that considers security and privacy concurrently under constraints of low resource and real-time operation, is adopted for addressing the current security limitations in RFID systems and in particular passive RFIDs; work is presented that shows the practicality of integrating a strong cryptographic primitive into a battery-less (sometimes referred to as passive) RFID together with a secure protocol and supporting random number generator (RNG) to produce a working prototype tag without the need for writing to non-volatile memory during its normal operation. This is believed to be the first reported integrated implementation for such a design. A number of innovations, in terms of very low power, very low number of cycles and very low area for the strong cryptographic primitives, were made to achieve the required performance within the stringent constraints imposed by low frequency passive RFIDs. The results from a manufactured prototype, including a dedicated 0.18μm CMOS chip, are presented to demonstrate functionality and performance.

2 Holistic Approach

The fundamental concepts are in fact concerned with the generic problem of anonymous transfer and/or verification of identity in a real time (wireless/network) environment which in practice, if advances are to be made, necessitates the investigation of security versus privacy versus real time operation

versus resources in a holistic manner; existing approaches tended to focus on single aspects of this cost function at a time.

A holistic approach, as proposed in Fig. 2, investigates security and privacy concurrently at all levels (protocol, primitives, and physical) under a range of practical constraints dictated by intended usage.

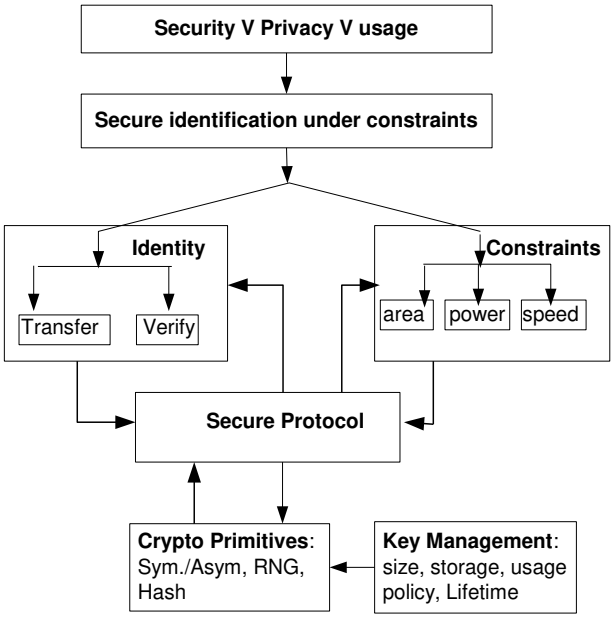

Fig. 2. Holistic approach

From Fig. 2 two key technical challenges may be identified in the context of RFID:

The first challenge is the development of practical secure protocols between the tag and reader which do not leak private information; indeed even the best previous attempts, as indicated in the introduction, have vulnerabilities so a revised protocol is needed.

The second challenge is the design of very low area and very low power high-strength cryptographic primitives for the tag since RFIDs impose stringent restrictions on resources in terms of area, power and number of cycles consumed. This in turn imposes serious limitations on the attainable security strength. Strong ciphers usually require significant resources for their implementations. To enable strong security to be incorporated in RFIDs it is therefore necessary to challenge the low resource/power design space for existing strong ciphers. This necessitates devising very low resource/power implementations commensurate with the very

tight area, power and timing constraints for the most challenging (RFID) applications. Previous attempts have failed to do so. For example at the lowest frequencies, approx. 100kHz, RFIDs, a crypto-engine would need to operate using single digit microwatts and provide a response to the challenge in a few milliseconds.

3 Protocols

For an authentication system, the objective is to prove knowledge of an identifier without compromising the identifier to any potential attacker. In such a system, security would be considered breached if the identifier can be copied whereas the privacy would be considered weak if any predictable bit sequence (which could then be associated with an individual) can be gained by an attacker.

3.1 Types of protocol

The existing protocols for battery-less RFID systems fit into a number of categories that have already been reviewed in detail in [8,13] and briefly summarized below:

static ID: When energized, the tag responds by returning a string of bits composing a fixed identifier, for example an electronic product code. Such schemes are common in the retail sector and use write-enable unlocking passwords and are typically removed or disabled at the point-of-sale.

refreshed ID: As with static ID, the tag repeatedly broadcasts its identifier when energized, however, on successful reading by a legitimate reader a new identifier is generated by the reader and sent to the tag typically with a write-enable unlocking password.

hashed ID: The tag performs a hashing operation, H(ID), on its own identifier, storing the new result and transmits part of the result to the reader as its temporary identifier. All tags in this category must perform an NVRAM write operation to store H(ID).

keyed authentication: The tag performs a key dependant cryptographic hash operation with its identifier with a once-only random number, a nonce, (N) to yield an authentication code (MAC) which is transmitted to the reader. There are a number of variations in this category depending on the source of N; these are tag generates Nt, reader transmits Nr to tag or both.

Table 1 summarises the communication and tag operation overhead (all are assumed to include transmission, reception and non-volatile memory storage) for the various schemes.

Table 1. Types of tag and their operations

Type	Reader to tag	On-tag operations	Tag to reader
static	none	-	ID
refreshed	newID+passwd	NVwrite	ID / newID
hashed	none	H(ID), NVwrite	part H(ID)
auth (Reader)	*Nr*	H(ID,*Nr*)	H(ID,*Nr*)
auth (Tag)	none	gen(*Nt*), H(ID,*Nt*)	*Nt*,H(ID,*Nt*)
auth (Mutual)	*Nr*	gen(*Nt*), H(ID,*Nr*,*Nt*)	*Nt*,H(ID,*Nr*,*Nt*)

In terms of accessing the security or privacy of an RFID system a number of assumptions are made in terms of the avenues of attack and their goals whilst meeting some operational requirements for the system.

The assumed requirement for this system is to provide entity authentication. In a real system there may be many readers per operator and multiple operators. A protocol which supports the use of a single tag by different operators would be advantageous. The bearer of the tag seeks to prove its identity to the operator by presenting an RFID tag to the operator's reader. A second requirement is that the owner wishes their identifying information to remain confidential from an attacker. In this context the identifying information is taken to be any predictable bit sequence. It is assumed that, beyond the identifier, all further information is stored in a central database (or set of databases) with the possibility of later off-line lookup; the latter enables the use of non-networked hand-held readers.

3.2 Methods of attack

This section provides a brief overview of possible attack methods that can be mounted on RFID systems, each may seek to challenge privacy or security aspects:

eavesdropping: The attacker (Eve) passively monitors the communications between tag/reader.

man-in-the-middle: In a traditional communications system the attacker (Mallory) places himself between the communicating parties. This is not practical for very short range RFID systems. However, the attacker may use a radio relay, see below.

radio relay: The attacker shares a covert radio link with an accomplice. The accomplice relays information from an authentic tag remote from the reader to the attacker who is close to the reader, thus the attacker gains the advantage of virtual presence of the tag. The attacker may also modify these communications. The simple radio-relay attack cannot be prevented by purely cryptographic means; countermeasure to this attack is based on limiting the acceptable propagation time between challenge and response. It is common risk to all contactless systems. Limiting the distance over which such a relay can be effective is the subject of distance bounding protocols, relying on the timing accuracy to which a transponder response to a random challenge can be measured [22,23]. In practice low bandwidths and noisy multi-path signal environments make this somewhat more difficult.

denial of service: All radio links are vulnerable to local jamming, however in the context of RFID of concern is the permanent DoS attack where the attackers' actions effectively disable a tag or reader to prevent future authentications taking place.

counterfeit tag: The attacker attempts to generate (valid) responses for a tag using a fake tag. A legitimate tag may have been previously observed.

malicious reader: The attacker attempts to generate challenges to pretend to be a legitimate reader and to communicate with legitimate tags to gain some advantage.

reverse engineering: The reader is assumed to contain a tamper resistant trusted computing module which is beyond practical attack (contains battery, sensors and wipes stored information making it useless on detecting a physical attack). It is assumed that the costs of reverse engineering a tag will be beyond the economic advantage gained from doing so.

side channel analysis: The attacker attempts to monitor EM fluctuations from the tag or inject faults in order recover key information from the tag.

Adopting a low frequency and good clock/power management circuitry together with running a TRNG during cryptographic operations makes mounting such attacks considerably harder. However, this risk is somewhat unquantifiable in practice.

reader networks: The links between readers and databases are considered beyond attack from the perspective on an RFID protocol and would be protected by more traditional network security schemes (eg TLS).

3.3 Analysis using games

A protocol may be analyzed as a set of games played out by the legitimate participants and would-be attackers of the system. The holder of the tag may be considered to be the *prover* and the reader system the *verifier*.

authentication game: The verifier seeks a message from the prover to show they know some secret (the identifier). Typically in order to avoid replay attacks this involves a unique challenge issued by the verifier. This game tests half of the security model for a system.

counterfeit game: An attacker may try to copy a tag or the tag's responses with the aim of either compromising the tag's identifier or seek to duplicate responses from an authentic tag. This game tests the second half of the security model for a system.

anonymity game: An attacker seeks a static or predictable identifier with the aim of tracking the tag or its carrier. The attacker may eavesdrop, modify or replicate communications between tag/reader or create their own malicious reader to mount such an attack. There is a totalitarian variation of this game where the attacker is a legitimate reader of tags and seeks to track *all* tags. However, for say N tags, generating a much shorter watch-list of say √N tags is considered an acceptable compromise for a totalitarian model. This game tests the privacy mode for a system.

There are very many different scenarios and methods of attack which can be played out. A brief summary is given in Table 2.

Table 2. Tag ID protection

Type	Authentication denial	Counterfeit	Anonymity
static	× large no of duplicated fake IDs cannot determine real one	× ID in clear can directly copy	× ID is in clear
refreshed	× mandates a single authority / database for refreshing ID, loss of data link	~ ID in clear but of limited lifetime	× reader can use predictable sequence for "new ID"
hashed	× desynchronization / loss of chain-of-IDs possible and irrecoverable	✓ strong	× future values of ID can be pre-computed
auth(Reader)	✓ strong	✓ strong	× reader can use standardized challenge
auth(Tag)	× really needs single database to mitigate replay attacks ideally store all responses – impractical!	× tag can use small set of Nt with known auth codes	✓ strong
auth(Mutual)	✓ strong	✓ strong	✓ strong

3.4 Double-Challenge-Response Protocol

The novel authentication protocol developed here falls into the auth(Mutual) category, which is the only category with the possibility of strong resistance to the three games. Random numbers are generated by both reader and tag and a keyed hash operation used to produce the authentication code. This novel protocol is based on [24] with a repeated challenge being used to avoid the inevitable authentication code collisions (birthday paradox) and provide security of at minimum $O(2^{64})$ and ideally $O(2^{80})$. Allowing for the possibility of a time-memory trade-off, a key length of 128-bits will be used. The actual complexity of an attack will depend on the number of tags within the much larger key space. An assumption that there are less than 2^{64} tags within the 2^{128} key space is made.

It should be noted that the XOR operation is not suitable for combining the reader and tag nonces, *Nr* and *Nt* (the tag has not committed to *Nt* thus could attempt to cheat the reader), thus concatenation was used instead.

Such a protocol avoids the tag having to perform any NVwrite operations however does require transmission of *Nr* by the reader. The inclusion of *Nr* (a random number the reader is content with) prevents the trivial replay attack.

The protocol starts by the reader issuing a challenge to which a tag must respond. In this protocol the challenge consists of a random value, *Nt* (of an

unpredictable nature which the reader is satisfied with). The tag takes this value, generates a random value of its own, *Nt* (a value that the tag is satisfied is unpredictable). These values are combined in the tag with a secret identifier, *ID*, using a strong cryptographic operation, *H*. The output from *H* is truncated to the required length and broadcast by the tag, as the authentication code *X*, together with the random value the tag generated, *Nt*. The reader can then use the tag's response to query a database containing known tag identifiers (and repeating the cryptographic operation, *H*, for each) to determine which identifier the tag knows. To achieve the required security level whilst maintaining short messages, this process requires repeating a second time with a different random value of *Nr* to finally prove the authenticity of the tag.

The protocol is summarised by the following algorithm:

```
reader:   Nr ← random number
          transmit Nr
tag:      Nr ← received value
          Nt ← random number
          X ← H(ID,Nr|Nt)
          transmit Nt and (part) X
reader:   Nt1,pX1 ← received value
          for {all IDs in database}
                X′ ← H(IDi,Nr|Nt1)
                if (part) X′ = pX1
                      Nr2 ← random number
                      transmit Nr2
                      Nt2,pX2 ← received value
                      Y′ ← H(IDi,Nr2|Nt2)
                      if (part) Y′ = pX2 and pX1 ≠ pX2
                            tag is IDi
                      end if
                end if
          end for
```

The protocol ensures privacy by preventing any active or passive attacker from gaining any information which is distinguishable from a random sequence. First consider the cryptographic operation, this converts a *plaintext* to *ciphertext* using a *key* such that any set of ciphertext without knowledge of the key cannot be

used to recover plaintext or the key (at a lower complexity than brute force trying all keys). By definition, successive outputs from a strong cipher will be indistinguishable from a random bit stream (else it would have a distinguishing attack). In terms of privacy, given a guaranteed source of random plaintext for the challenge and the key remaining secret, then the generated response will be indistinguishable from a random sequence. In this protocol all the challenges and responses in normal operation are indistinguishable from a random sequence. If a malicious reader was to issue a standard challenge, *Nr* ensures that the tags response remains indistinguishable.

An alternative visual representation of this protocol is given in Fig. 3.

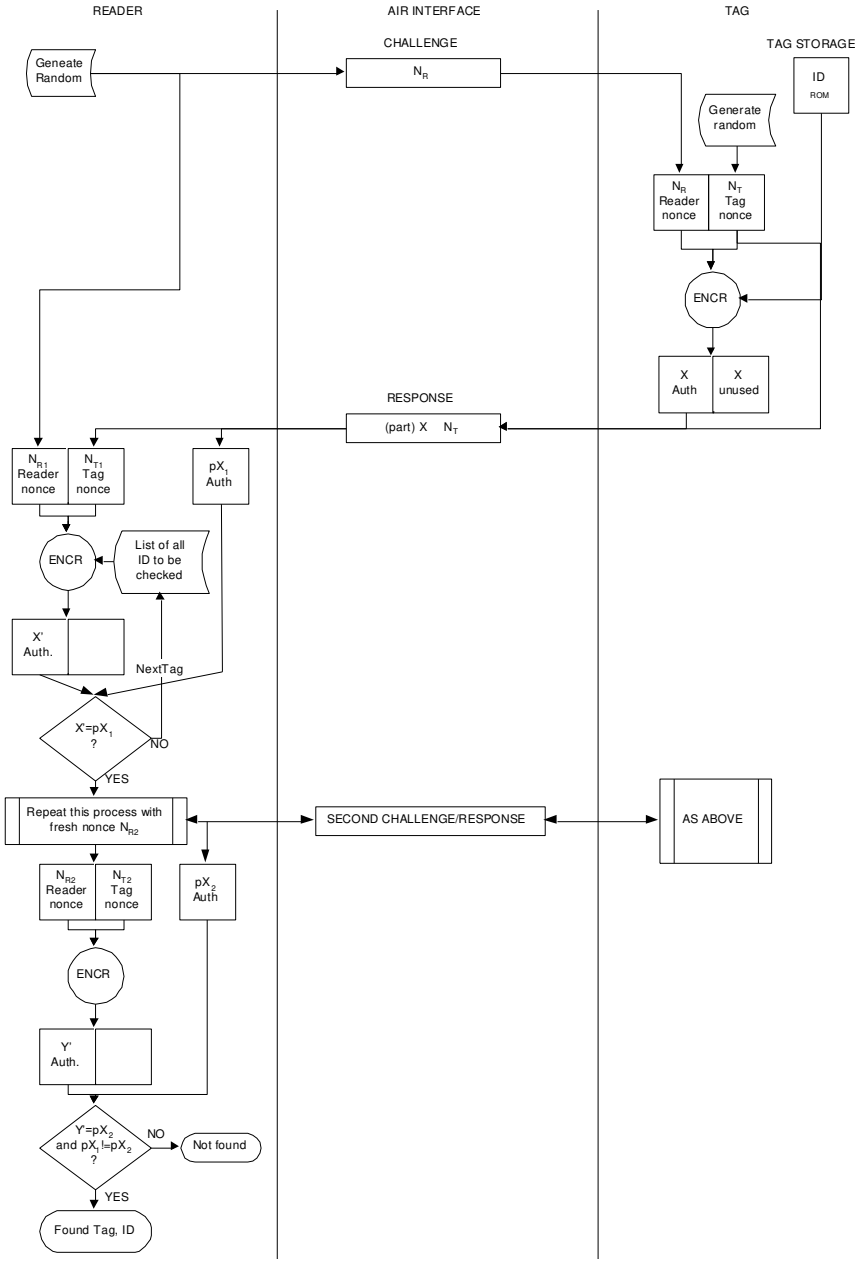

Fig. 3. Double challenge response protocol

As the internal identifier of the tag remains unchanged there is easy support for multiple reader databases and privacy is protected by the dependence of the authentication message on the unpredictable *Nt* (a random number the tag is content with). This forces the reader / database to perform comparison with all known tags for a match (computationally expensive) and thus limits the size of databases. For databases, say at the national level, this may be mitigated by the user of the tag supplying some (any) additional information of the users choosing to reduce the search space (eg a pin number or date of birth).

4 The Cryptography Primitives

The starting place for selection of a suitable keyed hash or block cipher primitive is to determine the required strength. A brute-force attack strength of 2^{64} is selected as a suitable design strength. Thus, *Nt* and *Nr* must both be 64-bits. Concatenation gives a 128-bit block size. To avoid collisions, order 2^N, a key length of 2N is needed, i.e. 128 bits. To prevent lookup table creation of low order ($<2^{64}$), the authentication code needs to be 64-bits and then only part (i.e. half) the response. Thus a low resource, accepted as cryptographically strong, primitive with 128-bit block size and 128-bit key is sought.

The obvious choices are SHA-1 [25] and the AES [26], recent work [27,28] has shown the AES is lower resource than SHA-1. The authors' related work [29] offers even more superior low-resource (power-area-time) performance thus used as the cipher primitive for the tag.

4.1 Analysis against attack games

Both notions of security and privacy can be analysed by estimating the amount of work that needs to be done by an attacker to gain an advantage. Using $O(2^N)$ to indicate a non-polynomial level of effort against the previously described attack games.

he security analysis for a system using the proposed protocol is as follows: a legitimate verifier knows a list of possible IDs and is seeking to verify that the tag has one of these. Two challenge-response cycles provides authentication to the required security level against counterfeit responses to challenges. The attacker has no control over *Nr* but still has a number of attack options all at least $O(2^{80})$:

(a) an attacker could attempt to store a partial table of (Nr,Nt|X) for pairs of responses from a valid tag; to succeed two successive correct responses are required. For a table with 2^m entries (each pair totalling 384 bits) giving a memory complexity of $2^{m+8.6}$ and a time complexity to acquire the data of 2^{m+1} challenges. The probability of a known challenge, Nr occurring has a time complexity of 2^{64-m}. Thus the attacker has to wait by the reader for this amount of time (potentially at risk). The preparation phase requires time-memory complexity of $2^{2m+9.6}$ and the attack has a waiting time of 2^{64-m}. It should be noted that with a 10Hz challenge response cycle such an attack would be impractical (max 2^{20} challenges per day). For one-days(!) waiting time m=43 with a 50% probability of success thus precomputation is 2^{95}.

(b) brute force test all IDs $O(2^{128})$

(c) attempt key recovery attack on AES (only half of X is known) at least $O(2^{128})$

(d) respond with random auth code twice $O(2^{64\times2})$.

The tag once programmed is write protected (or could even have the key uniquely defined during manufacture eg laser writing) thus, permanent DoS attacks are not possible. It is an essential part of the system security that the tag IDs be assigned from a set of uniform random numbers.

The privacy can be tested using the anonymity game: there exists an adversary who does not have prior knowledge of the ID and seeks any predictable bit sequence (an identifier). The best attack is to choose a fixed Nr, however the tag generates its own Nt thus both Nt and (part) X appear random $O(2^{64})$. The adversary gains two random numbers and can only attempt AES key recovery as the best attack $>O(2^{80})$.

The totalitarian sub-game on first inspection appears somewhat easier in that the list of tags, length M ($M << 2^{64}$) is known, however, the reader must do work O(M) to recover the ID for each tag. Thus to recover all tags $O(M^2)$ per reader, say there are coincidentally $M^{0.5}$ readers (a conservative assumption) then total work is at least $O(M^{2.5})$. So for an M of 50 million this is approx $O(2^{64})$.

There remains the possibility of a radio relay in which the attacker shares a covert radio link with a legitimate tag thus gaining an assumption of possession at a distance. If this is the only communication channel, such an attack cannot be countered by cryptographic means and instead is protected by using either

screened reader enclosure or additional factor of identification (for example a PIN number entered on a keypad adjacent to the reader) [30].

4.2 Random Number Generator

There are very many software methods for generating random numbers however their "goodness" depends on the application. For cryptographic security a random number generator must be both unpredictable and uniform. There are two main sets of tests currently used for such random number generators, Diehard [31] and NIST [32], used to provide an indication of confidence for uniform random key generation. Arguably, such tests are far from perfect; consider a simple counter encrypted with an all zero key passed through a strong cipher such as the AES, it would pass all the tests however, the future sequence would be wholly deterministic rather than random, an attacker knowing this counter-obscuration was being employed could simply decrypt the current state (using the all zero key) to recover the counter and predict any future state.

RNGs are defined as pseudo random number generators (PRNG) or true random number generators (TRNG). To be of use for cryptography deterministic PRNGs must have an internal state which is undeterminable by an attacker.

To meet our design requirements for battery-less RFID the generator cannot store its current state in the NVRAM, the generator must reach the random state within 10's of milliseconds and use very little power. Many generators can take some considerable time to accumulate sufficient entropy to reach a random state.

Hardware random number generators, rely on random processes in the physical world, such as thermal noise and chaos. Unfortunately, many such processes generate non-uniform statistics, examples include Gaussian noise and 1/f "noise" from the quantum nature of the electron. Frequently a *corrector* circuit (PRNG) to compensate for non-uniform behaviour of the physical world is necessary.

Table 3 presents a summary of existing methods used for hardware random number generators, together with the most applicable reference for low-frequency battery-less RFID. None were found to be suitable for this application.

Table 3. Hardware RNG approaches

Approach	**Process, power, area, time**
Amplified noise	2µm CMOS, 1.5mm^2 3.5mW@100kHz [33]
Bank of independent oscillators	For cryptographic purposes, ~100 oscillators required [34,35]; would consume orders of magnitude too much power and area.
Metastability	0.35µm, 0.031mm^2, 2.92µW for 500 bps, 200 seconds to become random, accurate biasing needed [36]
non-linear analog 'chaotic' mapping based	0.18µm 3.024mW(estimated): too much power. Neither area or time to reach random state given in [37]
clock jitter of HF-LF oscillator pair	0.18µm 2.3mW, 0.0016mm^2, 10Mbps [38], still significant power

For this application, a random bit is required approx. every 500µs (2kbps). The available clock is 125kHz, attempting to generate a very low frequency oscillator at 2kHz would require relatively large components and not be viable. The alternative is to generate an oscillator >>125kHz however if running continuously would consume much power. A second engineering issue arises from the weak power supply which may provide a convenient mechanism for the slow and fast oscillators to lock together.

This problem is overcome using free running fast oscillators which are enabled only during the transitional periods of the low frequency clock.

The aims for the generator are provide near uniform and unpredictable random *Nt* soon after power up and continue to do so to prevent an attacker from obtaining a fixed (but encrypted) identifier thus defeating the anonymity game. Conversely the security relies on the generator within the reader which is not so resource critical. This is a somewhat weaker requirement than an influence-free, truly-uniform distribution mandated for random key generation.

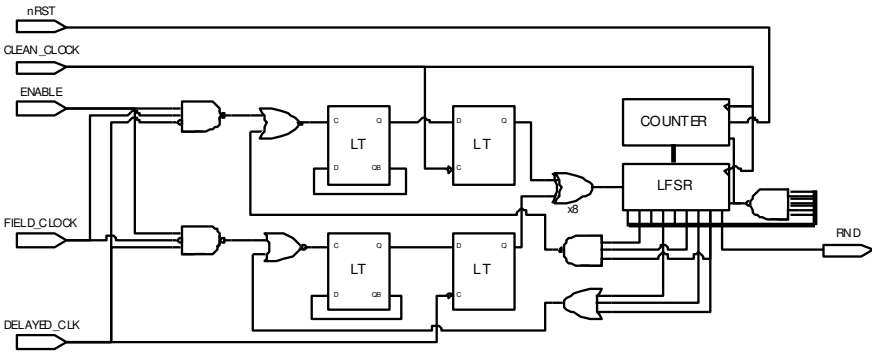

Fig. 4. Circuit diagram of random generator

Two gated high speed oscillators are used, with a free running frequency of ~2GHz. The gating functions being defined such that one oscillator conditionally runs during the rising edge of the (relatively slow unstable) clock and the second the falling edge. Both operate approximately 1/8 cycles with the possibility of both operating during the same cycle. Both oscillators never run at the same instant in time. Further, closely-placed latches are used to minimize power consumption and prevent meta-stability which may otherwise incur an additional power penalty. These outputs are then combined with a feedback polynomial in a linear feedback shift register. To prevent adverse statistics from the all-zero state a counter is used to restart the generator uniformly.

Testing a hardware random number generator needs to be made under normal operating conditions so at only a few transactions per second presents a practical problem in collecting the approx 11Mbytes of data required by the test suites. For this system it takes approx 3 days to acquire sufficient data to assess the continuously powered operation. However for the more usual tag powering down between each series of a small number of challenges takes considerable longer, approx 3 weeks allowing sufficient powered-off period to avoid memory remanence.

To date the RNG in Fig. 4 passes 14/15 of the DIEHARD tests, failing part of the count-the-ones test. Further refinement of the generator and testing is still a work in progress. One option, we have already tested, which passed all the tests was to feed the (not quite uniform) random bits into the AES key and plaintext inputs and perform the encryption operation. As the AES hardware is already present this does not increase the area and only adds 2.8ms to the response time. In this application the AES is used to remove the slight non-uniformity in the RNGs statistics; it should never be used to generate ‘random numbers’ starting from a counter.

5 Prototype System

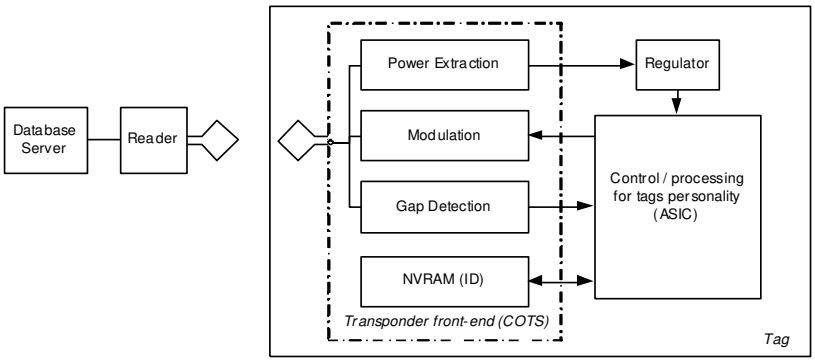

Fig. 5. Block diagram of system

In order to control cost whilst demonstrating the practicality of a strong cryptographic protocol on a low frequency, 125kHz, battery-less RFID, an off the shelf front end and NVRAM integrated circuit was used [39]. This is shown in Fig. 5. In a monolithic implementation the integration would remove the need for many of the I/O drivers and further reduce the total power consumption.

The air interface for the module has been defined to be minimalist. It uses on-off keying average bit rate RF/27 for reader to tag communication and Manchester modulation at RF/16 (data rate of RF/32) for the return channel. The tag acts as a slave to the reader and processes four commands to completely define the protocol and permit tag programming.

The tag's configuration register in NVRAM (if write enabled) may be updated with a CFG(*m*) command to clear the write-enable status, set the operating mode for the random number generator and anti-collision on read mode.

A second command KEY(*k*) if the tag is write-enabled permits modification of the tag's 128-bit key in NVRAM.

The IV(*Nr*) command supplies the tag with the reader's 64-bit random and triggers the tag to perform its cryptographic operation (the tag has already generated a random, *Nt*):

$$X = \mathrm{AES}\ (\ key, Nr \mid Nt\ )$$

The tag then transmits half of *X* as the message authentication code (MAC) together with *Nt* (total 128-bits). This is encapsulated between synchronization tokens and repeated until the SILENCE command is received (or power is lost). At which time the tag resets refreshing its random, *Nt*.

In anti-collision mode the reply is punctuated by periods of silence of between 1 to 16 message periods. Repetition of the same message to a challenge is helpful for environments attempting to read a number of tags within the same time frame. It is also possible then to be extended to the classical singulation methods based on the response, *X* (eg tree-walking).

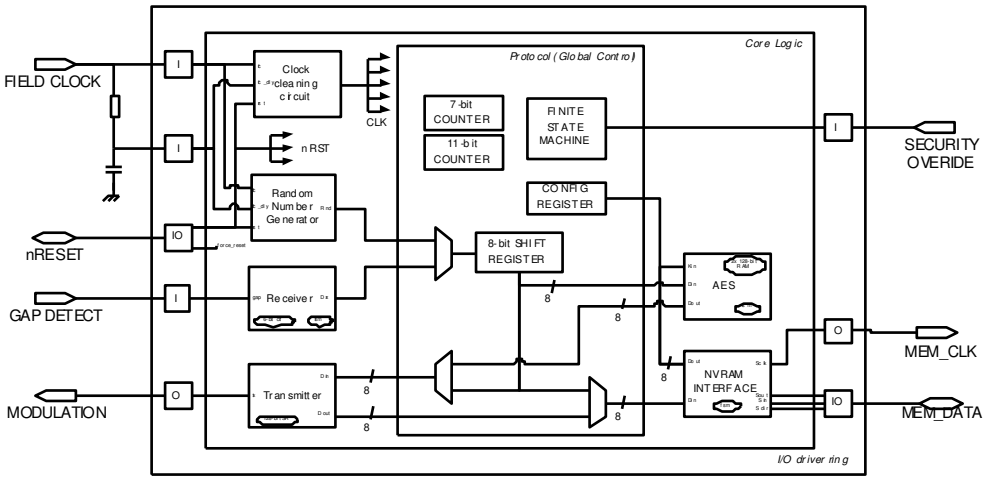

Fig. 6. Block diagram of ASIC

An ASIC has been designed and fabricated on 0.18 µm CMOS to interface to the front end and integrates a random number generator, AES crypto primitive, modem, NVRAM interface, controlling protocol and clock management circuitry (Fig. 6).

The use of a low frequency RF (sinusoid) as a clock combined with a relatively high impedance power source results in a need to 'clean-up' the clock to prevent unintended clock transitions as the slow rising edge approaches the threshold voltage due the varying current demands of the on-tag logic. This is done using a delayed version of the clock created using a simple RC delay and the circuit shown in Fig. 7.

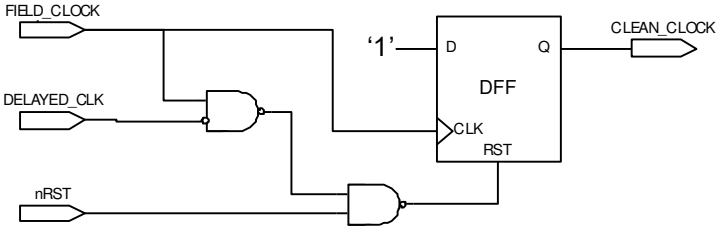

Fig. 7. Clock cleaning circuit

The protocol requires a source of random bits which may also be conveniently generated from the poor clock source using the random number generation circuit already described. The generator is only enabled when required, to conserve power.

The NVRAM has a bidirectional serial interface for read and write commands this is converted to a more conventional 8-bit RAM style interface by the interface module shown in Fig. 6. The NVRAM is used to store a configuration word (read on reset into the tags configuration register) and the tags ID.

The receive (Rx) module decodes the OOK data sent by the reader and passes it to the protocol controller for interpreting the commands. The controller includes timeouts to prevent the tag from locking up due to communication errors.

The low power 8-bit design for AES encryption is keyed using the tags ID and is used to hash the random number generated in the tag and the IV sent by reader to create the required MAC. This design uses a single 8-bit implementation for SubBytes and requires 356 cycles (inclusive of key and data I/O) to perform AES encryption whilst maintaining very low power consumption.

The random and auth code are loaded into a 128-bit register for transmission. This simplifies extension to multi-tag environments. The transmit (Tx) module encodes responses using Manchester coding and serially outputs this modulation to the antenna.

The design was described using VHDL and synthesized, placed, routed and taped-out using Cadence tools. As with most designs on deep-sub micron processes, it is routing limited. After cell placement and routing the back-annotated netlist was simulated using ModelSim and validated as a system using a behavioural model for the rest of the system and against known test vectors. Modelled power results were obtained using the system model to generate switching activity together with extracted layout parasitics. The area results, post layout including clock tree, are expressed using the process independent measure of NAND Gate Equivalent (GE).

6 Performance results

Table 4 shows the modelled power consumption and Table 5 the timing results for a typical challenge-response cycle. These are reinforced with actual

measurements later in this chapter. For comparison, the relatively lengthy write times and power consumption for EEPROM makes the total time to receive and write a new tagID (128-bit key) 330ms. This validates the assumption to avoid NVRAM writes during normal challenge-response operation.

Table 4. Modelled Results, bias 1.8V 125kHz clock

Module	**Power, µW**	**Area, GE**
Controller	0.50	899
RandGen	3.36 (34%)	110
Crypto(AES)	2.76 (28%)	4655 (56%)(2x128bit mem 2700 GE)
TxUnit	1.06	1481(128bit tx reg 1350 GE)
The rest	2.29	1115
TOTAL	9.97	8260

Table 5. Timing for challenge-response cycle

State	**Time, ms**	**Notes**
key from NVram	2.8	direct to AES module
generate random	33 (38%)	
receive IV	11.1 (min) 14.3 (typ) 17.4 (max)	2+64 bits
crypto (AES)	2.7	356-16 cycles
transmit auth	33.8 (39%)	4+64+64 bits
receive silence command	0.8	2+2 bits
TOTAL	84.2 (min) 87.4 (typ) 90.5 (max)	11 Hz

The core area of the ASIC is 397 by 395µm (0.157mm^2). This is surrounded by the power rings, I/O driver cells and pads. The design has 4 power pads, 4×Inputs, 2×Outputs and 2×Bidirectional pins. The total chip size is <1mm^2. The layout and a micrograph of a manufactured chip packaged in SOIC16 are shown in Fig. 8.

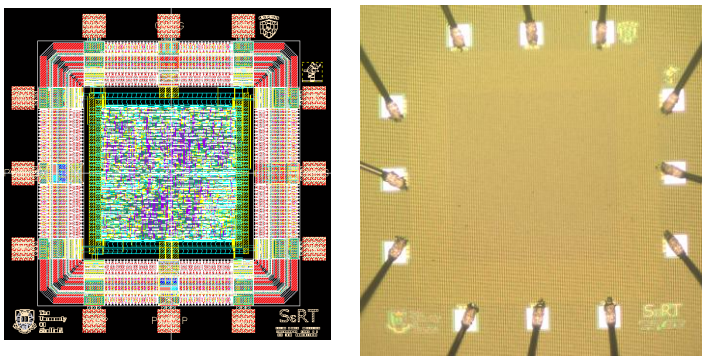

Fig. 8. CAD layout and die micrograph 0.18mm CMOS

A credit-card size prototype has been assembled using a wound wire antenna and a small PCB containing the secure RFID transponder (SεRT) ASIC (this work), COTS transponder front end [39] and a 1.8V regulator. This is shown in Fig. 9.

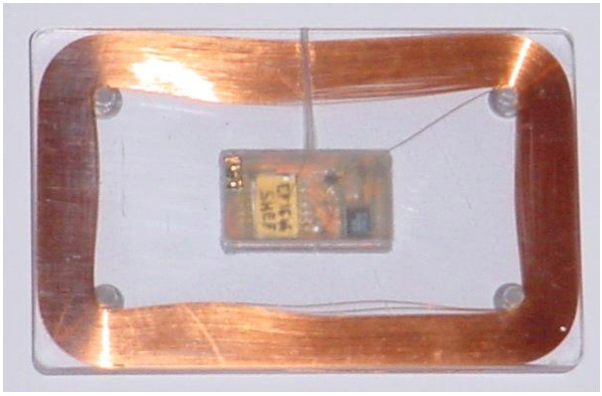

Fig. 9. Prototype battery-less secure tag

A simple reader was constructed using off the shelf components based around a MicroChip 16F627A PIC, the dev. kit for the Atmel 2270B base-station chip and controlled via RS232 using a PC to test the system. A number of different tests have been performed including a week continuous operation. Overall, the tag responded to 99.75% of challenges by the reader. The challenge-response cycle (including 9600 baud serial communication to the PC, database lookup and comparison) on average could be performed 6.28 times per second.

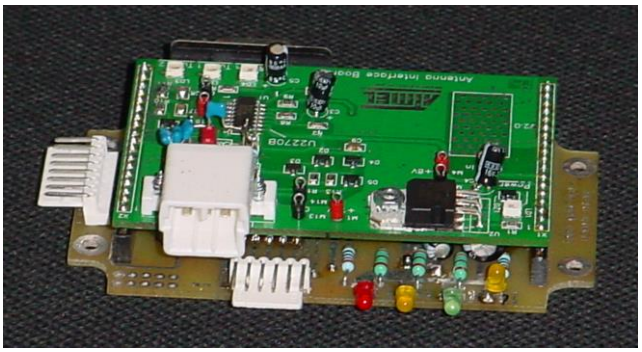

Fig. 10. Assembled RFID reader

The measured performance results for the prototype are tabulated in Table 6. The power results are for standard process options, the low power option could not be selected due to incompatibility with other designs in the multi-project wafer.

Table 6. Measured results

Dimension	Parameter	Value
RF	centre frequency (kHz)	126.2
Area	core dimensions (µm)	397 x 395
	core area (mm^2)	0.157
	chip dimensions (µm)	956 x 956
	chip area (mm^2)	0.914
Power (0.8Vcore)	core, RNG off	1.19 µW
	core, RNG for IV	1.36 µW
Power (1.8Vcore)	core (RNG off)	6.4 µW
	core (RNG for IV gen)	9.6 µW
	core (RNG IV+noise)	11.1 µW
	Demand on front end @ 2.8V	138 µW
Time	IV comms	14.3 ms
	tag computation	2.68 ms
	Auth comms	33.4 ms
	Transactions (whole system)	6.28 Hz

It should be noted that the time can be reduced by performing the RNG calculation during IV reception and the I/O ring power consumption largely avoided by moving to the more usual single ASIC for the entire tag.

7 Conclusion

It is argued that to address RFID security versus privacy concerns, a holistic approach as adopted in this paper is necessary; such approach considers security and privacy implications concurrently under usage constraints, where protocol level and cryptography primitives level issues, are investigated together taking into account the severe constraints on area, power and cycle count. The application of this approach in this paper has resulted in what is believed to be the first real demonstration of a passive (battery-less) RFID using the AES in a MAC

whilst maintaining a good notion of privacy. The tag has a measured average core power consumption of 1.36μW when operated in its normal mode at 125kHz with a bias of 0.8V.

It is shown that in order to achieve both security and privacy a tag must contain both an established secure strong cryptographic primitive and an unpredictable random source. To support one-time-programmable (OTP) tags it is highly desirable to avoid needing retained state variables (i.e. avoid writing to NVRAM); this effectively excludes PRNGs which must maintain their internal state when the tag is not powered. Thus an on-tag TRNG with relatively low latency and low power consumption is required.

It is further argued that mutual authentication is not a requirement for security and privacy, merely a lesser requirement of trust in own random number generation is needed.

It should be noted that the challenge-response cycle time is dominated by data transmission times together with on-tag random number generation. Similarly, random number generation tops the power table 34% followed by the AES at 28%.

Acknowledgements. This work was funded by the UK EPSRC and the University of Sheffield while Mr Good was at Sheffield University. The authors wish to thank Jo Spreutels and Erwin Deumens of IMEC and Lisa Wong and Mark Wilmott at the Microelectronic Support Unit, Rutherford-Appleton Laboratory for assistance with the design flow and foundry service.

References

1. T. Phillips, T. Karygiannis and R. Kuhn, “Security Standards for the RFID Market”, IEEE Computer Society, Security and Privacy, pp 85–89, 1540–7993/05, 2005.
2. EPCglobal Inc, available at www.epcglobalinc.org
3. The RFID Journal, available atwww.rfidjournal.com
4. R.J. Anderson and M.G. Kuhn, “Low cost attacks on tamper resistant devices”, in Proc. Security Protocols Workshop, NewYork, LNCS, vol. 1361, pp 125–136, Springer-Verlag, 1997.
5. A.R. Peslak, “An Ethical Exploration of Privacy and Radio Frequency Identification”, Journal of Business Ethics, vol 59, pp 327–345, Springer, 2005.
6. V. Lockton and R.S. Rosenberg, “RFID: The next serious threat to privacy”, Ethics and Information Technology, vol 7, pp 221–231, Springer, 2006.
7. S.L. Garfinkel, A. Juels and R. Pappu, “RFID Privacy: An Overview of Problems and Proposed Solutions”, IEEE Security & Privacy, May/June 2005.

8. A. Juels, “RFID Security and Privacy: A Research Survey”, IEEE J. on Selected Areas in Communications, vol. 24 no. 2, pp 381–394, invited paper, Feb 2006.
9. Article-29 Data Protection Working Party, “Working document on data protection issues related to RFID technology”, WP 105, European Commission, Internal Market Directorate-General, Office No C100-6/136, Jan 2005.
10. S.A. Weis, S.E. Sarma, R.L. Rivest and D.W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, Security in Pervasive Computing 2003, LNCS, vol. 2802, pp 201–212, Springer, 2004.
11. M. Ohkubo, K. Suzuki and S. Kinoshita, “RFID Privacy Issues and Technical Challenges”, Communications of the ACM, Vol. 48, No. 9, pp 66–71, Sept. 2005.
12. Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) website: www.nocards.org, 2003.
13. M. Lehtonen, T. Staake, F. Michahelles and E. Fleisch, “From Identification to Authentication – A Review of RFID Product Authentication Techniques”, RFIDsec06, Graz Austria, July 2006.
14. S. Engberg, M. Harning and C. Jensen, “Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience”, Conf. on Privacy, Security and Trust (PST), New Brunswick, Canada, Oct. 2004.
15. C. Chatmon, T.v. Le and M. Burmester, “Secure anonymous RFID authentication protocols”, Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006.
16. T. Dimitriou, “A Lightweight RFID Protocol to protect against Traceability and Cloning attacks”, IEEE SecureComm05, Sept 5-9, Athens, Greece, Sept 2005.
17. J. Yang, J. Park, H. Lee, K. Ren and K. Kim, “Mutual Authentication Protocol for Low-cost RFID”, ECRYPT Workshop on RFID and Lightweight Crypto, Graz, Austria, July 14-15, 2005.
18. G. Tsudik, “YA-TRAP: Yet Another Trivial RFID Authentication Protocol”, IEEE Intl. conf. on Pervasive Computing and Communications (PerCom06), Pisa, Italy, March 2006.
19. Z. Kfir and A. Wool, “Picking virtual pockets using relay attacks on contactless smartcard systems”, available at http://eprint.iacr.org/2005/052, 2005.
20. A.S.W. Man, E.S. Zhang, V.K.N. Lau, C.Y. Tsui and H.C. Luong, “Low Power VLSI Design for a RFID Passive Tag baseband System Enhanced with an AES Cryptography Engine”, 1st Annual RFID Eurasia conf., 5-6 Sept. 2007, pp 1-6, ISBN: 978-975-01566-0-1, 2007
21. R.C. Tausworthe, “Random Numbers Generated by Linear Recurrence Modulo Two”, Mathematics and Computation, vol, 19, pp 201-209, 1965
22. S. Brands and D. Chaum, “Distance-bounding protocols”, Advances in Cryptology EUROCRYPT ’93, LNCS vol. 765, pp 344–359, Springer-Verlag, May 1993.
23. G.P. Hancke, M.G. Kuhn, “An RFID Distance Bounding Protocol”, proc. 1st intl. conf. on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM’05) ISBN 0-7695-2369-2/05, IEEE, 2005

24. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong Authentication for RFID Systems Using the AES Algorithm”, CHES 2004, LNCS, vol. 3156, pp. 357–370, 2004.
25. National Institute of Standards and Technology (NIST), “Secure Hash Standard (SHS)”,FIPS 180-3, available at http://www.itl.nist.gov/fipspubs/, June 2007.
26. NIST, “Advanced Encryption Standard (AES)”, FIPS 197, available at: http://www.itl.nist.gov/fipspubs/, Nov. 2001.
27. J-P. Kaps and B. Sunar, “Energy Comparison of AES and SHA-1 for Ubiquitous Computing”, in proc. Embedded And Ubiquitous Computing (EUC’06), Seoul, Korea, pp. 372-381, 1-4 Aug 2006
28. M. Kim, J. Ryou, Y. Choi and S. Jun, “Low-cost Cryptographic Circuits for Authentication in Radio Frequency Identification Systems”, IEEE Tenth Intl. Symp. on Consumer Electronics, (ISCE '06), pp. 1-5, 2006
29. T. Good and M. Benaissa, “692nW Advanced Encryption Standard (AES) on a 0.13μm CMOS”, ***to appear***, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, DOI 10.1109/TVLSI.2009.2025952, 2009
30. Bruce Schneier, “Blog on security”, available online at: http://www.schneier.com/blog/archives/2005/11/the_security_of_2.html
31. G. Marsaglia, “DIEHARD tests”, available at: http://www.stat.fsu.edu/pub/diehard/
32. NIST, “A statistical test suite for random and pseudorandom number generators for cryptographic applications”, SP800-22, available at: http://csrc.nist.gov/publications/PubsSPs.html, 2001
33. C.S. Petrie and J.A. Connelly, “A noise-based IC random number generator for applications in cryptography”, IEEE TCAS-I, Vol. 47, Iss. 5, pp. 615-621, May 2000
34. B. Sunar, W.J. Martin and D.R. Stinson, “A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks”, Transactions on Computers, vol. 56, Iss. 1, pp. 109-119, Jan. 2007
35. D. Schellekens, B. Preneel and I. Verbauwhede, “FPGA Vendor Agnostic True Random Number Generator”, Field Programmable Logic and Applications (FPL '06), pp. 1-6, Aug. 2006
36. J. Holleman, B. Otis, S. Bridges, A. Mitros and C. Diorio, “A 2.92μW Hardware Random Number Generator”, Proc. of the 32nd European Solid-State Circuits Conf. (ESSCIRC 2006), pp. 134-137, Sept. 2006
37. T. Zhou, Z. Zhou, M. Yu and Y. Ye, “Design of A Low Power High Entropy Chaos-Based Truly Random Number Generator”, IEEE Asia Pacific Conf. on Circuits and Systems (APCCAS 2006), 4-7 Dec. 2006, pp. 1955-1958, 2006
38. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti and M. Varanonuovo, “A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC”, IEEE Transactions on Computers, vol. 52, no. 4, April 2003
39. Atmel Inc, “U3280 100-150kHz transponder interface datasheet”, available at: http://www.atmel.com/dyn/resources/prod_documents/doc4688.pdf

Response to reviewers

First, we would like to thank all of the anonymous reviewers for their helpful comments which not only improved readability but resulted in a much stronger contribution overall. Each reviewer's comments have been addressed individually in the following sections.

***Reviewer #1**:*

The paper is well written and the research has been very well conducted. Performance metrics are well defined and achieved as shown in the paper.

We thank the reviewer for their generous comment.

***Reviewer #2**:*

- *The paper presents a holistic approach to address the problem of security and privacy in RFID system. The idea is interesting. Usually security and privacy are two different aspects of a system. Sometimes are conflicts. Another issue the authors considered is the resource constraints. I suggest to revise the paper for another round review.*

A paragraph on the RFID security issue added to the introduction. Details of privacy in terms of identifier leakage added to section 3 together with detailed further explanation of how this protocol addresses the privacy issue.

- *The big problem of the current paper is its result. The results presented are mainly focused on resources, e.g., power consumption, area, and running time. But how is the basic function, i.e., the effectiveness in security and privacy is not described.*
  For exmaple, in Section 3.2, the authors discuss many methods of attack, does the approach presented here address the challenges? The authors should give a theorotical analysis of their approach or quantitative verification.

Surprising comments here given the level of detail we have covered on the effectiveness of the security and privacy of the system in the original manuscript in section 4.1 and in the testing of the RNG in section4.2.
To assist the reader easily locate the details, the title of section 4.1 has been changed for extra clarification.
Also, some of the basic properties inherent in a strong cipher have been added to aid understanding.
The additional explanations in section 3 cover relevant explanations relating to effectiveness.

- *Detailed explanation for the figures or tables should be added, such as Fig.1, Fig. 3, and algorithm in page 10.*

Figure 1 is described in the first paragraph of the introduction and is merely intended as a visual aid to readers less familiar with the field.
The description of the protocol was provided diagrammatically in fig.3 and programmatically as an algorithm.
As s requested the descriptive text has been extended together with its relevance to security and privacy.

In the abstract, some abbrevations are not defined, such as RFID, ASIC, and AES.

Definitions added.