ALGSICS — Combining Physics and Cryptography to Enhance Security and Privacy in RFID Systems

N. Bird[1], C. Conrado[1], J. Guajardo[1], S. Maubach[2⋆], G.-J. Schrijen[1], B. Skoric[1], A.M.H. Tombeur[1], P. Thueringer[3], and P. Tuyls[1]

[1] Philips Research Europe, Eindhoven, The Netherlands
{neil.bird,claudine.conrado,jorge.guajardo,geert.jan.schrijen,
boris.skoric,a.m.h.tombeur,pim.tuyls}@philips.com
[2] Department of Mathematics, University of Texas at Brownsville, Brownsville, Texas 78520, USA
stefan.maubach@gmail.com
[3] Philips Semiconductors, Gratkorn, Austria
peter.thueringer@philips.com

Abstract. RFID-tags can be seen as a new generation of bar codes with added functionality. They are becoming very popular tools for identification of products in various applications such as supply-chain management. The widespread deployment of RFID technology will depend to a large extent on its acceptance by the general public. Thus, developing privacy and security technologies specifically suited to the constrained environment of RFID tags continues to be a key problem. In this paper, we introduce several new mechanisms that are cheap to implement or integrate into RFID tags and that at the same time enhance the security of the tags and the privacy of the individual carrying the tags. These new mechanisms are based on physical principles alone or on their combination with cryptographic methods. We also review previous works that use physical principles to provide security and privacy in RFID systems.

Key Words. RFID, privacy, cheap security solutions, sensors, physics and cryptography

1 Introduction

It is envisioned that in the near future RFID tags will be as ubiquitous as bar codes are today and, in fact, even more pervasive as they are expected to be embedded in every object from clothes to posters, from microwaves to food packages, from the smallest to the largest, thus enabling the so-called Internet of Things. The pervasiveness of RFID tags, their ability to carry more information than bar codes, their expected low cost (below 10 US dollar cents), and their lack of need for line of sight communication also pose interesting challenges to

⋆ Work performed while at Philips Research Laboratories, The Netherlands

those interested in their widespread adoption. Such challenges include both privacy and security concerns. On the privacy front, we can identify concerns on the part of consumers who will be carrying tagged objects. In particular, the wireless communication capabilities of RFID tags and their simple functionality (when queried they simply reply with their unique identifier) could make it easier to track people based on tag identifiers as well as to find out consumer preferences clandestinely. Similarly, companies and government organizations will also be more vulnerable to espionage as it will be much easier to gather information on the competition or the enemy and much harder to detect such spying activities. We refer the reader to the surveys of Juels *et al.* [24, 21] for a comprehensive survey of privacy issues in RFID. On the security front, we have the authentication problem. In other words, how a legitimate party can assess whether an RFID tag embedded in an object (and thus the object itself) is authentic or not. The ability to authenticate legitimate tags has direct implications on industry's ability to decrease the counterfeit market, which in 2004 was expected to surpass the 500 billion USD per year mark [18, 46]. Thus, it is clear that solutions for authentication and privacy in RFID systems need to be developed. In fact, as we will see, both the academic and business communities have dedicated a lot of effort to these problems.

Based on the solutions that are known today, we propose to divide security and privacy solutions for RFID into two groups[4]: algorithmic solutions and solutions that either combine cryptography and physical principles, or that simply take advantage of a physical process. By algorithmic solutions, we mean those solutions based on traditional cryptographic mechanisms (e.g. public-key and symmetric-key primitives) or mechanisms which have been developed explicitly for the RFID environment but which make use of some type of cryptographic primitive (even if the primitive in question is not a standardized one, such as the AES[34]). Examples of RFID security solutions based on algorithmic methods include: basic access control through passwords as specified in standards [2, 12], minimalistic cryptography [20] and lightweight protocols [27, 37], solutions based on symmetric-key cryptography (e.g. [13, 11]), hash functions (e.g. [49]), and elliptic curve based solutions [47, 5, 31, 43]. However, at the present moment, solutions based on traditional public-key cryptography, symmetric-key cryptography, and hash functions are out of the question for the cheapest of RFID tags. Notice that the "low cost" requirement is an economics requirement. On the one hand, RFID tags are envisioned as more powerful substitutes for bar codes. On the other hand, if they are to be widely deployed (as bar codes are) then they also need to be in the same price range as a bar code, which only requires ink to be printed on a given item and thus, has cost close to zero.

In the search for cheaper solutions, researchers have turned away from algorithmic approaches. Thus, ideas have been developed such as the `kill` com-

[4] Clearly, it is possible to come up with many different classifications depending on the aim of the study. For example, see [3] for a classification according to the way the reader participates in the authentication protocol.

mand[5], the blocker tag [25, 22] and similar blocking/proxy mechanisms [16, 40]. More engineering oriented approaches have also been introduced such as the IBM clipped tags [28] or distance bounding protocols [33]. Finally, we have begun to see the development of techniques that take advantage of noise in the communication channel between reader and tag to camouflage their communication [8, 9]. We will refer to such approaches as *algsics* methods[6]. In other words, approaches that combine the physical properties of RFID tags (or their environment) with traditional cryptographic primitives or that simply make use of physics to enhance the privacy friendliness and security of tags.

In this paper, we propose several additional mechanisms to enhance privacy and security of RFID tags. Some of our proposals combine environmental information to disable or enable the RFID tag. Although the combination of sensors with RFID tags is not new [38, 36], the realization that such environmental information can be used to enhance privacy is. A second possibility that we explore is the use of delays in revealing a secret key used to later establish a secure communication channel. We would like to point out that we do not claim that all the solutions presented in this paper will constitute stand-alone solutions to the privacy (or security) problems in RFID. Rather, we believe that these solutions will enhance other security and privacy solutions. It is possible that such methodology will in the end be the way towards securing RFID.

The remainder of this contribution is organized as follows. In Sect. 2, we introduce solutions which make use of sensor information to enhance consumer privacy. Section 3 describes a new RFID proxy mechanism that we call a sticky tag. Sticky tags allow the implementation of the `kill` command without its disadvantages by resurrecting the tag wherever and whenever the user considers it safe to do so. In Sect. 4, we explain how we can use time delays in the messages exchanged between the tag and the reader to enhance security. Section 5 summarizes related work proposing *algsics* solutions. Finally, we end with some conclusions in Sect. 6.

2 Physics at the Service of Privacy

In this section, we describe two solutions that enhance the privacy of users carrying objects with embedded RFID tags. They assume the integration of sensors in the RFID tag functionality. Two questions[7] may arise: whether this is possible at all and if this can be done in a battery-free manner. These two questions

[5] Although not application friendly, the `kill` command is a rather effective mechanism to safeguard the privacy of individuals.

[6] The first three letters of algorithmic and the last four of physics.

[7] A third question (how much would such sensor-RFID cost?) will dictate whether such a solution will experience widespread adoption or not. To be successfully adopted at the item level, we require a price in the range of $0.05 per tag [48], otherwise only targeted applications will be able to benefit from this technology. The experience of [38] seems to indicate that today it is possible to build RFID tags including sensor functionality under a $1 but far from the $0.05 mark. Thus, time will only tell whether sensor-RFID will be able to be embedded into everyday objects or not.

can be positively answered as [38, 30, 36] provide evidence of the feasibility of this approach. In what follows, we describe two scenarios which take advantage of embedded sensor functionality in an RFID tag to make the technology more privacy friendly.

2.1 Tag Privacy Protection Via Moisture Dependent Contact

It is envisioned that RFID tags will be embedded in clothing to support activities such as supply chain and retailer product management. In addition, such tags could also support other applications such as smart washing machines. Smart washing machines could be equipped with an RFID reader, which allows the machine to access clothing information. Therefore, the machine could autonomously select a washing program based on that information as well as it could advise the user to remove an item which needs a different washing program. However, including RFID tags in clothing raises privacy concerns to those that wear such garments (see for example [1]). To enhance the privacy of users in this situation, a modified tag is proposed. The tag operates normally prior to sale. At the point of sale, the tag is *disabled*, e.g. by burning a ROM component or wire, which can be done by applying a large amount of power to the tag at the point of sale reader/terminal. Notice that we do not completely kill the tag but rather disable its RF interface. Once in the disabled state, the tag can still function but only if enough conducting moisture is present. This can be done by means of a switch (put in a strategic location such as the tag's antenna) that can only make electric contact if conducting liquid is present. Therefore, the tag is effectively disabled in the street (as long as it stays dry) and can be finally re-enabled when the washing machine pumps water onto the clothes. One may worry that tag readout is hampered by large volumes of water absorbing RF radiation. However, studies have shown that this is not a problem. In particular, it is well known that at low frequencies (in the 10 to 20 MHz range) water is transparent to an RF signal [29, pages 2-6–2-7]. At higher frequencies, the attenuation is significant and it is highly frequency dependent. For example, the study in [10] shows that the attenuation of the signal travelling a distance of 6 cm varies between 7 dB and 23.5 dB for frequencies between 100 MHz and 950 MHz. Notice, however, that there are starting to appear solutions which can perform well in the presence of water and metals at high frequencies as shown in [35]. Finally, for the particular case of an RFID-tag operating in the 13.56 MHz band, a weakening of the signal by 10 dB is deemed acceptable. It can be shown experimentally that at frequencies around 10 MHz the RF signal penetrates 25 cm into salty liquid, which is more than sufficient for the washing machine example.

2.2 Tag Privacy Protection Via Light Controlled Tag Activation

In this section, we describe the idea of controlling access to the powering circuit of the RFID tag via a fully integrated light-sensitive diode which can detect the presence of a laser-beam, e.g., from a laser pointer. This allows for the presence of a secure light-controlled ON/OFF switch on the tag. When the tag is powered

by a reader and a laser-beam is pointed at the light-sensor, a digital ON code is written in the RFID's non-volatile memory. This ON code can, by means of an active switch (e.g., a MOS-transistor), be used to enable the power-supply voltage to parts of the RFID-chip, or enable other circuits to the rest of the chip, in such a way that the chip becomes fully functional. Even when the tag is taken out of the reader field, this ON state remains stored in memory. The tag can also be set in its OFF mode under similar conditions. When the tag is powered by a reader and a laser beam is pointed again to the light-sensor, then an OFF bit will be written in non-volatile memory and the power-supply voltage is disabled from the rest of the tag. In that case, the tag is not functional anymore until it is switched ON again by means of the laser beam. As with the moisture dependent switch, a consumer carrying items with such a modified RFID tag could disable the tag at the point of sale terminal and re-enable it again once he/she is in a safe environment, e.g., home. Thus, future ambient intelligent applications would still be supported and the user's privacy not affected. Clearly, a potential attacker, intending to track someone via the RFID tags that his victim is carrying, would be required to point a light source at each consumer tag that needs to be enabled without this activity being detected by the victim.

Even though such a switch provides the desired functionality of access control to the tag, it suffers from the drawback that a laser beam needs to be pointed to the tag. Thus, this could be considered as undermining one of RFID's main advantages: no line of sight communication. As an alternative, it is also possible to make an RFID tag that will only function if enough environmental light is present. In this case, the user can protect his tags from being read out by an unauthorized party simply by covering the tag such that no light can reach its photo detector or by keeping the tags in the dark. Notice that in many situations, this would not be an unnatural thing to assume (just think of a grocery bag). Alternatively, an RFID tag could be part of a label that can be closed or opened (covered/uncovered) such that light to the tag is blocked or passed, respectively. This way the user is in control of the readout of his tags and can choose when and where her tags may be read. No special reader is required for reading out the RFID tag. The silicon-area required for the light-sensitive diode, including control circuits, can be very small [39]. This results in a cheap protection method that can be, if necessary, combined with other existing privacy enhancing technologies. As a final remark notice that the idea of a light switch is similar in flavor to that of a Faraday cage enclosing a passport that only allows reading of the passport's contents when the metallic cover surrounding the passport is physically opened [23].

3 Sticky Tags and Privacy

Current privacy preserving solutions for RFID are such that they either add cost to the tag by including additional hardware to perform cryptographic functions (such as the computation of a hash function or an encryption of a message with a symmetric or public-key algorithm, e.g. [49, 13, 4]) or require the modification of

current tag specifications to perform additional operations. On the other hand, the most widely available (standardized) solution for privacy concerns is the `kill` command that permanently disables the tag. This solves the privacy problem but it gives up the advantages that RFID tags could provide in other environments. Thus, the idea proposed in this section should be seen as middle ground between the two extremes of rendering tags completely useless with the `kill` command or having additional costs added to current RFID tags. In a way, it can be seen as yet another instantiation (yet with different properties and characteristics) of a privacy sentinel [44] or watchdog tag [16].

The basic idea is to allow the `kill` command to completely disable the RF functionality of the RFID tag but to allow access to the information in the tag via a second interface, which requires proximity to the tag. This second interface could take different forms:

- The simplest instantiation of the second interface would be a contact-based interface. In this case, proximity means "as close as it is physically possible," i.e. touching the disabled tag. We emphasize that adding a contact interface to an RFID tag is not new. However, to the authors' knowledge the idea that a second interface can be used in combination with a second (more powerful) tag to "resurrect" the functionality of the killed tag and guarantee privacy (and security) for the user is novel.
- A second possibility is a modified antenna system which upon receiving the `kill` command changes its configuration. For example, the read-range could be limited by the `kill` command to 1 mm. By a modified antenna system, we mean both an antenna which changes its range (for example, via clipped tags as in [28]) or simply a system consisting of two antennas. The first antenna has a normal range and it gets disabled upon the tag receiving the `kill` command whereas the second antenna has a very short range and it is not affected by the `kill` command.

The second interface can then be used by another device, presumably a more powerful RFID tag both in terms of computational power and security, to access the data in the original RFID tag and communicate in a secure manner with RFID readers. We will refer to this device in what follows as a *sticky tag* to illustrate the fact that we expect such devices to be implemented as a sticky label that adheres to objects whose original RFID tags have been killed. "Sticking" our new more powerful tag on the less powerful tag has the effect of "resurrecting" the tag. Now the user is able to take advantage of the information stored in the killed tag just as if the tag in the object had never been killed. This has the added advantage that the identifier is now transmitted to the readers in a secure manner (if the sticky tag is equipped with cryptographic functionality) or in a more secure environment, since it is the user that decides where and when to resurrect the killed tag. The sticky tag is also envisioned to be re-usable, i.e., users could have a bag of such sticky tags and attach them to objects whose RFID tags have been killed. Once the object's usable life has expired, the user could simply detach the tag and store it for future use after discarding the object. The manufacturer who would also like to check an object's information

once the object is in the recycling phase, could similarly resurrect the originally embedded RFID tag by using a sticky tag as well. Figure 1 depicts an illustration of the system. In particular, a standard reader powers up both antennas, the sticky tag's antenna and the original RFID tag's antenna. Since the RFID tag's antenna has been disabled, only if the sticky tag is present will the reader obtain a response from the RFID tag. Notice that the sticky tag acts as a bridge between the disabled RFID tag and the RFID reader. As such, the sticky tag, when queried, forwards the information residing in the original RFID tag to the reader. Also the sticky tag does not need to have an identifier (e.g. EPC) of its own.

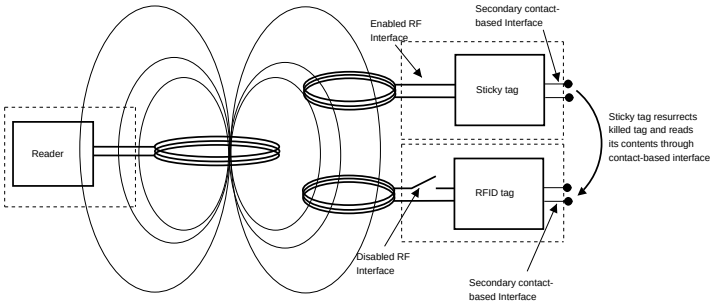


Fig. 1. Sticky tag in the presence of a reader with a secondary contact-based interface

In addition, the sticky tags do not necessarily have to be more powerful devices. A sticky tag, could simply be a much cheaper device without memory or functionality other than reviving the killed RF interface of the original tag. This instantiation would have the advantage of extremely low cost. Finally, an added advantage of sticky tags is that they could be used to resurrect RFID tags with a defective RF interface.

4 Time-Released Secrets and RFID

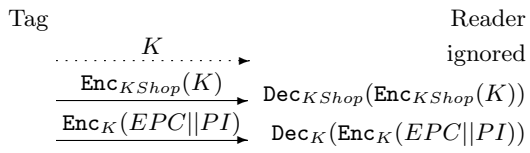
The solution that we present in this section tries to hinder the ability of a reader randomly placed in the street to read or identify a tag when a person passes by. The basic idea consists in implementing an actual physical time delay functionality in the RFID tag. This time delay forces the reading of sensible data to require more time when the tag is in an unprotected environment than when it is in a protected setting. Notice that in this case, the tag itself acts as the agent that releases the secret at a given time in the future. The user or user's devices (e.g. smart home appliances) are the party requesting access to the secret-key information. The unprotected environment may be, for instance, the users path from shop to home. In this case, the chances that an unauthorized reader is able to obtain any information from the tag are decreased thanks to the time delay between a reader requesting information (powering up the tag)

and the time when the tag actually responds. On the other hand, when the tag is in a protected environment, e.g. the shop or the users home, the tag responds without delay, thus not hindering trusted applications. Notice that the delay can be used to send the tag identification number (e.g. an EPC number), product information stored on the tag, or a key used to encrypt the previously mentioned data. One can think of many different configurations for the delay. For example, the delay could occur before any actual data is transmitted from the tag to the reader (after which the message would be transmitted normally) or there could be a permanent delay introduced between the bits (bytes, or any other part) of a message being transmitted. In the latter case, a one-time switch can be used to permanently change a fast-readable tag into a slow-readable tag. In what follows, we describe a particular implementation of the above idea.

An RFID built to support these delays could contain three areas of ROM. The first area stores the EPC and product information PI in Erasable ROM (E-ROM), which is fast-readable. The second area stores the symmetric encryption of the EPC and the PI, $\texttt{Enc}_K(EPC||PI)$, which is also fast-readable, while the third area stores the encryption key K, which is slowly-readable. Before purchase, the shop can quickly read the EPC and the PI from the E-ROM. When the product is sold, this fast reading path is destroyed or blocked, e.g. by erasing the E-ROM. Thus in an unprotected environment only the value $\texttt{Enc}_K(EPC||PI)$ can be read fast by any reader. Notice that this could potentially allow the tracking of the tag via the persistent identifier, $\texttt{Enc}_K(EPC||PI)$, but it does not reveal anything about the EPC or the PI, themselves. Finally, in the users home, a trusted device can slowly read the key K, quickly read the encrypted value $\texttt{Enc}_K(EPC||PI)$, and store the pairs $(\texttt{Enc}_K(EPC||PI), K)$ in a product database. When product information is needed, the home devices can use the quickly sent value $\texttt{Enc}_K(EPC||PI)$ as an identifier to search the database for the key K which can in turn be used to decrypt $\texttt{Enc}_K(EPC||PI)$ to give the EPC and the PI. A variation of the above scheme that does not require a switch is shown in Fig. 2. The advantage here is that the $EPC||PI$ value is never sent in the clear (even in the shop). In addition, there is no need for erasing or destroying the fast-reading path as in the previous system. Notice that in this scheme, the shop is always able to decrypt the encrypted value $\texttt{Enc}_K(EPC||PI)$ since the key K does not change. This allows allows the shop to be able to track whether the user entered their premises with an item for which they know the key (and associated product information).

The tags' tracking problem can be solved if the tags are assumed to have more capabilities, namely, a random number generator and the capability to evaluate hash values. The solution is as described above, except that the value $\texttt{Enc}_K(EPC, PI)$ is sent by the tag only after a challenge-response protocol ensures the tag that the reader knows the key K. This protocol is depicted in Fig. 3. Following the protocol of Fig. 3, we guarantee that only a reader that has time to slowly read the key K (less likely for an attacker) is able to correctly respond to the challenge and learn the value $\texttt{Enc}_K(EPC, PI)$. Notice that in any version of the protocol, an attacker is successful if he is able to keep the attacked tags in its

1. **Common Input:** Dashed arrows indicate delayed transmission of value.
2. **Tag Input:** The tag has stored in memory $\texttt{Enc}_{KShop}(K)$ and $\texttt{Enc}_K(EPC||PI)$ as well as the tag's secret key K.
3. **Honest Reader Input:** An honest shop reader knows the secret key $KShop$.
4. **Protocol in the shop:**



5. **Protocol in safe environment:**

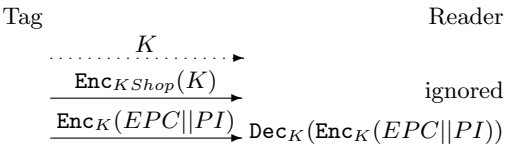


Fig. 2. Delayed tag identification without physical switch

1. **Common Input:** Ability to compute hash functions. Dashed arrows indicate delayed transmission of value. The tag has the ability to generate cryptographically strong random numbers.
2. **Tag Input:** The tag's secret key K.
3. **Protocol:** The protocol involves the exchange of the following messages:

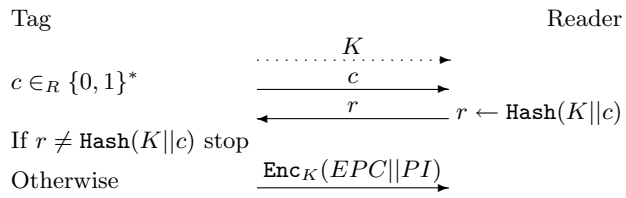


Fig. 3. Delayed tag identification with reader authentication

reader field long enough to obtain the secret key K. Adding the reader authentication step to the protocol comes at the added cost of requiring hardware to compute hashes, which tends to be expensive as shown in [14]. However, similar authentication protocols are possible involving a symmetric-key primitive such as the AES, which occupy less than half of the area required by a hash function [13]. Finally, another simple variant would have the tag send the EPC and/or the PI at normal speed at the shop and with a delay after the product is sold.

Remark 1. The idea of using a delay to enhance security is not new in cryptography. In particular, [32] (see also [42]), timed-release cryptography is introduced as a new primitive. The question that [32] asks is how someone can send an encrypted message into the future. The solution of [32] relies on escrow agents that know shares of the message or the encryption key via a secret-sharing scheme and agree to release the message (or the encryption key) some year(s) into the future. The solution that we present here can be seen as a timed-release system in a different time scale and with different granularity as the systems presented in [32, 42].

5 Related Work

In the past couple of years, we have seen the appearance of *algsics* methodologies in order to enhance the security and privacy friendliness of RFID tags. In this section, we survey these techniques. The *algsics* methods found in the literature can be divided as follows according to the ideas in which they are based:

Privacy sentinel and blocker tags. The concept of the privacy sentinel[8] was originally introduced in [16] while the blocker tag was originally introduced in [25] and its variants in [22]. Similar approaches have also been introduced in [40, 26, 45]. The idea is to provide users with a more powerful trusted device (the privacy sentinel device) that takes care of their privacy, manages their privacy preferences and could, for example, be integrated into a user's cell phone. The watchdog tag's (as it is called in [16]) main purpose is to manage the communication between the reader and the tags that the user is carrying. In addition, the watchdog tag could show warnings to the user, prompt him for authorization, and log all data transfers. Reference [40] extends the watchdog tag concept to include key management, authentication operations, and tag simulation (i.e. the privacy sentinel is able to mimic the operations of the less powerful tags that is managing). Juels et al. [26] consider the problems of tag relabeling, acquisition and ownership transfer. A somewhat different but related approach is the idea of the blocker tag [25] which protects tags from unauthorized reading by interfering with the normal singulation protocol used to identify tags by a reader. Singulation is based on a binary tree algorithm. At each step in the algorithm the reader requests all those tags with their next bit in their identifier equal to one (for the sake of argument) to reply and all those with a zero to stay quite. Eventually, the reader requests all bits and is also able to singulate the desired tag. The blocker tag interferes with this algorithm by always responding with all identifiers effectively simulating all tags or those tags designated within a given range of identifiers. The blocker tag is expected to be cheap and be of the same

[8] This terminology was introduced by Sarma in [44]. In what follows, we will use the term privacy sentinel and watchdog tag interchangeable. Notice that although the particular implementations might differ in specific features, the basic idea is the same: a proxy device that manages the communication of the RFID tag with the external world.

type as a regular RFID tag.

Channel disturbances. Recently, [9, 8] have taken advantage of the noise present (or artificially generated) in the communication channel between reader and tag to enhance the security of their communication. Chabanne and Fumaroli [9] take advantage of the noise in the channel to allow readers and tags to share a secret without a *passive* adversary being able to learn it. Both the readers and tags perform a protocol where information reconciliation and privacy amplification through the use of universal hash functions takes place. The scheme in [8] is somewhat different. It assumes the existence of *noisy tags* owned by the system which inject noise into the tag-reader communication channel. The noisy tags also share a secret key with the reader, which is used to pseudo-randomly generate noise. Whenever the tag sends its secret key to the reader, an eavesdropper will see a signal that is the sum of the signal corresponding to the tag's secret key and the noise injected by the noisy tags. On the other hand, the reader is able to replicate the noise generated by the noisy tags and it is able to subtract the noise signal from the received signal, thus recovering the tag's secret key.

Distance bounding protocols. As noticed in [15] in the context of RFID protocols[9] proximity implies trust. Thus, there has been some work towards developing distance-bounding protocols suited to the RFID environment. Reference [15] finds that looking at the signal noise (in particular to the Fano factor, which is used to approximate signal noise) and to the actual signal strength received by an RFID tag correlates fairly well to the tag distance from the reader. They can use this correlation to decide whether the energy received from the reader antenna can be considered to be in the far field or in the near field. Then, based on this decision, the RFID tag could have a policy of responding to the interrogating reader or not. This distance bounding protocol is combined in [15] with the idea of tiered revelation and authentication in which the tag reveals more and more information according to the level of authentication used by the reader. Reference [15] also noticed that the tiered level can also be associated with the amount of energy emitted by the reader. Thus, for example, a reader that requests more information will also be required to power the tag for a longer period of time while using a longer key size. The work in [17] proposes a new distance bounding protocol based on ultra-wideband pulse communication where the verifier is the reader and the prover the RFID tag, thus, it considers the reverse problem, i.e., the reader wants to verify that it is talking to an honest tag. The protocol makes use of a keyed hash function or symmetric-key primitive to generate a sequence of pseudo-random bits which upon a challenge from the verifier are returned by the prover. Only an honest prover can generate the correct sequence as he also knows the secret key used to generate the sequence.

Changing-tag systems. By changing-tag systems, we mean systems in which the tag or tags change physically. Examples are the works presented in [19, 28] as well as [6]. The work in [19] is interesting in that they suggest to physically split

[9] Cryptographically secure distance bounding protocols date back to 1993 as introduced in [7], however, [15] seems to be the first to suggest a protocol specifically suited to the RFID setting.

the IDs of RFID tags. In particular, their approach envisions splitting global RFID tag identifiers into a class ID (related to the class of objects) and a pure ID (which identifies the specific object, lot number, serial number, etc.). The idea is then for the user to be able to physically remove the class ID from the object and at a later stage attach a second tag with a different global ID, which might be unique in the user environment but not globally. The authors in [19] also notice that the same effect (changing IDs) can be achieved by using rewritable memory in an RFID tag. Reference [6] considers systems in which an object is associated with multiple RFID tags. Then, chaffing and winnowing in the sense of [41] can be used to disguise the true identity of the object[10]. In [28], the authors propose to physically disconnect the antenna and the chip in an RFID tag. In addition to allowing for visual confirmation (on the part of the consumer) that the tag communication capabilities have been disabled, it allows for this functionality to be "pasted" back on if the user desires to resurrect the RFID tag functionality once he/she is in a safe environment.

Tag switches. The work in [50] explores the idea of physically deactivating a tag via a physical bit-dependent switch. If the bit is set to one, the RFID tag answers as usual to a reader query whereas if the bit is set to zero, then the tag is deactivated until the user activates it again. The idea is based on the assumption that only someone with physical access (or close proximity) to the tag can activate it again. Thus, consumer privacy is safeguarded and at the same time, tag functionality is preserved for privacy-friendly environments. The author describes three possible implementations of the physically changeable bit (PCB). The first implementation consists in physically (dis)connecting the antenna from the chip, much in the same way as the clipped tags in [28]. Other methods include: including electrically erasable ROM memory in the tag, writing or erasing the PCB depending on user wishes, and using "magnetic bits" in the tags to represent (and set or unset) the PCB bits.

6 Concluding Remarks

In this paper, we have discussed and introduce solutions which show how the physics present in RFID systems can be leveraged to enhance security and privacy solutions at a low cost. We believe that this approach is promising in the sense that the cheapest RFID tags are constrained devices which will not allow (due to pricing requirements) the implementation of expensive cryptographic primitives. Thus, alternative methods to provide security need to be developed. We point out, as it has been done also in previous works, that the security guarantees provided by *algsics* methods are not the same as those provided by crypto protocols using sophisticated primitives (for example, most *algsics* solutions provide security in a weak model against passive adversaries). However, it is also true that in many cases such guarantees might be enough. For example, it might not be feasible to implement an active attack without easily being discovered.

[10] Reference [48] is the first to notice that chaffing and winnowing can be used in the RFID context but it assumes that the readers will be the ones generating the chaff.

Finally, the future might show that *algsics* solutions turn out to be effective additional countermeasures against attacks. In other words, when combined with other more sophisticated methods, the overall security (or privacy) guarantees of the system are enhanced.

Acknowledgements

Thanks to the anonymous referees for comments that help improved the contents and presentation of the paper. We also would like to thank Tim Kerins and Klaus Kursawe for their comments on a preliminary version of the paper. The observation that the protocol in Fig. 2 could pose a privacy problem to the user since the shop is always able to obtain the EPC and PI of the tag is also due to Klaus.

References

1. K. Albrecht. CASPIAN Press Release. Available at `http://www.boycottbenetton.com/PR_030407.html`, April 9th, 2003.
2. Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA. *13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0*, February 3rd, 2003. Technical Report. Available at `http://www.epcglobalinc.org/standards_technology/specifications.html`.
3. G. Avoine. *Cryptography in Radio Frequency Identification and Fair Exchange Protocols*. PhD thesis, EPFL, Lausanne, Switzerland, 2005. Available from `http://www.avoine.net/`.
4. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An Elliptic Curve Processor Suitable For RFID-Tags. Cryptology ePrint Archive, Report 2006/227, 2006. Available at `http://eprint.iacr.org/`.
5. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public key cryptography for RFID-tags. Printed handout of Workshop on RFID Security – RFIDSec 06, pages 61–76. ECRYPT Network of Excellence, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
6. L. Bolotnyy and G. Robins. Multi-tag radio frequency identification systems. In *Workshop on Automatic Identification Advanced Technologies — AutoID 2005*, pages 83–88, 345 E. 47th St, New York, NY 10017, USA, October, 2005. IEEE .
7. S. Brands and D. Chaum. Distance-bounding protocols (extended abstract). In T. Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, volume 765 of *LNCS*, pages 344–359. Springer-Verlag, 1994.
8. C. Castelluccia and G. Avoine. Noisy tags: A pretty good key exchange protocol for RFID tags. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS 2006*, volume 3928 of *LNCS*, pages 289–299, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.
9. H. Chabanne and G. Fumaroli. Noisy Cryptographic Protocols for Low-Cost RFID Tags. *IEEE Transactions on Information Theory*, 52(8):3562–3566, August 2006.

10. Y. Chan, M. Q.-H. Meng, K.-L. Wu, and X. Wang. Experimental Study of Radiation Efficiency from an Ingested Source inside a Human Body Model. In *IEEE Annual International Conference of the Engineering in Medicine and Bilogy Society — IEEE-EMBS 2005*, pages 7754–7757, September 1st-4th, 2005.
11. S. Dominikus, E. Oswald, and M. Feldhofer. Symmetric Authentication for RFID Systems in Practice. Printed handout of Workshop on RFID and Light-Weight Crypto, pages 25–31. ECRYPT Network of Excellence, July 13-15, 2005. Available at `http://www.iaik.tugraz.at/research/krypto/events/index.php`.
12. EPCGlobal Inc., Princeton Pike Corporate Center, Suite 202 Lawrenceville, NJ 08648, USA. *EPC^{TM} Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz – Version 1.0.9*, January 31st, 2005. Available at `http://www.epcglobalinc.org/standards_technology/specifications.html`.
13. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems — CHES 2004*, volume 3156 of *LNCS*, pages 357–370. Springer, 2004.
14. M. Feldhofer and C. Rechberger. A case against currently used hash functions in RFID protocols. Printed handout of Workshop on RFID Security – RFIDSec 06, pages 109–122. ECRYPT Network of Excellence, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
15. K. P. Fishkin, S. Roy, and B. Jiang. Some Methods for Privacy in RFID Communication. In C. Castelluccia, H. Hartenstein, C. Paar, and D. Westhoff, editors, *Security in Ad-hoc and Sensor Networks — ESAS 2004*, volume 3313 of *LNCS*, pages 42–53. Springer, 2005.
16. C. Floerkemeier, R. Schneider, and M. Langheinrich. Scanning with a purpose – supporting the fair information principles in RFID protocols. In H. Murakami, H. Nakashima, H. Tokuda, and M. Yasumura, editors, *International Symposium on Ubiquitous Computing Systems – UCS 2004*, volume 3598 of *LNCS*, pages 214–231, Tokyo, Japan, November 2004. Springer-Verlag.
17. G. Hancke and M. Kuhn. An RFID distance bounding protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 67–73, Los Alamitos, CA, USA, September 2005. IEEE Computer Society.
18. ICC Policy Statement: The fight against piracy and counterfeiting of intellectual property. Submitted to the 35th World Congress, Marrakech, Document no 450/986, ICC, June 1st, 2004.
19. S. Inoue and H. Yasuura. RFID privacy using user-controllable uniqueness. RFID Privacy Workshop, November 2003.
20. A. Juels. Minimalist Cryptography for Low-Cost RFID Tags. In C. Blundo and S. Cimato, editors, *Security in Communication Networks — SCN 2004. Revised Selected Papers*, volume LNCS 3352, pages 149–164. Springer-Verlag, September 8-10, 2004.
21. A. Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006. Extended version available from `http://www.rsasecurity.com/rsalabs/node.asp?id=2029`.
22. A. Juels and J. G. Brainard. Soft blocking: flexible blocker tags on the cheap. In V. Atluri, P. F. Syverson, and S. De Capitani di Vimercati, editors, *ACM Workshop on Privacy in the Electronic Society — WPES 2004*, pages 1–7. ACM Press, October 28, 2004.

23. A. Juels, D. Molnar, and D. Wagner. Security and Privacy Issues in E-passports. In G. Tsudik, D. Gollmann, and L. Gong, editors, *IEEE International Conference on Security and Privacy for Emerging Areas in Communications Networks — SecureComm 2005*, pages 74–88, 345 E. 47th St, New York, NY 10017, USA, September 05-09, 2005. IEEE Computer Society. Extended version IACR Cryptology ePrint Archive Report 2005/095, available at `http://eprint.iacr.org/2005/095`.
24. A. Juels, R. Pappu, and S. Garfinkel. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy*, 3(3):34–43, May/June 2005. Extended version available from `http://www.rsasecurity.com/rsalabs/node.asp?id=2029`.
25. A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In S. Jajodia, V. Atluri, and T. Jaeger, editors, *ACM Conference on Computer and Communications Security — CCS 2003*, pages 103–111. ACM Press, October 27-30, 2003.
26. A. Juels, P. Syverson, and D. Bailey. High-Power Proxies for Enhancing RFID Privacy and Utility. In G. Danezis and D. Martin, editors, *Privacy Enhancing Technologies — PET 2005*, volume 3856 of *LNCS*, pages 210–226. Springer, 2005.
27. A. Juels and S.A. Weis. Authenticating Pervasive Devices with Human Protocols. In V. Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3126 of *LNCS*, pages 293–308, Berlin, Germany, August 2005. Springer-Verlag.
28. G. Karjoth and P. Moskowitz. Disabling RFID tags with visible confirmation: Clipped tags are silenced. In *Workshop on Privacy in the Electronic Society – WPES*, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
29. T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips. *Draft Special Publication 800-98, Guidance for Securing Radio Frequency Identification (RFID) Systems*. National Institute for Standards and Technology, Gaithersburg, MD, USA, September 2006. Available for download at `http://csrc.nist.gov/`.
30. H. Kitayoshi and K. Sawaya. Long range passive rfid-tag for sensor networks. In *IEEE 62nd Vehicular Technology Conference — VTC-2005*, pages 2696–2700, Los Alamitos, CA, USA, 25-28 Sept., 2005. IEEE Computer Society.
31. S. S. Kumar and C. Paar. Are standards compliant elliptic curve cryptosystems feasible on RFID? Printed handout of Workshop on RFID Security – RFIDSec 06, pages 41–60. ECRYPT Network of Excellence, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
32. T. C. May. Timed-release crypto. Posting to the Cypherpunks Mailing List, February 10th, 1993. Available at `http://cypherpunks.venona.com/date/1993/02/msg00129.html`.
33. J. Munilla, A. Ortiz, and A. Peinado. Distance bounding protocols with void-challenges for RFID. Printed handout of Workshop on RFID Security – RFIDSec 06, pages 15–26. ECRYPT Network of Excellence, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
34. National Institute for Standards and Technology, Gaithersburg, MD, USA. *FIPS 197: Advanced Encryption Standard (AES)*, November 2001. Available for download at `http://csrc.nist.gov/encryption`.
35. KU Information & Telecommunication Technology Center. The University of Kansas. UHF KU-RFID Tag, 2006. Available at `http://www.rfidalliancelab.org/publications/ittc_press_release.shtml`.
36. K. Opasjumruskit, T. Thanthipwan, O. Sathusen, P. Sirinamarattana, P. Gadmanee, E. Pootarapan, N. Wongkomet, A. Thanachayanont, and M. Thamsirianunt. Self-powered wireless temperature sensors exploit RFID technology. *IEEE Pervasive Computing*, 5(1):54–61, Jan.-March 2006.

37. P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. Printed handout of Workshop on RFID Security – RFIDSec 06, pages 137–148. ECRYPT Network of Excellence, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
38. M. Philipose, J.R. Smith, B. Jiang, A. Mamishev, Sumit R., and K Sundara-Rajan. Battery-Free Wireless Identification and Sensing. *IEEE Pervasive Computing*, 4(1):37–45, January-March 2005.
39. S. Radovanovic, A.J. Annema, and B. Nauta. High-speed lateral polysilicon photodiode in standard CMOS technology. In *33rd European Solid-State Circuits Conference — ESSDERC'03*, pages 521–524. IEEE Computer Society, 16-18 Sept., 2003.
40. M. Rieback, B. Crispo, and A. Tanenbaum. RFID guardian: A battery-powered mobile device for RFID privacy management. In C. Boyd and J. M. González Nieto, editors, *Australasian Conference on Information Security and Privacy – ACISP'05*, volume 3574 of *LNCS*, pages 184–194, Brisbane, Australia, July 2005. Springer-Verlag.
41. R. L. Rivest. Chaffing and Winnowing: Confidentiality without Encryption. *CryptoBytes*, 4(1):12–17, Summer 1998.
42. R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release Crypto. LCS technical memo MIT/LCS/TR-684, MIT, February 1996.
43. K. Sakiyama, L. Batina, N. Mentens, B. Preneel, and I. Verbauwhede. Small-footprint ALU for public-key processors for pervasive security. Printed handout of Workshop on RFID Security – RFIDSec 06, pages 77–88. ECRYPT Network of Excellence, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
44. S. Sarma. Some issues related to rfid and security. Introductory Talk – RFIDSec 06, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
45. A. Soppera and T. Burbridge. Off by default - RAT: RFID acceptor tag. Printed handout of Workshop on RFID Security – RFIDSec 06, pages 151–166. ECRYPT Network of Excellence, July 2006. Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`.
46. T. Staake, F. Thiesse, and E. Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. In A. Omicini H. Haddad, L. M. Liebrock and R. L. Wainwright, editors, *ACM Symposium on Applied Computing — SAC 2005*, pages 1607–1612. ACM Press, March 13-17 2005.
47. P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, *Topics in Cryptology - CT-RSA 2006*, volume 3860 of *LNCS*, pages 115–131, Berlin, Germany, February 13-17 2006. Springer-Verlag.
48. S. Weis. Security and privacy in radio-frequency identification devices. Master thesis, Massachusetts Institute of Technology (MIT), Massachusetts, USA, May 2003.
49. S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, *First International Conference on Security in Pervasive Computing — SPC 2003*, volume 2802 of *LNCS*, pages 201–212. Springer-Verlag, March 2003.
50. C. C. Zou. PCB: Physically Changeable Bit for Preserving Privacy in Low-End RFID Tags. RFID White Paper Library, RFID Journal, May 2006.