RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management

Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum

Department of Computer Science, Vrije Universiteit, Amsterdam, The Netherlands
{melanie,crispo,ast}@cs.vu.nl

Abstract. RFID tags are tiny, inexpensive, inductively powered computers that are going to replace bar codes on many products, but which have many other uses as well. For example, they will allow smart washing machines to check for incompatible clothes (e.g., white shirts and red socks) and smart refrigerators to check for milk that is too old to be consumed. Subdermal tags with medical information are already being implanted in animals and people. However, a world in which practically everything is tagged and can be read at a modest distance by anyone who wants to buy an RFID reader introduces serious security and privacy issues. For example, women walking down the street may be effectively broadcasting the sizes of their RFID-tagged bras and medical data without realizing it. To protect people in this environment, we propose developing a compact, portable, electronic device called an RFID Guardian, which people can carry with them. In the future, it could be integrated into PDAs or cell phones. The RFID Guardian looks for, records, and displays all RFID tags and scans in the vicinity, manages RFID keys, authenticates nearby RFID readers, and blocks attempted accesses to the user's RFID tags from unauthorized readers. In this way, people can find out what RFID activity is occuring around them and take corrective action if need be.

1 Introduction

Nancy buys a sweater from her favorite department store. This store is her favorite because it has one of those new-fangled checkouts, which automatically tallies up her items and charges the total cost to her credit card. Nancy is not sure exactly how this system works, but she knows that a radio tag attached to the clothing supplies information to the store's computer system. But far more interestingly, this tag can also send instructions to her washing machine at home, which sets the length and temperature of wash cycles, and warns her whenever dark and light clothing are mixed in a single batch of laundry. The store offers a kiosk to disable the tags, but Nancy has never used it. Despite hearing news reports about targeted thefts and stalking, enabled by covert reading of RFID tags, she still does not understand why anyone would want to disable such useful functionality.

This scenario illustrates a typical use of Radio Frequency Identification (RFID), a popular identification and automation technology with serious unaddressed

security and privacy threats. Inductively-powered RFID chips transmit information via radio waves, removing the need for a clear line of sight. These passive tags are powered by their reading devices, eliminating the need for batteries (and their periodic replacement). This quality makes RFID tags useful for a variety of applications. But this usefulness comes at a cost; RFID introduces security and privacy threats that range from unauthorized data access, to snooping on tag-reader communications, to location tracking of physical objects and people. Tag deactivation has been suggested as a way to combat these threats. But a dead tag cannot speak (not even to the washing machine), and this loss of functionality is not always desired by consumers. So other methods of consumer RFID security and privacy protection are needed. Several on-tag security primitives have been proposed, like sleep/wake modes, hash locks, pseudonyms, blocker tags, on-tag cryptography, and tag-reader authentication. The problem is that many of these techniques are not implementable on low-cost Electronic Product Code (EPC) style tags (like that used in Nancy's sweater). Existing techniques also do not yet work cooperatively – they manage the security of individual RFID tags, as opposed to managing the privacy of consumers like Nancy. In the future, existing primitives must be combined to offer a holistic solution for protecting people in an RFID-enabled world.

In this paper, we suggest a new approach for personal security and privacy management called the RFID Guardian. The RFID Guardian is a compact battery-powered device, integratable into Personal Digital Assistants (PDAs) or cellphones, that people carry with them to manage their security and privacy in an RFID-tagged world. The RFID Guardian leverages in-band RFID communications to integrate four previously separate security properties into a single device: auditing, key management, access control, and authentication. This offers some functionality that is totally new within the realm of RFID, and adapts some existing functionality to work in new application scenarios and new combinations.

2 Radio Frequency Identification

Radio Frequency Identification (RFID) is the latest development in the decades-old trend of the miniaturization of computers. Passive RFID transponders are tiny resource-limited computers that are inductively powered by the energy of the request signal sent from RFID readers. Once the RFID tag receives enough energy to "power up" its internal electronics, the tag can decode the incoming query and produce an appropriate response by modulating the request signal using one or more subcarrier frequencies. These RFID tags can do a limited amount of processing, and have a small amount ($<$1024 bits) of storage. Semi-passive and active RFID tags require a battery for their operation, and have accordingly more functionality. However, battery-powered RFID chips present fewer security and privacy challenges than passive ones, so we will focus upon passive RFID throughout the rest of this paper.

RFID tags have become the darling of automation specialists and venture capitalists, due to their battery-free operation. This has led RFID to be used in a variety of applications, including supply chain management, automated payment, physical access control, counterfeit prevention, and smart homes and offices. RFID tags have also been integrated into an ever increasing number of personal and consumer goods including cars, passports, frozen dinners, ski-lift passes, clothing, public transportation tickets, casino chips, and medical school cadavers. Implantable RFID tags for animals allow concerned owners to label their dogs, fish, and livestock. In a logical but controversial next step, RFID has even been used for tagging people. RFID-based monitoring of school children is gaining popularity, amidst a cloud of debate. Trials have already initiated the RFID-tagging of school children in locations as diverse as Japan, India, and California. Even more surprisingly, hundreds of club-goers in three major European cities have voluntarily implanted themselves with RFID chips, about the size of a grain of rice, to pay their bar tabs and gain access to VIP areas. [1] Researchers speculate that these implantable RFID chips could also someday have medical applications.

2.1 Threat Model

Despite the utility of RFID automation, not everyone is happy with the proliferation of RFID tags. Privacy activists warn that pervasive RFID technology might bring unintended social consequences, much in the same way as the automobile and the television. As people start to rely on RFID technology, it will become easy to infer information about their behavior and personal tastes, by observing their use of the technology. To make matters worse, RFID transponders are also too computationally limited to support traditional security and privacy enhancing technologies. This lack of information regulation between RFID tags and RFID readers may lead to undesirable situations. One such situation is unauthorized data collection, where attackers gather illicit information by either actively issuing queries to tags or passively eavesdropping on existing tag-reader communications. So the next time that Nancy purchases an RFID-tagged bra from the department store, she may have no way of controlling which strangers with an RFID reader can read the brand and size information from the RFID tag. Other attacks include the unwanted location tracking of people and objects (by correlating RFID tag "sightings" from different RFID readers), and RFID tag traffic analysis (e.g. terrorist operatives could build a landmine that explodes upon detecting the presence of any RFID tag).

A growing number of countermeasures to these RFID security and privacy threats have been suggested, which fall into different categories: permanent tag deactivation (tag removal, destruction, or SW-initiated tag "killing"), temporary tag deactivation (Faraday cages, sleep/wake modes), on-tag cryptographic primitives (stream ciphers, reduced AES, reduced NTRU), on-tag access control

[1] Some Christian fundamentalists see these implantable RFID chips as a warning sign of the apocalypse.

(hash locks, pseudonyms), off-tag access control (blocker tags), and tag-reader authentication (lighweight protocols, adapted air interfaces). Unfortunately, this rich variety of solutions still faces a number of problems. Current on-tag cryptographic, access control, and authentication proposals require high-end RFID tags for their implementation, leaving the application scenarios that require the cheapest and simplest RFID tags unprotected (e.g. supply chain management). Access control and authentication policies are also commonly distributed across many individual RFID tags, hindering the policy updates that are necessary to protect personal security and privacy in dynamic real-world situations. Some countermeasures are also difficult to use together (e.g. blocker tags cannot provide access control for tags using pseudonyms or hash locks)[7]. This lack of integration is unfortunate because different RFID security and privacy proposals have complimentary strengths and weaknesses, that could be leveraged by using a centralized platform to tie these mechanisms together.

3 RFID Guardian

The RFID Guardian is a platform that offers centralized RFID security and privacy management for individual people. The idea is that consumers who want to enjoy the benefits of RFID-tagging, while still protecting their privacy, can carry a battery-powered mobile device that monitors and regulates their RFID usage.

The RFID Guardian is meant for *personal use*; it manages the RFID tags within physical proximity of a person (as opposed to managing RFID tags owned by the person, that are left at home). For this reason, the operating range of the RFID Guardian must extend at least from the head to toe of the user; a radius of 1-2 meters should be sufficient. This full-body coverage requires the RFID Guardian to be *portable*. It should be PDA-sized, or better yet, could be integrated into a handheld computer or cellphone. The RFID Guardian could then occupy a vacant shirt pocket, handbag, or belt loop, and thus remain close to the person that it is supposed to protect. The RFID Guardian is also *battery powered*. This is necessary to perform resource-intensive security protocols, such as authentication and access control, which would not be possible if the RFID Guardian was implemented on a passive device, like an RFID tag. The RFID Guardian also performs *2-way RFID communications*. It acts like an RFID reader, querying tags and decoding the tag responses. But far more interestingly, the RFID Guardian can also emulate an RFID tag, allowing it to perform direct in-band communications with other RFID readers. As we will see later, this tag emulation capability allows the RFID Guardian to perform security protocols directly with RFID readers.

The heart of the RFID Guardian is that it integrates four previously separate security properties into a single device:

1. Auditing (Discussed in Sect. 3.1)
2. Key management (Discussed in Sect. 3.2)

3. Access control (Discussed in Sect. 3.3)
4. Authentication (Discussed in Sect. 3.4)

Some of these security properties have never been available within the context of RFID before, and other properties have combined or extended existing mechanisms.

3.1 Auditing

Auditing is the act of recording and reviewing events that happen in the world. Just as regulatory bodies might audit corporate finances or mobile telephone usage, the RFID Guardian audits all RFID activity within radio range. RFID auditing serves multiple functions: It acts as a deterrent against abuse, it provides a means to detect illicit activity, and it provides a source of "evidence" to support later correctional measures. The RFID Guardian supports two forms of auditing, *RFID scan logging* and *RFID tag logging*, both of which are new in the context of RFID.

RFID Scan Logging. Nancy's favorite department store has recently discovered that RFID scanning is an excellent way to do targeted advertising ("You recently bought a Prada sweater – maybe you would be interested in buying our matching handbag"). Unfortunately, contrary to local privacy laws, the store manager forgot to put up a sign notifying the customers about the RFID scans.

RFID Scan Logging allows consumers to audit RFID scans in the vicinity. The RFID Guardian uses its "tag emulation" capabilities to listen to and decode the RFID scans in its environment. For each query, it records such information as: command codes, flags, parameters (e.g. RFID tag queried), passed data, and annotations (e.g. timestamp). The RFID Guardian stores this information and displays it upon request, similar to the way Internet firewalls record and display intrusion attempts. This information should ideally be filtered, based upon relevance to the user (e.g. the user's tags are specifically queried). [2] This log of RFID scans then enables the consumer to report illegal RFID scanning to the proper authorities.

RFID Tag Logging. RFID is not always desired by the general public, but its deployment is tolerated because the consumer can always choose to remove or deactivate RFID tags. The only problem is that knowledge of an RFID tag's existence is a necessary precondition for the tag's removal. A stalker could drop an RFID tag into Nancy's purse, or a well-meaning department store could forget to notify her about the RFID tag attached to her new sweater. The result is that, regardless of how it got there, Nancy is now RFID-trackable. And without knowing that the RFID tag is there, she is robbed of her liberty to deactivate it.

[2] Strict filtering and adequate storage space can help mitigate Denial of Service attacks that abuse RFID Scan Logging

RFID Tag Logging offers a solution by alerting individuals about RFID tags that appear "stuck" to them. The RFID Guardian conducts periodic RFID scans, which detect all tags within radio range. It then correlates to find the RFID tags that remain constant across time, and alerts the user of the discovery of these new tags. For example, when Nancy returns home with her sweater at the end of the day, the RFID Guardian can inform her that "one new RFID tag has been added since this morning". The frequency of scanning and tag discovery reports can be increased or decreased, but there is a tradeoff between privacy, accuracy, and battery life. Scanning too infrequently may not discover RFID tags until long after they have compromised the user's privacy. However, scanning often will place high demands on the RFID Guardian's battery, and frequent reporting increases the chance of "false positives".

3.2 Key Management

As RFID technology continues to improve, consumers find themselves with an increasing number of on-tag RFID security mechanisms. Consumers can deactivate and reactivate their RFID tags using kill, sleep, and wake operations, and can perform encryption, decryption, or authentication with crypto-enabled tags (see Sect. 2.1). Each of these on-tag security mechanisms require the use of secret authorization or cryptographic keys. Like most shared secrets, these RFID tag key values must be established, available on-demand, and periodically updated to adequately protect the security of the users.

The RFID Guardian is well suited to manage RFID tag keys for several reasons. First, the RFID Guardian's ability to perform 2-way RFID communications permits key transfer without relying upon the presence of extra non-RFID infrastructure. [3] Additionally, the RFID Guardian serves as a fully-functional RFID reader, so it can use tag keys "on-demand", to activate and deactivate security features on all RFID tags within radio range. Finally, the RFID Guardian can assist with refreshing RFID tag keys, by generating pseudorandom (or truly random) values, and assigning these new values to the appropriate tags with RFID queries. This entropy generation support is useful because some low-cost RFID tags might not be able to generate their own random key material.

3.3 Access Control

Nancy wants her RFID tagged items to work at the proper times; the RFID tag in her sweater must work with her washing machine, and the tags in her groceries must work with her smart refrigerator and microwave. However, Nancy is aware of the privacy risks inherent to RFID, and she does not want her tags to be readable by the entire world. Access control addresses Nancy's concerns by actively controlling which RFID readers can query which RFID tags under which

[3] A secure (encrypted and mutually authenticated) channel is required for RFID tag key transfer between RFID Readers and the RFID Guardian.

circumstances. The RFID Guardian provides granular access control by leveraging three main features: *coordination of security primitives*, *context-awareness*, and *tag-reader mediation*. All of these features are new in the context of RFID.

Coordination of Security Primitives. Nancy's desires reflecting the activity/inactivity of her tags are represented by a security policy, which is enforced by one or multiple access control mechanisms. In other words, Nancy has a variety of tools (e.g. hash locks, sleep/wake modes, pseudonyms) that she can use to restrict access to her RFID tags. Each access control mechanism has advantages and shortcomings that make it appropriate (or inappropriate) for specific application scenarios. Since a person's situation is constantly changing, the user should be able to leverage these mechanisms in a coordinated fashion, so they can fit application constraints at any given moment while enforcing a unified security policy. No tool currently exists that can automate this process, and people do not have the ability nor the patience to use these various mechanisms manually. The RFID Guardian fills this void by offering an integrated framework for the automated management of RFID security and privacy mechanisms.

The use of a unified security policy departs from the predominant approach of decentralized RFID security, which solely considers the security needs of individual RFID tags. Centralized policies, as used in the RFID Guardian, can manage the RFID privacy of physical entities, including that of individual users and fixed locations (e.g. protecting a supermarket from the competing grocer's RFID readers). Another benefit of centralized access control is ease of management, as it eliminates the need for the propagation and synchronization of security policy updates. The main disadvantage of centralized access control is that only RFID tags within of the operating range of the RFID Guardian will receive protection.

Context-Awareness. When Nancy leaves the protective haven of her house in the morning, the RFID tags on her person are exposed to an increased amount of risk. Accordingly, Nancy expects that RFID Guardian will then tighten the access control of these RFID tags. The RFID Guardian is specially designed to adapt access control settings to reflect the reality of a person's current situation. However, the RFID Guardian is only able to make these adjustments after it first perceives the situation itself. So a form of context-awareness is necessary.

Context is a fuzzy term that is used a lot in ubiquitous computing, which essentially refers to the situation that the user is in. There are two major ways in which the RFID Guardian can detect a person's context. First, the RFID Guardian can infer its own context information. For example, the RFID Guardian might be able to detect its location, using GPS or WiFi triangulation, or it could make note of the local time. Other kinds of context can also be detected, but the more "fuzzy" the context is, the harder it becomes to detect it, and to subsequently decide how to respond to it. Second, the RFID Guardian can receive context information from RFID readers. In this case, RFID readers send the RFID Guardian textual "context updates", which consist of an arbitrary

string of data that represents some situation. For example, the RFID reader at the front door of Nancy's house could send her RFID Guardian a message, informing it that it is leaving her property. While context updates are easier to use than context inference, there are there are still problems. Any untrusted RFID reader can send a context update, so it is necessary to use authentication to check the origin of these updates (see Sect. 3.4). Another problem of relying upon context updates is that, if the RFID Guardian is not in the vicinity of an RFID reader, it has no way of being able to determine its context.

Tag-Reader Mediation. Nancy decides that she doesn't want the department store to be able to access the RFID tags on her clothing anymore, so she modifies her preferences on the RFID Guardian. The RFID Guardian could propagate the policy updates to the RFID tags themselves (assuming that the RFID tags have their own security mechanisms, which many might not). However, another option is for the RFID Guardian to act as a "man-in-the-middle", mediating interactions between RFID readers and RFID tags. This centralizes the decision making in the RFID Guardian, and leaves the RFID tags free to perform their application-specific functions, without burning valuable power on making security decisions. Mediation can take either a constructive or destructive form, which is illustrated by the two opposing concepts of "RFID Proxy Functionality" and "Selective RFID Jamming".

RFID Proxy Functionality is an example of constructive mediation where the RFID Guardian forwards cryptographically-protected queries to RFID tags on the behalf of untrusted RFID readers. By mediating RFID tag access, RFID Proxy Functionality both enables per-usage security negotiations between the RFID Guardian and RFID readers, and also reduces the need for the revocation of cryptographic RFID tag keys (since RFID readers never have the tag keys to begin with.) Here is how RFID Proxy Functionality works: An untrusted RFID reader passes a request for a desired query to the RFID Guardian, preferably over a secure channel. Upon the successful completion of a possibly complex security negotiation, the RFID Guardian then re-issues the query in encrypted form, on the behalf of the RFID reader. The RFID Guardian then receives the encrypted tag response, decrypts it, and forwards the response to the RFID reader that requested it. Prerequisites for RFID Proxy Functionality are cryptographically-enabled RFID tags, the centralized storage of RFID tag keys (see Sect. 3.2), and 2-way RFID communications between the RFID Guardian and RFID readers (see Sect. 3). Unfortunately, RFID Proxy Functionality will not work with low-cost RFID tags that are too cheap to support the required on-tag security mechanisms.

Selective RFID Jamming is an example of destructive mediation where the RFID Guardian blocks unauthorized RFID queries on the behalf of RFID tags. By filtering RFID queries, Selective RFID Jamming provides off-tag access control for low-cost RFID tags that are not powerful enough to support their own on-tag access control mechanisms. Selective RFID Jamming is a new technique, which is inspired by the RFID Blocker Tag by Juels, Rivest, and Szydlo.[9]. Here

is how Selective RFID Jamming works: An RFID reader sends a query to an RFID tag, and the RFID Guardian captures and decodes the query in real-time. It then determines whether the query is permitted, and if the query is not allowed, the RFID Guardian sends a jamming signal that is just long enough to block the RFID tag response. Selective RFID Jamming differs from the RFID Blocker Tag in that it is implemented on battery-powered mobile devices, and that it uses Access Control Lists, source authentication (see Sect. 3.4), and a randomized jamming signal. (The paper [11] offers a detailed explanation of Selective RFID Jamming.) Selective RFID Jamming has a number of problems. First, its use is legally questionable, since it is conceivably a form of signal warfare. Secondly, the use of jamming may have an adverse affect on surrounding RFID systems, if not used sparingly. And third, malicious RFID readers can abuse Selective RFID Jamming by repeatedly performing unauthorized queries. This Denial of Service attack would cause both a flurry of jamming signals, and a major drain on the battery of the RFID Guardian. For these reasons, it is preferable to use other forms of access control, so long as the application scenario permits it.

3.4 Authentication

Access control regulates which RFID readers can access which RFID tags under which circumstances. However, this mechanism needs a reliable way to determine which reader is sending any given RFID query. Some RFID tags can perform direct authentication with RFID readers, but they cannot convey the authentication results to higher-level RFID privacy management systems. In contrast, the RFID Guardian offers "off-tag authentication" by authenticating RFID readers on the behalf of the RFID tags, and directly supporting the access control methods from the previous section.

RFID Guardian-reader authentication should be implemented over the two-way RFID communications channel (see Sect. 3), using any standard challenge-response algorithm that is widely implemented and understood. This challenge-response should support both one-way and mutual authentication, to address the risk of foreign RFID Guardians. The authentication protocol is always initiated by the RFID reader, since it requests RFID tag access asynchronously from the RFID Guardian. A key distribution scheme is also necessary to facilitate the exchange of shared keys between the RFID Guardian and RFID readers. Key pre-establishment is useful for swapping keys with RFID readers that the user plans to have a lasting relationship with (e.g. the neighborhood supermarket), and this key exchange could occur using a variety of out-of-band means. On-the-fly key distribution, on the other hand, is useful when the RFID Guardian wants to establish a temporary trust relationship with an unfamiliar RFID reader. For example, Nancy may want her RFID Guardian to perform a transaction with an RFID reader located at the supermarket that she happens to be visiting. On-the-fly key distribution could use in-band or out-of-band communications, and may even rely upon a supporting Public Key Infrastructure.

4 Related Work

Many RFID security and privacy techniques exist, but there is nothing in the state-of-the-art that provides all of the security properties of the RFID Guardian. Two-way RFID communications have been investigated by MIT's Auto-ID lab, which have designed an RFID tag emulator called the 'RFID Field Probe'. A semi-passive RFID tag is used to perform real-time diagnostics on RFID equipment, and their planned 'third generation' field probe will communicate RF field values back to the RFID Reader, using in-band RFID protocols.[10] RFID auditing has been preliminarily investigated by c't magazine, who's RFID Detektor[1] lights an LED to indicate the presence of any RFID activity. RFID tag key management hasn't been systematically addressed until this point, beyond a few suggestions to transfer RFID tag keys by printing keys on cash register receipts, saving keys on smart cards, emailing keys, sending keys to a PDA using non-RFID communications. Each of these methods are less usable than the RFID tag key management that the RFID Guardian provides.

RFID tag-reader authentication, access control, and cryptography schemes provide potentially useful tools for the RFID Guardian to leverage and coordinate. Vajda and Buttyan offer lightweight authentication protocols [12], and Weis, et. al, proposed a randomized hash lock protocol for authentication[13]. Feldhofer, et. al, proposes an extension to the ISO 18000 protocol, that would enable the in-band transmission of authentication data [3]. RFID access control mechanisms include tag deactivation, which was standardized by the EPCglobal consortium [2]. Juels also suggests the use of dynamic tag identifiers, called pseudonyms, that use a mechanism called "pseudonym throttling" to allow authenticated RFID readers to refresh the pseudonym list. [8] Juels, Rivest, and Szydlo also propose the RFID Blocker Tag, that interferes with RFID Readers by "spoofing" the RFID Reader's tree-walk singulation protocol.[9] Some cryptography is also suitable for the limited resources of RFID tags. Finkenzeller describes the use of stream ciphers, [5], and Feldhofer, et. al, describes a low-cost AES implementation, simulated to work in RFID tags. [4] Gaubatz, et. al, also describe a low cost NTRU implementation, designed for sensor networks, that brings public key cryptography closer to fitting the constraints of RFID [6].

5 Conclusion and Future Work

The RFID Guardian is a new approach for personal RFID security and privacy management. It is a compact battery-powered device, that ordinary people can carry with them in RFID-tagged environments. The RFID Guardian leverages in-band RFID communications to integrate four previously separate security properties into a single device: auditing, key management, access control, and authentication. This offers some functionality that is totally new within the realm of RFID, and facilitates the coordinated usage of existing RFID security and privacy mechanisms.

The RFID Guardian has a number of issues that require further research. The bulk of our future work includes designing the security protocols that will

hold this entire RFID personal privacy management architecture together. A big problem is that the RFID Guardian is a single point of failure. Anyone who compromises the Guardian has total control over the RFID tags, whether it is lost or taken over by a hostile entity. This can be improved by using PIN codes to lock the device, and synchronizing the information on the RFID Guardian with trusted fixed location (e.g. home-based) RFID systems. Lastly, we are currently working on an implementation of the RFID Guardian, which will be used to test and extend the ideas in this paper.

References

1. c't magazine, *Bauanleitung fur einen simplen rfid-detektor*, (2004), no. 9.
2. EPCglobal, *13.56 MHz ISM band class 1 radio frequency (RF) identification tag interface specification*.
3. Martin Feldhofer, *An authentication protocol in a security layer for RFID smart tags*, The 12th IEEE Mediterranean Electrotechnical Conference, vol. 2, IEEE, May 2004, pp. 759–762.
4. Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, Workshop on Cryptographic Hardware and Embedded Systems, LNCS, vol. 3156, IACR, Springer-Verlag, Aug 2004, pp. 357–370.
5. Klaus Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, John Wiley & Sons, Ltd., 2003.
6. G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, *State of the art in public-key cryptography for wireless sensor networks*, Proceedings of the Second IEEE International Workshop on Pervasive Computing and Communication Security, 2005.
7. Jan E. Hennig, Peter B. Ladkin, and Bernd Sieker, *Privacy enhancing technology concepts for RFID technology scrutinised*, Research Report RVS-RR-04-02, University of Bielefeld, D-33501 Bielefeld, Germany, Oct 2004.
8. Ari Juels, *Minimalist cryptography for low-cost RFID tags*, The Fourth International Conference on Security in Communication Networks, LNCS, Springer-Verlag, September 2004.
9. Ari Juels, Ronald L. Rivest, and Michael Szydlo, *The blocker tag: Selective blocking of RFID tags for consumer privacy*, Proceedings of the 10th ACM Conference on Computer and Communications Security, ACM Press, 2003.
10. Rich Redemske, *Tools for RFID testing and measurement*, 2005.
11. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, *Keep on blockin' in the free world: Personal access control for low-cost RFID tags*, 13th International Workshop on Security Protocols, Apr 2005.
12. István Vajda and Levente Buttyán, *Lightweight authentication protocols for low-cost RFID tags*, Second Workshop on Security in Ubiquitous Computing, October 2003.
13. Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, Security in Pervasive Computing, LNCS, vol. 2802, 2004, pp. 201–212.