ALGSICS - Combining physics and cryptography to enhance security and privacy in RFID systems

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

Neil Bird[1], Claudine Conrado[1], Jorge Guajardo[1], Stefan Maubach[2,⋆], Geert-Jan Schrijen[1], Boris Skoric[1], Anton M.H. Tombeur[1], Peter Thueringer[3], and Pim 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] IMAPP, Radboud University Nijmegen, Nijmegen, The Netherlands
s.maubach@science.ru.nl
[3] NXP, Gratkorn, Austria
peter.thueringer@nxp.com

Abstract. 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 their security and privacy properties. Our aim is to provide solutions that make use of existing (or expected) functionality on the tag or that are inherently cheap and thus, enhance the privacy friendliness of the technology "almost" for free. Our proposals, for example, make use of environmental information (presence of light temperature, humidity, etc.) to disable or enable the RFID tag. 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 also introduce the idea of a "sticky tag," which can be used to re-enable a disabled (or killed) tag whenever the user considers it to be safe. We discuss the security and describe usage scenarios for all solutions. Finally, we review previous works that use physical principles to provide security and privacy in RFID systems.

Keywords: RFID, privacy, cheap solutions, sensors, physics and crypto.

1 Introduction

The pervasiveness of RFID tags, their ability to carry more information than bar codes, their expected low cost (below US$0.10), and their lack of need for line of sight communication pose interesting challenges to 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 a unique identifier) could make it easier to track people based on tag identifiers as well as to find out consumer preferences clandestinely. Similarly,

⋆ Work performed while at Philips Research Laboratories, The Netherlands.

F. Stajano et al. (Eds.): ESAS 2007, LNCS 4572, pp. 187–202, 2007.

companies and defense 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. On the security front, there is the authentication problem, i.e., how a legitimate party can assess whether an RFID tag associated with an object (and thus the object) 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 [1].

Based on the solutions that are known today, we propose to divide security and privacy solutions for RFID into two groups: 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 solutions based on cryptographic mechanisms. Examples include: basic access control through passwords, minimalistic cryptography [2] and lightweight protocols [3], solutions based on symmetric-key cryptography (e.g. [4,5]), hash functions (e.g. [6]), and elliptic curve based solutions [7,8]. 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 if RFID tags 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` command, the blocker tag [9,10] and similar blocking/proxy mechanisms [11,12]. More engineering oriented approaches have also been introduced such as the IBM clipped tags [13], distance bounding protocols [14], or techniques that take advantage of noise in the communication channel to camouflage the reader-tag communication [15,16]. We will refer to all such approaches as *algsics* methods.

It is clear that the major advantages of tagging objects with RFID tags, as Juels [17] points out, are the abilities to uniquely identify objects and to automate tasks that previously had to be performed by a human. This will result in clear advantages to manufacturers of products or service providers. However, one may ask what is the general public case for tagging everyday objects? RFID tags also have the potential to enable new applications (only limited by the reader's imagination) such as smart refrigerators that are able to tell when a product's life has expired or when you have run out of milk, washing machines that simply need to be started and know based on clothing information what wash cycle it should run, intelligent posters that allow a consumer to know in which cinemas and at what times a movie is playing, and finally, as a an enabling technology in smart homes for the elderly and the cognitively impaired [17]. However, the possibilities offered by the wide deployment of RFID technology will only become true if the privacy of individuals is properly protected.

CONTRIBUTIONS. In this paper, we propose several additional mechanisms to enhance privacy and security of RFID tags. Our aim is to provide privacy

solutions which make use of existing (or expected) functionality on the tag or that are inherently cheap and thus, enhance the privacy friendliness of the technology "almost" for free. Some of our proposals make use of environmental information to disable or enable the RFID tag. Although the combination of sensors with RFID tags is not new [18,19], the realization that such environmental information can be used to enhance privacy is new and to the authors' knowledge has not been proposed before. 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 re-enabling 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 solutions that enhance the privacy of users carrying objects with associated RFID tags. We assume that guidelines for RFID privacy have been followed, such as placing the tag on the outside of the object and that this position has been clearly identified. This also allows consumers to have the option of removing the tag if desired. We also assume the integration of sensors in the RFID tag functionality. This assumption gives rise to several questions. The first question we ask is if this approach is feasible at all from a technical point of view and if such a sensor-RFID tag can be implemented in a battery-free manner. The answer to these two questions is positive as [18,20,19] provide evidence of the feasibility of this approach. The second question regards price. How much such a sensor-RFID tag costs will in the end 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 US$0.05 per tag [21]. The experience of [18] seems to indicate that today it is possible to build RFID tags including sensor functionality under a US$1 but far from the US$0.05 mark. In fact, some are already available, albeit only battery powered ones [22]. In the end, we expect that the continued decrease in silicon prices as well as consumer and customer requirements for additional functionality will enable the integration of sensor functionality into cheap RFID tags. In the following, we describe several scenarios which take advantage of embedded sensor functionality in an RFID tag to make the technology more privacy friendly. The basic idea

in all the solutions is to use environmental information as an on/off switch. By environmental information, we mean data from temperature, light presence (or absence), or humidity readings of the environment surrounding the sensor-RFID tag. Depending on the setting and the application, a certain sensor might be more appropriate than another. Then, whenever the chosen environmental information attains a certain value (or range of values) or the user "creates" the right environmental conditions, the RFID tag is able to transmit data to an interrogating reader. Otherwise, the tag functions as if it was completely disabled. In the next sections, we describe usage scenarios for particular sensors and we discuss advantages and disadvantages of such solutions.

2.1 Tag Privacy Protection Via Light Controlled Tag Activation

IDEA. The idea is to control 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 into 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, an OFF bit will be written in non-volatile memory and the power-supply voltage will be 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. 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 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, a wallet, or a purse). 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 his 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 [23]. This results in a cheap protection method that can be, if necessary, combined with other existing privacy enhancing technologies.

DISCUSSION. A consumer carrying items with such a modified RFID tag disables the tag at the point of sale terminal and re-enables it again once he/she is in a safe environment, e.g., at home. Thus, future ambient intelligent applications are still supported and the user's privacy not affected. Another example application of such a solution is in the tagging of bank notes. By turning off the RFID interface in his/her bank notes via their light-enabled switch, a user very simply avoids tracking. Another attack that is prevented is that in which a thief targets passers-by who are carrying 500 Euro notes in their wallets [24] by simply reading their tags. On the other hand, any person or organization desiring to verify the authenticity of the bank note can do so upon obtaining the bank note as a form of payment for a service or product. Notice that the light enabled switch does not support all the properties put forward by Juels and Pappu in [24]. In particular, it would only allow law enforcement agencies (or any authorized entity) to trace bank notes after detaining a potential suspect and not in an unobtrusive manner as suggested in [24]. Finally, 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.

2.2 Tag Privacy Protection Via Moisture Dependent Contact and Other Sensors

IDEA. Inclusion of RFID tags in clothing has been proposed as a means to support activities such as supply chain and retailer product management. However, including RFID tags in clothing raises privacy concerns to those that wear such garments (see for example [25]). 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 [26, pages 2-6–2-7]. At higher frequencies, the attenuation is significant and it is highly frequency dependent. For example, the study in [27] shows that the attenuation of the signal traveling 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 solutions starting to appear that can perform well in the presence of water and metals at high frequencies as shown in [28]. 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.

DISCUSSION. In addition to supporting activities such as supply chain and retailer product management, RFID tags associated with clothing items 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 or it could advise the user to remove an item that needs a different washing program via an alarm. A second example of a sensor used to enhance privacy is a temperature sensor for a smart refrigerator application. In this setting, RFID tags could be allowed to be read only in certain temperature ranges. Thus, when the groceries are in the refrigerator at a certain temperature range, the RFID tags associated with the groceries would be readable and otherwise not. Such an RFID tag would enable applications as diverse as : checking whether a product has been at the correct temperature during the whole supply-chain or placing an automatic order when the user has run out of certain food items. On the other hand, one can argue that whenever the temperature outside was also in the range of the refrigerator temperature, the RFID tag would be allowed to transmit and thus, the user would be traceable. However, the ability that an attacker has to trace someone would be highly dependent on weather conditions and not on the attacker's choice. This diminishes the attacker's tracing abilities or forces him to change environmental conditions around his target. In this case, security is also highly dependent on how close the attacker can get to his target and stay there for extended periods of time. Clearly the closer the attacker is to his target, the easier it is for him to be discovered but also the more successful he will be in cheating the system. Finally, notice that a single sensor will probably not be applicable to all scenarios, with the possible exception of the light sensor. For example, a humidity sensor might be suitable for clothing but not for electronic items, and similarly temperature sensors might work well with food but not with clothing. Light sensors, on the other hand, seem to allow a wide range of applications.

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 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 can provide in other applications. Thus, the idea proposed in this section can 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. It can also be seen as yet another instantiation (with different properties and characteristics) of a privacy sentinel [29] or watchdog tag [11].

IDEA. 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. Notice that the resurrecting functionality is different from the resurrecting duckling security policy of Stajano and Anderson [30], where a node in an ad-hoc network establishes a secure channel after being "resurrected" by an adjacent node. 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 [13]) 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. Notice that this instantiation might succumb to relay attacks. 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. Figure **??** 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 must not have an identifier (e.g. EPC) of its own.

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.

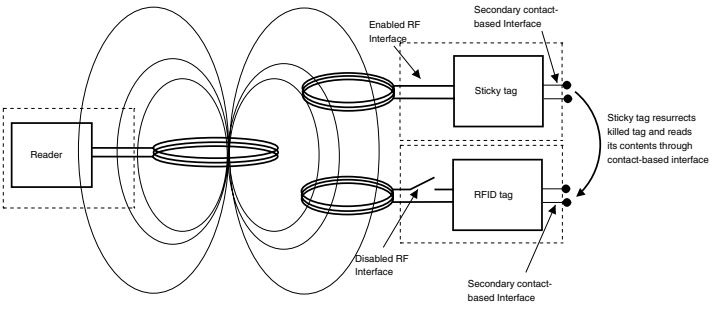

Fig. 1. Sticky tag in the presence of a reader with a secondary contact-based interface

DISCUSSION. As usual, at check-out the RFID tag is disabled. However, by attaching a sticky tag to the killed 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 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. A final usage case is the scenario in which a user returns a product to the shop because of regular maintenance, repair, or malfunction. In this case, the shop can use a sticky tag to read the product information available in the original tag associated with the object. Admittedly, a main issue with the sticky tags is usability. Can we expect that users will tag their groceries so that they can make use of their smart refrigerator? Notice that owning a smart appliance implies that the user has an interest in using the intelligence features in the refrigerator, otherwise he would not have bought it in the first place. In addition, attaching a sticky tag both at home and at the repair shop scenarios does not need to be a cumbersome activity. It could be similar to the customary practice of detaching anti-theft tags at clothing stores once an item has been sold or to adding a pricing tag to an item as it had been done for years (and in some places it is still done) before the widespread adoption of bar codes. On the other hand, a main advantage of the sticky tags is that they are an opt-in solution. By default, we are safeguarding individual's privacy and if they desire they can regain many of the advantages that RFID offers. Sticky tags would be best suited to objects that are meant for home use once they have bought (e.g., groceries, TVs, DVD players, etc.). Similarly, using sticky tags for clothing for example, would imply that the user needs to remember to detach the sticky tag from his clothing before going

out. Otherwise, he could risk traceability. This seems a burden not likely to be accepted by most people.

4 Time-Released Secrets and RFID

IDEA. This solution tries to hinder the ability of a reader randomly placed in the street to read or identify a tag when a person passes by. This achieved by implementing an actual physical time delay functionality in the RFID tag. This time delay forces the reading of sensitive data to require more time when the tag is in an unprotected environment than when it is in a protected setting. 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 user's 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 user's home, the tag responds without delay, thus not hindering trusted applications. Notice that the delay can be used to send the tag identification 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

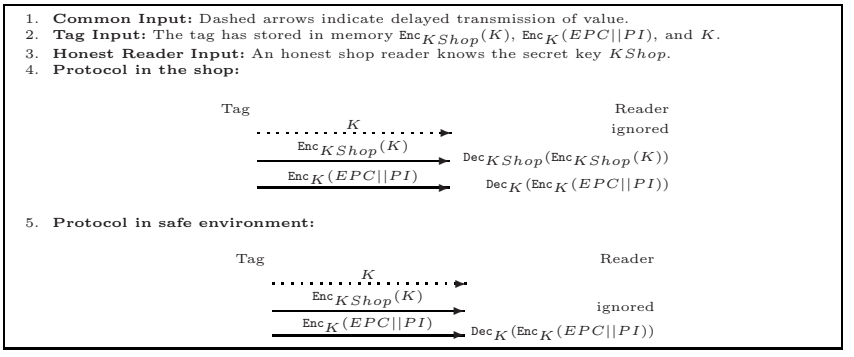

Fig. 2. Delayed tag identification without physical switch

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. 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. This, however, requires hardware to support a hash function or a dedicated encryption module (as opposed to just memory). 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.

DISCUSSION. The protocols presented here seem to be well suited for many applications. However, we would like to point out that in any version of the protocol, an attacker is successful if he is able to keep the attacked tags in its reader field long enough to obtain the secret key K. In particular, if the tag is stationary for long periods of time, then the attacker can seriously compromise the privacy of the user. Clearly, then security and usability can be traded off against each other. The longer it takes for the tag to release the next bit of its secret key, the longer the attacker will have to be present in the surrounding of the tag and thus, the less likely that he will obtain the whole secret information. On the other hand, the longer it takes for the tag to release the secret key, the longer that the legitimate user will have to wait when he wants to access the tag's encrypted information at home[1]. Given this limitation, delays appear to be well suited for objects that will not be carried outside the safe environment of the user very often (e.g., food, TVs, home electronics, etc.). On the other hand, tags incorporated into clothing would be less likely to be a privacy problem if using different privacy enhancing solutions such as those based on sensors. We end by noticing that the assumption that the attacker tends to be stationary and thus unable to query tags for extended periods of time is not new in the RFID setting (see for example [2]).

[1] This is only true the first time that the tag is queried at home.

Remark 1. The idea of using a delay to enhance security is not new in cryptography. In particular, May [31] introduces timed-release cryptography as a new primitive. 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 system of [31]. In the context of RFID security, Juels [2] seems to be the first to use delays to limit the ability of an attacker to perform successive queries to a tag by using a hardware-based throttling mechanism for his pseudonyms scheme. However,schemes such as the ones presented in this section and the ability to turn on and off the delays were not discussed.

5 Related Work

In this section, we survey other *algsics* methodologies found in the literature. They are organized according to the ideas in which they are based.

PRIVACY SENTINEL AND BLOCKER TAGS. The term "privacy sentinel" was introduced by Sarma in [29]. However, the concept of a proxy device that manages the communication of the RFID tag with the external world was originally introduced by Floerkemeier et al. [11] while the blocker tag was originally introduced by Juels et al. [9] (see also [10]). In what follows, we will use the term privacy sentinel and watchdog tag interchangeable. Similar approaches have also been introduced in [12,32,33]. 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 [11]) 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 [12] 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. [32] consider the problems of tag relabeling, acquisition and ownership transfer. A somewhat different but related approach is the idea of the blocker tag [9] 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 type as a regular RFID tag.

CHANNEL DISTURBANCES. Recently, [16,15] 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. Reference [16] takes 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. Readers and tags perform a protocol where information reconciliation and privacy amplification take place through the use of universal hash functions. The scheme in [15] is somewhat different. It assumes the existence of *noisy tags* owned by the system which inject noise into the 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 noisy tags' noise and it is able to subtract the noise signal from the received signal, thus recovering the tag's secret key. A similar approach to [15] is presented in [34]. The difference is that the authors do not assume the presence of a noisy tag but rather assume that the reader and tag can synchronize their communications. Both tag and reader send a pseudo-random sequence to each other, whenever their bits are different an eavesdropper will not know which bit was sent by the tag and which bit by the reader. On the other hand, both the tag and the reader are able to obtain each others keys.

DISTANCE BOUNDING PROTOCOLS. Cryptographically secure distance bounding protocols date back to 1993 as introduced in [35]. However, [36] seems to be the first to suggest a protocol specifically suited to the RFID setting. Notice that in the context of RFID protocols proximity implies trust. Fishkin et al. [36] find that looking at the signal noise (in particular to the Fano factor, which is used to approximate signal noise) and at the actual signal strength received by an RFID tag correlates fairly well with 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 [36] 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 [36] 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 [37] 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 [38,13] as well as [39]. The work in [38] is interesting in that they suggest to physically split 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 [38] also notice that the same effect (changing IDs) can be achieved by using re-writable memory in an RFID tag. Reference [39] considers systems in which an object is associated with multiple RFID tags. Then, chaffing and winnowing in the sense of [40] can be used to disguise the true identity of the object. Notice that Weis [21] was the first to notice that chaffing and winnowing can be used in the RFID context but he assumed that the readers would be the ones generating the chaff. In [13], 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 [41] 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 [13]. 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. In this category, we also include the `kill` command, which works by completely disabling the tag if the tag is presented with the correct password. Although not application friendly, the `kill` command is a rather effective mechanism to safeguard individuals' privacy.

6 Concluding Remarks

In this paper, we have discussed and introduced solutions that 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. 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 being discovered. 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.

References

1. Staake, T., Thiesse, F., Fleisch, E.: Extending the EPC Network — The Potential of RFID in Anti-Counterfeiting. In: Haddad, H., Liebrock, L.M., Wainwright, A.O. (eds.) SAC 2005, March 13-17, 2005, ACM Press, New York (2005)
2. Juels, A.: Minimalist Cryptography for Low-Cost RFID Tags. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 149–164. Springer, Heidelberg (2005)
3. Juels, A., Weis, S.: Authenticating Pervasive Devices with Human Protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 293–308. Springer, Heidelberg (2005)
4. Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong Authentication for RFID Systems Using the AES Algorithm. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 357–370. Springer, Heidelberg (2004)
5. Dominikus, S., Oswald, E., Feldhofer, M.: Symmetric Authentication for RFID Systems in Practice. Printed handout of Workshop on RFID and Light-Weight Crypto, pp. 25–31. ECRYPT Network of Excellence (July 13-15, 2005)
6. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) SPC 2003. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004)
7. Tuyls, P., Batina, L.: RFID-tags for Anti-Counterfeiting. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 115–131. Springer, Heidelberg (2006)
8. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: Public-Key Cryptography for RFID-Tags. In: PerCom 2007 Workshops. IEEE Conference on Pervasive Computing and Communications Workshops, New York, March 19-23, 2007, IEEE Computer Society, Los Alamitos (2007)
9. Juels, A., Rivest, R.L., Szydlo, M.: The blocker tag: selective blocking of RFID tags for consumer privacy. In: Jajodia, S., Atluri, V., Jaeger, T. (eds.) CCS 2003. ACM Conference on Computer and Communications Security, October 27-30, 2003, pp. 103–111. ACM Press, New York (2003)
10. Juels, A., Brainard, J.G.: Soft blocking: flexible blocker tags on the cheap. In: Atluri, V., Syverson, P.F., di Vimercati, S.D.C. (eds.) WPES 2004. ACM Workshop on Privacy in the Electronic Society, October 28, 2004, pp. 1–7. ACM Press, New York (2004)

11. Floerkemeier, C., Schneider, R., Langheinrich, M.: Scanning with a purpose – supporting the fair information principles in RFID protocols. In: Murakami, H., Nakashima, H., Tokuda, H., Yasumura, M. (eds.) UCS 2004. LNCS, vol. 3598, pp. 214–231. Springer, Heidelberg (2005)
12. Rieback, M., Crispo, B., Tanenbaum, A.: RFID guardian: A battery-powered mobile device for RFID privacy management. In: Boyd, C., González Nieto, J.M. (eds.) Information Security and Privacy. LNCS, vol. 3574, pp. 184–194. Springer, Heidelberg (2005)
13. Karjoth, G., Moskowitz, P.: Disabling RFID tags with visible confirmation: Clipped tags are silenced. In: WPES. Workshop on Privacy in the Electronic Society, Alexandria, Virginia, November 2005, ACM Press, New York (2005)
14. Munilla, J., Ortiz, A., Peinado, A.: Distance bounding protocols with void-challenges for RFID. Printed handout of Workshop on RFID Security – RFIDSec 06, pp. 15–26. ECRYPT Network of Excellence (July 2006)
15. Castelluccia, C., Avoine, G.: Noisy tags: A pretty good key exchange protocol for RFID tags. In: Domingo-Ferrer, J., Posegga, J., Schreckling, D. (eds.) CARDIS 2006. LNCS, vol. 3928, pp. 289–299. Springer, Heidelberg (2006)
16. Chabanne, H., Fumaroli, G.: Noisy Cryptographic Protocols for Low-Cost RFID Tags. IEEE Transactions on Information Theory 52(8), 3562–3566 (2006)
17. Juels, A.: RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications 24(2), 381–394 (2006), Extended version available from `http://www.rsasecurity.com/rsalabs/node.asp?id=2029`
18. Philipose, M., Smith, J., Jiang, B., Mamishev, A.: Battery-Free Wireless Identification and Sensing. IEEE Pervasive Computing 4(1), 37–45 (2005)
19. Opasjumruskit, K., Thanthipwan, T., Sathusen, O., Sirinamarattana, P., Gadmanee, P., Pootarapan, E., Wongkomet, N., Thanachayanont, A., Thamsirianunt, M.: Self-powered wireless temperature sensors exploit RFID technology. IEEE Pervasive Computing 5(1), 54–61 (2006)
20. Kitayoshi, H., Sawaya, K.: Long range passive rfid-tag for sensor networks. In: IEEE 62nd Vehicular Technology Conference — VTC-2005, September 25-28, 2005, pp. 2696–2700. IEEE Computer Society, Los Alamitos (2005)
21. Weis, S.: Security and privacy in radio-frequency identification devices. Master thesis, May 2003, Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts (2003)
22. Swedberg, C.: DHL Expects to Launch Sensor Tag Service by Midyear. RFID Journal (January 19th, 2007) Available at `http://www.rfidjournal.com/article/articleprint/2986/-1/1/`
23. Radovanovic, S., Annema, A., Nauta, B.: High-speed lateral polysilicon photodiode in standard CMOS technology. In: ESSDERC'03. 33rd European Solid-State Circuits Conference, September 16-18, 2003, IEEE Computer Society, Los Alamitos (2003)
24. Juels, A., Pappu, R.: Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In: Wright, R.N. (ed.) Financial Cryptography. LNCS, vol. 2742, pp. 103–121. Springer, Heidelberg (2003)
25. Batista, E.: Step Back' for Wireless ID Tech? Wired News (April 8th, 2003), Available at `http://www.wired.com/news/wireless/0,1382,58385,00.html`
26. Karygiannis, T., Eydt, B., Barber, G., Bunn, L., Phillips, T.: 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/`

27. Chan, Y., Meng, M.Q.H., Wu, K.L., Wang, X.: 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 (September 1st-4th, 2005), pp. 7754–7757 (2005)
28. 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`
29. Sarma, S.: Some issues related to rfid and security. Introductory Talk – RFIDSec 06 (July 2006) Available at `http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm`
30. Stajano, F., Anderson, R.J.: The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In: Malcolm, J.A., Christianson, B., Crispo, B., Roe, M. (eds.) Security Protocols. LNCS, vol. 1796, pp. 19–21. Springer, Heidelberg (2000)
31. May, T.C.: Timed-release crypto. Posting to the Cypherpunks Mailing List (February 10th, 1993) Available at `http://cypherpunks.venona.com/date/1993/02/msg00129.html`
32. Juels, A., Syverson, P., Bailey, D.: High-Power Proxies for Enhancing RFID Privacy and Utility. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 210–226. Springer, Heidelberg (2006)
33. Soppera, A., Burbridge, T.: Off by default - RAT: RFID acceptor tag. Printed handout of Workshop on RFID Security – RFIDSec 06, pp. 151–166. ECRYPT Network of Excellence (July 2006)
34. Haselsteiner, E., Breitfuss, K.: Security in near field communication (NFC). Printed handout of Workshop on RFID Security – RFIDSec 06, pp. 151–166. ECRYPT Network of Excellence (July 2006)
35. Brands, S., Chaum, D.: Distance-bounding protocols (extended abstract). In: Helleseth, T. (ed.) EUROCRYPT '93. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
36. Fishkin, K.P., Roy, S., Jiang, B.: Some Methods for Privacy in RFID Communication. In: Castelluccia, C., Hartenstein, H., Paar, C., Westhoff, D. (eds.) ESAS 2004. LNCS, vol. 3313, pp. 42–53. Springer, Heidelberg (2005)
37. Hancke, G., Kuhn, M.: An RFID distance bounding protocol. In: Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005, September 2005, pp. 67–73. IEEE Computer Society, Los Alamitos (2005)
38. Inoue, S., Yasuura, H.: RFID privacy using user-controllable uniqueness. RFID Privacy Workshop (November 2003)
39. Bolotnyy, L., Robins, G.: Multi-tag radio frequency identification systems. In: Workshop on Automatic Identification Advanced Technologies — AutoID, 345 E. 47th St, New York, October, 2005, NY 10017, pp. 83–88 (2005)
40. Rivest, R.L.: Chaffing and Winnowing: Confidentiality without Encryption. CryptoBytes 4(1), 12–17 (1998)
41. Zou, C.C.: PCB: Physically Changeable Bit for Preserving Privacy in Low-End RFID Tags. RFID White Paper Library, RFID Journal (May 2006)